# ОСНОВНЫЕ РЕЗУЛЬТАТЫ
анализа законодательства зарубежных государств и Российской Федерации в области управления данными, описания моделей правового регулирования управления данными

Москва 2019

СОДЕРЖАНИЕ

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем отчете применяют следующие термины с соответствующими определениями

Государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов

Доступ к информации – возможность получения информации и ее использования

Защита информации – принятие и реализация комплекса правовых, организационных и технических мер по определению, достижению и поддержанию конфиденциальности, целостности и доступности информации и средств ее обработки с целью исключения или минимизации неприемлемых рисков для субъектов информационного взаимодействия

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

Информация – сведения (сообщения, данные) независимо от формы их представления

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право

разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

Оборот данных – совокупность действий в процессе электронного обмена данными между участниками обмена данными, их информационными системами

Открытые данные – информация (в том числе документированная), созданная в пределах их полномочий государственными органами, либо поступившая в указанные органы и организации, а также информационно-аналитическими организациями, участвующими в публикации собственных открытых данных на территории Российской Федерации, которая подлежит размещению в сети Интернет в формате, обеспечивающем ее автоматическую обработку в целях повторного использования без предварительного изменения человеком (машиночитаемый формат) и может свободно использоваться в любых соответствующих закону целях любыми лицами независимо от формы ее размещения (простая совокупность сведений, база данных и т.д.)

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

Участники обмена (оборота) данными – органы и (или) лица, осуществляющие определенную совокупность действий в процессе электронного обмена данными и представляющие собой источник и/или приемник электронных данных

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем отчете применяют следующие сокращения и обозначения

5G − Fifth generation (Пятое поколение)

ABS − Australian Bureau of Statistics (Австралийское бюро статистики),

ANAO − Australian National Audit Office (Австралийское государственное ревизионное управление)

API − Application programming interface (Интерфейс прикладного программирования

APP − Australian Privacy Principles (Принципы неприкосновенности частной жизни Австралии)

ATO − Australian Taxation Office (Австралийское налоговое управление)

B2B − Business-to-business (бизнес − бизнесу)

B2G − Business-to-government (бизнес − правительству)

BDSG − Bundesdatenschutzgesetz (Федеральный закон о защите данных, Германия)

CDR − Consumer Data Right (Права на потребительские данные)

CGefI − Contrôle général économique et financier (Департамент общего экономического и финансового контроля, Франция)

CNIL − La Commission nationale de l'informatique et des libertés (Национальная комиссия информационных технологий и свобод, Франция)

CSIRO − Commonwealth Scientific and Industrial Research Organisation (Содружества по научным и промышленным исследованиям, Австралия)

CSIRT − Computer security incident response team (Команда компьютерной безопасности по реагированию на инциденты, ЕС)

CSV − Comma−Separated Values (значения, разделённые запятыми)

DESI − The Digital Economy and Society Index (Индекс цифровой экономики и общества)

DHS − Department of Human Services (Департамент социальных служб, Австралия)

DINSIC − Direction interministérielle du numérique et du système d'information et de communication de l'État (Межведомственная дирекция по управлению национальными информационными системами, Франция)

DIPA − Data Integration Partnership for Australia (Партнерство по интеграции данных для Австралии)

DSML − Directory Services Markup Language (Язык разметки служб каталогов)

DVA− Department of Veterans' Affairs (Департамент по делам ветеранов, Австралия)

EPSG − European Petroleum Survey Group (Европейская нефтепоисковая группа)

EPUB − Electronic Publication (Открытый формат электронных версий книг)

ETRS − European Terrestrial Reference System (Европейская земная система координат)

FISMA − Federal Information Security Modernization Act (Федеральный закон о модернизации информационной безопасности, США)

FTC − Federal Trade Commission (Федеральная торговая комиссия, США)

GDPR − General Data Protection Regulation/(Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Общий регламент по защите данных/ Регламент Европейского Парламента и Совета 2016/679 of 27 апрелял 2016 г.)

HTML − Hypertext Markup Language (язык гипертекстовой разметки)

HTTP − HyperText Transfer Protocol (протокол передачи гипертекста)

ICO − Information Commissioner's Office (Управление комиссара по вопросам информации, Великобритания)

ICT − Information and Communication Technologies (Информационно−коммуникационные технологии)

IEC − International Electrotechnical Commission (Международная электротехническая комиссия

INSPIRE − Infrastructure for Spatial Information in the European Community (Инфраструктура для пространственной информации в ЕС)

ISO− International Organization for Standardization (Международная организация по стандартизации)

IT − Information Technology (Информационные технологии)

IWG − Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen − (Закон о повторном использовании информации государственного сектора, Германия)

LAPSI − Legal aspects of (reusing) public sector information (Правовые аспекты (повторного использования) информации государственного сектора)

LDAP − Lightweight Directory Access Protocol (Легко расширяемый протокол доступа к каталогам)

MADIP − Multi-Agency Data Integration Project (Проект мульти-агентской интеграции данных, Австралия)

MAGDA − Making Australian Government Data Available (информационная платформа Австралии « Обеспечение доступности данных правительства Австралии»)

NGISS − National Government Information Sharing Strategy (Национальная правительственная стратегия обмена информацией)

NIEM − National Information Exchange Model (Национальная модель обмена информацией)

NLR-T − New Land Registry - Titles (Новый реестр земель - Титулы, Австралия)

NRI – Networked Readiness Index (Индекс сетевой готовности)

OAIC − Office of the Australian Information Commissioner (Управления австралийского комиссара по информации)

ODF − Open Document Format (открытый формат документов)

OGL − Open Government License (Открытая государственная лицензия)

OOXML − Office Open XML (Серия форматов файлов для хранения электронных документов пакетов офисных приложений)

OSA − Official Secrets Act (Закон о государственной тайне, Сингапур),

OSCI − Online Services Computer Interface (Компьютерный интерфейс онлайн-сервисов)

PDF − Portable Document Format (Формат переносимого документа)

PDF/A − Portable Document Format/Archive (Формат переносимого документа/Архив)

PDPA − Personal Data Protection Act (Закон о защите персональных данных, Сингапур)

RGI − Référentiel Général d'Interopérabilité (Справочная информация по системам взаимодействия, Франция)

SSN − Social Security number (Номер социального страхования),

STIX − Structured Threat Information Expression (структурированное представление информации об угрозах)

TAXII − Trusted Automated eXchange of Indicator Information (Доверенный автоматизированный обмен информацией об индикаторах),

TMG − Telemediengesetz (Закон о телемедиа, Германия)

U.S.C. − United States Code (Кодекс Соединённых Штатов Америки

URL − Uniform Resource Locator (унифицированный указатель ресурса)

UTF − Unicode Transformation Format (формат преобразования Юникода)

WGS − World Geodetic System (Всемирная система геодезических параметров Земли)

WofG − Whole-of-government approach (Общегосударственный подход)

XML − Extensible Markup Language (расширяемый язык разметки)

АБС − Австралийское бюро статистики

АБУ − Административно-бюджетное управление США

ВСНП − Всекитайское Собрание Народных Представителей

ВТО − Всемирная торговая организация

ГДР − Германская Демократическая Республика

ГИС − Государственная информационная система

ЕАЭС − Евразийский экономический союз

ЕС − Европейский Союз

ЕСИА − Единая система идентификации и аутентификации

ЕСПЧ − Европейский суд по правам человека

ИКТ − Информационно-коммуникационные технологии

ИТ − Информационные технологии

КИИ − Критическая информационная инфраструктура

КНР − Китайская Народная Республика

МВД − Министерство внутренних дел

МЧС − Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий

ОАЭ − Объединенные Арабские Эмираты,

ООН − Организация Объединенных Наций

ОЭСР − Организация экономического сотрудничества и развития

США − Соединенные Штаты Америки

ТЭК − Топливно-энергетический комплекс

ФСБ − Федеральная служба безопасности Российской Федерации

ФСКН − Федеральная служба Российской Федерации по контролю за оборотом наркотиков

ФСТЭК − Федеральная служба по техническому и экспортному контролю

ФТС − Федеральная таможенная служба

ЭВМ − Электронно-вычислительная машина

# ВВЕДЕНИЕ

В условиях формирования цифрового государства увеличивается объем информации, представленной в цифровой форме и содержащейся в государственных информационных системах, а также иной информации, находящейся в распоряжении государственных органов. Усложняется информационный обмен в государственном секторе. Информация, представленная в цифровой форме, и результаты ее автоматизированной обработки вытесняют бумажный документооборот при принятии государственными органами юридически значимых решений.

Во исполнение Указа Президента Российской Федерации от 7 мая 2018 г. № 204 и в целях реализации национальной программы «Цифровая экономика Российской Федерации» (далее – Программа), утвержденной президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 24 декабря 2018 г. № 16, в рамках формирования национальной системы управления данными планируется утверждение единых требований к управлению данными и их жизненным циклом, в том числе требования к систематизации, кодированию, качеству и безопасности данных в национальных реестрах, включающих перевод накопленной архивной информации в бумажном виде в реестровую модель, а также механизма по обновлению требований. Данные требования совместно с разработанным планом-графиком перехода должны обеспечить взаимное соответствие и нормализацию данных, используемых при межведомственном электронном взаимодействии, в информационных ресурсах государственных органов власти, единство форматов и атрибутов данных, автоматизацию процессов межведомственного взаимодействия при оказании государственных услуг и исполнение функций федеральными органами исполнительной власти.

В соответствии с Концепцией создания и функционирования национальной системы управления данными, утвержденной распоряжением Правительства Российской Федерации от 3 июня 2019 г. № 1189-р, под

государственными данными понимается информация, содержащаяся в информационных ресурсах органов и организаций государственного сектора, а также в информационных ресурсах, созданных в целях реализации полномочий органов и организаций государственного сектора. При этом управление государственными данными определяется, как совокупность процессов сбора, хранения, обработки, предоставления, распространения и уничтожения государственных данных, обеспечения качества государственных данных, включая их систематизацию и гармонизацию.

Указанные определения терминов «государственные данные» и «управление государственными данными» не являются легальными правовыми дефинициями и отражают управленческий взгляд на происходящие в настоящее время процессы оптимизации и развития менеджмента данных в государственном секторе. В то же время указанные процессы влияют на развитие отечественного законодательства. Так, в соответствии с Концепцией создания и функционирования национальной системы управления данными и планом мероприятий («дорожной картой») по созданию национальной системы управления данными, утвержденной распоряжением Правительства Российской Федерации от 3 июня 2019 г. № 1189-р, предусмотрена разработка проекта федерального закона о национальной системе управления данными, которая в настоящее время трансформирована в разработку проекта федерального закона о внесении изменений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации. При этом наряду с разработкой указанного законопроекта предполагается разработка и иных нормативных правовых актов, принятие которых потребуется в целях обеспечения актуальности, достоверности, целостности и иных характеристик государственных данных при управлении ими, которая будет осуществляться в рамках отдельных правительственных планов и «дорожных карт».

В результате одновременно с совершенствованием управления данными в государственном секторе существуют предпосылки для развития правового регулирования в публично-правовой сфере, связанной с формированием, хранением, использованием данных, предоставлением доступа к ним и иными способами их обработки в государственном секторе. Данные изменения, которые активно происходят не только в Российской Федерации, но и в зарубежных государствах, требуют правового осмысления.

# 1 Краткий обзор национального законодательства зарубежных государств с выявлением зарубежных государств — лидеров правового регулирования в области управления данными

## 1.1 Анализ международных рейтингов в области управления данными

### 1.1.1 Рейтинги государств в области управления данными

Проведенные в последнее время международные рейтинги государств в области управления данными в зависимости от применяемой методики определяют государства-лидеры в данной области. Среди рейтингов следует выделить:

– рейтинг на основе индекса сетевой готовности (NRI) Всемирного экономического форума,

– рейтинг развития электронного правительства (E-government development rank) Организации Объединенных Наций,

– рейтинг на основе индекса цифровой экономики Европейской Комиссии (I-DESI),

– рейтинг на основе индекса Digital Economies Vary Across the World (DEVAW),

– рейтинг мировой цифровой конкуренции (The IMD World Digital Competitiveness Ranking).

### 1.1.2 Рейтинг государств в соответствии с индексом сетевой готовности[1]

[1] Данный рейтинг опубликован в составе доклада Всемирного экономического форума – Глобальный доклад об информационных технологиях 2016 г. Инновации в цифровой экономике (The Global Information Technology Report 2016. Innovating in the Digital Economy)World Economic Forum. The Global Information Technology Report 2016. Innovating in the Digital Economy. URL: http://reports.weforum.org/global-information-technology-report-2016/ (дата обращения 01.08.2019)

В данном рейтинге оценивается состояние сетевой готовности 139 стран мира на основе использования индекса сетевой готовности (Networked Readiness Index, NRI).

Индекс сетевой готовности рассчитывается на основе системы сводных и элементарных показателей, включающей:

A. Субиндекс среды:

1. Политические и регуляторные условия (9 показателей);

2. Бизнес- и инновационные условия (9 показателей);

B. Субиндекс готовности:

3. Инфраструктура (4 показателя);

4. Экономической доступности (3 показателя);

5. Навыки (4 показателя);

C. Субиндекс использования:

6. Индивидуальное использование (7 показателей);

7. Использование в бизнесе (6 показателей);

8. Использование правительством (3 показателя);

D. Субиндекс воздействия:

9. Экономическое воздействие (4 показателя);

10. Воздействие на социальную сферу (4 показателя).

С точки зрения отбора зарубежных государств для исследования опыта правового регулирования управления данными наиболее репрезентативным в системе рейтингования на основе индекса сетевой готовности (NRI) является показатель 1.02 Законы в области информационно-коммуникационных технологий (1.02 Laws relating to ICTs). Указанный показатель оценивает степень развития законодательного регулирования в области информационно-коммуникационных технологий. Страны, занимающие лидирующее положение в соответствии с указанным показателем по состоянию на 2015 г., показаны на рисунке 1.

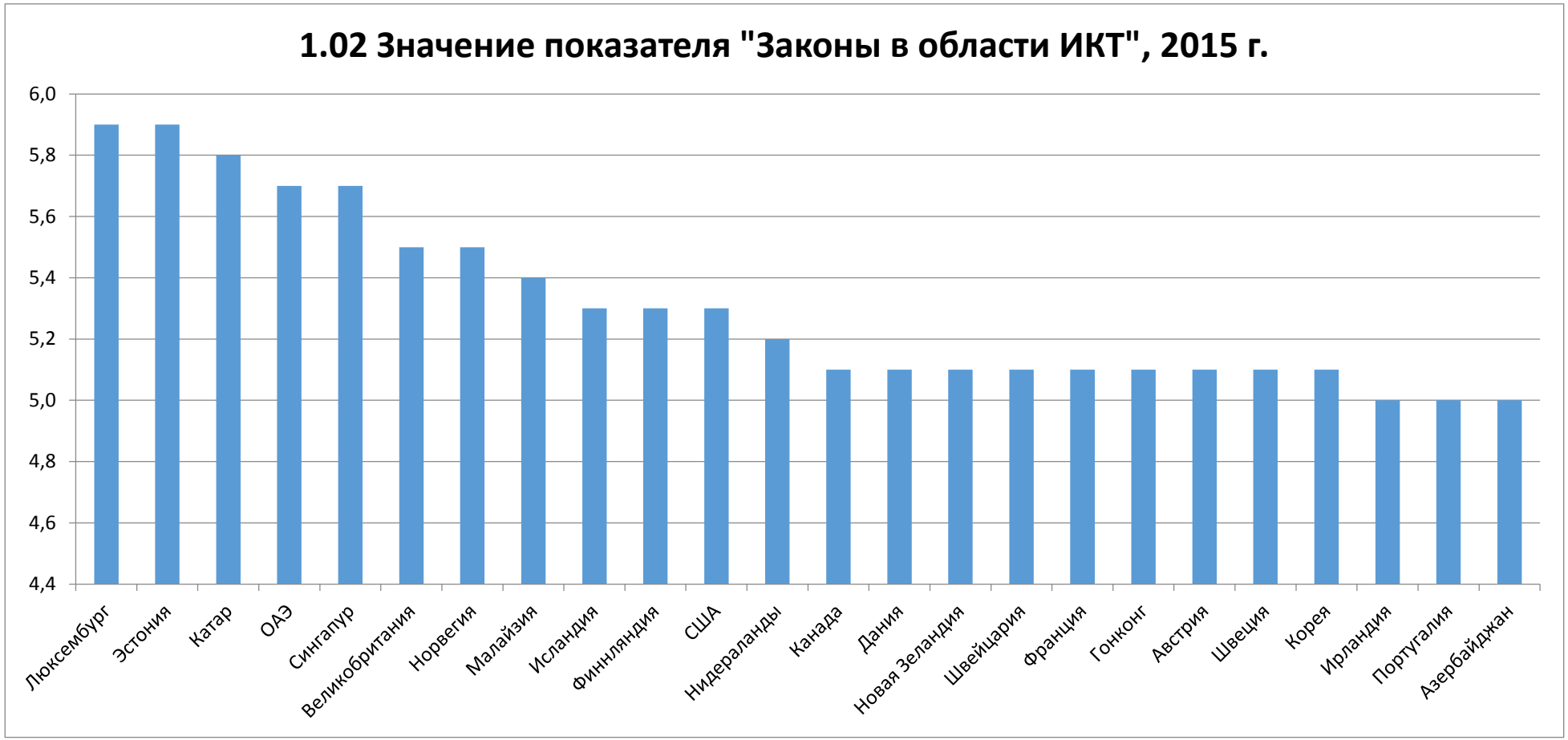


Рисунок 1 − Оценка лидирующих стран мира по показателю «1.02 Законы, относящиеся к информационно-коммуникационным технологиям» (по состоянию на 2015 г.)

В соответствии с показателем «1.02 Законы, относящиеся к информационно-коммуникационным технологиям» в системе рейтингования на основе индекса сетевой готовности (NRI) лидирующими государствами являются:

– Люксембург,
– Эстония,
– Катар,
– ОАЭ,
– Сингапур,
– Великобритания,
– Норвегия,
– Малайзия,
– Исландия,
– Финляндия,
– США.

1.1.3 Рейтинг развития электронного правительства (E-government development rank)[2]

Система рейтингования развития электронного правительства (E-government development rank) основана на применении индекса развития электронного правительства (E-Government Development Index) и охватывает государства-члены ООН.

Рассматриваемая система рейтингования предусматривает разделение стран по уровню развития электронного правительства на четыре группы: очень высокий уровень, высокий уровень, средний уровень, низкий уровень.

---

[2] Источником данных для приведенных в настоящем разделе рейтингов является Доклад ООН «UN E-Government Survey» 2018. United Nations. UN E-Government Survey 2018. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018 (дата обращения 01.08.2019)

Рейтинг ведущих стран по индексу электронного правительства по состоянию на 2018 г. представлен на рисунке 2.

В соответствии с индексом развития электронного правительства в системе рейтингования ООН лидирующими государствами являются:

– Дания,
– Австралия,
– Республика Корея,
– Великобритания,
– Швеция,
– Финляндия,
– Сингапур,
– Новая Зеландия,
– Франция,
– Япония,
– США,
– Германия.

1.1.4 Рейтинг государств в соответствии с индексом цифровой экономики[3]

Система рейтингования «Индекс цифровой экономики и общества» (The Digital Economy and Society Index (DESI) основана на применении индекса, который агрегирует соответствующие показатели эффективности цифрового развития в Европейском союзе и отслеживает эволюцию конкурентоспособности стран Европы в области цифровых технологий.

[3] Рейтинг опубликован в Докладе об индексе цифровой экономики и обществе 2018 (Digital Economy and Society Index Report 2018 Report). European Commission. Digital Economy and Society Index 2018 Report. https://digital-agenda-data.eu/charts/desi-composite#chart={%22indicator%22:%22desi_sliders%22,%22breakdown%22:{%22desi_1_conn%22:5,%22desi_2_hc%22:5,%22desi_3_ui%22:3,%22desi_4_idt%22:4,%22desi_5_dps%22:3},%22unit-measure%22:%22pc_desi_sliders%22,%22time-period%22:%222018%22} (дата обращения 01.08.2019)

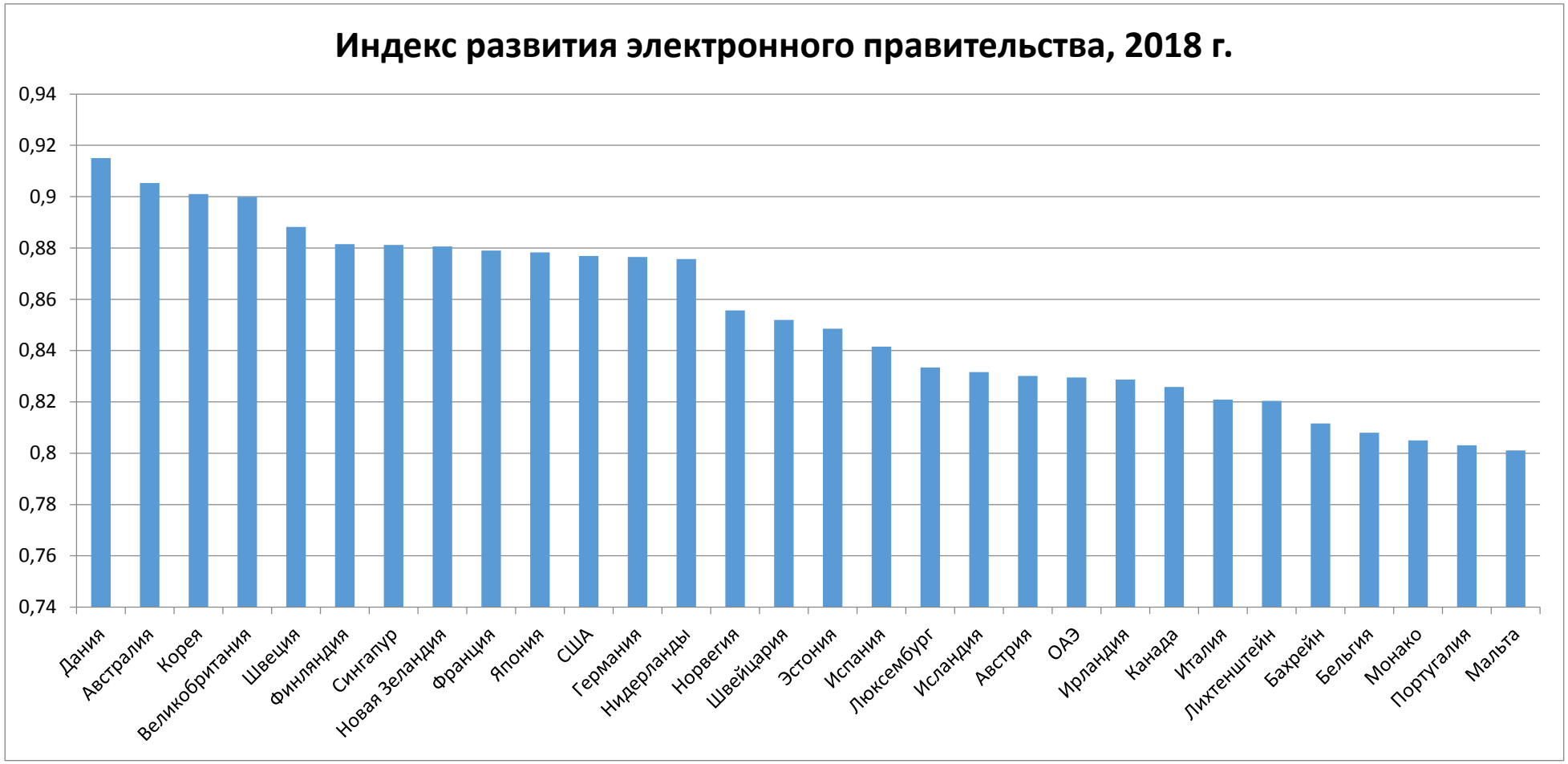


Рисунок 2 − Оценка стран-членов ООН по индексу развития электронного правительства (по состоянию на 2018 г.)

Расчет индекса DESI строиться на значениях показателей, оценивающих:

- связность,
- человеческий капитал,
- использование интернет-сервисов,
- интегрированность цифровых технологий,
- общественные цифровые сервисы.

Рейтинг стран Европейского союза в соответствии с индексом DESI по состоянию на 2018 г. показан на рисунке 3.В соответствии с индексом DESI лидирующими государствами являются:

- Швеция,
- Нидерланды,
- Финляндия,
- Дания,
- Люксембург,
- Великобритания,
- Эстония,
- Ирландия,
- Бельгия,
- Мальта.

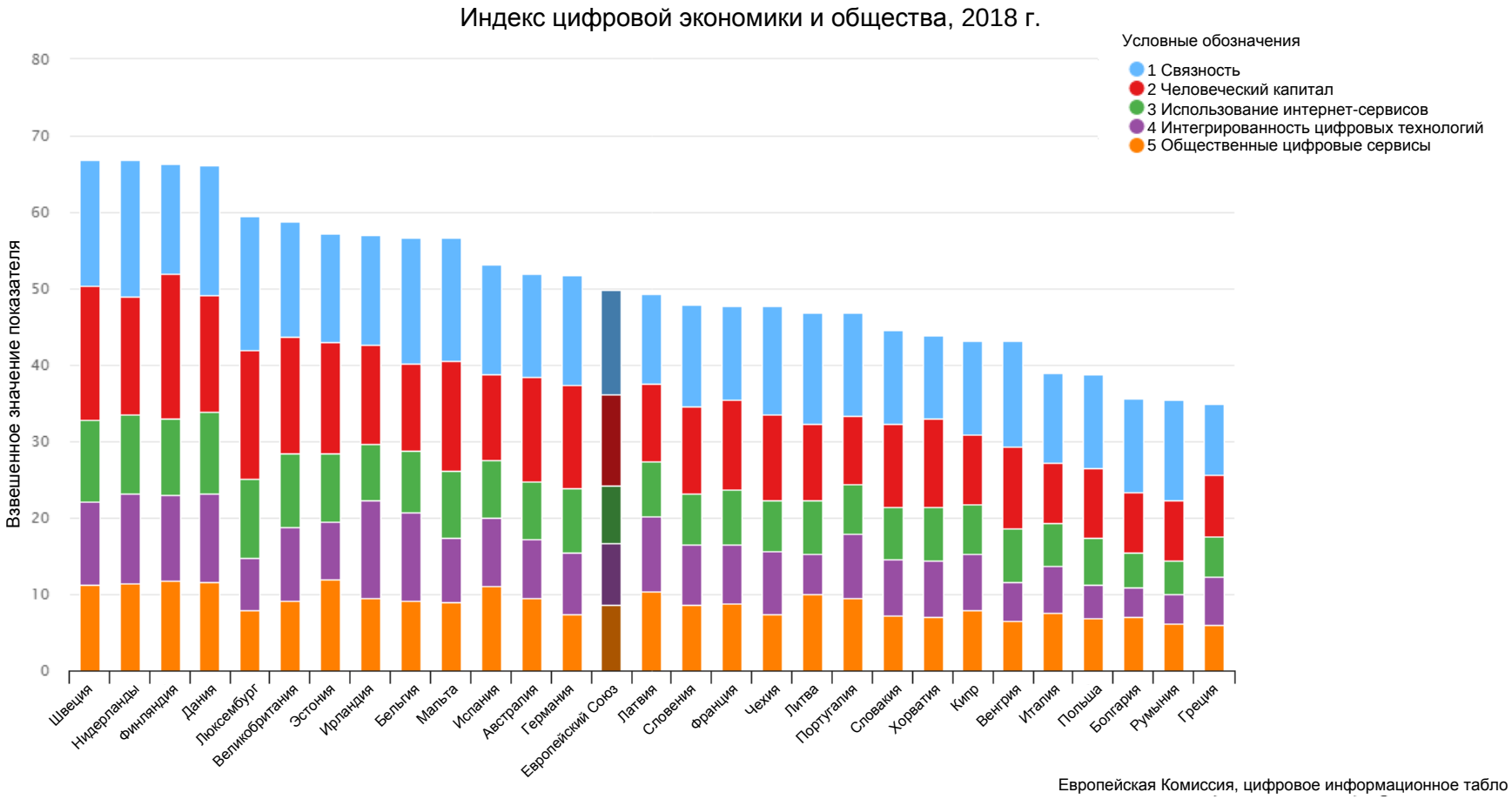


Рисунок 3 − Оценка стран Европейского Союза по индексу цифровой экономики и общества (DESI)

(по состоянию на 2018 г.)

1.1.5 Рейтинг государств в соответствии с индексом «Изменение цифровых экономик во всем мире» (Digital Economies Vary Across the World, DEVAW)[4]

Система рейтингования «Индекс оценки цифровизации: как конкурентоспособность и доверие к цифровой экономике различаются по всему миру» (Digital Evolution Index: How Competitiveness And Trust In Digital Economies Vary Across The World) включает оценивание государства по индексам оценки состояния цифровизации экономик и темпа развития цифровизации экономик.

Рейтинг стран в соответствии с вышеуказанными индексами по состоянию на 2017 г. представлен на рисунках 4 и 5. В соответствии с индексом оценки состояния цифровизации экономик лидирующими государствами являются:

– Норвегия,
– Швеция,
– Швейцария,
– Дания,
– Финляндия,
– Сингапур,
– Республика Корея,
– Великобритания,
– Гонконг,
– США.

---

[4]Указанный рейтинг опубликован в Докладе исследовательского университета Тафтса «Цифровая планета 2017. Как конкурентоспособность и доверие к цифровой экономике различаются по всему миру» (Digital Planet 2017. How competitiveness and trust in digital economies vary across the world) The Fletcher School, Tufts University. Digital Planet 2017. How competitiveness and trust in digital economies vary across the world. https://sites.tufts.edu/digitalplanet/files/2017/05/Digital_Planet_2017_FINAL.pdf (дата обращения 01.08.2019)

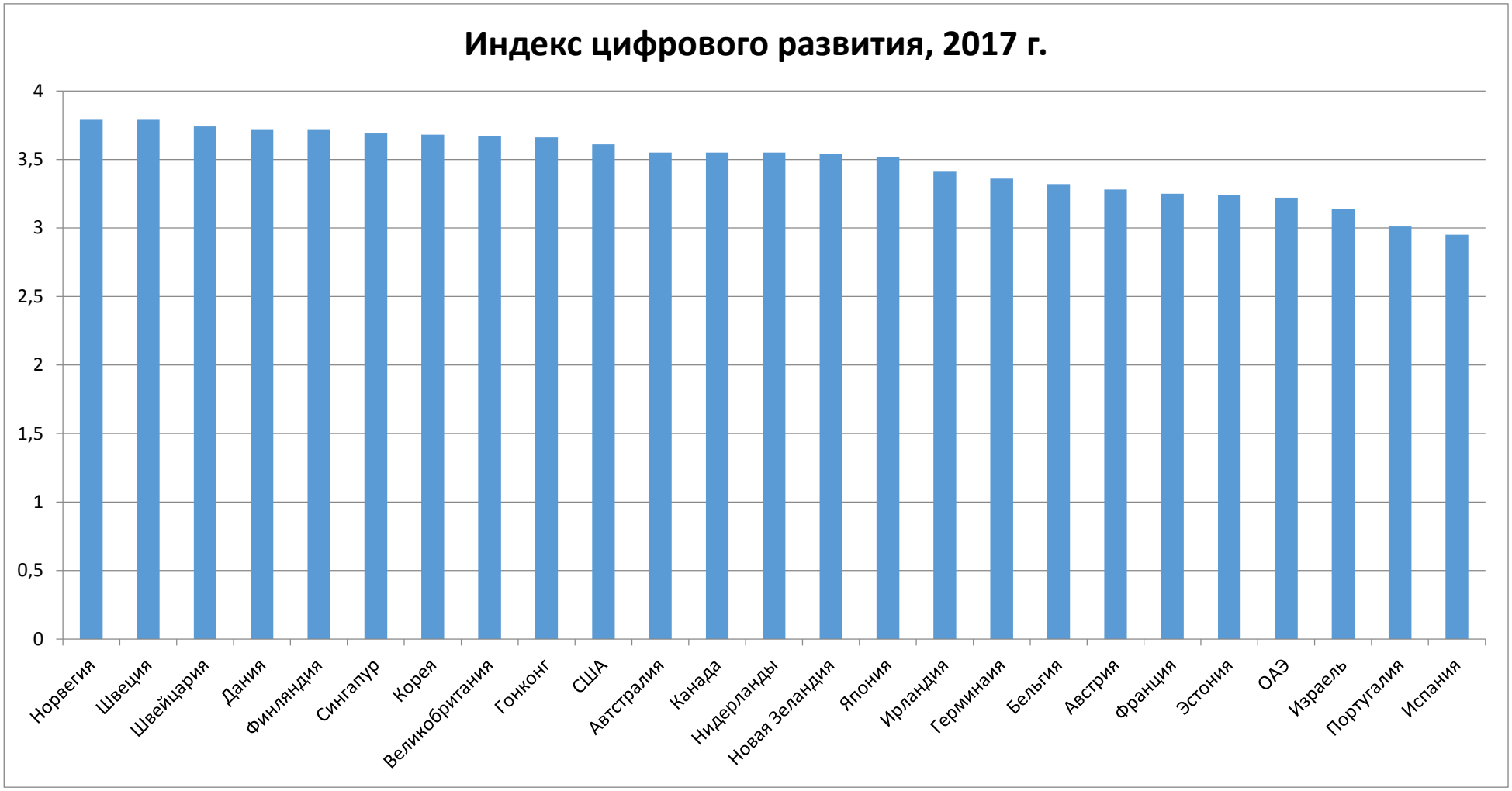


Рисунок 4 − Оценка лидирующих стран мира по индексу оценки цифровизации (по состоянию на 2017 г.)


Рисунок 5 − Оценка лидирующих стран мира по индексу оценки развития цифровизации (по состоянию на 2017 г.)

В соответствии с индексом оценки темпа развития цифровизации экономики лидирующими государствами являются:

– Китай,
– Малайзия,
– Боливия,
– Кения,
– Россия,
– Турция,
– Саудовская Аравия,
– Бангладеш,
– Колумбия,
– ОАЭ.

1.1.6 Рейтинг государств в соответствии с рейтингом мировой цифровой конкуренции[5]

Система рейтингования «World Digital Competitiveness Ranking» предусматривает определение рейтинга государства по показателям, оценивающим знания, технологии, готовность к будущему, индекс оценки темпа развития цифровизации экономик.

Рейтинг лидирующих стран мира в соответствии с рейтингом мировой цифровой конкуренции по состоянию на 2018 г. показан на рисунке 6.

[5] Рейтинг приведен в Докладе «IMD Мировой рейтинг цифровой конкуренции 2018» (IMD World Digital Competitiveness Ranking 2018). IMD World Competitiveness Center. IMD World Digital Competitiveness Ranking 2018 URL: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2018/ (дата обращения 01.08.2019)

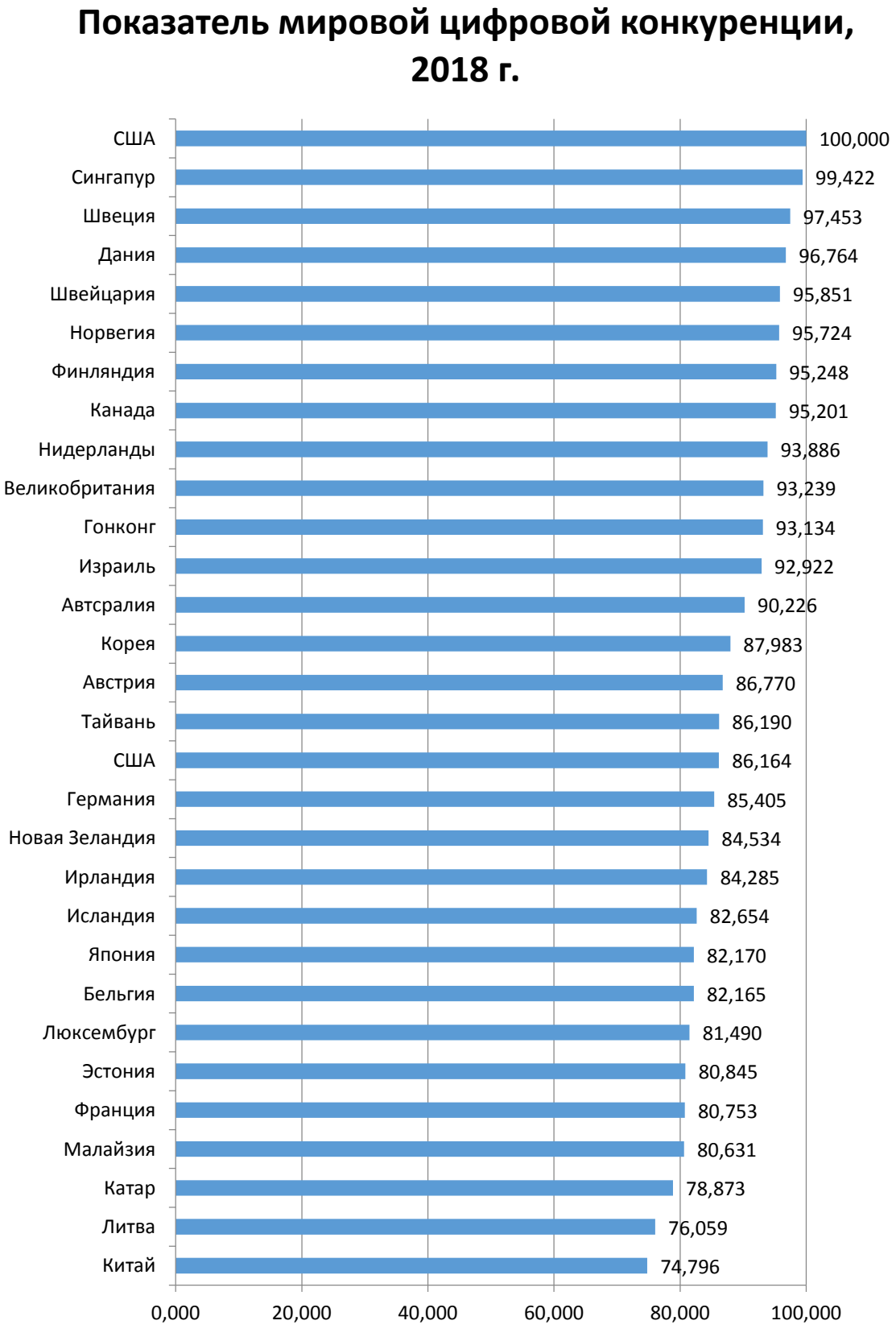


Рисунок 6 − Рейтинг стран мира в соответствии с рейтингом мировой цифровой конкуренции (по состоянию на 2018 г.)

В соответствии с рейтингом мировой цифровой конкуренции лидирующими государствами являются:

– США,
– Сингапур,
– Швеция,
– Дания,
– Швейцария,
– Норвегия,
– Финляндия,
– Канада,
– Нидерланды,
– Великобритания.

1.2 Краткий обзор законодательства и выбор государств для исследования зарубежного опыта правового регулирования управления данными

Приведенные рейтинги устанавливают государства, осуществляющие наиболее эффективное управление. Вместе с тем применяемые методики лишь частично принимают во внимание анализ действующего законодательства. В результате возникает вопрос о соответствии положения государства в рейтингах с уровнем развития в них права, с тем, какую роль играет право в обеспечении положения государства в рейтинге. В отечественной научной литературе отмечается, что «социологические методы оценки электронного государства показывают, что зачастую передовые позиции в использовании возможностей, создаваемых электронным государством, характерны для стран со средним уровнем

правового (и экономического) развития»[6]. Такие рейтинги, как правило, показывают практическую направленность развития цифровых технологий, но не учитывают в целом или частично правовые характеристики, в том числе связанные с методами реализации государственной власти.

Если исходить из анализа права, то следует принимать во внимание принятую в сравнительном правоведении классификацию национальных правовых систем, которая учитывает как технические характеристики права, так и социально-экономические условия его развития.

Различаются две правовые семьи – общего и романо-германского права.

В свою очередь в романо-германской правовой семье различается право стран Северной, Южной, Западной и Восточной Европы. Особое место в современном романо-германском праве занимают правовые системы Франции и Германии, оказавшие влияние на другие страны, воспринявшие понятийный аппарат и юридическую технику данных стран. Поэтому изучение их практики для России имеет особое значение по сравнению, например, с правом Австрии, которое тоже активно развивается в условиях ИКТ.

Эстония – пример страны, которая прошла этап социалистического права, но затем достигла положительных результатов, восприняв право ЕС.

Нидерланды наряду с Бельгией относятся к малым европейским странам, активно взаимодействующим в выработке правового регулирования в условиях ИКТ. В противоположность старо-голландскому праву, которое отличалось от права европейских стран и оказало влияние на Шотландию и ЮАР, современное право Нидерландов такого влияния не имеет.

---

[6] Богдановская И.Ю. Методы анализа электронного государства: к выработке комплексного подхода // Эволюция государственных и правовых институтов в условиях развития информационного общества / Отв. ред. И.Л. Бачило. М: ИГП РАН, 2012.

Из данной правовой семьи в исследуемой сфере выделяется группа Северного права, которая в данном исследовании представлена Норвегией.

В правовой семье общего права особую роль играют английское право и право США. Право Канады, Австралии и Новой Зеландии объединяет то, что они сохранили большее влияние английского права (английская королева – глава государства, английский парламент принимал для них законы, а Судебный комитет Тайного совета выступал высшей судебной инстанцией). Однако в XX в. Канада и Австралия приняли акты, ограничивающие влияние английского права (английского парламента и судебного комитета). В результате их право стало приобретать более самостоятельный характер. Новая Зеландия в большей мере сохранила влияние английского права. Из данной группы стран Австралия несколько активнее осуществляла законотворчество в исследуемой сфере. Поэтому в данной группе стран предметом исследования стало английское право, право США и Австралии.

Остальные правовые системы можно выделить в условные группы, но до уровня правовых семей они не развились.

Выделяется группа смешанного права. Национальные правовые системы данной группы восприняли нормы разных правовых культур (общего права, романо-германского права, религиозные нормы, обычное право). В настоящее время особый интерес имеет право Сингапура в силу его быстрого развития.

Право Израиля также относится к смешанным правовым системам. После длительного влияния английского права идет процесс формирования национального права, в том числе под влиянием религиозных норм. Трансплантация таких норм сложна в силу особенностей понятийного аппарата, юридической техники.

Между двумя культурами (общего права и права Китая) находится и право Гонконга, что определяет его трансформацию в поисках национальной модели.

К смешанным правовым системам относится и право Индии, построенное на сочетании религиозных норм и традиций общего права. Поиск завершенной национальной модели происходит в ней неоднозначно. На таком этапе развития вряд ли целесообразно говорить о возможном использовании правового опыта данной страны.

Право стран Азиатско-Тихоокеанского региона находится в стадии формирования, имеет ряд особенностей. Во многом право стран данной группы ориентируются на западное право, однако в практике правоприменения ему придают национальный характер.

Японское право в сфере ИКТ активно воспринимает опыт США. Выбор страны обусловлен влиянием США на национальное публичное право после второй мировой войны. В таком случае речь идет не столько о выработке оригинальных национальных норм, сколько об особенности восприятия зарубежного опыта.

Правовая система ОАЭ не входит ни в одну из сложившихся правовых семей. Более того, ОАЭ в определенной степени воспринимает зарубежное право. Категориальный аппарат, равно как и правовой механизм ОАЭ, имеет национальные особенности, в том числе обусловленные религиозными нормами.

На основе экспертного анализа рейтингов иностранных государств по различными системам рейтингования для исследования зарубежного опыта правового регулирования управления данными предлагается отобрать следующие страны:

– США,
– Австралия,
– Великобритания,
– Франция,
– Сингапур,
– Китай,
– Норвегия,

– Эстония,

– Республика Корея,

– Германия.

1.3 Исследование нормативных правовых актов зарубежных государств в области управления данными[7]

1.3.1 Нормативные правовые акты Европейского Союза

Директива открытых данных и последующего использования информации публичного сектора № 2019/1024 от 20.06.2019[8] вводит в оборот данные предприятий и учреждений, данные научных исследований, проводимых за счет бюджетных средств. Основной акцент сделан на максимально возможном открытии данных публичного сектора и формировании бизнес-моделей, использующих их. Положения предыдущей директивы сохранены, однако значительно дополнены. Во многом именно усиление акцента на открытых данных объясняет принятие новой директивы вместо поправок к предыдущей.

Директива уточняет возможность получения экономического преимущества компаниями в рамках частно-публичного партнерства от использования данных с целью соблюдения баланса интересов. Ранее Европейская комиссия установила, что некоторые компании получают необоснованное преимущество за счет доступа к публичным данным, фактически блокируя рынок данных либо получая завышенные

[7] В данном разделе исследуются нормативные правовые акты в области управления данными в зарубежных государствах, отобранных на основе анализа рейтингов государств в области цифрового развития и смежных областях, а также общего обзора и анализа соответствующего национального законодательства. Конкретный перечень указанных государств определен и обоснован в разделе 1.2 настоящего отчета.

[8] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. URL: http://data.europa.eu/eli/dir/2019/1024/oj (дата обращения 10.08.2019).

экономические преимущества. Новые положения директивы призваны решить выявленную проблему.

Директива определяет новые форматы раскрытия данных. В частности, поставлен акцент на развитие открытых данных в формате API. Введена категория особо значимых данных, список которых должен быть утвержден Европейской комиссией. Внимание также уделяется динамическим данным и особенностям их предоставления с максимально возможной достоверностью (актуальностью).

В Директиве сохранено платное предоставление информации, а также возможность предоставления информации на основании лицензии публичного органа. Обязательным остается требование о стандартизации условий таких лицензий. Исключительные лицензии возможны только в отдельно определяемых национальными юрисдикциями случаях.

Директива является определяющим документом в сфере экономики публичных данных всего Европейского союза.

Регламент 2016/679 о защите персональных данных[9] (далее - GDPR) обеспечивает единое регулирование персональных данных на территории ЕС в целом, что способствует формированию единого рынка данных и гарантирует защиту прав субъектов персональных данных.

Сформулированы основные принципы защиты персональных данных: законность, справедливость, транспарентность; целевое ограничение; минимизация данных (раскрывается ровно столько, сколько необходимо); ограничение хранения (хранится ровно столько, сколько действительно необходимо для исполнения цели сбора); целостность и конфиденциальность; ответственность (оператор должен следовать принципам и быть способным продемонстрировать соответствие им).

[9] Regulation (EU) 2016/679 (General Data Protection Regulation). URL: https://gdpr-info.eu/ (дата обращения 10.08.2019).

Среди ключевых прав вводится право на переносимость данных (data portability), предполагающее возможность субъекта запросить все данные, которые имеются в отношении него, получить их в доступном формате, а равно отозвать согласие на их обработку и поручить передать их полностью иному оператору.

Регламент 2018/1725 обработки персональных данных органами и организациями ЕС[10] определяет нормы обработки персональных данных органами ЕС с учетом положений Регламента о защите персональных данных, повторяет принципы, установленные GDPR.

Директива 2016/1148 о мерах обеспечения общего высокого уровня безопасности информационных систем[11] нацелена на достижение стабильности существенных услуг связи, уделяет внимание сохранению конфиденциальности информации при обеспечении информационной безопасности, исходит из общего принципа применения риск-ориентированного подхода при обеспечении информационной безопасности.

Директива 2007/2/EC об установлении инфраструктуры пространственной информации (INSPIRE)[12] гармонично дополняет современную политику формирования рынка публичных данных ЕС. Директива способствует установлению единой инфраструктуры, позволяющей публичным органам обмениваться пространственными

---

[10] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. URL: https://gdpr-info.eu/ (дата обращения 10.08.2019).

[11] 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. URL: http://data.europa.eu/eli/dir/2016/1148/oj (дата обращения 10.08.2019).

[12] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE). URL: http://data.europa.eu/eli/dir/2007/2/oj (дата обращения 10.08.2019).

данными (любые данные с прямой или косвенной ссылкой на конкретное местоположение или географическую область) в разных форматах, содержит рекомендацию к использованию для открытых данных таких же форматов. Наибольшей унификации подлежат форматы тех данных, которые используются или могут быть использованы наиболее широким кругом публичных органов и третьих лиц. Директива устанавливает, что некоторые пространственные данные имеют такую общественную значимость, что их предоставление должно быть бесплатным.

Стандартизация форматов информационного обмена в государственном секторе в ЕС основана на принципах открытости:

– участии всех заинтересованных лиц в разработке стандартов,

– широком использовании открытых стандартов и открытого (свободного) программного обеспечения в государственном секторе,

– предоставлении права на использование этих стандартов (спецификаций, форматов) на честных, разумных и недискриминационных условиях,

– участии государства в поддержке разработчиков стандартов и программного обеспечения.

Рекомендации Еврокомиссии по стандартным лицензиям, наборам данных и взимании пошлин за последующее использование[13] уточняют, что формальные лицензии не обязательны во всех случаях – чаще достаточно четкого указания, какая лицензия применяется (символьные системы Creative Commons, например). В любом случае условия использования информации должны быть доступны пользователю.

[13] Commission notice — Guidelines on recommended standard licences, datasets and charging for the reuse of documents. URL: http://data.europa.eu/eli/dir/2007/2/oj (дата обращения: 10.08.2019).

Отчет Еврокомиссии от 28.06.2019 об инструментах мониторинга рынка данных SMART[14] содержит анализ использования различных категорий данных. Германия, наряду с Францией, Испанией, Нидерландами и Италией, занимает лидирующие позиции по доходности от передачи данных по ЕС. Приведен прогноз на 2025 год по использованию данных в Европе по каждому инструменту мониторинга.

Инструменты мониторинга были проанализированы по 4 основным измерениям:

– измерение рабочей силы и навыков специалистов по данным и их потенциальный разрыв в навыках,

– измерение спроса и предложения данных,

– измерение бизнеса и экономики для понимания размера рынка данных и значение экономики данных,

– измерение международного контекста, сравнительный анализ с показателями Бразилии, Японии и США (ЕС занимает третье место по росту рынка и экономики данных после США и Японии).

Европейская комиссия в настоящее время работает над созданием Европейского мониторинга потоков данных, который будет отражать потоки данных через территорию ЕС[15].

Европейский мониторинг потока данных имеет две цели:

– построить карту потоков данных в ЕС для определения основных стратегических коридоров потоков данных,

– оценить экономическую ценность потоков данных для европейской цифровой экономики.

---

[14] URL: http://datalandscape.eu/sites/default/files/report/D2.6_EDM_Second_Interim_Report_28.06.2019.pdf (дата обращения: 02.08.2019).

[15] URL: https://ec.europa.eu/digital-single-market/en/european-data-flow-monitoring-initiative (дата обращения: 02.08.2019).

Для достижения первой цели в 2019 году запущен опрос компаний и государственных организаций для сбора агрегированных и анонимных данных:

– о количестве данных, хранящихся в облачных инфраструктурах компаний и государственных организаций ЕС (запасы данных),

– о данных, перемещаемые между облачными инфраструктурами на территории ЕС (потоки данных).

Собранные в ходе обследования данные будут затем использованы для разработки общедоступной агрегированной карты текущих запасов данных и потоков по территории ЕС с 2019 года для предварительного картирования и с 2020 года для окончательного картирования.

Отчет Еврокомиссии «О монетизации данных SMART» 2016/0063[16] определяет три основных пути монетизации данных:

– прямой доход от продажи данных,

– дополнительный доход от объединения данных с другими услугами или продуктами,

– обменные премии / торговые преимущества или скидки.

При этом названы условия развития концепции монетизации данных, среди которых упоминаются: повышение ясности правовой базы, определяющей монетизацию данных, меры поддержки малого и среднего предпринимательства для входа на рынок монетизации данных, расширение исследований в этой области,

Рабочий документ Еврокомиссии «Руководство по обмену данными частного сектора в европейской экономике данных»[17] (SWD / 2018/125)

---

[16] URL: http://datalandscape.eu/sites/default/files/report/D3.3_Data_Monetization_10.10.2018_GM.PDF (дата обращения: 02.08.2019).

[17] URL: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy (дата обращения: 02.08.2019).

устанавливает набор инструментов для компаний, которые являются владельцами данных, пользователями данных или тем и другим одновременно. Для этой цели он содержит руководство по юридическим, техническим и бизнес-аспектам совместного использования данных, которое можно использовать на практике при рассмотрении и подготовке обмена данными между компаниями из одного или разных секторов.

В документе названы принципы обмена данными в направлениях B2B и B2G (прозрачность, единая стоимость, конкуренция, уважение коммерческих интересов сторон и т.п.). Также указывается на возможность предоставления данных частного сектора государственным органам на льготных условиях при соблюдении принципов пропорциональности в использовании частных данных, ограничения целей использования, непричинения вреда, транспарентности и участия общества и т.д.

Приведены модели обмена данными между частными компаниями (открытые данные, монетизация данных, обмен данными на закрытых платформах) и частным и государственным сектором.

План быстрого реагирования на чрезвычайные ситуации от 13.09.2017 C (2017) 6100[18] разработан Еврокомиссией в целях повышения предотвращения кризисных ситуаций при угрозах кибербезопасности ЕС. План устанавливает цели и способы сотрудничества стран-членов и их органов, определяет антикризисные меры реагирования, предотвращения киберугроз, ликвидации их последствий. В целях реализации Плана государства-члены должны определить на национальном уровне организации межгосударственного взаимодействия, механизмы реагирования, сотрудничества и поддержания должного уровня защиты от киберугроз.

[18] URL: https://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=3&year=2017&number=6100&version=ALL (дата обращения: 02.08.2019).

Еврокомиссией организовано исследование ведущими учеными-юристами ЕС правовых аспектов повторного использования информации государственного сектора − LAPSI (legal aspects of (reusing) public sector information). В рамках данного проекта подготовлены документы по вопросам управления данными:

1) Позиционная бумага LAPSI n. 1: Принципы, регулирующие взимание платы за повторное использование информации государственного сектора[19].

В настоящее время организации государственного сектора вправе по умолчанию взимать плату за публичные данные в размере, необходимом для покрытия собственных издержек либо с минимальной наценкой.

Следуя Директиве ЕС о повторном использовании информации государственного сектора, LAPSI исходит из необходимости содействия появлению информационных сервисов и недискриминационного доступа к информации. В связи с этим анализируются случаи, когда плата взимается только в компенсационных целях (с нулевой маржой) или с установлением предельного значения наценки сверх затрат на обработку данных. В результате основные доводы сделаны в пользу второго варианта,

2) Концептуальная основа LAPSI n. 1: Политика начисления платы: концептуальная основа для руководства ЕС и для государств-членов[20],

3) Стратегическая рекомендация LAPSI 4: Конфиденциальность и защита личных данных[21],

---

[19] URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8342 (дата обращения: 02.08.2019).

[20] URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8345 (дата обращения: 02.08.2019).

[21] URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8366 (дата обращения: 02.08.2019).

4) Стратегическая рекомендация LAPSI 1: Вопросы законодательства о конкуренции при повторном использовании информации государственного сектора (PSI)[22].

1.3.2 Нормативные правовые акты Германии

А) Государственный строй и общая характеристика права Германии

Германия – федеративное государство с республиканской формой правления.

В Германии как парламентской республике правительство формируется парламентским путем. Бундестаг избирает главу правительства (федерального канцлера), по предложению последнего назначаются и увольняются остальные министры. По предложению министров из членов Бундестага назначаются парламентские статс-секретари. Они обеспечивают связь правительства и парламента, но связаны указаниями соответствующих министров. В отличие от США и Франции Президент Германии не оказывает существенного влияния на государственный аппарат, хотя формально назначает чиновников. Меньшую роль (к примеру, по сравнению с аппаратом Белого дома) играет и канцелярия президента, обеспечивающая его деятельность. Канцелярия приравнена к министерству.

Государственный аппарат Германии строится на принципе канцлерского руководства. Ведомство федерального канцлера имеет статус высшего федерального учреждения. В ведомстве действуют отделы, которые по сути контролируют деятельность всего государственного аппарата. Ведомство вырабатывает предложения по направлениям внутренней и внешней политики, оно играет большую роль в законотворческом процессе. Глава ведомства, имеющий ранг статс-секретаря, является важной политической фигурой.

---

[22] URL:http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8349 (дата обращения: 02.08.2019).

Количество министерств законодательно не урегулировано. На федеральном уровне функционируют в частности Министерства внутренних дел, юстиции, почты и телекоммуникаций, исследований и технологий. В состав правительства могут входить министры, не возглавляющие министерства (министры без портфеля).

Федеральное правительство также может с согласия Бундестага издавать общие административные предписания, осуществлять наблюдение за выполнением землями федеральных законов в соответствии с действующим правом.

Министерства делятся на отделы, подотделы, референтуры. Министерства руководят подчиненными федеральными учреждениями, самостоятельными федеральными ведомствами.

В Германии различается федеральное управление, управление земель по поручению федерации и собственно управление земель. Но в соответствии с ст. ст. 31, 70–75 и 91 Конституции федеральное право имеет приоритет над правом земель.

Земельные правительства состоят из премьер-министров и министров. Федерация включает 16 земель, а значит и 16 премьер-министров и правительств, возглавляющих систему управления земель. В связи с монопольным положением федерации в сфере управления иностранными делами и обороной в землях ФРГ нет соответствующих министерств. В остальном система земельных министерств, с учетом местных нужд и особенностей, примерно повторяет систему федеральных министерств, что обеспечивает тесные контакты центра и земель и практическое руководство многими местными делами из центра.

Правовая система Германии входит в романо-германскую правовую семью (или семью кодифицированного права). Право Германии изначально сыграло ключевую роль в формировании романо-германской правовой семьи. Частное право Германии и гражданский кодекс (Германское гражданское уложение) оказали значительное влияние на развитие права в

других странах, в том числе России. Публичное право пошло сложный путь развития, но в настоящее время оно получило завершенный характер как по методам регулирования, так и понятийному аппарату. Конституция (Основной закон) Германии действует с 1949 г. Большую роль в праве Германии играет академическая правовая доктрина, обосновывающая подходы к правовым институтам.

Б) Общий обзор законодательства в сфере управления данными

Регулирование управления данными, в том числе содержащихся в государственных информационных системах, осуществляется посредством актов федерального и земельного законодательства Германии (законов и подзаконных актов).

Термин «данные» используется в законодательстве Германии, при этом его содержание зависит от конкретного нормативного акта, и может быть абстрактным (любые данные) либо очень конкретным (конкретный перечень сведений).

При этом законодательство не содержит определений оборота данных или управления данными.

Федеральный закон о защите данных [23] (Bundesdatenschutzgesetz, BDSG) от 30.06.2017 применяется к обработке персональных данных государственными органами федерации и земель, где защита данных не регулируется земельным законодательством и где они выполняют публичные функции, а также частными организациями, полностью или частично, автоматическими средствами или иным образом.

В Законе закреплены правовые основы обработки персональных данных, статус субъектов данных, правовые способы защиты данных, структура, правовое положение, полномочия органов и должностных лиц по

[23] Bundesdatenschutzgesetz (BDSG). URL: https://www.gesetze-im-internet.de/englisch_bdsg/ (дата обращения: 02.08.2019)

защите данных на федеральном и земельном уровне, а также порядок их взаимодействия; в частности, отдельно урегулированы вопросы реализации GDPR и Директивы ЕС 2016/680.

Вместе с тем Германия отступает от положений GDPR в вопросах, в которых GDPR допускает отступления, оставляя вопрос на усмотрение государства-участника:

– обработка в контексте занятости (статья 88 GDPR; раздел 26 BDSG): BDSG разрешает обработку данных (в том числе специальных категорий персональных данных) в целях, вытекающих из трудового законодательства, законодательства о социальном обеспечении и защите, если нет оснований полагать, что субъект данных имеет законный интерес, чтобы его данные не обрабатывались,

– обработка специальных категорий данных (статья 9 (4) GDPR; раздел 22 BDSG): BDSG ввел дополнительные условия и ограничения в отношении обработки генетических данных, биометрических данных или данных, касающихся здоровья. В частности, разрешается обработка специальных категорий данных в оговоренных в BDSG случаях (например, в целях профилактической медицины, постановки медицинского диагноза, обеспечения общественного интереса в сфере здравоохранения, для обеспечения значимого общественного интереса, предотвращения угрозы общественной безопасности). При этом такая обработка допустима при принятии мер защиты прав субъектов данных (включая технические меры, шифрование, псевдонимизацию, ограничение доступа к данным и прочее),

– гарантии и отступления при обработке для целей архивирования в общественных интересах, научных исследованиях или статистических целях (статья 89 GDPR; раздел 27, 28, 50 BDSG): BDSG установлено, что ряд прав субъекта данных (право на доступ к данным, на ограничение обработки, на исправления, возражения) должны быть ограничены в той степени, в которой эти права могут сделать невозможным или нанести серьезный ущерб результатам исследования или статистики, и такие ограничения необходимы

для выполнения исследовательских или статистических целей, для целей архивирования в общественных интересах. Кроме того, право доступа не применяется, если данные необходимы для целей научных исследований, архивирования, а предоставление информации потребует непропорциональных усилий. По достижении указанных целей данные должны быть анонимизированы либо приняты иные меры по предотвращению раскрытия данных третьим лицам, если это не противоречит интересам субъекта данных,

– ограничения прав субъекта данных (статья 23 GDPR; раздел 32 и след. BDSG): GDPR допускает ограничение прав субъектов данных, если это необходимо для национальной безопасности, обороны, защиты независимости судей, предотвращения, расследования, судебного преследования уголовных преступлений, важных экономических интересов государства, защиты прав субъектов данных и пр. При этом BDSG в дополнение к этому устанавливает ограничения прав субъекта данных, если это необходимо для благополучия федерации и/или земель, для осуществления судебного процесса по частным искам, конфиденциальности передачи информации государственным органам, а также если реализация таких прав требует непропорциональных усилий или расходов, и т.д.,

– обязательства секретности (статья 90 GDPR; раздел 29 BDSG): BDSG установил правила защиты конфиденциальности данных, в частности, ограничивающие право надзорных органов на доступ к персональным данным или на информирование субъекта данных, если информация в силу закона должна оставаться в тайне,

– назначение сотрудников по защите данных (статья 37 (4) GDPR, раздел 38 BDSG): если GDPR устанавливает право обработчика данных назначить сотрудника по защите данных, то BDSG в отдельных случаях делает это обязанностью обработчика данных,

– кредитная информация и оценка (раздел 30 и след. BDSG): утверждены правила обработки персональных данных и закреплена

обязательность уведомления субъекта данных в случаях, связанных с обработкой данных для целей потребительского кредитования,

– общественное видеонаблюдение (раздел 4 BDSG): закреплена возможность видеонаблюдения за публичными местами в установленных законом целях (выполнение государственным органом возложенных на него задач, обеспечение общественной безопасности, защита жизни и здоровья и иных интересов присутствующих в общественном месте и т.п.), если ничто не указывает на законные интересы субъекта данных, которые определяются как первостепенные,

– обработка для других целей (статья 6 (4) GDPR, раздел 24 BDSG): GDPR говорит об обработке данных в совместимых целях, BDSG же разрешает обработку данных в нескольких разнородных целях, если обработка необходима для обеспечения общественной безопасности, уголовного преследования, обеспечения возможности осуществления судебного процесса по искам, а также если субъект данных не заинтересован в том, чтобы данные не обрабатывались,

– профилирование (статья 22 (2) GDPR, раздел 37 BDSG): GDPR закрепляет общий запрет на профилирование, кроме прямо указанных в нем случаев, BDSG расширяет перечень таких случаев,

– санкции за нарушения GDPR, на которые не налагаются административные штрафы (Раздел 41 и след. BDSG): BDSG ограничивает размеры штрафа за нарушение установленных в нем требований суммой 50 000 евро, при этом штрафы не могут налагаться на государственные органы.

Свободный доступ к официальной информации в Германии регулируется посредством ряда законов.

Закон о свободе информации от 05.09.2005 (IFG) [24] закрепляет право каждого на доступ к официальной информации федеральных органов власти. К такой информации отнесена любая официальная запись, сделанная органом власти, независимо от того, как она хранится (за исключением черновиков и заметок). Вместе с тем существует ряд исключений, когда данное право ограничивается. Среди таких случаев закон выделяет:

– защиту особых общественных интересов,
– защиту процесса принятия административного решения,
– защиту персональных данных,
– защиту интеллектуальной собственности и коммерческой тайны.

Законом о продвижении электронного правительства (EGovG) от 25.08.2013[25], Законом об улучшении онлайн-доступа к административным услугам (OZG)[26] от 14.08.2017, а также соответствующими законами земель на держателей официальной информации (государственные органы различного уровня, организации как государственные, так и частные некоммерческие с государственной долей участия в них, различные ассоциации) возложена обязанность обеспечивать доступ граждан, организаций и иных лиц к такой информации посредством порталов открытых данных либо по запросу. Также держатели официальной информации обязаны вести ее учет, формировать каталоги информации, публиковать обязательную для раскрытия информацию и пр.

Закон о повторном использовании информации государственного сектора от 13.12.2006[27] (Gesetz über die Weiterverwendung von Informationen

[24] Gesetz zur Regelung des Zugangs zu Informationen des Bundes. http://www.gesetze-im-internet.de/ifg/ (дата обращения 11.08.2019).
[25]Gesetz zur Förderung der elektronischen Verwaltung. http://www.gesetze-im-internet.de/egovg/ (дата обращения 14.08.2019).
[26] URL:http://www.gesetze-im-internet.de/ozg/ (дата обращения: 05.08.2019).
[27] IWG. URL: https://www.gesetze-im-internet.de/iwg/ (дата обращения: 02.08.2019)

öffentlicher Stellen, IWG) применяется к повторному использованию информации, доступной государственным органам, в частности для предоставления продуктов и услуг цифровой экономики.

Информация, которая подпадает под действие этого Закона, может быть использована третьими лицами на условиях, определенных владельцем информации. Доступ к информации, находящейся в распоряжении библиотек, музеев или архивов, а также к информации, являющейся объектом авторских или смежных прав или права промышленной собственности, предоставляется в соответствии с законодательством об интеллектуальной собственности, или если владелец информации разрешил ее использование.

Законом запрещены эксклюзивные (антиконкурентные) соглашения в части повторного использования информации, находящейся в распоряжении государственных органов, а также установлены условия использования такой информации, порядок определения сборов при использовании информации.

Закон о документах Службы государственной безопасности бывшей ГДР[28] (Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik, StUG) от 20.12.1991 обеспечивает доступ частных лиц и исследователей к архивам «Штази» – службы безопасности ГДР. В соответствии с Законом действует Федеральная комиссия по разбору архивов служб безопасности ГДР, занимающаяся восстановлением уничтоженных документов и составлением файлов.

Закон о регистрации[29] (Bundesmeldegesetz, BMG) от 03.05.2013 устанавливает перечень регистрирующих органов, фактов и событий, подлежащих регистрации, а также порядок регистрации и обработки

[28] URL: http://www.gesetze-im-internet.de/stug/ (дата обращения: 02.08.2019).
[29] URL: https://www.gesetze-im-internet.de/bmg/ (дата обращения: 05.10.2019).

(хранения, обмена, исправления, удаления) данными, собранными при проведении регистрации.

Для уточнения положений названного Закона на уровне земель приняты земельные законы и подзаконные акты, например, Закон Берлина об исполнении Закона о регистрации[30] (BlnAGBMG) от 07.07.2016, а также Постановление о передаче данных в Берлине[31] (MeldDÜV_BE) от 28.09.2017, которые утверждают перечень данных и порядок обмена ими между различными местными органами власти в целях выполнения ими своих административных функций.

Среди специальных законов, регулирующих оказание услуг, связанных с обменом информацией – Закон о телемедиа и Закон о телекоммуникациях.

Закон о телемедиа от 26.02.2007[32] (Telemediengesetz, TMG) распространяется на все электронные информационные и коммуникационные услуги, не являющиеся телекоммуникационными услугами по Закону о телекоммуникациях, которые представляют собой передачу сигналов по телекоммуникационным сетям, телекоммуникационных услуг согласно Закону о телекоммуникациях или радиовещания. Устанавливает обязанность защиты данных для поставщиков телемедиа-услуг.

---

[30] URL: http://gesetze.berlin.de/jportal/portal/t/lzh/page/bsbeprod.psml;jsessionid=C3E50D0A582242F50289F5EC463BF4F4.jp25?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=jlr-BMGAGBErahmen&doc.part=X&doc.price=0.0&doc.hl=1#focuspoint (дата обращения: 05.10.2019).

[31] URL: http://gesetze.berlin.de/jportal/portal/t/lxz/page/bsbeprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=25&numberofresults=64&fromdoctodoc=yes&doc.id=jlr-MeldD%C3%9CVBEpP20&doc.part=X&doc.price=0.0&doc.hl=1#focuspoint (дата обращения: 02.08.2019).

[32] Telemediengesetz. http://www.gesetze-im-internet.de/tmg/ (дата обращения: 02.08.2019)

Закон устанавливает требования к обработке персональных данных, относящихся к электронным информационным и коммуникационным услугам, выполняемым поставщиками телемедиа-услуг, формулирует специальные информационные требования (например, указание выходных данных владельца сайта), требования к обеспечению информационной безопасности (особенно с использованием шифрования) при оказании услуг.

Также TMG определяет, что для целей рекламы, исследования рынка или разработки телемедиа на основе потребностей поставщик услуг вправе создавать профили использования на основе псевдонимов, если получатель услуги не возражает.

Закон о телекоммуникациях от 22.06.2004[33] (Telekommunikationsgesetz) регулирует оказание телекоммуникационных услуг связи, предъявляет требования к поставщикам телеком-услуг по технической, организационной защите средств связи при оказании услуг в части защиты телекоммуникационной тайны и персональных данных пользователей услугами.

В Законе предусмотрены случаи и порядок обмена информацией между операторами связи и государственными органами. В частности, предусмотрена обязанность предоставлять информацию по запросам федеральных министерств, агентств и служб отдельные категории информации для модернизации сетевой инфраструктуры. Отдельно предусмотрена обязанность Федерального сетевого агентства по информированию правоохранительных органов о фактах, послуживших основанием для подозрения в правонарушениях, выявленных при оказании телекоммуникационных услуг.

---

[33]Telekommunikationsgesetz. https://www.gesetze-im-internet.de/tkg_2004/index.html (дата обращения: 02.08.2019)

Также в Законе определена процедура контроля над защитой данных и свободой информации, уведомления Федерального сетевого агентства и Федерального комиссара по защите данных и свободе информации о нарушениях защиты персональных данных.

Регулирование обеспечения безопасности и защиты данных осуществляется следующими нормативными актами.

Закон о повышении безопасности систем информационных технологий от 7.07.2015[34] (IT-Sicherheitsgesetz) создал в ФРГ правовую основу обеспечения кибербезопасности. В дополнение к обязательному уведомлению об инцидентах информационной безопасности, он устанавливает минимальные стандарты ИТ и требования к отчетности операторов критически важных инфраструктур (включая энергетику, водоснабжение, здравоохранение, телекоммуникации). Данным Законом дополняются положения законов о телемедиа (TMG) и закона о телекоммуникациях (TKG) в части защиты телемедиа- и телеком-инфраструктуры[35].

Вместе с тем в последние несколько лет активно выдвигаются предложения о пересмотре названного Закона с целью усиления борьбы с киберпреступностью. В марте 2019 г. Министерством внутренних дел опубликован проект Закона о безопасности ИТ– 2.0[36] (IT-SiG 2.0). В данном проекте полномочия правоохранительных органов расширены, предложены изменения в уголовном и уголовно-процессуальном законодательстве по

---

[34]IT-Sicherheitsgesetz.https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1565384375246 (дата обращения: 02.08.2019)

[35] Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=6 (дата обращения: 02.08.2019)

[36] https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 (дата обращения: 02.08.2019)

ужесточению наказания за киберпреступления. Сфера применения Закона распространяется на другие сферы экономики (помимо критически важных, упомянутых в действующем законе о повышении безопасности систем информационных технологий), в частности сферы, которые представляют общественный интерес, нарушения в которых могут привести к ухудшению фундаментальных интересов общества.

Законом о Федеральном ведомстве информационной безопасности[37] (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSI-Gesetz) от 14.08.2009 определено правовое положение данного ведомства (BSI), его задачи и полномочия. Ведомство учреждено для обеспечения информационной безопасности на федеральном уровне и подчинено Министерству внутренних дел. Законом закреплены специальные требования к поставщикам информационных услуг (интернет-площадки, операторы поисковых систем, облачные операторы) в части защиты информационных систем и обеспечения безопасности информационной сети. Установлена административная ответственность за нарушения в сфере обеспечения безопасности ИТ.

Постановление об определении критических инфраструктур[38] в соответствии с BSI-Gesetz (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, Kritis-VO) от 22.04.2016 принято Министерством внутренних дел по согласованию с Министерствами юстиции и защиты прав потребителей, экономики и энергетики, финансов, труда и социального обеспечения, продовольствия и сельского хозяйства, здравоохранения, транспорта и цифровой инфраструктуры, обороны,

---

[37] BSI-Gesetz. https://www.gesetze-im-internet.de/bsig_2009/__BJNR282110009.html (дата обращения: 02.08.2019)

[38] Kritis-VO. https://www.gesetze-im-internet.de/bsi-kritisv/ (дата обращения: 02.08.2019)

окружающей среды, охраны природы, строительства и ядерной безопасности в развитие положений Закона об информационной безопасности (IT-Sicherheitsgesetz). Постановлением конкретизирован перечень критически важных услуг в сферах энергетики, водоснабжения, продовольствия, здравоохранения, телекоммуникаций, транспорта, финансов. Установлены критерии и пороговые значения (формулы для расчета различных показателей) систем безопасности в каждом секторе экономики, регулируемом Законом об информационной безопасности.

Помимо федерального законодательства, управление данными осуществляется на уровне земельного законодательства.

Законы земель о защите персональных данных приняты во исполнение и в соответствии с GDPR и BDSG. Большей частью земельные законы повторяют положения GDPR. К указанным законам относятся Баварский закон о защите данных[39] (Bayerisches Datenschutzgesetz, BayDSG) от 15.05.2018 (GVBI. P. 230) BayRS 204-1-I, Закон о защите данных Гамбурга[40] (Hamburgisches Datenschutzgesetzes, HmbDSG) от 18.05.2018, Гессенский закон о защите данных и свободе информации[41] (Hessisches Datenschutz- und Informationsfreiheitsgesetz, HDSIG) от 3.05.2018 и т.д. по большей части земель.

Закон Бранденбурга о доступе к файлам и информации[42] (Akteneinsichts- und Informationszugangsgesetz, AIG) от 10.03.1998 предусматривает доступ граждан к государственным базам данных, за исключением данных, имеющих преобладающий общественный интерес

---

[39] URL: https://www.gesetze-bayern.de/(X(1)S(nzjymmxxpbdihomdbanqlx0f))/Content/Document/BayDSG/true?AspxAutoDetectCookieSupport=1 (дата обращения: 02.08.2019).

[40] URL: http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&st=lr&doc.id=jlr-DSGHA2018rahmen (дата обращения: 02.08.2019).

[41] URL: https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHEV1IVZ

[42] URL: http://bravors.brandenburg.de/gesetze/aig (дата обращения: 02.08.2019).

(сведения, имеющие значение для национальной обороны, международных отношений, судебного преследования и т.п.). Также может быть открыт доступ третьих лиц к базам, содержащим личные данные или данные компаний, если субъекты дали согласие на доступ к этим данным. Установлена процедура доступа к данным и порядок взимания платы за такой доступ. Законом прямо установлено, что он ограничивает право на личную жизнь, установленное Конституцией Бранденбурга.

Кроме нормативно-правовых актов Германии, можно выделить и иные источники для анализа регулирования данных.

Национальная стратегия электронного правительства (NEGS)[43], принятая Советом по ИТ-планированию в октябре 2015 г., создает основу деятельности электронного правительства в Германии и направлена на обеспечение открытости правительства страны, прозрачности его деятельности, свободного доступа к информации, находящейся в распоряжении государственных органов, а также к упрощению получения государственных услуг.

Программа оцифровки административных услуг[44] (Das Digitalisierungsprogramm des IT-Planungsrates) (21-е заседание Совета по планированию ИТ, решение от 13.10.2016) направлена на предоставление возможности получения административных услуг гражданами и предприятиями в электронном виде. Помимо обеспечения соответствия организационным, техническим и нормативным требованиям, программой определен приоритет удовлетворения нужд пользователей.

---

[43] Nationale E-Government-Strategie. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/NEGS/NEGS_Fortschreibung.html?nn=6839038 (дата обращения 13.08.2019).

[44] https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/21_Sitzung/18_Anlage1_Digitalisierungsprogramm.html?nn=9693774 (дата обращения: 02.08.2019).

Национальная стратегия кибербезопасности[45] (Cyber-Sicherheitsstragie für Deutschland), принятая Министерством внутренних дел в 2016 г., определяет основные направления политики Германии в области кибербезопасности, обозначает такие приоритетные направления развития как обеспечение безопасности электронного взаимодействия через шифрование и несмотря на шифрование, расширение концепции безопасной идентификации людей и вещей, распространение стандартов кибербезопасности, проведение исследований. Провозглашена совместная миссия государства и бизнеса по обеспечению ИТ-безопасности, развитие государственной архитектуры кибербезопасности.

Руководством по информационной безопасности в государственном управлении[46] (Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, решение Совета по планированию ИТ от 19.02.2013) определены основные направления ИТ-безопасности в государственном секторе. Среди них можно выделить информационный менеджмент, подготовка государственных служащих, обеспечение безопасности сетевой инфраструктуры, меры против кибер-атак, стандартизация.

Программа стандартизации[47] (STANDARDISIERUNGS AGENDA, решение Координационного центра по вопросам ИТ при Совете планирования ИТ от 02.09.2015) призвана обеспечить создание и использование единых стандартов обмена данными в электронном виде, поскольку использование различных форматов данных, интерфейсов, оборудования и т.п. затрудняет взаимодействие между субъектами обмена

---

[45] http://www.bmi.bund.de/cybersicherheitsstrategie/ (дата обращения: 02.08.2019).

[46] URL: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.pdf?__blob=publicationFile&v=2 (дата обращения: 02.08.2019).

[47] URL: https://www.it-planungsrat.de/DE/Standards/Standards_node.html (дата обращения: 02.08.2019).

данными и приводит к ошибкам в процессе обмена, потерям и искажениям данных и т.п. В рамках проекта «Внедрение нового стандарта метаданных немецких порталов открытых данных» внедрена новая модель метаданных, созданная в рамках проекта стандартизации Германии (портал GovData). Стандарты Совета размещены в Интернете[48].

В) Государственное управление оборота данными

Политику государства в сфере управления данными определяет федеральное правительство. Основная часть контрольно-надзорных функций в сфере оборотом данных (в том числе персональных) и их защиты возложена на Федерального комиссара по защите данных и на земельных комиссаров, которые имеет право запрашивать необходимую информацию, осуществлять мониторинг соблюдения законодательства о защите данных, проводить расследования, выносить предписания об устранении нарушений.

Управлением в области связи занимается Министерство транспорта и цифровых инфраструктур.

Для регулирования отдельных вопросов в федеральном правительстве практикуется организация межминистерских комитетов. Для управления развитием ИТ-технологий, создания стандартов обмена данными создан Совет по ИТ-планированию (совет по планированию ИТ-технологий; учрежденный на основании договора между федерацией и землями). Он состоит из представителей федерального правительства и земель (в т.ч. местных органов, общин). При назначении в состав Совета федерация и земли гарантируют, что назначаемый компетентен в вопросах, поставленных перед Советом.

При государственном управлении данными имеет место принятие совместных нормативных актов (например, Постановление об определении

[48] URL: http://www.xoev.de/sixcms/media.php/13/Standardisierungsagenda.pdf (дата обращения: 02.08.2019).

критических инфраструктур[49] в соответствии с BSI-Gesetz, в принятии которого участвовали почти все федеральные министерства).

1.3.3 Нормативные правовые акты Франции

А) Государственный строй и общая характеристика право Франции

Франция – унитарное государство со смешанной формой правления, в которой сочетаются элементы как президентской, так и парламентской республики, заложенные Конституцией 1958 г. Пятой Французской республики.

Главой государства выступает избираемый Президент республики.

Члены правительства (Совета министров) назначаются Президентом по предложению Премьер-министра. Президент вправе председательствовать в Совете министров. Премьер-министр руководит деятельностью правительства.

Государственный аппарат имеет глубокие исторические традиции, но его современная модель отражает идеи Пятой республики. Для французского государственного аппарата характерно его периодическое реформирование в целях повышения эффективности.

Аппарат имеет сложную иерархическую структуру. Большую роль играют аппарат Президента и Премьер-министра. Эти две службы тесно взаимодействуют. Генеральный секретариат аппарата Президента контролирует деятельность министерств и ведомств. Заместитель генерального секретаря отвечает за службу Елисейского дворца.

Аппарат Премьер-министра включает кабинеты самого Премьер-министра, Генерального секретариата правительства, Генерального секретариата национальной обороны.

---

[49] Kritis-VO. https://www.gesetze-im-internet.de/bsi-kritisv/ (дата обращения: 02.08.2019)

Ключевым звеном государственного аппарата выступают министерства. Они создаются на основании актов, определяющих круг их полномочий. Помощниками министра выступают государственные секретари.

При Премьер-министре действуют и иные службы (административного управления, информации, экономического и социального развития, научных исследований, охраны окружающей среды).

Зачастую баланс общественных интересов в аппарате государственного управления достигается посредством создания или наделения полномочиями нескольких органов, координирующих друг друга. В системе управления выделяются межминистерские органы, в которых ведущую роль играют чиновники аппаратов Президента и Премьер-министра. К таким органам относятся возглавляемые Президентом советы и возглавляемые Премьер-министром комитеты.

Во Франции к публичному сектору могут относиться не только государственные органы, но и публичные учреждения (établissement public). Развита конструкция юридических лиц публичного права. При этом отдельное государственное предприятие, например, может быть отнесено и к юридическим лицам частного права. Государственное предприятие относится к лицам публичного права, если за ним признан статус публичного учреждения. В большинстве случаев, однако, вопрос отнесения того или иного лица к публичным учреждениям решается в его учредительных документах. Выделение юридических лиц публичного права позволяет четко отделить сферу действия государства в публичном интересе и не смешивать ее с коммерческим направлением государственной деятельности, направленным на извлечение прибыли.

При рассмотрении материалов по Франции необходимо учитывать, что термин «служба» не соотносится в полной мере с одноименным российским термином и означает направление деятельности государства по реализации возложенных на него полномочий, которое может осуществляться как

самостоятельном органом власти, так и административной единицей внутри него. Термин «публичная служба» может означать в целом все обязанности государственных органов и действия по их реализации во Франции. Во французском языке термины «публичная служба» и «публичная услуга» обозначаются одинаково − Le Service Public. Для разграничения обычно, подразумевая публичные услуги, используется множественное число. Одновременно, даже во множественном числе употребление указанного термина может относиться как к органу власти, так и к его подразделению, ответственному за определенное направление государственной деятельности. Например, аппарат Премьер-министра включает в себя более ста «служб» (services), которые осуществляются различными административными органами[50]. Административные органы могут быть как независимыми (включая например, CNIL – Национальную комиссию информационных технологий и свобод, ответственную за защиту персональных данных), так и непосредственно подчиненными Премьер-министру. Отнесение их к «службам» Премьер-министра означает, что финансирование их деятельности осуществляется из бюджета администрации последнего.

Французское право относится к романо-германской правовой семье и сыграло большую роль в ее формировании. ГК Франции был воспринят многими странами. Для французского права характерно его деление на частное и публичное право. Административная юстиция в форме административных трибуналов решает публично-правовые споры.

Б) Общий обзор законодательства в сфере управления данными

Французское право не выделяет общий режим информации, а равно не выделяет общих субъектов информационных правовых отношений.

[50] https://www.gouvernement.fr/les-services-du-premier-ministre (дата обращения - 04.11.2019).

Одновременно во Франции устанавливается правовое регулирование отдельных категорий данных.

Французское право не использует терминов «оборот данных», «управление данными» в законодательстве. Вопросы оборота данных решаются в рамках института последующего использования информации в свете европейского правового регулирования.

В общих условиях использования открытых данных можно обнаружить определения терминов «публичная информация» и «набор данных»[51]. Под публичной информацией понимаются документы, не являющиеся объектами интеллектуальной собственности, созданные или полученные государственными или муниципальными органами, а также иными юридическими лицами публичного права, передаваемые любому лицу по его обращению или распространенные для всеобщего сведения.

Под набором данных понимается связанная совокупность ресурсов или единиц информации (файлы с данными, разъясняющие файлы, мобильные приложения, ссылки), а также метаданных (описание, дата публикации, ключевые слова, географический/временной охват), относящихся к определенной теме.

Основы правового регулирования оборота данных регулируются во Франции двумя правовыми актами - Книгой III Кодекса отношений между обществом и администрацией[52] (введена в 2015 г. ордонансом Президента Французской республики[53]) в части предоставления и использования данных

---

[51] Conditions d’utilisation. https://www.data.gouv.fr/fr/terms/ (дата обращения 10.08.2019).

[52] Code des relations entre le public et l'administration. URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000031366350 (дата обращения 10.08.2019).

[53] Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration //

государственных органов и Законом о технологиях и свободах от 06.01.1978[54], устанавливающем правовой режим персональный данных. Указанные акты сформированы под влиянием европейского права в рассматриваемой сфере.

Книга является наиболее общим актом, имплементирующим положения Директивы Европейского парламента и Совета от 20.06.2019 №2019/1024 и дополняющим их нормами национального права.

Закон о технологиях и свободах от 06.01.1978[55] (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) в первую очередь устанавливает правовое регулирование персональных данных. Большая часть положений утратила силу с введением в действие GDPR.

Закон о защите идентичности 2012 г.[56] вводит электронные карты гражданина и регулируют обработку и хранение персональных данных для случаев удостоверения личности французских граждан. Согласно Закону личность гражданина может быть удостоверена любым способом, в том числе достаточным является предъявление карты гражданина (документ удостоверения личности французского гражданина на территории Франции) или паспорта (паспорт по основному назначению используется для удостоверения личности на территории иностранных государств). И паспорт, и карта гражданина содержат ряд данных в электронной форме. Орган,

---

https://www.legifrance.gouv.fr/eli/ordonnance/2015/10/23/PRMX1516009R/jo/texte (Дата обращения - 14.11.2019)

[54] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624 (дата обращения 10.08.2019).

[55] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624 (дата обращения 10.08.2019).

[56] LOI n° 2012-410 du 27 mars 2012 relative à la protection de l'identité // JORF n°0075 du 28 mars 2012 page 5604, texte n° 2. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411&dateTexte=20170503 (date d'accès – 27.03.2017)

выдающий карты граждан, для удостоверения сведений взаимодействует с органами регистрации актов гражданского состояния.

Декрет о государственной информационной системе от 01.08.2014[57] (Décret n° 2014-879) предусматривает созыв Совета информационных систем государства не реже двух раз в год, определяющего направления стратегического развития государственных информационных систем. В состав Совета входят: генеральные секретари министерств; генеральный директор системы информационного взаимодействия в области обороны; генеральный директор администрации по публичным функциям; генеральный директор агентства безопасности информационных систем; директор бюджета и директор госзакупок. Каждое министерство разрабатывает план финансирования исполнения обязанности, возложенной на него в отношении информационных систем, и направляет его для ознакомления директору по цифровому развитию и системе информационного взаимодействия государства.

Декрет о Национальном агентстве[58] безопасности информационных систем[59] (Décret n° 2009-834 от 07.07.2009) предусматривает создание национального специализированного органа, который работает как с публичным, так и с частным сектором в целях обеспечения безопасности информационных систем и единой информационной инфраструктуры.

---

[57] Décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'Etat. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029337021 (дата обращения 10.08.2019).

[58] Агентства – органы власти, создаваемые для осуществления узко специализированной деятельности, решения конкретных задач в сфере специализации, в течение определенного ограниченного времени. URL: https://www.vie-publique.fr/fiches/20249-agences-administrations-de-mission (дата обращения 04.11.2019).

[59] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information». URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212 (дата обращения 10.08.2019).

Постановление о системе межведомственного взаимодействия[60] от 17.12. 2012 предусматривает создание межведомственной государственной информационной сети. Технические характеристики информационной сети не уточняются.

Отметим Решение Конституционного совета Франции n° 2012-652 DC от 22.03.2012. В проекте Закона о защите идентичности изменения предусматривалась возможность использования электронной подписи в качестве приложения к карте гражданина. Законопроект был направлен в Конституционный Совет, который должен был дать заключение о соответствии Конституции ряда его положений до его принятия и вступления в силу. Совет в 2012 г. признал положения законопроекта, вносившие важнейшие изменения, не соответствующими Конституции[61]. Проверке подлежали статьи 5 и 10 законопроекта, которые расширяли полномочия органов власти к доступу к персональным данным, хранящимся в информационной системе. В ряду таких данных находятся и биометрические: об отпечатках пальцев, о цвете глаз и т.д. Совет, ссылаясь на ст. 34 Конституции Франции и на ст. 2 Декларации прав человека 1789 г., определил, что сбор, обработка, хранение, использование и передача персональных данных должны в любом случае быть обоснованы необходимостью защиты публичного интереса, и их осуществление должно быть адекватным и пропорциональным такой цели. Исходя из этого, Совет заключил, что предлагаемые законопроектом меры обоснованы публичным

---

[60] Arrêté du 17 décembre 2012 portant création d'un service à compétence nationale dénommé «Réseau interministériel de l'Etat». URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026792328&categorieLien=id (дата обращения 10.08.2019).

[61] Le Conseil Constitutionnel. Décision n° 2012-652 DC du 22 mars 2012 // ORF n°0075 du 28 mars 2012 p. 5607, texte n°6: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582452 (date d'accès – 27.03.2017)

интересом, но предлагаемые им процедуры не пропорциональны публичному интересу. Таким образом, Совет признал ст. ст. 5 и 10 не соответствующими Конституции и нарушающими право на частную жизнь.

Оспаривались также положения ст. 3 законопроекта, которая внедряла новый функционал карты гражданина. Согласно этой статье по желанию держателя карты в нее включались также данные, позволявшие идентификацию в сетях электронных коммуникаций и использование электронной подписи. Для каждого использования карты лицо могло определять те данные, которые требовались. Одновременно обозначалось, что оказание государственных и муниципальных услуг онлайн не могло быть доступно только лицам, согласившимся на использование новых функций карты гражданина.

Оценивая ст. 3 на соответствие Конституции, Конституционный совет пришел к выводу, что положения статьи не детализировали природу данных, использование которых могло быть возможно, не содержали гарантий целостности и конфиденциальности таких данных и не определяли условий аутентификации лиц. Опираясь на изложенные доводы, Совет признал ст. 3 законопроекта не соответствующей Конституции.

В) Государственные органы в сфере управления данными

До октября 2019 г. развитие политики Франции в области оборота данных, функционирования открытых данных и функционирования межведомственных государственных систем осуществлялось Межведомственной дирекцией управления национальными информационными системами (DINSIC)[62], формируемой Премьер-

[62] Décret n° 2015-1165 du 21 septembre 2015 relatif à la direction interministérielle de la transformation publique et à la direction interministérielle du numérique et du système d'information et de communication de l'Etat. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031194412&categorieLien=cid (дата обращения 10.08.2019); Décret n° 2017-1584 du 20 novembre 2017 relatif à la

министром при Генеральном секретариате правительства[63] под руководством министра, ответственного за цифровое развитие[64].

25 октября 2019 года создана Межведомственная дирекция по цифровому развитию (DINUM) при Генеральном секретаре Правительства Франции (в ведении Премьер-министра)[65]. DINUM ответственна за организацию функционирования межведомственных государственных систем, рассматривает проекты законов и подзаконных актов министерств и ведомств в сфере своей компетенции, может осуществлять аудит по распоряжению Премьер-министра. DINUM является основным органом, организующим оборот государственных данных во Франции. Также он разрабатывает стратегию цифрового развития государства (стратегический документ исполнительной власти) и обеспечивает ее исполнение[66].

---

direction interministérielle de la transformation publique et à la direction interministérielle du numérique et du système d'information et de communication de l'Etat. https://www.legifrance.gouv.fr/eli/decret/2017/11/20/PRMX1732385D/jo/texte (дата обращения 10.08.2019).

[63] Генеральный секретариат Правительства Франции создан в 1935 г. Он находится под управлением Генерального секретаря Правительства и создается при Премьер-министре. Секретариат создан для обеспечения общего функционирования исполнительной власти, а также для ведения отделов (services) аппарата Премьер-министра. Fiche de synthèse n°28: Le secrétariat général du Gouvernement // http://www2.assemblee-nationale.fr/decouvrir-l-assemblee/role-et-pouvoirs-de-l-assemblee-nationale/l-organisation-des-travaux-de-l-assemblee-nationale/le-secretariat-general-du-gouvernement (дата обращения - 04.11.2019).

[64] Министр, ответственный за цифровое развитие в настоящий момент – Государственный секретарь Генерального секретариата Правительства. В его функции входит развитие политики цифрового развития государства. Décret n° 2017-1068 du 24 mai 2017 relatif aux attributions déléguées au secrétaire d'Etat chargé du numérique // https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034807011&dateTexte=&categorieLien=id (дата обращения - 04.11.2019).

[65] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique // https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D4ECB579ACEA6FD419A2720092289704.tplgfr31s_2?cidTexte=JORFTEXT000039281619&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000039281603 (дата обращения - 4.11.2019).

[66] В настоящий момент стратегия еще не опубликована.

### 1.3.4 Нормативные правовые акты Норвегии

А) Государственный строй и общая характеристика права Норвегии

Норвегия является унитарным государством, что определяет единство законодательства и системы государственных органов, действующих на территории всей страны. Форма правления – конституционная монархия установлена Конституцией 1814 г. Законодательная власть принадлежит однопалатному парламенту. Глава государства – король - подписывает законы, а также председательствует на заседаниях Кабинета (правительства). Король назначает Премьер-министра – как правило, лидера крупнейшей парламентской партии и предлагает ему сформировать правительство.

Право Норвегии относится к Северному праву, которое по ряду характеристик (роль кодификации, судебной практики, понятийному аппарату) отличается от стран романо-германского права. Право Норвегии тесно связано с другими странами данной группы.

Б) Общий обзор законодательства в сфере управления данными

В Норвегии действуют ряд законов и подзаконных актов, непосредственно регулирующих отношения в сфере оборота данных.

Закон о свободе информации[67] Норвегии 2006 года предусматривает содействие открытому и прозрачному государственному управлению, реализации права граждан на доступ к информации о деятельности публичных органов. Закон закрепляет принцип недискриминационного доступа к данным (недопустимости эксклюзивных соглашений о предоставлении данных), устанавливает процедуру запроса данных, обязанности государственных органов в раскрытии и предоставлении данных, условия и ограничения использования данных. Также в Законе закреплены правовые основы повторного использования данных.

---

[67] Freedom of Information Act. URL: https://app.uio.no/ub/ujur/oversatte-lover/data/lov-20060519-016-eng.pdf (дата обращения 08.08.2019).

Закон о публичном управлении 1967 года (с поправками 2003 года)[68] закрепляет основы деятельности административных органов (administrative agencies[69]) при принятии ими административных решений[70]. Помимо прочего, Закон устанавливает, что административные органы взаимодействует с гражданами в электронной форме по умолчанию, если они не решат от нее отказаться (модель opt-out).

Закон о защите персональных данных 2018 года[71] содержит принципы, аналогичные положениям законодательства ЕС в сфере защиты персональных данных (ранее действовавшая Директива 1995 года и нынешний Регламент 2016 года).

Помимо законодательных актов, на государственном уровне в Норвегии приняты стратегии, программные документы в области цифровизации государственного управления и оборота данных[72].

Концепция развития информационно-коммуникационных технологий отражена в Цифровой повестке (регулярно публикуется в форме рекомендаций Министерства местного управления и модернизации в

---

[68] Public Administration Act. URL: https://app.uio.no/ub/ujur/oversatte-lover/data/lov-19670210-000-eng.pdf (дата обращения 08.08.2019).

[69] Под административными органами понимается любой центральный либо местный орган исполнительной власти. Для целей закона частное юридическое лицо приравнивается к административному органу, если оно выполняет административные функции.

[70] Под административными решениями в законе понимаются решения, принимаемые во исполнение публичной власти и определяющие права и обязанности частных лиц (физических лиц или частных юридических лиц).

[71] Personal Data Act. URL: http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan033937.pdf (дата обращения 08.08.2019).

[72] Политические заявления, стратегии развития, законодательство, другие вопросы государственного управления и инфраструктуры в области электронного государства и электронных услуг для граждан и бизнеса отражены в Докладе о развитии электронного государства в Норвегии 2019 г.[72] Доклад является частью ежегодного исследования развития электронного государства в странах Европейского союза. См. Digital Government Factsheet 2019. Norway. URL: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Norway_2019.pdf (дата обращения 08.08.2019).

сокращенной[73] и полной[74] версии). Цифровая повестка Норвегии основана на следующих приоритетах развития:

– ориентированность на пользователя (вся система управления должна строиться на потребностях пользователей; минимизация барьеров к получению услуг; недопустимость повторного сбора идентичной информации и т.п.),

– эффективное использование ИКТ (использование административными органами общих решений для достижения совместных целей, использование возможностей рынка и т.п.),

– развитие цифровых компетенций и повышение вовлеченности в цифровые технологии (цифровизация образования на всех уровнях, повышение доверия к технологиям),

– цифровизация публичного сектора (использование публичными органами общих решений для достижения совместных целей, использование возможностей рынка и т.п.),

– надежная защита персональных данных и информационная безопасность (информационная безопасность и защита данных должны быть неотъемлемым элементом цифровизации; граждане должны иметь право и возможность контролировать свои данные; обработка данных должна соответствовать всем принципам защиты данных; должен поддерживаться риск-ориентированный подход к информационной безопасности).

---

[73] Digital agenda for Norway in brief. ICT for a simpler everyday life and increased productivity. URL: https://www.regjeringen.no/contentassets/07b212c03fee4d0a94234b101c5b8ef0/en-gb/pdfs/digital_agenda_for_norway_in_brief.pdf (дата обращения 08.08.2019).

[74] Digital Agenda for Norway. ICT for Growth and Value Creation. URL: https://www.regjeringen.no/contentassets/4339bb2154bd4b829f1d147bb2b26da8/en-gb/pdfs/stm201220130023000engpdfs.pdf (дата обращения 08.08.2019).

Стратегии во многом основаны на стратегии ЕС о построении Единого цифрового рынка 2015 года[75]. Отмечается важность интеграции в единое цифровое пространство ЕС, рецепции принципов интероперабельности ЕС.

Среди направлений цифровизации государственных услуг фигурируют:

– использование единой учетной записи в большинстве государственных электронных услуг,

– развертывание электронных сервисов для бизнеса,

– переход от принципа «с согласия» (opt-in) к принципу «по умолчанию» (opt-out) в вопросах электронного взаимодействия с пользователями,

– дальнейшее внедрение цифрового почтового ящиков граждан,

– развитие сервисов электронного здравоохранения (электронные рецепты и т.п.).

Министерством иностранных дел в 2019 году разработана Цифровая стратегия политики развития[76], направленная на поддержку цифровизации развивающихся стран в партнерстве с Норвегией. Приоритетными направлениями развития являются здравоохранение, образование, экология, сельское хозяйство, энергетика, гуманитарная помощь. Стратегия предполагает учреждение партнерских программ цифровизации (оказание помощи другим странам в устранении цифрового разрыва), главным образом в странах, где работают многие норвежские IT-компании. Также предполагается сотрудничество с международными организациями – ООН,

---

[75] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192 (дата обращения: 10.10.2019).

[76] Digitalisation for Development. Digital strategy for Norwegian development policy. https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/utvpolitikk/digital_strategynew.pdf (дата обращения 08.08.2019).

Всемирным банком и др. Цифровая стратегия основывается на следующих принципах:

– цифровая коммуникация должна быть общим правилом взаимодействия с государственными органами,

– идентификация в электронных публичных сервисах должна быть упрощенной и безопасной,

– граждане и организации должны получать сообщения из государственных органов в электронные почтовые ящики,

– уведомления из государственных органов должны поступать гражданам и организациям посредством СМС и электронной почты,

– поддержка граждан в использовании цифровых технологий при взаимодействии с государственными органами,

– развитие IT-решений должно осуществляться с учетом особенностей процессов в государственном секторе,

– информационная безопасность и защита данных,

– координация средств цифровизации для разных сервисов.

Инфраструктура цифровизации предполагает развитие цифрового профиля, системы электронных почтовых ящиков граждан и организаций, развитие государственных реестров и т.д. Пользователи должны быть вовлечены в развитие государственных услуг. Публичный сектор должен быть открытым и доступным, коммуникации с государственными органами должны быть ясными и понятными.

Деятельность в области кибернетической безопасности определена правительством в Национальной стратегии кибербезопасности 2018 года[77].

[77] National Cyber Security Strategy for Norway. URL:https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf (дата обращения 08.08.2019).

Принимающая во внимание современные вызовы цифровизации общества, Стратегия кибербезопасности имеет следующие цели:

– норвежские компании проходят процессы цифровизации в безопасном и надежном формате, а также способны защитить себя от киберугроз и инцидентов,

– критические социальные сервисы обеспечиваются надежной цифровой инфраструктурой,

– приоритет развития компетенций в сфере кибербезопасности,

– общество повышает навыки обнаружения и предотвращения кибератак,

– правоохранительные органы эффективно противодействуют киберпреступлениям.

Важная роль в кибербезопасности возлагается на развитое взаимодействие заинтересованных сторон. В частности, государство и бизнес должны совместно определять вызовы кибербезопасности, обмениваться опытом в противодействии угрозам. Взаимодействие должны быть основано на принципах прозрачности, доверия и взаимности. Государство должно содействовать формированию бизнес-сообщества, чьи приоритеты состоят в обеспечении кибербезопасности.

Национальная стратегия геоданных Норвегии на срок до 2025 г.[78] основывается на признании геоданных важных ресурсом, который может использоваться в самых разных областях: в экологии, энергетике, городском хозяйстве, на транспорте, в чрезвычайных ситуациях. Отмечается, что потенциал использования геоданных пока не реализован. Требуется развертывание инфраструктуры для более эффективного использования

[78] National geospatial strategy towards 2025. URL: https://www.regjeringen.no/contentassets/6e470654c95d411e8b1925849ec4918d/en-gb/pdfs/en_nasjonal_geodatastrategi.pdf (дата обращения 08.08.2019).

геоданных всеми заинтересованными лицами и сторонами. Инфраструктура должна быть удобной и доступной. Геоданные должны поставляться в машиночитаемом формате, иметь преимущественно характер открытых данных. Отдельное внимание уделяется вопросам финансирования инфраструктуры геоданных и справедливому распределению издержек и выгод от их использования.

Министерством торговли, промышленности и рыбного хозяйства Норвегии разработана стратегия «Норвегия - страна центров обработки данных»[79]. Данная Стратегия исходит из идеи, что государственные органы должны развивать цифровые инновации в различных отраслях, максимизировать пользу использования данных в целях устойчивого развития. Стратегия направлена на развитие индустрии обработки данных, а также на стимулирование частного бизнеса к использованию достижений в сфере обработки данных.

В) Государственные органы в сфере управления данными

Основными государственными органами, определяющими государственную политику и осуществляющими регулирование в сфере оборота данных, являются Правительство, Департамент информационной политики и реформ публичного сектора (Department of ICT Policy and Public Sector Reform), а также Министр цифрового развития (Minister of Digitalisation) при Министерстве местного управления и модернизации (Ministry of Local Government & Modernisation), Агентство государственного управления и электронного правительства (Agency for Public Management and e-Government), Агентство защиты данных (Data Protection Agency). Отраслевые органы государственной власти также принимают отдельные

[79] Strategy. Norway as a data centre nation. URL: https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/strategier/strategi-nfd-eng-nett-uu.pdf (дата обращения 08.08.2019).

правовые акты, касающиеся оборота данных в конкретных сферах общественных отношений.

1.3.5 Нормативные правовые акты Эстонии

А) Государственный строй и общая характеристика права Эстонии

Эстония – унитарное государство с республиканской формой правления. В качестве суверенного государства существует с 1991 г.

Президент Эстонии − глава государства назначает высших должностных лиц, Премьер-министра, Председателя Верховного суда, генерального аудитора, президента Банка Эстонии.

Кандидатура Премьер-министра утверждается парламентом. По сути, им становится лидер наиболее крупной парламентской партии.

Исполнительную власть осуществляет Кабинет. Вспомогательную деятельность осуществляет правительственный секретариат, руководитель которого имеет ранг государственного секретаря.

Кабинет также координирует деятельность государственных агентств.

В 2000 г. Кабинет Эстонии перешел с бумажного документооборота на цифровой формат деятельности – е-Кабинет. Министры получили возможность доступа к электронному Кабинету со своих девайсов. Система электронного Кабинета подключена к электронной консультативной системе. Последняя позволяет каждому из министров как обсуждать проекты с другими министрами, так и проводить общественное обсуждение. Документы подписываются в электронном виде и хранятся в архиве.

В настоящее время правовая система Эстонии принадлежит к правовой семье континентального (романо-германского) права. После советского периода право было приведено в соответствие с правом ЕС.

Б) Общий обзор законодательства в сфере управления данными

В Эстонии действуют ряд законов и подзаконных актов, регулирующих отношения в сфере оборота данных.

Закон Эстонии о публичной информации[80] 2000 года (Public Information Act) распространяется на органы исполнительной государственной власти и местного самоуправления, на юридических лиц публичного права, а также на частных лиц, выполняющие публичные функции[81]. Любое заинтересованное лицо может направить запрос на получение соответствующей информации и в течение пяти дней получить ответ. Закон обязывает государственные органы вести веб-сайты и размещать на них существенную часть публичной информации. Обладатели информации обеспечивают актуальность, точность и достоверность данных.

Обеспечение доступа к публичной информации[82] основывается на следующих принципах:

– обязанность предоставления публичной информации имеет целью обеспечение демократии и публичных интересов, реализацию каждым своих прав и свобод,

---

[80]Public Information Act. https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения 08.08.2019).

[81] Обязанности держателям информации распространяются на юридических лиц частного права и физических лиц, если эти лица выполняют публичные обязанности в соответствии с законодательством, или договорами, включая случаи предоставления образовательных, медицинских, социальных или других публичных услуг, - в отношении информация о выполнении своих обязанностей.

К держателям информации (data holders) также приравниваются предприятия, доминирующее на рынке или обладающие особыми или исключительными правами или являющиеся естественными монополиями, - в отношении информации об условиях и ценах поставки товаров и услуг и их изменениях; индивидуальные предприниматели, некоммерческие ассоциации, фонды и компании - в отношении информации об использовании средств, выделенных из государственного бюджета или бюджета местного самоуправления для выполнения общественных обязанностей или в качестве поддержки.

[82] Под публичной информацией в законе понимается информация, записанная на любом носителе и любым способом документированная, которая получается или создается в процессе исполнения публичных обязанностей, предусмотренных законом или подзаконными актами.

– доступ должен быть обеспечен каждому лицу в максимально возможные короткие сроки и наиболее удобным способом,

– при обеспечении доступа к информации не допускается нарушение права на частную жизнь и авторских прав,

– доступ к информации бесплатен, кроме случаев, когда закон позволяет покрывать прямые издержки на предоставление информации (в этих случаях держатель информации обязан опубликовать условия, на которых предоставляется информация за плату, с объяснением ценообразования; такие условия должны быть равными для всех и не должны нарушать конкуренции),

– любое лицо может оспорить ограничение доступа к информации, если такое ограничение нарушает его права или свободы.

Кроме того, Закон устанавливает правовые основы интероперабельности в сфере управления данными. В Законе закреплены принцип недопустимости дублирования сбора информации и концепция «базовых данных», определяющая авторитетный источник каждого вида информации, хранящихся в публичных базах данных. При создании новых баз данных или изменении в структуре существующих баз, Закон предписывает обязательную процедуру согласования с органами, ответственными за информационные технологии, защиту данных и сбор статистики.

Закон о защите персональных данных[83] 2018 года (Personal Data Protection Act) развивает и дополняет положения Регламента ЕС от 27.04.2016 №2016/679 о защите данных (GDPR). Закон устанавливает специальные случаи обработки персональных данных без согласия субъекта

[83]Personal Data Protection Act. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide (дата обращения 08.08.2019).

персональных данных, раскрывает требования к их защите при их обработке. Отдельное внимание уделено обработке персональных данных государственными органами при осуществлении их полномочий, а также деятельности по контролю и надзору в сфере обработки персональных данных.

Принципы управления сервисами и информацией[84] 2017 года (Principles for Managing Services and Governing Information), принятые Кабинетом, устанавливают новый подход к разработке и управлению публичными сервисами (услугами). Публичные сервисы должны быть основаны на потребностях пользователей и, по возможности, проактивными (то есть предоставляться автоматически или требовать лишь согласия пользователя). Среди них выделяются проактивные сервисы (proactive services), сервисы «по случаю» (even services, оказываемые несколькими публичными органами по конкретному запросу) и сервисы поддержки (support services, оказываемые госслужащим при осуществлении ими своих функций). Принципы устанавливают процедуру управления информацией (обеспечение управления, обмен данными во всех информационных системах и базах данных). Также учреждена система координации в сфере управления сервисами и информацией.

Закон Эстонии о кибербезопасности[85] 2018 года (Cybersecurity Act) имеет целью усиление безопасности информационных систем, используемых при оказании жизненно важных услуг. Закон устанавливает требования к поддержанию безопасности систем, процедуры предотвращения и

---

[84] Principles for Managing Services and Governing Information. URL: https://www.riigiteataja.ee/en/eli/507072017004/consolide (дата обращения 08.08.2019).

[85] Cybersecurity Act. URL: https://www.riigiteataja.ee/en/eli/523052018003/consolide (дата обращения 08.08.2019).

разрешения кибер-инцидентов, а также регулирует вопросы контроля, надзора и ответственности за нарушения в сфере кибербезопасности.

Требования к доступности вебсайтов и мобильных приложений и правила опубликования информации о доступе[86] (Requirements for accessibility of websites and mobile applications, and rules for publishing information describing accessibility) устанавливают, что доступность вебсайтов и мобильных приложений в соответствии с требованиями Закона о публичной информации означает, что они должны быть воспринимаемыми, понятными и надежными. При этом презюмируется, что вебсайт или приложение отвечают требованиям доступности, если они соответствуют европейскому стандарту (European standard EN 301 549 V2.1.2 2018-08).

Закон об обмене налоговой информации 2014 года[87] (Tax Information Exchange Act) в части управления данными устанавливает систему автоматизированного обмена финансовой информаций в целях контроля за исполнением налоговых обязательств. Требования к конвертации документов в электронной форме в электронные базы данных, позволяющих обеспечивать удобный доступ к информации в налоговой сфере[88] (The requirements for the conversion of the documents preserved in electronic form into electronic databases allowing excess to legible information) закрепляют требования к формату, метаданным, структуре направляемых в налоговые органы документов.

---

[86] Requirements for the accessibility of websites and mobile applications, and the rules for publishing information describing accessibility. URL: https://www.riigiteataja.ee/en/eli/ee/EVIM/reg/512042019003/consolide (дата обращения 08.08.2019).

[87] Tax Information Exchange Act. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042019004/consolide (дата обращения 08.08.2019).

[88] The requirements for the conversion of the documents preserved in electronic form into electronic databases allowing excess to legible information. https://www.riigiteataja.ee/en/eli/ee/RHM/reg/524092014007/consolide (дата обращения 08.08.2019).

Закон Эстонии о государственной тайне и засекреченной информации иностранных государств[89] 2007 года (State Secrets and Classified Information of Foreign States Act) устанавливает правовой режим государственной тайны, подразделяемой на 4 уровня: ограниченный (restricted), конфиденциальный (confidential), секретный (secret) и совершенно секретный (top secret). Кроме того, Закон регламентирует отношения, связанные с защитой засекреченной информации иностранных государств (classified information of foreign states).

Министерством экономики и коммуникаций Эстонии в 2011 году разработан документ «Интероперабельность государственных информационных систем»[90] (Interoperability of the State Information System). В документе под интероперабельностью понимается способность различных организаций взаимодействовать для достижения взаимовыгодных и согласованных общих целей, включая обмен информацией и знаниями между организациями посредством информационного обмена между информационными системами. Основой интероперабельности являются стандарты и открытые платформы. Принципы интероперабельности направлены на подготовку соответствующих правовых актов и разработку необходимых IT-решений. Данные принципы – стратегический документ, на который должны ориентироваться субъекты, обеспечивающие интероперабельности в публичной сфере, а также выступают ориентиром для развития интероперабельности в частном секторе.

Основой интероперабельности являются стандарты и открытые платформы. Принципы интероперабельности направлены на подготовку

---

[89] State Secrets and Classified Information of Foreign States Act. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042019009/consolide (дата обращения 08.08.2019).

[90] Interoperability of the State Information System. https://www.mkm.ee/sites/default/files/interoperability-framework_2011.doc (дата обращения 08.08.2019).

соответствующих правовых актов и разработку необходимых IT-решений. Интероперабельность государственных систем имеет своей целью:

– способствовать развитию сервис-ориентированного общества, где граждане смогут общаться с государством, не вникая в иерархическую структуру государственного аппарата и разделение компетенций в нем,

– обеспечивать прозрачность в принятии политических решений,

– поддерживать совместное развитие государственной информационной системы,

– создавать условия для свободной конкуренции,

– сокращать государственные расходы на ИТ.

Интероперабельность основана на следующих принципах: субсидиарность и пропорциональность; ориентированность на пользователя; доступность; безопасность и конфиденциальность; многоязычие; упрощение административных процедур; прозрачность; сохранение информации; открытость; повторное использование; технологическая нейтральность и адаптивность; результативность.

Последние достижения в области развития электронного государства в Эстонии, касающиеся стратегического планирования, законодательства, системы государственного управления, инфраструктуры, сервисов для граждан и бизнеса освещены в Докладе о развитии электронного государства [91] 2019 года. Доклад является частью ежегодного исследования Европейской комиссии о развитии электронного здравоохранения в странах Европы.

[91] Digital Government Factsheet 2019. Estonia. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Estonia_2019.pdf (дата обращения 08.08.2019).

Цифровая повестка Эстонии-2020[92] (Digital Agenda 2020 for Estonia) представляет собой стратегию развития цифровой экономики (принята Кабинетом в последней версии в 2018 году). В стратегии делается акцент не на внедрение информационных технологий в отдельные отрасли, а на создание развитой и безопасной среды для повсеместного обмена данными и IT-решениями. В связи с указанной целью стратегия имеет две основные части: одна посвящена развитию информационного общества, другая – кибербезопасности.

Ключевыми направлениями стратегии являются:

– развитие сверхскоростного широкополосного доступа в Интернет, внедрение сетей нового поколения (5G),

– упрощение процедур получения государственных услуг в электронном виде, чтобы взаимодействие было максимально «незаметным» для пользователей (проактивным),

– расширение возможностей использования аналитики данных и исследований в публичном секторе,

– внедрение приложений, основанных на искусственном интеллекте, в публичный сектор, реализация пилотных проектов,

– обеспечение прозрачности обработки персональных данных в публичном секторе (пользователь должен знать, кто, когда, каким образом и для каких целей использует его данные, а также должен иметь возможность для выражения согласия на обработку его данных в общественно-значимых целях – в исследования, разработке новых сервисов и т.д.),

– обучение ИКТ-специалистов, развитие ИКТ-навыков,

---

[92] Digital Agenda 2020 for Estonia. https://www.mkm.ee/sites/default/files/digitalagenda2020_final_final.pdf (дата обращения 08.08.2019).

– усиление готовности государства и частных лиц (предприятий) противодействовать угрозам кибербезопасности,

– поддержка частных инициатив в области электронного государства и кибербезопасности,

– развитие концепции «цифровой личности», программы электронного резидентства.

Другим стратегическим документом в сфере цифровизации государственного управления является План развития открытого государственного партнерства на 2018-2020 гг.[93] (Estonia's Open Government Partnership Action Plan for 2018-2020). Данный акт является стратегией, направленной на увеличение открытости, прозрачности, ориентированности на граждан сферы осуществления публичной власти посредством использования современных технологий. Например, план предполагает разработку новой информационной системы, обеспечивающей более активную вовлеченность в законотворческий процесс всех заинтересованный лиц.

В) Государственные органы в сфере управления данными

Основными государственными органами, определяющими государственную политику и осуществляющими регулирование в сфере оборота данных, являются Кабинет, Министерство экономики и коммуникаций (Ministry of Economic Affairs and Communications), входящие в состав Министерства Департамент государственных информационных систем (RISO, Government CIO Office), Департамент развития услуг информационного общества (ITAO, Department of Information Society Services Development), Агентство информационных систем (RIA, Estonian Information

[93] Estonia's Open Government Partnership Action Plan for 2018-2020. URL: https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/AVP/ogp_2018-2020_estonia.pdf (дата обращения 08.08.2019).

System Authority). Органом в сфере защиты данных является Инспекция защиты данных (EDPI, Estonian Data Protection Inspectorate), подчиняющаяся Министерству юстиции Эстонии. Отраслевые органы государственной власти также принимают отдельные правовые акты, касающиеся оборота данных в конкретных сферах общественных отношений.

1.3.6 Правовые акты США

А) Государственный строй и общая характеристика права США

США – федеративное государство с республиканской формой правления, установленной Конституцией 1787 г. на основе принципа «сдержек и противовесов».

Президент является главой государства и главой исполнительной власти. Он избирается на четыре года путем косвенных выборов. По совету и с согласия Сената он назначает высших должностных лиц. При Президенте создано Исполнительное управление, в состав которого входят Управление Белого дома, Совет национальной безопасности, Административно-бюджетное управление, Управление развития политики, Экономический совет, Административное управление, ряд других структур.

Система управления США сложна. Кроме исполнительных департаментов создаются иные органы для решения отдельных задач (агентства, комиссии, бюро). Также создаются межведомственные органы

Право США относится к правовой семье «общего права». По сути это понятие охватывает 51 правовую систему – федеральное право и право 50 штатов. Каждый штат имеет законодательный, исполнительные и судебные органы, конституцию и систему источников права.

На федеральном уровне действует старейшая писаная Конституция 1787 г. Традиционным источником права является судебный прецедент. Вместе с тем большую роль играют статуты (законы) и акты исполнительных органов (делегированное законодательство). Кодификация не достигла уровня стран романо-германского права. Правовую систему отличает ряд

терминологических и стилистических особенностей (tort, trust, judicial remedies).

Б) Общий обзор законодательства в сфере управления данными

Закон США об открытых, общедоступных, электронных и необходимых государственных данных 2018 г. (Open, Public, Electronic, and Necessary Government Data Act of 2018[94] (S. 760 / H.R. 1770) устанавливает, что открытые государственные информационные ресурсы, предоставляемые федеральными государственными органами (агентствами, за исключением некоторых, указанных в Законе), должны публиковаться в виде машиночитаемых данных. Если иное не запрещено законом, государственные и непубличные данные, находящиеся в распоряжении федерального правительства, должны быть доступны: (1) в открытом формате, который не препятствует использованию или повторному использованию и в формате, который оперирует стандартами, поддерживаемые организацией по стандартизации; и (2) в соответствии с открытыми лицензиями с юридической гарантией того, что данные будут доступны общественности бесплатно без каких-либо ограничений на копирование, публикацию, распространение, передачу, цитирование или адаптацию.

Каждое из агентств обязано: (1) сделать реестр данных доступным для общественности посредством Data.gov, и (2) назначить контактное лицо для связи с общественностью и реагирования на жалобы о соблюдении требований к открытым данным. В целях обеспечения конфиденциальности, безопасности или по иным причинам, определенным внутренними нормативными актами, агентство вправе вести закрытую часть реестра.

---

[94] Open, Public, Electronic, and Necessary Government Data Act. URL: https://www.congress.gov/bill/115th-congress/senate-bill/760?q=%7B%22search%22%3A%5B%22Open+Government+Data+Act%22%5D%7D&s=1&r=1 (дата обращения 08.08.2019).

Администрация общих служб (General Services Administration), федеральный орган исполнительной власти, управляющий государственной собственностью, ведущий реестры такой собственности, проводящий закупки в сфере IT для государственных и военных нужд и пр.[95], поддерживает единый публичный интерфейс в режиме онлайн в качестве точки входа, предназначенной для обмена данными Открытого правительства с общественностью.

Главный операционный директор каждого агентства направляет Конгрессу и Административно-бюджетному управлению Президента доклад (отчет) с оценкой охвата, качества, методов, эффективности и независимости усилий агентства в области оценки, исследований и анализа.

Административно-бюджетное управление (Office of Management and Budget, АБУ), орган Исполнительного офиса Президента США[96], в свою очередь направляет Конгрессу доклад, в котором обобщаются выводы, агентств, определяются тенденции, вытекающие из докладов, и при необходимости рекомендует меры дальнейшего укрепления потенциала агентств в области использования методов оценки данных. АБУ должно разрабатывать и поддерживать онлайн-хранилище инструментов, передовой практики и стандартов схем для облегчения внедрения практики открытых данных.

Закон о свободе информации 2016 г. (Freedom of Information Act 2016[97] (5 U.S.C. §552) требует полного или частичного раскрытия ранее не раскрытой информации и документов, контролируемых правительством

---

[95] 40 U.S.C. United States Code, 2001 Edition Title 40 - PUBLIC BUILDINGS, PROPERTY, AND WORKS CHAPTER 16 - GENERAL SERVICES ADMINISTRATION Sec. 751 - General Services Administration

[96] Reorganization Plan №1 of 1939 (5 U.S.C. app.)

[97] Freedom of Information Act. URL: https://www.congress.gov/114/bills/s337/BILLS-114s337enr.xml (дата обращения 08.08.2019).

Соединенных Штатов, по запросу. Закон определяет ведомственные отчеты, подлежащие раскрытию, устанавливает обязательные процедуры раскрытия и определяет девять исключений. Закон принят, чтобы сделать функции государственных органов более прозрачными.

Закон об основах обоснованной политики 2018 г. (Foundations for Evidence-Based Policymaking Act of 2018[98] (Public Law No 115-435) устанавливает требование, согласно которому крупнейшие государственные органы разрабатывают ежегодные планы сбора фактических данных. Эти планы включают: 1) вопросы политики, по которым каждый орган должен разрабатывать доказательства; 2) данные, которые необходимо собирать для сбора доказательств; и 3) другую информацию, необходимую для планирования деятельности. Эти планы включаются в стратегические планы, предусмотренные Законом о деятельности и результатах правительства (1993 г.; GPRA).

Каждый из этих органов назначает (1) координатора сбора фактических данных в рамках компетенции органа и (2) «статистического должностного лица» для консультирования по вопросам статистической политики, методов и процедур. Руководящие указания по стандартизации фактических данных дает АБУ.

При АБУ создается временный, рассчитанный на два года Консультативный комитет по данным для сбора доказательств, который будет выносить рекомендации, как содействовать использованию федеральных данных для сбора доказательств.

Агентства должны сделать свои данные «открытыми по умолчанию»; разработать планы открытых данных; сделать свои данные доступными в открытом формате и открытой лицензии, а также в виде машиночитаемых

---

[98] Evidence Act of 2018. URL: https://www.congress.gov/bill/115th-congress/house-bill/4174 (дата обращения 08.08.2019).

данных; и проводить всеобъемлющую инвентаризацию своих активов данных.

Закон о защите конфиденциальной информации и эффективности статистики 2002 г. (Confidential Information Protection and Statistical Efficiency Act of 2002[99] (116 Stat. 2899) устанавливает единообразную защиту конфиденциальности информации, собираемой статистическими органами, и позволяет обмениваться некоторыми данными между Бюро статистики и труда, Бюро экономического анализа и Бюро переписи населения. Учреждения сообщают АБУ о действиях, связанных с конфиденциальностью и обменом данными.

Закон предписывает ведомствам унифицированные подходы к защите информации от респондентов с тем, чтобы она не подвергалась воздействию, которое приводит к ненадлежащей или неожиданной идентификации респондента. По умолчанию данные респондента используются только в статистических целях. Если респондент дает информированное согласие, данные могут быть использованы в других целях.

Закон не дает статистическим органам новых полномочий в использовании федеральных данных о налогах на бизнес в сочетании с другими источниками для статистических целей. Такие данные защищены разделом 26, и потребуются новые законы, позволяющие другим учреждениям использовать такие данные, что поможет улучшить классификацию предприятий по отраслям и тем самым повысить точность отраслевой статистики. Более поздние предложения касаются этой перспективы.

---

[99] Confidential Information Protection and Statistical Efficiency Act of 2002. URL: https://www.eia.gov/cipsea/cipsea.pdf (дата обращения 08.08.2019).

Закон о модернизации информационной безопасности 2014 г. (Federal Information Security Modernization Act of 2014[100] (128 Stat. 3073), заменивший Закон о модернизации информационной безопасности 2002 г. (Federal Information Security Modernization Act of 2002 (FISMA, 44 U.S.C. § 3541), требует от каждого федерального агентства разрабатывать, документировать и осуществлять общую программу безопасности информации и систем, поддерживающих операции и активы агентства, включая те, которые предоставляются или управляются другим агентством.

Закон о модернизации информационной безопасности 2014 г. вносит изменения в Закон об управлении информационной безопасностью 2002 г. (FISMA) и предусматривает несколько изменений, которые модернизируют федеральные методы обеспечения безопасности для решения ее проблем. Эти изменения приводят к снижению общего объема отчетности, усилению непрерывного мониторинга в системах, повышению внимания к учреждениям за соблюдением отчетности, которая в большей степени сосредоточена на вопросах, вызванных инцидентами в области безопасности.

FISMA прямо подчеркивает политику, основанную на рисках, для обеспечения экономически эффективной безопасности. В целях поддержки и укрепления этого законодательства АБУ циркуляром А-130 «Управление федеральной информацией как стратегическим ресурсом» требует от органов федерального правительства:

– плана обеспечения безопасности,

– ответственности должностных лиц за обеспечение безопасности,

– периодической ревизии элементов управления безопасностью в сих системах,

---

[100] Federal Information Security Modernization Act of 2002: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf (дата обращения 08.08.2019).

– авторизации системной обработки до начала операций и периодически после них.

Заявленная цель Закона об электронном правительстве 2002 г. (E-Government Act of 2002[101]) заключается в совершенствовании управления и продвижения электронных государственных услуг и процессов путем создания должности главного информационного сотрудника в АБУ, а также путем разработки мер, которые требуют использования информационных технологий на основе Интернета для улучшения доступа граждан к правительственной информации и услугам и для других целей. Закон включает: FISMA (Закон об управлении информационной безопасностью 2002 года) в качестве раздела III (см. выше), CIPSEA (Закон о защите конфиденциальной информации и статистической эффективности) в качестве раздела V (см. выше).

Цель Закона о политике кабельной коммуникации 1984 г. (Cable Communications Policy Act of 1984[102] (98 Stat. 2779) − поиск баланса между FCC (Federal Communications Commission – Федеральная комиссия связи, федеральный орган исполнительной власти, регулятор в сфере теле-, радио-коммуникации, а также телефонной связи и спутниковой связи[103]), местными органами власти и компаниями товарных рынков, где в прошлом каждая из этих организаций соперничала за доминирование. Закон должен был стать решением сохраняющейся проблемы: кто или что должно осуществлять наибольшую власть над местными кабельными операциями. Государственные органы должны разрешать, но не обязывать, чтобы

---

[101] E-Government Act of 2002. URL: https://www.congress.gov/bill/107th-congress/house-bill/2458) (дата обращения 08.08.2019).

[102] Cable Communications Policy Act of 1984. URL: https://www.congress.gov/bill/98th-congress/senate-bill/66 (дата обращения 08.08.2019).

[103] Communication Act of 1934 (47 U.S.C. 151 et seq.) (дата обращения: (08 08 2019)

информация распространялась через некоммерческие общественные, образовательные и правительственные каналы кабельного телевидения.

Действие закона о защите конфиденциальности детей в Интернете 1998 г. (Children's Online Privacy Protection Act of 1998[104] (COPPA) (112 Stat. 2681-728) распространяется на веб-сайты или онлайн-ресурсы, чьей аудиторией являются лица младше 13 лет и веб-сайты или онлайн-ресурсы, которые сами собирают их персональные данные; чьей аудиторией являются лица младше 13 лет и веб-сайты или онлайн-ресурсы, которые позволяют третьим лицам собирать персональные данные детей; чьей аудиторией являются все лица, но имеются данные, что среди пользователей есть лица младше 13 лет, и их ПД персональные данные подлежат сбору, использованию, а также на рекламные сети или плагины, которые собирают персональные данные лиц младше 13 лет с веб-сайтов или онлайн-ресурсов.

В соответствии с COPPA персональные данные детей включают в себя: имя и фамилию, домашний адрес или адрес места пребывания, включая название населенного пункта и улицы, информацию об онлайн-контактах, аватар или имя пользователя, если такую информацию можно приравнивать к информации об онлайн-контактах, номер телефона, номер социального страхования, определитель пользователя (номер пользователя в cookies, IP-адрес, серийный номер процессора или устройства, уникальный идентификатор устройства и пр.), фотографию, видео, аудио, содержащие изображение ребёнка и/или его голос; информацию о геолокации, достаточную для определения названия улицы и города/городского поселения, информацию о ребёнке или его родителях, которую оператор

[104] Children's Online Privacy Protection Act of 1998. URL: https://searchcompliance.techtarget.com/definition/COPPA-Childrens-Online-Privacy-Protection-Act (дата обращения 08.08.2019).

собирает онлайн у ребёнка и совмещает ее с любым из видов ПД, перечисленных выше.

Под сбором персональных данных в соответствии с COPPA понимается 1) запрос, побуждение, поощрение ребёнка к предоставлению своих персональных данных онлайн; 2) предоставление ребёнку возможности сделать свои персональные данные публично доступными в идентифицирующей форме (сбор данных в данном случае не происходит, если оператор принимает надлежащие меры для удаления всех персональных данных из публикаций, сделанных ребёнком в сети, прежде чем они становятся общедоступными, а также для удаления всех персональных данных из своих записей; 3) пассивное отслеживание ребёнка онлайн (например, отслеживание при помощи GPS).

Под удалением персональных данных ребёнка понимается удаление с невозможностью воспроизведения этих данных в определенной форме и их возвращения в ходе ведения бизнеса.

Под раскрытием персональных данных ребёнка понимается:

– распространение собранных персональных данных операторами в любых целях, кроме цели предоставления персональных данных лицу, которое оказывает поддержку внешних операций веб-сайта или онлайн-сервиса (поддержка внешних операций веб-сайта или онлайн-сервиса включает: действия, необходимые для поддержания или анализа функционирования веб-сайта или онлайн-сервиса; осуществление сетевого соединения для веб-сайта или онлайн-сервиса; аутентификацию пользователей веб-сайта или онлайн-сервиса или персонализацию их данных; осуществление контекстной рекламы на веб-сайте или онлайн-сервисе, а также подсчет частоты контакта пользователей с контекстной рекламой; защиту безопасности и целостности пользовательского аккаунту, веб-сайта или онлайн-сервиса; обеспечение юридического и технического соответствия; удовлетворение запросов детей-пользователей в разовой форме с последующим удалением всех полученных персональных данных ребёнка;

удовлетворение запросов детей-пользователей на постоянной основе при условии получения родительского согласия с последующим использованием персональных данных ребёнка исключительно для целей этих запросов (без возможности раскрытия персональных данных и их комбинирования с иной информацией о ребёнке);

– опубликование собранных персональных данных в сети Интернет, на персональной домашней странице или опубликование скриншота, содержащего персональные данные, на веб-сайте или в онлайн-сервисе; в социальной сети, в электронной почтовой службе, на форуме, в чатах и пр.

В COPPA урегулирован вопрос получения согласия родителя на обработку персональных данных ребенка, а также порядок уведомления родителя. Так, оператор должен получить подтвержденное согласие, т.е. прежде чем собрать персональные данные ребёнка он должен уведомить родителя, что он собирает персональные данные, как их использует и кому передает, а родитель, в свою очередь, подтверждает согласие со сбором, использованием и/или распространением персональных данных.

В уведомлении указывают цели сбора данных, цели получения согласия, гиперссылку на онлайн-уведомление оператора, способы выражения согласия, указание, что, если родитель своевременно не дает согласия, оператор удаляет контактные данные родителя из своих записей.

В онлайн-уведомлении оператора, ссылка на которое размещается в зоне сайта, чьей аудиторией являются дети, указываются: имена, адреса, телефонные номера, адреса электронной почты операторов; описание данных, которые собирают операторы; указание на то, что родители могут редактировать и удалять персональные данные детей, а также запрещать последующий сбор и использование персональные данные их детей.

Оператор должен: доставить родителям форму согласия, которая заполняется и возвращается оператору по почте, посредством факсимиле или в виде скана; просить, чтобы родители при оплате ресурса использовали кредитную, дебетовую карту или любую иную платежную систему, которая

присылает оповещения о каждом денежном переводе основному владельцу счета; обзванивать родителей; связываться с родителями по видеоконференцсвязи; подтверждать личность родителя, проверяя удостоверение личности государственного образца в базе данных такой информации – когда подтверждение завершено, данные об удостоверении личности родителя, сохраненные в записях оператора, удаляются.

Уведомление родителя и его согласие не обязательно, если персональные данные ребенка и родителя используются в целях обеспечения безопасности ребенка без последующего распространения его данных, в целях выполнения единичного запроса ребенка, в целях поддержания функционала веб-сайта или онлайн-ресурса, в целях принятия мер предосторожности против наступления материальной ответственности, в целях выполнения требований судебного процесса, в целях оказания помощи при оперативных действиях, а также если пользователь ресурса, чья аудитория – дети, в ходе пользования ресурсом и при регистрации подтверждал, что он не ребенок.

Закон о защите частной жизни водителей 1994 г. (Driver's Privacy Protection Act of 1994[105] (18 U.S.C. § 2725) запрещает разглашение личной информации без явного согласия лица, к которому относится такая информация, за исключением обстоятельств, изложенных в 18 U.S.C. § 2721. Настоящие правила применяются к Federal Motor Carrier Safety Administration (федеральный орган исполнительной власти, способствующий повышению безопасности на дорогах – в том числе являбщийся ответственным органом за функционирование государственных информационных систем в сфере дорожной безопасности[106]), коммерческой организации Departments of Motor

[105] Driver's Privacy Protection Act of 1994. URL: https://www.law.cornell.edu/uscode/text/18/2721 (дата обращения 08.08.2019).

[106] The Motor Carrier Safety Improvement Act of 1999 (49 U.S.C. 113).

Vehicles, а также к другим «уполномоченным получателям личной информации» и устанавливают требования к учету «уполномоченных получателей».

Закон о справедливых и точных кредитных операциях 2003 г. (Fair and Accurate Credit Transactions Act of 2003[107] (117 Stat. 1952) направлен на усиление защиты от кражи личных данных путем стандартизации обработки номеров кредитных карт. Закон обеспечил физическим лицам свободный доступ к их кредитным отчетам и создал общенациональную систему оповещения.

Закон о честной кредитной отчетности 2003 г. (Fair Credit Reporting Act 2003[108] (FCRA) (15 U.S.C. § 1681) регулирует сбор кредитной информации потребителей и доступ к их кредитной отчетности. Федеральный орган, ответственный за соблюдение FCRA, – Office of Credit Ratings[109].

Закон о правах на образование и на конфиденциальность семьи (Family Educational Rights and Privacy Act[110] (20 U.S.C. §1232g) обеспечивает родителям доступ к записям об образовании их ребенка, право добиваться изменений в записях и контроль над раскрытием информации из архивных записей. Закон распространяется на образовательные учреждения и учреждения, которые получают средства в рамках программы, управляемой Министерством образования США. Орган, ответственный за исполнение акта – Family Policy Compliance Office (FPCO).

---

[107] Fair and Accurate Credit Transactions Act of 2003. URL: https://www.congress.gov/108/plaws/publ159/PLAW-108publ159.pdf (дата обращения 08.08.2019).

[108] Fair Credit Reporting Act. URL: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (дата обращения 08.08.2019).

[109] Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 USC 5301 note .

[110] Family Educational Rights and Privacy Act. URL: https://uscode.house.gov/view.xhtml?req=(title:20%20section:1232g%20edition:prelim) (дата обращения 08.08.2019).

Другие положения Закона, действующего с 2012 года, позволяют более широко раскрывать личную и справочную идентификационную информацию об обучающихся и регулировать студенческие удостоверения и адреса электронной почты. Например, школы могут поставлять внешним компаниям личную информацию ученика без его согласия.

Закон Грэмма–Лича–Блайли (Gramm–Leach–Bliley Act[111] (113 Stat. 1338) требует у Федеральной торговой комиссии[112], наряду с федеральными банковскими учреждениями и другими регулирующими органами, издавать нормативные акты, обеспечивающие защиту финансовыми организациями конфиденциальности личной финансовой информации потребителей. Такие учреждения должны уведомлять клиентов о своей политике конфиденциальности не реже раза в год (за исключением случаев, когда они освобождаются от ответственности), и прежде чем раскрывать личную финансовую информацию любого потребителя неаффилированной третьей стороне, давать уведомление и возможность потребителю отказаться от такого раскрытия. Пункт А также требует, чтобы FTC и другие учреждения издавали правила для защиты личной финансовой информации. Закон также ограничивает обмен информацией о номере счета в маркетинговых целях.

Закон о мобильности и подотчётности медицинского страхования (Health Insurance Portability and Accountability Act[113] (HIPAA) (110 Stat. 1936) используется для регулирования потока медицинской информации, защиты личной информации, хранящейся в сфере здравоохранения и медицинского страхования, от мошенничества и кражи, а также для устранения ограничений на медицинское страхование. Закон подписан Президентом

---

[111] Gramm–Leach–Bliley Act. URL: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (дата обращения 08.08.2019).

[112] The Federal Trade Commission Act (38 Stat. 717)

[113] Health Insurance Portability and Accountability Act. URL: http://counsel.cua.edu/fedlaw/Hipaa.cfm (дата обращения 08.08.2019).

Клинтоном в 1996 году, и в соответствии с ним федеральные органы (например, Управление санитарного надзора за качеством пищевых продуктов и медикаментов; далее – Управление) имеют право изучать электронные медицинские записи (и EHR, и EMR) и делать их копии в целях клинических исследований.

По общему правилу Управление обезличивает медицинские данные (удаляет имя и фамилию пациента), но также может использовать полноценные медицинские данные, если это необходимо для достижения цели исследования (реализации государственной миссии). Во втором случае обеспечивается конфиденциальность данных, хотя сохраняется возможность их раскрытия в исключительных случаях третьим лицам – например, в зале суда[114]. Данные, обрабатываемые Управлением, сегодня становятся федеральными данными. В соответствии с Законом об открытых, общедоступных, электронных и необходимых данных[115] федеральные данные – это данные, обрабатываемые федеральными органами власти в государственных информационных системах [116]. Федеральные данные публикуются в соответствующих реестрах США.

---

[114] Use of Electronic Health Record Data in Clinical Investigations, Guidance for Industry // U.S. Department of Health and Human Services Food and Drug Administration, Center for Drug Evaluation and Research (CDER), Center for Biologics Evaluation and Research (CBER), Center for Devices and Radiological Health (CDRH), July 2018 Procedural: https://www.fda.gov/media/97567/download (дата обращения: 10.08.2019)

[115] Open, Permanent, Electronic, and Necessary (OPEN) Government Data Act (S. 760 / H.R. 1770) https://www.congress.gov/115/bills/s760/BILLS-115s760is.pdf (дата обращения: 10.08.2019)

[116] К федеральным данным в соответствии с вышеупомянутым Актом относятся: публичные данные, непубличные данные (в т.ч. ПД), открытые данные; данные, используемые в информационной системе одного госоргана; данные, используемые в нескольких информационных системах государственных органов и бюро; данные, используемые в нескольких информационных системах государственных органов или создаваемые более чем одним государственным органом. В соответствии с Memorandum for the heads of executive departments and agencies – программные данные, статистические данные.

11.02.2019 Президент Трамп подписал Приказ «О сохранении лидерства США в области искусственного интеллекта» (Executive Order on Maintaining American Leadership in Artificial Intelligence)[117], который гласит, что к обработке федеральных данных и улучшению функционирования государственных информационных систем могут привлекаться фирмы, исследующие сферу искусственного интеллекта (AI-фирмы). Цель – облегчить управление данными, обрабатываемыми государственными органами[118]. Медицинские данные американских граждан как особая категория персональных данных может передаваться США третьим лицам без согласия на то пациентов, но во имя улучшения функционирования ГИСов. Будучи обезличенными, а именно такими по общему правилу в США являются федеральные данные, они не утрачивают связи с субъектом персональных данных, в связи с чем возникает множество рисков использования данных пациентов третьими лицами в корыстных целях.

С 2009 г. в США действует American Recovery and Reinvestment Act (далее – ARRA[119]), который определил направления реабилитации национальной экономики после финансового кризиса 2007–2008 гг. Одним из направлений стало повышение уровня компьютеризации медицинских учреждений и одновременно обеспечение безопасности медицинских данных пациентов, фиксируемых в электронных медицинских записях (Electronic medical records или EMR[120]), владельцами которых являются сами

---

[117] Executive Order on Maintaining American Leadership in Artificial Intelligence.:https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/ (дата обращения: 10.08. 2019)

[118] Federal Data Strategy: https://strategy.data.gov/ (дата обращения: 10.08. 2019)

[119] American Recovery and Reinvestment Act. https://www.congress.gov/bill/111th-congress/house-bill/1/text (дата обращения: 10.08.2019)

[120] Компьютеризация медицинских учреждений в США переживает процесс перехода от использования Electronic health records (EHR) к использованию Electronic medical records (EMR).

медицинские учреждения. Актом ARRA также была предусмотрена возможность обмена медицинскими данными через региональные центры и центры Штатов по хранению данных. Стали формироваться консолидированные базы медицинских данных.

В целях повышения безопасности аккумулируемых медицинских данных в 2009 году принят Health Information Technology for Economic and Clinical Health (HITECH) Act, которым введены крупные штрафы за нарушение в сфере хранения, обработки и передачи медицинских данных.

Закон о предотвращении хищения средств идентификации (Identity Theft and Assumption Deterrence Act[121] (112 Stat. 3007) является федеральным первым законом, криминализировавшим кражу личных данных. В дополнение к тому, что кража личных данных является преступлением, Закон предусматривает наказание лиц, совершившим или пытавшимся совершить кражу личных данных, и предусматривает конфискацию имущества, используемого или предназначенного для использования в мошенничестве. Закон также уполномочил Федеральную торговую комиссию «регистрировать и подтверждать получение жалоб физических лиц, которые утверждают, что у них есть разумное убеждение», что их

---

EHR содержат сведения об обращении пациента в разные медицинские учреждения; владельцем EHR является сам пациент или заинтересованное лицо; пациент имеет постоянный интерактивный доступ к EHR и может дополнять запись своими данными самостоятельно; EHR подключена к *Nationwide Health Information Network*.

EMR включают юридически значимые сведения о пациенте и медицинском учреждении, формируемые медицинскими учреждениями; сведения о факте оказания пациенту тех или иных медицинских услуг в медицинском учреждении; владелец EMR – медицинское учреждение; пациенту открыт доступ к результатам его медицинских исследовании через специальный портал – сервис не интерактивный, т.е. пациент не может вносить изменения в данные системы.

См. подробнее Garets D., Davis M. Electronic Medical Records vs. Electronic Health Records: Yes, There Is a Difference // A HIMSS Analytics. TM White Paper, 2006. https://www.aao.org/asset.axd?id=8e9b1f20-0ed6-4d2b-92f8e28fbaf378ec&t=634962799822530000 (дата обращения: 10. 08. 2019)

[121] Identity Theft and Assumption Deterrence Act. https://www.congress.gov/bill/105th-congress/house-bill/3601 (дата обращения 08.08.2019).

личная информация была «принята, украдена или иным образом незаконно приобретена».

Закон содержит расширительное определение кражи личных данных. Он включает в себя злоупотребление любой идентифицирующей информацией, которая может включать имя, SSN, номер счета, пароль или другую информацию, связанную с физическим лицом, для нарушения федерального законодательства или законодательства штата. Таким образом, определение охватывает злоупотребление существующими счетами, а также создание новых счетов.

Закон о частной жизни 1974 г. (Privacy Act of 1974[122] (88 Stat. 1896) устанавливает кодекс добросовестной информационной практики, который регулирует сбор, хранение, использование и распространение персональной информации о физических лицах, которая хранится в системах учета федеральными органами. Система записей – это группа записей, находящихся под контролем учреждения, из которой извлекается информация по имени лица или по какому-либо идентификатору, присвоенному этому лицу. Закон о конфиденциальности требует, чтобы учреждения публично уведомляли о своих системах учета путем публикации в Федеральном реестре. Закон запрещает разглашение информации из системы записей без письменного согласия соответствующего лица, за исключением случаев, когда разглашение осуществляется в соответствии с одним из двенадцати установленных законом исключений. Закон также предлагает отдельным лицам средства для получения доступа к своим записям и внесения в них изменений и устанавливает различные требования к ведению учета в агентстве. Кроме того, лицам, которым дано право

[122] Privacy Act of 1974. URL: https://www.justice.gov/opcl/privacy-act-1974 (дата обращения: 10.08.2019).

просматривать документацию с их именем, дано также право узнавать, были ли раскрыты записи, а также даются права на внесение исправлений.

К подзаконным актам, в соответствии с которыми осуществляется управление данными, относятся:

– Executive Order - Making Open and Machine Readable the New Default for Government Information (May 9, 2013) –Приказ об обязательном применении открытых и машиночитаемых стандартов для государственных данных,

– M-13-13 – Memorandum for the Heads of Executive Departments and Agencies (Project Open Data) - предписание государственным органам собирать или создавать информацию так, чтобы поддерживать последующую деятельность по обработке и распространению информации,

– Managing Information as a Strategic Resource[123] – циркуляр, устанавливающий политику в области управления информацией, приобретения, управления записями, открытых данных, рабочей силы, безопасности и конфиденциальности. В нем также подчеркивается роль конфиденциальности и безопасности в федеральном информационном жизненном цикле. Последующие изменения в циркуляре будут поощрять инновации, обеспечивать возможности надлежащего обмена информацией и способствовать широкомасштабному и быстрому внедрению новых технологий при одновременном укреплении защиты безопасности и конфиденциальности,

[123] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf (дата обращения 08.08.2019).

– OMB Circular A-119[124] – циркуляр, регулирующий использование и разработку добровольных консенсусных стандартов и деятельности по оценке их соответствия,

– Federal Cybersecurity: America's Data at Risk[125] – доклад об исключительной роли информации, содержащейся в системах государственных органов и потенциальной уязвимости этих органов.

Приказ «О сохранении лидерства США в области искусственного интеллекта»[126] разрешает привлекать к обработке федеральных данных и улучшению системы функционирования государственных информационных систем AI-фирмы. В соответствии с Приказом сообщества разработчиков искусственного интеллекта (AI) – вроде сообщества исследователей AI Facebook – https://research.fb.com/category/facebook-ai-research/, сообщества исследователей AI Google – https://ai.google/research/, и др. – получают возможность запрашивать федеральные данные у государства. Запрос таких данных производится, во-первых, с целью повышения качества федеральных данных за счёт их обработки высокими AI-технологиями. Во-вторых, с целью улучшения исследования, развития и тестирования самого искусственного интеллекта. Кейс-практика по данным, анализ которой необходим для воплощения положений данного приказа и Федеральной стратегии данных США в жизнь именуется «Use case» и публикуется на сайте Federal Data Strategy[127].

Мягкое право и общественные проекты включают:

---

[124] URL: https://www.nist.gov/standardsgov/what-we-do/federal-policy-standards (дата обращения 08.08.2019).

[125] URL: https://www.hsgac.senate.gov/imo/media/doc/2019-06-25%20PSI%20Staff%20Report%20-%20Federal%20Cybersecurity%20Updated.pdf (дата обращения 08.08.2019).

[126] Executive Order on Maintaining American Leadership in Artificial Intelligence. URL: https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/ (дата обращения: 10. 08. 2019)

[127] URL: https://strategy.data.gov/use-cases/ (дата обращения:10.08.2019)

– Education Data Exchange Network – автоматизированная система, предназначенная для поддержки передачи данных между федеральными и местными учреждениями образования и Министерством образования США,

– Federal Data Strategy[128] (Стратегия федеральных данных; ФД) устанавливает, что ее назначение состоит в использовании федеральных данных для общественного блага, формирования этического управления; в соответствии со Стратегией главы всех органов власти должны определить, какие ФД могут быть сообщены частным организациям, занимающимся исследованиями в сфере искусственного интеллекта. Модели взаимодействия с ФД должны соответствовать принципам защищенности, безопасности, приватности и конфиденциальности данных. В частности, органы власти должны обновить учетную документацию и документацию по обработке данных, чтобы гарантировать сохранение и дальнейшее использование данных. Должны быть приняты меры к улучшению доступа к данным и качеств данных, полученных с помощью использования AI – данные шаги должны основываться на заключениях сообществ исследователей искусственного интеллекта[129]. В Стратегии ФД также зафиксировано, что в течение 90 дней с момента публикации упомянутого Приказа директор Office of Management and Budget[130] должен опубликовать в Федеральном реестре[131] оповещение о приглашении общества к участию в определении (1) случаев, когда могут запрашиваться ФД, (2) способов/направлений повышения качества ФД и моделей взаимодействия с ФД, которые бы способствовали улучшению исследований, развития (R&D процессы) и тестирования

[128] URL: https://strategy.data.gov (дата обращения 08.08.2019).

[129] Sec. 5. Data and Computing Resources for AI Research and Development. https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/ (дата обращения: 10. 08. 2019)

[130] URL: https://www.whitehouse.gov/omb/ (дата обращения: 10. 08. 2019)

[131] URL: https://www.federalregister.gov/.https://www.whitehouse.gov/omb/information-for-agencies/federal-register/ (дата обращения: 10. 08. 2019)

искусственного интеллекта. Также в течение 90 дней с момента публикации Приказа Office of Management and Budget совместно со специальным комитетом (создается ad hoc) должны исследовать барьеры и модели использования ФД, которые затрудняют проведение исследований, развития (R&D процессы) и тестирования искусственного интеллекта. В течение 120 дней с момента публикации Приказа Office of Management and Budget совместно со специальным комитетом должен разработать рекомендации для ведения двух видов реестров: (1) реестров хранения и обработки данных, (2) реестров исходных кодов, которые бы способствовали проведению исследований, развитию (R&D процессы) и тестированию искусственного интеллекта. В течение 180 дней с момента публикации Приказа должны быть разработаны методы улучшения качества, применения и доступа к приоритетным данным, которые будут определены сообществами исследователей искусственного интеллекта. Определяя данные и модели, по которым они будут предоставлены широкой публике, органам власти, главы статистических агентств, менеджеры федеральных программ и прочие значимые государственные служащие совместно с Senior Agency Officials for Privacy (уполномоченным по вопросам невмешательства в частную жизнь) должны определить барьеры и требования, которые соответственно будут возникать и которым надо следовать при расширении доступа к ФД и улучшении способов использования ФД: а) вопросы защиты частной жизни; б) вопросы безопасности данных, связанные с объединением данных и моделей, в) документирование данных и их форматирования, в т.ч. необходимость использования интероперабельных и машиночитаемых форматов; г) изменения, необходимые для управления ФД и системой, и пр.;

– Data Incubator Project[132] предлагает современную, практически ориентированную учебную программу, использующую новейшие средства обучения,

– Cross-Agency Priority (CAP)[133] – инструмент, используемый руководством США для ускорения прогресса в приоритетных областях деятельности, реализация которых требует активного сотрудничества нескольких государственных органов. Долгосрочные по своему характеру цели направлены на межведомственное сотрудничество при решении общегосударственных управленческих задач,

– Current Federal Information Processing Standards[134] - единый перечень федеральных стандартов обработки информации.

Для межведомственного обмена информацией применяется Национальная модель обмена информацией (National Information Exchange Model, NIEM)[135]. NIEM – партнерство агентств и организаций на всех уровнях власти (федеральном, уровня штатов и местного уровня), целью которого является результативный обмен информацией в ключевых точках принятия решений в областях судопроизводства, общественной безопасности, реагирования на чрезвычайные ситуации, разведки и национальной безопасности. NIEM устанавливает согласованную терминологическую базу, правила взаимодействия и форматы данных для информационного обмена, не зависящие от того, каким образом информация хранится в отдельных информационных системах. На текущий момент NIEM поддерживает данные в форматах XSD и Microsoft Excel, а также инструментарий унифицированного языка моделирования (Unified Modeling

---

[132] URL: https://strategy.data.gov/incubator/ (дата обращения 08.08.2019).

[133] URL: https://www.performance.gov/CAP/leveragingdata/ (дата обращения 08.08.2019).

[134] URL: https://www.nist.gov/itl/current-fips (дата обращения 08.08.2019).

[135] URL: https://www.niem.gov/about-niem (дата обращения 08.08.2019)

Language, UML) для графического отображения обмена данными и элементов для каждого сообщения [136].

Законодательство штата Калифорния в области управления данными[137] включает:

– Закон о конфиденциальности потребителей 2018 г. (AB-375 Privacy: Personal Information: Businesses (California Consumer Privacy Act of 2018). Закон закрепляет обязанность компаний, собирающих или продающих персональные данные жителей Калифорнии, сообщать физическим лицам о категориях и перечнях персональных данных, которые компания собрала или продала, об источниках персональных данных, целях обработки данных и перечне лиц, имеющих доступ к такой информации,

– Образовательный кодекс (Education Code (EDC) (Статья 1. Regional Data-Processing Centers (Региональные центры обработки данных) [10500 - 10507]). Советы школьных округов вправе создавать и поддерживать центры обработки образовательных данных. Такие центры, отвечающие положениям законодательства штата, имеют право на финансовую помощь штата,

– Кодекс по вопросам охраны здоровья и безопасности (Health and Safety Code (HSC) (Article 1. General Provisions [40400 - 40408], Chapter 8.5. Health Care Cost Transparency Database [127671 - 127674] Статья 1. Общие положения, глава 8.5 «Доступ к базам данных о стоимости медицинских услуг»). Регулируется создание единой информационной базы. Данные о здравоохранении собираются с помощью многих разрозненных систем. Сбор этих данных обеспечит прозрачность расходов на здравоохранение, и эта информация будет использоваться в решениях о качестве здравоохранения, о расходах на него и о сокращении неравенства,

---

[136] URL: https://www.niem.gov/about-niem/niem-model (дата обращения 08.08.2019)
[137] URL: http://leginfo.legislature.ca.gov (дата обращения 08.08.2019).

– Организационный кодекс (Government Code (GOV) (ARTICLE 1. General Provisions [68500 - 68530]. Статья 1. Общие положения). Статья регламентирует процедуру запроса и обмена информацией между органами власти штата,

– Уголовный кодекс (Penal Code (PEN) (CHAPTER 11. Street Terrorism Enforcement and Prevention Act. Глава 11. Закон о борьбе и предотвращении уличного терроризма [186.20 - 186.36]) касаются работы централизованного реестра данных об огнестрельном оружии, доступа к информации и условий доступа к данным в реестре,

– Водный кодекс (Water Code (WAT) (CHAPTER 1. General Provisions. Глава 1. Общие положения. [12400 - 12402]), Закон об открытых и прозрачных данных о воде (The Open and Transparent Water Data Act) − регламентирует передачу информации государственными органами, доступа к информации в системах.

В) Государственные органы в сфере управления данными

Органы, отвечающие за регулирование сферы данных, включают следующие государственные учреждения в составе администрации Президента и независимые агентства правительства США: Административно-бюджетное управление (Office of Management and Budget), Федеральную торговую комиссию (Federal Trade Commission, охраняет конкуренцию и честную торговую практику), Службу валютного контроля (Office of Controller of Currency), Департамент здравоохранения и социальных служб (Department of Health and Human Services), Федеральную комиссию связи (Federal Communications Commission), Комиссию по ценным бумагам и биржам (Securities and Exchange Commission, осуществляет регулирование в сфере финансов), Бюро по финансовой защите потребителей

(Consumer Financial Protection Bureau), Департамент торговли (Department of Commerce) и др.[138].

Государственные учреждения в составе администрации Президента– в их числе Административно-бюджетное управление, Департамент здравоохранения и социальных служб и Департамент торговли отвечают наряду с другими управлениями и службами за наиважнейшие государственные направления, и главы таких органов входят в состав Кабинета.

1.3.7 Правовые акты Великобритании

А) Государственный строй и общая характеристика права Великобритании

Великобритания – унитарное государство с монархической формой правления. Так называемая «Вестминстерская модель управления» воспринята целым рядом стран. Государственное управление осуществляется правительством от имени короны.

Статус Премьер-министра также во многом определяется неписаными нормами. Королева назначает Премьер-министром лидера партии, победившей на выборах. Премьер-министр реализует такие полномочия королевы как назначение и увольнение министров, роспуск парламента, назначение на высшие государственные должности. Он самостоятельно определяет количество министров. Премьер-министр не имеет значительного аппарата. В своей деятельности он опирается на личный секретариат и секретариат кабинета.

Правительство – термин, объединяющий всех министров, но в таком виде данный орган никогда не собирается. Кабинет – более узкий орган,

[138] URL: https://www.usa.gov/branches-of-government

объединяющий ведущих министров. Они проводят заседания, принимают решения.

Министры могут возглавлять министерства либо быть министрами без портфеля. Большинство из них именуются государственными секретарями. Другие имеют особое название (к примеру, лорд-канцлер казначейства), третьи традиционно именуются министрами.

В министерствах есть должности государственного министра (по сути − заместителя министра). Взаимодействие министерств с Парламентом помогают осуществлять парламентские секретари министров.

Министерства имеют как центральный, так и региональный аппарат. Каждое министерство самостоятельно определяет собственную структуру.

Также в системе органов центральной администрации выделяются агентства, иные юридически самостоятельные органы центральной администрации и публичные корпорации.

Право Великобритании – термин, объединяющий английское право и право Шотландии, носящее смешанный характер. Английское право оказало значительное влияние на формирование правовой семьи общего права. В настоящее время английское право претерпевает изменения. В нем различается частное и публичное право. Судебные решения в большей степени основываются на законах (статутах), роль которых существенно возросла. Тем не менее английское право сохранило особенности понятийного аппарата как в сфере публичного, так и частного права.

Кроме судебных прецедентов, источниками права является статутное право, в которое входят статуты (акты Парламента) и делегированные акты. Большая часть делегированного законодательства представлена в виде правительственного нормотворчества. Делегированные акты имеют различные названия: правил, приказов, инструкций, актов, регламентов, автономного законодательства (актов местных органов власти / by-laws) и актов корпораций.

Наряду с правовыми источниками в последнее время возросла роль таких норм, как кодексы поведения, кодексы практики, стратегии, технические стандарты, принципы. В некоторых случаях указанные источники являются юридически обязывающими.

Б) Общий обзор законодательства в сфере управления данными

Основу регулирования цифровой экономики в Великобритании составляет Акт о цифровой экономике (Digital Economy Act 2017)[139]. Указанный акт регулирует вопросы доступа к цифровым сервисам (универсальное обслуживание); построение цифровой инфраструктуры; введения интернет-фильтров провайдерами; некоторые вопросы интеллектуальной собственности; ряд вопросов в сфере цифрового правительства (digital government), например, раскрытие некоторых категорий информации (в частности, в исследовательских целях).

В развитие указанного статута приняты акты рекомендательного характера, например Кодексы практики[140].

Законодательство Великобритании не выделяет общий режим информации, а равно не выделяет общих субъектов информационных правовых отношений. Одновременно в Великобритании устанавливается правовое регулирование отдельных категорий данных, отдельных информационных правоотношений.

Принципы информации (Information Principles 2011)[141] являются политическим документом, опубликованным секретариатом Кабинета при

---

[139] Digital Economy Act 2017. URL: http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted (дата обращения: 05.08.2019).

[140] См. например: Information sharing code of practice: public service delivery, debt and fraud, 2018. URL: https://www.gov.uk/government/consultations/digital-economy-act-part-5-data-sharing-codes-and-regulations/information-sharing-code-of-practice-public-service-delivery-debt-and-fraud (дата обращения: 05.08.2019).

правительстве коалиции консерваторов и либерал-демократов (2010–2015 годы), содержащим ряд принципов, которым должны следовать все органы власти в информационной сфере. Согласно данному документу информация – ценный актив, что предполагает систематизацию (по формату) и каталогизацию информации в структурированной и неструктурированной форме, (по содержанию). Для обеспечения связанности информации из разных информационных систем, принадлежащей разным лицам, предполагается разработка и внедрение открытых стандартов.

Информация может использоваться повторно как внутри организации, так и при обмене данными в государственном секторе и с частными лицами. Допускается создание авторитетного источника информации по определенным сферам («master data»).

Публичная информация (public information), под которой понимаются данные органов публичной власти (в широком смысле слова, включая необработанные данные), должна быть опубликована, за исключением ряда случаев. Реализация настоящего принципа предполагает установление расписания публикаций информации, основные каналы публикации, определение подхода к информационным посредникам. Законодательно установлена общая обязанность любого публичного органа (duty of every public authority) публиковать информацию о деятельности в соответствии с утверждаемыми ими схемами публикации (publication schemes). Мониторинг опубликования таких схем осуществляет Управление уполномоченного по информации (Офис уполномоченного по информации - ICO)[142].

---

[141] Information Principles 2011. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266284/Information_Principles_UK_Public_Sector_final.pdf (дата обращения: 05.08.2019).

[142] См. например: The Central Government sector monitoring report, 2009. URL: https://ico.org.uk/media/action-weve-taken/monitoring/2795/central-government-sector-monitoring-report.pdf (дата обращения: 05.08.2019).

Основы правового режима данных, в том числе в государственных информационных системах, и правового статуса участников их оборота правовые акты. устанавливаютя в следующих актах.

Акт о свободе информации (Freedom of Information Act 2000)[143] устанавливает право любого лица на доступ к информации, принадлежащей органам публичной власти (held by public authority). Право на доступ к информации (right of access to information) включает право быть информированным о наличии у органа публичной власти соответствующей информации и право на получение указанной информации по запросу лица.

В ряде случаев с заявителя взимается пошлина (fees). Ответ по общему правилу направляется в течение 20 рабочих дней со дня следующего за днем получения запроса, при условии уплаты пошлины. В ряде случаев максимальный срок ответа устанавливается в 60 рабочих дней.

По Акту может ограничиваться доступ к следующим категориям информации:

– информация, доступная заявителю другими средствами,
– информация, которая будет опубликована в будущем,
– информация органов безопасности,
– информация для целей национальной безопасности,
– информация по вопросам международных отношений,
– информация об отношениях органов публичной администрации в Соединенном Королевстве,
– информация о расследованиях,
– судебные документы,
– персональные данные,
– информация, составляющая коммерческую тайну (trade secret).

---

[143]Freedom of Information Act 2000. URL: http://www.legislation.gov.uk/ukpga/2000/36/contents (дата обращения: 05.08.2019).

В силу Раздела 11 (1A) указанного акта, с учетом положений раздела 102 Акта о защите свобод (Protection of Freedoms Act 2012)[144], устанавливается право на повторное использование наборов данных (datasets), если вопрос не урегулирован Положением о повторном использовании информации публичного сектора 2015 г. (The Re-use of Public Sector Information Regulations 2015.[145] PSI применяется, если набор данных представляет собой объект авторского права (базу данных) и государственный орган является единственным ее правообладателем. В таком случае право повторного использования данных предоставляется по лицензионному договору. Соответствующие понятия определяются в контексте законодательства об интеллектуальной собственности[146].

Под набором данных понимается информация, включающая в себя набор информации, хранящаяся в электронной форме, где вся или большая часть такой информации: была получена с целью предоставления органу публичной власти в связи с оказанием услуг или выполнением иных функций органа публичной власти; является фактической информацией; не была существенным образом изменена с момента получения такой информации.

Соблюдение указанного статута и иных актов в информационной сфере контролирует, в частности, Офис уплномоченного по информации[147], статус которого исследуется далее.

---

[144]Protection of Freedoms Act 2012. URL: http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted (дата обращения: 05.08.2019).

[145] The Re-use of Public Sector Information Regulations 2015. URL: http://www.legislation.gov.uk/uksi/2015/1415/contents (дата обращения: 05.08.2019).

[146] См. например: Copyright, Designs and Patents Act 1988. URL: http://www.legislation.gov.uk/ukpga/1988/48/contents (дата обращения: 05.08.2019); Copyright and Rights in Databases Regulations 1997. URL: http://www.legislation.gov.uk/uksi/1997/3032/contents/made (дата обращения: 05.08.2019).

[147] Information Commissioner’s Office. Official website. URL: https://ico.org.uk (дата обращения: 05.08.2019).

При секретариате Кабинета (Cabinet office) создана правительственная Цифровая служба (GDS), основной функцией которой является поддержание цифровой трансформации государства, в частности, путем поддержания и совершенствования работы портала GOV.UK.

Акт о свободе информации в Шотландии (Freedom of Information (Scotland) Act 2002)[148], устанавливает положения, учитывая особенности правовой системы Шотландии.

Положение об информации о состоянии окружающей среды (Environmental Information Regulations 2004)[149] принятое государственным секретарем в развитие положений Директивы 2003/4/ЕС[150] и устанавливающее обязанность уполномоченных государственных органов сообщать информацию об окружающей среде обратившемуся лицу в срок до 20 дней с момента обращения. Существуют ограничения; например, не может быть предоставлена информация об окружающей среде, которая содержит персональные данные.

Акт о государственной тайне (Official Secrets Act 1989)[151] запрещает разглашения информации, содержащей государственную тайну. К такой информации отнесена информация в сферах безопасности, разведывательной деятельности, обороны, международных отношений. За нарушение положений указанного Акта установлена ответственность в виде лишения свободы и штрафа.

---

[148] Freedom of Information (Scotland) Act 2002. URL: http://www.legislation.gov.uk/asp/2002/13/contents (дата обращения: 05.08.2019).

[149] The Environmental Information Regulations 2004. URL: http://www.legislation.gov.uk/uksi/2004/3391/contents (дата обращения: 05.08.2019).

[150] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003L0004 (дата обращения: 05.08.2019).

[151] Official Secrets Act 1989. URL: http://www.legislation.gov.uk/ukpga/1989/6/contents (дата обращения: 05.08.2019).

Положение о коммерческой тайне (Trade Secrets Regulations 2018)[152], делегированный акт, принятый в развитие положений Директивы 2016/943[153], защищает интересы обладателя информации, составляющей коммерческую тайну (trade secret holder). Акт определяет коммерческую тайну как информацию, которая не может быть легко получена третьим лицом, имеет коммерческую ценность, а обладатель такой информации предпринял надлежащие действия по сохранению таковой в тайне. Акт определяет сроки, ограничивающие установление режима коммерческой тайны, а также вопросы ответственности, в частности, возмещения убытков (damages).

Акт о защите данных (Data Protection Act 2018)[154] принят в развитие GDPR[155] и содержит аналогичное регулирование. Акт регулирует вопросы защиты персональных данных, в частности, принципы обработки, права субъектов персональных данных, обязанности оператора (controller).

Положение об авторских правах и правах на базы данных (Copyright and Rights in Databases Regulations 1997)[156] определяет понятие базы, под которой понимается собрание независимых произведений, данных и других самостоятельных материалов, которые составляют определенную систему, а

---

[152] The Trade Secrets (Enforcement, etc.) Regulations 2018. URL: http://www.legislation.gov.uk/uksi/2018/597/contents/made (дата обращения: 05.08.2019).

[153] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943 (дата обращения: 05.08.2019).

[154] Data Protection Act 2018. URL: http://www.legislation.gov.uk/ukpga/2018/12/contents (дата обращения: 05.08.2019).

[155] 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). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1565101770580&uri=CELEX:32016R0679 (дата обращения: 05.08.2019).

[156] The Copyright and Rights in Databases Regulations 1997. URL: http://www.legislation.gov.uk/uksi/1997/3032/contents/made (дата обращения: 05.08.2019).

также доступны с помощью электронных и других средств. Акт защищает права создателя базы данных на содержание таковой.

Основы правового регулирования информационного взаимодействия между различными государственными информационными системами регулируются следующим актами.

Стратегия развития информационно-коммуникационных технологий (Government ICT Strategy 2011)[157], является политическим документом, опубликованным секретариатом Кабинета и предполагающим создание общей информационно-телекоммуникационной инфраструктуры. Ранее государственные органы использовали различающиеся информационно-коммуникационные технологии (системы), что не было экономически эффективно и препятствовало информационному взаимодействию. Реализация стратегии помогает исключить дублирование данных и обеспечить возможность повторного использования таковых путем определенных стандартов. Переход к централизованной модели управления основывался на использовании облачных технологий.

Основные мероприятия по настоящему плану были завершены в 2016 году. Главным итогом осуществления такового является создание единой платформы электронного правительства GOV.UK.

Стратегия трансформации правительства[158] и Цифровая стратегия развития Великобритании[159], политические документы, принятые секретариатом Кабинета и рядом департаментов в 2017 году, поддерживают

---

[157] Government ICT Strategy 2011. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-government-government-ict-strategy_0.pdf (дата обращения: 05.08.2019).

[158] Government Transformation Strategy 2017 to 2020. URL: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020 (дата обращения: 05.08.2019).

[159] UK Digital Strategy 2017. URL: https://www.gov.uk/government/publications/uk-digital-strategy (дата обращения: 05.08.2019).

деятельность Цифровой службы по созданию единой платформы электронного правительства GOV.UK[160].

Косвенно к защите данных можно отнести Положение о безопасности сетей и информационных систем (Network and Information Systems Regulations 2018)[161] принято для имплементации положений Директивы ЕС 2016/1148 (NIS)[162]. Оно регулирует вопросы защиты цифровых информационных систем (критической инфраструктуры), определяет требования к операторам жизненно-важных услуг (operator of essential services).

Подходы к правовому регулированию унификации форматов представления информации и технологий информационного обмена в государственных информационных системах регулируют рассмотренные ниже документы.

Принципы открытых стандартов (Open Standards Principles 2018)[163], опубликованные секретариатом Кабинета в качестве политического документа, содержат следующие критерии выбора стандартов, которые должны:

- соответствовать потребностям пользователя,
- обеспечивать равный доступ поставщиков к гос. контрактам,
- быть гибкими и способными к изменениям,
- быть обоснованными,
- быть транспарентными.

---

[160] GOV.UK website. URL: https://www.gov.uk (дата обращения: 05.08.2019).

[161] The Network and Information Systems Regulations 2018. URL: http://www.legislation.gov.uk/uksi/2018/506/contents (дата обращения: 05.08.2019).

[162] 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. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 05.08.2019).

[163] Open Standards Principles. URL: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (дата обращения: 05.08.2019).

Выбор унифицированных форматов (стандартов) информации государственными органами должен основываться на указанных принципах.

Исправление неточных персональных данных (right to rectification) в государственной информационной системе регулируются на основании Акта о защите данных (Data Protection Act 2018)[164] и GDPR.

Если говорить о судебной практике в области персональных данных, то она в основном связана с негосударственными системами. Также существует практика ЕСПЧ в отношении защиты персональных данных, когда требования были обращены к государственным органам[165]. Можно привести в качестве примера дело «Secretary of State for the Home Department & Anor v TLU & Anor [2018] EWCA Civ 2217 (15 June 2018)»[166]. Указанное дело было связано с публикацией МВД электронной таблицы с персональными данными беженцев. Апелляция поддержала выводы суда первой инстанции о нарушениях законодательства в действиях Министерства.

Положение о повторном использовании информации, находящейся в распоряжении публичных органов власти (Re-use of Public Sector Information Regulations 2015)[167] регулирует право частных субъектов на повторное использование информации в коммерческих и некоммерческих целях.

---

[164] Data Protection Act 2018. URL: http://www.legislation.gov.uk/ukpga/2018/12/contents (дата обращения: 05.08.2019).

[165] См. например: Big Brother Watch and others v. The United Kingdom (2018). URL: https://hudoc.echr.coe.int/eng#{"itemid":["001-186048"]} (дата обращения: 05.08.2019); Catt v. the United Kingdom (2019). URL: https://hudoc.echr.coe.int/eng#{"itemid":["001-189424"]} (дата обращения: 05.08.2019).

[166] Secretary of State for the Home Department & Anor v TLU & Anor [2018] EWCA Civ 2217 (15 June 2018). URL: http://www.bailii.org/ew/cases/EWCA/Civ/2018/2217.html (дата обращения: 05.08.2019).

[167] The Re-use of Public Sector Information Regulations 2015. URL: http://www.legislation.gov.uk/uksi/2015/1415/contents/made (дата обращения: 05.08.2019).

Однако из указанного общего правила допустимости повторного использования существуют исключения. Так, не может быть передана для повторного использования:

– информация, содержащая персональные данные,

– конфиденциальная информация,

– информация о государственной тайне,

– информация, представляющая охраняемый объект права интеллектуальной собственности третьих лиц,

– документы, доступные иными способами, за исключением подачи запроса в соответствии с Актом о свободе информации.

Акт уточняет требования к запросу на повторное использование, а также определяет обязанность публичных органов публиковать перечни данных для повторного использования и условия доступа к таковым. Срок ответа на запрос составляет 20 рабочих дней.

Если публичный орган требует соблюдения иных условий, то такие условия не должны ограничивать способ повторного использования, а также препятствовать конкуренции хозяйствующих субъектов, носить дискриминационный характер.

В части стандартных лицензий (упоминаемых в настоящем акте и в Директиве 2019/102 можно выделить лицензию OGL[168], которая разработана Национальным архивом и используется органами власти и применяется к служебным произведениям, права на которые принадлежат органам власти (Crown copyright).

Раздел 14 указанного Акта устанавливает в качестве общего правила недопустимость заключения эксклюзивных соглашений о повторном

---

[168]Open Government License for public sector information. URL: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ (дата обращения: 05.08.2019).

использовании. От правила можно отступать в общественных интересах, при условии пересмотра таких соглашений каждые 11 лет. Любое эксклюзивное соглашение подлежит публикации.

За разрешение повторного использования может взиматься «разумная плата». Размер платы и условия использования публикуются.

Дополнительно отметим, что существуют акты рекомендательного характера, разъясняющие положения указанного Регламента[169].

В) Государственные органы в сфере управления данными

Функция созданной при секретариате Кабинета Правительственной Цифровой службы является поддержание цифровой трансформации Правительства, в частности, путем поддержания и совершенствования работы портала GOV.UK.

В соответствии с разделом 128 Акта о защите данных (Data Protection Act 2018), ICO проводит аудит (проверки) соблюдения законодательства о персональных данных. Процедура аудита определена соответствующим Руководством (A guide to ICO audits 2018)[170]. ICO выносит уведомления в отношении государственных органов[171].

Аудит проводит отдел обеспечения ICO. Проверяются политики и процедуры безопасности персональных данных, их соответствие

---

[169] Guidance on the implementation of the Re-use of Public Sector Information Regulations 2015 for re-users. URL: http://www.nationalarchives.gov.uk/documents/information-management/psi-implementation-guidance-re-users.pdf (дата обращения: 05.08.2019).

[170] A guide to ICO audits 2018. https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf (дата обращения: 05.08.2019).

[171] См. например: HMRC enforcement notice (10 May 2019) URL: https://ico.org.uk/action-weve-taken/enforcement/hmrc/ (дата обращения: 05.08.2019); IICSA monetary penalty notice (18 July 2018). https://ico.org.uk/action-weve-taken/enforcement/independent-inquiry-into-child-sexual-abuse/ (дата обращения: 05.08.2019); Secretary of State for Justice enforcement notice (21 December 2017). https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-justice/ (дата обращения: 05.08.2019).

законодательству и соответствие обработки таким политикам и процедурам. По результатам проверок готовится отчет ICO[172].

ICO также проводит мониторинг требований законодательства об информации в отношении органов, наиболее часто нарушающих права граждан, однако предметом мониторинга не являются непосредственно данные.

Совет стандартизации (Open Standards Board) создан Комитетом государственных расходов (Public Expenditure Committee (Efficiency Reform) (PEX(ER)) с целью содействия секретариату Кабинета в сфере стандартизации. В него входит, в частности, представитель Цифровой службы (GDS). Совет утверждает форматы информации для целей информационного обмена в публичном секторе.

Офис уполномоченного по информации (ICO) защищает информационные права граждан, контролирует соблюдениее законодательства в области персональных данных.

1.3.8 Правовые акты Австралии

А) Государственный строй и общая характеристика права Австралии

Австралия – федеративное государство с формой правления в виде парламентской монархии, установленной Конституцией 1901 года. Конституция распределяет полномочия между федерацией (официально именуемой Содружеством) и шестью штатами. Помимо шести штатов (Новый Южный Уэльс, Квинсленд, Южная Австралия, Тасмания, Виктория и

[172] См. например: Lancashire Police data protection audit report 2019. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2615173/lancashire-police-exec-summary-201905.pdf (дата обращения: 05.08.2019); Legal Ombudsman data protection audit report 2019. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2615063/legal-ombudsman-executive-summary.pdf (дата обращения: 05.08.2019); NHS England data protection audit report 2019. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2614990/nhs-england-audit-es-201901.pdf (дата обращения: 05.08.2019).

Западная Австралия) существуют три территории: Австралийская столичная территория, Северная территория и остров Норфолк.

Содружество осуществляет деятельность через ряд различных организационных структур, включая департаменты (departments of state), должностных лиц (office holders), органы власти (statutory authorities), в том числе государственные корпорации (statutory corporations), компании (companies) и трасты (trusts). Особенностью государственного управления Австралии является система так называемых «портфолио» (portfolio, portfolio departments), учреждаемых Кабинетом (федеральным правительством) на основании Указа об административных процедурах (Administrative Arrangements Order, AAO)[173]. В AAO уточняются вопросы, которыми занимается каждый государственный департамент, и законодательство, регулируемое каждым министром.

К исполнительной власти относятся департаменты, агентства. Каждый правительственный департамент имеет веб-сайт, на котором министры и парламентские секретари часто имеют собственные веб-сайты.

По предложению Премьер-министра Генерал-губернатор Австралии назначает министров, создает «портфельные» департаменты и официально распределяет исполнительную ответственность через AAO. Сформированы три группы органов высшего уровня[174]: некорпоративные образования (non-corporate Commonwealth entities); корпоративные образования (corporate Commonwealth entities); компании (Commonwealth companies).

Все образования и компании Содружества созданы в соответствии с полномочиями, вытекающими из Конституции, посредством принятия

---

[173] Governance structures in the public sector. https://www.finance.gov.au/resource-management/governance/overview/ (дата обращения 28.10.2019).

[174] Также существует секторальная классификация, которая применяется для представления финансовой информации о результатах деятельности образований и компаний Содружества по институциональным секторам.

законов и осуществления исполнительной власти[175]. Поскольку все образования и компании Содружества входят в состав исполнительной власти, все эти структуры государственного сектора подотчетны Парламенту. В число образований Содружества входят:

– государственные департаменты ( departments of state);

– парламентские департаменты ( parliamentary departments);

– образования, указанные в Положении PGPA (PGPA Act Rule) или в другом законодательстве;

– юридические лица (body corporate), созданные в соответствии с законодательством и предусмотренные в каком-либо законе или правилах в качестве образования Содружества.

Примерами некорпоративных образований Содружества являются государственные департаменты, парламентские департаменты или включенные в перечень образования (listed entity)[176].

Конституция устанавливает, что основные аспекты деятельности правительства осуществляются государственными департаментами. Государственный департамент обладает гибкостью для проведения различных политических и функциональных мер. Например, функции в департаментах могут иметь отдельное обозначение, придающее им

---

[175] Механизмы финансового и корпоративного управления образований Содружества определяются Законом о государственном управлении, деятельности и подотчетности 2013 г. (Public Governance, Performance and Accountability Act 2013; PGPA Act). https://www.finance.gov.au/resource-management/pgpa-act/ (дата обращения: 11.10.2019).

[176] Включенное в перечень образование - орган, лицо, группа лиц или организация (или любое сочетание этих лиц или организаций), которое предусмотрено правилами, установленными в соответствии с PGPA, но является юридическим лицом. Включенное в перечень образование могло бы стать частью другого некорпоративного образования Содружества, если бы оно не было включено в перечень. Например, Офис финансового управления (Australian Office of Financial Management) вошел бы в состав Министерства финансов (Department of the Treasury), если бы он не был включен в перечень юридических лиц для целей Закона о государственном управлении, деятельности и подотчетности 2013 г.

индивидуальность, и законодательство может использоваться для создания должностей или подразделений с точно очерченными функциями и обязанностями, которым оказывает административную поддержку тот или иной департамент.

Корпоративное образование Содружества - юридическое лицо, имеющее самостоятельную (отдельную) от Содружества правосубъектность и способное самостоятельно осуществлять юридические права, например, заключать договоры и владеть имуществом. Виды корпоративных образований лиц Содружества включают: Корпорацию пенсионного обеспечения (Commonwealth Superannuation Corporation), Авиационную службу (Airservices Australia) и Резервный банк (Reserve Bank of Australia).

Компании Содружества - это компании, учрежденные Содружеством в соответствии с Законом о корпорациях 2001 г. (Corporations Act 2001), который является основным нормативным актом, регулирующим деятельность этих компаний. Виды компаний Содружества включают: NBN Co Limited[177] и Australian Rail Track Corporation Limited[178].

Правовая система общего права унаследована от Англии во время колонизации. Австралия входит в Содружество, глава государства – английская королева. Длительное время британский Парламент принимал законы для Австралии, а Судебный комитет Тайного совета был ее высшей судебной инстанцией. Однако во второй половине XX в. австралийский Парламент принял ряд законов, ограничивающих распространение актов

[177] Австралийская государственная корпорация, которой поручено проектировать, строить и эксплуатировать Австралийскую национальную широкополосную сеть как монопольный оптовый поставщик широкополосного доступа. Она подотчетна двум министрам - министру финансов и министру связи. URL: https://www.nbnco.com.au/ (дата обращения: 28.10.2019).

[178] Австралийская железнодорожная корпорация является государственной корпорацией, основанной правительством Австралии в июле 1998 г., которая управляет большей частью межгосударственной железнодорожной сети Австралии. URL: https://www.artc.com.au/ (дата обращения: 28.10.2019).

британского парламента, право апелляции в Судебный комитет Тайного совета. В результате право Австралии начало приобретать самостоятельный характер, оставаясь в семье общего права. Источники права характерны для данной семьи – судебные прецеденты, статуты (акты парламента), делегированные акты.

Б) Общий обзор законодательства в сфере управления данными

В Австралии конфиденциальность и защита данных регулируется федеральными законами и законами штатов. Далее приводятся источники, относящиеся к Содружеству в целом и столичной территории (Commonwealth Government and Australian Capital Territory Government agencies). Применение или условия применения того или иногда документа к отдельным областям Содружества определяются самим документом.

Закон о свободе информации 1982 г.[179] (Freedom of Information Act 1982) устанавливает право физических лиц запрашивать доступ к документам у министров и большинства государственных органов. Такие запросы частных лиц могут касаться документов, содержащих их личную информацию, а также документов, содержащих другую информацию, такую как информация о государственной политике, программах и процессах принятия решений.

Закон позволяет запрашивать доступ к документам, находящимся в распоряжении министров, правительства Австралии и большинства агентств; позволяет требовать внесения изменений или аннотаций в любую информацию о лице. Закон устанавливает схему публикации информации, требующую публиковать в Интернете подробную информацию о функциях и структуре агентств, а также позволяет агентствам и министрам издавать документы, которые будут исключены из сферы действия Закона о свободе

[179] Freedom of Information Act 1982. URL: https://www.legislation.gov.au/Details/C2019C00198 (дата обращения: 05.08.2019).

информации, если это не запрещено требованиями секретности в другом законе.

Правила платы в области свободы информации (Freedom of Information (Charges) Regulations 2019)[180] определяют, как агентства или министры взимают плату за доступ к документам в соответствии с Законом о свободе информации.

Правила свободы информации (уполномоченные органы, основные должностные лица и годовая отчетность) (Freedom of Information (Prescribed Authorities, Principal Officers and Annual Report) Regulations 2017[181] определяют сроки сообщения информации Австралийскому комиссару информации для ежегодного доклада OAIC, указывает главных должностных лиц в уполномоченных органах для целей реализации Закона о свободе информации.

В соответствии с 93A Руководящих положений о свободе информации 1982 года (Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982)[182] Комиссар издает Руководящие принципы. Указанный раздел требует, чтобы министры и государственные органы учитывали эти принципы при выполнении функций в соответствии с Законом о свободе информации. Указанные принципы охватывают общие вопросы применения Закона и не являются законодательными инструментами.

---

[180] Freedom of Information (Charges) Regulations 2019. URL: https://www.legislation.gov.au/Details/F2019L00348 (дата обращения: 05.08.2019).

[181] Freedom of Information (Prescribed Authorities, Principal Officers and Annual Report) Regulations 2017. URL: https://www.legislation.gov.au/Details/F2017L01676 (дата обращения: 05.08.2019).

[182] Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982. URL: https://www.oaic.gov.au/assets/freedom-of-information/guidance-and-advice/foi-guidelines/foi-guidelines-combined-january-2019.pdf (дата обращения: 05.08.2019).

Принципы открытой информации государственного сектора (Principles on open public sector information)[183], разработанные OAIC, не имеют обязательной силы и действуют в соответствии с правовыми требованиями об управлении информацией, изложенными в Законе о свободе информации, Законе о неприкосновенности частной жизни 1988 года, Законе об архивах 1983 года и других законах и общем законодательстве. В то же время принципы будут применяться OAIC в рамках его задач по контролю за соблюдением государственными органами Закона о свободе информации.

Заявление правительства о публичной информации (Australian Government Public Data Policy Statement)[184] провозглашает данные, которыми располагает правительство, «стратегическим национальным ресурсом». Правительство обязуется оптимизировать использование и повторное использование общедоступных данных; раскрывать «не-чувствительные данные» (non-sensitive data) как открытые по умолчанию; сотрудничать с частным и исследовательским секторами. Заявление определяет публичные данные как все данные, собранные государственными органами для любых целей; не-чувствительные данные как обезличенные данные (anonymized) при условии, что они не идентифицируют физическое лицо и не нарушают требований к защите неприкосновенности частной жизни или безопасности.

«Документ для обсуждения: современное законодательство Австралии по обмену данными и их выпуску» (New Australian Government Data Sharing

[183]Principles on open public sector information. URL: https://www.oaic.gov.au/information-policy/information-policy-resources/principles-on-open-public-sector-information (дата обращения: 05.08.2019).

[184]Australian Government Public Data Policy Statement. URL: https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf (дата обращения: 05.08.2019).

and Release Legislation: Issues paper for consultation)[185], опубликованный 4.07. 2018 департаментом Премьер-министра и Кабинета (Department of the Prime Minister and Cabinet), определяет подход к новому законопроекту об обмене данными и выпуске информации, который будет направлен на обеспечение баланса между обменом данными, имеющимися в распоряжении правительства, и соответствующим управлением связанными с этим рисками. Документ излагает концепции и принципы, которыми можно руководствоваться при разработке новых механизмов обмена и выпуска данных. В то время как документ включает положения, включающие конфиденциальные данные, чтобы показать, как могут работать новые механизмы, данные о частных лицах и предприятиях являются лишь одной частью системы данных. Концепции и принципы, изложенные в документе, охватывают все данные, хранящиеся в распоряжении правительства Австралии, и предлагаемые документом механизмы обмена и выпуска данных обеспечат согласованную и масштабную основу, применимую к данным всех характеристик и чувствительности.

В сентябре 2019 года после общественных обсуждений Кабинет одобрил «Документ для обсуждения: Реформа законодательства регулирующего Обмен данными и их Выпуск» (Data Sharing and Release Legislative Reforms Discussion paper)[186], который развивает и уточняет отдельные аспекты оборота данных государственного сектора, обозначенные в предыдущем документе по данной теме («Документ для обсуждения: современное законодательство Австралии по обмену данными и их

[185]New Australian Government Data Sharing and Release Legislation: Issues paper for consultation. URL: https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation (дата обращения: 05.08.2019).

[186] Data Sharing and Release Legislative Reforms Discussion paper. https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf (дата обращения: 05.08.2019).

выпуску»), а также определяет дальнейшие шаги в формировании законодательной базы данной реформы.

Управление Комиссара по вопросам данных выпустило «Руководство по лучшей практике применения принципов обмена данными» (The Best Practice Guide to Applying Data Sharing Principles)[187].В принципах излагаются принципы обмена данными и излагается общая оперативная модель государственной службы в целях содействия согласованной и совместно используемой практике управления данными. Пять принципов обмена данными представляют собой:

– Проект − цель обмена данными;

– Данные − уровень детализации данных;

– Настройки − среда, в которой будут использоваться данные;

– Лица − кто имеет доступ к данным;

– Промежуточные результаты − какие результаты могут быть обнародованы.

Руководящие принципы состоят из трех частей:

– часть 1 содержит информацию и вопросы, которые хранители данных (data custodians) должны рассмотреть перед началом обмена данными, такие как зрелость организации в плане обмена данными и ее подход к управлению рисками,

– часть 2 разъясняет каждый из принципов в практическом порядке, начиная с оценки проекта. Эта часть предусматривает примеры того, как каждый принцип действует и ставит вопросы, чтобы помочь хранителям данных применять их,

---

[187] The Best Practice Guide to Applying Data Sharing Principles. URL: (дата обращения: 29.10.2019). https: //www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf. (дата обращения: 6.08.2019)

– часть 3 включает дальнейшие указания, как управлять соглашениями об обмене данными после их заключения.

Закон о неприкосновенности частной жизни[188] (Privacy Act 1988) принят для защиты частной жизни физических лиц и для регулирования обработки личной информации государственными органами и другими организациями с годовым оборотом более 3 млн. долл. США. Закон включает 13 принципов (Australian Privacy Principles, APP), которые применяются к некоторым организациям частного сектора, а также к большинству государственных органов. Кроме того, он регулирует конфиденциальность системы отчетности по потребительским кредитам, номерам налоговых документов, а также медицинские исследования.

В соответствии с Законом уполномоченное лицо вправе проводить расследования соблюдения Закона и добиваться применения гражданско-правовой ответственности за серьезные или повторные нарушения принципов (APP), если организация не приняла мер к исправлению положения.

Руководство по регулированию неприкосновенности частной жизни (Guide to Privacy Regulatory Action)[189], разработанное OAIC, опубликовано в мае 2018 года и регулярно обновляется. Руководство содержит подробное объяснение полномочий регулирования конфиденциальности, рассматривает правовую базу и цель полномочий, а также процедуры, применяемые Комиссаром для осуществления регулирующих полномочий.

Закон о переписи и статистике 1905 г.[190] (Census and Statistics Act 1905)

---

[188] Privacy Act 1988. URL: https://www.legislation.gov.au/Details/C2019C00198 (дата обращения: 05.08.2019).

[189] Guide to privacy regulatory action. URL: https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/ (дата обращения: 05.08.2019).

[190] Census and Statistics Act 1905. URL: https://www.legislation.gov.au/Details/C2016C01005 (дата обращения: 05.08.2019).

дает уполномоченному органу право проводить сбор статистических данных, включая перепись населения и жилищного фонда, а также право запрашивать статистическую информацию.

Закон обязывает Бюро статистики публиковать и распространять статистическую информацию и ее анализ, а также обеспечивать конфиденциальность информации, собранной в соответствии с Законом. Раздел 13 Закона предусматривает, что министр принимает решения, предусматривающие раскрытие, с письменного одобрения уполномоченного органа Бюро, категорий информации при определенных условиях.

Закон 2010 г. «О медицинских идентификаторах»[191] (Healthcare Identifiers Act 2010), Положение о медицинских идентификаторах 2010 г. [192] (Healthcare Identifiers Regulations 2010) реализует национальную систему присвоения уникальных идентификаторов физическим лицам, поставщикам медицинских услуг и организациям, оказывающим медицинские услуги. Идентификаторы назначаются Службой медицинских идентификаторов (HI Service) и подчиняются ей. Служба медицинских идентификаторов - это национальная система уникальной идентификации медицинских работников и отдельных лиц. Оператором Службы является главный исполнительный директор программы Medicare, которую курирует Департамент социальных служб.

Цель идентификаторов физических лиц состоит в корректной передаче информации о физических лицах между поставщиками медицинских услуг, а также выявлении и получении доступа к записям пациентов в системе My Health Record.

---

[191] Healthcare Identifiers Act 2010. URL: https://www.legislation.gov.au/Series/C2010A00072 (дата обращения: 05.08.2019).

[192] Healthcare Identifiers Regulations 2010. URL: https://www.legislation.gov.au/Series/F2010L01829 (дата обращения: 05.08.2019).

Закон «О медицинских записях» (My Health Records Act 2012)[193], Положение о медицинских записях (My Health Records Regulation 2012)[194], Правило о медицинских записях (My Health Records Rule 2016)[195], Руководство по медицинским записям (полномочия Комиссара по информации) (My Health Records (Information Commissioner Enforcement Powers Guidelines 2016)[196] регулируют управление данными в сфере медицинского обслуживания.

Национальные правила здравоохранения (неприкосновенность частной жизни) 2018 г. (National Health (Privacy) Rules 2018)[197]. Правила регулируют способы фиксирования и хранения информации о претензиях, полученную в рамках Программ льгот медицинского обслуживания и фармацевтики.

Помимо прочего, раздел 135AA (5) Национального закона о здравоохранении требует, чтобы эти правила запрещали учреждениям хранить информацию о претензиях, полученную в рамках Программы льгот Medicare и Программы фармацевтики, в одной и той же базе данных.

Закон 2010 г. об Австралийском информационном комиссаре[198] (Australian Information Commissioner Act 2010) устанавливает должность Комиссара, определяет его права, обязанности, ответственность. Закон также учреждает Офис информационного комиссара (OAIC), цели которого - продвигать и поддерживать право на неприкосновенность частной жизни и

---

[193] My Health Records Act 2012. URL: https://www.legislation.gov.au/Series/C2012A00063 (дата обращения: 05.08.2019).

[194] My Health Records Regulation 2012. URL: https://www.legislation.gov.au/Details/F2019C00520 (дата обращения: 05.08.2019).

[195] My Health Records Rule 2016. URL: https://www.legislation.gov.au/Details/F2016L00095 (дата обращения: 05.08.2019).

[196] My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016. https://www.legislation.gov.au/Details/F2016L00360 (дата обращения: 05.08.2019).

[197] National Health (Privacy) Rules 2018. URL: https://www.legislation.gov.au/Details/F2018L01427 (дата обращения: 05.08.2019).

[198] Australian Information Commissioner Act 2010. URL: https://www.legislation.gov.au/Details/C2010A00052 (дата обращения: 05.08.2019).

право на доступ к информации, а также контролировать реализацию государственной информационной политики. OAIC выполняет три основные функции:

– функции по обеспечению конфиденциальности, возложенные Законом о неприкосновенности частной жизни и другими законами;

– функции обеспечения свободы информации, в частности, надзор за осуществлением Закона о свободе информации 1982 года и пересмотр решений, принятых учреждениями и министрами в соответствии с этим законом;

– функции государственной информационной политики, возложенные на информационного комиссара в соответствии с Законом 2010 г.

Закон 1990 г. «О программе сопоставления данных (помощь и налоги)» [199] (Data-matching Program (Assistance and Tax) Act 1990) вместе с Руководством к программе сопоставления данных (Guidelines for the Conduct of the Data-Matching Program) регулируют порядок работы Налогового управления (Australian Taxation Office, ATO) и агентств социальной помощи, включая Услуги Австралии (Services Australia, предыдущее название – Департамент социальных служб; Department of Human Services, DHS) и Департамент ветеранов (Department of Veterans' Affairs, DVA) по использованию номеров налоговых файлов для сравнения личной информации в целях обнаружения неправильных платежей.

ATO является некорпоративным образованием Содружества, (non-corporate Commonwealth entities), входящим в портфолио Казначейства (Treasury), и оказывает услуги пяти министрам (Казначейству, Министру населения, городов и городской инфраструктуры, Министру жилищного строительства и помощника казначея, Помощнику министра по вопросам

[199] Data-matching Program (Assistance and Tax) Act 1990. URL: https://www.legislation.gov.au/Series/C2004A04095 (дата обращения: 05.08.2019).

пенсионного обеспечения, финансовых услуг и финансовых технологий, Помощнику министра финансов, благотворительности и по вопросам выборов)[200]. ATO возглавляется Комиссаром по налогообложению и Регистратором регистра предприятий, и поддерживается Исполнительным комитетом и другими корпоративными комитетами.

Департамент социальных служб создан в рамках финансового и административного портфолио. Руководит департаментом Секретарь, подчиненный Министру по делам государственной службы. Департамент несет ответственность за разработку политики услуг и обеспечение доступа к социальным, медицинским и другим платежам и услугам в рамках государственных программ, реализуемых Департаментом. Департамент ветеранов входит в портфолио «Оборона» (Defence) и является основным агентством по оказанию услуг, отвечающим за разработку и реализацию программ помощи ветеранам и военнослужащим. Закон и Руководство требуют, чтобы обязательное сопоставление данных проводилось в соответствии с письменными протоколами и техническими стандартами.

Агентства также проводят сопоставление данных для ряда целей (помимо выявления неправильных платежей, сделанных клиентам DHS, DVA или ATO). Это может включать сопоставление их собственных данных с данными, полученными из других правительственных учреждений Австралии, или из неправительственных государственных органов или предприятий частного сектора. Для такого вида сопоставления данных OAIC выпустило Руководство (Guidelines on Data Matching in Australian Government Administration)[201]. Ряд государственных структур[202] применяет его на

---

[200] https://www.ato.gov.au/About-ATO/Who-we-are/Executive-and-governance (дата обращения: 31.10.2019).

[201] URL: https://www.oaic.gov.au/privacy/guidance-and-advice/guidelines-on-data-matching-in-australian-government-administration/ (дата обращения: 05.08.2019). Выполнение руководящих принципов сопоставления имеет добровольный характер.

добровольной основе. Орган вправе просить освободить его от соблюдения некоторых руководящих принципов, если орган находит, что это отвечает общественным интересам.

В Руководстве по аналитике данных и австралийским принципам конфиденциальности (Guide to Data Analytics and Australian Privacy Principles)[203], разработанном OAIC и опубликованном 21.03.2018, указаны действия по анализу данных, которые включают большие данные, интеллектуальный анализ данных и интеграцию данных. Руководство предназначено как для государственных органов, так и для организаций частного сектора, на которые распространяется действие Закона о неприкосновенности частной жизни. Целью Руководства является помощь в выявлении и принятии решений проблем конфиденциальности. Руководство не является юридически обязывающим, однако OAIC ссылается на него при выполнении своих функций в соответствии с Актом о неприкосновенности частной жизни.

Руководство Де-идентификации и Закон о неприкосновенности частной жизни (De-identification and the Privacy Act)[204], разработанное OAIC и опубликованное 21.03.2018, содержит общие рекомендации по де-идентификации, помогающие субъектам APP защищать неприкосновенность частной жизни при использовании или обмене информацией, содержащей личную информацию. Определяется, когда де-идентификация может быть

---

[202] Указанный документ использует термин «agency» в смысле, приданном ему в разделе 6 Закона о неприкосновенности частной жизни, и включающем в себя, помимо прочего, министра или департамент Правительства (Minister or Government Department).

[203] Guide to Data Analytics and the Australian Privacy Principles. URL: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/ (дата обращения: 05.08.2019).

[204] De-identification and the Privacy Act. URL: https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/ (дата обращения: 05.08.2019).

уместной, как выбрать ее подходящие методы и как оценить риск повторной идентификации.

Система принятия решений по де-идентификации (De-identification Decision-Making Framework)[205] совместно разработана OAIC и Организацией Содружества по научным и промышленным исследованиям (Commonwealth Scientific and Industrial Research Organisation, CSIRO[206]), опубликована 18.09.2017. Это – практическое руководство для организаций, обрабатывающих личную информацию и рассматривающих возможность обмена ею или ее публикации в соответствии с их этическими обязанностями и правовыми обязательствами, например, согласно Закону о неприкосновенности частной жизни. Руководство является адаптацией британской Системы принятия решений об анонимности (Anonymisation Decision-Making Framework).

Национальная правительственная стратегия обмена информацией (NGISS)[207] создает основы развития информационного взаимодействия государственных информационных систем и определяет следующие принципы обмена информацией:

– обеспечивать лидерство (Provide leadership) – поддерживать и продвигать принципы обмена информацией; обмен информацией должен быть включен в качестве цели в организационные стратегические планы,

---

[205] De-identification Decision-Making Framework. https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/ (дата обращения: 05.08.2019).

[206] CSIRO является национальным научным агентством, проводящим исследования и предлагающим инновационные решения для промышленности, общества и окружающей среды. Является портфельным агентством Департамента промышленности, инноваций и науки (Industry, Innovation and Science). https://www.industry.gov.au/about-us/our-structure/our-portfolio-agencies (дата обращения: 31.10.2019).

[207] National Government Information Sharing Strategy. URL: https://www.finance.gov.au/sites/default/files/ngiss.pdf (дата обращения: 5.08.2019)

– демонстрировать ценность (Demonstrate value) – цель обмена информацией должна быть ясной,

– действовать сообща (Act collaboratively) – органам необходимо определить наборы ключевой информации, в отношении которых у них есть первичная информация, ответственность и контроль. Это поможет идентифицировать информационные ресурсы, которыми можно делиться, и определить, как лучше это делать,

– устанавливать четкое управление (Establish clear governance) - управление совместно используемой информацией так же важно, как и сама информация. Механизмы управления обменом информацией должны быть четко определены и последовательно применяться всеми государственными органами. Документация по вопросам управления должна включать информацию о подотчетности, полномочиях и надзоре; о контрольных показателях и конечных результатах; параметрах политики; о соответствующих стандартах и процессах; о координации и интеграция информации; об определении условий использования информации, об оценке критериев эффективности и иное,

– разрабатывать руководящие принципы управления (Establish custodianship guidelines) – выявлять и последовательно применять модели оптимальной практики управления в политике правительства является требованием Стратегии,

– необходимо определить функции и обязанности по управлению, включающие обязанности обеспечения точности, полноты охвата, безопасности и конфиденциальности; по управлению получением информации; по решению вопросов интеграции; по соблюдению стандартов; по разработке метаданных; по управлению техническим обслуживанием, доступом, использованием и распространением информации,

– обеспечивать интероперабельность (Build for interoperability) - способность государственных органов к уверенному управлению и обмену информацией имеет решающее значение для создания интегрированного

правительства. Поддержка учреждений в последовательной передаче и использовании информации должна быть реализована за счет использования рамочных программ операционной совместимости,

– использовать стандартизированную информацию (Use standards-based information). Чтобы обмен информацией был возможным, рентабельным и эффективным, создание, хранение и использование информации должно соответствовать стандартам. Поэтому на этапе создания инициативы по обмену информацией должны быть направлены на изучение стандартов подлежащей обмену информации,

– способствовать повторному использованию информации (Promote information re-use). Государственные структуры должны изучить условия использования различных элементов их информационного каталога, и не должны обмениваться информацией ради самого процесса; должно быть ясно определенное требование для повторного использования информации,

– обеспечивать конфиденциальность и безопасность (Ensure privacy and security). Конфиденциальность является основным основанием повторного использования информации. Правила конфиденциальности и безопасности должны соблюдаться, но не препятствовать ограниченному совместному доступу (shared access) к информации, когда это допустимо. Действующие положения[208] о неприкосновенности данных, относящихся к частной жизни, и конфиденциальности таких сведений по общему правилу запрещают обмен информацией, составляющей данную категорию. Некоторые государственные структуры уже имеют механизмы обмена не конфиденциальными данными, многие другие не вовлечены в межведомственный информационный обмен. Обмен данными между

[208]В данном случае речь о Законе о неприкосновенности частной жизни (Privacy Act 1988) и установленных им тринадцати принципах (Australian Privacy Principles), ссылки на которые приводились ранее в данном разделе.

ведомствами осуществляется в отдельных проектах, реализуемых в рамках Партнерства интеграции данных (DIPA)[209].

«Программный протокол. Сопоставление данных программ Centrelink and Medicare» (Program Protocol. Matching of Centrelink and Medicare Data)[210] является примером одного из протоколов сопоставления данных из различных баз данных, разработанный Министерством социальных услуг. Также существуют другие протоколы[211].

Примеры реализуемых проектов в области управления и использования публичных данных (public data):

1) Партнерство по интеграции данных (Data Integration Partnership for Australia, DIPA)[212].

Сотрудничество правительства Австралии с более чем 20 агентствами Содружества, которое улучшает техническую инфраструктуру данных и расширяет возможности интеграции данных в государственной службе. DIPA дает доступ только к контролируемым, де-идентифицированным и конфиденциальным данным для анализа политики и исследовательских целей. DIPA регулируется процедурами и законодательством агентств, в том числе Законом о неприкосновенности частной жизни.

DIPA состоит из нескольких компонентов, рассмотренных ниже.

Инфраструктура данных и их интеграция обеспечивается Бюро статистики и Институтом здравоохранения и социального обеспечения. Эти органы формируют основную техническую инфраструктуру DIPA, поставляя

---

[209] The Data Integration Partnership for Australia. URL: https://www.pmc.gov.au/public-data/data-integration-partnership-australia (дата обращения: 25.07.2019).

[210] Program Protocol. Matching of Centrelink and Medicare Data. URL: https://www.humanservices.gov.au/sites/default/files/2019-matching-of-centrelink-and-medicare-data-protocol.pdf (дата обращения: 05.08.2019).

[211] URL: https://www.humanservices.gov.au/organisations/about-us/publications-and-resources/centrelink-data-matching-activities (дата обращения: 05.08.2019).

[212] The Data Integration Partnership for Australia. https://www.pmc.gov.au/public-data/data-integration-partnership-australia (дата обращения: 05.08.2019).

инструменты для интеграции и фиксирования данных, включая производство долговременных и интегрированных активов данных. Доступ к архивам данных обеспечивают Департамент социальных служб (DSS); Министерство здравоохранения (Health); Министерство образования и обучения (DoET); Министерство финансов и Управление национальной разведки.

Технический обзор и рекомендации, предоставленные Data61. Data61 выполняет консультативную роль, помогая партнерским учреждениям принимать обоснованные решения с учетом последних разработок и эффективности данных, обеспечиваемых новыми технологиями.

2) Проект мульти-агентской интеграции данных (MADIP) (Multi-Agency Data Integration Project (MADIP)[213].

MADIP − партнерство шести государственных структур, которое объединяет национальные наборы данных, чтобы повысить их ценность для анализа политики, исследований и статистических целей. Партнеры - Бюро статистики, Налоговое управление и Департаменты образования и обучения, здравоохранения, человеческих служб (Department of Human Services) и социальных служб (Department of Social Services). MADIP фиксирует информацию из ряда наборов данных, касающихся здравоохранения, образования, государственных платежей, подоходного налога и демографии.

Каждый партнер MADIP собирает личную информацию, связанную с его функциями или деятельностью. Эта информация будет раскрыта в Бюро статистики MADIP. Используется только информация, необходимая для утвержденной цели (то есть не целостные наборы данных).

3) Программа Индекс местоположения (Loc-I)(Location Index (Loc-I))[214]

---

[213] Multi-Agency Data Integration Project (MADIP). https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP (дата обращения: 05.08.2019).

[214] Location Index (Loc-I). http://locationindex.org/ (дата обращения: 05.08.2019).

Индекс местоположения (Loc-I) - структура, которая обеспечивает согласованный способ беспрепятственной интеграции данных о людях, бизнесе и окружающей среде. Индекс нацелен на расширение характеристик базовых пространственных данных для сбора геопространственных данных (несколько географических регионов), которые необходимы для общественной безопасности и благополучия или имеют решающее значение при принятии решений на национальном или правительственном уровне. Индекс местоположения является частью программы DIPA, которая использует коллективные ресурсы Geoscience Australia, Организации Содружества по научным и промышленным исследованиям, Бюро статистики[215], Департамент сельского хозяйства[216] и Департамента окружающей среды и энергетики[217].

Всеми партнерами подписан Меморандум о понимании (Memorandum of Understanding, MOU), определяющий их вклады в Индекс местоположения для ресурсов и интеллектуальной собственности. Меморандум также определяет направления деятельности партнеров: владение бизнесом, управление проектами, техническое развитие и советники.

В) Государственные органы в сфере управления данными

---

[215] ABS является статистическим агентством. Поставляет статистические данные по широкому кругу экономических, социальных, демографических и экологических вопросов, охватывая правительство, бизнес и местное сообщество. Также выполняет координирующую функцию статистической деятельности других официальных органов как в Австралии, так и за рубежом. Входит в портфолио Казначейства (Treasury). https://www.directory.gov.au/portfolios/treasury/australian-bureau-statistics (дата обращения: 31.10.2019).

[216] Департамент сельского хозяйства (Department of Agriculture) http://www.agriculture.gov.au/about/who-we-are/portfolio-agencies (дата обращения: 31.10.2019).

[217] Департамент окружающей среды и энергетики (Department of Environment and Energy). https://www.directory.gov.au/portfolios/environment-and-energy (дата обращения: 31.10.2019).

Государственную политику в области государственных (публичных) данных реализует Кабинет и Департамент Премьер-министра. В настоящее время Кабинет осуществляет рекомендации Комиссии продуктивности (Productivity Commission)[218], в том числе проведение законодательной реформы. В состав Кабинета и Департамента Премьер-министра входит Управление Комиссара по данным (Office of National Data Commissioner). Задачами Управления являются:

– содействие расширенному использованию данных государственного сектора;

– стимулирование инноваций и экономических выгод от более широкого использования данных государственного сектора;

– укрепление доверия общества к использованию правительством данных.

Управление Комиссара по данным сотрудничает с Управлением Комиссара по информации в целях обеспечения конфиденциальности и безопасности данных. Предполагается, что Управление Комиссара по данным будет действовать в качестве независимого государственного органа (independent statutory body).

В рамках проводимой в настоящее время реформы управления государственными данными (данными публичного сектора), среди прочего предусмотрено руководство изменениями и поддержка в управлении и использовании данных, основанных на передовой практике, в рамках всей государственной службы, в том числе посредством осуществления нового законодательства, будет поручена Комиссару по данным[219]. Он отвечает за

---

[218] Australian Government's response to Productivity Commission Data Availability and Use Inquiry, 1 May 2018. https://dataavailability. pmc.gov.au/ (дата обращения: 31.10.2019).

[219] https://www.datacommissioner.gov.au/about/commissioner (дата обращения: 29.11.2019).

внедрение наиболее простого и безопасного способа обмена данными и их распространения в государственном секторе в целях получения большей общественной пользы.

Предполагается также, что значительную роль в проведении реформы будет играть Национальный консультативный совет по данным (National Data Advisory Council), консультирующий Комиссара по этике использования данных, участия общественности и оптимальным техническим практикам, а также развитию промышленности и международного сотрудничества.

1.3.9 Нормативные правовые акты Сингапура

А) Государственный строй и общая характеристика права Сингапура

Сингапур – унитарное государство с республиканской формой правления. Сингапур получил независимость в 1965 г.

Глава государства – Президент, избираемый на 6 лет. Он осуществляет часть полномочий самостоятельно, часть – по совету Кабинета (правительства). Президент назначает Премьер-министра и по его предложению членов Кабинета. По сути Кабинет формируется из членов партии, победившей на выборах. Кабинет несет коллективную ответственность перед парламентом.

Ключевой политической фигурой выступает Премьер-министр. Для Сингапура характерна централизованная система управления. Большую роль играет Офис Премьер-министра, контролирующий деятельность министерств. Каждый министр имеет парламентского секретаря и секретаря по административным вопросам. Министры могут возглавлять несколько министерств. Так, министр связи и информации одно время выполнял функции второго министра обороны.

Кроме министерств, на основе актов парламента создаются статутные органы (агентства). Они имеют большую самостоятельность в отличие от министерств. Статутные органы отчитываются перед соответствующим должностным лицом. Примером таких органов является Monetary Authority of Singapore (MAS), по сути выполняющий функции центрального банка

Сингапура. Он имеет свой аппарат управления, но возглавляется заместителем Премьер-министра. Другой пример статутного органа - Колледж гражданской службы (учебное заведение гражданских служащих), действующий под контролем отдела гражданской службы Офиса Премьер-министра.

Под руководством Офиса Премьер-министра действует Офис «умной нации и цифрового правительства» (SNDGO), реализующий государственные планы развития данного направления. Агентство по управлению технологиями, Министерство образования Ngee Ann Polytechnic, Skills Future Сингапура развивают платформы, основанные на блокчейне, - OpenCerts. Агентство кибербезопасности (CSA), функционирующее в рамках Офиса Премьер-министра, разрабатывает стратегию кибербезопасности. Агентство управления технологиями – также статутный орган (Gov Tech), созданный в 2016 г. В Офисе Премьер-министра действует группа, занимающаяся долгосрочным (стратегическим) планированием.

Правовая система Сингапура относится к смешанным правовым системам, для которых характерно сочетание нескольких правовых культур. Значительно влияние английского права, в силу чего договорное право, право собственности, деликатное право основываются на прецедентном праве. Судьи также обращаются к практике других стран общего права, прежде всего Канады и Австралии. Кроме того, суды практикуют обращения к практике и других стран. Несмотря на то, что законы являются источником права, большую роль играет административное регулирование.

Б) ) Общий обзор законодательства в сфере управления данными

Закон об управлении в публичном секторе 2018 (Public Sector (Governance) Act 2018)[220] предусматривает единый подход к услугам в государственном секторе. Он определяет направления обмена данными между государственными органами, регламентирует полномочия государственных органов при обмене данными, устанавливает ответственность за несанкционированное раскрытие и ненадлежащее использование информации.

Понятие «публичный орган» раскрывается в Законе об управлении в публичном секторе и означает юридическое лицо, учрежденное публичным законом для выполнения публичных функций, но исключая городской совет, созданный в соответствии с разделом 4 Закона о городских советах (гл. 329A). Публичные органы и их должностные лица имеют право делиться информацией, находящейся под их контролем, с другими государственными органами в той мере, в которой это разрешено направлением обмена данными, несмотря на любые обязательства в отношении конфиденциальности данных. Пункт 46 Закона вносит изменения в положения о секретности в нескольких актах. Поправка предусматривает раскрытие информации, если это разрешено законом.

Положения о защите данных не распространяются на публичный сектор. При обработке данных публичные органы подчиняются внутренним правительственным правилам и отраслевому законодательству.

Обмен данными частично регулируется Законом о конкуренции 2004 г. (Competition Act 2004)[221] и Кодексом конкуренции в области

---

[220] Public Sector (Governance) Act 2018. Personal Data Commission. https://sso.agc.gov.sg/Acts-Supp/5-2018/Published/20180305?DocDate=20180305 (дата обращения: 11. 08. 2019)

[221] Competition Act. https://sso.agc.gov.sg/Act/CA2004 (дата обращения: 11. 08. 2019)

телекоммуникаций (Telecoms Competition Code)[222]. Закон содействует функционированию рынка и повышению конкурентоспособности экономики, защиты бизнеса и потребителей от антиконкурентного поведения.

Закон о развитии медиа-сферы (Info-communications Media Development Authority Act 2016) регулирует сферу деятельности служб вещания и смежные с ней области: электронных записей, электронных подписей и пр.[223].

Закон о борьбе со спамом 2007 г. (Spam Control Act 2007, SCA)[224] регламентирует контроль над спамом и связанные с его распространением вопросы.

В соответствии с разделом 8A Закона о неправомерном использовании компьютеров и кибербезопасности 2017 г.[225] (Computer Misuse And Cybersecurity (Amendment) Act 2017, CMCA) получение и передача личной информации, полученной с нарушением законодательства, является преступлением. Примером подобного нарушения выступает несанкционированный доступ к данным в электронной форме и/или их модификация.

Закон о кибербезопасности 2018 г. (Cybersecurity Act 2018 (Act. 9 of 2018)[226] направлен на повышение уровня цифровой безопасности и устойчивости цифровых технологий во всех секторах промышленности,

---

[222]Telecoms Competition Code. https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/frameworks-and-policies/competition-management/telecom-competition-code/02-2012tccwef2july2014.pdf?la=en (дата обращения: 11. 08. 2019)

[223] Act is the Info-communications Media Development Authority Act 2016. https://sso.agc.gov.sg/Act/IMDAA2016 (дата обращения:15. 08. 2019)

[224] Spam Control Act. https://sso.agc.gov.sg/Act/SCA2007 (дата обращения: 2.09. 2019)

[225] Computer Misuse And Cybersecurity (Amendment) Act 2017. https://sso.agc.gov.sg/Acts-Supp/22-2017/Published/20170511?DocDate=20170511 (дата обращения: 2. 09. 2019)

[226] Cybersecurity Act 2018 (Act. 9 of 2018). https://sso.agc.gov.sg/Acts-Supp/9-2018/ (дата обращения: 30. 08. 2019)

которые оказывают основные услуги. В контексте оборота данных Закон определяет ответственность за несанкционированный доступ к данным.

Закон о защите персональных данных 2012 г. (Personal Data Protection Act 2012 (PDPA) [227] имеет экстерриториальный характер. Он не охватывает государственный сектор: такое изъятие закреплено не только в самом PDPA, но и в отдельном уведомлении о защите персональных данных[228]. Федеральный орган исполнительной власти, отвечающий за соблюдение закона, и соответственно, за безопасность оборота персональных данных, – Комиссия по защите персональных данных[229].

Поскольку PDPA не распространяется на государственный сектор для решения возникающего вопроса о регулировании оборота данных в определенной сфере следует обращаться к другим правовым актам. Следующие акты являются наиболее всеобъемлющими в регулировании конфиденциальности данных.

Несмотря на то, что публичные органы были освобождены от действия PDPA, они по-прежнему несут ответственность за защиту публичных данных и подчиняются другому законодательству и нормативным актам, касающимся безопасности данных. В частности, органы государственного сектора должны соблюдать правительственные инструкции и Закон об управлении государственным сектором. Принятый в прошлом году закон ввел стандартизированные ключевые корпоративные политики и обмен данными между государственными органами.

---

[227] The Personal Data Protection Act 2012 (PDPA). Personal Data Commission. https://www.pdpc.gov.sg/Legislation-and-Guidelines/Enforcement-of-the-Act (дата обращения: 4. 08. 2019)

[228]Personal Data Protection (Statutory Bodies) Notification 2013. https://sso.agc.gov.sg/SL/PDPA2012-S149-2013?DocDate=20180329 (дата обращения: 4.08. 2019)

[229] Section 5(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) URL: https://sso.agc.gov.sg/Act/IMDAA2016 (дата обращения: 12. 08. 2019)

Закон о банковской деятельности 1970 г. (Banking Act 1970)[230] устанавливает правила ее лицензирования и регулирования. Раздел 47 (1) Закона предусматривает, что «информация о клиентах никаким образом не может раскрываться банком или должностным лицом третьему лицу, за исключением случаев, прямо предусмотренных в настоящем Законе». Третье приложение к Закону устанавливает обстоятельства, при которых информация о клиенте может быть раскрыта. Кроме того, коммерческие банки подпадают под действие положений о банковской тайне, изложенных в Банковских правилах (Banking Regulations (гл. 19, п. 5). Правило 10 гласит, что раздел 47 и Третье приложение к Закону, измененные вторым и третьим приложениями к Правилам, применяются к коммерческим банкам, и любое лицо, нарушающее эти положения о секретности, подвергнется уголовным санкциям. Банки, имеющие лицензию Сингапура, попадают под действие Закона о банковской деятельности и Закона о денежно-кредитном регулировании Сингапура. Соответственно, такие банки находятся под надзором и регулированием Валютного управления Сингапура. Валютное управление Сингапура вправе отозвать лицензию, если будет установлено, что указанный банк «нарушает положения Закона». Эти правила влияют на то, как финансовые учреждения в Сингапуре обрабатывают данные клиентов, и могут ограничивать быстроту обмена данными в финансовом секторе.

Закон о биомедицинских исследованиях человека 2015 г. (Human Biomedical Research Act 2015, HBRA)[231] регулирует порядок их проведения. В разделах с 6 по 12 изложены требования, касающиеся соответствующего согласия на биомедицинские исследования на человеке. В разделе 13 и

---

[230] Banking Act 1970. https://sso.agc.gov.sg/Act/BA1970 (дата обращения: 12.08. 2019)

[231] Human Biomedical Research Act 2015. https://sso.agc.gov.sg/Act/HBRA2015 (дата обращения: 12. 08. 2019)

Пятом приложении к HBRA изложены обстоятельства, при которых в согласии на биомедицинские исследования на человеке может быть отказано. Закон о частных больницах и медицинских клиниках 1980 г. (Private Hospitals and Medical Clinics Act, PHMCA)[232] (раздел 13 и гл. 248) устанавливает правила контроля, лицензирования и инспектирования частных больниц, поликлиник, клинических лабораторий и учреждений здравоохранения и защиты конфиденциальности информации в любом из них.

Релевантным для области регулирования данных является также Закон о денежно-кредитном управлении 1970 г. (Monetary Authority of Singapore Act)[233] в части его главы 186.

Дополнительными источниками в области регулирования управления данными являются:

– рекомендации по ключевым понятиям в Законе о защите персональных данных[234],

– рекомендации по Закону о защите персональных данных по отдельным вопросам[235],

– консультативное руководство по соблюдению положений о защите данных[236],

– стратегия кибербезопасности Сингапура[237],

---

[232] Private Hospitals and Medical Clinics Act https://sso.agc.gov.sg/Act/PHMCA1980 (дата обращения: 5. 08. 2019)

[233] Monetary Authority of Singapore Act https://sso.agc.gov.sg/Act/MASA1970#legis (дата обращения: 12. 08. 2019)

[234] Advisory Guidelines On Key Concepts In Personal Data Protection Act .https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts-in-the-PDPA-Revised-15-July-2019.pdf (дата обращения: 12. 08. 2019)

[235] Advisory Guidelines On The Personal Data Protection Act For Selected Topics. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/FINAL-Advisory-Guidelines-on-PDPA-for-Selected-Topics-2-Jan-2019.pdf (дата обращения:12. 08. 2019)

[236] Advisory Guidelines On Enforcement For Data Protection Provisions. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-enforcement-of-dp-provisions-(210416).pdf (дата обращения: 1. 08. 2019)

– разъяснения Комиссии защиты данных[238], посвященные вопросам оборота данных[239],

– антиконкурентные соглашения и согласованная практика обмена данными [240].

B) Государственные органы в сфере управления данными

Министерство связи и информации (Ministry of Communications and Information, далее – MCI) является частью объединенного регулятора информационно-коммуникационных и медиа-систем Управления развития медиа-коммуникаций.

Обязанности защиты данных в отдельных секторах применяются соответствующими отраслевыми регуляторами. Например, MAS обеспечивает соблюдение положений о банковской тайне в соответствии с Законом о банковской деятельности.

Ряд нарушений, связанных с оборотом данных в публичном секторе, привел к созданию Премьер-министром Комитета безопасности данных в

---

237 https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf. (дата обращения: 5. 08. 2019)

238 Комиссия по защите личных данных (PDPC) создана 2.01.2013 для администрирования и соблюдения Закона о защите личных данных 2012 года (PDPA). PDPC служит главным органом в вопросах, касающихся защиты личных данных, и представляет правительство Сингапура на международном уровне по вопросам защиты данных. При администрировании и применении PDPA PDPC стремится сбалансировать необходимость защиты личных данных отдельных лиц и потребности организаций в использовании данных в законных целях. PDPC разрабатывает и внедряет политику защиты персональных данных, включая соответствующие положения и консультативные указания, чтобы помочь организациям соблюдать PDPA.

239 PDPC Guide to Data Sharing.://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/OtherGuides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf (дата обращения: 5.08. 2019)

240 CCS Guidelines on the Section 34 Prohibition 2016. https://www.cccs.gov.sg/-/media/custom/ccs/files/legislation/legislation-at-a-glance/cccs-guidelines/cccs-guidelines-on-the-section-34-prohibitions-2016.pdf (дата обращения 2. 09. 2019)

государственном секторе (далее – Комитет) [241] для анализа обеспечения безопасности данных в государственном секторе. Цели Комитета заключаются в анализе процессов, связанных со сбором и защитой персональных данных граждан публичными органами, а также вендорами (англ. «vendor»), получающими прибыль от оборота данных. Средствами достижения цели обозначены обязанности Комитета обеспечить выполнение следующих задач:

– рассмотрение способа и эффективности защиты данных правительством Сингапура. В таком анализе будут учитываться роли всех субъектов оборота данных в государственном секторе, включая поставщиков и иных уполномоченных третьих лиц,

– рекомендация технических мер, процессов и возможностей для улучшения государственной защиты данных граждан и реагирования на инциденты,

– разработка плана действий на ближайшие шаги и долгосрочные меры для реализации рекомендаций.

1.3.10 Нормативные правовые акты Китая

А) Государственный строй и общая характеристика права Китая

КНР является государством с республиканской формой правления. Государственная структура определена Конституцией[242] 1982 г.

Высшим органом государственной власти КНР является Всекитайское собрание народных представителей (ВСНП).

Изменение Конституции, принятие уголовных и гражданских законов, законов о государственной структуре и других основных законов и их

---

[241] Appointment of Public Sector Data Security Review Committee. https://www.pmo.gov.sg/Newsroom/Appointment-of-Public-Sector-Data-Security-Review-Committee (дата обращения: 5.08.2019)

[242] Конституция Китайской Народной Республики 1982 г. https://legalns.com/download/books/cons/china.pdf (дата обращения: 31.10.2019)

изменение осуществляет ВСНП. Принятие законов и внесение в них изменений, за исключением отнесенных к компетенции ВСНП, осуществляется Постоянным комитетом ВСНП.

ВСНП избирает Председателя и заместителя Председателя КНР. Председатель КНР на основании решений ВСНП публикует законы, назначает и смещает Премьера и заместителей Премьера Государственного совета, членов Государственного совета, министров, председателей комитетов, главного ревизора и др.

Высшим административным органом является Государственный совет. Он состоит из Премьера, заместителей Премьера, членов Государственного совета, министров, председателей комитетов, главного ревизора, начальника секретариата. Министры и председатели комитетов Совета руководят работой соответствующих ведомств.

Все министерства и комитеты Государственного совета на основе законов и административно-правовых актов, постановлений и распоряжений Совета в пределах компетенции данного органа издают распоряжения, инструкции и положения.

Правовая система Китая имеет длительную историю развития. В целом идеи права долго отрицались обществом. Постепенные изменения стали происходить в XX в. Наметилась вестернизация права, кодификация законодательства. Однако особенность восприятия права обществом сохранялась, что сказывалось на трудности восприятия европейских моделей. В середине XX в. китайская модель стала воспринимать советскую модель права, но позже стала отходить от нее. С одной стороны, Конституция 1982 г. сохраняет приверженность социалистической модели, но с другой – развитие рыночных отношений способствовало постепенной модернизации, новой кодификации, повышению роли юристов.

Б) ) Общий обзор законодательства в сфере управления данными

Положение об открытой государственной информации[243] в первоначальной версии было принято Государственным советом 05.04.2007 и вступило в силу 1.05.2008. В настоящее время Положение действует в редакции 2019 г (вступило в силу 15.05.2019).

Положение декларирует цели получения гражданами, юридическими лицами и иными организациями государственной информации, повышения прозрачности деятельности государственных органов, содействия управлению в соответствии с законодательством.

Положение регулирует принципы раскрытия государственной информации, область ее раскрытия, методы и процедуры ее раскрытия, надзор и безопасность при раскрытии государственной информации.

В соответствии с Положением государственные органы на всех уровнях должны создать и поддерживать системы открытой государственной информации для соответствующих административных органов и назначить органы управления, отвечающие за ежедневную работу с открытой правительственной информацией.

Согласно Положению об открытой правительственной информации в целях стимулирования и регулирования раскрытия экологической информации подразделениями государственных органов, ответственных за охрану окружающей среды приняты Меры открытой экологической информации (пилотной реализации)[244]. Названные Меры является административно-правовым актом, принятым Государственной администрацией охраны окружающей среды и обязательным для исполнения

---

[243] Regulations of the People's Republic of China on Open Government Information. URL: https://www.chinalawtranslate.com/en/ogi2019/ (дата обращения: 02.08.2019)

[244] Measures on Open Environmental Information (for Trial Implementation). URL: https://www.cecc.gov/resources/legal-provisions/measures-on-open-environmental-information-trial-cecc-full-translation (дата обращения: 02.08.2019)

подразделениями охраны окружающей среды государственных органов на всех уровнях управления. Меры вступили в силу в 2008 г.

Меры предусматривают реализацию прав и интересов граждан, юридических лиц и других организаций в получении экологической информации и содействие участию общественности в охране окружающей среды. Меры определяют принципы раскрытия экологической информации, область раскрытия экологической информации, методы и процедуры раскрытия, раскрытия экологической информации предприятиями, надзор и ответственность.

Заключение Главного управления Государственного совета о реализации Положения об открытой государственной информации[245] от 29. 04.2008 регулирует: систему управления открытой государственной информацией, координации доступа к ней, охрану государственной тайны при раскрытии информации, упреждающее раскрытие государственной информации, раскрытие государственной информации по запросам граждан, раскрытию информации государственных органов и предприятий.

Указанное заключение является обязательным для исполнения органами исполнительной власти всех уровней, министерствами и комиссиями Государственного совета и их подчиненными подразделениями.

Заключение Главного управления Государственного совета по совершенствованию раскрытия государственной информации по запросам[246] издано 12.01.2010. Заключение рассматривает вопросы раскрытия

---

[245] Opinions of the General Office of the State Council on Various Issues of Implementing the Open Government Information Regulations of the People's Republic of China. URL: https://law.yale.edu/sites/default/files/documents/pdf/Intellectual_Life/CL-OGI-State_Council_Opinions-English.pdf (дата обращения: 02.08.2019)

[246] Opinions of the General Office of the State Council on Improving the Work of Disclosing Government Information Upon Request. https://law.yale.edu/sites/default/files/documents/pdf/Intellectual_Life/CL-OGI_SCGO_Opinions_on_OGI_Request_2010_%28Eng%29.pdf (дата обращения: 02.08.2019)

информации по запросам граждан: понимание классификации государственной информации, разъяснение принципа «один запрос на каждый предмет информации», обработка запросов в зависимости от типа обработки информации, укрепление упреждающего раскрытия государственной информации, повышение качества ее раскрытия по запросам граждан, совершенствование проверок на предмет соблюдения секретности, координации и консультаций.

Уведомление Секретариата Главного управления о выпуске Руководства по внедрению Открытой государственной информационной каталоговой системы (временное)[247] издано 15. 01. 2009.

Уведомление Главного управления Государственного совета о секретности в работе с открытой государственной информацией[248] издано 20.11.2010. Уведомление рассматривает аспекты реализации Положения об открытой государственной информации в части проверки секретности в работе с нею:

– повышение роли экспертизы государственной тайны при работе с открытой государственной информацией,

– дальнейшая стандартизация экспертизы государственной тайны при работе с открытой государственной информацией,

– усиление надзора и инспекций экспертизы государственной тайны при работе с открытой государственной информацией.

---

[247] Notice of the General Office Secretariat Bureau of the State Council on Issuing the Open Government Information Catalog System Implementing Guide (Interim). URL:https://law.yale.edu/system/files/china-law-documents/ch_2009_SCGO_on_OGI_Catalgoue_System.docx (дата обращения: 02.08.2019)

[248] Notice of the General Office of the State Council on Further Improving Secrecy Examination in Open Government Information Work. URL: https://law.yale.edu/sites/default/files/china-law-documents/2010_SCGO_Notice_on_Secerecy_Examination.docx (дата обращения: 02.08.2019)

Заключение Главного управления Государственного совета по дальнейшему развитию открытости государственной информации в ответ на социальные проблемы в целях повышения доверия к правительству[249] издано 1.10.2013. Заключение акцентирует внимание на ненадлежащем раскрытии информации и ненадлежащей проверке конфиденциальности на уровне местных и ведомственных органов, что может серьезно угрожать безопасности государственной тайны. Заключение устанавливает требования к усилению проверок при раскрытии государственной информации на предмет государственной тайны, к процедурам проверок наличия государственной тайны.

Уведомление Главного управления Государственного совета о приоритетах на 2014 в раскрытии правительственной информации[250] издано 17. 03. 2014. Уведомление устанавливает требования:

– усилить работу по раскрытию государственной информации с соблюдением требований к объему, своевременности и точности информации,

– повысить раскрытие информации об административных полномочиях и процедурах,

– повысить раскрытие информации о финансовых фондах,

– повысить раскрытие о распределении государственных ресурсов,

– повысить раскрытие информации в сфере государственного управления и смежных областях,

---

[249] Opinions of the General Office of the State Council on Further Strengthening Open Government Information Responding to Social Concerns in order to Raise Government Credibility. https://law.yale.edu/sites/default/files/china-law-documents/ch_2010_SCGO_Notice_on_Secrecy_Exam_in_OGI_Work.docx (дата обращения: 02.08.2019)

[250] Notice of the General Office of the State Council Issuing the 2014 Open Government Information Work Priorities. URL: http://www.gov.cn/zhengce/content/2014-04/01/content_8728.htm (дата обращения: 30.10.2019)

– повысить раскрытие нормативной информации;

– улучшить процедуры подготовки и раскрытия государственной информации,

– обеспечить ресурсы, необходимые для подготовки и раскрытия государственной информации,

– ежегодно подавать в Главную канцелярию Государственного совета отчетность о раскрытии государственной информации.

Уведомление Главного управления Государственного совета об усилении и стандартизации статистической отчетности по раскрытию государственной информации[251] издано 23.06.2014.

Уведомление устанавливает в отношении статистической отчетности по раскрытию государственной информации:

– содержание статистической отчетности,

– распределение ответственности за предоставление отчетности,

– требования к порядку предоставления статистической отчетности,

– форму статистического отчета,

– инструкцию по публикации и процедурам, связанным с раскрытием статистической отчетности.

Уведомление Министерства финансов и Комиссии национального развития и реформ о сборах за предоставление открытой правительственной информации и по другим сопутствующим вопросам[252] издано 11.06.2008.

---

[251] Notice of the General Office of the State Council on Strengthening and Standardizing Reporting Work for Statistics on the Open Government Information Situation. URL: http://www.gov.cn/zhengce/content/2014-07/04/content_8919.htm (дата обращения: 02.08.2019)

[252] Notice of the Ministry of Finance and the National Development and Reform Commission on Fees Collected for Providing Open Government Information and Other Relevant Issues. URL: https://law.yale.edu/sites/default/files/documents/pdf/Intellectual_Life/CL-OGI-Notice_MOF-English.pdf (дата обращения: 02.08.2019)

Оно определяет виды сборов, основания освобождения от уплаты сборов, требования к административной процедуре, связанной с получением платы за предоставление государственной информации.

Уведомление Комиссии национального развития и реформ и Министерства финансов о стандартах сборов, взимаемых административными органами за предоставление открытой государственной информации по запросу и по другим сопутствующим вопросам[253] издано 16. 07.2008. Уведомление обязательно для исполнения органами государственной власти и их подразделениями, собирающих плату за предоставление государственных данных. Предметом Уведомления являются требования к указанным сборам, взимаемых административными органами.

Гражданское и уголовное законодательство Китая содержат положения о защите персональных данных. В частности, с 2017 г. действуют Общие правила гражданского права (General Rules of the Civil Law), статья 111 которых предусматривает, что персональные данные физических лиц защищены законом, а незаконный сбор, использование, обработка или передача персональных данных других лиц не допускается.

Закон о кибербезопасности[254] принят Постоянным комитетом ВСНП 6.11.2016 и введен в действие 1.07.2017. Закон устанавливает общие положения в области кибербезопасности, поддержка и продвижение кибербезопасности, обеспечение функционирования информационно-коммуникационных сетей, обеспечение информации в информационно-

---

[253] Notice of the National Development and Reform Commission and the Ministry of Finance on the Standards for Fees Collected by Administrative Organs for Providing Open Government Information upon Request and Other Relevant Issues. URL: https://law.yale.edu/system/files/documents/pdf/Intellectual_Life/CL-OGI-NDRC_MOF_July08-English.pdf (дата обращения: 02.08.2019)

[254] The Cybersecurity Law of the People's Republic of China. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (дата обращения:02.08.2019)

коммуникационных сетях, мониторинг, раннее обнаружение и действия в ответ на чрезвычайные обстоятельства, законодательно установленная ответственность в области кибербезопасности.

Положения Закон о кибербезопасности в части защиты персональных данных конкретизируются национальным стандартом «Технологии информационной безопасности − Требования к безопасности персональных данных»[255], введенным в действие 1.05.2018. Однако в настоящее время уже разрабатывается новая редакция Стандарта, размещенная в Интернете[256].

Стандарт в действующей редакции определяет:

– терминологическую базу в области защиты персональных данных,

– базовые принципы их защиты,

– процесс сбора персональных данных,

– правила их хранения,

– правила их использования,

– правила их защиты от вводимых в действие информационных систем,

– правила разрешения инцидентов, связанных с персональными данными,

– правила управления защитой персональных данных.

Разъяснение Верховного народного суда «О рассмотрении административных дел, связанных с открытой государственной

---

[255] Information security technology—Personal Information Security Specifications. URL:https://www.chinalawtranslate.com/en/persona-information-security-standards/ (дата обращения:02.08.2019)

[256] Information security techniques - personal information security specifications (Draft for solicitation of comments). URL: https://www.chinalawtranslate.com/%e4%bf%a1%e6%81%af%e5%ae%89%e5%85%a8%e6%8a%80%e6%9c%af%e3%80%80%e4%b8%aa%e4%ba%ba%e4%bf%a1%e6%81%af%e5%ae%89%e5%85%a8%e8%a7%84%e8%8c%83-%ef%bc%88%e5%be%81%e6%b1%82%e6%84%8f%e8%a7%81%e7%a8%bf%ef%bc%89/?lang=en#_Toc28802 (дата обращения:02.08.2019)

информацией»[257] принято 13.12. 2010 и введено в действие 13.08.2011. Оно определяет состав действий государственных органов, которые составляют предмет административного правонарушения, состав действий государственных органов, которые при подаче жалоб гражданами или организациями не признаются правонарушениями, процессуальные действия судов при обращении граждан или организаций с жалобами на действия государственных органов в части раскрытия государственной информации.

Основы правового регулирования в области геоданных образует Закон «О картографии и геодезии»[258]. Закон принят Постоянным комитетом ВСНП 28.12.1992. В Закон внесены изменения 29.08. 2002 и 27.04.2017. В части управления геоданными раздел VI Закона «Результаты картографии и геодезии» устанавливает требования:

– к направлению в соответствующие государственные органы результатов картографии и геодезии для их последующего хранения и использования,

– к систематизации, обработке и ведению картографических и геодезических данных,

– к применению требований государственной тайны к указанным данным,

– к распространению и публикации указанных данных.

В части управления картами и геоданными Закон «О картографии и геодезии» конкретизируется Положением об управлении картами[259]. Оно

---

[257] The Supreme People's Court Provisions on Certain Questions Concerning the Trial of Open Government Information Administrative Cases. URL: https://law.yale.edu/system/files/area/center/china/document/2011-8_en_spc_ogi_cases_provisions.pdf (дата обращения:02.08.2019)

[258] Surveying and Mapping Law of the People's Republic of China. URL: http://extwprlegs1.fao.org/docs/pdf/chn173733.pdf (дата обращения: 31.10.2019)

[259] Regulation on Map Management. URL: http://en.pkulaw.cn/display.aspx?cgid=261284&lib=law (дата обращения: 31.10.2019)

является административно-правовым актом Государственного совета, обязательным для лиц, занимающихся составлением и публикацией карт, доступных общественности, а также органов власти, осуществляющих надзор над соблюдением правовых требований в области картографии и геодезии. Положение принято 26. 11. 2015 и вступило в силу 1. 01. 2016.

Положение конкретизирует Закон «О картографии и геодезии» в части требований и процедур разработки и публикации различных видов картографической продукции, в том числе к механизмам формирования и обмена геоинформацией между правительственными ведомствами и публикации геоинформации в Интернете.

В медицинской сфере в части управления данными применяются Положение по ведению медицинской документации в медицинских учреждениях, а также Меры по управлению информацией о здоровье населения. Положение[260] является административно-правовым актом Национальной комиссии здравоохранения и планирования семьи, обязательным для медицинских учреждений всех видов и уровней. Положение вступило в силу 1.01.2014 и устанавливает:

– общие положения по ведению медицинской документации,

– требования к идентификации и форме медицинской документации,

– требования к ведению медицинской документации,

– требования к доступу и распространению медицинской документации,

– требования к изготовлению копий медицинской документации,

– требования к хранению медицинской документации.

---

[260] Regulation on medical records management in medical institutions. URL: http://en.nhc.gov.cn/2014-06/25/c_46464.htm (дата обращения: 31.10.2019)

Меры управления информацией о здоровье населения[261] также являются актом Национальной комиссии здравоохранения и планирования семьи, принятыми для пробного внедрения. Меры вступили в силу 5.05.2014. Они устанавливают требования к процедурам сбора, администрирования, использования, обеспечения безопасности и конфиденциальности медицинской информации о здоровье населения учреждениями любого уровня, связанными с услугами в области здравоохранения и планирования семьи.

В Китае действует ряд нормативных правовых актов в области сектора телекоммуникаций и Интернета, которые затрагивают управление данными. К указанным актам в первую очередь относятся:

– Регламент телекоммуникаций КНР 2016 г. (PRC Telecommunications Regulations),

– Администрирование лицензий на телекоммуникационную деятельность 2009 г. (Measures for Administration of Telecommunications Business Operating Licences),

– Управление информационными службами Интернета 2009 г. (Measures for Administration of Internet Information Services),

– Правила управления сетевыми издательскими службами 2016 г. (Regulations for Administration of Network Publishing Services),

– Положение об управлении новостными и информационными службами Интернета 2017 г. (Regulations on Internet News and Information Service Management),

– Цензура безопасности Интернет-продуктов и услуг 2017 г. (Measures on Internet Product and Service Security Censorship).

---

[261] Measures for the Administration of Population Health Information (Trial Implementation). http://www.law.hku.hk/cprivacy/archives/175 (дата обращения: 31.10.2019)

Начиная со вступления КНР в ВТО (2001 г.) происходит постепенная либерализация регулирования режима государственной информации и секторов телекоммуникаций, медиа и Интернета. Однако при продвижении к большей государственной прозрачности все еще превалируют давние тенденции, связанные с сохранением государственной тайны.

В) Государственные органы в сфере управления данными

Формирование государственной политики и нормативно-правового регулирования в области оборота данных осуществляется Министерством промышленности и информационных технологий (Ministry of Industry and Information Technology, MIIT). К функциям MIIT в указанной области относятся:

– содействие развитию основного технологического оборудования и инноваций в информационно-коммуникационном секторе;

– руководство построением информационных систем;

– обеспечение информационной безопасности.

Вопросы регулирования сборов за предоставление открытой правительственной информации относятся к компетенции Министерства финансов и Комиссии национального развития и реформ.

Регулирование оборота данных на отраслевом уровне осуществляется в сфере здравоохранения Национальной комиссией здравоохранения и планирования семьи, в сфере пространственных данных − Национальной администрацией геодезии, картографии и геоинформации.

Стандартизации в области оборота данных осуществляется Национальным комитетом стандартизации.

Управление данными, обеспечение безопасности и использование соответствующей инфраструктуры посредством законов, принятых Постоянным комитетом ВСНП; актов Государственного совета; распоряжений, инструкций и положений министерств и комитетов Государственного совета; постановлений собраний народных представителей провинций и городов центрального подчинения и их постоянных комитетов.

Кроме вышеуказанного деятельность в данной области регулируется национальными стандартами КНР.

В области цифровой экономики в Китае не установлен общий режим регулирования. В то же время установлено правовое регулирование отдельных областей, к наиболее значимым из которых относятся:

– раскрытие государственной информации,
– распространение аудио и видеоинформации,
– телекоммуникационные и сетевые инфраструктура и услуги,
– обеспечение кибербезопасности и защиты данных.

1.3.11 Нормативные правовые акты Республики Кореи

А) Государственный строй и общая характеристика права Республики Корея

Республика Корея – унитарное государство с республиканской формой правления, во главе которого стоит президент. Он избирается прямыми выборами на пять лет. Президент назначает министров. Президент и Премьер-министр являются председателем и вице-председателем на заседаниях Кабинета (правительства). Министры подотчетны Премьер-министру.

К исполнительной власти относятся независимые агентства. Одни агентства подчинены Президенту, другие - Премьер-министру.

Правительство Кореи с 1990-х годов формирует новые институты. Создано Агентство по цифровым возможностям и обеспечению (KADO) для развития доступа к Интернету. Закон об развитии облачных технологий и защите пользователей 2015 г. способствовал внедрению облачных технологий в систему управления.

Комиссия связи уполномочена регулировать оказание услуг (в том числе радиоуслуг), деятельность новостных провайдеров, расследование деятельности операторов связи, защиту пользователей, а также принятие превентивных мер против оборота незаконной или вредной информации.

Право Кореи не относится к известным правовым семьям в силу того, что находится в стадии формирования. Длительное время право не являлось основным регулятором общественных отношений. В настоящее время наблюдается определенная вестернизация права, которая, однако сочетается с сохранением национальных традиций восприятия права.

Б) Общий обзор законодательства в сфере управления данными

Нормативная правовая база Республики Кореи в области управления данными многое заимствует из правовых систем США и государств-членов Европейского союза.

Закон о защите персональной информации 2011 г. (Personal Information Protection Act 2011) определяет персональные данные как информацию, относящуюся к живому физическому лицу, посредством которой данное физическое лицо может быть идентифицировано на основании этой информации либо при её незатрудненном комбинировании с другой информацией.

Закон о развитии информационно-телекоммуникационных сетей и защите информации 2011 г. (Act on promotion of information and communications Nerwork Utilization and Data Protection, etc.) закрепляет аналогичное определение персональных данных, однако применяется только к персональной информации пользователей, к которым относятся все физические лица, использующие телекоммуникационные сервисы, оказываемые провайдерами онлайн-сервисов (это могут быть как операторы связи, так и Интернет-сервисы).

Закон о защите и использования данных о местонахождении 2016 г. (Act on the Protection, Use, etc. of Location Information 2016) имеет целями: защиту данных личного характера от разглашения, злоупотребления и использования не по назначению информации о местонахождении, создание безопасных условий использования информации о местонахождении; таким образом вносится вклад в улучшение качества жизни и развитие общественного благосостояния.

Закон о защите военной тайны (Military Secrets Protection Act 1993 г.) допускает ее раскрытие, если это соответствуют общественному интересу, при отправке такого запроса гражданином Кореи в Министерство национальной обороны.

Закон о биоэтике и безопасности данных 2005 г. (Bioethics and Safety Act, 2005) регулирует ключевые аспекты передачи генетических данных, включая согласие на обработку, конфиденциальность, меры безопасности, совместимость и надзор.

Закон о защите персональных данных, используемых государственным органами (Act on the Protection of Personal Information Maintained by Public Agencies, 2012) регулирует сбор и обработку персональных данных правительством в соответствии с рекомендациями ОЭСР, касающимися защиты неприкосновенности частной жизни. Данный Закон распространяется на все государственные органы.

Закон о защите информации и телекоммуникационной инфраструктуры 2001 г. (Act on the Protection of Information and Communications and Infrascture 2001) устанавливает порядок охраны критической информационной инфраструктуры. В законе нет определения критической информационной инфраструктуры, так как установлен субъектный характер критической информационной инфраструктуры – руководители центральных административных органов вправе определять информационно-коммуникационную инфраструктуру под своей юрисдикцией в качестве критически важной.

Закон об электронном правительстве 2001 г. (Electronic Government Act 2001) устанавливает порядок взаимодействия государственных органов при использовании административной информации. Закреплен механизм Административного центра обмена информацией, который распространяет административную информацию, под которой подразумевается информация, подготовленная или полученная органами исполнительной власти в рамках их обязанностей.

Закон о содействии использованию информационно-коммуникационных сетей и защите информации 2016 г. (Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. 2016). По его статье 47, посвященной сертификации систем управления информационной безопасностью (ISMS), сертификационный аудит проводит Управление Интернета и безопасности (KISA) или аттестационный орган, назначаемый Министерством науки и ИКТ (MSIT).

Закон об открытых данных устанавливает обязанность всех государственных органов (national institutions), кроме обоснованных случаев, раскрывать данные и обеспечивать их использование. Данные должны быть в удобном пользователям формате. Закон предусматривает координацию взаимодействия всех структур в сфере открытых данных, механизмы совершенствования системы открытых данных и стандартов предоставления информации, а также повышение квалификации государственных служащих в области открытых данных.

Закон о формировании условий и использования публичных данных 2013 г. (Act on Promotion of the Provision and Use of Public Data 2013) поощряет публикацию электронным образом обработанных данных или информации, созданной государственными учреждениями с целью развития/стимулирования/пропаганды публичного доступа и интеллектуальной индустрии. Закон регулирует публикацию и свободное многократное использование данных в публичных и коммерческих целях в 15 стратегически важных сферах, включая уличное движение, погоду, космос, социальное благополучие, здравоохранение, питание, туризм и окружающую среду.

Цель Закона о раскрытии информации государственными органами 1996 г. (Act on Disclosure of Information by Public Agencies 1996) состоит в обеспечении прозрачности государственных дел, что реализуется посредством механизма, обязывающего государственные органы раскрывать информацию. Данный Закон устанавливает порядок запроса, а также случаи,

при которых органы государственной власти должны публиковать информацию.

Закон о развитии отрасли пространственных данных 2009 г. (Spatial Data Industry Promotion Act 2009) вводит определение пространственных данных как информации о местоположении любого естественного или искусственного объекта, существующего в любом наземном, подземном, водном, подводном или другом пространстве, и другую относящуюся к объекту информацию. Цель закона заключается в содействии развитию национальной экономики и повышению качества жизни путем укрепления конкурентоспособности отрасли пространственных данных.

В) Государственные органы в сфере управления данными

В Республике Корее управление данными осуществляют несколько структур. Комиссия связи Кореи состоит из пяти членов, два из которых, включая председателя, назначаются президентом самостоятельно. Остальные три назначаются президентом по предложению законодательного органа.

Агентство креативного контента Кореи является правительственным агентством, которое осуществляет контроль и координацию контент-индустрии.

В данной сфере действует Административный центр обмена информацией, а также Управление Интернета и безопасности (KISA) назначаемое Министерством науки и ИКТ (MSIT).

1.3.12 Итоговый перечень зарубежных государств с наиболее развитым правовым регулированием в области управления данными

В ходе исследования имеющихся в законодательстве зарубежных государств нормативных правовых и иных актов произведен экспертный анализ охвата нормативно правовым регулированием различных вопросов управления данными. Основным критерием отбора являлся максимально полный охват правовым регулированием различных вопросов управления данными и фактическое наличие соответствующих источников права для последующего анализа. Он позволил выделить следующие зарубежные

государства, в которых правовое регулирование управления данными является наиболее развитым и представляет интерес для дальнейшего детального исследования:

– Великобритания,
– Австралия,
– Сингапур,
– Франция,
– Германия,
– Эстония.

Также целесообразно рассмотреть право ЕС наряду с национальным правом государств-членов ЕС.

1.4 Исследование нормативных правовых актов Российской Федерации в области управления данными[262]

1.4.1 Общая характеристика правового регулирования управления данными в Российской Федерации

Концепция создания и функционирования национальной системы управления данными, утвержденная распоряжением Правительства Российской Федерации от 3 июня 2019 г. № 1189-р[263] (далее соответственно – Концепция, Распоряжение № 1189-р) вводятся понятия государственных данных и управления государственными данными. Под государственными данными понимается информация, содержащаяся в информационных ресурсах органов и организаций государственного сектора, а также в информационных ресурсах, созданных в целях реализации полномочий

[262] Настоящий раздел является дополнительным к требованиям технического задания.

[263] Распоряжение Правительства Российской Федерации от 03.06.2019 № 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий дорожную карту») по созданию национальной системы управления данными на 2019 - 2021 годы» // СЗ РФ. 2019. № 23. Ст. 3041.

органов и организаций государственного сектора. Управление государственными данными определяется как совокупность процессов сбора, хранения, обработки, предоставления, распространения и уничтожения государственных данных, обеспечения качества государственных данных, включая их систематизацию и гармонизацию. Вместе с тем указанная концепция не носит нормативного характера и предложенные в ней термины и определения не являются легальными дефинициями.

Нормативными правовыми актами Российской Федерации термин «управление данными» не определен. Понятия «управление» и «данные» в отдельности используются в ряде нормативных правовых актов, но в совокупности могут трактоваться как осуществление одного или совокупности действий по формированию (сбору, записи, систематизации, исследованию, анализу, накоплению), хранению, использованию (изменению, преобразованию, гармонизации, предоставлению, раскрытию, распространению), обеспечению доступа к данным, их удалению, а также иной обработке данных.

Основные положения, регулирующие отношения в области управления данными в Российской Федерации, установлены Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[264] (далее – Закон № 149-ФЗ), в том числе посвященные вопросам применения информационных технологий, обеспечения защиты информации, поиска, получения, передачи и ее распространения, отдельными федеральными законами или отдельными положениями федеральных законов, принятыми в соответствии с ними подзаконными актами, указами Президента Российской Федерации и иными нормативными правовыми актами и национальными стандартами.

---

[264] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Часть I). Ст. 212.

Для целей настоящего исследования следует учитывать, что система нормативного правового регулирования в области управления данными в Российской Федерации в краткосрочной перспективе должна быть изменена в целях достижения концептуальных задач, определенных Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[265] (далее – Указ № 204).

В соответствии с подпунктом «ж» пункта 1 Указа № 204 Правительству Российской Федерации поручено в срок до 2024 года обеспечить достижение ускоренного внедрения цифровых технологий в экономике и социальной сфере. В целях реализации поручения Президента Российской Федерации протоколом от 4 июня 2019 г. № 7 президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам утверждена национальная программа «Цифровая экономика Российской Федерации»[266], (далее – Программа цифровой экономики), в рамках которой утверждены, в частности, федеральный проект «Информационная инфраструктура»[267] и федеральный проект «Цифровое государственное управление»[268].

Реализация федерального проекта «Цифровое государственное управление» призвана обеспечить использование цифровых технологий и создание платформенных решений в сферах государственного управления и оказания государственных услуг, предполагает осуществить окончательный переход на электронное взаимодействие граждан и организаций с

---

[265] Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СЗ РФ. 2018. № 20. Ст. 2817.

[266] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» // https://digital.gov.ru/ru/activity/directions/858/.

[267] Там же. П. 4.2.

[268] Там же. П. 4.6.

государством, а также организовать удобное взаимодействие для граждан и организаций.

В соответствии с пунктом 1.2 федерального проекта «Цифровое государственное управление» на Министерство экономического развития Российской Федерации возложена задача в срок до 31 декабря 2020 г. разработать и обеспечить принятие федерального закона и иных нормативных правовых актов, закрепляющих целевое состояние предоставления государственных и муниципальных услуг, в том числе предусмотреть:

– создание реестровой модели их предоставления,

– проактивность,

– экстерриториальность,

– типизацию и стандартизацию приоритетных региональных и муниципальных услуг,

– многоканальность,

– машиночитаемое описание процесса оказания услуг,

– исключение участия человека в процессе принятия решения при предоставлении приоритетных государственных услуг,

– создание единой системы сбора обратной связи от получателей услуг,

– иные направления совершенствования предоставления государственных услуг.

Следует отметить, что в случае каждой государственной или муниципальной информационной системы, в функции которой входит предоставление государственных или муниципальных услуг, важно осуществить анализ возможности применения реестровой модели предоставления государственных и муниципальных услуг. Особенностью управления государственными данными в таких системах является обстоятельство, что юридически значимыми данными в них являются данные реестров (записи в реестрах), а не исходные документы. Так, к ключевой

проблеме создания государственных информационных систем можно отнести включение в них данных прошлых лет («ретроспективные» данные), что зачастую сопряжено с необходимостью перевода в электронный вид большого объема документов и данных прошлых лет, существующих в бумажном виде или хранящихся в устаревших электронных форматах, не предполагающих возможность трансформации в форматы хранения данных в реестрах современных государственных информационных систем.

Значимым фактом также является установление федеральным проектом «Цифровое государственное управление» обязанности внедрения федеральными органами исполнительной власти широкого круга цифровых платформ в целях организации различных видов межведомственного взаимодействия, облегчения предоставления государственных и муниципальных услуг, обеспечения прав граждан Российской Федерации и иностранных граждан (например, создание цифровой платформы «Образование в РФ для иностранцев», платформы поиска работы и подбора персонала на базе информационно-аналитической системы Общероссийская база вакансий «Работа в России» и иных платформ).

В целях настоящего исследования необходимо учесть, что регулирование отношений в области управления данными в Российской Федерации может быть значительно трансформировано в связи с необходимостью разработки и обеспечения утверждения в срок до 31 декабря 2024 г. Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации комплекса национальных документов, направленных на реализацию Цифровой повестки ЕАЭС, в том числе утверждения Положения о координации, мониторинге отборе и продвижении проектов (инициатив), и создания механизма отбора и поддержки проектов (инициатив) по внедрению цифровых технологий и платформ на

пространстве ЕАЭС (пункт 2.1 федерального проекта «Цифровое государственное управление»)[269].

Формирование единого подхода к управлению данными в Российской Федерации должно быть обеспечено Правительством Российской Федерации до 2022 года в соответствии с Концепцией, которая разработана в целях реализации мероприятий федерального проекта «Цифровое государственное управление» Программы цифрового развития. Концепция определяет основные цели, задачи и принципы создания и функционирования национальной системы управления данными.

Национальная система управления данными состоит из следующих взаимосвязанных элементов:

– совокупность нормативных правовых, организационных, методологических правил и процедур, регулирующих отношения органов и организаций государственного сектора, юридических и физических лиц в сфере управления государственными данными, а также обеспечивающих деятельность участников системы,

– федеральная государственная информационная система «Единая информационная платформа национальной системы управления данными» и иные информационно-технологические элементы системы,

– цифровая аналитическая платформа предоставления статистических данных.

Также следует отметить, что с 1 июля 2019 г. по 31 марта 2020 г. в Российской Федерации проводится эксперимент по повышению качества и

[269] Там же.

связанности данных, содержащихся в государственных информационных ресурсах[270].

В рамках указанного эксперимента предусмотрено создание и функционирование федеральной государственной информационной системы «Единая информационная платформа национальной системы управления данными» (далее – Единая платформа управления данными).

Создание и обеспечение функционирования Единой платформы управления данными, а также выполнение иных функций ее оператора возложено на Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации самостоятельно или с привлечением подведомственных ему учреждений в соответствии с законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ и услуг для обеспечения государственных и муниципальных нужд.

Значимым фактом для развития системы управления данными в Российской Федерации является то, что федеральным проектом «Информационная инфраструктура» Программы цифровой экономики предусмотрен ряд мероприятий, направленных:

– на создание генеральной схемы развития сетей связи и инфраструктуры хранения и обработки данных Российской Федерации на период 2019 - 2024 годов,

– на создание глобальной конкурентоспособной инфраструктуры обработки и хранения данных на основе отечественных разработок,

– на разработку комплекса мер по повышению экспортного потенциала услуг по обработке и хранению данных и облачных сервисов,

---

[270] Постановление Правительства Российской Федерации от 03.06.2019 № 710 «О проведении эксперимента о повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» // СЗ РФ. 2019. № 23. Ст. 2963.

– на реализацию первоочередных мероприятий по снятию административных барьеров в целях повышения экспортного потенциала услуг по обработке и хранению данных и облачных сервисов,

– на реализацию комплекса мер по повышению экспортного потенциала услуг по обработке и хранению данных и облачных сервисов,

– на создание распределенной системы центров обработки данных (в том числе с использованием отечественного оборудования), обеспечивающей обработку данных, формируемых российскими гражданами и организациями на территории Российской Федерации,

– на обеспечение хранения и обработки информации, создаваемой органами государственной власти и местного самоуправления в государственной единой облачной платформе по сервисной модели,

– на создание и введение в опытную эксплуатацию государственной единой облачной платформы[271].

Важным аспектом развития управления данными в Российской Федерации является создание технических и программных средств, продуктов, сервисов и платформенных решений на базе «сквозных» цифровых технологий. Под «сквозными» цифровыми технологиями понимаются направления развития информационных технологий, определяемые в соответствии с Положением о проведении конкурсного отбора на предоставление государственной поддержки компаний – лидеров по разработке продуктов, сервисов и платформенных решений на базе «сквозных» цифровых технологий, утвержденным постановлением Правительства Российской Федерации от 3 мая 2019 г. № 549 «О государственной поддержке компаний – лидеров по разработке продуктов, сервисов и платформенных решений на базе «сквозных» цифровых

[271] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» // https://digital.gov.ru/ru/activity/directions/858/. П. 4.6.

технологий»[272] (далее – Положение об отборе «сквозных» цифровых технологий). В соответствии с пунктом 5 Положения об отборе «сквозных» цифровых технологий направлениями «сквозных» цифровых технологий являются:

– большие данные,
– нейротехнологии и искусственный интеллект,
– системы распределенного реестра,
– квантовые технологии,
– новые производственные технологии,
– промышленный интернет,
– компоненты робототехники и сенсорика,
– технологии беспроводной связи,
– технологии виртуальной и дополненной реальностей.

Значимыми для управления данными следует выделить системы распределенного реестра, развитие которых предусмотрено Дорожной картой развития «сквозной» цифровой технологии «Системы распределенного реестра»[273] (далее – Дорожная карта). В соответствии с пунктом 1 Дорожной карты системы распределенного реестра предусматривают:

– технологии организации и синхронизации данных как совокупность методов и инструментов, направленных на определение, организацию и усовершенствование взаимосвязей между частями и элементами распределенных баз данных, а также на обеспечение их согласованности и приведение к соответствию,

---

[272] Постановление Правительства Российской Федерации от 03.05.2019 № 549 «О государственной поддержке компаний - лидеров по разработке продуктов, сервисов и платформенных решений на базе "сквозных" цифровых технологий» // СЗ РФ. 2019. № 19. Ст. 2305.

[273] Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» // https://digital.gov.ru. 2019.

– технологии обеспечения целостности и непротиворечивости данных (консенсус) как совокупность методов и инструментов, направленных на приведение в соответствие имеющихся данных в децентрализованной сети к единой внутренней логике и структуре по заранее определенным правилам, а также обеспечение синхронизации и согласования данных между узлами децентрализованной сети,

– технологии создания и исполнения децентрализованных приложений и смарт-контрактов как совокупность методов и инструментов, направленных на создание приложений, обеспечивающих взаимодействие неограниченного количества участников распределенной системы, и на разработку, поддержание и выполнение компьютерных алгоритмов, предназначенных для автоматизации процессов исполнения контрактов. Децентрализованные приложения обладают прозрачной и открытой логикой, обеспечивающей гарантированное исполнение заданных функций в рамках систем распределенного реестра.

1.4.2 Общий перечень нормативных правовых актов, регулирующих управление данными в Российской Федерации

Гражданский кодекс Российской Федерации (часть первая[274]) регулирует отношения, связанные с участием в корпоративных организациях или с управлением ими (корпоративные отношения), определяет правовое положение участников гражданского оборота, основания возникновения и порядок осуществления права собственности и других вещных прав, общие положения об объектах гражданских прав.

[274] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СЗ РФ. 1994. № 32. Ст. 3301.

Гражданский кодекс Российской Федерации (часть вторая)[275] регулирует договорные и иные обязательства.

Гражданский кодекс Российской Федерации (часть четвертая)[276], определяет основания возникновения и порядок осуществления прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальных прав).

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[277]регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу и распространение информации, применении информационных технологий и обеспечении защиты информации.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[278] регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[279] регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти,

---

[275] Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ // СЗ РФ. 1996. № 5. Ст. 410.

[276] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52 (Часть I). Ст. 5496.

[277] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Часть I). Ст. 212.

[278] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (Часть I). Ст. 4736.

[279] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (Часть I). Ст. 3451.

органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[280] регулирует отношения, связанные с обеспечением доступа пользователей информацией к информации о деятельности государственных органов и органов местного самоуправления.

Федеральный закон от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»[281] регулирует отношения, связанные с обеспечением доступа пользователей информацией к информации о деятельности судов.

---

[280] Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009. № 7. Ст. 776.

[281] Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СЗ РФ. 2008. № 52 (Часть I). Ст. 6217.

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»[282] регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»[283] регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[284] регулирует отношения, возникающие в связи с предоставлением государственных и муниципальных услуг соответственно федеральными органами исполнительной власти, органами государственных внебюджетных фондов, исполнительными органами государственной власти субъектов Российской Федерации, а также местными администрациями и иными органами местного самоуправления, осуществляющими исполнительно-распорядительные полномочия.

Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»[285] устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской

---

[282] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283.

[283] Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. С. 8220-8235.

[284] Федеральный закон от 27.07.2010 N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. 2010. № 31. Ст. 4179.

[285] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. Ст. 2895.

Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Федеральный закон от 21 июля 2005 г. № 115-ФЗ «О концессионных соглашениях»[286] регулирует отношения, возникающие в связи с подготовкой, заключением, исполнением, изменением и прекращением концессионных соглашений, устанавливает гарантии прав и законных интересов сторон концессионного соглашения. Определяет порядок и условия заключения концессионных соглашений в целях привлечения инвестиций в экономику Российской Федерации, обеспечение эффективного использования имущества, находящегося в государственной или муниципальной собственности.

Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»[287] определяет основы правового регулирования отношений, возникающих в связи с подготовкой проекта государственно-частного партнерства, проекта муниципально-частного партнерства, заключением, исполнением и прекращением соглашения о государственно-частном партнерстве, соглашения о муниципально-частном партнерстве, в том числе соответствующие полномочия органов государственной власти, органов местного самоуправления, устанавливает гарантии прав и законных

---

[286] Федеральный закон от 21.07.2005 № 115-ФЗ «О концессионных соглашениях» // СЗ РФ. 2005. № 30 (Часть II). Ст. 3126.

[287] Федеральный закон от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2015. № 29 (Часть I). Ст. 4350.

интересов сторон соглашения о государственно-частном партнерстве, соглашения о муниципально-частном партнерстве.

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[288] регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Указ Президента Российской Федерации от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет»)[289] определяет порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет».

Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на

---

[288] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СЗ РФ. № 15. Ст. 2036.

[289] Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // СЗ РФ. 2015. № 21. Ст. 3092.

2017 – 2030 годы»[290] определяет цели, задачи и меры по реализации внутренней и внешней политики в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Постановление Правительства Российской Федерации от 10 июля 2013 г. № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с «Правилами использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»)[291] устанавливает порядок использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной

[290] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

[291] Постановление Правительства Российской Федерации от 10.07.2013 № 584 «Об использовании федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // СЗ РФ. 2013. № 30 (Часть II). Ст. 4108.

форме» (далее – единая система) в целях, установленных пунктом 1 требований к федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утвержденных постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977[292], а также в случаях, при которых доступ с использованием информационно-телекоммуникационной сети «Интернет» к информации, содержащейся в государственных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе.

Постановление Правительства Российской Федерации от 6 июля 2015 г. № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона «Об информации, информационных технологиях и о защите информации»[293] устанавливает правила осуществления контроля за размещением технических средств информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями, на территории

---

[292] Постановление Правительства Российской Федерации от 28.11.2011 № 977 «О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // СЗ РФ. 2011. № 49 (Часть IV). Ст. 7284.

[293] Постановление Правительства Российской Федерации от 06.07.2015 № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона "Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2015. № 28. Ст. 4240.

Российской Федерации и правила осуществления контроля за соблюдением требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации.

Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»[294] определяет требования к порядку реализации мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем и дальнейшему хранению содержащейся в их базах данных информации, осуществляемых федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации в целях повышения эффективности реализации полномочий органов исполнительной власти в результате использования информационно-коммуникационных технологий либо органами исполнительной власти, выступающими в качестве публичных партнеров, и частными партнерами в соответствии с соглашениями о государственно-частном партнерстве в целях реализации указанных соглашений.

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах

---

[294] Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // СЗ РФ. 2015. № 28. Ст. 4241.

исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»[295] определяет общий порядок обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности, а также на подведомственных им предприятиях, в учреждениях и организациях.

Постановление Правительства Российской Федерации от 13 июня 2012 г. № 584 «Об утверждении Положения о защите информации в платежной системе»[296] устанавливает требования к защите информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем и операторами услуг платежной инфраструктуры в платежной системе (далее соответственно - информация, операторы, агенты).

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных

---

[295] Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» // СЗ РФ. 2005. № 30 (Часть II). Ст. 3165.

[296] Постановление Правительства Российской Федерации от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе» // СЗ РФ. 2012. № 25. Ст. 3380.

при их обработке в информационных системах персональных данных»[297] устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.

Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия»)[298] определяет назначение и правила формирования и функционирования единой системы межведомственного электронного взаимодействия, а также основы информационного обмена, осуществляемого с ее применением между информационными системами федеральных органов исполнительной власти, государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления, государственных и муниципальных учреждений, многофункциональных центров, иных органов и организаций в целях предоставления государственных и муниципальных услуг, документов (сведений), размещенных в государственных информационных системах и иных информационных системах, и исполнения государственных и муниципальных функций в электронной форме.

Постановление Правительства Российской Федерации от 7 июня 2019 г. № 733 «Об общероссийских классификаторах технико-экономической и

---

[297] Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. 2012. № 45. Ст. 6257.

[298] Постановление Правительства Российской Федерации от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» // СЗ РФ. 2010. № 38. Ст. 4823.

социальной информации»[299] устанавливает порядок разработки, ведения, изменения и применения общероссийских классификаторов технико-экономической и социальной информации.

Приказ ФСБ России от 13 ноября 1999 г. № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»[300] устанавливает основные принципы, организационную структуру системы сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, порядок проведения сертификации этих средств, порядок регистрации сертифицированных средств, а также порядок проведения инспекционного контроля за сертифицированными средствами.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[301] устанавливает требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения,

---

[299] Постановление Правительства Российской Федерации от 07.06.2019 № 733 «Об общероссийских классификаторах технико-экономической и социальной информации» // СЗ РФ. 2019. № 24. Ст. 3093.

[300] Приказ ФСБ России от 13.11.1999 № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2000. № 3.

[301] Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета. 2013. № 136.

искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

1.4.3 Перечень нормативных правовых актов, регулирующих функционирование отдельных государственных информационных систем в Российской Федерации

Федеральный закон от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей»[302] регулирует отношения, возникающие в связи с государственной регистрацией юридических лиц при их создании, реорганизации и ликвидации, при внесении изменений в их учредительные документы, государственной регистрацией физических лиц в качестве индивидуальных предпринимателей и государственной регистрацией при прекращении физическими лицами деятельности в качестве индивидуальных предпринимателей, а также в связи с ведением государственных реестров – единого государственного реестра юридических лиц и единого государственного реестра индивидуальных предпринимателей.

Федеральный закон от 30 декабря 2015 г. № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации»[303] регулирует отношения, возникающие при осуществлении геодезической и картографической деятельности, включая поиск, сбор, хранение, обработку, предоставление и распространение пространственных данных, в том числе с использованием информационных систем.

---

[302] Федеральный закон от 08.08.2001 № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей» // СЗ РФ. 2001. № 33 (Часть I). Ст. 3431.

[303] Федеральный закон от 30.12.2015 № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2016. № 1 (Часть I). Ст. 51.

Федеральный закон от 13 июля 2015 г. № 218-ФЗ «О государственной регистрации недвижимости»[304] регулирует отношения, возникающие в связи с осуществлением на территории Российской Федерации государственной регистрации прав на недвижимое имущество и сделок с ним, подлежащих в соответствии с законодательством Российской Федерации государственной регистрации, государственного кадастрового учета недвижимого имущества, подлежащего такому учету согласно настоящему Федеральному закону, а также ведением Единого государственного реестра недвижимости и предоставлением предусмотренных настоящим Федеральным законом сведений, содержащихся в Едином государственном реестре недвижимости.

Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[305] регулирует отношения, возникающие в сфере охраны здоровья граждан и в том числе возникающие в связи с созданием и эксплуатацией единой государственной информационной системой в сфере здравоохранения.

Федеральный закон от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» [306] устанавливает правовую основу и принципы организации индивидуального (персонифицированного) учета сведений о гражданах Российской Федерации, постоянно или временно проживающих (пребывающих) на территории Российской Федерации иностранных гражданах и лицах без гражданства в целях обеспечения реализации их прав в системе обязательного пенсионного страхования, а также в целях

---

[304] Федеральный закон от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости» // СЗ РФ. 2015. № 29 (Часть I). Ст. 4344.

[305] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // СЗ РФ. 2011. № 48. Ст. 6724.

[306] Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» // СЗ РФ. 2011. № 14. Ст. 1401.

предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций.

Федеральный закон от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния»[307] определяет порядок ведения Единого государственного реестра записей актов гражданского состояния.

Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»[308] регулирует отношения, возникающие в связи с созданием и эксплуатацией государственной информационной системы в области средств массовой информации.

Федеральный закон от 15 июля 1995 г. № 101-ФЗ «О международных договорах Российской Федерации»[309] определяет порядок заключения, выполнения и прекращения международных договоров Российской Федерации, регулирует вопросы единой государственной системы регистрации и учета международных договоров Российской Федерации.

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»[310] регулирует вопросы ведения единых реестров технической документации и федерального информационного фонда технических регламентов и стандартов.

Федеральный закон от 22 мая 2003 г. № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской

---

[307] Федеральный закон от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния» // СЗ РФ. 1997. № 47. Ст. 5340.

[308] Закон Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации» // Российская газета. 1992. № 32.

[309] Федеральный закон от 15.07.1995 № 101-ФЗ «О международных договорах Российской Федерации» // СЗ РФ. 1995. № 29. Ст. 2757.

[310] Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // СЗ РФ. 2002. № 52 (Часть I). Ст. 5140.

Федерации»[311] определяются правила применения контрольно-кассовой техники при осуществлении расчетов в целях обеспечения интересов граждан и организаций, защиты прав потребителей, обеспечения установленного порядка осуществления расчетов, полноты учета выручки в организациях и у индивидуальных предпринимателей, в том числе в целях налогообложения и обеспечения установленного порядка оборота товаров, регулируются вопросы передачи данных в государственную информационную систему мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации, или федеральную государственную информационную систему мониторинга движения лекарственных препаратов для медицинского применения от производителя до конечного потребителя с использованием в отношении лекарственных препаратов для медицинского применения средств идентификации.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[312] определяет особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных.

Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»[313] регулирует вопросы государственной федеральной информационной статистической системы.

---

[311] Федеральный закон от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» // СЗ РФ. 2003. № 21. Ст. 1957.

[312] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (Часть I). Ст. 3451.

[313] Федеральный закон от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» // СЗ РФ. 2007. № 49. Ст. 6043.

Федеральный закон от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений»[314] регулирует отношения, возникающие при выполнении измерений, установлении и соблюдении требований к измерениям, единицам величин, эталонам единиц величин, стандартным образцам, средствам измерений, применении стандартных образцов, средств измерений, методик (методов) измерений, а также при осуществлении деятельности по обеспечению единства измерений, предусмотренной законодательством Российской Федерации об обеспечении единства измерений, в том числе при выполнении работ и оказании услуг по обеспечению единства измерений, регулирует вопросы ведения единого перечня измерений.

Федеральный закон от 6 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете»[315] регулирует вопросы, связанные с функционированием государственного информационного ресурса бухгалтерской (финансовой) отчетности.

Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»[316] регулирует вопросы, связанные с функционированием единой информационной системы в сфере закупок.

Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации»[317] устанавливает правовые основы стандартизации, в том числе функционирования национальной системы стандартизации, и

---

[314] Федеральный закон от 26.06.2008 № 102-ФЗ «Об обеспечении единства измерений» // СЗ РФ. 2008. № 26. Ст. 3021.

[315] Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете» // СЗ РФ. 2011. № 50. Ст. 7344.

[316] Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // СЗ РФ. 2013. № 14. Ст. 1652.

[317] Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации» // СЗ РФ. 2015. № 27. Ст. 3953.

направлен на обеспечение проведения единой государственной политики в сфере стандартизации.

Федеральный закон от 23 ноября 2009 г. № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации»[318] регулирует отношения, возникающие в связи с созданием и эксплуатацией государственной информационной системы в области энергосбережения и повышения энергетической эффективности.

Федеральный закон от 3 декабря 2011 г. № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»[319] регулирует отношения, возникающие в связи с созданием, эксплуатацией и совершенствованием государственной информационной системы топливно-энергетического комплекса, включая сбор, обработку информации для включения в данную систему, хранение такой информации, обеспечение доступа к ней, ее предоставление и распространение.

Федеральный закон от 21 июля 2014 г. № 209-ФЗ «О государственной информационной системе жилищно-коммунального хозяйства»[320] регулирует отношения, возникающие при создании, эксплуатации и модернизации государственной информационной системы жилищно-коммунального хозяйства, в том числе сборе, обработке информации для ее включения в данную информационную систему, хранении такой информации,

---

[318] Федеральный закон от 23.11.2009 № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2009. № 48. Ст. 5711.

[319] Федеральный закон от 03.12.2011 № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса» // СЗ РФ. 2011. № 49 (Часть IV). Ст. 7060.

[320] Федеральный закон от 21.07.2014 № 209-ФЗ «О государственной информационной системе жилищно-коммунального хозяйства» // СЗ РФ. 2014. № 30 (Часть I). Ст. 4210.

обеспечении доступа к ней, ее предоставлении, размещении и распространении.

Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации»[321] регулирует отношения, возникающие в связи с созданием и эксплуатацией государственной информационной системы промышленности.

Градостроительный кодекс Российской Федерации[322] регулирует отношения, возникающие в связи с созданием и эксплуатацией государственных информационных систем обеспечения градостроительной деятельности.

Постановление Правительства Российской Федерации от 8 июля 2014 г. № 631 «Об общефедеральном учете выданных паспортов граждан Российской Федерации, удостоверяющих личность граждан Российской Федерации за пределами территории Российской Федерации, в том числе содержащих электронный носитель информации»[323] определяет правила ведения общефедерального учета паспортов граждан Российской Федерации, удостоверяющих их личность за пределами территории Российской Федерации, в том числе содержащих электронный носитель информации.

Постановление Правительства Российской Федерации от 29 декабря 2008 г. № 1057 «Об утверждении Положения о межведомственной интегрированной автоматизированной информационной системе федеральных органов исполнительной власти, осуществляющих

---

[321] Федеральный закон от 31.12.2014 № 488-ФЗ «О промышленной политике в Российской Федерации» // СЗ РФ. 2015. № 1 (Часть I). Ст. 41.

[322] Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ // СЗ РФ. 2005. № 1 (Часть I). Ст. 16.

[323] Постановление Правительства Россйиской Федерации от 08.07.2014 № 631 «Об общефедеральном учете выданных паспортов граждан Российской Федерации, удостоверяющих личность граждан Российской Федерации за пределами территории Российской Федерации, в том числе содержащих электронный носитель информации» // СЗ РФ. 2014. № 28. Ст. 4071.

контроль в пунктах пропуска через государственную границу Российской Федерации»[324] определяет порядок формирования, обеспечения и функционирования межведомственной интегрированной автоматизированной информационной системы федеральных органов исполнительной власти, осуществляющих контроль в пунктах пропуска через государственную границу Российской Федерации, порядок доступа к необходимой для проведения контроля в пунктах пропуска информации, предоставления, использования и защиты информации, а также взаимодействия федеральных органов исполнительной власти, осуществляющих контроль в пунктах пропуска.

Постановление Правительства Российской Федерации от 30 января 2016 г. № 48 «О федеральной государственной информационной системе «Единый фонд геологической информации о недрах» (вместе с «Положением о федеральной государственной информационной системе «Единый фонд геологической информации о недрах»)[325] определяет порядок создания и эксплуатации федеральной государственной информационной системы «Единый фонд геологической информации о недрах», состав геологической информации о недрах, представляемой обладателями информации в информационную систему, порядок информационного взаимодействия оператора информационной системы с обладателями информации и ее пользователями, порядок обеспечения доступа к информации, содержащейся

[324] Постановление Правительства Российской Федерации от 29.12.2008 № 1057 «Об утверждении Положения о межведомственной интегрированной автоматизированной информационной системе федеральных органов исполнительной власти, осуществляющих контроль в пунктах пропуска через государственную границу Российской Федерации» // СЗ РФ. 2009. № 3. Ст. 382.

[325] Постановление Правительства Российской Федерации от 30.01.2016 № 48 «О федеральной государственной информационной системе «Единый фонд геологической информации о недрах» // СЗ РФ. 2016. № 6. Ст. 844.

в информационной системе, порядок взаимодействия информационной системы с иными государственными информационными системами.

Распоряжение Правительства Российской Федерации от 28 декабря 2018 г. № 2963-р «Об утверждении Концепции создания и функционирования в Российской Федерации системы маркировки товаров средствами идентификации и прослеживаемости движения товаров»[326] определяет основные требования к государственной информационной системе маркировки товаров средствами идентификации и прослеживаемости движения товаров.

Приказ Минкомсвязи России от 19 января 2015 г. № 7 «Об утверждении Положения о федеральной государственной информационной системе «Единая система нормативной справочной информации», а также Перечня нормативной справочной информации, подлежащей размещению в федеральной государственной информационной системе "Единая система нормативной справочной информации»[327] определяет вопросы функционирования федеральной государственной информационной системы «Единая система нормативной справочной информации».

Приказ Минэкономразвития России №412, МВД России №645, Министра обороны Российской Федерации № 1183, Минюста России № 216, МЧС России № 422, Минздравсоцразвития России № 782н, Минкомсвязи России № 120, ФСБ России № 425, ФСКН России № 370, ФТС России №

---

[326] Распоряжение Правительства Российской Федерации от 28.12.2018 № 2963-р «Об утверждении Концепции создания и функционирования в Российской Федерации системы маркировки товаров средствами идентификации и прослеживаемости движения товаров» // СЗ РФ. 2019. № 1. Ст. 87.

[327] Приказ Минкомсвязи России от 19.01.2015 № 7 «Об утверждении Положения о федеральной государственной информационной системе «Единая система нормативной справочной информации», а также Перечня нормативной справочной информации, подлежащей размещению в федеральной государственной информационной системе "Единая система нормативной справочной информации» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2015. № 39.

1638, ФМС России № 264, ФНС России № ММВ-7-6/437а от 3 сентября 2010 г. «О функционировании государственной информационной системы «Правоохранительный портал Российской Федерации» (вместе с «Положением о государственной информационной системе «Правоохранительный портал Российской Федерации», «Регламентом подготовки и размещения информации в государственной информационной системе «Правоохранительный портал Российской Федерации», «Регламентом межведомственного обмена информацией с использованием государственной информационной системы «Правоохранительный портал Российской Федерации»)[328] определяет цели и правила функционирования государственной информационной системы «Правоохранительный портал Российской Федерации».

1.4.4 Нормативные правовые акты, регулирующие концептуальные вопросы управления данными в Российской Федерации

Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»[329] определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной

---

[328] Приказ Минэкономразвития России № 412, МВД России № 645, Министра обороны Российской Федерации № 1183, Минюста России № 216, МЧС России № 422, Минздравсоцразвития России № 782н, Минкомсвязи России № 120, ФСБ России № 425, ФСКН России № 370, ФТС России № 1638, ФМС России № 264, ФНС России № ММВ-7-6/437а от 03.09.2010 «О функционировании государственной информационной системы "Правоохранительный портал Российской Федерации» // http://legalacts.ru/doc/prikaz-minekonomrazvitija-rf-n-412-mvd-rf.

[329] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[330] определяет национальные цели развития Российской Федерации на период до 2024 года, в том числе в части управления данными.

Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[331] определяет стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

Национальная программа «Цифровая экономика Российской Федерации», утвержденная президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7)[332] определяет структуру национального проекта «Цифровая экономика Российской Федерации», его целевые показатели, мероприятия, сроки и исполнителей в целях достижения национальных целей развития Российской Федерации на период до 2024 года, предусмотренных Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

---

[330] Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СЗ РФ. 2018. № 20. Ст. 2817.

[331] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[332] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» // https://digital.gov.ru/ru/activity/directions/858/.

Постановление Правительства Российской Федерации от 3 июня 2019 г. № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (вместе с «Положением о проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах»)[333] устанавливает порядок проведения эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах.

Концепция создания и функционирования национальной системы управления данными и план мероприятий («дорожная карта») по созданию национальной системы управления данными на 2019–2021 годы, утвержденная распоряжением Правительства Российской Федерации от 3 июня 2019 г. № 1189-р[334], определяет цели, задачи и принципы создания и функционирования национальной системы управления данными, порядок ее создания, основные составляющие ее элементы, а также общую оценку ожидаемого социально-экономического эффекта от ее создания.

Концепция создания государственной единой облачной платформы, утвержденная распоряжением Правительства Российской Федерации от 28 августа 2019 г. № 1911-р[335], определяет принципы создания государственной единой облачной платформы, перевода информационных систем в государственную единую облачную платформу и обеспечения защиты информации в государственной единой облачной платформе, подход к

[333] Постановление Правительства Российской Федерации от 03.06.2019 № 710 «О проведении эксперимента о повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» // СЗ РФ. 2019. № 23. Ст. 2963.

[334] Распоряжение Правительства Российской Федерации от 03.06.2019 № 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий дорожную карту») по созданию национальной системы управления данными на 2019 - 2021 годы» // СЗ РФ. 2019. № 23. Ст. 3041.

[335] Распоряжение Правительства Российской Федерации от 28.08.2019 № 1911-р «Об утверждении Концепции создания государственной единой облачной платформы»

переходу на использование государственной единой облачной платформы, поставщиков услуг облачных вычислений и программных услуг, принципы перехода на использование государственной единой облачной платформы и ожидаемые результаты.

Договор о Евразийском экономическом союзе от 29 мая 2014 г.[336] учреждает Евразийский экономический союз как международную региональную организацию экономической интеграции для обеспечения свободы движения товаров, услуг, капитала и рабочей силы, проведения скоординированной, согласованной или единой политики в отраслях экономики государств-членов союза.

Решение Коллегии Евразийской экономической комиссии от 9 июня 2015 г. № 63 «О Методике анализа, оптимизации, гармонизации и описания общих процессов в рамках Евразийского экономического союза»[337] определяет методические рекомендации и технические требования к проектированию и описанию общих процессов при формировании технологических документов, регламентирующих информационное взаимодействие при реализации средствами интегрированной информационной системы внешней и взаимной торговли общих процессов.

Решение Коллегии Евразийской экономической комиссии от 26 декабря 2017 г. № 190 «Об утверждении Положения о модели данных Евразийского экономического союза»[338] определяет цель создания, общие

---

[336] Договор о Евразийском экономическом союзе // 2015. Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 2015.

[337] Решение Коллегии Евразийской экономической комиссии от 09.06.2015 № 63 «О Методике анализа, оптимизации, гармонизации и описания общих процессов в рамках Евразийского экономического союза» // http://www.eaeunion.org. 2015.

[338] Решение Коллегии Евразийской экономической комиссии от 26.12.2017 № 190 «Об утверждении Положения о модели данных Евразийского экономического союза» // http://www.eaeunion.org. 2017.

принципы и порядок разработки, развития, распространения и применения модели данных Евразийского экономического союза.

Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года»[339] определяет цели, принципы, задачи, направления и механизмы сотрудничества государств-членов по вопросам реализации цифровой повестки Евразийского экономического союза до 2025 года.

1.4.5 Техническое регулирование управления данными в Российской Федерации

Федеральный закон от 27декабря 2002 г. № 184-ФЗ «О техническом регулировании»[340] устанавливает особенности технического регулирования в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну.

Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации»[341] определяет цели и основные задачи развития искусственного интеллекта в Российской Федерации, а также меры, направленные на его использование в целях обеспечения национальных интересов и реализации стратегических

---

[339] Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» // http://www.eaeunion.org. 2017.

[340] Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // СЗ РФ. 2002. № 52 (Часть I). Ст. 5140.

[341] Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // СЗ РФ. 2019. № 41. Ст. 5700.

национальных приоритетов, в том числе в области научно-технологического развития.

Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»[342] определяет порядок лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и

[342] Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» // СЗ РФ. 2012. № 17. Ст. 1987.

телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), осуществляемой юридическими лицами и индивидуальными предпринимателями.

Постановление Правительства Российской Федерации от 3 мая 2019 г. № 549 «О государственной поддержке компаний - лидеров по разработке продуктов, сервисов и платформенных решений на базе «сквозных» цифровых технологий»[343] определяет правила предоставления субсидий из федерального бюджета на государственную поддержку компаний – лидеров по разработке продуктов, сервисов и платформенных решений на базе «сквозных» цифровых технологий и порядок проведения конкурсного отбора на предоставление государственной поддержки компаний – лидеров по разработке продуктов, сервисов и платформенных решений на базе «сквозных» цифровых технологий.

Распоряжение Правительства Российской Федерации от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия

---

[343] Постановление Правительства Российской Федерации от 03.05.2019 № 549 «О государственной поддержке компаний - лидеров по разработке продуктов, сервисов и платформенных решений на базе "сквозных" цифровых технологий» // СЗ РФ. 2019. № 19. Ст. 2305.

системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти»[344] определяет технические требования к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти.

Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»[345] устанавливает требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

«Методический документ. Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11 февраля 2014 г.[346] детализирует организационные и технические меры защиты информации, принимаемые в государственных информационных системах в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17[347].

---

[344] Распоряжение Правительства Российской Федерации от 02.10.2009 № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти» // СЗ РФ. 2009. № 41. Ст. 4818.

[345] Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // Российская газета. 2013. № 208.

[346] «Методический документ. Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014 // http://fsctec.ru. 2014.

[347] Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета. 2013. № 136.

К национальным стандартам Российской Федерации в области управления данными относятся:

– ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»,

– ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»,

– ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем»,

– ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»,

– ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»,

– ГОСТ 2.051-2006 «Единая система конструкторской документации. Электронные документы. Общие положения»,

– ГОСТ 2.053-2006 «Единая система конструкторской документации. Электронная структура изделия. Общие положения»,

– ГОСТ 2.611-2011 «Единая система конструкторской документации. Электронный каталог изделий. Общие положения»,

– ГОСТ 2.612-2011 «Единая система конструкторской документации. Электронный формуляр. Общие положения»,

– ГОСТ 7.0-99 «Система стандартов по информации, библиотечному и издательскому делу. Информационно-библиотечная деятельность, библиография. Термины и определения»,

– ГОСТ 7.70-2003 «Система стандартов по информации, библиотечному и издательскому делу. Описание баз данных и машиночитаемых информационных массивов. Состав и обозначение характеристик»,

– ГОСТ 7.73-96 «Система стандартов по информации, библиотечному и издательскому делу. Поиск и распространение информации. Термины и определения»,

– ГОСТ Р 22.0.02-94 «Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий»,

– ГОСТ Р 22.0.05-94 «Безопасность в чрезвычайных ситуациях. Техногенные чрезвычайные ситуации. Термины и определения»,

– ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»,

– ГОСТ 34.320-96 «Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы»,

– ГОСТ 34.321-96 «Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными»,

– ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения»,

– ГОСТ 20886-85 «Организация данных в системах обработки данных. Термины и определения»,

– ГОСТ 22487-77 «Проектирование автоматизированное. Термины и определения»,

– ГОСТ 25868-91 «Оборудование периферийное систем обработки информации. Термины и определения»,

– ГОСТ 26553-85 «Обслуживание средств вычислительной техники централизованное комплексное. Термины и определения»,

– ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

– ГОСТ Р 7.0.8-2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения»,

– ГОСТ Р 7.0.10-2010 «Система стандартов по информации, библиотечному и издательскому делу. Набор элементов метаданных «Дублинское ядро»,

– ГОСТ Р 43.2.2-2009 «Информационное обеспечение техники и операторской деятельности. Язык операторской деятельности. Общие положения по применению»,

– ГОСТ Р 50646-2012 «Услуги населению. Термины и определения»,

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»,

– ГОСТ Р 50779.11-2000 «Статистические методы. Статистическое управление качеством. Термины и определения»,

– ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»,

– ГОСТ Р 51170-98 «Качество служебной информации. Термины и определения»,

– ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»,

– ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»,

– ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения»,

– ГОСТ Р 51904-2002 «Программное обеспечение встроенных систем. Общие требования к разработке и документированию»,

– ГОСТ Р 52292-2004 «Информационная технология. Электронный обмен информацией. Термины и определения»,

– ГОСТ Р 52438-2005 «Географические информационные системы. Термины и определения»,

– ГОСТ Р 52573-2006 «Географическая информация. Метаданные»,

– ГОСТ Р 52591-2006 «Система передачи данных пользователя в цифровом телевизионном формате. Основные параметры»,

– ГОСТ Р 52653-2006 «Информационно-коммуникационные технологии в образовании. Термины и определения»,

– ГОСТ Р 52872-2012 «Интернет-ресурсы. Требования доступности для инвалидов по зрению»,

– ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»,

– ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»,

– ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования»,

– ГОСТ Р 53339-2009 «Данные пространственные базовые. Общие требования»,

– ГОСТ Р 53801-2010 «Связь федеральная. Термины и определения»,

– ГОСТ Р 54097-2010 «Ресурсосбережение. Наилучшие доступные технологии. Методология идентификации»,

– ГОСТ Р 55062-2012 «Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения»,

– ГОСТ Р 56174-2014 «Информационные технологии. Архитектура служб открытой Грид-среды. Термины и определения»,

– ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»,

– ГОСТ Р 56875-2016 «Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий»,

– ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 «Системная и программная инженерия. Описание архитектуры»,

– ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем»,

– ГОСТ Р 57773-2017 (ИСО 19157:2013) «Пространственные данные. Качество данных»,

– ГОСТ Р ИСО/МЭК 2382-23-2004 «Информационная технология. Словарь. Часть 23. Обработка текста»,

– ГОСТ Р ИСО 8000-2-2014 «Качество данных. Часть 2. Словарь»,

– ГОСТ Р ИСО 9000-2015 «Системы менеджмента качества. Основные положения и словарь»,

– ГОСТ Р ИСО 9241-110-2009 «Эргономика взаимодействия человек-система. Часть 110. Принципы организации диалога оригинал документа»,

– ГОСТ Р ИСО 9241-210-2012 «Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем оригинал документа»,

– ГОСТ Р ИСО 10303-1-99 «Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 1. Общие представления и основополагающие принципы»,

– ГОСТ Р ИСО 15188-2012 «Принципы управления проектами стандартизации терминологии»,

– ГОСТ Р ИСО 15489-1-2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования»,

– ГОСТ Р ИСО 15926-2-2010 «Системы промышленной автоматизации и интеграция. Интеграция данных жизненного цикла для перерабатывающих предприятий, включая нефтяные и газовые производственные предприятия. Часть 2. Модель данных»,

– ГОСТ Р ИСО/ТС 18308-2008 «Информатизация здоровья. Требования к архитектуре электронного учета здоровья»,

– ГОСТ Р ИСО 19439-2008 «Интеграция предприятия. Основа моделирования предприятия»,

– ГОСТ Р ИСО 21500-2014 «Руководство по проектному менеджменту (PMBOK)»,

– ГОСТ Р ИСО 23081-1-2008 «Система стандартов по информации, библиотечному и издательскому делу. Процессы управления документами. Метаданные для документов. Часть 1. Принципы»,

– ГОСТ ISO 9000-2011 «Системы менеджмента качества. Основные положения и словарь»,

– ГОСТ ISO 22745-11-2017 «Системы промышленной автоматизации и интеграция. Открытые технические словари и их применение к основным данным. Часть 11. Руководящие принципы по формулированию терминологии»,

– ГОСТ Р ИСО/МЭК 9834-3-2009 «Информационная технология. Взаимосвязь открытых систем. Процедуры действий уполномоченных по регистрации ВОС. Часть 3. Регистрация дуг дерева идентификатора объекта, расположенных ниже дуги, администрируемой совместно ИСО и МСЭ-Т»,

– ГОСТ Р ИСО/МЭК ТО 10032-2007 «Эталонная модель управления данными»,

– ГОСТ Р ИСО/МЭК 11179-1-2010 «Информационная технология. Регистры метаданных (РМД). Часть 1. Основные положения»,

– ГОСТ Р ИСО/МЭК 11179-3-2012 «Информационная технология. Регистры метаданных (РМД). Часть 3. Метамодель регистра и основные атрибуты»,

– ГОСТ Р ИСО/МЭК 19762-1-2011 «Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь. Часть 1. Общие термины в области АИСД»,

– ГОСТ Р ИСО/МЭК 20000-1-2013 «Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами»,

– ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»,

– ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»,

– ГОСТ Р ИСО/МЭК 33001-2017 «Информационные технологии. Оценка процесса. Понятия и терминология»,

– ГОСТ Р ИСО/ТС 14048-2009 «Экологический менеджмент. Оценка жизненного цикла. Формат документирования данных»,

– ГОСТ Р 56272-2014/ISO/TS 15926-8:2011 «Системы промышленной автоматизации и интеграция. Интеграция данных жизненного цикла перерабатывающих предприятий, включая нефтяные и газовые производственные предприятия. Часть 8. Практические методы интеграции распределенных систем: практическая реализация сетевого языка онтологий (OWL)».

## 2 Анализ национального законодательства зарубежных государств-лидеров правового регулирования в области управления данными и правового регулирования управления данными в Российской Федерации

### 2.1 Основы правового режима данных, в том числе в государственных информационных системах, и правового статуса участников их оборота

#### 2.1.1 Правовой режим данных в Европейском союзе

Регулирование оборота данных и данных европейских информационных систем не унифицировано. Отсутствуют общие положения о правовых режимах информации, общие определения статуса субъектов указанных режимов. Термин «владелец информации» также не применяется.

Одновременно установлено правовое регулирование отдельных категорий данных: данных публичного сектора, открытых данных, персональных данных, пространственных данных.

Европейское право устанавливает правовые основы оборота данных публичного сектора, общие для всех стран-участников, с уклоном в развитие института открытых данных и реализацию права на доступ к информации. Правовое регулирование открытых данных на уровне ЕС было впервые установлено Директивой 2003/98/ЕС от 17.11.2003 о последующем использовании информации государственного сектора.[348] В п. 8 преамбулы Директивы отмечается, что государственные органы используют и производят информацию для выполнения возложенных на них публичных обязанностей, однако для развития информационного общества необходимо также установить правовое регулирование последующего использования производимых ими данных. Преамбула упоминает, кроме того, реализацию

[348] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information http://data.europa.eu/eli/dir/2003/98/2013-07-17 (дата обращения 5 04 2019)

права на знание, относя его к фундаментальным правам в демократическом режиме.

В 2013 г. действие Директивы распространено на библиотеки (включая университетские), музеи и архивы[349]. Часть 8 преамбулы Директивы, вносившей изменения, содержит четкое указание, что государственные органы обязаны делать публично доступной любую информацию, не относящуюся к информации ограниченного доступа. Директива, тем не менее, не вносит изменений в национальные режимы условий ограничения доступа.

Принимая во внимание необходимость совершенствования норм об открытых данных, Европейская комиссия провела с июня 2017г. по январь 2018г. публичную консультацию об усовершенствовании Директивы и опубликовала результаты[350]. В частности, был поставлен вопрос о предоставлении государственными органами динамических данных в онлайн-режиме. Кроме того, было отмечено, что многие органы ссылаются на право *sui generis* на базы данных для отказа в запрашиваемой информации. Комиссия также провела оценку влияния Директивы и обнародовала результаты 25.04.2018.[351]

Результатом указанных действий стало принятие Директивы 2019/1024 от 20.06.2019 об открытых данных и последующем использовании

---

[349] Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public Texte présentant de l'intérêt pour l'EEE. // http://data.europa.eu/eli/dir/2013/37/oj (дата обращения 16 05 2019)

[350] Synopsis report of the public consultation on the revision of the Directive on the reuse of public sector information. 25th April, 2018 // https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-revision-directive-reuse-public-sector-information (дата обращения 31 05 2019)

[351] Impact Assessment on the review of the Directive 2003/98/EC on the reuse of public sector information // https://ec.europa.eu/digital-single-market/en/news/impact-assessment-review-directive-200398ec-reuse-public-sector-information (дата обращения 17 04 2019)

информации публичного сектора[352]. Новая Директива вводит в сферу оборота открытых данных также данные предприятий и учреждений, данные исследований, проводимых за счет бюджетных средств. Основной акцент сделан на максимально возможном открытии данных государственного сектора и формировании бизнес-моделей, использующих их. Положения предыдущей директивы сохранены, однако значительно дополнены. Во многом именно усиление акцента на открытых данных объясняет принятие новой директивы вместо поправок к предыдущей.

Основные субъекты Директивы 2019/1024 от 20.06.2019: государственные органы, государственные предприятия и учреждения, создающие информацию публичного сектора в рамках реализации их полномочий, имеющие обязанность предоставлять запрашиваемую третьими лицами информацию; третьи лица – любые иные лица, как физические, так и юридические, в распоряжении которых находится информация публичного сектора. Третьи лица могут иметь дополнительные обязанности по использованию полученной ими информации в соответствии с условиями лицензии использования, установленными органом, предоставившим такую информацию или сделавшим ее общедоступной.

Персональные данные регулируются Регламентом о защите персональных данных 2018/1725 от 23.10.2018 (GDPR)[353]. Регламент обеспечивает единое регулирование персональных данных на территории ЕС в целом, что способствует формированию единого рынка данных и

---

[352] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information // http://data.europa.eu/eli/dir/2019/1024/oj (дата обращения 10 11 2019)

[353] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) // http://data.europa.eu/eli/reg/2018/1725/oj ( дата обращения6 10 20190

гарантирует защиту прав субъектов персональных данных. Регламент обеспечивает гарантии реализации права субъекта персональных данных – физического лица на контроль над его персональными данными, включая их уточнение, понимание количества обрабатываемых данных и цели их обработки.

Регламент установил основные принципы защиты персональных данных (см. книгу 1).

Среди ключевых для оборота данных в целом стоит отметить право на «переносимость данных» (data portability), установленное в ст. 22 Регламента, предполагающее возможность субъекта запросить все данные, имеющиеся о нем, получить их в доступном формате, а равно отозвать согласие на их обработку или поручить передать их полностью иному оператору персональных данных, если это технически возможно. Примечательно, что указанное право не применяется к данным, обработка которых необходима для реализации функции публичного органа в публичном интересе.

С целью обеспечения защиты субъектов персональных данных не только в государствах-участниках, но и при их обработке органами самого Европейского союза также принят Регламент 2018/1725 об обработке персональных данных органами и учреждениями Европейского союза и свободном движении таких данных[354]. Регламент повторил принципы обработки персональных данных, установленные GDPR, а также уточнил ряд особенностей использования данных, в том числе предусмотрел возможность их обработки в иных целях, сходных с целью сбора, если согласия субъекта нет (ст. 6).

---

[354] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) // http://data.europa.eu/eli/reg/2018/1725/oj (дата обращения 24 11 2019)

Основные субъекты правового режима персональных данных: субъект персональных данных, оператор персональных данных (data controller) и лицо, осуществляющее обработку по поручению (data processor). Субъект персональных данных наделен правомочием контролировать использование предоставленных им данных в целях их предоставления, знать и запрашивать в этой связи необходимую информацию у оператора. Оператор определяет цели и способы обработки персональных данных, обязан принимать необходимые меры по их защите и обрабатывать их в соответствии с общими принципами обработки персональных данных

Помимо общего регулирования оборота данных в публичной сфере, Европейским союзом также установлены особенности регулирования отдельных категорий значимых данных. Директива 2007/2/ЕС от 14.03.2007 об установлении инфраструктуры пространственных данных в Европейском сообществе (INSPIRE)[355] способствует установлению единой инфраструктуры, позволяющей государственным органам обмениваться пространственными данными без барьеров во взаимодействии разных форматов. Во внимание также принимаются данные, которые могут влиять на окружающую среду, находящиеся в распоряжении третьих лиц. Преамбула Директивы призывает государства ЕС предложить таким третьим лицам внести вклад в формирование национальной инфраструктуры пространственных данных. С учетом внимания новой Директивы об открытых данных к динамическим данным, Директива о пространственных данных гармонично дополняет современную политику ЕС по формированию рынка публичных данных, а равно позволяет оценивать качество окружающей среды.

[355] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) // http://data.europa.eu/eli/dir/2007/2/oj (дата обращения 20 01 2019)

Итак, общий правовой режим данных в Европейском праве создается путем принятия отдельных регулирующих актов в сферах, оказывающих влияние на единый европейский рынок данных. На наднациональном уровне сформирован правовой статус субъекта персональных данных. Развитие оборота публичных данных, упрощение доступа к пространственным данным, обеспечивается директивами, оставляющими странам ЕС большую свободу в определении национального регулирования, но определяющими основные направления его развития.

Недавно (20.07.2019) принята Директива ЕС 2019/1024 об открытых данных и повторном использовании информации государственного сектора[356], которая заменила Директиву 2003/98 и расширила сферу действия прежней Директивы об открытых данных. Новая Директива в основном направлена на экономические аспекты повторного использования данных. Кроме того, она дополнительно к ранее установленной сфере действия распространяет свое действие на организации, предоставляющие свои данные для повторного использования, музеи, архивы, библиотеки и т.п., усиливает прозрачность государственных и частных партнерств, касающихся информации государственного сектора, ограничивая эксклюзивные соглашения.

2.1.2 Правовой режим данных в Германии

Государственные органы располагают огромным количеством различных данных, собранных в процессе административной деятельности, которые могут быть повторно использованы.

[356] Directive (EU) 2019/1024 of 20 June 2019 on open data and the re-use of public sector information. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&rid=1 (дата обращения: 10.11.2019)

В Германии на национальном уровне существует Закон о повторном использовании данных (IWG)[357], в основном воспринявший положения Директивы 2003/98. Однако в связи с принятием Директивы 2019/1024 законодательство Германии находится в процессе актуализации.

Закон о свободе информации от 05.09.2005 (IFG)[358] закрепляет право на доступ каждого к официальной информации федеральных органов власти. К ней отнесена любая официальная запись (за исключением черновиков и заметок). Вместе с тем существует ряд исключений, когда данное право ограничивается. Среди них закон выделяет:

– защиту особых общественных интересов (международные отношения, военные интересы государства, его безопасность, внешний финансовый контроль и вопросы внешней торговли, служебная или профессиональная тайна и т.п.),

– защиту процесса принятия административного решения: информация может быть предоставлена по окончании соответствующей процедуры,

– защиту персональных данных: информация предоставляется с согласия собственника данных либо в специально установленных случаях,

– защиту интеллектуальной собственности и коммерческой тайны: информация предоставляется с согласия собственника информации.

В области обработки данных и информационных систем наряду с федеральными законами действуют законы земель. На практике земельные законы в большей части дублируют положения федерального законодательства. Следует отметить законы «о прозрачности» земель

---

[357] Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen. https://www.gesetze-im-internet.de/iwg/ (дата обращения: 10.08.2019)

[358] Gesetz zur Regelung des Zugangs zu Informationen des Bundes. http://www.gesetze-im-internet.de/ifg/ (дата обращения 11.08.2019).

Гамбурга и Рейнланд-Пфальца, устанавливающие более свободный доступ к официальной информации по сравнению с федеральным законом. Также особое место в земельном законодательстве занимает Закон еще одной земли – Бранденбурга «О доступе к файлам и информации» от 10.03.1998 (AIG)[359]. Его особенность в том, что он, помимо данных, указанных в федеральном законе, разрешает доступ к базам, содержащим личные данные или данные компаний, если такие субъекты дали согласие на доступ к их данным. Законом прямо установлено, что он ограничивает право на личную жизнь, установленное Конституцией земли.

Для обеспечения свободного доступа к официальной информации в Германии реализуется Национальная стратегия электронного правительства (NEGS)[360], принятая в обновленном виде в октябре 2015 г. Данная стратегия создает основу деятельности электронного правительства. Этому также способствовало включение в Основной закон Германии положений об электронном взаимодействии и сотрудничестве федерального правительства и органов власти земель.

Положения об электронном правительстве получили развитие также в ряде федеральных законов, включая Закон о продвижении электронного правительства (EGovG) от 25.08.2013[361], Закон об улучшении онлайн-доступа к административным услугам (OZD) от 14.08.2017, а также в соответствующих законах земель.

---

[359] Akteneinsichts- und Informationszugangsgesetz. http://bravors.brandenburg.de/gesetze/aig (дата обращения 14.08.2019).

[360] Nationale E-Government-Strategie. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/NEGS/NEGS_Fortschreibung.html?nn=6839038 (дата обращения 13.08.2019).

[361] Gesetz zur Förderung der elektronischen Verwaltung. http://www.gesetze-im-internet.de/egovg/ (дата обращения 14.08.2019).

Держатели официальной информации обязаны обеспечивать доступ граждан, организаций и иных лиц к такой информации. К таким держателям информации относятся государственные органы различного уровня, организации, как государственные, так и частные некоммерческие с государственной долей участия в них, различные ассоциации.

Доступ к публичной информации может быть открыт посредством организации порталов открытых данных либо по запросу. Ответ на запрос дается по общему правилу в течение 30 дней, если отсутствуют основания для отказа. Данные должны предоставляться в машиночитаемой форме и снабжаться метаданными (например, когда они собраны или кто предоставляет данные). Метаданные размещаются на национальном портале метаданных GovData[362], так что их может найти любой желающий.

Также на держателей официальной информации возложена обязанность вести ее учет, формировать ее каталоги, публиковать обязательную для раскрытия информацию и пр.

Контроль за соблюдением законодательства о свободе информации возложен на Федерального комиссара по защите данных.

Правовое регулирование персональных данных в Германии подчинено требованиям GDPR[363]. Национальное законодательство, в частности федеральный закон о защите персональных данных (BDSG)[364], а также законы земель во многом повторяют положения GDPR. При этом национальное законодательство отступает от положений GDPR по вопросам, связанным с обработкой данных в сфере занятости, в исследовательских,

---

[362] Das Datenportal für Deutschland. https://www.govdata.de/ (дата обращения: 15.08.2019).

[363] Regulation (EU) 2016/679 (General Data Protection Regulation). https://gdpr.eu/tag/gdpr/ (дата обращения 13.08.2019).

[364] Bundesdatenschutzgesetz. https://www.gesetze-im-internet.de/bdsg_2018/index.html (дата обращения 17.08.2019).

архивных, статистических целях, по ограничениям прав субъектов данных, профилированию, общественному видеонаблюдению и некоторых других. Вместе с тем отдельные отступления BDSG подверглись критике надзорных органов, некоторые из которых прямо рекомендуют, чтобы контролеры не полагались на ограничения прав субъекта данных в соответствии с разделом 32 BDSG. Также отступление в отношении видеонаблюдения в разделе 4 BDSG недавно признано недействительным Федеральным административным судом в том, что касается работы видеонаблюдения частными лицами.

Регулированию обработки персональных данных также посвящены отдельные разделы специальных законов. В частности, Закон о Телемедиа (TMG) от 26.02.2007[365] устанавливает требования к обработке персональных данных, относящихся к электронным информационным и коммуникационным услугам, выполняемым поставщиками телемедиа-услуг. Закон о телекоммуникациях (TKG) от 22.06.2004[366] регулирует оказание телекоммуникационных услуг связи, предъявляет требования к поставщикам телеком-услуг по технической, организационной защите средств связи при оказании услуг в части защиты телекоммуникационной тайны и персональных данных пользователей услугами. В Законе предусмотрены случаи и порядок обмена информацией между операторами связи и государственными органами. В частности, предусмотрена обязанность предоставлять информацию по запросам федеральных министерств, агентств и служб отдельные категории информации для модернизации сетевой инфраструктуры. Также в TKG определена процедура контроля за защитой

[365] Telemediengesetz. https://www.gesetze-im-internet.de/tmg/index.html (дата обращения 14.08.2019).

[366] Telekommunikationsgesetz. https://www.gesetze-im-internet.de/tkg_2004/index.html (дата обращения 10.08.2019).

данных и свободой информации, уведомления Федерального сетевого агентства и Федерального комиссара по защите данных и свободе информации о нарушениях защиты персональных данных и возможных негативных последствиях такого нарушения.

Также регулирование обработки персональных данных осуществляется на уровне земель. В каждой земле есть местный закон о защите персональных данных, который в основном воспроизводит положения Федерального закона о защите персональных данных (BDSG) и GDPR.

2.1.3 Правовой режим данных во Франции

Общее правовое регулирование данных и государственных информационных систем не унифицировано. Законодательство Франции не устанавливает общих норм о правовых режимах информации в целом, не определяет общего круга субъектов информационных правоотношений. Регулируются отдельные категории данных: данных публичного сектора, открытых данных, персональных данных, некоторых отраслевых данных (например, данных о налоговой задолженности).

Информация публичного сектора, вопросы ее последующего использования, предоставления и распространения регулируются Книгой III Кодекса отношений между обществом и администрацией[367]. Французское право гармонично вписало наднациональные нормы европейского права в действующий и более широкий нормативный акт.

Положения Кодекса устанавливают ограничения права на запрос информации. Не могут быть затребованы незавершенные документы, а также подготовительные материалы. Государственный орган имеет также право не предоставлять информацию в случаях злоупотребления правом на запрос

---

[367] Code des relations entre le public et l'administration. https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000031366350(дата обращения: 11. 08. 2019)

информации (например, одновременной или систематической подачи одинаковых запросов). Доступ к административным документам реализуется одним из следующих способов:

– непосредственным ознакомлением с документом,

– отправлением и изготовлением копии документа, без нанесения ему вреда, с возложением издержек на запрашивающего по принципу предельной цены,

– по электронной почте и без сбора, если документ доступен вэ электронной форме,

– путем публикации в Интернете.

Молчание компетентного органа в течение месяца с момента получения запроса приравнивается к отказу в информации. Любой отказ должен быть мотивирован в письменной форме с указанием способов обжалования. У лица есть два месяца с момента отказа для обжалования.

Кодекс вводит специальную категорию информации: данные для сообщения (les données de référence). Их публикация является государственной обязанностью. Данные для сообщения должны соответствовать следующим критериям: они представляют собой общее упоминание для идентификации или обозначения лиц, продуктов, услуг, территорий; они часто используются лицами частного и публичного права, отличными от органа, в распоряжении которого находятся такие данные; их последующее использование требует поддержания высокого качества их предоставления. Список данных для сообщения установлен декретом Государственного совета[368].

---

[368] Décret n° 2017-331 du 14 mars 2017 relatif au service public de mise à disposition des données de référence. https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=C49A75316B5545B2041F83902D900816.tplgfr34s_2?cidTexte=JORFTEXT000034194946&idArticle=LEGIARTI000034195955&dateTexte=20170316 (дата обращения 16 05 2019)

Ст. L322-1 формулирует принцип последующего использования информации: если иное не разрешено администрацией, последующее использование публичной информации осуществляется при условии, что такая информация не изменяется, ее смысл не искажается и указаны дата и источник последнего опубликования. Информация может предоставляться на условиях лицензии, при этом платное предоставление информации в любом случае требует лицензии. Примечательно, что во Франции также в 2017 г. рассматривалось дело, связанное со злоупотреблением правом *sui generis* на базы данных для отказа в запрашиваемой информации. Решение Государственного совета от 8.02.2017 по делу общества «NotreFamille.com»[369] гласит, что установление органом ограничений на извлечение публичной информации из баз данных в распоряжении органа на основе отсылки к исключительному праву на базу данных неосновательно и не может быть принято во внимание. Общество запрашивало информацию об актах гражданского состояния с целью ее цифровизации и организации представления в публичном доступе в Интернете, тогда как правила последующего использования запрашиваемых документов предполагали только возможность ознакомления либо в зале для чтения, либо на официальном сайте органа в Интернете.

Каждое министерство назначает лицо, ответственное за доступ к административным документам, а также формирует Комиссию доступа к административным документам как самостоятельный орган. Комиссия формируется из одиннадцати лиц, представляющих разные интересы и

[369] Conseil d'État. 10ème - 9ème chambres réunies. N° 389806. ECLI:FR:CECHR:2017:389806.20170208. lecture du mercredi 8 février 2017. https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000034017890&fastReqId=453311552&fastPos=1 (дата обращения 12.05.2019)

органы, в том числе включая профессора какого-либо из университетов. Состав Комиссии обновляется наполовину раз в три года.

Правовое регулирование персональных данных во Франции установлено в Законе о технологиях и свободах n° 78-17 от 6.01.1978[370]. Под влиянием наднационального права, однако, Закон по большей части имплементирует положения европейских актов либо повторяет их. С вступлением в силу Регламента ЕС о защите персональных данных вопрос их правового регулирования в национальном праве исчерпан. Одновременно Закон содержит положение, позволяющее лицу распоряжаться доступом к данным после его смерти. В 2016 г. Законом о цифровой республике[371] внесен ряд изменений в Закон об информационных технологиях и свободах, в числе которых вводилась ст. 40-1[372], регулирующая порядок распоряжения данными лица после его смерти. Согласно введенной статье, лицо может оставить соответствующие распоряжения, которые делятся на общие (générales), устанавливающие волю лица об использовании всей совокупности данных о нем, и специальные (particulières), устанавливающие волю лица по поводу распоряжения персональными данными.

Следует отметить, что нормы об общих распоряжениях не получили реализации. Согласно Закону, общие распоряжения могут быть зарегистрированы у доверенного лица, сертифицированного Национальной

---

[370] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 (дата обращения 17. 05. 2018)

[371] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique. обращенияhttps://www.legifrance.gouv.fr/affichTexte.do;jsessionid=C91E77329E1254E85267CFE55D12556E.tplgfr32s_2?cidTexte=JORFTEXT000033202746&dateTexte=20180111(дата обращения 17.05.2018)

[372] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000000886460&idArticle=LEGIARTI000033219717&dateTexte=20180111&categorieLien=id (дата обращения 27.05.2018)

комиссией информационных технологий и свобод (la Commission nationale de l'informatique et des libertés - CNIL), а также вносятся в реестр. Правила ведения реестра должны быть определены декретом Государственного Совета с учетом мотивированного и опубликованного мнения CNIL. Ни один из подзаконных актов до сих пор не был издан уполномоченными субъектами. При отсутствии официальных комментариев по этому вопросу нормы об общих распоряжениях тем не менее не устраняются французским законодателем и, видимо, будут реализованы позднее.

Специальные распоряжения регистрируются у соответствующего оператора информационной системы. Например, можно распорядиться своим аккаунтом посредством специальных механизмов в социальной сети. Если распоряжений пользователем оставлено не было, наследники имеют право на доступ к информации, непосредственно связанной с доступом к наследуемому имуществу, а также обратиться с требованием об удалении аккаунта из общего доступа. При этом все издержки в любом случае несет владелец социальной сети.

Во французском праве также содержатся специальные положения отраслевого регулирования о порядке предоставления информации. Например, статья L104 книги налоговых процедур Франции устанавливает, что должностное лицо налогового органа по общему правилу предоставляет информацию о налоговой задолженности запрашивающего лица. В отношении третьих лиц информация не предоставляется, за исключением случаев, когда информация касается местных налогов или иных определенных видов налога и в предоставляемых данных фигурирует запрашивающее лицо, даже если запрос касается иного лица[373].

---

[373] Livre des procédures fiscales. https://www.legifrance.gouv.fr/affichCode.do;jsessionid=61AAA2448C37FCCDA85036CA22A

### 2.1.4 Правовой режим данных в Эстонии

Правовыми актами Эстонии, закрепляющими основы правового режима данных и правовой статус участников оборота данных, являются Акт о публичной информации[374], Акт о защите персональных данных[375], Акт о государственной тайне и засекреченной информации иностранных государств[376], а также ряд иных документов.

Акт о публичной информации регулирует отношения, связанные с доступом к информации о деятельности публичных органов и организаций, выполняющих публично значимые функции. В содержание данного Акта заложены положения Директив ЕС о доступе к информации публичного сектора (Директивы 2003 года[377], Директивы 2013 года[378], в настоящий момент ведется имплементация положений Директивы 2019 года об открытых данных[379]). Под публичной информацией понимается «информация, которая записывается и документируется любым способом и на любом носителе, и которая получена или создана при исполнении

---

3F194.tplgfr44s_2?cidTexte=LEGITEXT000006069583&dateTexte=20191104 (дата обращения 04.11.2019).

[374]Public Information Act. https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения: 14.08.2019).

[375]Personal Data Protection Act. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide (дата обращения: 14.08.2019).

[376]State Secrets and Classified Information of Foreign States Act. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042019009/consolide (дата обращения: 14.08.2019).

[377] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32003L0098 (дата обращения: 14.08.2019).

[378] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information. https://eur-lex.europa.eu/eli/dir/2013/37/oj (дата обращения: 14.08.2019).

[379] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024 (дата обращения: 14.08.2019).

публичных обязанностей, предусмотренных законом или изданным на его основе правовых актах» (§ 3).

К субъектам, обязанным обеспечивать доступ к публичной информации (т.н. держателям информации – data holders), относятся органы государственной власти, юридические лица публичного права, а также юридические лица частного права или физические лица, если они исполняют публичные обязанности в соответствии с законом, административным актом или соглашением, в том числе оказывают образовательные, медицинские, социальные и иные публичные услуги. Помимо перечисленных лиц, в круг обязанных субъектов входят: предприятия, занимающие доминирующее положение на рынке, имеющие специальное или эксклюзивное право, являющиеся естественными монополиями – в отношении информации о предложении товара/услуг и ценообразовании; индивидуальные предприниматели, некоммерческие ассоциации, фонды и компании – в отношении информации о расходовании средств, полученных из государственного или муниципального бюджета для исполнения публичных обязанностей или в качестве финансовой помощи (§ 5).

Обеспечение доступа к публичной информации основывается на следующих принципах:

– обязанность предоставления публичной информации имеет целью обеспечение демократии и публичных интересов, реализацию каждым прав и свобод,

– доступ должен быть обеспечен каждому лицу в максимально возможные короткие сроки и наиболее удобным лицу способом,

– при обеспечении доступа к информации не допускается нарушение права на частную жизнь и авторских прав,

– доступ к информации бесплатен, кроме случаев, когда закон позволяет покрывать прямые издержки на предоставление информации (в этих случаях держатель информации обязан опубликовать условия, на которых предоставляется информация за плату, с объяснением

ценообразования; такие условия должны быть равными для всех и не должны нарушать конкуренцию),

– любое лицо может оспорить ограничение доступа к информации, если такое ограничение нарушает его права или свободы.

Доступ к публичной информации обеспечивается двумя способами: посредством ответа на запрос и посредством раскрытия информации.

Ответ должен быть дан в пятидневный срок (при наличии оснований – в 15-дневный срок с предварительным уведомлением о продлении срока) в письменной форме (в исключительных случаях – в устной). В законе закреплен исчерпывающий перечень оснований отказа в доступе к информации по запросу (см. § 23).

В Законе закреплен обширный перечень информации, которую обязаны раскрывать ее держатели (см. § 28). Информация размещается на веб-сайте, а также в иных публично доступных источниках. Закон обязывает высшие органы власти, суды, правительственные органы, юридические лица публичного права, муниципальные органы вести веб-сайты. В отдельном нормативном акте (Требованиях к доступности вебсайтов и мобильных приложений и правилах опубликования информации о доступе[380]) содержатся требования к размещению информации на веб-сайте.

Закон учреждает информационный портал Эстонии (Estonian information gateway) – веб-сайт, предоставляющий доступ к публичной информации и публичным электронным услугам.

Для обеспечения доступа к информации закон предписывает соблюдение держателями информации организационных требований: вести

---

[380] Requirements for the accessibility of websites and mobile applications, and the rules for publishing information describing accessibility. https://www.riigiteataja.ee/en/eli/ee/EVIM/reg/512042019003/consolide (дата обращения: 14.08.2019).

учет документов, в том числе создать их реестр (это относится к органам публичной власти и юридическим лицам публичного права); обеспечивать доступ к информации на регулярной основе; содействовать в направлении запроса о доступе к информации; соблюдать требования к ограничению доступа к информации; и др.

Акт о публичной информации выделяет категорию информации ограниченного доступа (restricted information). Руководитель публичного органа может ограничить доступ к информации и классифицировать ее как информацию для внутреннего использования (information intended for internal use) в соответствии с установленными основаниями (см. § 35).

Другой правовой акт, закрепляющий правовой режим данных – Акт о защите персональных данных Эстонии регулирует отношения по обработке и защите персональных данных. Помимо данного акта, прямым действием в данной сфере обладает Регламент ЕС о защите данных 2016 года (GDPR)[381].

Под персональными данными понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъекту персональных данных»); идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано, прямо или косвенно, в частности посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, сетевой идентификатор или на один или несколько факторов, характерных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности этого физического лица.

---

[381] 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). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1564943268451&uri=CELEX:32016R0679 (дата обращения: 14.08.2019).

Основанием обработки персональных данных является либо информированное согласие лица, либо основание, предусмотренное законом (в большинстве эти основания направлены на защиту публичных интересов, интересов третьих лиц или интересов самого субъекта персональных данных).

В отношениях по обработке персональных данных выделяется два основных субъекта – оператор (controller) и обработчик (processor). Оператор – физическое или юридическое лицо, публичный орган или иное лицо, которое определяет цели и средства обработки персональных данных. Обработчиком является лицо, которое обрабатывает персональные данные от имени оператора.

Под государственной тайной в соответствии с Актом о государственной тайне и засекреченной информации иностранных государств[382] 2007 года понимается информация, предусмотренная исключительно данным Актом или изданным в соответствии с ним актом, которая требует защиты от разглашения в интересах национальной безопасности или внешних сношений Эстонской Республики, за исключением секретной информации иностранных государств. Выделяется «секретная информация иностранных государств» - информация, полученная от иностранного государства, Европейского союза, НАТО, организации или учреждения, учрежденного в соответствии с международным соглашением, которая передается Эстонии на основании международных соглашений и которая была засекречена ее составителем, а также информация, созданная в целях выполнения Эстонской Республикой международного соглашения, подлежащего засекречиванию.

---

[382] State Secrets and Classified Information of Foreign States Act. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042019009/consolide (дата обращения: 14.08.2019).

Актом предусмотрена процедура отнесения информации к государственной тайне, срок действия режима государственной тайны, требования к защите государственной тайны, порядок доступа к ней, порядок передачи носителей с государственной тайной и другие вопросы.

2.1.5 Правовой режим данных в Великобритании

Законодательство Великобритании не выделяет ни общего режима информации, ни общих субъектов информационных правовых отношений. Одновременно устанавливается правовое регулирование отдельных категорий данных, отдельных информационных правоотношений.

Правительство Великобритании разработало эффективную политику, направленную на раскрытие данных публичными органами[383]. Она строится на следующих принципах: информация представляет собой ценный актив, информация должна использоваться и защищаться соразмерно ее ценности, информация должна иметь качество, достаточное для цели ее использования,информация может использоваться повторно,информация, находящаяся в ведении государственных органов, должна быть опубликована, за исключением ряда случаев, граждане и бизнес должны иметь право доступа к информации о себе 384.

Основу правового регулирования исследуемого вопроса составляют Акт о свободе информации[385] (место указанного акта в системе НПА, как и других указанных ниже актов определено в соответствующем разделе настоящего исследования). Акт устанавливает право на доступ к информации, находящейся в распоряжении публичных органов.

---

[383] https://www.gov.uk/government/publications/open-data-white-paper-unleashing-the-potential (дата обращения: 05. 08. 2019)

[384] Information Principles 2011. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266284/Information_Principles_UK_Public_Sector_final.pdf (дата обращения: 05.08.2019).

[385] Freedom of Information Act 2000. http://www.legislation.gov.uk/ukpga/2000/36/contents (дата обращения: 05.08.2019).

Право на доступ к информации включает:

– право быть информированным о наличии у органа публичной власти соответствующей информации,

– право на получение указанной информации по запросу лица.

Актом (раздел 19) установлена общая обязанность публикации информации о деятельности органов публичной власти в соответствии с утверждаемыми ими схемами публикации. Целью схемы публикации является предоставление доступа к информации, которую власти обычно раскрывают без запроса[386].

Мониторинг опубликования таких схем осуществляет Офис уполномоченного по информации (ICO)[387], контролирующего соблюдение информационных прав граждан, законодательство в сфере персональных данных.

Акт содержит ограничение по предоставлению следующих категорий информации:

– информация, которая будет опубликована в дальнейшем,

– информация для целей национальной безопасности,

– информация по вопросам международных отношений,

– информация об отношениях между государственными органами Соединенного Королевства,

– информация о расследованиях,

– персональные данные,

– информация, составляющая коммерческую тайну.

---

[386] Liddle C., McMenemy D. A Scottish freedom of information regime for a denationalised environment: rhetorical or authentically practical? Information & Communications Technology Law, 2015, no 3, p. 234.

[387] См. например: The Central Government sector monitoring report, 2009. https://ico.org.uk/media/action-weve-taken/monitoring/2795/central-government-sector-monitoring-report.pdf (дата обращения: 05.08.2019).

Указанный перечень является закрытым.

Правительственная Цифровая служба (GDS), являющаяся частью секретариата Кабинета, отвечает за координацию деятельности в области открытых данных, в частности путем поддержания портала GOV.UK – информационной системы, на которой сосредоточен основной массив открытых данных, владельцем которых являются органы публичной власти Великобритании[388]. Место данного органа в системе органов исполнительной власти и ее полномочия раскрыты в соответствующем разделе настоящего исследования.

Основным источником права в области защиты государственной тайны является Акт о государственной тайне (Official Secrets Act 1989)[389]. Защиту государственной тайны Великобритании также регулируют иные акты[390].

Перечень информации, относимой к государственной тайне, отсутствует[391]. В качестве ориентира могут выступать сферы:

– безопасности и разведывательной деятельности,

– обороны,

– международных отношений,

– расследования преступлений.

За разглашение сведений, составляющих государственную тайну, предусмотрена уголовная ответственность до двух лет лишения свободы и штраф.

---

[388] Safarov I. Institutional Dimensions of Open Government Data Implementation: Evidence from the Netherlands, Sweden, and the UK. Public Performance & Management Review, 2016, no 2, pp. 305-328.

[389] Official Secrets Act 1989. http://www.legislation.gov.uk/ukpga/1989/6/contents (дата обращения: 05.08.2019).

[390] Шамсутдинов Р.Р. Сравнительный анализ правовой защиты государственной тайны в Российской Федерации и в Великобритании // Символ науки. 2016. № 3. С. 134.

[391] Журавленко Н.И. Организация защиты информации в развитых зарубежных странах. Уфа, 2014. С. 162.

Основным источником права в области защиты коммерческой тайны в Великобритании является Регламент о коммерческой тайне[392]. Данный акт, принятый с целью гармонизации положений национального права[393] с требованиями Директивы 2016/943[394], регулирует вопросы защиты интересов обладателя информации, составляющей коммерческую тайну.

Под коммерческой тайной в соответствии с разделом 2 указанного Акта понимается информация, которая:

– не является общеизвестной и не может быть легко получена третьим лицом,

– в силу неизвестности третьим лицам имеет потенциальную коммерческую ценность,

– сохраняется в тайне в результате действий обладателя такой информации.

В целом право Великобритании не содержит ограничений на виды информации, на которые может быть распространен режим коммерческой тайны[395]. Обладателю информации, составляющей коммерческую тайну, противостоит любое лицо, которое обязано не разглашать указанную информацию, если она получена незаконно или используется с нарушением доверия. При нарушении законодательства о коммерческой тайне обладатель информации имеет право обратиться в суд и взыскать убытки. Срок исковой

---

[392]Trade Secrets (Enforcement, etc.) Regulations 2018. http://www.legislation.gov.uk/uksi/2018/597/contents/made (дата обращения: 05.08.2019).

[393] Montagnon R. The Trade Secrets Directive – consistency of approach required, with or without Brexit. Journal of Intellectual Property Law & Practice. 2016, issue 9, pp. 643–644.

[394] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943 (дата обращения: 05.08.2019).

[395] Сорокина А.Э. Охрана коммерческой тайны по законодательству зарубежных стран (на примере Великобритании и Германии) // Вестник Московского университета МВД России. 2013. №.1. С. 62.

давности составляет 6 лет с момента прекращения нарушения или с момента, когда лицо узнало о нарушении и определило надлежащего ответчика по иску.

Основным источником в сфере защиты данных в Великобритании является Акт о защите данных[396], принятый в развитие положений GDPR[397]. Во многих случаях статут отсылает к положениям GDPR, лишь уточняя таковые.

Так, например, ст. 6 GDPR содержит, в качестве одного из оснований обработки персональных данных, общественный интерес. В качестве такового статут понимает:

– осуществление правосудия,
– выполнение функции любой из палат Парламента,
– выполнение возложенной на лицо обязанности,
– «деятельность, которая способствует демократическим процедурам».

Раздел 14 статута уточняет критерии значимости решения, принимаемого на основании исключительно автоматизированной обработки персональных данных по смыслу ст. 22 GDPR, а раздел 18 уточняет правила трансграничной передачи персональных данных. Нормы части 3 указанного статута (разделы 29–81) содержат положения об обработке компетентными органами в правоохранительной деятельности. Принципы обработки и права субъектов изложены аналогично GDPR.

---

[396] Data Protection Act 2018. http://www.legislation.gov.uk/ukpga/2018/12/contents (дата обращения: 05.08.2019).

[397] 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). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1565101770580&uri=CELEX:32016R0679 (дата обращения: 05.08.2019).

В целях поиска релевантных принципов обработки, прав субъектов персональных данных, обязанностей операторов необходимо обращаться к положениям GDPR, который имеет непосредственное действие (британское законодательство в области персональных данных регулирует вопросы, оставшиеся за рамками GDPR, и не должно ему противоречить).

Если говорить о коллизиях законодательства о персональных данных и законодательства о коммерческой тайне, то, по мнению ученых, нормы законодательства о персональных данных имеют приоритет. Например, если решение принимается на основании исключительно-автоматизированной обработки персональных данных, алгоритм которых защищен режимом коммерческой тайны, право субъекта на общую информацию об алгоритме принятия решения имеет приоритет[398].

Основу правового регулирования составляет Регламент об авторских правах и правах на базы данных[399], который принят, в частности, для имплементации положений Директивы 96/9/ЕС[400]. В рамках указанного регламента защищаются именно «нетворческие базы данных» (которые потребовали существенных инвестиций).

Под базой данныхзакон понимает собрание независимых произведений, данных и других самостоятельных материалов, которые представляют собой определенную систему, а также доступны с помощью электронных и других средств.

Права обладателя прав на базу данных защищены от действий любых третьих лиц по извлечению всего содержимого / существенной части или по

---

[398] Malgieri G. Trade Secrets v Personal Data: a possible solution for balancing rights, International Data Privacy Law, 2016, issue 2, p.107.

[399] Copyright and Rights in Databases Regulations 1997. http://www.legislation.gov.uk/uksi/1997/3032/contents/made (дата обращения: 05.08.2019).

[400] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009 (дата обращения: 10.08.2019)

систематическому копированию содержимого путем установления запрета на осуществления таких действий под угрозой применения гражданско-правовых санкций.

Если база данных создана работником, то ее создателем считается работодатель. Указанное правило распространяется и на государственных служащих.

В ряде случаев действуют положения, исключающие противоправность копирования в публичных целях, например, когда база данных публикуется в соответствии с возложенной на орган обязанностью.

В настоящей части также стоит упомянуть об открытых данных. Несмотря на отсутствие статута, прямо регулирующего указанные вопросы, ранее упоминаемые Акт о свободе информации (Freedom of Information Act 2000)[401] и Регламент о повторном использовании информации, находящейся в распоряжении публичных органов власти (Re-use of Public Sector Information Regulations 2015)[402], с учетом ограничений в области персональных данных и государственной тайны, создают основу функционирования сервиса «Find open data» на платформе GOV.UK, который позволяет искать тематические наборы данных по 12 отраслям[403].

Таким образом, в правовых актах Великобритании предусмотрены различные правовые режимы информации и статусы участников ее оборота (их права и обязанности), которые могут применяться одновременно в отношении одной и той же информации и одного и того же участника.

Законодательство Великобритании в отношении данных, находящихся в ведении органов публичной власти, использует термин «held by public

---

[401] Freedom of Information Act 2000. http://www.legislation.gov.uk/ukpga/2000/36/contents (дата обращения: 05.08.2019).

[402] The Re-use of Public Sector Information Regulations 2015. http://www.legislation.gov.uk/uksi/2015/1415/contents/made (дата обращения: 05.08.2019).

[403] Find Open Data. https://data.gov.uk (дата обращения: 05.08.2019).

authorities». Из указанного следует возможность осуществления именно полномочия владения в отношении информации в информационных системах. Распоряжение информацией в таких системах, ограничения и порядок реализации указанного правомочия предусмотрены вышеназванными актами в отношении соответствующих категорий информации.

2.1.6 Правовой режим данных в Австралии

Ввиду федеративного государственного устройства Австралии в ее праве сформировались специфические правовые режимы в отношении отдельных видов данных:

1) публичные данные

В 2015 году федеральное правительство опубликовало Заявление о политике публичных данных[404], в котором признало данные, которыми оно располагает, стратегическим национальным ресурсом. Публичные данные определены как все данные, собранные государственными органами для любых целей; не-чувствительные данные как обезличенные данные, при условии, что они не идентифицируют физическое лицо и не нарушают требования к защите неприкосновенности частной жизни или безопасности. В отношении этих данных было объявлено об их раскрытии и повторном использовании общедоступных данных.

Законодательство в данной сфере неравномерно развито на уровне штатов и территорий, поэтому далее анализируется регулирование в области оборота публичных данных на федеральном уровне, но рассматриваются и отдельные нормативно-правовые акты штатов, когда это целесообразно.

---

[404] Australian Government Public Data Policy. https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf (дата обращения: 16 10 2019)

В настоящее время в Австралии происходит реформа законодательства об обмене данными публичного сектора (Data Sharing and Release Reform). Новое законодательство будет предусматривать для государственных учреждений (хранителей данных; data custodians) альтернативное разрешение на обмен данными государственного сектора с аккредитованными организациями, такими как государственные учреждения, органы власти штатов и территорий и неправительственные организации, такие как университеты.

Предполагается, что новое законодательство будет иметь широкую сферу применения и применяться ко всем данным государственного сектора, собираемым или генерируемым образованиями Содружества. Законопроект будет разрабатываться с учетом режимов обмена данными в Новом Южном Уэльсе, Южной Австралии и Виктории, а также новых режимов в других штатах и территориях (и, возможно, с учетом возможности их оперативной совместимости).

Субъекты правоотношений, их правовой статус, а также механизмы управления данными, включая механизмы правоприменения и подотчетности будут определены при разработке регулирующего законодательства, в том числе требований и принципов (requirements and guidelines) поддержки деятельности государственных структур и образований по обмену данными.

2) личная информация (personal information)

Становление законодательства о личной информации происходило в Австралии под влиянием Руководящих принципов ОЭСР по защите конфиденциальности и трансграничных потоков персональных данных[405]. Отдельные положения Руководящих принципов нашли отражение в Законе о

[405] OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (дата обращения 20.10.2019)

неприкосновенности частной жизни 1988 г.[406], в частности принципы конфиденциальности. При этом в законодательстве не предусмотрено единого права на неприкосновенность частной жизни. Хотя Австралия подписала Международную конвенцию о гражданских и политических правах 1966 г.[407], право на неприкосновенность частной жизни, предусмотренное статьей 17 Конвенции, не имплементировано в национальное законодательство.

Неприкосновенность частной жизни регулируется федеральным законодательством и законодательством штатов и территорий, каждое из которых исходит из базовых принципов конфиденциальности. Хотя все соответствующие законы основаны на принципах ОЭСР, существуют значительные различия в их применении от юрисдикции к юрисдикции. В некоторых случаях (особенно в отношении данных в сфере здравоохранения) отмечается частичное совпадение положений федерального законодательства и законов отдельных штатов[408].

Также следует отметить, что Офис австралийского информационного комиссара (OAIC) полагает допустимым рекомендовать источники иностранного или международного права[409] в качестве информационных ресурсов отдельных вопросов (например, в рамках практического

---

[406] Kirby M. Privacy protection, a new beginning: OECD principles 20 years on. Privacy Law & Policy Reporter, 1999, no 3. http://www5.austlii.edu.au/au/journals/PrivLawPRpr/1999/41.html (дата обращения12.10.2019)

[407] International Covenant on Civil and Political Rights. https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (дата обращения 20.10.2019)

[408] Watts D., Casanovas P. Privacy and data protection in Australia: a critical overview (extended abstract). https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf (дата обращения 21.10.2019)

[409] Как правило, это акты США, Канады, Европейского союза, Великобритании.

руководства для разработчиков мобильных приложений[410]: Конфиденциальность на мобильных устройствах).

Высказываются предположения, что новое законодательство об обмене данными и их обнародовании изменит методы работы правительства Австралии с данными, включая персональную информацию. На сегодняшний день независимая оценка воздействия предлагаемой концепции обмена данными публичного сектора на неприкосновенность частной жизни, а также сильных и слабых сторон предлагаемой концепции, была проведена независимым консультантом по запросу Департамента Премьер-министра и Кабинета[411].

3) потребительские данные

В Австралии разрабатывается концепция Права на потребительские данные (Consumer Data Right, CDR), в рамках которого права потребителей на их данные будет являться их неотъемлемым правом[412]. В пункте 56AI Закона приведено нечеткое понятие данных CDR (CDR data). В понятие входит «информация, входящая в категорию информации, указанную в документе, обозначающем сектор, или информация, которая не охвачена, но впоследствии прямо или косвенно получена из этой информации, относящейся к определенному сектору». Более четкое определение CDR data будет содержаться в подлежащих разработке правилах, при этом возможно изменение объема производных данных в зависимости от сектора экономики.

---

[410] Mobile privacy: a better practice guide for mobile app developers. https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/#appendix-b-resources (дата обращения: 30.10.2019)

[411] Galexia Privacy Impact Assessment on the Proposed Data Sharing and Release (DS&R) Bill and Related Regulatory Framework. https://www.datacommissioner.gov.au/sites/default/files/2019-09/PIA_Proposed%20DS%26R%20Framework_2019June.pdf (дата обращения: 30.10.2019).

[412] Productivity Commission. (2017). Data availability and use (Report No. 82). Canberra: Productivity Commission: https://www.pc.gov.au/inquiries/completed/data-access/report (дата обращения: 31. 10. 2019)

Правовой режим этой категории данных будет распространен на данные, генерируемые потребителями при использовании определенных технологий, а также связанных с ними продуктов и услуг, поставляемых частным сектором.

Следует отметить особенности правового регулирования в отношении оборота данных в Австралии:

1) публичные данные

Основным документом, определяющим правовой режим открытых данных публичного сектора, является Заявление федерального правительства о политике публичных данных. Из ключевых положений Заявления следует отметить следующие:

– неконфиденциальные данные должны быть открытыми по умолчанию, сохраняться и часто обновляться,

– неконфиденциальные данные исследований, финансируемых государством, по возможности должны быть открыты для использования и повторного использования,

– государственные органы должны взимать плату только за специализированные услуги передачи данных и по возможности публиковать полученные ими данные как по умолчанию открытые,

- данные должны быть доступными с помощью бесплатных и простых в использовании интерфейсов прикладного программирования (API),

– все новые системы должны обеспечивать интероперабельность, доступность данных и информации, а также экономичный доступ к данным,

– обмен данными между государственными органами должен быть безопасным и обеспечивающим конфиденциальность в интересах индивидуальной и национальной безопасности, коммерческой тайны,

– федеральные государственные органы должны открыто взаимодействовать с органами штатов и территорий в целях обмена данными и их интеграции в вопросах, имеющих важное значение для каждой юрисдикции, равно как на федеральном уровне.

В Заявлении указано, что минимумом обязанностей государственных органов является:

– опубликование надлежащим образом анонимизированных государственных данных на сайте data.gov.au,

– опубликование данных в машиночитаемом, пространственно-территориальном формате с высококачественным, простым в использовании и свободно доступным API; с описательными метаданными и с использованием согласованных открытых стандартов,

– обновление данных в автоматическом режиме,

– по общему правилу, опубликование данных по лицензии Creative Commons by Attribution.

Доступ к публичным данным может быть открыт через data.gov.au или непосредственно через государственный орган, хранящий данные. Отказ в доступе к публичным данным может быть обжалован пользователем путем публичного запроса, доступного на сайте data.gov.au.

2) личная информация

В Конституции Австралии отсутствует норма, прямо закрепляющая право на неприкосновенность частной жизни[413]. Закон о неприкосновенности частной жизни[414] регулирует правовой режим личной информации (информации о здоровье, этнической принадлежности, сексуальной ориентации, членстве в профсоюзе). Закон распространяется на публичный сектор и национальный частный сектор. На основании положений Закона о неприкосновенности частной жизни сформированы 13 принципов неприкосновенности частной жизни (APP), которые являются краеугольным

[413] Богдановская И.Ю. Источники права на современном этапе развития «общего права». Диссертация доктора юридических наук. М., 2007. С. 77.

[414] Privacy Act 1988. https://www.legislation.gov.au/Details/C2014C00076 (дата обращения: 20.10.2019)

камнем защиты неприкосновенности частной жизни. Они определяются как «законодательство, основанное на принципах», что делает их гибкими и адаптивными при применении к различным категориям субъектов. Принципы технологически нейтральны, что позволяет адаптировать их к меняющимся технологиям и методам обработки личной информации.

Закон вводит ключевые понятия. «Личная информация» означает информацию или мнение об идентифицированном лице или о лице, которое может быть идентифицировано: (a) вне зависимости от того, является ли эта информация или мнение правдивой; и (b) независимо от того, фиксирована ли эта информация или мнение в материальной форме.

Также введено понятие идентифицирующей информации, к которой, среди прочего, относятся полное имя лица, его псевдоним или предыдущее имя; дата рождения и пол; наименование нынешнего или последнего известного работодателя данного лица и иные сведения.

Закон определяет понятие «идентификатора» как разновидности идентифицирующей информации, и «государственного идентификатора». Последнее понятие характеризуется тем, что включает идентификаторы, которые присвоены государственными органами, указанными в Законе.

Нарушение принципов неприкосновенности частной жизни является «вмешательством в личную жизнь». что приводит к регулятивным действиям и штрафам, которые применяются к некоторым организациям частного сектора, а также к большинству правительственных органов[415]. Кроме того,

[415] Существует целый ряд разнообразных структур управления, которые могут быть созданы на основе Закона о государственном управлении, результатах деятельности и подотчетности (Public Governance, Performance and Accountability Act). https://www.legislation.gov.au/Series/C2013A00123 (дата обращения: 30.10.2019); специального законодательства или административных процедур. При этом Министерство финансов на своем сайте поясняет, что практика присвоения названий с течением времени привела к различиям в названиях органов (например, комиссия могла в равной степени обозначать одно лицо, группу лиц, образование Содружества (Commonwealth entity),

Закон регулирует конфиденциальность системы отчетности по потребительским кредитам, номерам налоговых документов, а также медицинских обследований.

В соответствии с Законом уполномоченное лицо – Австралийский информационный комиссар – вправе проводить расследования соблюдения Закона и добиваться применения мер гражданско-правовой ответственности за серьезные или повторные нарушения принципов, если организация не приняла меры к исправлению положения. Закон не предусматривает судебной защиты принципов конфиденциальности, но закрепляет право подать жалобу, сначала в соответствующую организацию или, если нет удовлетворительного ответа, Комиссару.

Другие акты федерального законодательства также регулируют обработку частной информации, в том числе находящейся в распоряжении государства. Среди основных актов: Закон о переписи и статистике 1905 г., Закон о свободе информации 1982 г., отдельные нормативно-правовые акты приняты в области медицинских записей и идентифицирующей налоговой информации.

В соответствии с исследованием, проведенным по запросу правительства Австралии Комиссией продуктивности[416], в более чем 175 законодательных актах Австралии закреплено свыше 500 положений о

---

исследовательский или консультативный орган). Статус органа определяется не его наименованием, а лежащей в его основе структурой управления. См. также: Types of governance structures. https://www.finance.gov.au/resource-management/governance/policy/structure-types/#f1. (дата обращения: 31.10.2019)

Поскольку в задачи данной работы не входит исследование системы управления на федеральном уровне и уровне штатов, для обозначения различных структур (комиссий, агентств, организаций) управления будет использоваться термин «структура» или «агентство» кроме случаев, когда речь идет о функциях или полномочиях образования.

[416] Productivity Commission. Data Availability and Use, Report No 82. Canberra, 2017. https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf (дата обращения: 25.10.2019)

защите неприкосновенности частной жизни и конфиденциальности данных. Подавляющее их большинство запрещает обмен данными, за исключением оговоренных законодателем ситуаций.

3) право на потребительские данные (CDR Data)

1.08.2019 Парламент Австралии одобрил законопроект, предусматривающий предоставление потребителям и малым предприятиям новых прав в отношении их данных[417]. Закон вводит понятие права «на потребительские данные» (Consumer Data Right, CDR) и «открытого банкинга» (open banking), а также вносит изменения в ряд законов[418]. Права потребителей на потребительские данных - это право потребителей указать своему поставщику (например, банку) передать другим поставщикам информацию о потребителе. CDR Data включает следующие категории: (i) Данные о продукте (Product Data) - данные CDR, которые не относятся к потребителям, а являются общей информацией о продукте поставщика (условия поставки или наличие продукта), и (ii) Потребительские данные (Consumer Data) - данные, которые являются специфическими для потребителя (например, содержат его имя и контактные данные, реквизиты счета и детали сделки).

Закон по сути представляет собой основанную на принципах правовую основу, поскольку он предусматривает разработку и принятие дополнительных документов. Большая часть регулирования (регулятивное бремя и обязательства, устанавливаемые в рамках CDR) должна быть разработана Комиссией конкуренции и защиты прав потребителей (Australian Competition & Consumer Commission, ACCC) и другими субъектами.

---

[417] Treasury Laws Amendment (Consumer Data Right) Act 2019. https://www.legislation.gov.au/Details/C2019A00063 (дата обращения: 25.10.2019)

[418] Изменения вносятся в Competition and Consumer Act 2010 (CC Act), Privacy Act 1988, Australian Information Commissioner Act 2010 (AIC Act).

Кроме того, реализация концепции CDR требует создания общих технических стандартов, облегчающих и повышающих безопасность доступа потребителей к данным о них, хранящимся в коммерческих предприятиях, и, по их выбору, обмена этими данными через интерфейсы прикладного программирования (API) с доверенными, аккредитованными третьими сторонами. Пока такие технические стандарты для поддержки обмена данными с учетом интересов потребителей находятся в стадии разработки[419].

В отношении основ правового статуса обладателя (собственника или владельца) данных и иных участников их оборота отметим следующее:

1) личная информация:

– физические лица: Закон о неприкосновенности частной жизни предоставляет физическим лицам инструменты контроля над обработкой их личной информации. Среди прочего Закон позволяет делать запросы в отношении субъектов, обрабатывающих информацию, требовать прекращения прямого маркетинга, направлять жалобы на оператора, неправильно использовавшего личную информацию;

– субъекты, на которых распространяется Закон о неприкосновенности частной жизни: органы исполнительной власти и организации с годовым оборотом более 3 млн. долл., ряд других организаций, обрабатывающих личную информацию. Закон не распространяется на операторов малого бизнеса (если они не собирают и не обрабатывают информацию о здоровье), что исключает из сферы его действия до 85% предприятий частного сектора[420];

---

[419] CDR design complete documentation (August 2019). https://treasury.gov.au/consumer-data-right (дата обращения: 31.10.2019).

[420] Watts D., Casanovas P. Privacy and Data Protection in Australia: a Critical overview. https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf (дата обращения: 26.10.2019)

2) публичные данные: Упомянутое выше Заявление о политике публичных данных возлагает на государственные органы обязанности обеспечивать доступ к данным публичного сектора неограниченному кругу лиц при соблюдении условий, связанных с де-идентификацией данных.

Перечень лиц, являющихся государственными органами, определяется в соответствии с Законом о государственном управлении, эффективности и подотчетности 2013 г[421]. Перечень таких органов приведен на сайте Министерства финансов[422].

3) право на потребительские данные: Закон о праве на потребительские данные определяет трех ключевых участников системы CDR: держателей данных (data holders), потребителей CDR (CDR consumers) и аккредитованных получателей данных (accredited data recipients).

Держателями данных являются первоначальные держатели данных, на которые распространяется право передачи, например, в банковском секторе это – банки и кредитные союзы.

Потребителями данных CDR могут быть как физические лица, так и юридические лица, у которых есть доступ к данным, хранящимся у держателя данных, и право на распоряжение о совместном использовании этих данных с аккредитованным лицом.

Аккредитованным получателем данных для целей CDR является лицо или организация, аккредитованные и получившие данные CDR в результате их раскрытия в соответствии с правилами, регулирующими CDR.

В отношении правовых основ обеспечения доступа к данным, их предоставления и распространения следует отметить следующее:

---

[421] Public Governance, Performance and Accountability Act 2013 (PGPA Act). https://www.legislation.gov.au/Series/C2013A00123 (дата обращения 02 09 2019)

[422] Flipchart and List of Commonwealth entities and companies. URL: https://www.finance.gov.au/resource-management/governance/#flipchart (дата обращения 16 09 2019)

1) личная информация: Закон о неприкосновенности частной жизни предусматривает право физического лица на доступ и корректировку своих персональных данных (Принцип 12). Организация, на которую распространяется действие указанного Закона, обязана предоставить запрашивающему лицу доступ к его личной информации. Срок ответа на запрос составляет 30 дней.

Закон (Принцип 6) определяет пределы, в которых организация, на которую распространяется действие указанного закона, может использовать или раскрывать личную информацию.

Организация, владеющая личной информацией лица, может использовать или раскрывать личную информацию только в целях, для которых она была собрана (т. н. первичная цель), или для вторичной цели, если применимы исключения, установленные данным Законом. Исключения составляют случаи, когда:

– лицо дало согласие на вторичное использование или раскрытие информации,

– лицо обоснованно ожидало бы, что организация, участвующая в программе APP, будет использовать или раскрывать свою личную информацию для вторичных целей, и эта цель связана с основной целью сбора или, в случае чувствительной информации, непосредственно связанной с основной целью,

– вторичное использование или раскрытие требуется или разрешено федеральным законодательством или приказом суда или в соответствии с ним.

2) публичные данные: Доступ к ним осуществляется на основании Заявления о политике публичных данных, которое обязывает государственные органы предоставлять данные через специализированный

сайт data.gov.au или напрямую по обращению субъектов. Кроме того, в разработке находится новое законодательство по обмену данными и их раскрытию[423], которое упростит процессы обмена данными.

3) право на потребительские данные: По общему правилу доступ к данным может быть предоставлен только пользователям, получившим аккредитацию Комиссии конкуренции и защиты прав потребителей. Аккредитации предшествует процедура установления пригодности третьей стороны (обращающегося за аккредитацией лица) в качестве получателя данных[424].

Предполагается, что данные могут также подпадать под действие CDR через механизм взаимности, т.е. те, кто намерен получить аккредитацию и определенные данные по запросу потребителя, должны быть готовы поделиться эквивалентными данными в ответ на запрос потребителя. Детали и степень взаимности будут рассматриваться в соответствии с правилами CDR (CDR Rules) после их разработки и принятия[425].

Таким образом, как и в большинстве рассматриваемых правопорядков, в Австралии действует законодательство, регулирующее публичные данные, а также категорию личной информации - близкой, хотя и не в полной мере тождественной понятию персональных данных (например, как оно

---

[423] New Australian Government Data Sharing and Release Legislation: Issues paper for consultation. URL: https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation (дата обращения: 20.10.2019)

[424] Treasury Laws Amendment (Consumer Data Right) Bill 2019. Division 3—Accreditation etc. Subdivision A—Accreditation process. https://www.legislation.gov.au/Details/C2019A00063 (дата обращения: 20.10.2019)

[425] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, pp. 25–26. https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6370_ems_ce513d68-7222-49f4-a2fe-67e1c2b32fed/upload_pdf/712911.pdf;fileType=application%2Fpdf (дата обращения: 20.10.2019)

определено в Общем регламенте по защите данных - General Data Protection Regulation (GDPR).

В то же время находятся в разработке правовые основы режима новой категории данных - данных, генерируемых потребителями при использовании определенных технологий, а также связанных с ними продуктов и услуг, предоставляемых частным сектором - права на потребительские данные.

2.1.7 Правовой режим данных в Сингапуре

Персональные данные в Сингапуре защищены в соответствии с Законом о защите персональных данных 2012 г. (PDPA).

PDPA имеет два основных положения:

– положения «Не звоните» (don not call) (позволяет пользователям отказываться от нежелательных маркетинговых коммуникаций);

– положения о защите данных.

Положения о защите данных содержат девять основных обязательств в области обработки персональных данных:

– открытость: предоставление информации о политике, практике и процедурах защиты данных организации по запросу,

– согласие: сбор, использование или раскрытие персональных данных только если физическое лицо дало согласие, также предусматривается разрешение на отзыв согласия,

– ограничение цели: сбор, использование или раскрытие персональных данных пользователей только в целях, указанных в соглашении,

– уведомление: уведомление отдельных лиц о целях, в которых организация намеревается собирать, использовать или раскрывать персональные данные во время или до сбора, использования или раскрытия,

– точность: обеспечение точности и полноты собранных персональных данных,

– защита: принятие мер безопасности для защиты собранных персональных данных и контроля для предотвращения

несанкционированного доступа, сбора, использования, раскрытия данных или подобных рисков,

– ограничение срока хранения: прекращение хранения персональных данных или удаление средства, с помощью которых персональные данные могут быть связаны с лицами, когда они больше не нужны для деловых или юридических целей,

– ограничение передачи: для передачи данных в другое государство в соответствии с требованиями, изложенными в правилах, обеспечение стандарта защиты, предоставляемого для передаваемых данных, сопоставимого с защитой, предоставляемой в соответствии с PDPA,

– доступ и исправление: по запросу предоставление субъектам данных информацию о том, каким образом их персональные данные были использованы или раскрыты. Исправление любой ошибки или упущения в персональных данных человека по запросу.

Значительная часть положений была принята Комиссией по защите персональных данных Сингапура с момента ее создания (2013 г.) для администрирования и соблюдения PDPA.

Правовой статус участников оборота данных в информационных системах регулируется Законом о государственном секторе (управлении) 2018[2] (см. книга 1).

Статья 107 вносит изменения в раздел 3 (2) (b) Закона о государственных органах (глава 319) для содействия оперативному обмену данными между государственными органами.

Законы о конфиденциальности не распространяются на общедоступные данные, и оборот таких данных не подпадает под действие законодательства.

Основным законом в области защиты государственной тайны является Акт о государственной тайне (Official Secrets Act; OSA)[426]. В соответствии с разделом 5 (1) (i) OSA, лица, получившие конфиденциальную информацию, работая на правительство, могут передавать такую информацию только уполномоченным лицам. Они будут виновны в совершении преступления, если сообщат информацию лицам, которые не имеют на это полномочий.

Преступления выражается в передаче конфиденциальной информации и понимании, что эта информация является секретной и конфиденциальной и что он не имеет полномочий на ее передачу.

Помимо лица, передающего конфиденциальную информацию, лица, которые получают такую конфиденциальную информацию, также будут виновны в совершении преступления согласно разделу 5 (2) OSA, если они знают, что эта информация является секретной и конфиденциальной.

«Шпионаж» включает такие действия, как подход, осмотр или вход в «запрещенное место», создание фотографий, рисунков, планов или заметок, которые могут быть полезны иностранной державе или врагу, получение, сбор, запись или передача конфиденциальной информации, которая может быть полезной иностранной державе или врагу.

Акт о государственной тайне охватывает не только секретную информацию (информацию, которая подпадает под категорию тайны). В качестве наглядного примера выступает положение о распространении действия Акта на информацию, которая была получена субъектом ввиду занимаемой им должности в правительстве[427]. Таким образом, положения Акта о государственной тайне охватывают широкий спектр режимов информации.

---

[426] Official Secrets Act 2012. https://sso.agc.gov.sg/Act/OSA1935#pr1- (дата обращения: 20.09.2019)

[427] Там же.

### 2.1.8 Правовой режим данных в Российской Федерации

Понятие правового режима информации не раскрыто российским законодательством. Тем не менее общеотраслевыми и отраслевыми нормативными правовыми актами в сфере управления данными установлены отдельные параметры различных правовых режимов информации.

Целевое назначение правового режима информации заключается в установлении прав и обязанностей субъектов оборота данных и управления ими, защите данных, в обеспечении информационной безопасности и баланса интересов субъектов оборота данных.

Правовые режимы информации характеризуются основаниями возникновения соответствующих режимов, а именно правовые режимы информации, основания существования и содержание которых вытекает из международных обязательств России и правовые режимы информации, установленные Конституцией и федеральными законами. В основе как общего правового режима информации, так и специальных правовых режимов информации лежат конституционные нормы.

Общий правовой режим информации базируется на конституционной норме, установленной в статье 29 и провозгласившей право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Указанной нормой определены параметры общего режима информации, предполагающие ее открытость и свободу действий субъектов в рамках закона. Законность действий субъекта устанавливает границы его правомерного поведения и границы действия общего режима. Эти границы, в частности, определяются другими конституционными нормами: осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц (статья 17); каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (статья 23) и др.

Конституционные основы специальных правовых режимов информации вытекают из таких конституционных норм, как упомянутая

статья 23: каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, ограничение этого права допускается только на основании судебного решения; статья 24: сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются; статья 29: перечень сведений, составляющих государственную тайну, определяется федеральным законом и др.

В законах развиваются конституционные положения, определяются вид правового режима и его носитель, основания введения, субъект правового режима, режимные меры и правила деятельности. Федеральное законодательство содержит большое количество как законодательных актов в целом, посвященных регулированию правовых режимов информации, так и отдельных норм в законодательных актах других отраслей законодательства, в комплексных законодательных актах. Базовым является Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»[428] (далее – Закон № 149-ФЗ). Хотя в нем не используется термин «правовой режим», основные элементы правового режима информации, основанного на конституционных нормах, в нем содержатся.

В частности, в соответствии с Законом устанавливаются следующие определения действий в отношении данных:

– доступ к информации – возможность получения информации и ее использования (пункт 6 статьи 2 Закона № 149-ФЗ);

– конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не

[428] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Часть I). Ст. 212.

передавать такую информацию третьим лицам без согласия ее обладателя (пункт 7 статьи 2 Закона № 149-ФЗ);

– предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц (пункт 8 статьи 2 Закона № 149-ФЗ);

– распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц (пункт 9 статьи 2 Закона).

Согласно статье 5 Закона № 149-ФЗ информация может являться объектом публичных, гражданских и иных правовых отношений.

В соответствии с данным Законом информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

В частности, статьями 7 и 8 Закона определяется правовой режим общедоступной информации:

– к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен (часть 1 статьи 7 Закона);

– общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации (часть 2 статьи 7 Закона);

– не может быть ограничен доступ к (часть 4 статьи 8 Закона):

1) нормативным актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за

исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

В Законе приводится классификация информации в зависимости от порядка ее предоставления или распространения. Из четырех приведенных в Законе групп две имеют общий правовой режим. Это информация, свободно распространяемая, и информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению. Различие между ними заключается в степени обязательности предоставления или распространения информации. Третья группа предполагает введение специального правового режима: это информация, распространение которой в России ограничивается или запрещается. И еще одна группа включает информацию, которая может иметь разный правовой режим и быть объектом как публично-правовых отношений, так и частноправовых. Речь идет об информации, предоставляемой по соглашению лиц, участвующих в соответствующих отношениях. Предметом таких соглашений может быть информация, составляющая коммерческую тайну (например, соглашение между двумя коммерческими структурами о передаче информации, являющейся секретом производства, договор коммерческой концессии и др.), государственную тайну (договор между двумя государствами о передаче сведений, составляющих государственную тайну), а также в рамках договора оказания информационных услуг может передаваться открытая информация.

Открытой является информация, доступ к которой не ограничен законодательством, а также обладателем информации.

Отнесение информации к общедоступной означает, что любое лицо без указания и обоснования причин и целей может ее получить. В соответствии с Законом № 149-ФЗ понятие «доступ к информации» включает возможность не только получения информации, но и ее использования. Однако введена оговорка, что общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений распространения такой информации. Иными словами, хотя информация является общедоступной и получение ее гарантируется, в части использования могут быть установлены ограничения. Правительством Российской Федерации принято значительное количество постановлений, устанавливающих порядок доступа к той или иной информации.

Правовые режимы информации могут возникать в силу установленных законом требований или в результате совершения ряда действий субъектом управления данными. Например, правовой режим персональных данных установлен Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных»[429], и не требуется дополнительных действий субъекта персональных данных, чтобы этот режим начал действовать. В отличие от этого, для введения режима коммерческой тайны законодатель установил необходимость совершения определенных действий, чтобы в отношении уже существующей информации был установлен режим коммерческой тайны.

Конституцией, федеральными законами, Указами Президента Российской Федерации установлены особенности правового режима отдельных видов данных, составляющих конфиденциальную информацию, различные виды тайн, включающие, в том числе:

---

[429] СЗ РФ. 2006. № 31 (Часть I). Ст. 3451.

– данные, составляющие личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (Конституция Российской Федерации[430]),

– данные, относящиеся к государственной тайне (Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»[431]),

– персональные данные (Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[432]),

– фискальные данные (Федеральный закон от 22 мая 2003 г. № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации»[433]),

– данные, относящиеся к коммерческой тайне (Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»[434]),

– данные, относящиеся к налоговой тайне (Налоговый кодекс Российской Федерации[435]),

– данные, относящиеся к банковской тайне (Гражданский кодекс Российской Федерации (часть вторая)[436], Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»[437], Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»[438]),

---

[430] Конституция Российской Федерации // СЗ РФ. 2014. № 31. Ст. 4398.
[431] СЗ РФ. 1995. № 49. Ст. 4775.
[432] СЗ РФ. 2006. № 31 (Часть I). Ст. 3451.
[433] СЗ РФ. 2003. № 21. Ст. 1957.
[434] СЗ РФ. 2004. № 32. Ст. 3283.
[435] СЗ РФ. 1998. № 31. Ст. 3824.
[436] СЗ РФ. 1996. № 5. Ст. 410.
[437] СЗ РФ. 1996. № 6. Ст. 492.
[438] СЗ РФ. 2002. № 28. Ст. 2790.

– данные, относящиеся к нотариальной тайне (Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-1[439]),

– данные, входящие в состав кредитной истории, и (или) код субъекта кредитной истории (Федеральный закон от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»[440]),

– данные, относящиеся к тайне страхования (Гражданский кодекс Российской Федерации (часть вторая), Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»[441], Федеральный закон от 24 июля 1998 г. № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»[442]),

– данные, относящиеся к конфиденциальности арбитража (третейского разбирательства) (Федеральный закон от 29 декабря 2015 г. № 382-ФЗ «Об арбитраже (третейском разбирательстве) в Российской Федерации»[443]),

– данные, ставшие известными гражданам в ходе оперативно-розыскной деятельности (Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[444]),

– данные, которые стали известны эксперту в связи с экспертизой по административному делу (Кодекс административного судопроизводства Российской Федерации от 8 марта 2015 г. № 21-ФЗ[445]),

– данные о новых решениях и технических знаниях, полученных сторонами по договору подряда (Гражданский кодекс РФ (часть вторая),

---

[439] Российская газета. 1993. № 49.
[440] СЗ РФ. 2005. № 1 (Часть I). Ст. 44.
[441] СЗ РФ. 2010. № 49. Ст. 6422.
[442] СЗ РФ. 1998. № 31. Ст. 3803.
[443] СЗ РФ. 2016. № 1 (Часть I). Ст.2.
[444] СЗ РФ. 1995. № 33. Ст. 3349.
[445] СЗ РФ. 2015. № 10. Ст. 1391.

– иные данные, относящиеся к видам тайн, иной информации конфиденциального характера.

Перечисленные акты устанавливают ограничения на доступ к указанной информации, ее использование, обработку, предоставление и иные действия с такой информацией, что в свою очередь, не позволяет обеспечить ее вовлечение в оборот в полном объеме.

Параметры правового режима информации, содержащейся в государственных информационных системах, установлены Законом № 149-ФЗ. В соответствии с частью 1 статьи 14 Закона государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

Согласно части 9 статьи 14 данного Закона информация, содержащаяся в государственной информационной системе, является государственным информационным ресурсом. Информация, содержащаяся в государственных информационных системах, является официальной.

Законодательством устанавливается круг лиц, являющихся участниками оборота данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (пункт 5 статьи 2 Закона № 149-ФЗ).

Правовое положение обладателя информации определено недостаточно точно: оно адекватно в частноправовых отношениях (например, субъект персональных данных вправе самостоятельно принимать решение о предоставлении их оператору или иному лицу, если такая обязанность не установлена законом; обладатель коммерческой тайны также праве определять круг лиц, допущенных к ней, и ограничивать доступ остальных лиц). В публично-правовых отношениях обладатель информации (если это Российская Федерация, субъект федерации, муниципальное образование, от

имени которых правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами), вправе разрешать или ограничивать доступ к информации, а в установленных случаях обязан предоставлять запрашиваемую информацию.

Правовой статус обладателя информации, то есть лица, самостоятельно создавшего информацию либо получившего на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (пункт 5 статьи 2 Закона № 149-ФЗ), регулируется в статье 6 Закона, в силу которой обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект федерации, муниципальное образование (часть 1); обладатель информации, если иное не предусмотрено федеральными законами, вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, использовать информацию, в том числе распространять ее, по своему усмотрению, передавать информацию другим лицам по договору или на ином установленном законом основании, защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами, осуществлять иные действия с информацией или разрешать осуществление таких действий (часть 3); обладатель информации при осуществлении своих прав обязан соблюдать права и законные интересы иных лиц, принимать меры по защите информации, ограничивать доступ к ней, если такая обязанность установлена законами (часть 4).

Цель, которую преследовал федеральный законодатель, вводя понятие «обладатель информации», заключалась в описании - по аналогии с гражданско-правовыми категориями «собственник», «титульный владелец», но с учетом особенностей информации как нематериального объекта –

правового статуса лица, правомочного в отношении конкретной информации решать вопрос о ее получении другими лицами и о способах ее использования как им самим, так и другими лицами. Как следует из приведенных законоположений, вопрос, становится ли лицо обладателем определенной информации, то есть приобретает ли оно применительно к этой информации права и обязанности, вытекающие из правового статуса обладателя информации, должен решаться исходя из существа правоотношений, связанных с ее получением, передачей, производством и распространением. При этом сам по себе доступ лица к информации не означает, что данное лицо становится ее обладателем по смыслу Закона № 149-ФЗ, то есть что оно вправе совершать с информацией действия, являющиеся прерогативой обладателя информации.

В отношении информации устанавливаются правовые режимы, связанные с объемом доступа к информации, объемом действий, направленных на предоставление, распространение информации.

В частности, такие нормы содержатся в статье 9 Федерального закона от 21 июля 2014 г. № 209-ФЗ «О государственной информационной системе жилищно-коммунального хозяйства»[446], в соответствии с которой правомочия обладателя государственного информационного ресурса системы и обладателя прав на результаты интеллектуальной деятельности, связанные с созданием системы, в том числе на программные средства системы, от имени Российской Федерации осуществляет федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

---

[446] Федеральный закон от 21.07.2014 № 209-ФЗ «О государственной информационной системе жилищно-коммунального хозяйства» // СЗ РФ. 2014. № 30 (Часть I). Ст. 4210.

Информация, содержащаяся в системе, является официальной. Государственный информационный ресурс системы подлежит защите в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации.

Аналогичный правовой режим установлен для иных информационных систем, с помощью которого можно установить объём правомочий обладателя информации, содержащейся в таких информационных системах.

Так из содержания статьи 12 Федерального закона от 3 декабря 2011 г. № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»[447] правомочия обладателя информации, содержащейся в государственной информационной системе топливно-энергетического комплекса (далее – ГИС ТЭК), от имени Российской Федерации осуществляет уполномоченный орган, обеспечивающий доступ к информации, содержащейся в ГИС ТЭК, в порядке, установленном Правительством Российской Федерации, в соответствии с законодательством об информации, информационных технологиях и о защите информации, законодательством о государственной тайне, о коммерческой тайне и иной охраняемой законом тайне и с учетом указанного Федерального закона.

Установлено, что данные, содержащиеся в ГИС ТЭК, являются информацией ограниченного доступа, за исключением информации, недопустимость ограничения доступа к которой установлена федеральными законами, а также информации, включенной в перечень, утверждаемый Правительством Российской Федерации (часть $2^1$ статьи 12). В указанной статье также определено, что правом доступа к информации, включая информацию ограниченного доступа, содержащейся в системе, с

---

[447] Федеральный закон от 03.12.2011 № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса» // СЗ РФ. 2011. № 49 (Часть V). Ст. 7060.

возможностью ее обработки обладает уполномоченный орган, а также организации, осуществляющие эксплуатацию сегментов данной системы. Иные пользователи ГИС ТЭК обладают правом доступа к информации, содержащейся в системе, без возможности ее обработки.

Под доступом к информации в данном случае понимается возможность получения и использования информации, содержащейся в информационной системе, в порядке, установленном указанным постановлением Правительства Российской Федерации, в соответствии с законодательством об информации, информационных технологиях и о защите информации, о государственной тайне, о коммерческой тайне и иной охраняемой законом тайне. Под использованием информации в контексте статьи 6 Федерального закона № 149-ФЗ понимается «в том числе распространение ее обладателем, по своему усмотрению».

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»[448] (далее – Закон № 98-ФЗ), определяя статус обладателя информации, составляющей коммерческую тайну, и закрепляя ряд его прав, связывает их возникновение с моментом установления им в отношении этой информации режима коммерческой тайны, предусматривающего принятие мер по охране ее конфиденциальности, включая определение перечня информации, составляющей коммерческую тайну, ограничение доступа к такой информации путем установления порядка обращения с ней и контроля за соблюдением установленного порядка, учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана, регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на

[448] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283.

основании гражданско-правовых договоров, нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (часть 1 статьи $6^1$, части 1 и 2 статьи 10).

Наряду с указанными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты ее конфиденциальности, другие не противоречащие законодательству Российской Федерации меры, при том что такие меры признаются разумно достаточными, если ими исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя и обеспечивается возможность ее использования работниками и передачи ее контрагентам без нарушения режима коммерческой тайны (части 4 и 5 статьи 10 Закона № 98-ФЗ).[449]

Таким образом, в отношении объема прав по обладанию информацией, содержащейся в информационных системах органов власти, можно судить о реализации комплекса прав по определению доступа к информации, использования, в том числе распространения и предоставления информации, защиты нарушенного в связи с использованием информации права обладателя такой информации, а также осуществления иных действий или разрешения действий с информацией.

Предполагается, что объем прав в этом случае будет зависеть от факта отнесения информации к той или иной категории доступности (общедоступная, государственная тайна, коммерческая тайна, иная охраняемая законом тайна и др.).

---

[449] См. Постановление Конституционного Суда Российской Федерации от 26.10.2017 № 25-П.

Пунктом 12 статьи 2 Закона № 149-ФЗ введено понятие оператора информационной системы, под которым понимается гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Федеральными законами устанавливаются понятия отдельных операторов обработки данных.

Так, в соответствии с пунктом 2 статьи 3 Федерального закона № 152-ФЗ «О персональных данных»[450] под оператором обработки персональных данных понимается государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Полномочия оператора в данном случае определяются, в том числе, как использование персональных данных, то есть совершение действий (операций) с персональными данными в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Статьей $1^1$ Федерального закона от 22 мая 2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации»[451] вводятся понятия оператора информационных

---

[450] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (Часть I). Ст. 3451.

[451] Федеральный закон от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» // СЗ РФ. 2003. № 21. Ст. 1957.

систем маркировки (лицо, являющееся оператором государственной информационной системы мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации, и оператором федеральной государственной информационной системы мониторинга движения лекарственных препаратов для медицинского применения от производителя до конечного потребителя с использованием в отношении лекарственных препаратов для медицинского применения средств идентификации) и оператора фискальных данных (организация, созданная в соответствии с законодательством Российской Федерации, находящаяся на ее территории, получившая в соответствии с законодательством о применении контрольно-кассовой техники разрешение на обработку фискальных данных).

Указанными федеральными законами определяются требования к таким операторам и особенности осуществления ими деятельности по обработке данных.

Согласно части 5 статьи 14 Закона № 149-ФЗ, если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

Функции и полномочия операторов государственных информационных систем могут также реализовывать концессионеры в соответствии с заключенными в отношении соответствующих систем концессионными соглашениями (особенности подготовки, заключения, исполнения и прекращения концессионного соглашения, объектом которого являются

объекты информационных технологий или объекты информационных технологий и технические средства обеспечения функционирования объектов информационных технологий установлены статьей 532 Федерального закона от 21 июля 2005 № 115-ФЗ «О концессионных соглашениях»[452]) либо частные партнеры в соответствии с соглашениями о государственно-частном партнерстве (пункт 19 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676[453]).

Правительством Российской Федерации принято значительное количество постановлений, а на уровне федеральных органов исполнительной власти – приказов, устанавливающих функции и полномочия операторов информационных систем, государственных информационных систем.

Провайдеры данных (информационные посредники). Провайдеры хостинга в соответствии с Законом №149-ФЗ оказывают услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к Интернету.

Провайдеры, иные лица, оказывающие услуги по размещению информации в информационной системе, непосредственно участвуют в обеспечении доступа к программно-техническим средствам государственных информационных систем и информации, содержащейся в них.

---

[452] Федеральный закон от 21.07.2005 № 115-ФЗ «О концессионных соглашениях» // СЗ РФ. 2005. № 30 (Часть II). Ст. 3126.

[453] Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // СЗ РФ. 2015. № 28. Ст. 4241.

Нормативными правовыми актами, регулирующими функционирование государственных информационных систем, определяются права и обязанности пользователей таких систем.

Так, например, частью 3 статьи 5 Федерального закона от 3 декабря 2011 г. № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»[454] (далее – Закон № 382-ФЗ) пользователями ГИС ТЭК (лицами, обладающими правом доступа к информации, содержащейся в системе) являются уполномоченный орган, иные органы государственной власти, органы местного самоуправления, а также юридические лица и физические лица.

Согласно части 5 статьи 12 Закона № 382-ФЗ уполномоченным органом государственной власти обеспечивается доступ к информации, содержащейся в ГИС ТЭК, с использованием программно-технических средств данной системы:

1) субъектам ГИС ТЭК, предоставляющим в обязательном порядке информацию для включения в государственную информационную систему топливно-энергетического комплекса, в отношении предоставленной ими информации и общедоступной информации, содержащейся в ГИС ТЭК (респонденты системы);

2) пользователям ГИС ТЭК к информации, которая содержится в ГИС ТЭК и доступ к которой ограничен настоящим Федеральным законом и другими федеральными законами, при наличии у таких пользователей права доступа к этой информации.

Таким образом, управление данными в каждой государственной информационной системе, правовой режим информации, содержащейся в

---

[454] Федеральный закон от 03.12.2011 № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса» // СЗ РФ. 2011. № 49 (Часть IV). Ст. 7060.

ней, функции и полномочия лиц, участвующими в обороте данных в системе, правила деятельности определяются широким кругом общеотраслевых и специальных (отраслевых) нормативных правовых актов, в том числе действующих исключительно в отношении такой информационной системы.

2.1.9 Выводы

Правовое регулирование управления данными в странах ЕС континентальной правовой семьи (Франции, Германии, Эстонии) характеризуется выделением специального законодательства в сфере обеспечения доступа к информации публичного сектора и отдельного регулирования в сфере защите персональных данных. Действуют также отдельные законы о разных видах информации ограниченного доступа (о государственной тайне, о коммерческой тайне и др.)

Законодательство о доступе к информации публичного сектора закрепляет обязанности раскрытия и предоставления информации не только государственными органами, но и иными лицами, выполняющими публичные функции, или чья деятельность финансируется из публичных средств. Законодательство стран Европейского союза отличается четкой регламентацией форм и процедур обеспечения доступа к информации публичного сектора.

В законодательстве стран Европейского союза большое внимание уделяется вопросам правового режима открытых данных как особого вида информации публичного сектора, размещаемой в открытом доступе в машиночитаемом формате и предназначенной для повторного использования.

В странах Европейского союза происходит унификация правовых режимов информации посредством имплементации директив и принятия регламентов. Наиболее унифицированным правовым режимом информации в странах Евросоюза является правовой режим персональных данных, обработка которых регулируется на уровне Регламента ЕС.

В странах общего права (Австралии, Великобритании) и Сингапуре также выделяются две группы режимов информации:

– общий режим (режим открытой/общедоступной информации),

– специальные правовые режимы информации.

Режим открытой/общедоступной информации присутствует во всех рассматриваемых странах. Специальные правовые режимы представлены различными институтами, имеющими схожее, но не всегда одинаковое регулирование: персональные данные, личная информация, право на потребительские данные, режим государственной тайны, коммерческой тайны и др.

## 2.2 Основы правового регулирования информационного взаимодействия между различными государственными информационными системами

### 2.2.1 Правовое регулирование в Европейском союзе

Общее правовое регулирование взаимодействия между государственными информационными системами в странах ЕС не принято, однако действуют нормативные акты, регулирующие взаимодействие данных систем в некоторых сферах, имеющих значение для Евросоюза. Наиболее яркий пример взаимодействия информационных систем в ЕС обнаруживается в сфере финансов. Ст. 127 Договора о функционировании ЕС[455] определяет одной из целей установления Европейской системы центральных банков обеспечение стабильного функционирования систем оплаты и клиринга.

[455] Consolidated version of the Treaty on the Functioning of the European Union - PART 3: UNION POLICIES AND INTERNAL ACTIONS. TITLE VIII: ECONOMIC AND MONETARY POLICY. Chapter 1: Economic policy. Article 126 (ex Article 104 TEC) // http://data.europa.eu/eli/treaty/tfeu_2008/art_126/oj (дата обращения 11.08.2019)

На уровне Союза действует несколько единых информационных систем финансовой сферы. Например, TARGET 2 – система валового расчета в режиме реального времени, владельцем и оператором которой является Евросистема (Европейский центральный банк и национальные центральные банки государств зоны евро)[456]. Платежные поручения направляются для обработки на платформе и зачитываются одно за одним на постоянной основе с немедленной выдачей результата. Платформа используется центральными и коммерческими банками для переводов в рамках реализации денежной политики, межбанковских и коммерческих платежей. Предшествующая система – TARGET – была создана путем объединения уже действовавших ранее национальных систем, что создавало технические трудности. TARGET 2 – технологически единая платформа. К ее созданию были привлечены центральные банки Франции, Германии и Италии, выступающие поставщиками услуг от имени Евросистемы. В качестве дополнения к TARGET 2 в ноябре 2018 г. реализована система мгновенной оплаты (TIPS)[457], обеспечивающая быстрый перевод денежных средств между организациями и физическими лицами.

В настоящий момент Евросистема планирует разработку новой информационной системы[458], которая предполагает введение новых сервисов. Например, будет создано единое для всех участников системы окно (Eurosystem single market infrastructure gateway). Интерфейс позволит выбирать виды соединений, обеспечивая конкуренцию между поставщиками услуг по соединению. За счет создания дополнительных копий данных будет

---

[456] What is TARGET 2? https://www.ecb.europa.eu/paym/target/target2/html/index.en.html (дата обращения 15.08.2019)

[457] What is TARGET Instant Payment Settlement (TIPS)?. https://www.ecb.europa.eu/paym/target/tips/html/index.en.html (дата обращения 15.08.2019)

[458] https://www.ecb.europa.eu/paym/target/consolidation/html/index.en.html (дата обращения 16.08.2019)

централизовано управление правами доступа (Common reference data). Пользователи смогут видеть историю своих данных (common data warehouse).

Для повышения эффективности управления внешними границами и внутренней безопасностью ЕС Европейская комиссия внесла ряд предложений по модернизации и развитию информационных систем в этой сфере. Комиссия внесла законодательные предложения по двум сводам правил в декабре 2017 года (с поправками июня 2018 года), устанавливающим рамки взаимодействия информационных системам ЕС, обеспечивающими пограничную и визовую деятельность, а также полицейского и судебного сотрудничества, убежищ и миграции. После завершения законодательной процедуры в первом чтении в парламенте и Совете оба закона вступили в силу 11 июня 2019 года. Новые правила направлены на улучшение проверок на внешних границах ЕС, позволяют лучше выявлять угрозы безопасности и мошенничества с личными данными, а также помогают в предотвращении незаконной миграции и в борьбе с нею[459].

В ЕС также уделяется внимание поддержанию критической инфраструктуры систем связи и их взаимодействию. В частности, Директивой 2016/1148 от 6.07.2019 поддерживается общий высокий уровень безопасности сети и информационных систем в ЕС[460], установлены основы взаимодействия и поддержания безопасности операторов существенных услуг и поставщиков цифровых услуг. Директива предусматривает обязанность всех стран ЕС утвердить национальную стратегию безопасности

---

[459] http://data.europa.eu/eli/reg/2019/817/oj, http://data.europa.eu/eli/reg/2019/818/oj (дата обращения 15. 08. 2019)

[460] 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. http://data.europa.eu/eli/dir/2016/1148/oj (дата обращения 17.08.2019)

сети и информационных систем, устанавливает требования к безопасности и уведомлениям об инцидентах для операторов существенных услуг и поставщиков цифровых услуг. Оператором существенных услуг признается лицо, соответствующее установленным в Директиве критериям. В частности, приложение № 2 к Директиве определяет типы операторов (напр., транспорт, регистраторы доменов и т.п.). Критерии отнесения указанных типов операторов к операторам существенных услуг установлены в ч.2 ст. 5 Директивы (любые частные и публичные лица, оказывающие услуги, необходимые для поддержания критической общественной и/или экономической деятельности, предоставление которых зависит от информационных систем; инцидент в таких системах может оказать существенное негативное влияние на оказание предлагаемой услуги в целом). В ряду операторов существенных услуг фигурируют также точки Интернет-обмена (IXP), обеспечивающие взаимодействие двух и более независимых систем для упрощения обмена трафиком.

Директива предусматривает организационно-административные меры по исполнению ее положений: учреждает Группу взаимодействия (Cooperation group) для стратегического взаимодействия и обмена информацией между странами, а также систему ответов о компьютерных инцидентах (CSIRTs network) для удобства взаимодействия. Каждое государство обязано создать орган, уполномоченный обеспечивать безопасность сети и информационных систем.

Ст. 8 Директивы предусматривает обязанность каждого государства иметь орган, выступающий единой точкой взаимодействия по компьютерным инцидентам с органами других стран ЕС, Группой взаимодействия, а равно между национальными органами. Каждое государство также формирует одну или несколько команд реагирования на компьютерные инциденты (CSIRTs). Команда реагирования может получать уведомления об инцидентах напрямую, а если государство назначило

получателем таких уведомлений иной орган, команда должна иметь беспрепятственный доступ к такой информации.

Таким образом, на уровне ЕС функционирует единая система предотвращения компьютерных инцидентов, а также сообщения между уполномоченными органами государств и командами по предотвращению инцидентов, обеспечивающая безопасность взаимодействия, устойчивое функционирование систем связи. Хотя европейское право отдельно не регулирует взаимодействия государственных информационных систем, оно предусматривает общие меры безопасности единой инфраструктуры связи, а равно создает и развивает единые системы в финансовой сфере.

2.2.2 Особенности правового регулирования в Германии

Национальная стратегия электронного правительства 2015 г. закрепляет основные цели и направления деятельности Совета по ИТ-планированию и создает основу для совместной ориентации федерального правительства, земель и муниципалитетов на дальнейшее развитие электронного правительства, в том числе составляющих его государственных информационных систем, которые в ряде случаев сводятся к электронным базам данных и порталам государственных органов.

Положения об электронном правительстве получили развитие в ряде федеральных и земельных законов. Закон о продвижении электронного правительства (EGovG) от 25.08.2013[461] содержит общие положения об электронных базах данных государственных органов и межведомственном взаимодействии. Согласно Закону, органы власти обязаны хранить все файлы в электронном виде, бумажные оригиналы подлежат возврату тем, от кого они были получены, либо уничтожаются. Проведение административных процедур также переводится в электронную форму. При предоставлении

[461] Gesetz zur Förderung der elektronischen Verwaltung. http://www.gesetze-im-internet.de/egovg/ (дата обращения 14.08.2019).

доступа к электронным базам данных, файлам осуществляется удаленная идентификация личности заявителя, в том числе посредством использования электронной подписи. Если при электронных административных процедурах необходима плата, то государственные органы обязаны предоставлять возможность оплаты посредством электронных средств платежа с последующей выдачей электронных подтверждений платежа.

Оказание административных услуг в электронном виде регулируется Законом об улучшении онлайн-доступа к административным услугам (OZD) от 14.08.2017, по которому государственные органы обязаны предлагать свои услуги в электронном виде посредством порталов. Порталы федеральных органов власти и органов земель в последующем объединятся в единую портальную сеть.

Для заказа административных услуг и работы пользователей используются учетные записи пользователей. При этом назначается специальный орган, ответственный за учетные записи.

В отдельных сферах деятельности применяются специальное регулирование о взаимодействии государственных информационных систем. Так, законом о телекоммуникациях (TKG)[462] предусмотрены случаи и порядок обмена информацией между операторами связи и государственными органами. Предусмотрена обязанность предоставлять по запросам федеральных органов отдельные категории информации для модернизации сетевой инфраструктуры. Отдельно предусмотрена обязанность Федерального сетевого агентства информировать правоохранительные органы о фактах, послуживших основанием для подозрения в правонарушениях, выявленных при оказании телекоммуникационных услуг.

---

[462] Telekommunikationsgesetz. https://www.gesetze-im-internet.de/tkg_2004/index.html (дата обращения 10.08.2019).

Законодательством земель уточнены процедуры формирования государственных информационных систем, межведомственного взаимодействия и обмена данными, оказания административных услуг и др. Например, постановление о передаче данных в Берлине от 28.09. 2017[463] подробно освещает процессы регулярных обменов данными и автоматического межведомственного обмена данными в разрезе сфер деятельности (образовательная, правоохранительная деятельность, проведение выборов, здравоохранение и т.п.). При предоставлении данных в госсектор также могут предъявляться отдельные требования к форматам передачи данных, например при передаче данных о налогах[464]. Также приняты отдельные законы в целях регулирования трансграничной передачи данных по отдельным сферам, например, по выявлению нелегальных доходов, мониторингу пассажирских перевозок, обеспечению внешней торговли и др. Действуют отдельные нормы, позволяющие осуществлять повторное использование данных иными государственными службами.

В целях бесперебойного доступа к государственным услугам установлены требования к защите ИТ-инфраструктуры и передаваемой по сетям информации, а также предусмотрена необходимость использования технических стандартов связи.

Национальная стратегия кибербезопасности[465] определяет основные направления политики в области обеспечения кибербезопасности; в ней

---

[463] Verordnung zur Übermittlung von Meldedaten in Berlin Vom 28. September 2017. : http://gesetze.berlin.de/jportal/portal/t/lxz/page/bsbeprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=25&numberofresults=64&fromdoctodoc=yes&doc.id=jlr-MeldD%C3%9CVBEpP20&doc.part=X&doc.price=0.0&doc.hl=1#focuspoint (дата обращения: 17.08.2019).

[464] https://www.gesetze-im-internet.de/altvdv/ (дата обращения 14. 08. 2019)

[465] Cyber-Sicherheitsstrategie für Deutschland. http://www.bmi.bund.de/cybersicherheitsstrategie/ (дата обращения 15.08.2019).

обозначены приоритетные направления ее развития: безопасность электронного взаимодействия через шифрование и, несмотря на шифрование, расширение концепции безопасной идентификации лиц и вещей, распространение стандартов кибербезопасности, проведение исследований.

Закон о повышении безопасности систем информационных технологий от 7.07.2015 (IT-Sicherheitsgesetz)[466] создал единую правовую базу кибербезопасности. В дополнение к обязательному уведомлению об инцидентах информационной безопасности Закон устанавливает минимальные стандарты ИТ и требования к отчетности для операторов критически важных инфраструктур (энергетику, водоснабжение, здравоохранение, телекоммуникации). В настоящее время опубликован проект Закона о безопасности ИТ–2.0 (IT-SiG 2.0)[467]. В проекте Закона полномочия правоохранительных органов расширены, вносятся изменения в уголовное и уголовно-процессуальное законодательство с усиления мер борьбы с киберпреступностью. Сфера применения Закона распространяется на другие сферы экономики (помимо критически важных), в частности на сферы, имеющие общественный интерес, нарушения в которых приведут к ущербу «фундаментальным интересам общества».

Постановлением об определении критических инфраструктур в соответствии с BSI-Gesetz (Kritis-VO) от 22 апреля 2016 года[468] уточнен

---

[466]Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1565384375246 (дата обращения: 20.08.2019)

[467] Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 (дата обращения 20.08.2019).

[468]Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz //Режим доступа: https://www.gesetze-im-internet.de/bsi-kritisv/ (дата обращения 18.08.2019).

перечень критически важных услуг в сферах энергетики, водоснабжения, продовольствия, здравоохранения, телекоммуникаций, транспорта, финансового сектора. Установлены критерии и пороговые значения (формулы расчета различных показателей) систем безопасности в каждом секторе экономики, регулируемом Законом об информационной безопасности.

2.2.3 Особенности правового регулирования во Франции

Во Франции осуществляется реформа публичной службы. В результате опросов населения, а также привлечения данных комитета молодежи и коллегии экспертов сформирована Программа трансформации публичной службы до 2022 г.[469] Выделены пять ключевых направлений реформирования, среди которых также фигурирует цифровое преобразование публичной службы. В рамках реализации указанного направления реформирования во Франции создаются координирующие органы, осуществляющие как цифровизацию оказания государственных услуг в целом, так и упрощающих взаимодействие государственных информационных систем.

Взаимодействие государственных информационных систем различных органов и реализация проектов по созданию межведомственных систем находятся в ведении DINU. DINU[470] получила полномочия определения общих принципов и правил урбанизации и создания государственных информационных систем, она также получила полномочия организации операций по взаимодействию информационных систем в ведении различных

---

[469] https://www.modernisation.gouv.fr/action-publique-2022/comprendre/action-publique-2022-un-programme-pour-accelerer-la-transformation-du-service-public (дата обращения 20. 06. 2019)

[470] В соответствии с информацией, указанной в книге 1, с 25 октября 2019г. указанные полномочия осуществляются Межведомственной дирекцией по цифровому развитию (DINU). Ранее они осуществлялись Межведомственной дирекцией по взаимодействию государственных информационных систем (DINSIC).

органов власти[471]. DINU отвечает и за ведение единой системы электронного межведомственного взаимодействия Франции (RIS), созданной на основании постановления от 17 декабря 2012 г.[472]

Разработаны правоприменительные документы для цифрового государства: права лиц, в отношении которых принимаются индивидуальные решения с помощью алгоритма (март 2017 года), процедура безопасного доступа к публичным базам данных (март 2017 года), лицензии на бесплатное повторное использование публичной информации (апрель 2017 года), электронный доступ к основным данным соглашений о грантах (май 2017 года), Государственная служба справочных данных (июнь 2017 года), электронный процесс, заменяющий заказное письмо (декабрь 2017 года), обмен информацией между администрациями (в настоящее время рассматривается CNIL), France Connect частных лиц и агентов (сентябрь 2018), административные документы, которые могут быть опубликованы без анонимизации (октябрь 2018).

Разработаны: Закон государства, обслуживающего доверенную компанию (эксперимент по обмену информацией между администрациями с помощью API) в августе 2018 года, Закон О защите персональных данных (автоматические индивидуальные решения, принятые на основе алгоритмической обработки) в июне 2018 года.

---

[471] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique. https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D4ECB579ACEA6FD419A2720092289704.tplgfr31s_2?cidTexte=JORFTEXT000039281619&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000039281603 (дата обращения 04.11.2019).

[472] Arrêté du 17 décembre 2012 portant création d'un service à compétence nationale dénommé «Réseau interministériel de l'Etat». https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026792328&categorieLien=id (дата обращения 01. 11. 2019)

Уточнены европейские нормы: примеры – пересмотр директивы «общественный сектор информации» (июнь 2017 года – октябрь 2018 года), транспонирование директивы «доступность» (октябрь 2018 года).[473]

В 2018 г. принята Хартия принципов взаимодействия государственных информационных систем[474] (концептуальный документ, не имеющий юридической силы), не устанавливающая технических норм, однако определяющая принципы взаимодействия. Например, требование о прозрачности взаимодействия информационных систем может оцениваться с точки зрения отзывов пользователей. Взаимодействие не обязательно обеспечивается единым административным или технологическим решением, необходимо учитывать возможности и потребности каждого органа, в ведении которого находится информационная система. Механизмы разделения издержек должны, с одной стороны, быть максимально упрощенными, с другой - позволять каждому министерству выиграть от взаимодействия информационных систем. Равноправие министерств в возможностях развития взаимодействия информационных систем обеспечивалась созданием отдельного межведомственного координирующего органа (DINSIC до 25 октября 2019 г.).

На уровне подзаконных актов также имеются положения, посвященные взаимодействию ведомств и информационных систем. Так, Декрет о государственной информационно-коммуникационной системе n° 2014-879 от 1.08.2014[475] предусматривает созыв Совета информационных систем

---

[473] https://www.numerique.gouv.fr/uploads/Bilan_DINSIC_2017-2018.pdf (дата обращения 16. 11. 2019)

[474] Principes de mutualisation du SI de l'Etat. https://www.numerique.gouv.fr/uploads/201811-CSIC-Fiche_05-principes-mutualisation.pdf (дата обращения 05. 11. 2019)

[475] Décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'Etat.

государства не реже двух раз в год. В Совет входят генеральные секретари министерств; генеральный директор системы информационного взаимодействия в области обороны; генеральный директор администрации по публичным функциям; генеральный директор агентства безопасности информационных систем; директор бюджета и директор государственных закупок. Каждое министерство разрабатывает план финансирования исполнения обязанности, возложенной на него в отношении информационных систем, и направляет его на ознакомление директору по цифровому развитию и системе информационного взаимодействия государства.

Для безопасности информационных систем во Франции создано Национальное агентство безопасности информационных систем[476], принимающее заявления об инцидентах как от организаций, так и от государственных органов.

Таким образом, во Франции взаимодействие государственных информационных систем централизовано. Одновременно в связи с тем, что DINU, в полномочия которой вошли создание принципов и правил создания государственных информационных систем, организация взаимодействия информационных систем, была учреждена недавно, в настоящий момент трудно детально охарактеризовать уточненный подход к обеспечению взаимодействия государственных информационных систем.

---

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029337021 (дата обращения 24. 06. 2019)

[476] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information» // https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212 (дата обращения 14. 06. 2019)

### 2.2.4 Особенности правового регулирования в Эстонии

Отдельная глава в Акте о публичной информации Эстонии посвящена базам данных и государственным информационным системам. Под базой данных понимается структурированная совокупность данных, обрабатываемых в информационной системе государства, органа местного самоуправления, юридического лица публичного права или юридического лица частного права, выполняющего публичные обязанности, которая создается и используется для выполнения функций, предусмотренных законом, изданным на его основе правовым актом или международным договором.

Создание базы данных осуществляется на основании закона или принятого на основании закона правового акта. Не допускается создание баз данных, предназначенных для сбора аналогичной информации. Для этого создание новой базы данных и изменения существующих баз данных должны быть согласованы с Министерством экономики и коммуникаций, Инспектором по защите данных и органом по статистике.

Государственная информационная система состоит из баз данных, которые взаимодействуют с государственной информационной системой и зарегистрированы в государственной информационной системе, а также систем, обеспечивающих ведение баз данных (support systems).

К системам, поддерживающим ведение баз данных в государственной информационной системе, относятся: система классификаций; геодезическая система; система адресов; система мер безопасности для информационных систем; уровень обмена данными информационных систем; система управления государственной информационной системой. Обмен между базами данных, входящими в государственную информационную систему, осуществляется на уровне обмена данными государственной информационной системы. При учреждении базы данных и включении её в государственную информационную систему база подлежит регистрации в органах управления государственной информационной системой.

У каждой базы данных есть администратор (chief processor, administrator) – публичный орган, юридическое лицо публичного права или лицо частного права, выполняющее публичные обязанности, которое учреждает базу данных и осуществляет управление данными и сервисами. Администратор базы данных отвечает за управление базой данных и её развитие. Администратор может уполномочить другой публичный орган, юридическое лицо публичного права или, на основании договора о закупках или публичного договора, лицо частного права на выполнение задач по обработке данных и ведению базы данных. Данное лицо приобретает статус авторизованного обработчика (authorised processor). Авторизованный обработчик обязан выполнять инструкции главного процессора при обработке данных и ведении базы данных, а также обеспечивать безопасность базы данных.

У базы данных должно быть положение (statute), которое устанавливает порядок ведения базы данных, администратора базы данных, состав данных, подлежащих сбору в базу данных, поставщиков данных, и другие организационные вопросы. Поставщиками данных могут быть лица, обязанные поставлять данные в соответствии с законодательством, либо лица, добровольно делающие это.

Доступ к базам данных по умолчанию должен быть открытым неограниченному кругу лиц, если к данным не ограничен доступ законом или на основании закона.

Принципы управления сервисами и информацией 2017 года[477] устанавливают организационно-правовые основы управления данными для оказания публичных электронных услуг. Под управлением данными понимается деятельность, способствующая достижению целей публичного

[477] Principles for Managing Services and Governing Information: https://www.riigiteataja.ee/en/eli/507072017004/consolide (дата обращения: 14.08.2019).

управления посредством управления, обмена информацией и обмена ею во всех информационных системах и базах данных. Управление данными обеспечивает качество и доступность информации, управление рисками и оптимизацию расходов на хранение, обмен и использование информации, а также преемственность управления данными.

Указанные принципы обязывают государственные органы упорядочивать деятельность, связанную со сбором, обработкой и хранением данных (проводить инвентаризацию данных, уточнять данные, прекращать обработку данных при отсутствии ее оснований и т.п.). Государственные органы должны выявлять потребности различных групп пользователей в информации, учитывать их при разработке процессов и услуг.

Публичные органы обязаны сотрудничать друг с другом в оказании публичных услуг. По общему правилу обмен информацией между публичными органами осуществляется в электронном виде.

Электронный обмен данными между публичными органами обеспечивается посредством межведомственного центра обмена документами через уровень обмена данными информационных систем (т.н. X-Road). Обмениваемые документы должны включать в себя метаданные, зарегистрированные в специальной системе RIHA.

X-Road является технической основой единой платформы, к которой подключены государственные органы и частные компании. Основная задача X-Road заключается в том, чтобы правильно синхронизировать информацию между разными базами, убирать дубли, обеспечивать проактивное оказанение государственной услуги. В настоящее время в Эстонии платформа X-Road синхронизирует и позволяет «общаться» между собой 170 базам данных. Разрабатывается X-Road как открытое программное обеспечение, что позволяет Эстонии экономить на развитии и поддержке электронных услуг.

Принципы также закрепляют порядок взаимодействия с государственным органом посредством использования официального электронного адреса на портале eesti.ee.

Министерством экономики и коммуникаций разработаны Принципы интероперабельности государственных информационных систем[478]. Под интероперабельностью понимается способность различных организаций взаимодействовать между собой для достижения взаимовыгодных и согласованных общих целей, включая обмен информацией и знаниями между организациями посредством обмена ими между информационными системами. Основой интероперабельности являются стандарты и открытые платформы. Принципы интероперабельности направлены на подготовку соответствующих правовых актов и разработку необходимых IT-решений. Интероперабельность государственных систем имеет целью:

– способствовать развитию сервис-ориентированного общества, где граждане смогут общаться с государством, не вникая в иерархическую структуру государственного аппарата и разделение компетенций в нем,

– обеспечивать прозрачность в принятии политических решений,

– поддерживать совместное развитие государственной информационной системы,

– создать условия для свободной конкуренции,

– сокращать государственные расходы на ИТ.

Принципы интероперабельности – субсидиарность и пропорциональность; ориентированность на пользователя; доступность; безопасность и конфиденциальность; многоязычие; упрощение административных процедур; прозрачность; сохранение информации;

---

[478] Interoperability of the State Information System. https://www.mkm.ee/sites/default/files/interoperability-framework_2011.doc (дата обращения: 14.08.2019).

открытость; повторное использование; технологическая нейтральность и адаптивность; результативность.

Таким образом, в Эстонии получило развитие унифицированное регулирование в сфере использования государственных информационных систем. Для обмена данными между системами используется централизованная модель.

2.2.5 Особенности правового регулирования в Великобритании

В настоящее время действует Стратегия трансформации правительства (Government Transformation Strategy 2017 to 2020)[479] и Цифровая стратегия развития (UK Digital Strategy 2017)[480], которые содержат положения, основываясь на которых Цифровая правительственная служба продолжает формирование единой платформы электронного правительства GOV.UK, представляющей собой централизованную информационную систему, в рамках отдельных сервисов которой происходит обмен информацией с органами публичной власти или между ними[481].

Платформа GOV.UK, построенная в соответствии с Руководством[482] и Принципами открытых стандартов[483], управляемая Цифровой службой, включает следующие сервисы:

– Gov.uk Design System – платформа для создания новых сервисов, в соответствии с вышеуказанными стандартами,

---

[479] Government Transformation Strategy 2017 to 2020: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020 (дата обращения: 05.08.2019).

[480] UK Digital Strategy 2017. https://www.gov.uk/government/publications/uk-digital-strategy (дата обращения: 05.08.2019).

[481] GOV.UK website. https://www.gov.uk (дата обращения: 05.08.2019).

[482] Guidance: Technology Code of Practice, 2019.: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice (дата обращения: 05.08.2019).

[483] Policy paper: Open Standards principles, 2018. https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (дата обращения: 05.08.2019).

– Gov.uk Verify – аналог российской ЕСИА,

– Gov.uk Pay – национальная система онлайн-платежей,

– Gov.uk Notify – система обмена сообщениями (данными) для органов власти и их должностных лиц,

– Gov.uk PaaS – платформа веб-хостинга, предоставляющая возможность осуществления проектов в общественном секторе на базе системы управления данными,

– Gov.uk Registers – сервис, который представляет структурированные наборы данных и возможность интеграции с API (програмный интерфейс приложения) сервисом для построения своих сервисов,

– GOVWifi - государственная сеть Wi-Fi для органов власти,

– Digital marketplace (beta – версия) – сервис для организаций государственного сектора по поиску людей и технологий для цифровых проектов: цифровых продуктов и облачных сервисов (госзакупки в сфере IT).

В рамках Цифровой правительственной службы действует Сеть государственных услуг (PSN)[484]. Сеть позволяет государственным органам осуществлять информационное взаимодействие, сокращая дублирование информации.

Сбор персональных данных для государственных органов урегулирован ранее упомянутыми Data Protection Act 2018 и GDPR.

Косвенно к защите данных (не на этапе сбора, но на этапе, когда они находятся в системе) можно отнести и Регламент безопасности сетей и информационных систем[485], который принят для имплементации положений

---

[484] Public Services Network (PSN): https://www.gov.uk/government/groups/public-services-network (дата обращения: 05.08.2019).

[485] The Network and Information Systems Regulations 2018. URL: http://www.legislation.gov.uk/uksi/2018/506/contents (дата обращения: 05.08.2019).

Директивы ЕС 2016/1148 (NIS)[486]. В целом Регламент соответствует положениям директивы NIS, следовательно, в рамках настоящей части исследования, анализ положений указанного акта не является необходимым.

Соединенное Королевство активно участвует в отраслевом международном обмене информацией. Так, например, в налоговой сфере, основываясь на международных договорах об обмене налоговой информацией (TIEAs)[487], принимая во внимание международные стандарты обмена (Модельное соглашение об обмене налоговой информацией ОЭСР (OECD Model TIEA)[488] органы власти страны могут запрашивать и получать налоговые сведения об определенных лицах.

Следовательно, деятельность GDS по созданию и развитию сервисов единой цифровой платформы регулируется в основном актами стратегического планирования. Централизованный подход к взаимодействию сервисов и исключение дублирования данных достигается путем создания единой информационной платформы GOV.UK.

2.2.6 Особенности правового регулирования в Австралии

Основой информационного взаимодействия между государственными информационными системами является Национальная правительственная стратегия обмена информацией (NGISS)[489] 2009 г. Основной задачей NGISS была разработка скоординированного подхода и основы для обмена данными

---

[486] 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. https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 05.08.2019).

[487] Guidance. Automatic Exchange of Information: introduction. URL: https://www.gov.uk/guidance/automatic-exchange-of-information-introduction (дата обращения: 05.08.2019).

[488] Tax Information Exchange Agreements (TIEAs). https://www.oecd.org/ctp/exchange-of-tax-information/taxinformationexchangeagreementstieas.htm (дата обращения: 05.08.2019).

[489] National Government Information Sharing Strategy. URL: https://www.finance.gov.au/sites/default/files/ngiss.pdf (дата обращения 12. 01. 2019)

между различными агентствами и между правительствами всех уровней власти (all levels of government in Australia – Commonwealth, state and local). NGISS не предписывает единообразного подхода к обеспечению взаимодействия, ограничиваясь унификацией обмена информацией на всех уровнях государства. Реализация Стратегии осуществляется через девять принципов обмена информацией (см. книгу 1) и предлагаемый государственным органам набор инструментов и методов реализации каждого принципа. Предполагается, что государственные органы самостоятельно разрабатывают и реализуют план развития информационного взаимодействия, включая определение условий передачи данных.

Следует отметить, что одной из целей разработки Национальной правительственной стратегии обмена информацией было создание инструментов, призванных обеспечить стандартизированный подход к созданию систем информационного взаимодействия.

Правовой режим государственных информационных систем законодательно не определен. Возможно, однако, что определенные подходы, связанные с интеграцией государственных инфолрмационных систем, их отраслевой спецификой или иными практическими аспектами получат отражение при разработке нового законодательства по обмену данными и их раскрытию[490].

В целом в Австралии широко используется регулирование основанное на принципах (principle-based regulation), что еще в 2010 году было рекомендовано Комиссией правовой реформы (Australian Law Reform

[490] New Australian Government Data Sharing and Release Legislation: Issues paper for consultation. URL: https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation (дата обращения 20 05 2019)

Commission) в качестве основного подхода к регулированию конфиденциальности информации (information privacy)[491].

2.2.7 Особенности правового регулирования в Сингапуре

В Сингапуре законы о конфиденциальности не распространяются на общедоступные данные, и оборот таких данных в государственных информационных системах не подпадает под действие законодательства. Общедоступные данные содержатся на правительственном портале Data.gov.sg, запущенном в 2011 г. в качестве единого портала правительства для его общедоступных наборов данных из 70 государственных учреждений и их информационных систем[492]. На сегодняшний день создано более 100 приложений с использованием открытых данных правительства. Примечательно, что функционал портала выходит за рамки базового хранилища данных. Он направлен на то, чтобы сделать правительственные данные актуальными и понятными общественности посредством активного использования диаграмм и статей.

Цели этого портала включают обеспечение единого доступа к общедоступным государственным данным, передачу правительственных данных и анализ через визуализации и статьи, облегчение процесса поиска и обработки данных для анализа и исследования.

Этот веб-сайт является инициативой Министерства финансов и поддерживается Технологическим агентством Сингапура.

Принципы обмена данными: данные должны быть легко доступны, они должны быть доступны также для совместного создания, должны быть

---

[491] For Your Information: Australian Privacy Law and Practice (ALRC Report 108). В редакции от 16.08.2010. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/4-regulating-privacy/regulatory-theory/ (дата обращения: 24 05 2019)

[492] Портал открытых данных Сингапура. https://data.gov.sg/ (дата обращения 12. 06. 2019)

выпущены своевременно, должны быть переданы в машиночитаемом формате, должны быть максимально необработанными.

В целях регулирования возможности повторного использования государственных данных правительством Сингапура была разработана лицензия на открытые данные (англ. Singapore Open Data License). Согласно ее условиям, пользователи могут использовать, получать, загружать, копировать, распространять, передавать, модифицировать и адаптировать наборы данных или любые подготовленные на их основе анализы или приложения, как в коммерческих, так и в некоммерческих целях. При этом пользователи ограничены в получении прав на любые персональные данные, должны соблюдать права третьих лиц, в том числе права на патенты, товарные знаки и права разработчиков, а также при использовании данных должны давать ссылку на источник данных.

С апреля 2018 г. действует Закон, регулирующий обмен данными между государственными учреждениями (Public Sector (Governance) Act 2018). Закон направлен на создание согласованной структуры управления в государственных органах и поддержку единого правительственного подхода к оказанию услуг в государственном секторе. Раздел 2 Закона большей частью посвящен вопросу совместного использования данных, при этом установлены также меры наказания за несанкционированное раскрытие и ненадлежащее использование информации. Принятие Закона повлекло за собой изменения во многих законодательных актах в части формулировок секретности государственных данных.

Несмотря на то, что положения, касающиеся регулирования такого обмена, не закреплены нормативными актами, действует большое количество государственных проектов, регулирующих оборот таких данных; например,

реализована сеть TradeNet[493], которая обеспечивает обмен электронными данными между государственными департаментами. В Сингапуре также действует большое количество программ развития обмена данными в условиях стремительного развития цифровой экономики. В рамках модернизации информационного взаимодействия повышенное внимание уделяется регулированию оборота данных в государственных системах.

Аналогичное регулирование внедряется в других сферах государственного управления, например, в медицине. Для такого вида обмена используется специальный термин – Electronic Data Interchange (EDI), который фигурирует в проектах, основа которых заключается в реализации государственной политик обмена данными. Портал Data.gov.sg представляет собой площадку для реализации программы обмена данными, в том числе между различными государственными информационными системами, которая наглядно демонстрирует успехи Сингапура на рассматриваемом направлении.

2.2.8 Особенности правового регулирования в Российской Федерации

Общие требования к межведомственному информационному взаимодействию определены Федеральным законом от 27 июля 2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[494] (далее – Закон № 210-ФЗ) и иными нормативными правовыми актами.

В соответствии с частями 7 и 8 статьи $7^1$ Закона № 210-ФЗ Правительством Российской Федерации утверждены перечень сведений, находящихся в распоряжении государственных органов субъектов федерации, органов местного самоуправления, территориальных

---

[493] Государственная платформа обмена данными. https://www.ntp.gov.sg/public/government-services (дата обращения 10 06 2019)

[494] СЗ РФ. 2010. № 31. Ст. 4179.

государственных внебюджетных фондов, подлежащие обязательному предоставлению федеральному органу исполнительной власти, органу государственного внебюджетного фонда Российской Федерации или многофункциональному центру по межведомственному запросу[495] и перечень сведений, необходимых для предоставления государственных услуг исполнительными органами государственной власти другого субъекта федерации, территориальными государственными внебюджетными фондами и муниципальных услуг органами, предоставляющими муниципальные услуги, на территории другого субъекта Российской Федерации[496]. Требования к форматам сведений, указанных в части 7 статьи $7^1$ Закона определяются уполномоченными федеральными органами исполнительной власти.

Правила обмена документами в электронном виде при организации информационного взаимодействия федеральных органов исполнительной власти, органов исполнительной власти субъектов федерации, государственных внебюджетных фондов установлены постановлением Правительства Российской Федерации от 25 декабря 2014 № 1494[497].

В соответствии с частью $7^2$ Закона № 210-ФЗ в рамках межведомственного информационного взаимодействия может быть реализован межведомственный запрос о предоставлении документов и информации, необходимых для государственных и муниципальных услуг.

Федеральным законодательством установлены общие требования к информационному взаимодействию между различными государственными

---

[495] Распоряжение Правительства Российской Федерации от 29.06.2012 № 1123-р «О перечне сведений, находящихся в распоряжении государственных органов субъектов РФ, органов местного самоуправления, территориальных государственных внебюджетных фондов» // СЗ РФ. 2012. № 28. Ст. 3924.

[496] / СЗ РФ. 2015. № 5. Ст. 865.

[497] СЗ РФ. 2015. № 1 (Часть II). Ст. 284.

информационными системами, в том числе в части взаимодействия с единой системой идентификации и аутентификации.

В соответствии с частью $4^1$ статьи 14 Закона № 149-ФЗ Правительство Российской Федерации определяет случаи, при которых доступ с использованием Интернета к информации, содержащейся в государственных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе идентификации и аутентификации, а также порядок использования единой системы идентификации и аутентификации.

Правилами использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, утвержденными постановлением Правительства Российской Федерации от 10 июля 2013№ 584[498], определено, что зарегистрированные в федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – единая система) получают санкционированный доступ к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах.

---

[498] СЗ РФ. 2012. № 25. Ст. 3380.

Межведомственное взаимодействие, не предполагающее использования системы электронного документооборота, осуществляется путем обмена документированной информацией.

В соответствии с частью 2 статьи 11 Закона № 149-ФЗ документирование информации, не составляющей государственную тайну, осуществляется по правилам делопроизводства, установленным уполномоченным федеральным органом исполнительной власти в сфере архивного дела и делопроизводства.

Согласно пункту 3 Правил делопроизводства в федеральных органах исполнительной власти, утвержденных постановлением Правительства Российской Федерации от 15 июня 2009 г. № 477 «Об утверждении Правил делопроизводства в федеральных органах исполнительной власти»[499] (далее – Правила делопроизводства), федеральный орган исполнительной власти на основе Правил делопроизводства с учетом условий и специфики своей деятельности разрабатывает инструкцию по делопроизводству, утверждаемую руководителем органа по согласованию с федеральным органом исполнительной власти в области архивного дела.

В соответствии со статьей 16 Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»[500] (далее – Закон № 5485-1) взаимная передача сведений, составляющих государственную тайну, осуществляется органами государственной власти с санкции органа государственной власти, в распоряжении которого находятся эти сведения.

Органы государственной власти, запрашивающие сведения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений в соответствии с требованиями раздела VI Закона № 5485-1. Их руководители несут персональную

---

[499] СЗ РФ. 2009. № 25. Ст. 3060.
[500] СЗ РФ. 1997. № 41. Стр. 8220 – 8235.

ответственность за несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну.

Таким образом, действующим законодательством регулируются взаимодействие между различными государственными информационными системами в части межведомственного информационного взаимодействия федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, государственных внебюджетных фондов, в том числе в части взаимодействия с единой системой идентификации и аутентификации.

2.2.9 Выводы

В странах Европейского союза уделяется большое внимание вопросам информационного взаимодействия в публичном секторе: приняты нормативно-правовые основы; разработаны регламенты межведомственного взаимодействия; созданы технические условия для обмена данными между разными государственными системами; определены компетентные органы, ответственные за координацию информационного взаимодействия. Развивается концепция интероперабельности, означающая качественно новый подход к государственному управлению, основанный на информационном взаимодействии всех публичных органов в рамках единой экосистемы.

Безопасность информационного взаимодействия в странах ЕС обеспечивается национальной и наднациональной системами защиты критической информационной инфраструктуры, механизмами предотвращения инцидентов.

Основными механизмами государственного регулирования информационного взаимодействия в странах общего права (Австралии, Великобритании) и в Сингапуре являются:

– акты стратегического планирования (Стратегии развития информационно-коммуникационных технологий, Национальная правительственная стратегия обмена информацией и прочие),

– использование регулирования, основанного на общих принципах (principle-based legislation), подлежащих последующей имплементации государственными структурами,

– разработка фреймворков, предоставляющих набор инструментов и методов для реализации каждого принципа,

– отсутствие законов или актов делегированного нормотворчества, непосредственно регулирующих вопросы информационного взаимодействия и относящихся ко всем государственным информационным структурам,

– регулирование ключевых вопросов информационного взаимодействия (роли участников, вопросы управления, технические протоколы) в рамках отдельных проектов по интеграции данных публичного сектора.

2.3 Подходы к правовому регулированию унификации форматов представления информации и технологий информационного обмена в государственных информационных системах

2.3.1 Правовое регулирование в Европейском союзе

Европейское право не устанавливает единого технического регулирования во всех сферах деятельности государств-участников. Однако в некоторых сферах, имеющих значение для достижения и реализации целей создания ЕС, устанавливаются технические рекомендации и стандарты.

Регулирование в сфере унификации форматов и технических требований в финансовой сфере устанавливается на уровне ЕС самостоятельным органом контроля за финансовыми рынками ЕС – ESMA[501]. ESMA разрабатывает технические рекомендации и стандарты в финансовой

[501] European Securities and Markets Authority // https://www.esma.europa.eu/about-esma/who-we-are (дата обращения 22 04 2019)

сфере[502], а также ведет мониторинг и публикует информацию о соответствии им в отдельных государствах Союза. Например, ЕС принял Директиву 2004/109/ЕС от 15.12. 2004 о транспарентности информации для инвесторов на финансовых рынках[503], которой было введено требование о едином европейском формате финансовых отчетов, которые эмитенты, подпадающие под действие Директивы, обязаны ежегодно подавать. Европейской комиссией установлены технические стандарты единого формата уведомлений[504]. В соответствии с ее требованиями используется формат XHTML, не требующий дополнительных механизмов для обеспечения понятности содержимого и свободно распространяемый. Одновременно для обмена деловой информацией установлен открытый стандарт XBRL. EMSA готовит рекомендации о реализации указанных положений[505].

Директива 2007/2/ЕС от 14.03.2007 об установлении инфраструктуры пространственных данных в Европейском сообществе (INSPIRE)[506] также стала основанием унификации форматов, позволявшей упрощать обмен пространственными данными. В Директиве делается акцент на необходимости оценки значимости конкретного набора данных: наибольшей унификации подлежат в первую очередь форматы таких данных, которые

---

[502] https://www.esma.europa.eu/convergence/guidelines-and-technical-standards (дата обращения 03 09 2019)

[503] Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonization of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC // http://data.europa.eu/eli/dir/2004/109/oj (дата обращения 30 06 2019)

[504] Commission Delegated Regulation (EU) 2018/815 of 17 December 2018 supplementing Directive 2004/109/EC of the European Parliament and of the Council with regard to regulatory technical standards on the specification of a single electronic reporting format // http://data.europa.eu/eli/reg_del/2019/815/oj (дата обращения 10 04 2019)

[505] ESEF Reporting Manual. Preparation of Annual Financial Reports in Inline XBRL // https://www.esma.europa.eu/sites/default/files/library/esma32-60-254_esef_reporting_manual.pdf (дата обращения 26 05 2019)

[506] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) // http://data.europa.eu/eli/dir/2007/2/oj (дата обращения 07 04 2019)

используются или могут быть использованы наиболее широким кругом публичных органов и третьих лиц. В целях реализации Директивы принят обширный пласт технических рекомендаций, относящихся как ко всем данным в целом, так и к специфическим категориям (например, географические названия, океанографические географические данные, зоны естественного риска и т.п.)[507].

Технические документы общего характера устанавливают особенности имплементации Директивы INSPIRE в целом. В одном из таких документов - концептуальной модели INSPIRE[508], определяющей необходимые элементы гармонизации взаимодействия, указано, что для использования применяются стандарты ISO 19101. Документы ЕС дополняют ряд особенностей, не уточняемых этим стандартом, а также содержат обобщения. Наряду с моделью общее значение имеют Определения терминов[509], указывающие список тем, подпадающих под регулирование Директивы INSPIRE. Методология разработки спецификации данных[510] описывает процесс от разработки требований к пользователю до спецификации данных и предлагает методологическую базу, включая первичную разработку спецификации и последующее ее усовершенствование. Детализированное регулирование каждой из тем устанавливается тематическими спецификациями: например, по энергоресурсам, строениям, минеральным ресурсам и т.п.

---

[507] https://inspire.ec.europa.eu/Technical-guidelines3 (дата обращения 31 05 2019)

[508] INSPIRE Generic Conceptual Model, Version 3.4, 2014 // https://inspire.ec.europa.eu/documents/inspire-generic-conceptual-model (дата обращения 26 05 2019)

[509] Definition of Annex Themes and Scope (D 2.3, Version 3.0), 2008 // https://inspire.ec.europa.eu/documents/definition-annex-themes-and-scope-d-23-version-30 (дата обращения 11 06 2019)

[510] Methodology for the development of data specifications: baseline version (D 2.6, Version 3.0), 2008 // https://inspire.ec.europa.eu/documents/methodology-development-data-specifications-baseline-version-d-26-version-30 (дата обращения 28 06 2019)

Отдельно устанавливается ряд технических рекомендаций по сетевым сервисам, в том числе уточняющие используемые форматы и стандарты. Например, в технической рекомендации по сервисам загрузки[511] предусматривается, что при описании пространственного объекта координирующий орган предоставляет схему в формате XML для описания. При этом используется стандарт ISO 19142.

Внимание отведено и метаданным о пространственных данных. Регламентом Европейской комиссии о метаданных N 1205/2008 от 03.12.2008 [512] установлены особенности создания метаданных для различных наборов пространственных данных. В качестве используемого формата установлен XML, также даются рекомендации по идентификации и классификации пространственных данных и сервисов в метаданных.

Одновременно в рамках реализации положений европейских актов о данных в публичном секторе действует Европейский портал данных, предлагающий программы обучения созданию и использованию открытых данных. В рамках обучения рассматриваются также общие форматы открытых данных, наиболее используемые участниками – CSV, XML, KML, JSON и т.д.[513]

Таким образом, унификация форматов данных на уровне ЕС осуществляется в определенных сферах, исходя из специфики принимаемого европейского нормативного правового акта и его назначения.

---

[511] Technical Guidance for the implementation of INSPIRE Download Services, 2013 // https://inspire.ec.europa.eu/documents/technical-guidance-implementation-inspire-download-services (дата обращения 22 07 2019)

[512] Commission Regulation (EC) No 1205/2008 of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata (Text with EEA relevance) // http://data.europa.eu/eli/reg/2008/1205/oj (дата обращения 04 08 2019)

[513] https://www.europeandataportal.eu/en/resources/training-companion/open-data-formats (дата обращения 31 07 2019)

### 2.3.2 Особенности подхода к правовому регулированию в Германии

Принятая в ЕС Концепция интероперабельности служит основой унификации форматов информации и технологий ее обмена в государственном секторе Германии.

Советом планирования ИТ 02.09.2015 утверждена Программа стандартизации[514], призванная обеспечить создание и использование единых стандартов обмена данными в электронном виде, поскольку использование различных форматов данных, интерфейсов, оборудования и т.п. затрудняет взаимодействие между субъектами обмена данными и приводит к ошибкам в процессе обмена, потерям данных и их искажениям и т.п. Программа реализуется Координационным центром ИТ-стандартов (KoSIT), правовое положение которого определяется Концепцией создания KoSIT. Деятельность KoSIT контролируется консультационным советом, состоящим из представителей федерального правительства, правительств земель, местных администраций и Федерального ведомства информационной безопасности.

Германия ориентирована на стандартизацию посредством объединения заинтересованных сторон и создания открытых платформ для координации. Унификация формата обмена данными имеет смешанный характер, т.е. допустимо применять как единые, так и отраслевые стандарты. Обязанность операторов государственных информационных систем использовать единые стандарты и форматы данных также прослеживается в различных

---

[514] Standardisierungsagenda. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.pdf?__blob=publicationFile&v=2 (дата обращения 14.08.2019).

законодательных актах, в частности в Законе о повторном использовании информации государственного сектора (IWG)[515].

Среди национальных стандартов обмена данными выделяются:

XDOMEA[516] – стандарт обмена данными для документов, процессов и файлов, а также других связанных данных между различными системами администрирования. Стандарт учитывает процессы обмена информацией, ведения бизнеса, осуществления доставки, обмена файлами и данными.

XRechnung играет в Германии решающую роль в реализации Директивы 2014/55 EC об электронных платежах и является основой обмена электронными счетами с администрациями различного уровня.

XTA 2 разработан в целях безопасной и надежной передачи данных даже через принципиально небезопасный Интернет. Использование этого стандарта также имеет дополнительную ценность в защищенных сетях, таких как сквозная безопасность и адресация, или даже доказательство целостности сообщений, которые не охватываются только сетевым уровнем.

OSCI − стандарт протокола для безопасной, конфиденциальной передачи электронных данных в государственном секторе. Стандарт обеспечивает достижение целей защиты целостности, подлинности, конфиденциальности и отслеживаемости сообщений. В частности, OSCI используется в незащищенных сетях, таких как Интернет, но также предлагает дополнительные функции в защищенных сетях и, в частности, обеспечивает совместимость. OSCI Transport обеспечивает безопасное и

---

[515] GESETZ ÜBER DIE WEITERVERWENDUNG VON INFORMATIONEN ÖFFENTLICHER STELLEN. https://www.gesetze-im-internet.de/iwg/ (дата обращения: 10.08.2019)

[516] Sitzung des IT-Planungsrats vom 5. Oktober 2017. Entscheidung 2017/39. Standard für den Austausch von Akten, Vorgängen und Dokumenten. https://www.it-planungsrat.de/SharedDocs/Entscheidungen/DE/2017/Entscheidung_2017_39.html?nn=10144556 (дата обращения 11.08.2019)

бесперебойное использование сторонних приложений управления, которые могут быть аутентифицированы и идентифицированы электронными подписями на различных уровнях, в зависимости от требований законодательства бизнес-операций.

Lateinische Zeichen in UNICODE. ИТ-процедуры, используемые в государственной администрации Германии, в настоящее время различаются по количеству писем, которые могут быть обработаны и переданы. Заглавные буквы латинского алфавита, используемого в Германии, в основном поддерживаются, но существуют значительные различия в отношении ряда знаков, обычно используемых в других государствах ЕС. Это все чаще приводит к проблемам, потому что, в частности, имена лиц с необычными в Германии диакритическими знаками отражены в регистрах с электронным управлением по-разному. Это приводит к ошибкам в идентификации лиц в контексте автоматизированных процессов, что чревато высокими последующими затратами. Данным стандартом утвержден набор латинских символов, используемых на территории ЕС, в том числе при трансграничном обмене данными.

DCAT-AP.de действует в качестве общеобязательной основы обмена метаданными между немецкими порталами открытых данных. Данный стандарт широко применим. Законом о повторном использовании информации государственного сектора (IWG) предусмотрена обязанность поставщиков данных предоставлять запрашиваемые данные в совокупности с метаданными.

Целью стандарта XVergabe является создание условий для устойчивого подхода к созданию единого доступа к различным платформам государственных закупок. Между участниками, участвующими в торгах и платформами определен стандарт кроссплатформенного обмена данными, что должно привести к более широкому принятию участников торгов и, следовательно, к более активному участию в процессе цифрового взаимодействия.

XFall (разрабатывается и внедряется в одной из земель Германии – Нижней Саксонии, в дальнейшем будет расширено его применение на федеральном уровне) – это общий «транспортный» стандарт передачи данных для специальных нормативных процедур подачи заявок, в частности для передачи данных приложений между центральными прикладными платформами и децентрализованными, а следовательно, и различными специализированными процедурами.

С помощью стандарта XBau и XPlanung (оператор – земля Гамбург), процессы и нормы законодательства об общественных зданиях описываются на «техническом языке» строительных норм и правилах, а также законов о пространственном планировании. Это обеспечивает основу отображения всех требований к пространственному планированию в Германии и их реализации при построении правовых процедур в единой модели данных и формате файлов.

2.3.3 Особенности подхода к правовому регулированию во Франции

С административно-организационной точки зрения обязанности по унификации форматов взаимодействия возложены на DINU[517]. С одной стороны, Франция стремится сохранить свободу использования различных форматов и стандартов. С другой стороны, для унификации форматов и упрощения взаимодействия устанавливаются рекомендации о применяемых стандартах, а равно, когда речь идет о реализации единой цели взаимодействия, - установление более ограниченного круга форматов.

Выделим несколько предметов регулирования унификации форматов: унификацию форматов взаимодействия органов власти между собой и с

[517] В соответствии с информацией, указанной в книге 1, с 25 октября 2019 г. указанные полномочия осуществляются Межведомственной дирекцией по цифровому развитию (DINU). Ранее они осуществлялись Межведомственной дирекцией по взаимодействию государственных информационных систем (DINSIC).

физическими, юридическими лицами; унификацию форматов размещения информации органами власти на их сайтах в Интернете.

Постановлением от 20.04.2016[518] утверждена справочная информация по системам взаимодействия (RGI, V2.0)[519]. Она охватывает взаимодействие в трех основных группах отношений: между органами власти, между органами власти и организациями, между органами власти и физическими лицами. Стандарт уточняет, что для внутренних нужд органы власти свободно определяют, какие нормы и стандарты будут применяться. Одновременно рекомендуется следовать предлагаемым RGI стандартам по умолчанию. В остальных случаях положения RGI являются обязательными к исполнению органами власти.

RGI выделяет ряд уровней взаимодействия. Политический и юридический уровни обеспечивают формирование общих норм взаимодействия. Организационный уровень детально определяет действия участников взаимодействия. Семантический уровень охватывает значения слов и отношения между ними, а также весь жизненный цикл информации, включая сбор и декомпозицию. Технический уровень условно делится на две части: протоколы обмена информацией и синтаксис (форматы данных, обеспечивающие их передачу, вне зависимости от их содержания). В справочную информацию, таким образом, включены разделы: 2. Организация требований взаимодействия; 3. Взаимодействие техническое; 4. Взаимодействие синтаксическое; 5. Взаимодействие семантическое.

---

[518] Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité // https://www.legifrance.gouv.fr/eli/arrete/2016/4/20/PRMJ1526716A/jo/texte (дата обращения 28 10 2019)

[519] Référentiel Général d'Interopérabilité V2 version, 2015 // https://references.modernisation.gouv.fr/sites/default/files/Referentiel_General_Interoperabilite_V2.pdf )дата обращения 15 10 2019)

Критерии отбора стандартов для рекомендации установлены в п. 1.7. RGI. Они включают открытость, релевантность, надежность (стандарт уже используется в технической среде, и его применение не вызывает значительных проблем), технологическую независимость от каких-либо устройств или технологических инфраструктур, легкость применения (не требуется значительных затрат), а также признанность отраслью. Для краткого описания каждого из отобранных по указанным критериям стандартов дается ссылка на Wikipedia. Такой подход аргументирован тем, что RGI не будет так часто обновляться. Постоянное же обновление Wikipedia позволит получить наиболее исчерпывающую информацию о предлагаемом стандарте. Каждому предлагаемому стандарту также дается указание статуса (на наблюдении, рекомендуемый, устаревающий, неиспользуемый), кратко характеризующее его применимость в отрасли. Так, например, рекомендуемые форматы для документов – PDF, ODF, DocBook, PDF-A. На наблюдении находятся форматы OOXML, EPUB3. Для организации данных рекомендуются XML, XSD, JSON, OData, LDIF. DSML указан как устаревающий.

Кроме того, RGI включает профили взаимодействия. Профиль взаимодействия – набор стандартов, подобранных по совместимости для реализации конкретной цели. Выбор иных стандартов ограничен в связи с необходимостью избежать использования разных форматов. Например, профиль взаимодействия P3 «Коммуникации межличностные и бюрократические» предусматривает возможность использования файлов в форматах PDF и ODF. При этом PDF указывается в качестве основного формата для документов, изменение содержания которых не требуется, а ODF – для документов с изменяемым содержанием.

Таким образом, французский подход к правовому регулированию унификации форматов информации строится на основе централизованного регулирования специально созданным административным органом (DINU), определения общих рекомендаций по возможности употребления форматов.

### 2.3.4 Особенности подхода к правовому регулированию в Эстонии

Унификация форматов информации и технологий информационного обмена в государственных информационных системах основана на общеевропейской концепции интероперабельности[520], в которой повышенное внимание уделяется стандартизации. В европейской концепции интероперабельности выделяются шесть этапов внедрения стандартов: определение необходимых стандартов с учетом имеющихся потребностей; оценка выбранных стандартов на предмет их прозрачности, недискриминационности и т.п.; имплементация стандартов; мониторинг соблюдения; управление развитием стандартов; документирование стандартов и размещение их в открытых каталогах. Такая сложная структура стандартизации призвана обеспечить её прозрачность. Открытость предполагает участие всех заинтересованных лиц в разработке, совершенствовании и общественном обсуждении стандартов/спецификаций, их доступность любому лицу, а также предоставление права на использование этих стандартов (спецификаций, форматов) на честных, разумных и недискриминационных условиях (FRAND – fair, reasonable and non-discriminatory). Открытость стандартизации в государственных информационных системах означает также, что техническая инфраструктура информационного взаимодействия должна по возможности быть основана на открытом программном обеспечении, а государство, в свою очередь, должно оказывать поддержку сообществам разработчиков такого программного обеспечения.

Перечисленные требования получили развитие в Принципах интероперабельности государственной информационной системы,

---

[520] European Interoperability Framework. https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf (дата обращения: 07.08.2019).

разработанных Министерством экономики и коммуникаций[521]. Данное министерство определяет потребности публичных органов в стандартах в сфере IT, продвигает стандарты, распространяет о них информацию и т.п. Непосредственно же разработкой стандартов, адаптацией международных стандартов занимается Центр стандартизации[522] (технический комитет) в сотрудничестве с Международной организацией стандартизации (International Organization for Standardization, ISO), Совместным комитетом по IT (IT Joint Committee, JTC1) Международной электротехнической комиссией (International Electrotechnical Commission, IEC), Ассоциацией в сфере IT (IT Association CEN/ISSS) при Европейском комитете стандартизации (European Committee for Standardization, CEN).

Большая часть стандартов Эстонии в сфере электронного документооборота разработана техническим комитетом стандартизации EVS/TK 22 «Information and documentation» на основе стандартов ISO/TC 46 и ISO/TC 171.

В Принципах интероперабельности государственной информационной системы, а также в Цифровой повестке 2020 для Эстонии[523] указывается, что публичный сектор должен быть активным членом IT-сообществ в сфере стандартизации, участвовать в международных организациях по стандартизации.

В Эстонии установлен минимальный набор открытых стандартов, которые обязаны использовать публичные органы, а также открытые

---

[521] Interoperability of the State Information System. https://www.mkm.ee/sites/default/files/interoperability-framework_2011.doc (дата обращения: 21.08.2019).

[522] Estonian Centre for Standardisation. https://www.evs.ee/ (дата обращения: 21.08.2019).

[523] DIGITAL AGENDA 2020 FOR ESTONIA // Режим доступа: https://www.mkm.ee/sites/default/files/digitalagenda2020_final_final.pdf (дата обращения: 21.08.2019).

стандарты, которые рекомендуется использовать при разработке информационных систем. Ниже приведены некоторые открытые форматы, которые публичные органы обязаны использовать при взаимодействии друг с другом и с третьими лицами (орматы предусмотрены в Принципах интероперабельности государственной информационной системы):

– CSV (Comma Separated Value [.csv]) – формат постраничных файлов,

– HTML (HyperText Markup Language [.html]) – гипертекстовый язык для создания веб-документов,

– BDOC – digital signature format (Estonian standard EVS 821:2009) – формат цифровой подписи,

– JPEG (Joint Photographic Experts Group [.jpg]) – графический формат,

– GZIP – формат архива,

– MPEG (Moving Picture Experts Group [.mpeg]) – видео формат (MPEG4/ISO/IEC 14496),

– ODF (Open Document Format [.odf]) – открытый формат для офисных приложений,

– PDF (Portable Document Format [.pdf]) – формат документов,

– PDF/A (Portable Document Format/Archive) – формат архива документов .pdf,

– PNG (Portable Network Graphics [.png]) – формат растровой графики,

– SVG (Scalable Vector Graphic [.svg]) – формат векторной графики,

– XML (Extensible Hypertext Markup Language [.xml]) – гипертекстовый язык.

В некоторых нормативно-правовых актах Эстонии непосредственно закрепляется формат предоставления информации для определенных целей. Например, в Требованиях к доступности веб-сайтов и мобильных

приложений и правилах опубликования информации о доступе[524] установлено, что веб-сайты и мобильные приложения публичных органов должны быть воспринимаемыми, работоспособными, понятными и надежными. При этом презюмируется, что веб-сайт или приложение отвечают требованиям доступности, если они соответствуют стандарту – имеется в виду European standard EN 301 549 V2.1.2 (2018-08). В Требованиях к конвертации документов в электронной форме в электронные базы данных[525], позволяющие обеспечивать удобный доступ к информации, закреплены требования к формату, метаданным, структуре предоставляемых в налоговые органы документов. Установлено, что заявитель обязан представлять файлы в форматах del, .csv, .txt, .prn или в иных форматах, которые одобрены налоговым органом.

Актом о бухгалтерском учёте[526] предусмотрено, что с 1.07. 2019 в сфере публичных закупок должны использоваться только электронные счета в машиночитаемом формате. Информация предоставляется в соответствии с конкретным стандартом − EVS 923: 2014 (национальном стандартом, основанном на формате XML) либо европейским стандартом в сфере электронного выставления счетов[527]. При этом не предусмотрено использование единственного программного обеспечения обработки

---

[524] Requirements for the accessibility of websites and mobile applications, and the rules for publishing information describing accessibility https://www.riigiteataja.ee/en/eli/ee/EVIM/reg/512042019003/consolide (дата обращения: 14.08.2019).

[525] The requirements for the conversion of the documents preserved in electronic form into electronic databases allowing excess to legible information. https://www.riigiteataja.ee/en/eli/ee/RHM/reg/524092014007/consolide (дата обращения: 21.08.2019).

[526] Accounting Act. https://www.riigiteataja.ee/en/eli/517012017005/consolide (дата обращения: 21.08.2019).

[527] CEN/TC 434 - Electronic Invoicing: https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:1883209,25&cs=126F1BDBC8D6D6141F550EB578B4A9CF4 (дата обращения: 21.08.2019).

электронных счетов – публичные органы и организации вправе выбирать любую из доступных на рынке платформ, связанных между собой соглашениями об обмене информацией[528].

Таким образом, в Эстонии уделяется большое внимание вопросам стандартизации и унификации форматов (технологий) информационного взаимодействия. Большая часть форматов разрабатывается на основе международных стандартов. В законодательстве также содержатся прямые ссылки на использование того или иного формата (стандарта) при информационном взаимодействии в публичном секторе.

2.3.5 Особенности подхода к правовому регулированию в Великобритании

Вопрос о соотношении технико-юридических и правовых норм и, как следствие, нормативных правовых и нормативных технических актов актуален в российской теории права[529]. Подобный теоретический вопрос не является однако актуальным для британской доктрины. Указанное не препятствует должному регулированию унификации форматов представления информации, в том числе и через использование юридически-обязательных технических стандартов.

Правовые основания унификации форматов представления информации в государственных информационных системах содержатся в Принципах открытых стандартов[530], программном документе (Policy paper) опубликованном секретариатом Кабинета (Cabinet Office).

---

[528] eInvoicing in Estonia. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eInvoicing+in+Estonia (дата обращения: 21.08.2019).

[529] См. например: Ковалева Н.В. Природа и функции технико-юридических норм // Государство и право. 2016. № 11. С. 5-12.

[530] Open Standards Principles. https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (дата обращения: 05.08.2019).

Указанный документ содержит набор принципов, на которых должен основываться выбор стандартов. Из указанного акта можно вывести следующие основные требования к таким стандартам, которые должны:

– соответствовать потребностям пользователя,

– обеспечивать равный доступ поставщиков к государственным контрактам,

– быть гибкими и способными к изменениям,

– быть обоснованными,

– быть транспарентными.

Выбор унифицированных форматов (стандартов) предоставления информации государственными органами тоже должен основываться на указанных принципах.

Совет стандартизации (Open Standards Board)[531], созданный Комитетом эффективности государственных расходов (Public Expenditure Committee (PEX(ER) с целью содействия секретариату Кабинета в сфере стандартизации, в который входит, в частности, представитель Цифровой службы (GDS), утвердил ряд нижеперечисленных стандартов, обязательных к использованию государственными органами:

– Руководство по обмену с государственными документами (Guidance: Sharing or collaborating with government documents, 2019)[532], устанавливающее стандарт ODF 1.2 для обмена документами между (с) государственными органами,

---

[531] https://www.gov.uk/government/groups/open-standards-board (дата обращения: 18 07 2019)

[532] Guidance: Sharing or collaborating with government documents, 2019. https://www.gov.uk/government/publications/open-standards-for-government/sharing-or-collaborating-with-government-documents (дата обращения: 05.08.2019).

– Руководство к просмотру государственных документов (Guidance: Viewing government documents, 2019)[533], которое устанавливает стандарт HTML5 (или PDF/A-1 ISO/IEC 19005-1:2005 и PDF/A-2 ISO/IEC 19005-2:2011) для долгосрочного хранения) для доступа лиц к опубликованным государственным документам,

– Руководство по обмену информацией о киберугрозах (Guidance: Exchanging Cyber Threat intelligence, 2019)[534], которое устанавливает два стандарта для использования специалистами в сфере анализа киберугроз: STIX 2 и TAXII 2.

– Руководство по публикации данных о грантах (Guidance: Publishing grant data, 2019)[535], которое вводит стандарт Three Sixty Giving для публикации информации о грантах. Стандарт основывается на стандартах (совместим со стандартами) JSON, CSV, UTF-8, ISO 8601,

– Руководство по стандарту кросс-платформенной кодировки (Guidance: Cross platform character encoding profile, 2019)[536], которое вводит стандарт UTF-8 для исключения перекодировки текстовой информации при передаче из одной платформы на другую,

---

[533] Guidance: Viewing government documents, 2019. https://www.gov.uk/government/publications/open-standards-for-government/viewing-government-documents (дата обращения: 05.08.2019).

[534] Guidance: Exchanging Cyber Threat intelligence, 2019. https://www.gov.uk/government/publications/open-standards-for-government/exchanging-cyber-threat-intelligence (дата обращения: 05.08.2019).

[535] Guidance: Publishing grant data, 2019. https://www.gov.uk/government/publications/open-standards-for-government/data-standard-for-grant-making (дата обращения: 05.08.2019).

[536] Guidance: Cross platform character encoding profile, 2019. https://www.gov.uk/government/publications/open-standards-for-government/cross-platform-character-encoding-profile (дата обращения: 05.08.2019).

– Руководство по открытым данным о контрактах (Guidance: Open contracting data, 2019)[537], которое вводит формат OCDS V.1.1 для предоставления метаданных о заключении государственных контрактов. При этом сами документы в системе могут содержаться в иных релевантных форматах, например, PDF,

– Руководство по размещению вакансий (Guidance: Publishing vacancies, 2019)[538] , которое утверждает формат JobPosting при размещении в HTML описания вакансии,

– Руководство по обмену данными о местоположении (Guidance: Exchange of location point, 2019)[539], которое утверждает формат ETRS89 (EPSG:4258) для Европы и WGS 84 для остального мира в целях обмена информацией о местоположении,

– Руководство по постоянным идентификаторам (Guidance: Persistent resolvable identifiers, 2019)[540], которое утверждает стандарты HTTP 1.1 и URL для идентификации сайтов.

Существуют и иные, менее релевантные стандарты.

Среди рекомендуемых стандартов в сфере информационной безопасности, которые не утверждают форматов файлов, но содержат ряд иных требований, нужно упомянуть: ISO 27001 (информационная

---

[537] Guidance: Open contracting data, 2019. https://www.gov.uk/government/publications/open-standards-for-government/open-contracting-data-standard-profile (дата обращения: 05.08.2019).

[538] Guidance: Publishing vacancies, 2019. https://www.gov.uk/government/publications/open-standards-for-government/publishing-vacancies-online-standards-profile--2 (дата обращения: 05.08.2019).

[539] Guidance: Exchange of location point, 2019. https://www.gov.uk/government/publications/open-standards-for-government/exchange-of-location-point (дата обращения: 05.08.2019).

[540] Guidance: Persistent resolvable identifiers, 2019.: https://www.gov.uk/government/publications/open-standards-for-government/persistent-resolvable-identifiers (дата обращения: 05.08.2019).

безопасность)[541] и BS 10012 PIMS (система управления персональными данными)[542].

Таким образом, в Великобритании в рамках централизованной модели обмена данными (с использованием системы GOV.UK) решена задача унификации форматов предоставления и обмена информацией, что достигнуто путем издания принципов и стандартов, представляющих собой нормативно-технические акты, содержащие юридические и технические нормы, относящиеся к органам публичной власти.

2.3.6 Особенности подхода к правовому регулированию в Австралии

В Австралии разработан ряд документов, направленных на унификацию отдельных аспектов по обработке информации.

Концепция цифрового развития Австралии определена Стратегией цифровой трансформации[543], разработанной Агентством цифровой трансформации[544]. Стратегия цифровой трансформации определяет цели развития на период до 2025 для трех стратегических приоритетов:

– «правительство, с которым легко иметь дело»,
– «правительство, информированное вами»,
– «правительство, соответствующее цифровой эпохе».

Первое направление развития предусматривает оказание гражданам всех государственных услуг в электронном виде, а также электронную идентификацию физических лиц для предоставления доступа к указанным услугам.

---

[541] ISO/IEC 27001:2013 Preview Information technology. Security techniques. Information security management systems. Requirements. https://www.iso.org/standard/54534.html (дата обращения: 05.08.2019).

[542] BS 10012 - The standard for a personal information management system (PIMS). https://www.itgovernance.co.uk/bs10012_pims (дата обращения: 05.08.2019).

[543] Digital Transformation Strategy. https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-transformation-strategy/digital-transformation-strategy.pdf (дата обращения: 30.08.2019).

[544] https://www.dta.gov.au/about-us (дата обращения: 30.08.2019).

Второй приоритет предусматривает развитие электронных услуг на основе политики, опирающейся на данные и аналитику, а также адаптацию этих услуг к потребностям граждан.

Третий приоритет декларирует соответствие передовому опыту развития в области электронных технологий, использование современного технического опыта и методов деятельности. Инициативы и меры реализации приоритетов развития электронных услуг определены Дорожной картой[545], являющейся составной частью Стратегии цифровой трансформации.

В части унификации форматов информации и технологий информационного обмена в рамках реализации Дорожной карты приняты:

1) Стандарт цифровых услуг[546]

Стандарт направлен на применение улучшение разработки и оказания государственных услуг с целью достижения их простоты, ясности и своевременности. Стандарт устанавливает 13 критериев услуг:

– построение сервисов на основе глубокого понимания потребностей пользователей и среды использования,

– создание междисциплинарной команды под управлением опытного менеджера по продукту для разработки, создания, эксплуатации и улучшения сервисов,

– проектирование и создание сервисов на основе гибкого и клиенто-ориентированного процесса,

– понимание инструментов и систем, необходимых для создания, размещения, эксплуатации и оценки услуг, а также способов их адаптации и применения,

---

[545] Roadmap. https://www.dta.gov.au/digital-transformation-strategy/roadmap-page (дата обращения: 30.08.2019).

[546] Digital Service Standard. https://www.dta.gov.au/help-and-advice/about-digital-service-standard (дата обращения: 30.08.2019).

– понимание данных и информации в рамках сервиса с определением соответствующих правовых мер, мер конфиденциальности и безопасности,

– использование адаптивных методов проектирования с применением общих схем для проектирования и руководства по стилю,

– максимальное использование открытых стандартов и общих государственных платформ,

– открытие новых кодов по умолчанию,

– доступность сервиса всем пользователям независимо от их возможностей и среды,

– тестирование сервисов в среде, полностью отображающей реальность,

– измерение и публикация данных о реальной результативности сервиса в сопоставлении с заявленной,

– обеспечение альтернативных каналов доступов к сервисам,

– поощрение пользователей к использованию выбранной цифровой услуги.

2) Стратегия платформы цифровых услуг[547]

Стратегия определяет лучшие методы для увеличения всесторонности и последовательности государственных услуг. Стратегия предназначена для подразделений государственных органов, которые создают платформы цифровых сервисов и управляют ими.

Оказание государственных услуг в соответствии со Стратегией платформы для цифровых услуг предусматривает применение подхода «Совокупного правительства» (a whole-of-government approach, WofG). Цифровые платформы WofG включают ряд технологий, которые позволяют государственным органам разрабатывать, обмениваться и подключать услуги

[547] Digital Service Platforms Strategy. URL: https://www.dta.gov.au/book/export/html/769 (дата обращения: 30.08.2019).

без необходимости самим проектировать, тестировать и эксплуатировать базовые системы. Ключевой характеристикой цифровых платформ WofG является то, что они являются многократно используемыми «строительными блоками» для построения простых и общих информационных сервисов. Доступ к ним осуществляется через простые, общегосударственные API, которые, в свою очередь, обеспечивают доступ к базовой инфраструктуре и могут быть легко заменены при необходимости.

3) Руководство стратегии информационного содержания[548]

Руководство устанавливает основу создания, структурирования и управления информационным содержанием сервисов. Руководство охватывает:

– понимание экосистемы контента,
– запуск контентной стратегии,
– идентификацию потребностей, связанных с деятельностью,
– идентификацию потребностей пользователей контента,
– аудит контента,
– установление целей и измерение успешности контентной стратегии,
– установление модели управления контентом,
– устранение избыточности контента,
– улучшение информационной архитектуры,
– стратегию оптимизации поиска информации,
– выбор и конфигурирование системы менеджмента контентом,
– управление запросами контента,
– управление неотложными (срочными) запросами контента.

4) Руководство по информационному содержанию[549]

---

[548] Content Strategy Guide. https://guides.service.gov.au/content-strategy/ (дата обращения: 30.08.2019).

Руководство предназначено для помощи государственным органам в простом, ясном и быстром создании контента. Руководство охватывает:

– структурирование контента,
– стиль написания,
– доступность и инклюзивность,
– знание пунктуации и грамматики,
– знание терминов и словесных оборотов,
– применение цифр и чисел,
– правила форматирования,
– виды контента,
– правила для поисковых движков,
– рекомендации по применению самого Руководства,
– разработку контентной стратегии.

5) Руководство по стилю[550]

Руководство по стилю было первым общегосударственным руководством такого рода. Оно было опубликовано в 1966 г. В настоящее время готовится его 7-е издание, призванное отразить современный стиль и требования к государственным изданиям, применимые ко всем правительственным учреждениям.

Государственные данные по умолчанию должны публиковаться с соблюдением открытых стандартов[551]. В частности, разрешенные для использования соответствии с указанными стандартами файлы должны быть в формате:

---

[549] Content Guide. https://guides.service.gov.au/content-guide/ (дата обращения: 30.08.2019).

[550] Style Manual. https://www.dta.gov.au/our-projects/style-manual (дата обращения: 30.08.2019).

[551] https://toolkit.data.gov.au/Publishing_your_data.html#Standards (дата обращения: 30.08.2019).

– таблицы − CSV, XLS, or XLSX,

– записи пространственных данных − KML, WMS, WFS,

– записи текстовых данных − TXT, RTF, ODT, DOC или DOCX, PDF.

Для унификации форматов информации и технологий информационного обмена предусмотрено применение стандартов следующих органов по стандартизации:

– Международная организация по стандартизации[552],

– Открытый геопространственный консорциум[553],

– Национального органа стандартизации[554].

Применяемые при унификации форматов информации и технологий информационного обмена австралийские стандарты включают:

– AGLS[555] (National Archives standard for making online information and services visible, manageable and interoperable),

– ANZLIC[556] Spatial Metadata Profile,

– SDMX[557] (Statistical Data and Metadata Exchange standard managed by the Australian Bureau of Statistics),

– AIXM[558] (Aeronautical Information Exchange Model standard),

– AS/NZS4819[559] Rural and Urban Addressing,

– AS 4590[560] Interchange of client information.

---

[552] https://www.iso.org/standards-catalogue/browse-by-ics.html (дата обращения: 30.08.2019).

[553] http://www.opengeospatial.org/standards (дата обращения: 30.08.2019).

[554]: https://www.standards.org.au/ (дата обращения: 30.08.2019).

[555] http://www.agls.gov.au (дата обращения: 30.08.2019).

[556] https://www.anzlic.gov.au/ (дата обращения: 30.08.2019).

[557] https://www.abs.gov.au/ausstats/abs@.nsf/Lookup/1407.0.55.002main+features22013 (дата обращения: 30.08.2019).

[558] : http://www.aixm.aero/page/versions (дата обращения: 30.08.2019).

[559] https://www.standards.org.au/standards-catalogue/sa-snz/communication/it-004/as-slash-nzs--4819-2011 (дата обращения: 30.08.2019).

[560] http//www.standards.org.au/standards-catalogue/sa-snz/communication/it-004/as--4590-dot-1-colon-2017 (дата обращения: 30.08.2019).

Дорожной картой также запланировано принятие стандарта на API-интерфейсы (планировалось на период июль 2018 г. - июнь 2019 г., но на текущий момент не выполнено).

Для отдельных операций с данными разработаны специальные руководящие документы, которые направлены на унификацию форматов информационного взаимодействия в рамках конкретных проектов. Круг лиц, на который распространяются те или иные акты, определяется непосредственно в самих актах. Агентство цифровой трансформации разрабатывает платформы и инструменты, помогающие государственным органам повышать качество цифровых услуг. В рамках проекта «Цифровая личность» (Digital Identity) Агентством были разработаны рамки де-идентификации данных[561], которые является результатом адаптации британского Руководства к принятию решений по анонимности (The Anonymisation Decision-Making Framework) и выполняет роль практического руководства по де-идентификации для государственных органов и предприятий, включая некоммерческие организации и организации частного сектора. Данные рамки не являются пошаговым механизмом и скорее направлены на формирование единообразного подхода в анализе и контроле над рисками для конфиденциальности, а также в принятии обоснованных решений при взаимодействии с заинтересованными сторонами.

Другим примером являются Рамки надежной цифровой идентификации[562], которые предлагают набор правил и стандартов, которым должны следовать аккредитованные члены при цифровой идентификации. В

---

[561] The De-Identification Decision-Making Framework https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS3 (дата обращения 18 07 2019)

[562] Trusted Digital Identity Framework. https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework (дата обращения 12 09 2019)

настоящее время рамки включают 19 политик, среди которых «обзор архитектуры»[563], который описывает функции участников и их взаимодействие, профили общих характеристик провайдеров идентификации и цифровых услуг[564], требования к тестированию технической интеграции[565] и сервисных операций[566] и др.

Унификацию подходов и процедур управления информацией курирует Национальный архив, играющий ключевую роль в реализации правительственных инициатив по преобразованию цифровых технологий и стимулированию электронного правительства. Национальный архив руководит реализацией политики «Цифровой непрерывности 2020» (The Digital Continuity Policy 2020), в рамках которых разработан ряд документов, направленных на единообразное проведение государственной политики в области управления информацией. Реализация указанной политики дала толчок к разработке значительного количества стандартов в области управления информацией и совместимости данных.

Среди таковых следует упомянуть политику защиты информации[567] - руководящие указания по реализации государственной политики в области управления безопасностью, безопасности персонала, физической

---

[563] Architecture Overview. https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-architecture-overview.pdf (дата обращения 12 09 2019)

[564] Attribute Profile. https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-attribute-profile.pdf (дата обращения 10 09 2019)

[565] Technical Integration Testing Requirements. https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/Trusted%20digital%20identity%20framework%202/Technical%20Integration%20Testing%20Requirements.pdf дата обращения (16 08 2019)

[566] Service Operations Testing Requirements. https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/Trusted%20digital%20identity%20framework%202/Service%20Operations%20Testing%20Requirements.pdf (дата обращения 10 09 2019)

[567] The Protective Security Policy Framework.: https://www.protectivesecurity.gov.au/Pages/default.aspx (дата обращения 10 09 2019)

безопасности и информационной безопасности. Указания включают блоки «управление», «безопасность персонала», «информационная безопасность», «физическая безопасность». Каждый блок реализован через набор утвержденных политик, например в рамках блока «информационная безопасность» разработаны политики, подлежащие применению ко всем информационным активам, принадлежащим австралийскому правительству, или активам, доверенным австралийскому правительству третьими сторонами в пределах Австралии: «Конфиденциальная и секретная информация», «Доступ к информации», «Защита информации от киберугроз», «Надежные ИКТ системы»[568].

Другим примером реализации заложенного в Политике Цифровой непрерывности 2020 принципа совместимости данных является Стандарт метаданных правительства Австралии (Версия 2.2)[569], который описывает структурированные способы внесения записей, собираемых и используемых в федеральных государственных органах, призванных обеспечивать высокую степень достоверности электронных систем учета и метаданных, их подлинность и удобство использования.

Офис Информационного комиссара (OAIC) также рекомендует использовать международные источники регулирования вопросов стандартизации[570]. Среди таковых упоминаются Рекомендация ОЭСР по управлению рисками цифровой безопасности для экономического и

---

[568] Information security. Core requirements. URL: https://www.protectivesecurity.gov.au/information/Pages/default.aspx (дата обращения 15 10 2019)

[569] Australian Government Recordkeeping Metadata Standard. URL: http://www.naa.gov.au/Images/AGRkMS-Version-2.2-June-2015_tcm16-93990.pdf (дата обращения 11 08 2019)

[570] Guide to Securing Personal Information. URL: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/#appendix-b-additional-resources (дата обращения 15 10 2019)

социального процветания[571], международные стандарты, опубликованные Международной организацией стандартизации (ISO)[572].

В целом унификация форматов информации и технологий информационного обмена в государственных информационных системах обеспечивается путем принятия руководящих положений, стандартов. Поскольку разработка и поддержка имплементации указанных документов осуществляется в рамках отдельных программ, акты о стандартизации принимаются различными государственными органами.

2.3.7 Особенности подхода к правовому регулированию в Сингапуре

Управление государственными информационными ресурсами и системами осуществляется в рамках национальной инициативы «Умная нация» (Smart nation), определяющей три направления деятельности государственных органов в сфере информатизации:

– цифровая экономика,
– цифровое государство,
– цифровое общество.

В рамках направления «Цифровая экономика» действуют Принципы реализации цифровой экономики (DIGITAL ECONOMY FRAMEWORK FOR ACTION), устанавливающие основные логические и организационные правила работы с данными.

В рамках направления «Цифрового государства» действует Схема работы цифрового государства (Digital Government Blueprint), описывающая принципы и цели работы государственного сектора в электронной среде.

---

[571] Digital Security Risk Management. URL: http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm (дата обращения 06 07 2019)

[572]ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT. URL: https://www.iso.org/isoiec-27001-information-security.html (дата обращения 06 07 2019)

В рамках направления «Цифрового общества» программным документом является Схема цифровой готовности населения (Digital Readiness Blueprint).

Программа реализуется профильными органами исполнительной власти – Группой развития Умной нации и цифрового государства (Smart Nation and Digital Government Group; SNDGO) и Государственным технологическим агентством (Government Technology Agency (GovTech)). Данные органы подчинены непосредственно Премьер-министру.

Более детально принципы унификации форматов работы с государственной информацией для частного сектора излагают документы Государственного технологического агентства, в том числе:

- Руководство по цифровизации однородных органов (Ministry Family Digitalisation Guide),
- Стандарты цифровых услуг (Digital Service Standards,
- Технический стек Правительства Сингапура (Singapore Government Tech Stack).

Таким образом, унификация форматов информации и технологий информационного обмена в государственных информационных системах в Сингапуре обеспечивается государственными органами на основе общих рекомендаций и стандартов.

2.3.8 Особенности подхода к правовому регулированию в Российской Федерации

Законодательством Российской Федерации не установлены общие нормы унификации данных в государственных информационных системах, однако действуют различные отраслевые требования к форматам данных в государственных информационных системах (в основном реализуется структурирование данных посредством формата XML) и технологии унификации указанных форматов.

В соответствии с частью 3 статьи 14 Закона № 149-ФЗ государственные информационные системы создаются и эксплуатируются на основе

статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

В отношении ряда государственных информационных систем действуют отдельные нормативные правовые акты, определяющие форматы предоставления в них сведений.

Так, приказом Минэкономразвития России от 5 июня 2018 № 286 «Об утверждении формата предоставления сведений годовой бухгалтерской (финансовой) отчетности юридических лиц Федеральной службой государственной статистики в рамках межведомственного информационного взаимодействия»[573] установлен формат таких сведений.

Приказом Росстата от 17 апреля 2018 №179 «Об утверждении порядка сбора сведений о населении в электронной форме, определяющего требования к программному обеспечению, техническим средствам, включая носители информации, каналам связи, средствам защиты и форматам представления данных в электронной форме»[574] утверждены требования к форматам предоставления сведений о населении посредством Единого портала государственных и муниципальных услуг (функций).

Приказом Росстата от 7 июля 2011 №313 «Об утверждении Унифицированного формата транспортного сообщения при обмене электронными документами между территориальными органами Росстата и респондентами»[575] определены форматы электронного документооборота в рамках сдачи первичных статистических данных через систему сбора статистической отчетности.

---

[573] http://www.pravo.gov.ru. 2018.
[574] http://www.pravo.gov.ru. 2018.
[575] http://gks.ru.

Приказом Минэнерго России от 3 августа 2015 № 536 «Об утверждении требований к технологиям информационного взаимодействия в интеграционном сегменте государственной информационной системы топливно-энергетического комплекса, в том числе к форматам представления информации в рамках данного сегмента государственной информационной системы топливно-энергетического комплекса»[576] утверждены требования к технологиям информационного взаимодействия в интеграционном сегменте ГИС ТЭК.

Форматы предоставления данных в различные государственные информационные системы различаются, что является препятствием к обеспечению информационного взаимодействия государственных информационных систем.

2.3.9 Выводы

Стандартизация форматов является ключевым направлением развития интероперабельности в странах ЕС.

В некоторых сферах (например, в финансовом секторе, в налоговых отношениях) в правовых актах стран ЕС закреплены стандарты, которые должны использовать государственные органы и хозяйствующие субъекты при информационном взаимодействии.

Особенностью подходов к регулированию унификация форматов в странах общего права и Сингапуре является разработка принципов, стандартов и руководств, которые позволяют государственным структурам решить задачу унификации форматов. В ряде случаев такие документы носят обязательный характер (например, требования к интернет-сайтам правительства), в иных – дают возможность структурам-владельцам

[576] http://www.pravo.gov.ru. 2015.

информационных систем самостоятельно разработать регулирующие документы, руководствуясь положениями руководящих принципов.

2.4 Подходы к выявлению и разрешению противоречий в данных, содержащихся в различных государственных информационных системах

2.4.1 Общие подходы в праве Европейского союза

В европейском праве нет общих положений по выявлению и устранению противоречий в данных из европейских информационных систем. Выявление и разрешение противоречий может осуществляться в рамках законодательства о персональных данных по инициативе самого субъекта персональных данных.

В основе управления персональными данными в европейском праве сохраняется подход, установленный GDPR[577], при котором любой субъект персональных данных имеет право узнать, какие его данные обрабатываются, и при необходимости потребовать их уточнения или удаления. Особенностям исправления и изъятия данных посвящена секция 3 Регламента. Ст. 16 дает субъекту персональных данных право получить от оператора без дополнительных задержек исправление недостоверных данных, относящихся к нему. Принимая во внимание цели обработки, субъект персональных данных также имеет право требовать дополнить недостающие данные, в том числе посредством дополнительного заявления. Ст. 17 также дает право требовать удаления данных в определенных случаях. Данное право получило название права «быть забытым».

Среди оснований удаления выделим отзыв согласия субъектом персональных данных, достижение цели, для которой данные были собраны

[577] 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) (Text with EEA relevance) // http://data.europa.eu/eli/reg/2016/679/oj (дата обращения 26 09 1019)

или обрабатываются, неправомерную обработку, обработку для рекламы, и т.п. Кроме того, ст. 18 уточняет случаи ограничения доступа к персональным данным субъекта персональных данных на определенный срок, в том числе если субъектом персональных данных подано заявление о недостоверности или неполноте данных на время, необходимое для проверки данных оператором. Субъект персональных данных должен быть уведомлен об ограничении до начала его осуществления. Ст. 19 уточняет, что в любом случае оператор уведомляет иных получателей данных о исправлениях, дополнениях, удалениях.

Особенно подробное регулирование система уточнения и удаления данных получает в Регламенте № 2016/794 от 11.05.2016, устанавливающем правовое регулирование системы межгосударственного сотрудничества по раскрытию преступлений и поиску преступников – Европол[578]. Европол действует в качестве посредника между государствами, позволяя им обмениваться данными о преступниках, подозреваемых, обвиняемых, а также о некоторых деталях совершенных ими или вменяемых им преступлений. В связи с этим специальное регулирование получают как персональные данные в целом, так и право на их удаление. Процесс исправления данных получает регулирование не только в отношении реализации права субъекта персональных данных, но и в отношении данных, собранных из источников с разной степенью достоверности. Ст. 29 устанавливает порядок оценки надежности данных. Предоставляющее государство должно осуществить оценку данных исходя из следующей классификации: А) нет сомнений в аутентичности, достоверности и компетенции источника или источник

[578] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA // http://data.europa.eu/eli/reg/2016/794/oj (дата обращения 08 10 2019)

информации был признан достоверным во всех случаях; B) источник информации был признан достоверным в большинстве случаев; C) источник информации в большинстве случаев был признан недостоверным; X) достоверность источника не может быть оценена. Кроме того, помимо указанных, предоставляющее государство должно оценить информацию с присвоением следующих кодов: 1) достоверность информации несомненна; 2) информация, известная источнику, но не известная должностному лицу, предоставившему ее; 3) информация известна не источнику, но подтверждена иной собранной информацией; 4) информация известна не источнику и не может быть подтверждена.

Европол имеет право при оценке информации уведомить все государства, относящиеся к делу, о необходимости переквалификации какого-либо из кодов и просить их дать согласие на изменение. Европол не вправе самостоятельно менять коды без указанного согласия государств, относящихся к делу. Если предоставляющее государство не установило коды, Европол самостоятельно оценивает информацию исходя из имеющихся у него сведений. Оценка отдельных данных и информации осуществляется с согласия заинтересованных стран. Если соглашение в отношении отдельных данных или в целом не достигнуто, Европол присваивает им коды X и 4. Информация, получаемая Европолом из открытых источников, оценивается им исходя из предложенной классификации кодов. Если информация получена в результате проводимого Европолом анализа и сопоставления данных, Европол проводит оценку при согласии заинтересованных стран.

На сайте информационной системы Европола уточнено, что информация, внесенная в систему, остается в полном распоряжении владельца данных и не может быть изменена каким-либо образом Европолом

или государством-участником. Владелец информации отвечает за достоверность и надежность данных, их своевременное обновление, подтверждение сроков хранения данных[579].

Ст. 36 предоставляет субъекту персональных данных право требовать от Европола информации об обрабатываемых в отношении него данных. Ст. 37 устанавливает особенности уточнения и удаления данных по запросу субъекта. Такой запрос подается в Европол через уполномоченное государство. Европол имеет право ограничить данные вместо удаления, если имеются основания полагать, что правомерным интересам субъекта может быть причинен вред.

Таким образом, особенности уточнения данных в информационных системах ЕС в целом не устанавливаются, однако предусмотрена защита интересов субъекта персональных данных, имеющего право требовать их удаления, исправления или уточнения. Кроме того, на примере Европола допустимо заключить, что специальное регулирование ЕС может более детально регламентировать особенности учета достоверности информации и ее исправления как самими субъектами персональных данных, так и государствами ЕС.

2.4.2 Особенности подходов в праве Германии

В соответствии с Законом об улучшении доступа к административным услугам (OZG) для оказания административных услуг создаются учетные записи пользователей услуг. Для создания учетной записи осуществляется сбор данных пользователя, включая данные свидетельства о личности пользователя. Данные свидетельства имеют неодинаковый уровень доверия, что позволяет в дальнейшем определять возможность получения административных услуг, соответствующих уровню доверия. Для создания и

---

[579] https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system (дата обращения 30 08 2019)

управления учетными записями пользователей на федеральном и земельном уровнях назначается специальный государственный орган. Административный орган, оказывающий услугу пользователю, имеет право с согласия пользователя в электронном виде получить данные из органа, ответственного за учетные записи. Таким образом, данные, имеющиеся у органа, ответственного за учетные записи пользователей административных услуг, имеют статус проверенных.

Аналогичный подход применяется к публичным данным. Орган, собравший данные, выступает ответственным за их качество. В частности, по Закону о свободе информации (IFG)[580] орган, в который поступает запрос пользователя о предоставлении данных и получивший данные из органа, собравшего данные, предоставляет запрашиваемые данные и не обязан при этом проверять их достоверность.

В соответствии с GDPR[581], а также федеральным законодательством Германии (BDSG[582] и земельным законодательством о защите данных) устанавливается принцип качества персональных данных. Персональные данные должны быть точными и при необходимости незамедлительно обновляться. Оператор обработки данных обязан принимать разумные меры, чтобы неточные или недостоверные данные были уничтожены либо исправлены.

При этом контроллер, являющийся уполномоченным органом по защите персональных данных, обязан предоставлять субъекту персональных данных информацию о праве субъекта на доступ, исправление, удаление и

---

[580] Gesetz zur Regelung des Zugangs zu Informationen des Bundes http://www.gesetze-im-internet.de/ifg/ (дата обращения 11.08.2019)

[581] Regulation (EU) 2016/679 (General Data Protection Regulation) //Режим доступа https://gdpr.eu/tag/gdpr/ (дата обращения 13.08.2019)

[582] Bundesdatenschutzgesetz // Режим доступа: https://www.gesetze-im-internet.de/bdsg_2018/index.html (дата обращения 17.08.2019)

ограничение обработки его данных, а также о праве контролера на исправление или удаление данных.

Таким образом, ответственным за качество данных выступает орган, осуществляющий их сбор. Иные государственные органы, получившие данные от органа, выполнившего первичный сбор данных, не проверяют достоверность данных. Контроль над качеством данных возложен на федерального уполномоченного по защите данных. Наряду с этим субъект, чьи данные содержатся в информационных системах, имеет право в любое время контролировать их и заявлять требования об исправлении некорректных данных.

2.4.3 Особенности подходов в праве Франции

Французское право не содержит общих положений по устранению противоречий в информации государственных информационных систем, однако устанавливает правила разрешения противоречий в режимах информации.

Положения, определяющие порядок разрешения противоречий в отношении разграничения режимов конфиденциальности и открытости при предоставлении данных, установлены Книгой III Кодекса отношений между обществом и администрацией[583]. Кодекс в ст. L311-5 непосредственно определяет информацию, не подлежащую передаче. При этом список открыт в той мере, в какой оставляет отсылку к другим видам тайны. В том числе не подлежат передаче сведения, содержащие:

– тайну межведомственного сообщения исполнительной власти,
– тайну национальной безопасности,
– сведения о внешней политике Франции,

---

[583] Code des relations entre le public et l'administration // https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000031366350 (дата обращения 22 09 2019)

– относящиеся к безопасности государства, общества, личности либо информационных систем,

– относящиеся к деньгам либо публичному кредитованию,

– сведения о ходе административных процедур или подготовительных действий к таким процедурам, если не получено разрешение от компетентного органа,

– сведения о расследовании и предотвращении противоправных действий,

– относящиеся к другим тайнам, защищаемым законом.

Предусмотрена специальная процедура рассмотрения Комитетом по тайной статистике вопросов о предоставлении статистики из баз данных компетентных органов с соблюдением тайны. Установлены также нормы защищенного ознакомления с истребованной информацией.

Ст. L311-6 Кодекса устанавливает, что предоставлению никому, кроме заинтересованного лица, не подлежит информация:

– передача которой могла бы повлечь нарушение режима частных тайн,

– содержащая оценочную информацию в отношении лица, которое указано напрямую или которое можно легко определить,

– раскрывающая информацию о действиях лица, что может повлечь причинение им вреда.

Если информация содержит сведения, указанные в ст. L311-5 и ст. L311-6 Кодекса, то она подлежит сообщению третьим лицам, в том числе доведению до всеобщего сведения только после того, как конфиденциальные сведения изъяты. Информация, содержащая персональные данные, также может быть опубликована с предварительным изъятием данных (анонимизация), за исключением случаев, прямо поименованных в Кодексе. Например, допускается размещение с сохранением персональных данных:

– документов информирования общества об организации администрации, включая списки уполномоченных лиц,

– национального реестра ассоциаций и реестра предприятий,

– документов публичного информирования регулируемых видов деятельности, в частности: адвокатов, судебных приставов, нотариусов и архитекторов,

– информации о сданных экзаменах и выигранных конкурсах, в том числе о дипломах,

– информации, необходимой для организации спортивных мероприятий,

– информации национального реестра избранных в процессе голосования лиц,

– информации для организации и осуществления туристических мероприятий.

Кодекс также останавливается на случаях, когда публичный субъект осуществляет административное действие исключительно исходя из алгоритмической обработки данных. Административные решения, принятые на основе алгоритмической обработки, получают специальное регулирование. Об этом должно быть прямо указано получателю принятом в отношении него административном решении на основе алгоритмической обработки. По запросу лица ему сообщается, какие правила определяли обработку и какие основные характеристики определяли способ обработки. Администрация должна по запросу лица сообщить следующую информацию:

– степень и способ использования обработки алгоритмических данных для принятия решения,

– обрабатываемые данные и их источники,

– параметры обработки либо, в противном случае, их взвешенную оценку, применительно к ситуации запрашивающего,

– операции, произведенные путем обработки.

Таким образом в условиях прозрачности сообщения об обрабатываемых данных не исключается возможность невластного субъекта подать возражение и уточнить необходимые данные.

С целью упрощения порядка сбора данных во Франции предусматривалась реализация принципа одноразового сбора необходимых данных (Tell us once), указанного в п. b) 3.1.2. Карты стратегического развития межведомственной системы государства 2013г.[584]. Национальное собрание одобрило в 2012 г. предложение о принятии закона об упрощении права и процедуры административных действий[585], о котором также говорится в Карте стратегического развития. Такой подход позволил бы устранить необходимость параллельного сбора данных, обеспечивая обмен ими в рамках системы взаимодействия. Но указанный закон принят не был и предлагаемый способ реализации остался в области планирования.

Право субъекта персональных данных на устранение в них противоречий во Франции рассматриваются в контексте общеевропейского права и не обладает спецификой.

Проект закона содержал множество положений, способствующих унификации взаимодействия органов власти с юридическими лицами, однако в нем содержались и положения, напрямую не связанные с предметом его регулирования. В частности, в проект внесено положение, что изменение часов нагрузки работника за неделю или год в соответствии с коллективным соглашением не будет означать изменения условий трудового договора[586]. Кроме того, во время рассмотрения проекта в новом чтении Национальной ассамблеей было внесено множество дополнений, не связанных с

---

[584] Cadre stratégique SI Etat, 2013 https://references.modernisation.gouv.fr/sites/default/files/03%20-%20Cadre%20strat%C3%A9gique%20SI%20Etat%20-%20version%201.0%20F%C3%A9vrier%202013.pdf (дата обращения 12 10 2019)

[585] https://www.economie.gouv.fr/adoption-loi-sur-simplification-droit-et-allegement-charge-administrative (дата обращения 12 10 2019)

[586] Для изменения условий трудового договора (*modification du contrat de travail*) необходимо согласие работника. Однако возможно некоторое изменение условий труда, которое не составляет изменения трудового договора (например, переход на новое рабочее место в том же офисе).

обсуждением проекта ранее. Конституционный совет Франции признал внесение Национальной ассамблеей новых положений не соответствующим конституционной процедуре принятия законопроектов, а положения по изменению условий трудового договора - не соответствующими Конституции[587]. Решение Конституционного совета в рамках конституционного контроля над законопроектами (контроля *ex ante*) послужило основанием непринятия законопроекта.

Право субъекта персональных данных на устранение в них противоречий во Франции рассматриваются в контексте общеевропейского права и не обладает спецификой.

Таким образом, французское право на нормативном уровне устанавливает правила устранения противоречий в режимах информации при предоставлении публичных данных иным лицам, оберегая как конфиденциальную публичную информацию, так и относящуюся к частным лицам. Одновременно в связи с реформированием системы межведомственного взаимодействия во Франции предпринимаются попытки устранить дублирование сбора необходимой информации государственными органами. Французское право при этом в целом предполагает возможность невластного субъекта уточнить или исправить необходимые данные.

2.4.4 Особенности подходов в праве Эстонии

В Эстонии Актом о публичной информации[588] в §43[6] закреплена концепция базовых данных. Суть данной концепции заключается в признании авторитетного (эталонного) источника конкретной информации, хранящейся в разных базах данных. Авторитетным источником информации

---

[587] Décision n° 649 DC du 15 mars 2012 // https://www.conseil-constitutionnel.fr/decision/2012/2012649DC.htm (дата обращения 14 09 2019)

[588] Public Information Act // Режим доступа: https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения: 14.08.2019).

признана база данных, целью которой был сбор этой информации. При этом законодательством запрещен сбор разными базами данных одной и той же информации. В соответствии с данной концепцией при выявлении противоречий в данных, обрабатываемых в разных базах данных, приоритет - за информацией, содержащейся в первичной базе данных.

Акт о публичной информации закрепляет обязанность держателя информации не предоставлять заведомо ложную, неточную или неверную информацию и, при сомнениях, проверять правильность и достоверность информации (§ 9). Также установлен запрет размещения устаревшей, неточной или вводящей в заблуждение информации на веб-сайте публичных органов (§ 32).

Принципы управления сервисами и информацией 2017 г.[589] устанавливают обязанность публичных органов проводить инвентаризацию находящихся в их распоряжении данных, устранять дублирования, проверять истечение срока хранения данных (§ 13). Публичные органы должны обеспечивать достоверность и актуальность сведений о находящихся в их ведении базах данных (проверять статус главного обработчика информации) в административной системе государственной информационной системы.

Публичный орган должен анализировать необходимость в использовании информации, устанавливать дублирование информации в разных форматах и местах хранения; выявлять пропущенные сроки хранения информации; классифицировать информацию в соответствии с требованием Акта об архивах. Орган должен принимать меры к удалению лишней информации и по прекращении её сбора к устранению дублирования информации.

---

[589] Principles for Managing Services and Governing Information // Режим доступа: https://www.riigiteataja.ee/en/eli/507072017004/consolide (дата обращения: 14.08.2019).

При устранении дублирования информации приоритет должен отдаваться информации, хранящейся в формате данных (information stored as data, структурированных массивах данных) перед информацией на бумажных носителях, на электронной почте и т.п. (§ 12).

Если информацию в информационной системе обрабатывают несколько публичных органов, главный обработчик несет ответственность за хранение, возможность использования и защиту информации, за передачу информации в публичные архивы или её уничтожение, за обеспечение доступа к информации.

В соответствии с Актом о защите персональных данных 2018 г.[590] у субъекта данных есть право требовать у оператора/обработчика исправления любых неточных персональных данных о себе, удаления неполных данных (если это вытекает из цели обработки) либо всех персональных данных, если они обрабатываются с нарушением закона или если отпала необходимость в их обработке (§ 25). При этом оператор, получивший требование субъекта персональных данных об исправлении или удалении данных, обязан направить соответствующее уведомление лицу, предоставившему эти данные и лицам, которым эти данные были переданы оператором. Лица, которые получили данные от оператора, также обязаны исправить или удалить соответствующие данные.

У субъекта персональных данных также есть право оспорить юридически значимое решение, принятое на основе автоматизированной обработки его персональных данных (§ 21).

Аналогичные права субъектов персональных данных и корреспондирующие обязанности операторов и обработчиков

---

[590] Personal Data Protection Act // Режим доступа: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide (дата обращения: 14.08.2019).

предусмотрены в Общем Регламенте ЕС о защите данных (GDPR) 2016 г.[591] (статьи 16 и 17). Право на удаление персональных данных в GDPR называется, как говорилось ранее, «правом быть забытым».

Таким образом, в Эстонии помимо общих для всех стран ЕС положений о возможности удаления/уточнения персональных данных, хранящихся в государственных информационных системах, предусмотрены оригинальные подходы к выявлению и разрешению противоречий в данных (утвержден принцип базовых данных, закреплены обязанности администраторов систем регулярно проводить инвентаризацию хранящихся данных).

2.4.5 Особенности подходов в праве Великобритании

Из изложенного выше следует, что информационное взаимодействие между гражданами и органами государственной власти и непосредственно между органами государственной власти происходит в рамках единой централизованной информационной системы GOV.UK, ее отдельных сервисов, с использованием утвержденных форматов файлов (стандартов).

Основные противоречия возникают в сфере защиты персональных данных. Такие конфликты, связанные, в частности, с нарушением права на исправление неточных персональных данных в государственной информационной системе; они решаются на основании Акта о защите данных[592] и GDPR[593]. Основными субъектами, выявляющими и

---

[591] 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) // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1564943268451&uri=CELEX:32016R0679 (дата обращения: 14.08.2019).

[592] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (дата обращения 24 08 2019)

[593] https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения 05 08 2019)

разрешающими противоречия, являются субъекты персональных данных и ICO.

Административная и судебная практика по вопросу выявления и разрешения противоречий в отношении данных, находящихся в ведении государственных органов, не так развита, как практика в отношении частных субъектов – контроллеров (операторов).

В качестве релевантных актов ICO отметим различные уведомления в отношении государственных органов[594]. Из анализа основных актов вытекает вывод, что ICO по итогам проверки выносит предостережения о недопустимости нарушения законодательства о персональных данных (enforcement notices). При неисполнении требований ICO выносится постановление (penalty notice), предусматривающее финансовые санкции, в пределах, установленных в GDPR.

Контроль над размещением соответствующей информации с использованием установленных стандартов, в связи с функционированием системы GOV.UK осуществляет Цифровая служба.

2.4.6 Особенности подходов в праве Австралии

Выявление и разрешение противоречий в данных, содержащихся в различных государственных информационных системах, может быть осуществлено как по инициативе физических лиц в отношении данных, составляющих их личную информацию, так и в рамках сопоставления данных информационных систем правительственными учреждениями.

---

[594] См. например: HMRC enforcement notice (10 May 2019) URL: https://ico.org.uk/action-weve-taken/enforcement/hmrc/ (дата обращения: 05.08.2019); IICSA monetary penalty notice (18 July 2018) URL: https://ico.org.uk/action-weve-taken/enforcement/independent-inquiry-into-child-sexual-abuse/ (дата обращения: 05.08.2019); Secretary of State for Justice enforcement notice (21 December 2017) URL: https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-justice/ (дата обращения: 05.08.2019)

В законодательстве Австралии предусмотрены следующие особенности разрешения противоречий в данных, содержащихся в различных государственных информационных системах, по инициативе физических лиц. Физическим лицам такое право на исправление личной информации дано Законом о неприкосновенности частной жизни, а также Законом о свободе информации. Закон о неприкосновенности частной жизни закрепляет право на исправление личной информации, хранящейся в организации частного или публичного сектора, если таковые сведения являются неточными, устаревшими, неполными, не имеющими значения или вводящими в заблуждение. Принципы неприкосновенности частной жизни (APP), возлагают корреспондирующее обязательство на субъекта APP предпринять разумные шаги для исправления личной информации, чтобы гарантировать, что с учетом цели, для которой она хранится, она является точной, актуальной, полной и не вводящей в заблуждение.

Принцип 13 действует параллельно с иными возможными механизмами, не заменяя их. При этом предусмотренной Законом о неприкосновенности частной жизни и в частности Принципом 13 процедурой можно воспользоваться только в отношении информации, хранящейся в информационных системах лиц, являющихся субъектами указанного Закона[595].

Для информации, содержащейся в государственных информационных системах, физическое лицо может использовать Закон о свободе информации, который также дает право лицу обратиться в уполномоченный орган или к министру с требованием об изменении или аннотировании

---

[595] Chapter 13: APP 13 — Correction of personal information. URL: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information/#interaction-of-app-13-and-other-apps (дата обращения 20 07 2019)

информации о нем, если такое лицо получило доступ к документу, содержащему эту информацию, если информация является неполной, неправильной, устаревшей или вводящей в заблуждение, а также если эта информация используется, использовалась или доступна для использования в административных целях.

В законодательстве также предусмотрено разрешение противоречий в данных, содержащихся в различных государственных информационных системах, в рамках процедуры сопоставления данных.

Офис Информационного комиссара разработал Руководство по сопоставлению данных в органах федеральной исполнительной власти в соответствии с принципами неприкосновенности частной жизни (APP) и Закону о неприкосновенности частной жизни. Документ должен использоваться учреждениями, которые занимаются обработкой личной информации и намерены использовать сопоставление данных для определения необходимости принятия административных мер. Руководство не носит обязывающего характера.

Если государственный орган использует иную программу сопоставления данных, то по требованию Комиссара он обязан подать последнему отчет о выполнении программы. Кроме того, Руководство позволяет освободить какой-либо орган от выполнения отдельных требований по основаниям, связанным с общественными интересами.

Примером протоколов сопоставления данных, разработанных не в рамках описанного выше Руководства АОИК, может служить набор протоколов, используемых Centrelink. Centrelink является программой Департамента социальных служб, ответственного за ряд государственных выплат и услуг пенсионерам, безработным, семьям, опекунам, родителям, инвалидам, аборигенам, учащимся и лицам с различным культурным и языковым происхождением.

Для Centrelink сопоставление данных является одним из ключевых механизмов контроля, используемых для борьбы с мошенничеством и

несоблюдением требований закона. На сегодняшний день Centrelink разработаны следующие протоколы:

– 2004 г. PAYG-протокол сопоставления данных,

– 2016 г. Протокол сопоставления данных о доходах, не связанных с занятостью (NEIDM),

– 2017 PAYG протокол сопоставления данных,

– 2017 г. Протокол сопоставления данных дневного ухода за детьми в семье,

– 2017 г. Протокол сопоставления данных о доверительных бенефициарах,

– 2017 г. Протокол сопоставления данных годового отчета об инвестиционном доходе,

– 2019 г. Согласование протоколов данных Centerlink и Medicare.

Программный протокол сопоставления данных 2017 PAYG (Pay-As-You-Go (PAYG) Data-Matching) определяет, что под сопоставлением данных понимается сравнение двух или более наборов данных для выявления сходств или расхождений. В протоколе термин «сопоставление данных» используется для обозначения использования компьютерных методов для сравнения данных, содержащихся в двух или более компьютерных файлах, в целях выявления неправильной оплаты. Кроме того, определены организации, которые связаны положениями данных руководящих принципов - Департамент социальных служб и Налоговое управление (ATO). Протокол разграничивает некоторые функции указанных ведомств: Департамент отвечает за данные обо всех получателях пособий по безработице, а Управление - за сопоставление данных.

Протокол описывает требования к качеству данных (Data Quality), интегрированности данных (Data Integrity) и к безопасности данных (Data Security), а также описывает процесс сопоставления данных и действия, следующие после проверки. Протокол определяет процедуру получения объяснений физического лица – получателя пособия в случае выявленных

системой несоответствий, а также действия Департамента после получения объяснений и/или запрошенных документов физического лица.

Centerlink использует специальные программы для расчета отдельных показателей (Совпадение данных по доходам, не связанным с занятостью NEIDM) и сопоставления данных граждан с непогашенными долгами (протокол Tax Garnishee). Целью является блокирование налоговых возвратов лицам, не погасившим налоговой задолженности.

Таким образом, в Австралии на нормативном уровне регламентировано право физических лиц требовать внесения изменения в сведения о них, внесенные в государственные информационные системы, а также установлен порядок реализации этого правомочия. При этом сопоставление данных, содержащихся в информационных системах различных государственных ведомств, по инициативе самих ведомств, должно осуществляться ими на основании самостоятельно разработанных протоколов сопоставления данных. Такие протоколы могут основываться на Руководстве по сопоставлению данных, разработанном Комиссаром, или же разрабатываться ведомствами самостоятельно в соответствии с Законом о неприкосновенности частной жизни и под контролем Комиссара.

2.4.7 Особенности подходов в праве Сингапура

Выявление и исправление противоречий, содержащихся в данных, производится каждым органом/оператором государственной информационной системы самостоятельно. Однако для унификации форматов взаимодействия в рамках программы «Умная нация» создается цифровая платформа обработки государственных данных Core Operations Development Environment and eXchange (CODEX)[596]. Данная платформа

---

596 https://www.smartnation.sg/whats-new/press-releases/codex--re-engineering-the-government-s-digital-infrastructure (дата обращения 10 08 2019)

является одним из национальных проектов, что свидетельствует о существенном значении устранения противоречий в данных.

Основными подходами к выявлению и устранению ошибок в государственных данных являются:

– создание «общей архитектуры» государственных данных для реализации единых стандартов и форматов для бесшовного информационного взаимодействия между государственными органами,

– систематическое изменение режима данных для наименее чувствительных категорий и передача для коммерческого использования в форме открытых данных.

Таким образом, государственные органы Сингапура, в чьей компетенции находятся информационные системы, самостоятельно производят выявление и разрешение противоречий в данных, содержащихся в государственных информационных системах, на основе общегосударственных стандартов и принципов. Проверка совместимости полученных данных и отсутствие ошибок (дедупликация, очистка систем данных) производится при объединении систем в облачной платформе.

2.4.8 Особенности подходов в праве Российской Федерации

Подходы к выявлению и разрешению противоречий в данных, содержащихся в различных государственных информационных системах, в том числе при принятии юридически значимых решений рассмотрим на примерах судебной практики (обширная практика по данному вопросу отсутствует).

Так, судебным решением признано, что в случае противоречия данных в государственной информационной системе государственная услуга,

оказываемая уполномоченным органом государственной власти, признается оказанной ненадлежащим образом[597].

При рассмотрении дела было установлено, что уполномоченный орган государственной власти пояснял, что ошибки в кадастровом паспорте земельного участка обусловлены исключительно техническими проблемами информационной системы государственного кадастра недвижимости, в связи с чем принимались меры к доработке программного обеспечения.

Суд определил, что деятельность уполномоченного лица органа государственной власти относится к сфере публичного права. В публичном праве органы власти наделены властными полномочиями относительно иных лиц. Соответственно такие органы должны соблюдать гарантии, обеспечивающие соблюдение принадлежащим иными лицам прав и законных интересов.

К указанным гарантиям относится требование ясности, четкости, определенности, понятности, недвусмысленности актов органов власти.

Кадастровый паспорт земельного участка составлен с нарушением требований к его оформлению, и поэтому есть основания полагать, что государственная услуга по оформлению и выдаче кадастрового паспорта земельного участка, за которой обращался гражданин, была оказана ненадлежащим образом. Ссылка административного ответчика на технические проблемы информационной системы не освобождает орган кадастрового учета от обязанности соблюдения требований закона.

По аналогии права можно рассматривать выявления противоречий данных различных государственных систем (открытые данные о таких прецедентах отсутствуют).

---

[597] См. Определение Московского городского суда от 26.01.2016 № 33а-598/2016.

Статьей 61 Федерального закона от 13 июля 2015 № 218-ФЗ «О государственной регистрации недвижимости»[598] определен порядок исправления ошибок, содержащихся в Едином государственном реестре недвижимости, в том числе технических ошибок (описок, опечаток, грамматических или арифметических ошибок либо подобных ошибок), допущенных органом регистрации прав при осуществлении государственного кадастрового учета и (или) государственной регистрации прав и приведших к несоответствию сведений, содержащихся в Едином государственном реестре недвижимости, сведениям, содержащимся в документах, на основании которых вносились сведения в Единый государственный реестр недвижимости.

Указанным порядком утвержден в том числе порядок представления и форма заявления об исправлении технической ошибки в записях.

Таким образом, в связи с отсутствием общеотраслевых нормативных правовых актов, определяющих общие нормы процедуры выявления и устранения противоречий данных, содержащихся в государственных информационных системах, в том числе устранения технических ошибок, рекомендуется распространить положения порядка исправления ошибок, содержащихся в Едином государственном реестре недвижимости, на прочие отраслевые государственные информационные системы.

2.4.9 Выводы

В законодательстве стран Европейского союза предусмотрены механизмы разрешения противоречий в данных, обрабатываемых в государственных информационных системах:

– установлен запрет на дублирование сбора идентичной информации,

---

[598] Федеральный закон от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости» // СЗ РФ. 2015. № 29 (Часть I). Ст. 4344.

– определены администраторы баз данных, отвечающих за актуальность и достоверность информации,

– выстроена система координации процедур создания и изменения государственных информационных систем,

– закреплена концепция «базовых данных» (Эстония), устанавливающая авторитетный источник данных,

– закреплен приоритет структурированных данных, хранящихся в информационных системах, перед информацией на бумажном носителе.

Отдельный механизм выявления и разрешения противоречий предусмотрен в законодательстве о защите персональных данных. Субъект персональных данных вправе обратиться к оператору/обработчику с требованием удалить/исправить неактуальные персональные данные. У субъекта персональных данных также есть право оспорить юридически значимое решение, принятое на основе автоматизированной обработки его персональных данных (например, если решение было принято на основе обработки недостоверных или устаревших сведений).

В странах общего права и в Сингапуре на нормативном уровне также регламентировано право физических лиц требовать внесения изменения в сведения о них, внесенные государственные информационные системы, а также установлены процедуры реализации этого правомочия.

В отношении сопоставления данных, содержащихся в информационных системах государственных ведомств по инициативе самих ведомств, следует сделать вывод о разработке ведомствами протоколов на основании руководящих принципов, изданными уполномоченным органом. При этом, однако, по ряду стран информация об унифицированных процедурах разрешения противоречий в данных, содержащихся в различных государственных информационных системах, не выявлена.

2.5 Подходы к мониторингу и аудиту государственных информационных систем на предмет достоверности и иных качественных показателей, содержащихся в них данных

2.5.1 Общие подходы в праве Европейского союза

В европейских странах в последнее время создано огромное количество хранилищ открытых данных, в том числе правительственных данных, различных уровней (ЕС, национальный, региональный). Еврокомиссия способствует созданию и реализации проектов, направленных на визуализацию, структуризацию, гармонизацию, обработку открытых данных для их последующего использования. Одним из таких проектов и примеров государственно-частного партнерства выступает платформа Open Data Monitor[599]. Создание платформы позволило собрать открытые данные из различных источников (каталогов) и обработать их для последующего использования. При сборе данных использованы метрики: качественные (машиночитаемость, доступность, полнота, обнаруживаемость и пр.) и количественные (общие размеры данных, количество наборов данных, в том числе уникальных, количество собранных каталогов, баз данных и т.п.). Также платформа выполняет различные аналитические функции, такие как:

– сравнение данных государственных органов (национальных/ местных) с указанием изменений и обновлений каталогов,

– отражение качества метаданных,

– сортировка доступных каталогов по конкретным тематическим доменам,

– показ лицензионной информации,

– предоставление данных в определенных открытых форматах,

[599] Open Data Monitor //: https://opendatamonitor.eu (дата обращения 25.08.2019).

– выявление расхождений между доступными открытыми данными стран-членов ЕС.

В отчете Еврокомиссии об инструментах мониторинга рынка данных SMART 2016/0063 от 28.06.2019 600, основанном на количественных данных в целом по ЕС и о каждой стране ЕС, обрисовывается текущее положение вещей в области использования различных категорий данных. Германия, Франция, Испания, Нидерланды и Италия занимают лидирующие позиции по доходности от передачи данных по ЕС.

Европейский мониторинг потока данных имеет две цели:

– построить карту потоков данных в ЕС для определения основных стратегических коридоров этих потоков,

– оценить экономическую ценность потоков данных для европейской цифровой экономики.

Для достижения первой цели в 2019 году развернут опрос компаний и государственных органов для сбора агрегированных и анонимных данных о:

– количестве данных, хранящихся в облачных инфраструктурах компаний и государственных органов ЕС (запасы данных),

– данных, перемещаемые между облачными инфраструктурами на территории ЕС (т. е. потоки данных).

Аудит данных в ЕС осуществляется в нескольких направлениях.

Одним из таких направлений является проверка достоверности данных Евростатом в рамках его деятельности. Евростат проверяет, соответствуют ли данные базовым критериям, которые служат для оценки достоверности данных. Проверка является ключевой задачей во всех областях статистики и

---

[600] Отчет Еврокомиссии об инструментах мониторинга рынка данных SMART 2016/0063 от 28.06.2019 // http://datalandscape.eu/sites/default/files/report/D2.6_EDM_Second_Interim_Report_28.06.2019.pdf (дата обращения 30 09 2019)

осуществляется в рабочем процессе Европейской статистической системы (ESS), которая состоит из Евростата и статистических органов стран ЕС. Регламент (ЕС) № 223/2009 Европейского парламента и Совета от 11.03. 2009[601] о европейской статистике образует правовую базу подготовки европейской статистической программы, обеспечивая основу разработки и распространения европейской статистики. Нынешняя программа учреждена Регламентом (ЕС) № 99/2013 Европейского парламента и Совета от 15.01.2013 г. о Европейской статистической программе на период с 2013 по 2017 год[602]. Она продлена до 2020 г.[603]. Основным инструментом проверки данных выступает их валидация, т.е. проверка данных оценивает их достоверность. Положительный результат не гарантирует правильности данных, но отрицательный результат гарантирует, что данные неверны.

В части персональных данных на территории ЕС мониторинг и аудит осуществляется в рамках GDPR надзорными органами, учрежденными странами ЕС.

Таким образом, ЕС осуществляет общий мониторинг оборота данных на территории государств-участников, собирая аналитическую информацию позволяющую вырабатывать оценки развития экономики данных на рынке

---

[601] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009R0223 (дата обращения 25.08.2019).

[602] Regulation (EU) No 99/2013 of the European Parliament and of the Council of 15 January 2013 on the European statistical programme 2013-17 // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1409068106403&uri=CELEX:32013R0099 (дата обращения 25.08.2019).

[603] Regulation (EU) 2017/1951 of the European Parliament and of the Council of 25 October 2017 amending Regulation (EU) No 99/2013 on the European statistical programme 2013-17, by extending it to 2020 // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.284.01.0001.01.ENG (дата обращения 25.08.2019).

ЕС. Отдельные контрольные мероприятия проводятся на основании европейских актов.

2.5.2 Особенности подходов в праве Германии

В Законе об электронном правительстве[604], по которому все услуги и взаимодействие осуществляются в электронном виде, предусмотрено, что государственный орган должен хранить электронный образ полученного документа в разборчивом и читаемом виде для последующих процедур аудита. Также при совместной обработке данных несколькими органами ответственным назначается одно из участвующих ведомств, которое хранит соответствующий образ.

В сфере защиты персональных данных полномочиями по контролю и аудиту соблюдения законодательства о защите данных наделен Федеральный комиссар защиты данных и свободы информации (п. 1 раздела 8 BDSG)[605]. Комиссар вправе контролировать деятельность государственных органов и частных организаций с долей государственного участия. В свою очередь Комиссар подчинен Федеральной счетной палате. Комиссар осуществляет мониторинг и обеспечивает применение законодательства в сфере защиты данных, проводит аудит по собственной инициативе, по обращениям граждан либо иных органов, проводит расследования и др.

В каждой из земель также назначаются комиссары защиты данных, взаимодействующие с Федеральным комиссаром. Федеральный и земельные комиссары в их полномочиях по защите данных во много повторяют статус Уполномоченного по защите данных ЕС, действующего согласно GDPR.

---

[604] Gesetz zur Förderung der elektronischen Verwaltung //Режим доступа: http://www.gesetze-im-internet.de/egovg/ (дата обращения 14.08.2019).

[605] Bundesdatenschutzgesetz //Режим доступа: https://www.gesetze-im-internet.de/bdsg_2018/index.html (дата обращения 17.08.2019).

Также среди органов контроля и надзора за обработкой данных, законом о телекоммуникациях (TKG)[606] фигурирует Федеральное сетевое агентство, взаимодействующие с Федеральным комиссаром и Федеральным управлением информационной безопасности при нарушениях обработки данных, угрозах безопасности при оказании телекоммуникационных услуг.

Таким образом, в Германии подходы к мониторингу и аудиту государственных информационных систем направлены на обеспечение сохранности документов в электронной форме и проверке органами, осуществляющими мониторинг и аудит, в том числе комиссарами защиты данных.

2.5.3 Особенности подходов в праве Франции

Во Франции реализуются различные формы контроля публичных органов и подведомственных им организаций. Упор сделан на квалифицированный министерский внутренний аудит. Поскольку внутренний аудит является основным, аудит информационных систем осуществляется в рамках общих положений об аудите.

Декретом Министерства бюджета, публичных счетов, публичной службы и реформирования государства № 2011-775 от 28.06.2011 о внутреннем аудите в администрации была введена система профессионального внутреннего аудита каждого министерства[607]. По ст. 2 Декрета под руководством министра, ответственного за реформирование государства, действует Комитет гармонизации внутреннего аудита (CHAIE), который объединяет ответственных лиц за внутренний аудит каждого министерства, представителей генерального директора публичных финансов,

---

[606] Telekommunikationsgesetz // Режим доступа: https://www.gesetze-im-internet.de/tkg_2004/index.html (дата обращения 10.08.2019).

[607] Décret no 2011-775 du 28 juin 2011 relatif à l'audit interne dans l'administration // https://www.legifrance.gouv.fr/jo_pdf.do?numJO=0&dateJO=20110630&numTexte=50&pageDebut=&pageFin (дата обращения 22 06 2019)

генерального директора бюджета, а также иных квалифицированных лиц, назначаемых Премьер-министром. CHAIE утверждает нормативные акты в отношении внутреннего аудита, а также ежегодно проверяет политику аудита в каждом министерстве и дает рекомендации. Циркуляром Премьер-министра от 30.06.2011[608] уточнен порядок внутреннего аудита в министерствах, предусматривающий создание министерского комитета внутреннего аудита, который определяет политику аудита, утверждает программу внутреннего аудита (отдельные виды аудита) и обеспечивает ее исполнение.

В отношении информационных систем также могут реализовываться формы внешнего и смешанного контроля. Декретом Председателя совета министров n°55-733 от 26.06.1955 об экономическом и финансовом контроле [609] были установлены процедуры экономического и финансового контроля (CGefI). В CGefI выделен аудит как во внутреннем министерском контроле (смешанный контроль), так и во внешнем. Так, в 2018 г., согласно отчету CGefI[610], CGefI привлекались к внутреннему министерскому аудиту цифровых рисков и цифровой безопасности. Кроме того, на сайте CGefI создан раздел, посвященный контролю над информационными системами в распоряжении субъектов публичного права, в котором кратко

[608] La circulaire du Premier ministre du 30 juin 2011 sur la mise en oeuvre de l'audit interne dans l'administration // https://www2.economie.gouv.fr/files/CirculairePM-30-06-2011_0.pdf (дата обращения 6 08 2019)

[609] Décret n°55-733 du 26 mai 1955 relatif au contrôle économique et financier de l'Etat // https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4F994518EBDD70B55684DB74A2EB10D7.tpdjo02v_2?cidTexte=LEGITEXT000006060746&dateTexte=20120727 (дата обращения 11 06 2019)

[610] CGefI, Rapport d'activité, 2018 // https://www.economie.gouv.fr/files/2018-Rapport-d-activite-CGefi_0.pdf (дата обращения 15 08 2019)

обосновывается стратегическая и экономическая значимость информационных систем[611].

Кроме того, агентство, отвечающее за безопасность информационных систем (ANSSI), также осуществляет мониторинг подведомственных ему информационных систем. Функцию надзора над безопасностью систем в отношении услуг государства координирует Субдиректорат по операциям[612].

В соответствии с Декретом создания Межведомственной дирекции по цифровому развитию (DINU)[613], заменившей DINSIC, утвержденном Премьер-министром, DINU может по поручению Премьер-министра или министра отдельного министерства осуществлять аудит, контроль или оценку как проектов об информационных системах, так и самих информационных систем отдельных министерств или организаций, находящихся в компетенции таких министерств.

В связи с активным развитием государственных информационных систем и цифровизацией управления деятельность каждого из министерств по созданию и развитию информационных систем подлежит также внешней координации. Межведомственная дирекция по управлению национальными информационными системами (DINSIC)[614] наделена полномочиями мониторинга развития государственных информационных систем в форме предварительного одобрения проектов развития и создания государственных

---

[611] https://www.economie.gouv.fr/cgefi/controle-des-systemes-dinformation-dans-organismes-publics (дата обращения 2 09 2019)

[612] https://www.ssi.gouv.fr/agence/organisation/les-sous-directions/centre-operationnel-de-la-securite-des-systemes-dinformation-cossi/ (дата обращения 10 08 2019)

[613] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique // https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D4ECB579ACEA6FD419A2720092289704.tplgfr31s_2?cidTexte=JORFTEXT000039281619&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000039281603 (дата обращения 04.11.2019).

[614] С 25 октября 2019г. DINSIC была заменена на Межведомственную дирекцию по цифровому развитию (DINU). Одновременно DINU сохраняет полномочия по проведению указанного контроля.

информационных систем, утверждаемых каждым министерством в соответствии с его компетенцией.

В соответствии со ст. 3 Декрета о государственной информационно-коммуникационной системе n° 2014-879 от 1.08.2014[615] каждый министр утверждает план инвестирования, включающий проекты и деятельность министерства, а также организаций, находящихся в его компетенции, в сфере информационно-коммуникационных систем. План направляются на ознакомление Межведомственному директору по управлению национальными информационными системами равно как и проекты, соответствующие необходимым требованиям, в частности предполагаемой стоимости, утвержденные постановлениями министра, ответственного за реформирование государства, министра, ответственного за цифровое развитие и министра, ответственного за бюджет. Презюмируется, что мнение Межведомственного директора вынесено в пользу соответствия, если в течение месяца с момента получения документов не последовало ответа. В течение этого срока Межведомственный директор вправе запрашивать дополнительную информацию у министерства, что влечет удлинение указанного срока. Мнения направляются Премьер-министру, трем указанным выше министрам, а также другим заинтересованным министрам

Мнения DINSIC размещаются на официальном сайте с выделением тем и министерств, готовивших проект, с предложением выражать мнения[616]. Мнения обычно содержат оговорку, что глубокий внутренний аудит не проводился, в связи с чем мнение сформулировано на базе имеющейся

---

[615] Décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'Etat // https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029337021 (дата обращения 2 11 2019)

[616] URL: https://www.numerique.gouv.fr/publications/avis-conformes/ (дата обращения 19 08 2019)

информации. Например, в 2017 г. было запрошено мнение о проекте второй волны системы информации и телефонии, в части проекта 3.20 в отношении объединения на одном сайте услуг Премьер-министра и ряда самостоятельных ведомств[617]. Мнением Межведомственного директора было подтверждено соответствие проекта. Но анализ документации позволил выявить ряд рисков, в связи с чем во мнениях были изложены соображения о возможные них и о путях их минимизации (например, избыток разрабатываемых инфраструктур – предлагается сократить их количество в целях информационной безопасности).

Таким образом, во Франции контроль над государственными информационными системами имеет следующие формы: внутренний, внешний и смешанный, предварительное согласование. При этом отдельный акцент во французском праве сделан на квалифицированном постоянном внутреннем министерском аудите. Любые изменения в отношении информационных систем, проекты их развития рассматриваются с 25 октября 2019 г. Межведомственной дирекцией по цифровому развитию (DINU) и должны быть ею одобрены посредством вынесения мнения о соответствии. Кроме того, DINU наделена полномочиями внешнего контроля над информационными системами в ведении отдельных министерств (по обращению соответствующего министра либо по обращению Премьер-министра), который может включать как аудит, так и иные формы контроля (оценку, экспертизу).

2.5.4 Особенности подходов в праве Эстонии

Отдельные вопросы мониторинга и аудита государственных информационных систем в эстонском законодательстве получили отражение

---

[617] https://www.numerique.gouv.fr/uploads/segur_phase_2_art_3.pdf (дата обращения 19 08 2019)

в Акте о публичной информации[618] и Принципах управления сервисами и информацией[619].

Акт о публичной информации предписывает каждому публичному органу вести реестр документов, полученных или созданных данным органом (§ 11). Документы должны вноситься в реестр не позднее одного рабочего дня с момента его получения или создания. В реестр вносится следующая информация: от кого документ получен или кому предоставлен; дата получения или предоставления документа; способ получения/предоставления документа; реквизиты документа; тип документа; ограничения на доступ к документу; срок хранения документа для его обработки (если предусмотрен законом); должность и имя ответственного за обработку документа лица.

Доступ к реестру должен быть открытым, за исключением информации ограниченного доступа. Публичные органы обязаны создавать индексы и инструкции для удобства поиска информации в реестре, обеспечивать условия для полнотекстового поиска с использованием компьютерных поисковых систем (§ 12).

Помимо документов регистрироваться должны и базы данных, составляющие государственную информационную систему. База данных регистрируется в административной системе государственной информационной системы. Перед регистрацией ответственный сотрудник обязан проверить базу данных, обеспечить её соответствие установленным в законодательстве требованиям (§ $43^7$).

---

[618] Public Information Act // Режим доступа: https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения: 14.08.2019).

[619] Principles for Managing Services and Governing Information // Режим доступа: https://www.riigiteataja.ee/en/eli/507072017004/consolide (дата обращения: 14.08.2019).

Принципы управления сервисами и информацией устанавливают основы управления информацией в государственной информационной системе. Управление информацией призвано обеспечить качество и доступность информации; управление рисками и сокращение издержек по хранению, обмену и использованию информации; преемственность управления при кадровых и иных организационных изменениях (§ 11).

Публичный орган должен осуществлять обзор информации, созданной в связи с выполнением его основных функций, источников и мощностей для хранения данных. В процессе обзора (инвентаризации) орган должен определить: информацию, необходимую для осуществления его функций; дополнительную информацию, которая создана или получена при осуществлении его функций; источники информации; форматы и места хранения данных; сроки ее хранения; условия доступа к ней; пользователей информации.

Орган должен анализировать необходимость в использовании информации, выявлять дублирование информации в разных форматах и местах хранения и пропущенные сроки хранения информации, классифицировать информацию по Акту об архивах. Он должен удалять лишнюю информацию и прекращать её сбор, устранять дублирование данных. При устранении дублирования приоритет должен отдаваться информации, хранящейся в структурированных массивах данных, перед информацией на бумажных носителях, на электронной почте и т. п. (§ 12). Орган должен обеспечить хранение, возможность использования и защиту информации до момента отправления информации в публичные архивы или ее уничтожения.

Внесение информации в систему может осуществляться только авторизованным лицом, прошедшим идентификацию.

Если орган управляет информационной системой совместно с лицом частного права, в соглашении между ними должны быть предусмотрены условия о хранении, обеспечении доступности и защиты информации, а

также обязательств по передаче информации органу при прекращении договора или прекращении осуществления лицом частного права публичных обязанностей.

При разработке новой информационной системы орган должен определить сроки хранения информации в данной системе. При передаче информации из одной информационной системы в другую не подлежит передаче информации с истекшим сроком хранения и информация, не нужная органу при использовании новой информационной системы.

При разработке информационной системы, в которой обрабатываются персональные данные, должны быть обеспечены технические и организационные возможности физическим лицом отследить обработку его персональных данных (кому и когда предоставлены персональные данные, кто и когда их использовал).

В законодательстве Эстонии отсутствуют положения о независимом (внешнем) мониторинге и аудите государственных информационных систем. Однако сфере использования государственных информационных систем осуществляется не только аудит и мониторинг, но и контрольно-надзорная деятельность. Субъектами, осуществляющими надзор за соблюдением требований Акта о публичной информации, является Инспекция по защите данных, вышестоящие над держателями данных органы; Министерство экономики и коммуникаций.

Инспекция осуществляет надзор над деятельностью держателей данных (§ 45). Надзор осуществляется как на основании обстоятельств (например, по жалобам граждан), так и по инициативе Инспекции. Инспекция проверяет исполнение обязанностей по предоставлению информации по запросу, по раскрытию информации, в том числе полноту информации на веб-сайте. Инспекция может давать рекомендации по имплементации требований Акта о публичной информации. Уполномоченные лица Инспекции имеют право запрашивать объяснения и документы у держателей данных; проверять документы (как общедоступные,

так и ограниченные в доступе); выносить предписания по соблюдению требований законодательства; делать предложения владельцам информации по оптимизации доступа к информации. Решение по итогам надзорных мероприятий доводится до сведения заинтересованных лиц, а также публикуется на сайте Инспекции (§ 50).

Инспекция вправе вынести держателю данных предписание об устранении следующих нарушений: незаконный отказ в предоставлении информации; нарушение сроков предоставления информации; неисполнение требований по распространению информации, в том числе по размещению информации на веб-сайте; незаконное установление ограниченного режима информации (и наоборот) и др. (§ 51). Держатель информации в течение пяти рабочих дней обязан принять меры к исполнению предписания и уведомить Инспекцию об исполнении (§ 52). При неисполнении предписания держателем информации и отказе в его обжаловании в административном суде Инспекция обращается в вышестоящий над держателем информации орган, а также инициирует привлечение держателя к ответственности (§ 52).

Надзор над управлением базами данных и содействие в разрешении споров в процессе их использования осуществляет Министерство экономики и коммуникаций и уполномоченные им лица. Уполномоченные вправе выносить предписания главным и авторизованным обработчикам баз данных (§ $53^1$).

Инспекция подает ежегодный отчёт об исполнении требований Акта о публичной информации (в том числе о выявленных нарушениях, вынесенных предписаниях и т.п.) в Конституционный комитет Парламента и Канцлеру юстиции, а также размещает отчет на своём сайте (§ 52).

Ответственность в виде штрафа до 300 условных единиц установлена за предоставление заведомо некорректной информации, за предоставление информации ограниченного доступа; за неисполнение требований предписаний Инспекции. Производство по названным делам осуществляется Инспекцией во внесудебном порядке (§ $54^1$).

В Эстонии предусмотрены процедуры внутреннего аудита/мониторинга государственных информационных систем. Мониторинг/аудит государственных информационных систем направлен на инвентаризацию данных, хранящихся в информационных системах, обеспечение актуальности, полноты информации. Помимо мониторинга/аудита в отношении государственных информационных систем проводятся контрольно-надзорные мероприятия, направленные на выявление правонарушений и принятие мер к их пресечению.

2.5.5 Особенности подходов в праве Великобритании

В соответствии с разделом 128 Акта о защите данных ст. 58.1(b) GDPR ICO проводит аудит (проверки) в области соблюдения законодательства о персональных данных. В руководстве ICO[620] отмечено, что он проверяет организации, в том числе и публичного сектора, не только на соответствие законодательству в области персональных данных, но и в области свободы информации.

Планирование аудита (проверки) основывается на риск-ориентированном подходе, который предполагает выявление контроллеров (операторов) и секторов с высоким риском нарушений. Указанное предполагает учет, в частности: сообщений об утечках, полученных ICO жалоб, отчеты контроллеров, сообщений в СМИ, иной информации.

Организация может запросить добровольный аудит; вместе с тем окончательный выбор остается за ICO.

Аудит может включать в себя следующие области: управление защитой данных, обучение персонала, безопасность персональных данных,

[620] A guide to ICO audits 2018. URL: https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf (дата обращения: 05.08.2019)

запросы субъектов персональных данных, осуществление прямого маркетинга, обмен информацией,управление записями,оценка рисков (DPIA).

Перед аудитом запрашиваются необходимые документы контроллера, регулирующие порядок обработки персональных данных. Также перед аудитом допускается устный опрос персонала по телефону.

По итогам аудита готовится отчет. Краткая версия такового публикуется. Отчет включает:

– рейтинг доверия по каждой из областей,

– несоответствия и риски,

– рекомендации по минимизации рисков.

Через 6–12 месяцев после аудита может быть проведен повторный аудит (проверка). Аудит не является карательной мерой, обычно принудительных санкций за несоответствия не накладывается. Вместе с тем ICO оставляет за собой право на такие действия при выявлении серьезных несоответствий.

На основании отчетов ICO за 2019 год в отношении государственных органов можно сделать следующие выводы:

– сферы проверки выбираются исходя из направлений деятельности государственного органа и не являются одинаковыми для различных органов,

– обычно государственным органам присваивается приемлемый уровень доверия по итогам проверки каждой сферы деятельности,

– в качестве проблем выделяются: несоответствие процессов обработки ряду требований ст. 30 GDPR и недостаточное внимание к обучению персонала информационной безопасности и защите данных[621],

---

[621] См. например: Lancashire Police data protection audit report 2019. URL: https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2615173/lancashire-police-exec-summary-201905.pdf (дата обращения: 05.08.2019); Legal Ombudsman data protection audit report 2019. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2615063/legal-ombudsman-executive-summary.pdf (дата обращения: 05.08.2019); NHS

– рекомендации об устранении рисков носят конкретизированный характер и зависят от выявленных несоответствий в ходе проверки.

Таким образом, за исключением ранее упомянутых в одном из предыдущих разделов проверок схем публикаций органами публичной власти, основное внимание ICO приковано к аудиту соблюдения законодательства о персональных данных.

2.5.6 Особенности подходов в праве Австралии

Термин «мониторинг» не используется в исследуемом законодательстве применительно к государственным информационным системам, однако отмечается широкое применение термина «аудит государственных информационных систем». На федеральном уровне аудит государственных информационных систем не выделен в направление аудита и не имеет специального законодательного регулирования. Аудит осуществляет Генеральный ревизор, являющийся независимым должностным лицом, подотчетным Парламенту.

Основные функции Генерального ревизора включают проверку финансовых ведомостей, результативности работы и достоверности данных, иные функции предусмотрены Законом 1997 г. о Генеральном ревизоре[622]. Отчеты Генерального ревизора выносятся на рассмотрение Парламента, и в тот же день, когда отчеты разрешены к публикации, они публикуются на веб-сайте Управления национального аудита.

Национальное ревизионное управление (Australian National Audit Office, ANAO) создано для содействия Генеральному аудитору. ANAO поддерживает проведение Генеральным ревизором полного спектра

---

England data protection audit report 2019. https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2614990/nhs-england-audit-es-201901.pdf (дата обращения: 05.08.2019)

[622] Auditor-General Act 1997. URL: https://www.legislation.gov.au/Details/C2018C00036 (дата обращения 10 07 2019)

аудиторских проверок и связанных с ними услуг и действует на основании Закона о Генеральном ревизоре, Закона о государственном управлении, результативности и подотчетности 2013 г.[623] и Закона о государственной службе[624].

Аудит ANAO проводится в том же порядке, что и обычные аудиторские проверки. ANAO разрабатывает руководства[625], публикует сводные материалы, в которых выявляет и анализирует общие повторяющиеся проблемы, недостатки и примеры передовой практики, выявленные в ходе аудита результативности работы.

Перечень стандартов ANAO состоит из семи стандартов[626], среди них нет ни одного ориентированного на аудит государственных информационных систем. При этом в ANAO действует Группа контроля качества систем и анализа данных, которая обеспечивает ANAO качественную ИТ-поддержку и ресурсы в области аудита качества и эффективности[627]. Кроме того, намерение ANAO развивать собственные компетенции в области ИТ-аудита подтверждается проведенным в 2012 году внешним аудитом ANAO (проводится независимым аудитором, назначаемым

---

[623] Public Governance, Performance and Accountability Act 2013. URL: https://www.legislation.gov.au/Details/C2017C00269 (дата обращения 16 10 2019)

[624] Public Service Act 1999. URL: https://www.deepl.com/translator#en/ru/Public%20Service%20Act%201999 (дата обращения 29 06 2019)

[625] Review of ANAO better practice guides. URL: https://www.anao.gov.au/work/better-practice-guide/review-anao-better-practice-guides (дата обращения 16 10 2019)

[626] Australian National Audit Office Auditing Standards 2018. URL: https://www.legislation.gov.au/Details/F2018L00179 (дата обращения 04 11 2019)

[627] Systems Assurance and Data Analytics Group. Roles, requirements and responsibilities. URL: https://www.anao.gov.au/careers/business-areas/systems-assurance-and-data-analytics-group (дата обращения 07 09 2019)

для аудита деятельности самого ANAO)[628] с целью оценки возможностей и ресурсов ANAO в области аудита информационных технологий (ИТ).

Из отчетов ANAO видно, что аудит информационных систем может являться составной частью более масштабного аудита информационных технологий федеральных ведомств[629].

Примером имплементации аудита информационных систем публичного сектора является штат Западная Австралия. Аудит информационных систем как самостоятельный вида проверок не закреплен законодательством штата. Тем не менее функции и полномочия Генерального аудитора, определенные законодательством штата в соответствующем Законе 2006 г.[630], обязывают его не реже раза в год направлять парламенту штата отчет о работе. Законодательной базой аудита является указанный выше Закон 2006 г., а также Стандарты, принятые Австралийским советом по стандартам аудита и подтверждения достоверности данных[631], и Заявление о практике аудита[632]. Органы штата, в

---

[628] External audit: IT Capability and Resourcing. Report by the Independent Auditor. https://www.anao.gov.au/files/external-audit-it-capability-and-resourcing-pdf 9дата обращения 12 09 2019)

[629] Perfomance Audit Report. Information Technology at the Department of Health and Ageing. URL: https://www.anao.gov.au/work/performance-audit/information-technology-department-health-and-ageing. Performance Audit Report. Information Technology in the Department of Veterans' Affairs-Follow-up Audit. https://www.anao.gov.au/work/performance-audit/information-technology-department-veterans-affairs-follow-audit (дата обращения 14 10 2019)

[630] Auditor General Act 2006.: https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_4780.pdf/$FILE/Auditor%20General%20Act%202006%20-%20%5B00-00-02%5D.pdf?OpenElement (дата обращения 09 10 2019)

[631] Australian Auditing Standards. https://www.auasb.gov.au/Pronouncements/Australian-Auditing-Standards.aspx (дата обращения 15 11 2019)

[632] Audit Practice Statement. https://audit.wa.gov.au/wp-content/uploads/2018/07/AuditPracStatement-July2018.pdf (дата обращения 18 06 2019)

отношении которых у Генерального аудитора существуют полномочия аудита, установлены Законом 2006 г.

В отчетах Генеральный аудитор обращает внимание Парламента на любой случай, в котором функции подотчетных органов власти не были адекватными или не были надлежащим образом выполнены. Офис Генерального аудитора на протяжении одиннадцати лет проводит ежегодный аудит информационных систем штата. Данный вид проверок относится к так называемому малому аудиту.

Малый аудит оценивает эффективность работы структур, механизмы внутреннего контроля и соблюдение законодательства, политики и добросовестности. В частности, в рамках ежегодного аудита информационных систем основное внимание уделяется компьютерной среде государственного сектора для определения того, насколько они поддерживают конфиденциальность, целостность и доступность информации. Целью проверки информационных систем является общий уровень компьютерного контроля структур, значительно использующих компьютерную среду, для выяснения, поддерживают ли они точность и целостность данных финансовой отчетности и ключевых показателей эффективности. В этот вид проверок входит и ежегодный аудит выборочной совокупности отдельных важных нефинансовых компьютерных приложений[633].

Офис Генерального аудитора Западной Австралии вправе привлечь к аудиту внешних подрядчиков, в том числе к аудиту информационных систем, оставаясь, однако, всецело ответственным за работу и содержание аудиторского отчета.

---

[633] Transparency Report. https://audit.wa.gov.au/wp-content/uploads/2018/05/Transparency-Report_May2018-3.pdf (дата обращения 22 10 2019)

По итогам аудита органы местного самоуправления в соответствии с Разделом 7.12A Закона о самоуправлении 1995 г.[634] обязаны изучить аудиторский отчет и принять меры по вопросам, поднятым в аудиторском отчете. Если аудитор выявил вопросы, оцененные им как существенные, местное самоуправление должно подготовить отчет о том, какие меры будут приняты. Копия отчета направляется министру местного самоуправления и размещается на веб-сайте местного самоуправления.

Примером подхода к ежегодному аудиту информационных систем структур публичного сектора в Западной Австралии является структура годового отчета Генерального аудитора за 2018 год[635]. В рамках аудита проверке подлежат два направления: ключевых бизнес-приложений, используемых структурами публичного сектора, и общей системы компьютерного контроля и ее возможностей.

Целью аудита общей системы является выявление ее слабых сторон, могущих серьезно влиять на деятельность правительства и скомпрометировать конфиденциальную информацию, находящуюся в распоряжении публичного сектора.

При аудите программных приложений определяется ряд приложений, которые обеспечивают процессы организации, касающиеся финансов, человеческих ресурсов, управления делами, лицензирования и выставления счетов.

Так, в 2018 году были обследованы бизнес-приложения, применяемые рядом органов штата: Система управления кадровой рекламой − Комиссия по государственному сектору, Усовершенствованная инфраструктура учета −

---

[634] LOCAL GOVERNMENT ACT 1995 - SECT 7.12A: http://classic.austlii.edu.au/au/legis/wa/consol_act/lga1995182/s7.12a.html (дата обращения 19 10 2019)

[635] Information Systems Audit Report 2019. https://audit.wa.gov.au/wp-content/uploads/2019/05/IS-Report-2019.pdf (дата обращения 10 11 2019)

Horizon Power[636], Система льгот пенсионеров − Управление государственных доходов, Новый земельный реестр − Управление земельной информации Западной Австралии.

При аудите исследовались систематическая обработка данных и содержание данных в разрезе следующих категорий контроля:

– политика и процедуры – являются ли они надлежащими и поддерживают надежную обработку информации,

– безопасность конфиденциальной информации – действует ли контроль обеспечения целостности и конфиденциальности информации и доступности информации в любое время,

– ввод данных – является ли ввод данных вводом точной, полной и авторизованной информации,

– резервное копирование и восстановление – адекватно и доступно ли в случае аварии,

– вывод данных – являются ли отчеты в режиме онлайн или на бумажном носителе точными и полными,

– обработка данных – обрабатывается ли информация по назначению и в приемлемые сроки,

– разделение обязанностей – исключена ли ситуация, при которой никто из сотрудников не выполняет и не может выполнять несовместимые обязанности,

– контрольный журнал – гарантирует ли контроль над журналами транзакций точность и полноту истории транзакций,

– обслуживание мастер-файлов, управление интерфейсами, подготовка данных – контроль за подготовкой данных, сбор и обработка первичных

[636] Horizon Power - энергетическая компания, принадлежащая правительству штата.

документов для обеспечения достоверности информации, точности, полноты и своевременности данных прежде чем они поступят в приложение.

Подходы к аудиту приложений, использующих данные государственных информационных систем, в Западной Австралии прослеживается на примере аудита одного из приложений - New Land Registry - Titles (NLR-T), которое применяет Управление земельной информации Западной Австралии (Landgate) для управления данными о собственности на землю и местонахождении собственности[637].

Приложение частично автоматизирует оформление земельных участков в бумажной форме. Приложение разработано и продолжает поддерживаться по соглашению с внешним подрядчиком в области ИКТ с использованием общедоступной облачной инфраструктуры.

Landgate является государственным органом, подотчетным Министру земель. Орган управляет информацией о собственности и земле и ведет реестр прав собственности на землю в соответствии с Законом 1893 г. о передаче земли. Орган использует Приложение NLR-T для управления информацией о праве собственности на землю, включая передачу права собственности, ипотеку и погашение ипотечных кредитов.

Отчет Генерального аудитора содержит перечень проблем в области функционирования Приложения, рекомендации по их устранению, а также устанавливает сроки необходимых изменений. В отчете также приводится ответ Landgate, подтверждающий согласие с выводами Генерального аудитора, а также информирующий о шагах, которые сделаны или будут сделаны к указанной в отчете дате, для выполнения всех рекомендаций Генерального аудитора.

---

[637] Information Systems Audit Report 2019. Стр.29. URL: https://audit.wa.gov.au/wp-content/uploads/2019/05/IS-Report-2019.pdf (дата обращения 26 09 2019)

Целью аудиторских проверок в области систем общего компьютерного контроля (ОКК) является оценка уровня конфиденциальности, целостности и доступности средств компьютерного контроля информационных систем. Общий компьютерный контроль включает контроль над информационными технологиями, компьютерными операциями, доступом к программам и данным, над программными изменениями. Генеральный аудитор самостоятельно определяет направления контроля; его отчеты за 2017 и 2018 годы показывают, что аудит проводится по следующим направлениям: информационная безопасность, непрерывность деятельности, управление ИТ-рисками, ИТ-операции, контроль над изменениями, физическая безопасность.

Для оценки потенциала обследуемых организаций используются модели зрелости возможностей[638] как способ оценки уровня развития и возможностей механизмов контроля ИТ. Модель внедрена Офисом Генерального аудитора на основании общепринятого передового отраслевого опыта[639] и дает ориентиры для оценивания результатов работы органа.

Изучение опыта штата показывает, что роли участников процесса аудита информационных систем в целом определены, равно как и определены действия участников аудита по итогам проверки. При проведении аудита Генеральный аудитор придерживается руководств и аналитических материалов, опубликованных на федеральном уровне, но

---

[638] Модель зрелости можно рассматривать как набор структурированных уровней, описывающих, насколько вероятно, что поведение, практика и процессы организации могут надежно и устойчиво давать требуемые результаты. URL: https://www.apsc.gov.au/capability-maturity-models (дата обращения 17 10 2019)

[639] Работу в области информирование о лучших практиках и существующих разработках в области оценки человеческого капитала и организационного потенциала государственного и частного секторов осуществляет Комиссия государственной службы Австралии. URL: https://www.apsc.gov.au/publications (дата обращения 01 10 2019)

использует самостоятельно разработанные методологии аудита информационных систем и формы итоговых отчетов.

Таким образом, характерной особенностью аудита является акцент на проверку качества (зрелости) управления информационными системами, которое должно обеспечить конфиденциальность информации, имеющейся в распоряжении государственных органов. Отдельное внимание уделяется отношениям таких структур с привлекаемыми третьими лицами, которым на аутсорсинг передаются отдельные задачи по обеспечению функционирования ИКТ, а также приобретению приложений, обсуживающихся в «облаке». Ключевой задачей аудита является подтверждение того, что идентификация рисков и обеспечение соответствующей функциональности, безопасности и надежности контролируется проверяемыми структурами всегда, вне зависимости от привлечения подрядных организаций.

Качество данных, находящихся в информационных системах, их актуальность и достоверность не являются объектом аудиторской проверки.

2.5.7 Особенности подходов в праве Сингапура

За цифровизацию государственных систем и органов отвечает уполномоченный орган − Агентство государственных технологий[640], внутри которого действуют различные комитеты, в том числе Комитет по рискам и аудиту. Комитет занимается определением и оперативным устранением рисков оборота государственных данных, методиками работы с противоречиями внутри ГИСов и т.д.

Однако каждый государственный орган самостоятельно управляет своими данными и/или своим сектором данных внутри общей инфраструктуры, определяет процедуры проверки данных, устранения

[640] https://www.tech.gov.sg/digital-government-transformation/ (дата обращения 05 09 2019)

ошибок, проверки систем и распределение ответственности за нарушения с вендорами информационных компонентов. Например, Министерство здравоохранения самостоятельно управляет ошибками и утечками данных[641].

Как правило, государственные органы назначают сотрудников, ответственных за внутренний аудит, обеспечение информационной безопасности.

2.5.8 Особенности подходов в праве Российской Федерации

Система мониторинга и аудита данных государственных информационных систем в Российской Федерации осуществляется посредством создания и развития федеральной государственной информационной системы координации информатизации.

Пунктом 4 Положения о федеральной государственной информационной системе координации информатизации, утвержденного постановлением Правительства Российской Федерации от 14 ноября 2015 № 1235 «О федеральной государственной информационной системе координации информатизации»[642], определены задачи данной федеральной системы, в том числе:

– учет мер по созданию, развитию, модернизации, эксплуатации информационных систем и компонентов информационно-коммуникационной инфраструктуры, осуществляемых федеральными органами исполнительной власти и органами управления государственными внебюджетными фондами (далее - мероприятия по информатизации), и мониторинг реализации мероприятий по информатизации,

---

[641] https://www.gov.sg/~/sgpcmedia/media_releases/parl/press_release/P-20190228-2/attachment/Order%20Paper%20-%201Mar19.pdf (дата обращения 05 09 2019)

[642] СЗ РФ. № 47. Ст. 6599.

– планирование и обеспечение проектного управления реализацией федеральными органами исполнительной власти и органами управления государственными внебюджетными фондами мер по информатизации,

– контроль за соблюдением требований, предусмотренных частью $2^1$ статьи 13 Закона №149-ФЗ к размещению технических средств информационных систем, используемых субъектами системы координации, и требований, указанных в подпункте «в» настоящего пункта,

– планирование и реализация мероприятий по информатизации в отношении информационных систем и компонентов информационно-коммуникационной инфраструктуры, информация о которых размещена в системе координации, а также обеспечение взаимодействия участников планирования,

– мониторинг и анализ результативности создания, развития и эксплуатации федеральными органами исполнительной власти и органами управления государственными внебюджетными фондами информационных систем и компонентов информационно-коммуникационной инфраструктуры на всех этапах их существования,

– сбор, обработка и хранение разработанных государственными органами, органами управления государственными внебюджетными фондами и органами местного самоуправления в результате создания и развития информационных систем алгоритмов и (или) программ для электронных вычислительных машин в национальный фонд алгоритмов и программ для электронных вычислительных машин,

– обеспечение предоставления субъектам системы координации содержащихся в национальном фонде алгоритмов и (или) программ для электронных вычислительных машин для использования при внедрении информационных технологий в их деятельность,

– обработка и анализ сведений об уровне информатизации федеральных органов исполнительной власти, органов исполнительной власти субъектов федерации и органов местного самоуправления,

– контроль за выполнением субъектами Российской Федерации обязательств, предусмотренных соглашением о субсидиях на реализацию проектов, направленных на становление информационного общества в субъектах федерации, а также за соблюдением ими условий выделения указанных субсидий,

– мониторинг выполнения проектов в сфере информатизации в субъектах Российской Федерации.

В целях информационной открытости деятельности органов исполнительной власти и органов местного самоуправления, повышения качества и доступности предоставляемых ими государственных и муниципальных услуг в Российской Федерации созданы государственные информационные системы «Федеральный реестр государственных и муниципальных услуг (функций)» и «Единый портал государственных и муниципальных услуг (функций)».

В соответствии с пунктом 5 Правил ведения федеральной государственной информационной системы «Федеральный реестр государственных и муниципальных услуг (функций)», утвержденных постановлением Правительства Российской Федерации от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»[643], размещение сведений о государственных услугах (функциях) в реестре государственных услуг (функций), предоставляемых (исполняемых) федеральными органами исполнительной власти, государственными корпорациями и (или) органами государственных внебюджетных фондов, входящем в состав федерального реестра, осуществляют федеральные органы исполнительной власти,

[643] СЗ РФ. 2011. № 44. Ст. 6274.

государственные корпорации, органы государственных внебюджетных фондов, предоставляющие соответствующие государственные услуги (исполняющие соответствующие государственные функции) после включения соответствующей государственной услуги (функции) в перечень государственных услуг и государственных функций по осуществлению государственного контроля (надзора).

Одним из принципов правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации, в том числе в государственных информационных системах, является достоверность информации (пункт 6 статьи 3 Закона № 149-ФЗ), обеспечиваемая системой нормативных правовых актов, регулирующих жизненный цикл государственной информационной системы. В соответствии с частью 2 статьи 10 Закона № 149-ФЗ информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

Часть 9 статьи 14 Закона № 149-ФЗ определяет, что государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

Согласно части 8 статьи 14 Закона № 149-ФЗ технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны

соответствовать требованиям федерального законодательства о техническом регулировании.

В соответствии с частью 1 статьи 5 Федерального закона от 27 декабря 2002 № 184-ФЗ «О техническом регулировании»[644] (далее – Закон № 184-ФЗ) в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа обязательными требованиями наряду с требованиями технических регламентов являются требования, установленные государственными заказчиками, федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, государственного управления использованием атомной энергии, государственного регулирования безопасности при использовании атомной энергии, и (или) государственными контрактами (договорами).

Для обеспечения защиты информации, содержащейся в государственных информационных системах, применяются средства защиты, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям к безопасности информации в соответствии со статьей 5 Закона № 184-ФЗ, а также уполномоченными государственными органами, операторами государственных информационных системах принимаются меры организационного характера, установленные специальными нормативными правовыми актами (при наличии) в отношении каждой из государственных информационных систем, регулирующими контроль достоверности информации исходя из специфики данных системы,

---

[644] СЗ РФ. 2002. № 52 (Часть I). Ст. 5140.

а также нормативными актами в области обеспечения безопасности и противодействия техническим разведкам, технической защиты информации, в том числе определяются должностные лица, ответственные за защиту информации, утверждены и вводятся в действие локальные нормативные акты, регулирующие порядок защиты и контроля информации.

Согласно пункту 1 Требований, мероприятия по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем и дальнейшему хранению содержащейся в их базах данных информации, осуществляются федеральными органами исполнительной власти.

В целях выполнения требований о защите информации, предусмотренных пунктом Требований, органы исполнительной власти определяют требования к защите информации, содержащейся в системе органа исполнительной власти, для чего осуществляют:

– определение информации, подлежащей защите от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации,

– анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать система,

– классификацию системы в соответствии с требованиями о защите информации,

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в системе, и разработку на их основе модели угроз безопасности информации,

– определение требований к информационной системе (подсистеме) защиты информации, содержащейся в системе.

Создание государственной информационной системы осуществляется в соответствии с техническим заданием с учетом модели угроз безопасности информации, а также уровней защищенности персональных данных при их

обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных и требований настоящего документа.

Модель угроз безопасности информации и (или) техническое задание на создание системы согласуются с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

Техническое задание на создание государственной информационной системы должно включать требования к защите информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации и классификацию государственной информационной системы в соответствии с требованиями о защите информации.

Пунктом 5 Требований определены последовательные этапы создания системы: разработка рабочей документации на государственную информационную систему и ее части, разработка или адаптация программного обеспечения, пусконаладочные работы, предварительные испытания системы, проведение опытной эксплуатации государственной информационной системы, проведение приемочных испытаний системы.

Техническое задание на создание государственной информационной системы утверждается должностным лицом федерального органа исполнительной власти, на которое возложены соответствующие полномочия (пункт 4 Требований).

Этап разработки рабочей документации на систему и ее части включает разработку, согласование и утверждение документации, содержащей сведения, необходимые для выполнения работ по вводу системы в эксплуатацию и ее эксплуатации, и порядка эксплуатации системы, содержащего сведения, необходимые для выполнения работ по поддержанию уровня эксплуатационных характеристик (качества) системы (в том числе по

защите информации), установленных в проектных решениях, указанных в пункте 6 настоящего документа, в том числе контроль работоспособности системы и компонентов, обеспечивающих защиту информации. Орган исполнительной власти или частный партнер осуществляют эксплуатацию системы в соответствии с рабочей документацией.

Доработка программно-технических средств государственной информационной является развитием системы. В соответствии с пунктом 17 Требований мероприятия по развитию системы осуществляются в соответствии с требованиями, установленными для создания системы.

Статьей 13.14 Кодекса Российской Федерации об административных правонарушениях[645] предусмотрена ответственность за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Ответственность за незаконные разглашение или использование сведений, составляющих коммерческую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, предусмотрена частями 2 - 4 статьи 183 Уголовного кодекса Российской Федерации[646].

Таким образом, мониторинг и аудит государственных информационных систем, защита данных, содержащихся в государственных информационных системах, их достоверность, регулируется системой нормативных правовых актов, устанавливающих координацию информатизации, федеральные реестры данных и обеспечивающих контроль

[645] СЗ РФ. 2002. № 1 (Часть I). Ст. 1.
[646] СЗ РФ. 1996. № 25. Ст. 2954.

и защиту государственных информационных систем и содержащихся в них данных на всех стадиях жизненного цикла (создание, эксплуатация и совершенствование систем).

Указанный комплекс мер, принятых на федеральном уровне, ставит целью обеспечение контроля и проверки функционирования государственных систем, однако, не затрагивает вопросов достоверности исходных сведений, направляемых в государственные информационные системы.

2.5.9 Выводы

В странах Европейского союза предусмотрены процедуры внутреннего и внешнего аудита государственных информационных систем.

Внутренний аудит предполагает проведение администратором информационных систем регулярных инвентаризационных мероприятий, направленных на выявление неточностей в обрабатываемых данных, дублирования информации и т.п.

Внешний аудит - главным образом контрольно-надзорные мероприятия вышестоящих органов и специально уполномоченных органов в сфере информационных технологий. По результатам внешнего аудита выносятся предписания об устранении нарушений, даются рекомендации по повышению эффективности государственных информационных систем, а виновные лица привлекаются к юридической ответственности. Реализация внутреннего и внешнего аудита обеспечивается требованиями к ведению реестров данных, координационными механизмами на этапах создания, изменения, прекращения ведения государственных информационных систем.

В странах общего права и Сингапуре выделяются следующие подходы:

– проведение аудита (проверок) на предмет соблюдения законодательства в области персональных данных, который включает проверку различных сфер регулирования и не имеет фокуса на аудите непосредственно информационных систем, в том числе государственных (Великобритания),

– аудит государственных информационных систем как одного из направлений аудита деятельности структур государственного сектора. Характерной особенностью такого аудита является упор на проверку качества (зрелости) управления информационными системами, которое должно обеспечить конфиденциальность информации, имеющейся в распоряжении структур публичного сектора, а также акцент на способности проверяемых структур обеспечить безопасность и надежность информационных систем.

Качество данных, находящихся в информационных системах, их актуальность и достоверность не являются объектом аудиторской проверки.

2.6 Правовое регулирование монетизации данных в государственных информационных системах, их продажи и оказания платных услуг с их использованием

2.6.1 Правовое регулирование в Европейском союзе

Директивой № 2019/1024 от 20 июня 2019 г. об открытых данных и последующем использовании информации публичного сектора[647] и предшествующей ей Директивой № 2003/98/ЕС от 17 ноября 2003г. о последующем использовании информации публичного сектора[648]. В новой Директиве сохраняется подход к ценообразованию за предоставление информации исходя из ограничения по возмещению предельных издержек. Возможность предоставления информации на основании лицензии публичного органа также сохраняется равно как и обязательное требование о стандартизации условий таких лицензий. Исключительные лицензии, как и

[647] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information // http://data.europa.eu/eli/dir/2019/1024/oj (дата обращения 13 10 2019)

[648] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information // http://data.europa.eu/eli/dir/2003/98/2013-07-17 (дата обращения 21 10 2019)

раньше, возможны только в отдельно определяемых национальными юрисдикциями случаях.

Европейской комиссией также в период действия предыдущей Директивы были выработаны дополнительные рекомендации о стандартизации лицензий и установлению цены за предоставление информации[649]. Уточняется, что формальные лицензии не обязательны во всех случаях – чаще достаточно указания, какая лицензия применяется (символьные системы Creative Commons, например). В любом случае условия использования информации должны быть доступны пользователю. Выделены пять категорий данных, которые с большей необходимостью должны быть предоставлены для последующего использования: геопространственные данные; пространственные данные о Земле и окружающей среде (погода, качественные показатели воды и земли); транспортные данные; статистические данные; данные о компаниях. Установлено деление видов издержек и более детально описаны возможные способы вычисления предельных издержек для определения цены предоставления данных публичного сектора.

Для понимания тенденция развития законодательства ЕС в сфере монетизации данных полезно обратиться к Отчету Еврокомиссии от 10 октября 2018 г. «О монетизации данных SMART» 2016/0063[650].

Отчет определяет три основных пути монетизации данных:

– прямой доход от продажи данных,

---

[649] Commission notice — Guidelines on recommended standard licences, datasets and charging for the reuse of documents № 2014/C 240/01, 24.07.2014 // https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2014.240.01.0001.01.ENG (дата обращения 03 08 2019)

[650] http://datalandscape.eu/sites/default/files/report/D3.3_Data_Monetization_10.10.2018_GM.PDF (дата обращения 06 10 2019)

– дополнительный доход от объединения данных с другими услугами или продуктами,

– обменные премии/ торговые преимущества или скидки.

В отчете названы условия развития концепции монетизации данных, среди которых упоминаются повышение ясности правовой базы, влияющей на монетизацию данных, поддержка малого и среднего предпринимательства для входа на рынок монетизации данных, расширение исследований в этой области.

Еврокомиссией организованы исследования силами ведущих ученых-юристов ЕС правовых аспектов повторного использования информации государственного сектора (LAPSI). В рамках данного проекта подготовлены различные документы по вопросам управления данными. В частности, в Позиционной бумаге LAPSI n. 1 «Принципы, регулирующие взимание платы за повторное использование информации государственного сектора»[651] отмечено, что в настоящее время по умолчанию организации государственного сектора вправе взимать плату за публичные данные в размере, необходимом для покрытия собственных издержек либо с минимальной наценкой. В развитие Директивы ЕС о повторном использовании информации государственного сектора LAPSI опирается на необходимость содействия появлению информационных сервисов и недискриминационный доступ к информации. В связи с этим приводится анализ вариантов, когда плата взимается только в компенсационных целях (с нулевой маржой) или с установлением предельного значения наценки сверх

[651] Позиционная бумага LAPSI n. 1: Принципы, регулирующие взимание платы за повтрное использование информации государственного сектора // http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8342 (дата обращения 29 10 2019)

затрат на обработку данных. В результате анализа основные доводы сделаны в пользу второго варианта.

2.6.2 Правовое регулирование в Германии

Закон «О повторном использовании информации государственного сектора» [652] устанавливает порядок доступа к информации государственного сектора, которая доступна для повторного использования. Отдельно оговорено, что информация, на которую имеют право библиотеки, музеи или архивы, а также информация, на которую распространяются авторские или смежные права или права промышленной собственности, может быть использована, только если это разрешено правомочиями, входящими в названные права или если субъект разрешил это использование.

Информация для повторного использования должна передаваться во всех запрашиваемых форматах и на тех языках, на которых она доступна, органом государственного сектора. И если это не требует «непропорциональных усилий» государственного органа, она должна передаваться полностью или частично в электронном виде, в открытом и машиночитаемом формате вместе со связанными метаданными. И форматы, и метаданные должны в максимально возможной степени соответствовать признанным стандартам.

Данный закон устанавливает плату за повторное использование информации в размере затрат на воспроизведение, предоставление и повторную передачу. Однако Законом определены исключения.

Если плата предусмотрена, государственные органы должны рассчитывать ее в соответствии с объективными критериям, отвечающими прозрачности, которая установлена. Также доходы таких организаций от

---

[652] Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen // Режим доступа: https://www.gesetze-im-internet.de/iwg/ (дата обращения: 10.08.2019)

предоставления информации и разрешения на их повторное использование в соответствующем отчетном периоде не должны превышать затрат на их сбор, производство, воспроизведение и распределение плюс «разумную норму прибыли». Сборы должны рассчитываться в соответствии с принципами бухгалтерского учета, применимыми к соответствующим органам государственного сектора.

Государственный орган обязан публиковать условия и фактическую сумму сборов, если такие сборы установлены за доступ к соответствующему набору данных, включая основные расчеты через общедоступные сети. В свою очередь данный Закон гарантирует равный доступ всех пользователей к информации повторного использования. Государственный орган может установить условия дальнейшего использования. Условия использования должны быть пропорциональными, не ограничивать конкуренцию и возможности для повторного использования данных. Условия повторного использования, которые применяются, должны быть определены заранее и, если это технически возможно, опубликованы в общедоступных сетях.

Во многом этим и объясняется, почему не предоставляются данные в эксклюзивном ключе. Названным законом запрещены эксклюзивные соглашения в части повторного использования информации, находящейся в распоряжении государственных органов, а также установлены условия использования такой информации, порядок определения сборов при использовании информации.

В законодательстве Германии можно выделить ряд законов земель, которые регулируют порядок доступа к государственным базам данным. В частности, Закон Бранденбурга о доступе к файлам и информации (AIG)[653] от

---

[653] Akteneinsichts- und Informationszugangsgesetz //Режим доступа: http://bravors.brandenburg.de/gesetze/aig (дата обращения 14.08.2019).

10 марта 1998 года устанавливает свободный доступ к базам данных, включая базы, содержащие личные данные или данные компаний, если такие субъекты выразили согласие на доступ. Законом также предусмотрена возможность местной администрации устанавливать плату за такой доступ. Размер платы определяется земельным правительством и Комитетом внутренних дел земли, при этом размер платы рассчитывается таким образом, чтобы обеспечить баланс затрат государственного органа на предоставление информации и интересов субъектов, реализующих свое право на доступ к информации.

Кроме того, в Германии широко применяются Открытые данные. По оценкам специалистов, опубликованные (открытые) данные обладают высоким экономическим потенциалом, в том числе для создания новых, ранее невозможных бизнес-моделей.

В Берлине, одной из передовых земель в области Открытых данных, активно используется портал «http://www.daten.berlin.de/». Многие исследовательские компании, институты, организации гражданских инициатив используют опубликованные на портале данные для их анализа в общественных интересах, для организации информационных служб и создания новых услуг. Среди порталов открытых данных также следует назвать портал открытых данных «http://www.odis-berlin.de» и Геопортал «https://www.geoportal.de».

В Берлине разработана Стратегия Открытых данных[654], в рамках которой проводится множество исследований и опросов в целях совершенствования нормативного регулирования и прикладного применения Открытых данных.

---

[654] Projekt Zukunft// Режим доступа: https://projektzukunft.berlin.de/ (дата обращения 17.08.2019).

Таким образом, в основной массе доступ к данным, содержащимся в государственных информационных системах, предоставляется на безвозмездной основе, что согласуется с расширенным толкованием концепции электронного правительства и упрощения доступа к административным услугам государственных органов. При этом в законодательстве как федеральном, так и земельном предусмотрена возможность взимания платы за доступ к публичной информации в целях компенсации затрат государственных органов на ее предоставление заинтересованным лицам. Наряду с этим ведется обширная исследовательская работа в направлении конкретизации и развития законодательных положений о монетизации государственных данных, в том числе и в целях взимания платы не только в компенсационных целях, но и с минимальной наценкой.

2.6.3 Правовое регулирование во Франции

Монетизация данных в государственных информационных системах реализуется посредством открытых данных и последующего использования информации. Ст. L322-1 Кодекса отношений между обществом и администрацией закрепляет общее условие последующего использования информации публичного сектора: информация не изменяется, ее смысл не искажается и указаны дата и источник последнего опубликования, если не было получено согласия публичного органа на иное ее использование. Ст. 322-6 Кодекса возлагает на публичные органы, которые создают или используют данные, обязанность создать и сделать доступным для пользователей список основных документов, в которых такие данные содержатся. Такой список должен ежегодно обновляться. Например, такой список размещен на сайте Центра экономически-финансовой

документации[655]. На сайте указаны общие условия использования. Предусматривается также использование специальных условий, которое осуществляется заключением договора об использовании между публичным органом и получателем данных. Для заключения такого договора нужно обратиться в центр путем заполнения формы в Интернете.

Помимо условий использования, в отношении информации из государственных информационных систем публичным органом также могут быть предоставлены лицензии. Наиболее четко различие между условиями использования и предоставлением лицензии прослеживается на примере открытых данных. Портал и сервисы открытых данных во Франции находятся в компетенции миссии ETALAB, одного из структурных подразделений DINSIC[656]. Общие условия использования открытых данных, утвержденные ETALAB, размещены в открытом доступе на сайте открытых данных[657], а также примерный список лицензий установлен ст. D323-2-1 Кодекса. Уточняется, что сам функционал платформы используется свободно и бесплатно. Исходный код платформы также размещен в открытом доступе по ссылке «https://github.com/opendatateam/udata». Примечательно, что открытые данные могут быть опубликованы не только публичными органами, но и иными лицами. Указано, что публичные органы публикуют наборы данных при использовании открытой лицензии[658]. Эта открытая лицензия установлена и разработана ETALAB. Она позволяет использовать данные следующими способами: воспроизведение и копирование; адаптация, модификация, изъятие и переработка в целях создания «производной

---

[655] https://www.economie.gouv.fr/cedef/repertoire-des-informations-publiques-des-ministeres-economiques-et-financiers-conditions (дата обращения 21 08 2019)

[656] https://www.etalab.gouv.fr/qui-sommes-nous (дата обращения 15 08 2019)

[657] https://www.data.gouv.fr/fr/terms/ (дата обращения 18 07 2019)

[658] Licence Ouverte V 2.0 https://www.etalab.gouv.fr/wp-content/uploads/2017/04/ETALAB-Licence-Ouverte-v2.0.pdf (дата обращения 01 10 2019)

информации»; сообщение, распространение, перераспределение, публикация и передача данных; использование в коммерческих целях, например путем объединения с другими данными, а также включение в собственный продукт или приложение. Условием использования является только обязательное указание источника и даты последнего обновления используемой информации. При этом пользователь может также разместить гиперссылку на набор используемых данных с указанием их принадлежности.

Иные лица, размещающие информацию на портале открытых данных, используют одну из открытых лицензий, соответствующих open definition[659]. Среди наиболее используемых выделяются Creative Commons CCZero (CC0), Open Data Commons Public Domain Dedication and Licence (PDDL), Creative Commons Attribution 4.0 (CC-BY-4.0) и иные. Кроме того, ETALAB на отдельной странице в Интернете размещает все доступные списки используемых лицензий[660]. Для программ ЭВМ предлагается использование таких свободных лицензий как Apache 2.0, MIT, BSD 2, BSD 3 и т.д. Примечательно, что в списке не содержатся лицензии GPL и иные вирусные лицензии.

В отдельных случаях может требоваться дополнительное согласование и уточнение условий использования. В таком случае, в соответствии со ст. D323-2-2 Кодекса отношений между обществом и администрацией[661] Одобрение осуществляется Премьер-министром в течение двух месяцев со дня подачи заявления. Заявление на согласование лицензии должно указывать данные, в отношении которых она будет выдана, и обосновывать специфику их использования. Все согласованные лицензии также

---

[659] http://opendefinition.org/licenses/ (дата обращения 09 10 2019)
[660] URL: https://www.data.gouv.fr/fr/licences (дата обращения 14 08 2019)
[661] URL: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000034504993&cidTexte=LEGITEXT000031366350&dateTexte=29991231 (дата обращения 23 09 2019)

опубликованы на специальной странице, посвященной лицензиям, на сайте ETALAB[662]. Например, для Национального института индустриальной собственности (INPI) в отдельном порядке согласованы две лицензии: на использование базы данных товарных знаков Франции, базы данных патентов Франции и ЕС, а также лицензия на использование данных из Реестра коммерции и обществ.

По общему правилу последующее использование информации публичного сектора не подлежит отплате (ст. L324-1 Кодекса отношений между обществом и администрацией). Одновременно публичные органы могут устанавливать возмещение за предоставление информации, когда такой орган обязан за счет собственных средств покрывать существенную часть издержек, связанных с осуществлением его публичных миссий. Равно ст. L324-2 Кодекса предусматривает возмещение за оцифровку информации для университетских библиотек, музеев и архивов. Размеры возмещений устанавливаются исходя из критериев объективности, транспарентности, подтверждаемости (vérifiables), и не-дискриминации. Одновременно, отдельным декретом также устанавливаются способы расчета возмещений и органы, которые могут устанавливать их[663]. В силу юридической техники содержание декрета частично включено также в текст Кодекса. Так, в ст. D324-5-1 Кодекса установлен указанный список. Например, Национальный институт географической информации и лесоводства может устанавливать плату за предоставление базы данных геолокализованных адресов. На

[662] URL: https://www.data.gouv.fr/fr/licences (дата обращения 24 09 2019)

[663] Décret n° 2016-1617 du 29 novembre 2016 relatif aux catégories d'informations publiques de l'Etat et de ses établissements publics administratifs susceptibles d'être soumises au paiement d'une redevance de réutilisation. https://www.legifrance.gouv.fr/eli/decret/2016/11/29/PRMJ1630605D/jo/texte (дата обращения 10 08 2019)

официальном сайте ETALAB также размещена таблица с уточнением способов расчёта максимального размера возмещений[664].

Кроме того, в главе 5 раздела 2 книги 3 Кодекса отношений между обществом и администрацией установлено правовое регулирование предоставления исключительного права на использование данных государственного сектора. Общие положения об исключительности, соответствующие установленным европейским правом подходам, не применяются к соглашениям между публичными лицами, с учетом конкурентного права. Соглашения об исключительности прозрачны и должны публиковаться в Интернете.

Особые случаи использования данных и уточнение взимания платы за них также регулируются и другими актами. Например, последующее использование данных системы регистрации транспортных средств осуществляется исключительно в целях, перечисленных в ст. L330-5 транспортного кодекса[665] (например, для целей статистических или исследовательских без того, чтобы полученные данные могли указать на конкретное лицо). Специфика особенного режима таких данных обусловлена их персональным характером. На сайте Министерства внутренних дел уточняется, что использование таких данных возможно только после получения лицензии, одобренной министерством, и является платным[666]. При этом в любом случае полученные данные запрашивающее лицо может использовать в коммерческих целях, а также предоставить право требования

---

[664] https://www.data.gouv.fr/fr/Redevances (дата обращения 24 06 2019)

[665] Code de la route. https://www.legifrance.gouv.fr/affichCode.do;jsessionid=72937776B1BC54575C2A628ED8BF4EB1.tplgfr25s_3?idSectionTA=LEGISCTA000006143842&cidTexte=LEGITEXT000006074228&dateTexte=20190903 (дата обращения 07 11 2019)

[666] https://www.interieur.gouv.fr/Repertoire-des-informations-publiques/La-reutilisation-des-donnees-du-systeme-d-immatriculation-des-vehicules (дата обращения 18 10 2019)

лицензии иному лицу вместо себя. Остальные способы использования согласуются отдельно в выдаваемой лицензии.

Французское право также использует концессионные соглашения и соглашения о государственном заказе, в которых могут содержаться условия использования данных публичного сектора. Например, в 2017 г. введены положения, уточняющие отношения с концессионерами по использованию данных[667]. Когда концессионеру передается исполнение публичной миссии, он обязан предоставить доступ к базам данных. Орган может свободно извлекать и использовать такие данные, а также делать базу данных общедоступной с предоставлением возможности последующего использования.

В 2015 г. контракты частно-публичного партнерства были отменены, и Ордонансом n° 2015-899 от 23 июля 2015 г. они включены в правовое регулирование государственного заказа[668]. Среди разновидностей договоров государственного заказа выделяются, например, государственный заказ «концепция-реализация», предполагающий возможность осуществления исполнителем исследования, а затем проведения работ (ст. 33), договоры государственного заказа глобальные секторные, которые позволяют поручить исполнителю создание и поддержание информационно-коммуникационных систем в интересах Министерства внутренних дел (п. 2° ст. 35).

Реализуя положения европейского права о последующем использовании информации публичного сектора, Франция предоставляет

---

[667] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique – закон о цифровой республике https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id (дата обращения 22 10 2019)

[668] Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030920376&categorieLien=id (дата обращения 15 11 2019)

данные в формате открытых данных для последующего использования, а также отдельные виды данных на особенных условиях (лицензиях, соглашениях исключительности). При этом по общему правилу данные могут использоваться и в коммерческих целях. Плата за использование данных публичного сектора взимается только в установленных законом случаях с указанием способа расчёта взимаемых сумм возмещения издержек.

2.6.4 Правовое регулирование в Эстонии

Вопросы оплаты предоставления данных из государственных информационных систем регулируются Актом о публичной информации Эстонии[669]. По общему правилу плата за такие данные с заявителя не взимается и расходы несет сам публичный орган, за исключением случаев, предусмотренных законом. Заявитель должен платить до 0,19 евро за каждую страницу документа, начиная с 21 страницы, если иное не предусмотрено законом.

Держатель информации может освободить заявителя от оплаты стоимости предоставления информации, если:

– взимание платы является экономически неэффективным,

– заявитель нуждается в информации для исследовательских целей,

– заявитель нуждается в информации для осуществления своих прав или обязанностей, а также в случае, если у заявителя отсутствуют финансовые возможности для покрытия расходов.

Плата взимается с заявителя перед предоставлением информации.

Ряд вопросов, касающихся монетизации открытых данных, в настоящий момент урегулированы на уровне Директивы Европейского союза

---

[669] https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения: 14.08.2019).

об открытых данных 2019[670], положения которой должны быть имплементированы в национальное законодательство. Положения Директивы развивают уже предусмотренные правила взимания платы за предоставление данных публичными органами, а также устанавливают принципы недискриминационного доступа к информации публичного сектора.

В Эстонии действует портал открытых правительственных данных[671], включающий информацию публичного сектора, которая может быть использована как в коммерческих, так и в некоммерческих целях. На данном портале открывается доступ не только к базам данных, но и к приложениям, основанным на публичных данных.

Для некоторых баз открытых данных предусмотрены специальные лицензии на использование. Так, в отношении топографической базы данных Земельным советом Эстонии разработаны лицензионные правила использования[672]. В частности, за держателем сохраняются все авторские права на базу данных. Лицензиат получает право на бесплатное использование данных в течение неопределенного срока, добросовестно, в соответствии с законодательством и лучшей практикой. Лицензиат может создавать производные базы данных, адаптировать и комбинировать данные со своими собственными (или другими) данными, продуктами или услугами, использовать данные в коммерческих или некоммерческих целях, распространять данные. В свою очередь, лицензиат обязуется ссылаться на

---

[670] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024 (дата обращения: 02.09.2019).

[671] Estonian Open Government Data Portal // Режим доступа: https://opendata.riik.ee/en/ (дата обращения: 02.09.2019).

[672] Licence of open data by Estonian Land Board // Режим доступа: https://geoportaal.maaamet.ee/eng/Ordering-Data/Open-Data-for-download/Estonian-Topographic-Database-p618.html?plugin_act=litsents (дата обращения: 02.09.2019).

источник данных при публикации и распространении данных (а также удалять ссылку по запросу лицензиара). Ссылка должна содержать имя лицензиара, название данных и дату извлечения данных из базы данных.

Лицензия исключают любую ответственность за качество данных в той степени, насколько это позволяет закон (to the maximum extent permitted by law), то есть исключает любые гарантии и заверения, иные обязательства. Лицензиат соглашается использовать данные, учитывая возможные неточности. Лицензиар не несет ответственности за любые ошибки или упущения в данных и за любые потери, вызванные их использованием. Лицензиар не отвечает за прямой или косвенный ущерб, который может возникнуть при использовании данных или невозможности их использования. В соответствии с лицензией лицензиар стремится обновлять базу данных на регулярной основе, но не гарантирует непрерывное предоставление данных в любой момент времени.

Итак, в Эстонии реализован общий для стран Европейского союза подход к монетизации данных в государственных информационных системах. По общему правилу данные предоставляются бесплатно, за исключением случаев, предусмотренных законом. Размер оплаты стоимости предоставления данных законодательно регламентирован. Данные предоставляются на конкурентных, недискриминационных началах. Как правило, данные предоставляются пользователю на основании лицензионного соглашения по модели Creative Commons с незначительной спецификой. В законодательстве Эстонии отсутствуют положения о государственно-частном партнерстве в области использования данных, что, однако, не исключает развитие совместных государственно-частных проектов в области использования данных на договорных началах.

2.6.5 Правовое регулирование в Великобритании

Как было отмечено выше, основу правового режима доступа к информации, находящейся в государственной информационной системе GOV.UK, составляет Акт о свободе информации. Вместе с тем Акт

концентрируется на единичных запросах об информации, а не на повторном использовании наборов данных, находящихся в государственной системе бизнесом.

Повторное использование наборов данных урегулировано в Регламенте о повторном использовании информации, находящейся в ведении государственных органов[673]. Регламент содержит положения, аналогичные европейским Директивам 2003/98/ЕС[674] и 2019/1024[675], подтверждая право частных субъектов на повторное использование информации, находящейся в ведении государственных органов в коммерческих и некоммерческих целях.

Однако у указанного общего правила допустимости повторного использования в иных целях существуют исключения. Так, не могут быть переданы для повторного использования:

– сведения, содержащие персональные данные,

– конфиденциальная информация,

– сведения, охраняемые в соответствии с законодательством о государственной тайне,

– сведения, представляющие охраняемый объект права интеллектуальной собственности третьих лиц,

– документы, доступные иными способами, за исключением подачи запроса в соответствии с Актом о свободе информации.

Акт уточняет требования к запросу на повторное использование, а также содержит обязанность государственных органов публиковать перечни

---

[673] The Re-use of Public Sector Information Regulations 2015. URL: http://www.legislation.gov.uk/uksi/2015/1415/contents/made (дата обращения: 05.08.2019).

[674] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003L0098 (дата обращения: 05.08.2019).

[675] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. https://eur-lex.europa.eu/eli/dir/2019/1024/oj (дата обращения: 05.08.2019).

данных для повторного использования и условия доступа к таковым. Срок ответа на запрос по общему правилу составляет 20 рабочих дней.

Если государственный орган требует соблюдения определенных условий, например, заключения лицензионного соглашения, такие условия не должны ограничивать способ повторного использования, а также не должны препятствовать конкуренции хозяйствующих субъектов, содействовать принципу недискриминации заявителей.

В части стандартных лицензий (упоминаемых в настоящем акте и в Директиве 2019/1024) укажем лицензию OGL[676], которая разработана Национальным архивом, используется рядом органов власти и применяется к служебным произведениям, права на которые принадлежат органам публичной власти (Crown copyright).

Раздел 14 указанного акта устанавливает в качестве общего правила недопустимость заключения эксклюзивных соглашений о повторном использовании. От этого правила можно отступать «в общественных интересах», при условии пересмотра таких соглашений каждые 11 лет. Любое эксклюзивное соглашение подлежит публикации.

За разрешение повторного использования может взиматься «разумная плата». Размер платы и условия использования должны быть опубликованы.

Необходимо отметить, что существуют акты рекомендательного характера, разъясняющие положения указанного Регламента. Одним из таких актов является Руководство по внедрению Регламента о повторном использовании информации, находящейся в ведении государственных

[676]Open Government License for public sector information.: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ (дата обращения: 05.08.2019).

органов для повторных пользователей (Guidance on the implementation of the Re-use of Public Sector Information Regulations 2015 for re-users) [677].

Руководство разъясняет, что под информацией публичного сектора понимается любая информация (контент) независимо от ее носителя (формы), включая печатные, цифровые или электронные звукозаписи, произведенная, хранящаяся или распространяемая органом государственного сектора. Указанная информация включает, но не ограничивается следующими категориями:

– законодательство,

– официальные отчеты о работе парламентов Великобритании, Шотландии,

– кодексы практики,

– геопространственные данные,

– метеорологические данные,

– консультационные и программные документы,

– статистика,

– финансовые и производственные данные,

– годовые отчеты, публикуемые государственными ведомствами, агентствами и местными органами власти,

– данные публичных реестров,

– патентная информация,

– руководящие указания по охране труда и технике безопасности,

– формы документов, публикуемые органами власти,

– сообщения для прессы,

---

[677] Guidance on the implementation of the Re-use of Public Sector Information Regulations 2015 for re-users https://www.nationalarchives.gov.uk/documents/information-management/psi-implementation-guidance-re-users.pdf (дата обращения: 05.08.2019)

– технические отчеты,

– информация о местном планировании,

– схемы публикации в соответствии с Актом о свободе информации,

– информация, хранящаяся в библиотеках, музеях и архивах.

Повторное использование означает использование информации государственного сектора в целях, отличных от первоначальной цели, для которой информация была подготовлена, хранится, собирается или распространяется.

В Руководстве также обращено внимание на то, что запрос на повторное использование – далеко не единственный способ сделать информацию доступной частным субъектам. В числе прочего руководство называет: информацию из государственных реестров, запрос на доступ к информации, иные способы.

Для облегчения доступа к информации органы публичной власти должны:

– публиковать информацию в существующем формате, преимущественно в электронном,

– использовать стандартные лицензии,

– рассматривать возможность повторного использования информации, в отношении которой был получен запрос в соответствии с Актом о свободе информации.

Также Руководство содержит разъяснения по вопросам возможных коллизий с тесно связанными актами в сфере защиты персональных данных, свободы информации, авторского права, открытых данных и иных сферах.

Дополнительно Руководство разъясняет ряд иных положений Регламента[678].

Любые жалобы, в части исполнения требований Регламента, Руководства органами публичной власти рассматриваются в административном порядке ICO.

Также существует возможность обратиться в трибунал 1 уровня (First-tier Tribunal).

Дополнительно стоит отметить, что платформа GOV.UK представляет возможность через сервис Gov.uk Registers, используя предусмотренные API, извлекать структурированные наборы данных, находящихся в ведении государственных органов в форматах CSV и ODS, в полном соответствии с вышеуказанным Регламентом.

Таким образом, в Великобритании существует правовая база, в рамках которой реализуется монетизация данных из системы GOV.UK.

2.6.6 Правовое регулирование в Австралии

Заявление федерального правительства о политике публичных данных [679] определяет публичные данные как все данные, собранные государственными органами для любых целей. Из ключевых решений, вынесенных в рамках данного Заявления, следует отметить следующие:

– неконфиденциальные данные должны быть открытыми по умолчанию, должны сохраняться и часто обновляться,

---

[678] Guidance on the implementation of the Re-use of Public Sector Information Regulations 2015 for re-users. URL: http://www.nationalarchives.gov.uk/documents/information-management/psi-implementation-guidance-re-users.pdf (дата обращения: 05.08.2019).

[679] Australian Government Public Data Policy Statement. https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf (дата обращения 11 08 2019)

– неконфиденциальные данные исследований, финансируемых государством по возможности должны быть открыты для использования и повторного использования,

– федеральные государственные учреждения (entities) должны взимать плату только за специализированные услуги передачи данных и по возможности должны публиковать полученные ими данные как по умолчанию открытые,

– когда это возможно, такие данные должны быть доступными с помощью бесплатных и простых в использовании интерфейсов прикладного программирования (API),

– все новые системы должны обеспечивать обнаруживаемость, интероперабельность, доступность данных и информации, а также экономичный доступ для облегчения доступа к данным,

– обмен данными между государственными учреждениями должен быть безопасным и обеспечивающим конфиденциальность для поддержания индивидуальной и национальной безопасности, коммерческой тайны,

– федеральные государственные учреждения должны открыто взаимодействовать со штатами и территориями в целях обмена данными и их интеграции в отношении вопросов, имеющих важное значение для каждой юрисдикции и на федеральном уровне.

В Заявлении было заявлено, что минимально закрепленным объемом обязанностей австралийских государственных учреждений является:

– опубликование надлежащим образом анонимизированных государственных данных на сайте data.gov.au или связанно с ним для возможности обнаружения и доступности данных,

– опубликование данных в машиночитаемом, пространственно-территориальном формате с высококачественным, простым в использовании и свободно доступным API; с описательными метаданными и с использованием согласованных открытых стандартов,

– обновление данных в автоматическом режиме,

– по общему правилу, опубликование данных по лицензии Creative Commons By Attribution.

Фактический доступ к публичным данным может быть сделан через data.gov.au или непосредственно через государственную организацию, которая хранит эти данные. Отказ в доступе к публичным данным может быть обжалован. пользователи могут обжаловать это решение путем использования функции публичного запроса, доступной на сайте data.gov.au.

Для помощи государственным учреждениям в том, как приступить к опубликованию наборов открытых данных, содержащихся в их информационных системах, был разработан инструментарий для работы с открытыми данными – Open Data ToolKit[680]. Инструментарий содержит перечень подробных инструкций для государственных учреждений, среди которых:

– техническая и иная поддержка в вопросах функционирования data.gov.au, включающая вопросы присоединения к платформе, опубликования датасетов, их визуализации, структуру описания данных, единый подход к опубликованию данных[681],

– рекомендации по разработке собственной политики обнародования данных публичного сектора и ссылки на разработанные и опубликованные политики отдельных государственных структур[682],

– рекомендации по составлению практических планов по повышению уровня открытости данных, включающие подходы к самооценке, советы по созданию стратегий открытых данных, а также по выбору для данных для формирования датасетов[683],

---

[680] Open Data Toolkit. https://toolkit.data.gov.au/ (дата обращения 28 09 2019)
[681] How to use data.gov.au. https://toolkit.data.gov.au/How_to_use_data.gov.au.html (дата обращения 10 08 2019)
[682] Policy. https://toolkit.data.gov.au/Policy.html (дата обращения 06 10 2019)
[683] Planning. https://toolkit.data.gov.au/Planning.html (дата обращения 30 09 2019)

– рекомендации по публикации открытых данных, включая инструкции по созданию наборов данных из новых или существующих данных, что такое метаданные и как их добавлять, какие лицензии могут быть использованы для открытых данных, инструменты для поиска опубликованных данных и иные рекомендации.

Аналогичный подход по разработке инструментария для работы с открытыми данными прослеживается и на уровне штатов. Примером могут служить инструкции и рекомендации, разработанные для учреждений Южной Австралии[684].

Условия использования наборами государственных данных, размещенных на портале data.gov.au, приведены на этом же сайте[685]. Опубликование данных по лицензии Creative Commons By Attribution означает, что пользователь вправе делиться информацией (копировать и распространять материал на любом носителе или в любом формате), а также адаптировать ее (любым образом преобразовывать и развивать материал) как в некоммерческих, так и в коммерческих целях. Лицензия Creative Commons By Attribution означает, что лицензиар не может отозвать эти свободы, пока пользователь соблюдает условия лицензии. Важно отметить, что в Условия использования пользователь уведомляется о том, что наборы данных, предоставляемые через data.gov.au, были созданы различными государственными органами. В связи с этим никто не гарантирует пользователю качество или своевременность данных.

Проект data.gov.au был создан в рамках Департамента Премьер-министра и Кабинета и впоследствии был передан в Агентство цифровой

---

[684] Policies and Guidelines. https://dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/policies-and-guidelines; Toolkits. https://dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/toolkits (дата обращения 10 06 2019)

[685] Terms of Use. https://data.gov.au/page/about (дата обращения 12. 10. 2019)

трансформации (DTA). В настоящее время работа портала data.gov.au обеспечивается открытой программной платформой MAGDA (Making Australian Government Data Available), которая первоначально была разработана в качестве открытого агрегатора данных для data.gov.au. Сейчас платформа MAGDA развивается благодаря Data 61[686], Агентству цифровой трансформации (Digital Transformation Agency), CSIRO по земельным и водным ресурсам CSIRO Land and Water[687] и ряду иных ведомств.

Требования к защите информации, доступ к которой осуществляется путем доступа к открытым данным публичного сектора, реализуется программными средствами, заложенными в платформу MAGDA[688] и описанными в документации проекта.

Кроме того, условия использования портала data.gov.au содержат оговорку, ограничивающую ответственность data.gov.au перед пользователем сайта (в том числе, государственным учреждением, размещающим наборы данных). Среди прочего указано, что data.gov.au прилагает все разумные усилия, чтобы загруженная информация не были скомпрометирована, однако не гарантирует отсутствие вредоносных кодов на портале. Тем самым ответственность за минимизацию рисков, обычно проистекающих из работы с сайтами в Интернете, использование соответствующего и современные

---

[686] DATA 61 - подразделение SCIRO, ведущая австралийская группа инноваций в области данных. DATA 61 сотрудничает с правительствами (а также с коммерческим сектором) в целях содействия эффективного обнаружения данных, обеспечения доступа к ним при одновременной защите частной жизни и проведения углубленного анализа данных.

[687] SCIRO – государственное юридическое лицо, созданное и функционирующее в соответствии с положениями Закона о научных и промышленных исследованиях 1949 года (Science and Industry Research Act 1949). Задачами SCIRO являются проведение прикладных исследований для содействия промышленности Австралии, продвижения интересов австралийского общества и достижения иных общественно значимых целей, определенных в соответствии с регулирующим законодательством. https://www.csiro.au/en/About/We-are-CSIRO (дата обращения 14 06 2019)

[688] Magda Documentation. https://magda.io/docs/ (дата обращения 11 06 2019)

файерволлов и антивирусного программного обеспечения для защиты своих компьютерных систем. Кроме того, указано, что data.gov.au не несет ответственности за убытки, вызванные информацией, которую пользователь отправляете на сайт или через него.

Правительственные открытые данные по интеллектуальной собственности (IPGOD) и государственные открытые данные по интеллектуальной собственности (IPGOLD) являются общедоступными наборами данных по правам интеллектуальной собственности (размещенными на сайте data.gov.au).

IPGOD обновляется ежегодно и является первым полным и общедоступным национальным реестром IP (intellectual property), связывающим права на коммерческие номера в простом формате данных. IPGOLD - это еженедельно обновляемая версия IPGOD, которая позволяет получать максимально актуальные данные за всю историю администрирования прав интеллектуальной собственности.

Служба Интеллектуальной собственности (IP Australia) является государственным федеральным учреждением, управляющим правами интеллектуальной собственности (ИС) и законодательством в отношении патентов, товарных знаков, образцов и прав селекционеров.

Наборы данных, размещенных на сайте data.gov.au отслеживают все аспекты процесса подачи заявки, включая основные даты, заявителей и их заявки, а также вид предоставленных прав ИС. Они также собирают вспомогательную информацию, такую как уникальные идентификаторы, сведения о заявителях и их агентах. Это позволяет проводить исследования и анализ на уровне отдельной компании. Данные также позволяют пользователям узнавать, где произошли инновации по географическому положению, размеру предприятия и типу технологии.

В рамках «Национальной повестки дня в области инноваций и науки: Платформы для структуры открытых данных» Правительство Австралии рассматривает возможности повышения ценности общедоступных данных,

создавая платформы для системы открытых данных. Проект «Регулирование как платформа» (Regulation as a Platform)[689] является таким проектом, целью которого является максимизация ценности регулирования в качестве ключевого набора данных правительства.

В рамках данного проекта должна быть решена задача по преобразованию существующего государственного регулирования в цифровую логику, что включает:

– преобразование нормативных правил в машиночитаемую логику, отражающую замысел и функционирование регулирования,

– проверка качества этих правил и их утверждение для публикации на открытой платформе,

– предоставление любому лицу возможности использовать данные регулирования через API открытой платформы для разработки инструментов и услуг, упрощающих взаимодействие конечных пользователей с регулирующими органами в целях снижения затрат, времени и сложности.

Конечная цель заключается в использовании потребителями инфраструктуры Платформы через публичные API для разработки инструментов и услуг, помогающих снизить нагрузку на компанию, управлять сложностью и экономить время и деньги пользователей, что обеспечит, по мнению создателей, значительный, в том числе коммерческий потенциал данного проекта и отдельных приложений, разработанных на его основе:

– для пользователей (владельцев бизнеса, специалистов по контролю соответствия и юристов-практиков), позволяя им автоматизировать и упростить утомительные и повторяющиеся ручные процессы и обеспечивая поддержку решений по вопросам соответствия или в качестве инструмента

[689] DATA 61. SCIRO.Regulation as a Platform. https://data61.csiro.au/en/Our-Work/Future-Cities/Optimising-service-delivery/RaaP (дата обращения 29 06 2019)

проверки при внесении изменений в нормативные акты или при рассмотрении новых видов деятельности,

– для частного и государственного секторов, оставляя им возможность создания собственных приложений для решения собственных проблем с соблюдением нормативных требований или требований конечных пользователей.

Несмотря на то, что значительная категория данных публичного сектора по общему правилу относится к категории открытых данных, в Австралии практикуется коммерческий доступ к наборам данных публичного сектора − микроданным (Microdata). Под микроданными понимаются данные, собираемые Бюро статистики (Australian Bureau of Statistics (ABS)) из целого ряда источников, включая исследования, переписи населения и административные сборы данных. Эта информация используется для создания файлов микроданных, содержащих подробную информацию о физических лицах, компаниях и других группах. В таких файлах каждая запись или строка набора данных содержит информацию, относящуюся к одному лицу, домашнему хозяйству или бизнесу.

Определение о переписи населения и статистических данных (выпуск информации и доступ к ней) 2018 г. (The Census and Statistics (Information Release and Access) Determination 2018) позволяют ABS предоставлять доступ к неидентифицированным индивидуальным статистическим данным (микроданным) для проведения социально-экономических исследований и анализа. Определение не обязывает ABS публиковать файлы микроданных, а лишь устанавливает такую возможность, определяя минимальные условия, которые должны быть согласованы ранее открытия доступа к микроданным, а также санкции при нарушении этих условий.

Доступ к микроданным открывается по разрешению, данному ABS в отношении конкретной заявки. Условия и порядок использования микроданных зависят от типа микроданных, доступ к которым запрашивается пользователем. Некоторые наборы данных (Census

TableBuilder[690] Guest) доступны в качестве гостевого пользователя без регистрации. Для доступа ко всем другим сериям данных TableBuilder или микроданных требуется регистрация и приобретение подписки.

Порядок определения оплаты обеспечивает одинаковые условия доступа к сервисам и микроданным и опубликован на соответствующем разделе сайта ABS[691], при этом с отдельных категорий лиц (физических лиц, студентов и сотрудников некоторых вузов) плата может быть снижена или совсем не взиматься при выполнении условий (например, участие университета в соглашении, заключенном с ABS). Подписка на сервисы ABS обеспечивает пользователям доступ ко всем учетным периодам в рамках определенной серии данных, доступ к новым наборам данных в день их публикации, возможность в любое время (без дополнительной оплаты) добавить в свою организацию неограниченное количество участников и иные возможности.

В целом определение стоимости доступа к микроданным и иным платным инструментам ABS определяется в соответствии с политикой ценообразования ABS[692] , которая, в свою очередь, основана на

---

[690] Table Builder - онлайновый инструмент создания таблиц и графиков на основе лежащих в их основе микроданных. Существуют опции отображения подсчетов, процентов и относительных среднеквадратических ошибок в таблице или вычисления средних, медиан и квантилей для непрерывных переменных, таких, как доход. Таблицы и графики обрабатываются автоматически, чтобы защитить конфиденциальность и конфиденциальность до того, как результаты будут предоставлены пользователю. About TableBuilder. https://www.abs.gov.au/websitedbs/D3310114.nsf/home/About+ TableBuilder (дата обращения 31 10 2019)

[691] Prices. https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Microdata +prices (дата обращения 04 09 2019)

[692] ABS Pricing Policy. https://www.abs.gov.au/websitedbs/D3310114.nsf/51c9a3d36edfd0dfca256acb00118404/12bb13b927110e44ca2569a80013bec1!OpenDocument (дата обращения 19 08 2019)

правительственной Системе взимания платы (Фреймворк)[693]. Данный документ был призван повысить согласованность действий по взиманию платы и содействовать определению того, когда целесообразно взимать плату за ту или иную деятельность правительства. Система взимания платы правительством охватывает виды деятельности, при которых правительство взимает сборы с неправительственного сектора за свою деятельность - регулирование, поставка товаров, оказание услуг или доступ к ресурсам или инфраструктуре. Система взимания платы устанавливает различные базовые рекомендации по определению платы, взимаемой в следующих основных категориях:

– плата, взимаемая с неправительственного сектора в целях возмещения некоторых или всех значительных издержек, связанных с регулирующей деятельностью, в рамках которой правительство стремится контролировать или влиять на поведение, управлять рисками и/или обеспечивать защиту общества,

– плата, взимаемая в рамках коммерческой деятельности, когда государство участвует на рынке товаров/услуг, и пользователь, как правило, обладает определенной свободой действий,

– платы, взимаемая за предоставление конкретных прав, привилегий или доступа к государственным ресурсам, инфраструктуре и/или оборудованию. Некоторые из этих видов деятельности могут иметь регулятивный (законодательный) компонент или требовать принятия законодательства, другие могут быть связаны с контрактами.

В зависимости от категории взимаемой платы указанный Фреймворк рекомендует применение различных моделей ценообразования.

---

[693] Australian Government Charging Framework (the Charging Framework). :https://www.finance.gov.au/resource-management/charging-framework/ дата обращения 03 06 2019)

Политика ценообразования ABS устанавливает определяет ключевые принципы, основываясь на которых, ведомство разрабатывает различные подходы к определению стоимости услуг по предоставлению доступа к информации, собираемой Бюро статистики. Политика ценообразования ABS определяет также базовый объем информации (ABS Basic Information Set), доступ к которому бесплатен в системе самообслуживания на сайте ABS.

Принимая во внимание требования к защите частной жизни и конфиденциальности, микроданные выпускаются с использованием специальных методов и систем, защищающих конфиденциальность.

Конфиденциальность микроданных обеспечивается Серией ABS[694], которая представляет собой краткий обзор законодательной базы для обеспечения конфиденциальности данных. Обзор объясняет, как оценивать риски конфиденциальности и управлять ими с применением модели пяти сейфов, и описывает методы обработки данных как часть общего подхода к управлению рисками. Документ носит общий характер, при этом уделяя повышенное внимание управлению риском раскрытия информации при обработке микроданных (часть 5) и использовании микроданных ABS и их воздействии на качество исследований (часть 6). Обязательства пользователей микроданных установлены Руководством к их ответственному использованию[695].

В целом объем допустимого использования данных Бюро статистики, в том числе право на модификацию, зависит от условий получения доступа к информации. Так, пользователи обладают широкими правомочиями по использованию продукта, доступ к которому осуществляется на условиях

---

[694] The Confidentiality Information Series.: https://www.abs.gov.au/ausstats/abs@.nsf/mf/1160.0 (дата обращения 25 10 2019)

[695] 1406.0.55.003 - Responsible Use of ABS Microdata, User Guide.: https://www.abs.gov.au/ausstats/abs@.nsf/mf/1406.0.55.003 (дата обращения 21 10 2019)

лицензии Creative Commons Attribution 4.0 International[696]. В то же время использование микроданных ограничено неисключительной, не подлежащей передаче лицензии от ABS для Уполномоченных пользователей на использование микроданных в статистических и исследовательских целях, как это разрешено АБС в соответствии с Обязательствами по микроданным[697].

Таким образом, в Австралии предоставление данных публичного сектора по умолчанию предполагается бесплатным и осуществляется на основании соответствующих лицензий. Коммерческий доступ предусмотрен лишь к определенным наборам данных и обеспечивается на основании разрешения уполномоченного органа, ограничивающего при этом возможность повторного использовании данных с иными целями, нежели указанными в запросе.

Следует отметить, что в исследуемом законодательстве отсутствуют специальные положения, регулирующие создание и деятельность государственно-частных партнерств в области использования данных. При этом государственно-частные партнерства могут быть созданы заинтересованными сторонами путем структурирования ими договорных отношений.

2.6.7 Правовое регулирование в Сингапуре

Правительство Сингапура высоко оценивает значение оборота данных для экономического развития, в связи с чем для решения проблем такого оборота государственные органы объединяют усилия не только между собой,

---

[696] Creative Commons licensing.: https://www.abs.gov.au/websitedbs/D3310114.nsf/4a256353001af3ed4b2562bb00121564/8b2bdbc1d45a10b1ca25751d000d9b03?opendocument? (дата обращения 03 06 2019)

[697] Microdata Undertakings. : https://www.abs.gov.au/websitedbs/D3310114.nsf/4a256353001af3ed4b2562bb00121564/fbc2f58b38f184bfca2573a6001001d3!OpenDocument (дата обращения 12 07 2019)

но и с частными компаниями. В частности, Комиссия по конкуренции Сингапура (Credit Counselling Singapore; CCS)[698] провела исследование[699] с целью исследования ландшафта данных в Сингапуре. Исследование было проведено в сотрудничестве с Комиссией по защите персональных данных (Personal Data Protection Commission: PDPC) и Ведомством интеллектуальной собственности Сингапура (The Intellectual Property Office of Singapore; IPOS)[700].

Помимо агрегаторов данных и брокеров данных, которые напрямую монетизируют оборот собранных ими данных, исследование показало, что прямая монетизация независимо собранных данных не имеет места в крупнейших секторах. Государственные органы также не монетизируют данные напрямую: данные обычно передаются бесплатно, например, через источники открытых данных[701]. Наиболее распространенный обмен данными происходит на уровне «маркетплейсов», о чем рассказано в следующем пункте.

2.6.8 Правовое регулирование в Российской Федерации

Вопрос о платности или бесплатности предоставления информации напрямую не относится к характеристике ее правового режима: возможно установление платы в рамках общего правового режима и отсутствие платы в рамках специального правового режима и наоборот.

В соответствии с частью 9 статьи 8 Закона № 149-ФЗ установление платы за предоставление государственным органом или органом местного

---

[698] Независимая неправительственная организация, зарегистрированная как благотворительная.

[699] https://www.cccs.gov.sg/-/media/custom/ccs/files/media-and-publications/publications/occasional-paper/ccs-big-data-paper-16-aug-2017nonconfi-final.pdf (дата обращения 16 05 2019)

[700] Уставной совет при Министерстве юстиции правительства Сингапура.

[701] URL: https://www.data.gov.sg. (дата обращения 16 05 2019)

самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Предоставляется бесплатно информация (часть 8 статьи 8 Закона № 149-ФЗ):

1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

В соответствии с частью 4 статьи 14 Закона № 149-ФЗ, если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьей 14 Федерального закона от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[702] (перечень содержит широкий круг информации о деятельности государственных органов Российской Федерации), государственные информационные системы должны обеспечивать размещение такой информации в Интернете в форме открытых данных.

Часть 4 статьи 8 Закона № 149-ФЗ определяет перечень информации, доступ к которой не может быть ограничен, а именно:

нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое

---

[702] Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009. № 7. Ст. 776.

положение организаций и полномочия государственных органов, органов местного самоуправления;

информация о состоянии окружающей среды;

информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информация, накапливаемая в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

иная информация, недопустимость ограничения доступа к которой установлена федеральными законами. Перечни информации, которая не может быть засекречена, установлены и в других законодательных актах. Для сравнения приведем перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию, закрепленный статьей 7 Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»[703]:

– о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях,

– о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности,

---

[703] Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. С. 8220-8235.

– о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям,

– о фактах нарушения прав и свобод человека и гражданина,

– о размерах золотого запаса и государственных валютных резервах Российской Федерации,

– о состоянии здоровья высших должностных лиц Российской Федерации,

– о фактах нарушения законности органами государственной власти и их должностными лицами.

Согласно части 1 статьи 14 Закона № 149-ФЗ государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

Таким образом,

если нормативным правовым актом, предусматривающим создание государственной информационной системы предусмотрено, что она создается в целях реализации полномочий государственного органа (государственных органов) или для обеспечения обмена информацией между государственными органами,

установление платы за предоставление данных из такой системы возможно только в случаях и на условиях, которые установлены федеральными законами. Из этого следует, что ни в постановлениях Правительства Российской Федерации, ни тем более в нормативных правовых актах федеральных органов исполнительной власти не должны устанавливаться случаи и условия платы за предоставление информации, если закон об этом умалчивает.

Однако зачастую законодатель поручает решать указанные вопросы Правительству Российской Федерации. При этом вопросы оплаты часто решаются по-разному в зависимости от субъекта, которому информация

предоставляется. Федеральным органам государственной власти, органам государственной власти субъектов федерации и местного самоуправления она предоставляется безвозмездно. На безвозмездной основе информация может предоставляться также пользователю для исследовательских, учебных и других некоммерческих целей. В иных случаях она предоставляется пользователям, как правило, на платной основе.

Плата за предоставление данных из государственных информационных систем, в частности, установлена в соответствии со следующими федеральными законами:

– пунктом 2 части 2 статьи 5 Федерального закона от 28 декабря 2013 г. № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации»[704] за предоставление содержащихся в государственном адресном реестре сведений об адресах в случае предоставления их на бумажном носителе и за предоставление обобщенной информации, полученной в результате обработки содержащихся в государственном адресном реестре сведений об адресах,

– частью 4 статьи 18 Федерального закона от 6 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете»[705] за пользование государственным информационным ресурсом бухгалтерской (финансовой) отчетности,

– частью 6 статьи 10 Федерального закона от 30 декабря 2015 г. № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении

---

[704] Федеральный закон от 28.12.2013 № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный закон "Об общих принципах организации местного самоуправления в Российской Федерации» // http://www.pravo.gov.ru. 2013.

[705] Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете» // СЗ РФ. 2011. № 50. Ст. 7344.

изменений в отдельные законодательные акты Российской Федерации»[706] за предоставление физическим и юридическим лицам, органам государственной власти и органам местного самоуправления пространственных данных и материалов, содержащихся в государственных фондах пространственных данных,

– частью 2 статьи 63 Федерального закона от 13 июля 2015 г. № 218-ФЗ «О государственной регистрации недвижимости»[707] за предоставление сведений, содержащихся в Едином государственном реестре недвижимости, аналитической и иной информации,

– частью 11 статьи 21 Федерального закона от 9 июля 1999 г. № 160-ФЗ «Об иностранных инвестициях в Российской Федерации»[708] за предоставление выписки из Государственного реестра аккредитованных филиалов, представительств иностранных юридических лиц, являющийся информационной системой о филиале, представительстве иностранного юридического лица или справки об отсутствии запрашиваемой информации,

– частью 2 статьи 7 Федерального закона от 14 марта 2009 г. № 31-ФЗ «О государственной регистрации прав на воздушные суда и сделок с ними»[709] за предоставление за предоставление информации о зарегистрированных правах на воздушные суда, выдачу копий договоров, а также документов, выражающих содержание односторонних сделок, совершенных в простой письменной форме (Единый государственный реестр прав на воздушные суда),

---

[706] Федеральный закон от 30.12.2015 № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2016. № 1. Ст. 51.

[707] Федеральный закон от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости» // СЗ РФ. 2015. № 29 (Часть I). Ст. 4344.

[708] Федеральный закон от 09.07.1999 № 160-ФЗ «Об иностранных инвестициях в Российской Федерации» // СЗ РФ. 1999. № 28. Ст. 3493.

[709] Федеральный закон от 14.03.2009 № 31-ФЗ «О государственной регистрации прав на воздушные суда и сделок с ними» // СЗ РФ. 2009. № 11. Ст. 1260.

– частью 6 статьи 10 Федерального закона от 8 ноября 2007 г. № 257-ФЗ «Об автомобильных дорогах и о дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»[710] за сведения из Единого государственного реестра автомобильных дорог,

– частью 7 статьи 57 Градостроительного кодекса Российской Федерации за предоставление сведений, документов и материалов, содержащихся в государственных информационных системах обеспечения градостроительной деятельности.

Порядок доступа к информации, содержащейся в государственных информационных системах, как на безвозмездной, так и на возмездной основе определяется в отношении каждой государственной информационной системы как правило, в соответствии с отдельным нормативным правовым актом.

Если такая система создается и функционирует в иных целях, плату за предоставление данных из такой системы возможно установить в соответствии с нормативным правовым актом, регулирующим порядок предоставления доступа данных, если в нормативном правовом акте, предусматривающем создание данной системы, или иных нормативных правовых актах, регулирующих функционирование системы, не установлены соответствующие ограничения.

В соответствии с пунктом 21 части 1 статьи 4 Федерального закона от 21 июля 2005 г. № 115-ФЗ «О концессионных соглашениях»[711]

---

[710] Федеральный закон от 08.11.2007 № 257-ФЗ «Об автомобильных дорогах и о дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2007. № 46. Ст. 5553.

[711] Федеральный закон от 21.07.2005 № 115-ФЗ «О концессионных соглашениях» // СЗ РФ. 2005. № 30 (Часть II). Ст. 3126.

государственные информационные системы могут быть объектами концессионного соглашения (далее – Закон № 115-ФЗ).

Согласно пункту 19 части 1 статьи 7 Федерального закона от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»[712] (далее – Закон № 224-ФЗ) данные системы могут быть объектами соглашения о государственно-частном партнерстве.

Монетизация в случае участия частных лиц в создании и функционировании государственной информационной системы реализуется путем установления концессионной платы (статья 7 Закона № 115-ФЗ) или возмещения расходов частного партнера (пункт 8 части 2 статьи 12 закона № 224-ФЗ)

Следует отметить, что часть $1^6$ статьи 5 Закона № 115-ФЗ вводит ограничение в отношении лиц, которые могут выступать концессионерами по концессионным соглашениям, заключаемых в отношении государственных информационных систем. Так, концессионером по такому концессионному соглашению не могут являться иностранные инвесторы (иностранные физические лица и (или) иностранные юридические лица), российские юридические лица, решения которых прямо или косвенно могут определять иностранные физические лица и (или) иностранные юридические лица, иностранные государства, их органы, за исключением случаев, определенных международным договором Российской Федерации, федеральным законом, решением Президента Российской Федерации.

---

[712] Федеральный закон от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2015. № 29 (Часть I). Ст. 4350.

Аналогичный запрет установлен в отношении частных партнеров при заключении соглашений о государственно-частных партнерствах в соответствии с частью 10 статьи 5 Закона № 224-ФЗ.

При создании или модернизации государственной информационной системы на основании концессионного соглашения или соглашения о государственно-частном партнерстве функции оператора данной системы в пределах, в объемах и в сроки, которые предусмотрены соответствующим соглашением, осуществляются концессионером или частным партнером (часть $5^1$ статьи 14 Закона № 149-ФЗ).

Таким образом, законодательство Российской Федерации определяет различные механизмы монетизации государственных информационных систем, что делает такую сферу оборота данными привлекательной для потенциальных инвесторов.

2.6.9 Выводы

По общему правилу информация из государственных информационных систем в странах Европейского союза предоставляется любому лицу бесплатно. Вместе с тем взимание платы допускается при превышении установленных объемов данных, а также в иных случаях, предусмотренных законом.

Отдельные положения законодательства (в том числе на наднациональном уровне – Директивы ЕС) содержат требования к определению цены предоставления данных в случаях их монетизации: размер платы не должен превышать издержки на предоставление данных плюс «разумную добавочную стоимость», необходимую для поддержания сервиса. Информация должна предоставляться на недискриминационных началах.

В странах ЕС функционируют порталы открытых правительственных данных, которые могут быть использованы как в коммерческих, так и в некоммерческих целях.

В некоторых странах ЕС законодательство содержит положения о концессионных соглашениях и соглашениях о частно-публичном партнерстве, в которых могут содержаться условия использования данных публичного сектора (Франция).

В странах общего права и Сингапуре выявлены следующие подходы к регулированию монетизации данных в государственных информационных системах, их продажи и оказания платных услуг с их использованием:

– запрет на эксклюзивные соглашения о предоставлении доступа к данным публичного сектора, как общее правило; а также открытые и равные для всех условия доступа,

– бесплатное предоставление данных публичного сектора или взимание минимальной платы, обусловленной технической работой, связанной с ее предоставлением, как общее правило; плата взимается за специализированные услуги, связанные с данными,

– использование различных лицензий в качестве правового основания для использования данных,

– возможность коммерческого доступа к определенным наборам данных на основании разрешения уполномоченного органа, в том числе, ограничивающего возможности по повторному использованию данных.

2.7 Правовое регулирование использования специальных финансовых и юридических инструментов для создания и обеспечения функционирования «маркетплейсов» (электронных площадок по обмену данными) на основе данных

2.7.1 Правовое регулирование в Европейском союзе

Евросоюз активно развивает единый рынок данных, включая данные публичного сектора. Европейской комиссией в 2013 г. была утверждена

Стратегия элементов цепочки стоимости данных[713], направленная на развитие единой экосистемы данных, открытых данных, экономики знаний, стимулов к исследованиям с использованием данных. Европейский исследовательский центр рынка данных, поддерживая достижения указанной стратегии, оценивает, измеряет и определяет европейскую экономику данных, предоставляя отчеты об исследованиях[714]. На его сайте размещена схема движения данных (data landscape)[715], показывающая, что рынок данных объединяет между собой владельцев и пользователей данных. Основными посредниками-участниками рынка данных при этом выступают: маркетплейсы данных, хранящие, обновляющие и обменивающие данные как основные посредники (по данным на сайте их всего 14)[716], ИТ-поддержка (IT-enablers), обеспечивающая функционирование технической инфраструктуры (164)[717], средства аналитики, включая, например, социальную аналитику, аналитические платформы, искусственный интеллект, машинное обучение, визуализацию данных и т.п.[718], и вертикальные приложения, включающие аналитические инструменты для какой-либо отдельной сферы[719].

При оценке влияния Директивы № 2003/98/EC от 17 ноября 2003 г. о последующем использовании информации публичного сектора[720]

---

[713] Elements of a data value chain strategy, Last update: 8 November 2013. https://ec.europa.eu/digital-single-market/en/news/elements-data-value-chain-strategy (дата обращения 15 06 2019)

[714] http://datalandscape.eu/about (дата обращения 10 04 2019)

[715] http://datalandscape.eu/eu-data-landscape (дата обращения 15 04 2019)

[716] Список и карта маркетплейсов. http://datalandscape.eu/data-landscape-type/data-marketplaces (дата обращения 15 04 2019)

[717] Список и карта ИТ-поддержки

[718] http://datalandscape.eu/data-landscape-type/analytics (дата обращения 10 04 2019)

[719] http://datalandscape.eu/data-landscape-type/vertical-applications (дата обращения 10 04 2019)

[720] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.: http://data.europa.eu/eli/dir/2003/98/2013-07-17 (дата обращения 15 04 2019)

Европейская комиссия[721] среди проблем выделила блокировку данных публичного сектора: публичные органы заключают соглашения с частными организациями для увеличения потенциала информации последующего использования, что создает риски получения такими организациями завышенных привилегий «первого получателя» (excessive first-mover benefits).

К любой из платформ-маркетплейсов аналогично могут быть применены и положения конкурентного права. Основное регулирование в отношении запрета на злоупотребление доминирующим положением на рынке (ст. 102, бывшая 82) и согласованные действия (ст. 101, бывшая 81) установлено Договором о функционировании ЕС[722], что исключает необходимость дополнительной имплементации его положений в национальное законодательство. Указанные нормы находились также и в предыдущих учредительных договорах ЕС. Для имплементации положений дополнительно принят Регламент N 1/2003 от 16 декабря 2002 г., который принимался применительно к положениям предыдущего договора, но продолжает действовать и в договоре о функционировании ЕС[723]. Особенностью конкурентного права ЕС является его потенциально экстерриториальный характер.

Основанием для установления юрисдикции ЕС в отношении участников рынка является их возможность воздействовать на европейский рынок (effect of trade). Европейская комиссия выпустила рекомендации,

[721] Impact Assessment on the review of the Directive 2003/98/EC on the reuse of public sector information. https://ec.europa.eu/digital-single-market/en/news/impact-assessment-review-directive-200398ec-reuse-public-sector-information (дата обращения 2 02 2019)

[722] Consolidated version of the Treaty on the Functioning of the European Union.: http://data.europa.eu/eli/treaty/tfeu_2012/oj (дата обращения 28 05 2019)

[723] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32003R0001 (дата обращения 20 01 2019)

разъясняющие понятие возможности воздействия[724]. Они включают в себя три основных концепции: «торговлю между странами ЕС», т.е. действия участников рынка должны затрагивать экономическую активность, включающую как минимум два государства-члена ЕС; «возможность оказать воздействие», т.е. должно быть возможно предсказать с достаточной степенью вероятности на основе набора объективных факторов права или факта, что соглашение или действие может иметь влияние, прямое или косвенное, действительное или потенциальное, на торговлю между странами ЕС; «оценивамость», которая исходит из необходимости оценки объемов возможного влияния в каждой ситуации. Контроль над экономической концентрацией ЕС отдельно регулируется Регламентом No 139/2004 от 20 января 2004 г. о контроле за концентрациями между предприятиями[725]. Таким образом, даже если маркетплейсы находятся не на территории ЕС, но могут оказывать влияние на торговлю между странами ЕС, к ним будут при необходимости применены положения европейского права о защите конкуренции.

Европейская комиссия уделяет повышенное внимание недостаточной регламентированности деятельности платформ, необходимости обеспечения достойного обращения их с пользователями и предотвращения распространения нелегального контента[726]. Еще в 2016 г. Европейская комиссия выпустила Сообщение об онлайн-платформах и вызовах единого

---

[724] Guidelines on the effect on trade concept. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52004XC0427(06) (дата обращения 17 02 2019)

[725] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation).: http://data.europa.eu/eli/reg/2004/139/oj (дата обращения 07 05 2019)

[726] https://ec.europa.eu/digital-single-market/en/online-platforms-digital-single-market (дата обращения 10 02 2019)

европейского рынка[727], в котором она проанализировала возрастающую роль платформ, выделила их основные характеристики. В Сообщении установлены следующие направляющие принципы политики: ровное игровое поле[728] сопоставимых цифровых сервисов; удостоверение, что платформы ведут себя ответственно с целью защиты основных ценностей всех заинтересованных лиц; установление доверия, прозрачности и обеспечение добросовестности; сохранение рынков открытыми и недискриминационными для развития экономики данных.

Таким образом, ЕС активно участвует в развитии экономики знаний и рынка данных и содействует развитию деятельности маркетплейсов данных. Одновременно любые маркетплейсы как отдельная разновидность цифровых платформ могут попадать под положения о цифровых платформах, о защите потребителей цифровых благ, а также, вне зависимости от нахождения, под действие европейского конкурентного права.

2.7.2 Правовое регулирование в Германии

В законодательстве Германии нет закона, который бы напрямую регулировал устройство и функционирование маркетплейсов по обмену данными. Во многом такого рода регулирование осуществляется в

---

[727] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, Brussels, 25.5.2016, COM (2016) 288 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1466514160026&uri=CELEX:52016DC0288 (дата обращения 10 02 2019)

[728] Level playing field – концепция регулирования рынка, согласно которой не каждый участник имеет равные реальные возможности для выигрыша, но каждый участник рынка подчиняется одинаковому набору правил и получает равные потенциальные возможности получения выигрыша. Источник: Business Dictionary: http://www.businessdictionary.com/definition/level-playing-field.html (дата обращения 30 04 2019)

соответствии со Стратегией электронного правительства Германии и с Законом о повторном использовании информации государственного сектора.

Основным порталом Германии в области обмена данными является GovData («https://www.govdata.de»), через который осуществляется предоставление государственной информации. Через GovData органы государственной власти федерального правительства, земель и муниципалитетов предоставляют и получают данные. В частности, административным служащим, гражданам, компаниям и ученым должна быть предоставлена возможность доступа к данным и информации государственного управления в Германии на всех уровнях через центральный сайт. Цель состоит в том, чтобы эффективнее использовать данные.

Через GovData передаются данные следующего характера:

– население и общество,
– образование, культура и спорт,
– энергия,
– здоровье,
– международные договоры,
– правосудие, правовая система и общественная безопасность,
– сельское хозяйство, рыболовство, лесное хозяйство,
– правительство и государственный сектор,
– регионы и государственный сектор,
– транспорт,
– окружающая среда,
– бизнес и финансы,
– наука и техника.

За портал отвечает Офис бизнеса и координации GovData в Гамбурге. Основы деятельности GovData определены в административном соглашении.

Как правило, данные, доступные через GovData, могут использоваться безвозмездно. Если существуют какие-либо ограничения на использование

(компенсация понесенных расходов, запрет на коммерческое использование и т. п.), это обязательно указывается в соответствующей записи данных.

Таким образом, правовое регулирование маркетплейсов в Германии проходит стадию становления. В настоящее время доступ к публичным данным осуществляется на безвозмездной основе, однако прослеживается тенденция и интерес органов государственной власти к коммерциализации публичных данных.

2.7.3 Правовое регулирование во Франции

На сайте открытой платформы последующего использования публичных данных размещен список реализованных проектов последующего использования данных[729]. Например, А. Огусти осуществил сбор данных обо всех автоматических транспортных радарах на территории Франции[730]. Его база данных используется для поддержания аналогичного сервиса Министерства внутренних дел[731].

Маркетплейс данных означает цифровую платформу, в которой возможен обмен наборами данных между ее участниками. В настоящий момент действует несколько таких платформ. Например, Dawex[732], IOTA[733], Kochava[734], Dataspace[735], использующая блокчейн-технологии. Хотя французское право не устанавливает специального регулирования для таких маркетплейсов, некоторые положения могут быть применимы и к ним как к цифровым платформам.

---

[729] URL: https://www.data.gouv.fr/fr/reuses/?page=1 (дата обращения 26 06 2019)

[730] URL: https://www.data.gouv.fr/fr/datasets/radars-automatiques/ (дата обращения 19 09 2019)

[731] URL: https://radars.securite-routiere.gouv.fr/#/ (дата обращения (дата обращения 26 06 2019)

[732] URL: https://www.dawex.com/en/ (дата обращения 11 05 2019)

[733] URL: https://data.iota.org/#/ (дата обращения 11 05 2019)

[734] URL: https://www.kochava.com/data-marketplace/ (дата обращения 25 09 2019)

[735] URL: https://www.datapace.io/ (дата обращения 17 10 2019)

Ст. 242 бис Налогового кодекса Франции предусматривает ряд обязанностей предприятия, независимо от места его нахождения, которое как оператор платформы соединяет на расстоянии электронным путем лиц с целью продажи какого-либо блага, оказания услуги, обмена или предоставления каких-либо блага или услуги[736]. В частности, такое предприятие обязано в случае каждой трансакции сообщать достоверную, ясную и прозрачную информацию о налоговых и социальных обязанностях лиц, которые осуществляют трансакцию посредством такой платформы, в том числе путем предоставления ссылок на сайты имеющих отношение к трансакции публичных органов. Кроме того, платформа обязана направлять ежегодно до 31 января следующего года в электронном виде продавцам, исполнителям или лицам, участвующим в обмене или предоставлении услуг или благ, которые получили как пользователи платформы денежные средства из осуществленных посредством платформы трансакций, о которых платформа знает, документ, который должен содержать: идентификационные элементы оператора платформы; идентификационные элементы пользователя; статус лица или профессионала, указанный пользователем платформы; число и общую сумму брутто осуществленных пользователем трансакций в течение предыдущего года; координаты банковского счета, на которые поступают отчисления, если они известны оператору. Аналогичный документ в те же сроки платформа обязана направить налоговому органу. Обязанности распространяются на случаи, когда пользователем является лицо, учрежденное во Франции либо осуществляющее продажи, оказывающее услуги на территории Франции по смыслу ст. 258–259D Налогового кодекса. Закон также предусматривает ряд исключений из

[736] Code général des impôts. URL: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000037526190&cidTexte=LEGITEXT000006069577&dateTexte=20181231 (дата обращения 16 07 2019)

указанной обязанности для случаев, например, оказания услуг, когда оказывающий их получает выгоду без коммерческой цели и с разделением издержек оказания услуги с получателем.

Ряд положений о цифровых платформах также содержится в Кодексе потребления Франции[737]. Так, ст. 111-7 Кодекса устанавливает, что оператором онлайн платформы считается лицо, физическое или юридическое, которое предлагает профессионально, за плату или без нее, услуги доведения до всеобщего сведения в Интернете, основываясь на: классификации или референции, посредством математических алгоритмов, содержимого, благ или услуг предлагаемых или размещаемых третьими лицами; либо соединении различных сторон с целью продажи какого-либо блага, оказания услуги, обмена или предоставления содержимого, блага или услуги. Всякий оператор онлайн-платформы обязан сообщать потребителю достоверную, ясную и прозрачную информацию относительно: общих условий использования посреднического сервиса, который он предлагает, особенностей референсирования, классификации и дереференсирования содержимого, благ или услуг, к которым сервис позволяет получить доступ; существования договорного отношения, корпоративной связи или вознаграждения, если они влияют на классификацию или на референсирование содержимого, благ или услуг, предлагаемых или предоставляемых онлайн; статус оператора и права и обязанности сторон в сфере гражданского и налогового права, когда потребитель находится в отношении с профессионалами или непрофессионалами. Также предусматривается необходимость издания подзаконного акта – декрета –

---

[737] Code de la consommation. URL: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=9D9EE6F8EC8E205D245C1AB7970BF19C.tplgfr30s_2?cidTexte=LEGITEXT000006069565&dateTexte=20170223 (дата обращения 18 07 2019)

уточняющего условия использования ст. 111-7 Кодекса в зависимости от природы действия операторов платформы, устанавливающего особенности предоставления оператором платформы необходимого пространства для сообщения предусмотренных сведений до заключения договора. Декрет n° 2017-1434 от 29 сентября 2017г. об обязанности информирования операторами платформ принят в исполнение указанных положений[738]. Декрет дополняет также, что все операторы должны предоставлять на каждой странице в читаемой и легко доступной манере информацию о критерии классификации и способе его определения.

Ст. L111-7-1 Кодекса предусматривает, что операторы онлайн платформ, количество посещений которых превышает определенное число, обязаны также предоставлять потребителю информацию о лучших практиках. Особенности применения уточнятся Декретом n° 2017-1435 от 29 сентября 2017 г.[739]. Необходимый предел посещаемости равняется пяти миллионам посетителей за месяц на платформе. Декрет вступил в силу 1 января 2019 г. При этом уточняется, что оператор, который попадает по количеству посещаемости под обязательства ст. 111-7-1 Кодекса, имеет срок, равный полугоду, для принятия необходимых мер по реализации предусмотренного положения.

Таким образом, хотя маркетплейсы данных напрямую не регулируются французским правом, к ним могут также предъявляться требования такие же,

---

[738] Décret n° 2017-1434 du 29 septembre 2017 relatif aux obligations d'information des opérateurs de plateformes numériques. URL: https://www.legifrance.gouv.fr/eli/decret/2017/9/29/ECOC1716647D/jo/texte (дата обращения 01 10 2019)

[739] Décret n° 2017-1435 du 29 septembre 2017 relatif à la fixation d'un seuil de connexions à partir duquel les opérateurs de plateformes en ligne élaborent et diffusent des bonnes pratiques pour renforcer la loyauté, la clarté et la transparence des informations transmises aux consommateurs. URL: https://www.legifrance.gouv.fr/eli/decret/2017/9/29/ECOC1716648D/jo/texte (дата обращения 01 08 2019)

как к онлайн-платформам, как в сфере налогового права, так и в сфере потребительского.

2.7.4 Правовое регулирование в Эстонии

В Эстонии получило развитие «Правительственное Облако Эстонии» (Estonian Governmental Cloud)[740] - платформа для предоставления, управления и аудита IT-сервисов в государственном секторе. Платформа создана на основе государственно-частного партнерства – консорциума, состоящего из государственного Инфокоммуникационного Фонда[741] (RIKS - некоммерческого фонда, созданного в 2000 году и управляемого Министерством экономики и коммуникаций) и частных компаний, таких как Cybernetica, DELL EMC, Ericsson, OpenNode и Telia, каждая из которых имеет свою сферу ответственности в консорциуме.

В рамках данной платформы функционирует модуль Маркетплейс (Marketplace)[742], созданный по образцу Цифрового маркетплейса (Digital Marketplace) Великобритании. Маркетплейс предназначен для размещения, поиска и управления сервисов в рамках Правительственного Облака Эстонии.

Оплата использования IT-сервисов возможна по нескольким тарифным планам:

– плата по фиксированной цене за период времени (fixed pricing),

– плата по факту использования (usage-based), когда цена определяется на основе отчета об использовании.

---

[740] The Estonian Government Cloud. URL: https://e-estonia.com/solutions/e-governance/government-cloud/ (дата обращения: 09.09.2019).

[741] State Infocommunication Foundation. URL: http://riks.ee/609.html (дата обращения: 09.09.2019).

[742] Introducing Marketplace. URL: https://riigipilv.ee/blog-and-news/introducing-marketplace (дата обращения: 09.09.2019).

В Эстонии также получили развитие отраслевые платформы обмена данными. Так, на основе государственной информационной системы функционирует платформа обмена данными в сфере энергетики[743]. Платформа обеспечивает информационный обмен между всеми участниками отношений в сфере производства, поставки и потребления энергии, что позволяет повысить эффективность энергопотребления. Платформа функционирует на принципах равного обращения, учитывая при этом право участников рынка на равный доступ к информации об объемах потребления энергии и на быструю смену поставщика. В настоящее время разрабатываются решения, позволяющие обеспечить доступ к платформе не только участникам рынка, но и университетам, исследовательским центрам и разработчикам приложений[744].

В Эстонии отсутствует специальное законодательство, регулирующее вопросы создания, функционирования электронных площадок по обмену данными, а также защиты прав потребителей и обеспечения конкуренции на рынке обмена данных. К этим вопросам применимо общее законодательство о защите прав потребителей и защите конкуренции, а также некоторые положения законодательства об открытых данных (в части гарантий недискриминационного доступа к данным государственного сектора). К вопросам защиты данных применимо законодательство о защите персональных данных, а также законодательство о кибербезопасности.

---

[743] Electricity data exchange. URL: https://elering.ee/en/data-exchange (дата обращения: 09.09.2019).

[744] Access to electricity and gas smart meter data in Estonia powered by X-Road technology. URL: https://x-road.global/access-to-electricity-and-gas-smart-meter-data-in-estonia (дата обращения: 09.09.2019).

2.7.5 Правовое регулирование в Великобритании

В публичном секторе для государственных закупок в рамках GOV.UK существует Digital marketplace[745], который позволяет осуществлять закупки цифровых продуктов, облачных сервисов для правительственных нужд. Процессы размещения заявок, предложения продуктов регулируются Руководствами GDC[746]. Вместе с тем указанная площадка не является «электронной площадкой по обмену данными».

Если говорить о частных аналогах «маркетплейсов данных», можно выделить, например: oneTRANSPORT[747] или DAWEX[748].

На подобные «маркетплейсы» распространяются общие требования законодательства о защите персональных данных, потребительского законодательства, законодательства о защите конкуренции. Специального регулирования законодательство и судебная практика Великобритании не содержит.

Основу потребительского регулирования составляет Акт о правах потребителей (Consumer Rights Act 2015). Акт регулирует вопросы защиты прав потребителей не только в отношении товаров или услуг, но и в отношении цифрового контента (Глава 3 Акта о правах потребителей).

Из содержания ст. 2 следует, что под цифровым контентом понимаются данные, которые производятся и предоставляются в цифровой форме. При этом, исходя из положений ст. 33, можно утверждать, что нормы Главы 3 указанного Акта не распространяются на оказание услуг (например, SaaS).

---

[745] Digital Marketplace. URL: https://www.digitalmarketplace.service.gov.uk (дата обращения: 05.08.2019).

[746] См. например: Guidance: Buying and selling on the Digital Marketplace. URL: https://www.gov.uk/guidance/buying-and-selling-on-the-digital-marketplace (дата обращения: 05.08.2019).

[747] oneTRANSPORT Data Marketplace website. URL: https://onetransport.io (дата обращения: 05.08.2019).

[748] DAWEX website. URL: https://www.dawex.com/en/ (дата обращения: 05.08.2019).

Ст. 34 Акта о правах потребителей устанавливает требования к качеству контента. Надлежащее качество контента предполагает:

– пригодность контента для целей, для которых он обычно используется,

– отсутствие дефектов,

– безопасность,

– долговечность.

В соответствии со ст. 42 Акта, если контент не соответствует условиям договора, потребитель имеет право на замену или соразмерное уменьшение цены. Если цифровой контент вызвал повреждение устройства, то в соответствии со ст. 46 предприниматель обязан либо отремонтировать устройство, либо возместить ущерб. Договорная ответственность не может быть ограничена по сравнению с требованиями потребительского законодательства, в силу ст. 47 Акта[749].

Основным источником антимонопольного регулирования является Акт о конкуренции (Competition Act 1998)[750]. Акт содержит требования, запрещающие не непосредственно монополизацию рынка, но злоупотребление доминирующим положением на рынке, которое может выражаться в навязывании несправедливых цен; ограничении технического развития в ущерб потребителям; применение различных условий к аналогичным сделкам для одной категории потребителей и в иных формах. Акт содержит ряд норм, регулирующих вопросы расследования таких случаев и привлечения к ответственности.

---

[749] Consumer Rights Act 2015. URL: http://www.legislation.gov.uk/ukpga/2015/15/contents (дата обращения: 05.08.2019).

[750] Competition Act 1998. URL: http://www.legislation.gov.uk/ukpga/1998/41/contents (дата обращения: 05.08.2019).

Если владелец такой платформы является оператором жизненно-важных услуг или провайдером цифровых услуг по смыслу The Network and Information Systems Regulations 2018[751], на него дополнительно ложатся требования по обеспечению кибербезопасности такого маркетплейса, в соответствии с положениями указанного Регламента.

Таким образом, в Великобритании отсутствует специальное правовое регулирование «маркетплейсов» (электронных площадок по обмену данными).

2.7.6 Правовое регулирование в Австралии

Исследование не выявило отдельных нормативно-правовых актов, регулирующих в данной стране создание и функционирование электронных площадок по обмену данными. В то же время функционирование цифровых платформ[752], направленных на создание условий по обмену данными как публичного, так и частного сектора, позволяет сделать вывод, что положений общих положений законодательства о неприкосновенности частной жизни, а также разработанных руководящих принципов и требований к безопасности государственных информационных систем, оказалось достаточно для создания и функционирования подобных электронных площадок.

Data.gov.au является центральным источником открытых правительственных данных (open government data) Австралии. Любой желающий может получить доступ к анонимизированным публичным данным, опубликованным федеральными, региональными и местными

[751] The Network and Information Systems Regulations 2018. URL: http://www.legislation.gov.uk/uksi/2018/506/contents (дата обращения: 05.08.2019).

[752] В данном разделе будут рассмотрены только те цифровые платформы, целью создания которых и основной задачей является создание условий по обмену наборами данных между двумя и более лицами. Те цифровые среды, основной функцией которых является обеспечение доступа к цифровому контенту, его воссоздание и распространение, не рассматриваются в данном разделе, поскольку в них обмен данными носит, в основном, односторонний (от потребителя к владельцу платформы) и аксессорный характер.

органами власти. Размещенные данные рассматриваются как национальный ресурс, который имеет большое значение для роста экономики, улучшения услуг и преобразования результатов политики. В дополнение к правительственным данным как таковым на данном ресурсе выложены финансируемые государством исследовательские данные и наборы данных от частных учреждений, которые вызывают общественный интерес. На момент исследования сайт насчитывает более 30.000 общедоступных наборов данных. Помимо просмотра опубликованных данных, сайт data.gov.au позволяет визуализировать часть датасетов с помощью встроенных картографических инструментов; так, данные, содержащие геопространственное поле (например, широта и долгота), можно нанести на карту и просмотреть с помощью сервиса «Национальная карта» (National Map)[753]. Загрузка (публикация) государственных данных возможна только с адреса электронной почты правительства Австралии (заканчивающегося на «.gov.au»).

В качестве примера цифровой платформы, созданной для обмена данными частного сектора, можно привести Senate, цифровую платформу проекта Data Republic. Среди объективных затруднений, с которыми ассоциируется обмен данными, основатели проекта отмечают вопросы защиты неприкосновенности частной жизни и соблюдения требований законодательства об обработке персональных данных, потерю контроля за использованием данных после их предоставления, риски, сопряжённые с нахождением «чувствительных» массивов данных в одной централизованной информационной системе, опасность несанкционированного доступа, а также трудность переговоров об условиях соглашения.

[753] National Map. URL: https://nationalmap.gov.au/ (дата обращения 24 08 2019)

На сегодняшний день эти вопросы решаются в Senate следующим образом:

1) Условия использования самой платформы, а также условия доступа к наборам данных, представленных пользователями платформы, регулируется набором лицензионных соглашений. Некоторые из таких соглашений являются обязательными (например, лицензия, обуславливающая доступ к самой платформе Senate); условиях других лицензий, определяющих порядок пользования наборами данных, могут комбинироваться владельцами наборов данных по их усмотрению, исходя из заранее установленных платформой лицензионных «модулей».

2) Система управления данными основана на ряде параметров, определяемых «хранителем» данных при формировании набора данных. Среди таких параметров: условия лицензии, определение лиц, обладающих доступом, какой вывод данных допускается и при условии каких проверок, как защищены сами данные, установленные параметры аудита и пр.

3) Контроль над использованием данных основывается на системе «Пяти сейфов», позволяющей принимать решения об эффективном использовании конфиденциальных или «чувствительных» данных, разработанной UK Data Service и в последствии воспринятой ведомствами других стран. В рамках Senate эта система дополнена юридическим контролем и аудитом. Юридический контроль реализуется через лицензию и определяет пределы разрешенного использования; аудит лог-файлов позволяет организации – владельцу датасета отслеживать, кто получал доступ к данным, когда и как он был использован.

4) Возможность сопоставления данных, представленных в различных наборах (data matching), реализуемая через децентрализованные технологии. «Сырые» данные (raw data) в виде имен, адресов электронной почты, даты рождения не могут быть загружены на платформу, остальные же данные проходят предустановленные способы обработки, снижающие риск идентификации.

В целом возможности платформы, в том числе в отношении контроля над использованием загружаемых данных, а также имплементированные меры безопасности, делают платформу привлекательной для бизнеса, в том числе, и такого крупного, как банковский капитал[754]. Кроме того, данный проект был запущен на территории США и Сингапура на базе учрежденных в данных юрисдикциях дочерних обществ. При этом характерно, что проект не был распространен на какую-либо страну Европейского союза, что, очевидно, связано со строгостью требований GDPR по защите персональных данных.

Другим обстоятельством, подтверждающим, что правовые и технологические решения, заложенные при создании и функционировании платформы Senate, соответствуют общим положениям законодательства Австралии о неприкосновенности частной жизни и обороте данных, является сотрудничество Data Republic с отдельными штатами.

Так, в 2017 году правительство Нового Южного Уэльса (NSW) объявило о сотрудничестве с Data Republic для разработки платформы, лежащей в основе нового рынка данных, учреждаемого правительством NSW. Целью платформы Marketplace является обеспечение безопасного обнаружения, доступа и использования данных, хранящихся в государственных ведомствах NSW. В настоящее время портал NSW DataPortal[755] предусматривает возможность зарегистрированным пользователям создать определенные группы для просмотра и использования

[754] Data sharing technology unlocks analytics insights for ANZ. URL: https://www.datarepublic.com/case-study-anz (дата обращения 12 10 2019)

[755] NSW Data Portal. URL: https://portal.data.nsw.gov.au/arcgis/home/ (дата обращения 12 10 2019)

данных, загруженных государственными ведомствами[756]. При этом из функционала портала не следует возможность пользователей самостоятельно определять или иным образом коммерческие условия доступа или ограничения использования данных. Очевидно, следует сделать вывод, что такие наборы данных, являясь первоначально данными государственных реестров, подчиняются общему правовому режиму, установленному для открытых данных государственных систем NSW[757] и могут использоваться на условиях лицензии Creative Commons BY[758].

В целом электронные площадки по обмену наборами данных функционируют в рамках общих положений федерального и регионального законодательства, устанавливающего тот или иной режим для определенной категории данных.

2.7.7 Правовое регулирование в Сингапуре

Как было сказано ранее, Сингапур высоко оценивает степень влияния оборота данных на экономическое развитие, в связи с чем его правительство активно сотрудничает с частными компаниями в регулировании вопроса оборота данных. Помимо проблем пользователей с поиском данных (например, доступности данных, их актуальность и достоверность и т.п.), встает вопрос о монетизации, который затрагивает интересы пользователей данных.

---

[756] NSW Data Portal Tutorial. https://portal.data.nsw.gov.au/arcgis/apps/MapSeries/index.html?appid=86e47b08897642c9842c7b84d7dfd354 (дата обращения 16 11 2019)

[757] NSW. Open Data Policy. https://www.digital.nsw.gov.au/sites/default/files/NSW_Government_Open_Data_Policy_2016.pdf (дата обращения 23 10 2019)

[758] New South Wales Government Open Data Policy supports Creative Commons licensing for government data and information. https://creativecommons.org.au/blog/2013/11/new-south-wales-government-open-data-policy-supports-creative-commons-licensing-for-government-data-and-information/ (дата обращения 23 10 2019)

Министерство коммуникаций и информации (Ministry of Communications and Information, MCI) объединяет две стороны конфликта с использованием надежной инфраструктуры и технологий[759]. Рынок данных состоит из данных как государственного, так и частного секторов. Это помогает владельцам данных монетизировать их с помощью сборов за лицензирование данных. Такие функции помогают, по мнению данного Министерства, реализовать новые источники дохода и еще больше побудить владельцев делиться данными. В свою очередь, пользователям данных это помогает создавать приложения, продукты и услуги.

Сингапур возглавляет список стран, осуществляющих обмен данными через регулятивные «песочницы». В рамках поддержки развития цифрового государства Сингапур инициировал программу «песочниц» с целью стимулирования инноваций и обмена данными в масштабах страны. Одной из таких «песочниц» является платформа DEX[760], созданию и функционированию которых способствовало Управление развития средств массовой информации.

Песочницы данных регулируются в разных отраслях. Например, Денежно-кредитное управление Сингапура (Monetary Authority of Singapore, MAS) в рамках создания Fintech на государственном уровне выпускало проекты руководящих принципов по обороту данных в таких системах[761].

В настоящий момент Программа «Песочница данных» переросла в Программу совместной работы с данными (Data Collaborative Programme). Она стремится поддерживать и развивать отраслевых операторов,

---

[759] https://www.mci.gov.sg/pressroom/news-and-stories/stories/2014/12/data-marketplace (дата обращения 21 08 2019)

[760] https://www.dex.sg (дата обращения 21 08 2019)

[761]:https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/2018%20Nov%20Sandbox%20Express/Consultation%20Paper%20on%20Sandbox%20Express.pdf (дата обращения 11 10 2019)

исследующих способы внедрения и управления механизмами, обеспечивающими безопасный и экономически устойчивый обмен данными[762].

2.7.8 Правовое регулирование в Российской Федерации

Создание и обеспечение функционирования электронных площадок по обмену данными, «маркетплейсов» различного правового статуса и предназначения, в том числе «маркетплейсов», предполагающих осуществление коммерческой деятельности и извлечение прибыли в интересах физических лиц и (или) организаций, не урегулировано нормативными актами, имеющими универсальный характер, и регулируется широким кругом нормативных актов, в том числе:

– Гражданским кодексом Российской Федерации[763] (в том числе главой 52, поскольку в большинстве случаев характер фактических отношений участников площадок по обмену данных строится по модели агентского договора),

– Законом № 149-ФЗ,

– отдельными федеральными законами или отдельными положениями федеральных законов (например, Федеральным законом от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах»[764], Федеральным законом от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг»[765], в части регулирования функционирования электронных площадок, специализированных электронных площадок, деятельности операторов электронных площадок и операторов специализированных электронных площадок в соответствии со

---

[762] Руководство по обмену данными. https://www2.imda.gov.sg/-/media/Imda/Files/Industry-Development/Innovation/Guide-to-Data-Sharing-PowerPoint.pdf?la=en (дата обращения 24 09 2019)

[763] Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ // СЗ РФ. 1996. № 5. Ст. 410.

[764] СЗ РФ. 2011. № 48. Ст. 6726.

[765] СЗ РФ. 1996. № 17. Ст. 1918.

статьей $24^1$ Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»[766], деятельности агрегаторов информации о товарах (услугах) при продаже товаров (выполнении работ, оказании услуг) в соответствии с Законом Российской Федерации от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей»[767] и иными федеральными законами в зависимости от рода деятельности «маркетплейса»),

– решениями о создании «маркетплейсов» организаций и локальными нормативными актами об их функционировании (например, создание «маркетплейса» пассажиров железнодорожного транспорта в соответствии с распоряжением ОАО «РЖД» от 24 марта 2017 г. № 543р[768]).

В числе электронных площадок по обмену данными следует выделить цифровые платформы как отдельный вид.

Цифровая платформа – система алгоритмизированных взаимовыгодных отношений значимого количества независимых участников отрасли экономики (или сферы деятельности), осуществляемых в единой информационной среде, приводящая к снижению транзакционных издержек за счёт применения пакета цифровых технологий работы с данными и изменения системы разделения труда[769].

На данный момент цифровые платформы допустимо разделить на следующие группы:

---

[766] СЗ РФ. 2013. № 14. Ст. 1652.

[767] СЗ РФ, 1996. № 3. Ст. 140.

[768] http://www.consultant.ru/document/cons_doc_LAW_218604 (дата обращения 14 10 2019)

[769] Цифровые платформы. Подходы к определению и типизации // Цифровая экономика https://files.data-economy.ru/digital_platforms.pdf. (дата обращения 16 08 2019)

1. Инструментальная цифровая платформа. Данный вид платформы направлен на создание программного обеспечения или программных решений. Примерами являются различные операционные системы, например, Android. Существенной характеристикой инструментальных цифровых платформ является факт использования преимущественно разработчиками программ, поскольку они направлены на создание новых программных решений, тогда как обработка персональных данных отсутствует.

2. Инфраструктурная цифровая платформа. Данная цифровая платформа предоставляет ИТ-сервис и информацию для принятия решений. Примерами являются ГОСУСЛУГИ, PREDIX. Существенные характеристики такого вида цифровой платформы: предоставляется информация, а не только технологические решения, в платформе принимают участие потребители, поставщики информации, разработчики сервисов, существуют возможности сбора больших данных, осуществляется обработка персональных данных.

3. Прикладная цифровая платформа. Данная цифровая платформа обеспечивает обмен экономическими ценностями. Примерами являются: Яндекс Такси, Авито, поисковые системы. Существенными характеристиками данного вида платформы является обеспечение заключения сделок между ее пользователями и осуществление в рамках цифровой платформы обработки персональных данных, наличия возможностей сбора больших данных (Big Data).

В отечественном законодательстве не предусмотрено специального правового регулирования деятельности платформенных компаний, так же как и любых других «маркетплейсов». Исходя из экспертного анализа существующего правового регулирования, можно выделить следующие механизмы, предусмотренные законодательством, с использованием которых государство в настоящее время оказывает наибольшее влияние на деятельность «маркетплейслов» и платформенных компаний:

1) антимонопольные механизмы:

– запрет на злоупотребление доминирующим положением хозяйствующих субъектов (статья 5 Федерального закона от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции»[770], далее – Закон № 135-ФЗ);

– запрет на недобросовестную конкуренцию (статья 11 Гражданского кодекса Российской Федерации, перечни форм недобросовестной конкуренции, установленные Законом № 135-ФЗ), в том числе при проведении торгов;

– осуществление государственного контроля за экономической концентрацией (приложение № 19 к Договору о Евразийском экономическом союзе[771]);

2) информационные механизмы:

– требования о раскрытии информации, связанной с деятельностью организации;

– обеспечение конфиденциальности информации, в том числе персональных данных;

3) корпоративные механизмы, связанные с управлением организацией;

4) договорные механизмы:

– установление требований к условиям договоров присоединения, заключаемых с «маркетплейсами», в том числе с платформенными компаниями;

– обеспечение исполнения обязательств (страхования, банковской гарантии) и иные договорные механизмы;

5) иные механизмы:

– экономические механизмы стимулирующего характера, например, уменьшение налоговой нагрузки (льготный режим налогообложения), субсидии или иные преференций;

---

[770] СЗ РФ. № 31 (Часть I). Ст. 3434.

[771] http://www.pravo.gov.ru. (дата обращения 22 01 2019)

– регулирование товарных рынков.

В целях защиты имущественных интересов Российской Федерации в случае создания «маркетплейсов» (электронных площадок обмена данными) в государственных информационных системах обеспечения защиты конкуренции, информации и прав потребителей и при создании и обеспечении функционирования частных «маркетплейсов» в решении о создании «маркетплейса», принимаемом в форме федерального закона, иного правового нормативного акта или локального нормативного акта организации, как правило, указываются (или должны быть указаны) следующие положения:

– о полномочиях представителей государства в органах управления организации или иных учредителей электронной площадки обмена данных,

– функции и полномочия создаваемой электронной площадки обмена данных,

– права и обязанности организации,

– порядок передачи федерального имущества в качестве имущественного взноса Российской Федерации,

– особенности распоряжения имуществом организации, в том числе расходования денежных средств, инвестирования временно свободных средств,

– полномочия органов управления организации,

– персональные квалификационные требования к лицам, замещающим должности в ее органах управления,

– порядок регламентации деятельности организации,

– порядок реализации членства в организации, в том числе процедура принятия в члены организации иных организаций,

– порядок определения эффективности деятельности организации,

– порядок соблюдения прав и обязанностей участников электронной площадки обмена данными, процедуры урегулирования конфликтов и медиации,

– порядок осуществления споров участников электронной площадки обмена данными, в том числе в форме онлайн-разбирательства,

– порядок формирования стратегии развития организации,

– порядок внутреннего контроля деятельности организации,

– ответственность организации.

Обоснование создание электронной площадки обмена данных электронной площадки обмена данных должно включать:

– финансово-экономическое обоснование,

– требования к составу федерального имущества, необходимого для деятельности создаваемой организации (при учреждении «маркетплейса» в государственной информационной системе»),

– состав организаций, участие которых необходимо в деятельности создаваемой организации, требования к их компетенции (в случае создания пула частных учредителей),

– определение социальной миссии электронной площадки обмена данных (при учреждении «маркетплейса» в государственной информационной системе») или ее коммерческой эффективности (частный «маркетплейс»).

Специальные требования к защите информации при создании и обеспечении функционирования «маркетплейсов» не установлены. В соответствии с частью 2 статьи 16 Закона № 149-ФЗ государственное отношения в сфере защиты информации регулируются путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации. Одной из мер защиты информации является лицензирование деятельности по технической защите конфиденциальной информации. Постановлением Правительства Российской

Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»[772] утверждено Положение, которое определяет порядок лицензирования деятельности по технической защите конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями. Под такой защитой понимается комплекс мероприятий и (или) услуг по защите информации от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях ее уничтожения, искажения или блокирования доступа к ней.

Таким образом, управление данными на электронных площадках обмена данными регулируется законодательством только в отдельных аспектах деятельности организаций, осуществляющих деятельность в указанной сфере, и требует отдельного участия законодателя для создания условий полноценного, то есть с учетом всех необходимых особенностей, функционирования таких площадок, в том числе «маркетплейсов» и цифровых платформ.

2.7.9 Выводы

В странах ЕС отсутствует специальное регулирование в сфере электронных площадок по обмену данными (маркетплейсов). На подобные площадки распространяются общие положения договорного права и права интеллектуальной собственности, законодательства о защите персональных данных и кибербезопасности, о защите прав потребителей и о защите конкуренции, а также положения налогового законодательства о налогообложении деятельности по продаже цифрового контента.

В некоторых странах (например, во Франции) предусмотрены законодательные положения, регулирующие деятельность онлайн-платформ

---

[772] СЗ РФ. 2012. № 7. Ст. 863.

(товарных агрегаторов), однако они не содержат специфических требований к онлайн-платформам в сфере обмена данными.

Для стран общего права и Сингапура характерны следующие особенности:

– отсутствие «маркетплейса» на основе данных как самостоятельной правовой категории. По этой причине ни в одном из исследуемых правопорядков не выявлено специального регулирования отношений, связанных с созданием и функционированием такого рода «маркетплейсов», а также специальных норм, направленных на защиту прав потребителей и обеспечение конкуренции на подобных площадках обмена данными,

– распространение на отношения, связанные с деятельностью «маркетплейсов» данных, действующих норм конкурентного права законодательства о защите прав потребителей, законодательства о защите персональных данных, законодательства о кибербезопасности.

3 Описание моделей правового регулирования управления данными в национальном законодательстве зарубежных государств и их сравнительно-правовой анализ

3.1 Правовой режим данных и правовой статус различных участников оборота данных

В данном разделе рассматриваются подходы к регулированию информации. А именно - какого рода информация подвергается регулированию. В рамках анализа было выявлено, что выделяют информацию (сведения; сообщения, данные) независимо от формы их представления) следующего рода:

– персональные данные,
– публичные данные,
– общедоступные данные,
– пространственные данные,
– открытые данные,
– информация ограниченного доступа.

Общей чертой регулирования информации у всех стран является отдельное регулирование персональных данных, а также регулирование информации публичного сектора посредством отдельных нормативных актов, которые определяют, какого рода информация и на каких условиях подлежит регулированию.

Таким образом, особое внимание будет уделено подходу разных стран к регулированию информации, которую государство предоставляет для вторичного использования и к которой оно осуществляет открытый доступ.

Для Германии, Эстонии и Франции характерны следующие черты:

– предоставления для вторичного доступа информации, которые собраны в процессе административной деятельности,

– создание специального сайта, через который осуществляется распространение информации для вторичного использования,

– обязанности раскрытия и предоставления информации как органами публичной власти, так и иными лицами, выполняющими публичные функции, или же лицами, деятельность которых финансируется из публичных средств,

– также прослеживается влияние права ЕС, что способствует унификации законодательства данных стран.

В свою очередь Австралии и Великобритании присущи следующие черты:

– наличие политики правительства по отношению к публичным данным,

– особая роль принципов, на которых основывается развитие законодательства по отношению к данным.

Непосредственный анализ моделей будет раскрываться в пункте «регулирование отдельных категорий данных, включая персональные данные, «открытые данные» и другие», так как данные пункты являются взаимосвязанными.

3.2 Регулирование отдельных категорий данных, включая персональные данные, «открытые данные» и другие

На основе анализа выделяемых в разных странах отдельных категорий данных и способа построения правового регулирования для определения критерия формирования моделей правового регулирования выделим две ключевые группы данных: данные, относящиеся к личности (например, персональные данные) и данные публичного сектора. Регулирование двух выделенных групп отличается наибольшей значимостью для формирования экономики данных и позволяет сочетать правовое регулирование в защиту интересов как частных, так и публичных лиц, обеспечивая общий баланс интересов.

В качестве критерия выделения моделей применительно к выделенным ключевым группам данных принимается институционализация правового регулирования. Под институционализацией в рамках анализа понимается

наличие обособленных групп норм правового регулирования, образующих системные связи с иными нормами юрисдикции и оказывающих непосредственное влияние на них, позволяющие однозначно утверждать о сформированности юридического института правового регулирования каждой из выбранных категорий. Для оценки институционализации рассматривается юридическая техника систематизации норм, наличие отсылочных норм в нормативных правовых актах смежных областей.

На основе вышеизложенного возможно выделить три основные модели правового регулирования: модель институционализированного регулирования (Эстония, Франция, Германия, Великобритания), модель децентрализованного регулирования (США, Австралия), смешанную модель (Сингапур).

В модели институционализированного регулирования однозначно сформированы крупные правовые институты персональных данных и последующего использования информации публичного сектора. Институционализация регулирования раскрывается в первую очередь в применении правовых актов или их частей, собирающих и систематизирующих правовые нормы для установления общего правового режима в целом, безотносительно к отрасли права. Так, во Франции последующее использование публичной информации регулируется Кодексом отношений между обществом и администрацией[773], в Германии − Законом о

[773]Code des relations entre le public et l'administration. https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000031366350 (дата обращения 12 05 2019)

повторном использовании данных (IWG)[774], в Эстонии − Актом о публичной информации[775].

Данная модель образовалась во многом под влиянием европейского права, способствующего гармонизации национального права на всей территории ЕС. Выделим ряд особенностей, свойственных выделению категорий данных в рассматриваемой модели.

Во-первых, как отдельный правовой институт выделяются персональные данные. Персональные данные и право на частную жизнь регулируются отдельно. Таким образом реализуется право физического лица – субъекта персональных данных контролировать обработку и сбор данных о нем вне зависимости от связи таких данных с его частной жизнью. Право субъекта персональных данных включает правомочия запрашивать у оператора персональных данных объем обрабатываемых данных, предлагать при необходимости к ним замечания и уточнения, требовать удаления данных.

В основу предоставления данных положены принципы автономии воли и информированности, реализуемые посредством требования по общему правилу о получении согласия субъекта персональных данных на их обработку. При получении согласия обязательным является условие об указании цели обработки, что позволяет субъекту персональных данных контролировать их использование и при необходимости требовать прекращения неправомерного использования в целях, иных, чем обозначенные цели их сбора.

---

[774] Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen. Режим доступа: https://www.gesetze-im-internet.de/iwg/ (дата обращения: 10.08.2019).

[775] Public Information Act. https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения: 14.08.2019).

Данные публичного сектора также получают отдельное регулирование. При этом под влиянием европейского права зачастую открытые данные, последующее использование информации устанавливают единую систему регулирования данных публичного сектора. Под влиянием европейского права стимулируется максимально возможное раскрытие данных государственными органами в формате открытых данных для развития экономики данных. Особенности установления правил раскрытия и использования информации, определения цены ее предоставления регулируются единым сводом общих положений, обязывающих органы власти руководствоваться ими при установлении политики использования данных, находящихся в их распоряжении.

При этом нормы о последующем использовании включают и случаи использования органом власти, осуществляющим сбор информации, такой информации в целях, отличных от сбора и обработки в соответствии с его компетенцией. Из правового регулирования последующего использования изымается предоставление лицу информации, непосредственно касающейся его прав и законных интересов.

Открытые данные и последующее использование информации публичного сектора объединяются в один правовой институт исходя из их единой социально-экономической направленности – формирования экономики данных.

Наконец, в дополнение к институтам персональных данных и последующего использования информации устанавливается отдельное регулирование и иных категорий данных: пространственных данных, коммерческой тайны, государственной тайны.

Таким образом, модель институализированного регулирования характеризуется созданием институтов персональных данных, последующего использования публичной информации. Для модели характерно принятие единых нормативных правовых актов с нормами абстрактного, общего содержания. Достоинство такой модели состоит в устранении необходимости

принимать регулирование в каждой отдельной сфере общественных отношений; таким образом исключается дублирование правовых норм и устанавливается необходимость вводить специальное правовое регулирование в ситуациях, когда становится необходимым идти на изменение общего режима. Недостаток модели состоит в ее негибкости по отношению к отдельным сферам общественных отношений. Кроме того, единый правовой акт создает в доктрине и практике правоприменения ряд обыкновений и догматических предписаний, которые при изменении общественных отношений или появления новых оказывается трудно обойти.

Модель децентрализованного регулирования характерна больше для стран общего права, за исключением Великобритании. Регулирование тех или иных институтов осуществляется в основном посредством принятия необходимых норм в конкретной сфере общественных отношений.

В Австралии, несмотря на принятие Закона о неприкосновенности частной жизни [776], определяющего правовой режим личной информации и являющегося основой для формулирования 13 принципов неприкосновенности частной жизни, действуют также и дополнительные акты: Закон о переписи и статистике 1905 года (CSA Census and Statistics Act 1905), Закон о свободе информации 1982 года (Freedom of Information Act 1982), и т.д. В итоге в праве Австралии одновременно действует более 500 положений о защите неприкосновенности частной жизни и конфиденциальности данных; эти положения закреплены более в чем 175 правовых актах [777].

---

[776] Privacy Act 1988. https://www.legislation.gov.au/Details/C2014C00076 (дата обращения 11 04 2019)

[777] Productivity Commission 2017, Data Availability and Use, Report No. 82. Canberra. https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf (датао обращения 30 05 2019)

В то же время децентрализация оставляет больше возможностей для активного и изощренного развития права. Например, в Австралии потребителям и малым предприятиям были предоставлены новые права[778], в том числе право на потребительские данные (Consumer Data Right, CDR) и «открытый банкинг» (open banking). Каузальная система правового регулирования способствует облегченному реформированию необходимого набора прав и обязанностей именно в меняющихся общественных ситуациях, таким образом не обременяя все потенциальные случаи общественного взаимодействия и оставляя им возможность более свободного развития до получения регулирования.

Правовой режим последующего использования информации публичного сектора определяется не на законодательном уровне, но на подзаконном - в рамках политики органов исполнительной власти. В США, например, право последующего использования информации публичного сектора до сих пор не получает прямого регулирования. Положения об открытых данных приняты на подзаконном уровне на основании ряда других подзаконных актов. Например, основа развитию открытых данных была заложена в Политике открытых данных США[779]. Политика определяет данные как структурированную информацию. Открытые данные определяются как структурированная информация, которая подлежит полному раскрытию и предоставлению конечному пользователю. Открытые данные, согласно документу, должны быть публичными, доступными (по формату), описанными (включая метаданные для организации раскрываемой

[778] Treasury Laws Amendment (Consumer Data Right) Act 2019 https://www.legislation.gov.au/Details/C2019A00063( дата обращения 02 11 2019)

[779]USA. Memorandum on Open Data Policy. Managing Information as an Asset (“the Open Data Memorandum”, also known as M-13-13). May 9, 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf (дата обращения 12.05.2019)

информации), доступными для последующего использования (данные раскрываются на открытой лицензии без ограничений для их использования), полными, своевременными, а также управляемыми после публикации (контакт для принесения замечаний и предложений по раскрытым данным, сообщений об ошибках). Выделенные свойства открытых данных в целом повторяют подход иностранной доктрины к их рассмотрению[780]. В США действует также Акт о свободе информации, регламентирующий порядок предоставления информации по запросу[781], однако открытые данные регулируются на уровне актов исполнительной власти.

В Австралии аналогично правила оборота публичных данных устанавливаются на подзаконном уровне – в Заявлении правительства о политике публичных данных[782]. При этом в субъектах австралийской федерации (как и в американской) тоже нет унификации развития законодательства о публичной информации.

Такой подход позволяет государству, с одной стороны, формировать экономику данных исходя из постоянно меняющихся политических и социально-экономических потребностей, с другой – при необходимости изменять политику раскрытия данных.

Итак, модель децентрализованного регулирования характеризуется каузальным установлением правового регулирования для отдельных сфер общественных отношений, в том числе на уровне подзаконных актов. В условиях данной модели создается больше возможностей для развития

---

[780]Charalabidis Y. et al. The World of Open Data. Concepts, Methods, Tools and Experiences. Springer International Publishing, 2018. P. 2.

[781]USA. Freedom of Information Act in a form showing all amendments to the statute made by the “FOIA Improvement Act of 2016”. https://www.foia.gov/foia-statute.html (дата обращения 12.05.2019)

[782] Australian Government Public Data Policy Statement. https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf (дата обращения 25 06 2019)

инновационных сфер оборота данных, уменьшается регулятивная нагрузка на общество и государство. Но вместе с тем физические лица в таких случаях могут не получать должных гарантий соблюдения их прав и законных интересов.

Смешанная модель характеризуется неоднородностью подходов к правовому регулированию рассматриваемых отношений. Она свойственна юрисдикциям, которые развивают правовое регулирование на основе синтеза опыта зарубежных стран и определяют необходимость установления того или иного подхода исходя из особенностей национальной правовой системы.

Смешанным моделям свойственна неполная институционализация. Принятые единые нормативные правовые акты могут содержать значительные изъятия. Например, в Сингапуре, несмотря на Закон о защите персональных данных[1], его действие не распространяется на государственные данные. В отношении государственных данных регулирование осуществляется на подзаконном уровне.

С одной стороны, в Сингапуре установлен режим персональных данных, что исключает неясности, свойственные правовому регулированию личной информации в модели децентрализованного регулирования. Для ряда иных категорий данных также приняты единые нормативные правовые акты - Акт о государственной тайне (Official Secrets Act, OSA)[783], Закон о государственном секторе (управлении) 2018 (Public Sector(Governance) Act 2018)[2]. Таким образом для больших групп общественных отношений устанавливаются единые нормы правового регулирования, что позволяет избегать необходимости каузального правотворчества.

---

[783] https://sso.agc.gov.sg/Act/OSA1935#pr1- (дата обращения 15 09 2019)

С другой стороны, в Сингапуре нормы о конфиденциальности не распространяются на общедоступные данные, а их оборот не регулируется законодательно. Общедоступные данные содержатся на правительственном портале, который был первоначально создан правительством для собственных наборов общедоступных данных[784]. При таком подходе повторяется особенность модели децентрализованного регулирования, дающая исполнительной власти возможность и право самостоятельно определять степень раскрытия данных.

Таким образом, смешанная модель сочетает различные приемы юридической техники в соответствии с национальными потребностями. Преимущество такой модели состоит в возможности адаптировать действующее правовое регулирование к изменяющимся общественным отношениям с осмысленным привлечением зарубежного опыта. Несомненный недостаток такой модели – в отсутствии унифицированной юридической техники, снижающий возможность одинаковых ожиданий в отношении того или иного правового регулирования.

Выделенные модели обусловлены во многом социально-политическими и экономическими особенностями рассматриваемых стран: развитием их правосознания, экономики, государственного строя. В целом каждая из моделей может быть применена, имея как достоинства так и недостатки.

Правомерно выделять модели правового регулирования не только исходя из совокупности средств юридической техники, используемых в общем для правового регулирования категорий данных, но и для отдельных категорий данных.

---

[784] Портал открытых данных Сингапура. https://data.gov.sg/ (дата обращения 29 02 2019)

Так, в отношении доступа к информации государственных органов по предмету регулирования выделяются, например, две модели: модель открытых данных (США, Австралия, Сингапур) и модель доступа к информации публичного сектора (Европейский союз в целом и европейские страны, Великобритания).

Модель открытых данных включает использование и размещение информации только в формате открытых данных. Объем раскрываемой информации определяется подзаконными актами исполнительной власти и не обеспечивается правовыми гарантиями более высокого уровня.

Модель доступа к информации публичного сектора, сформировавшаяся под влиянием европейского права, объединяет различные механизмы реализации права на доступ к информации публичного сектора, включающие открытые данные как один из механизмов. В рамках данной модели правовое регулирование устанавливается на уровне законов и создает дополнительные механизмы для обжалования отказа (административного или судебного обжалования) в информации.

В отношении персональных данных постановка вопроса о выделении моделей невозможна. Персональные данные – отдельно сформировавшаяся категория, правовое регулирование которой не присутствует в таких странах, как США или Австралия. Большинство рассмотренных стран, имеющих правовое регулирование персональных данных, принадлежит к Европейскому союзу, что исключает возможность выделения моделей ввиду единства европейского подхода и небольшого объема данных других стран для сравнения.

Наконец, допустимо выделить модели правового регулирования геопространственных данных по степени участия частных юридических лиц: модель национального регулирования (Сингапур, Южная Корея) и модель взаимодействия (ЕС, США).

Модель национального регулирования устанавливает условия централизации сбора и управления геопространственными данными,

осуществляемого только на основании разрешения государственного органа и под его контролем. Южная Корея, например, устанавливает обязательные требования к получению разрешения Министра землевладения, инфраструктуры и транспорта для использования геопространственных данных. Такая модель может замедлять развитие новых технологий по получению и использованию геопространственных данных в отсутствие экономических стимулов конкурирующих компаний на рынке.

Модель взаимодействия предусматривает, что частные организации также могут заниматься сбором геопространственных данных. В то же время в Европейском союзе, например, исходя из того, что часть получаемых частным сектором данных может быть не только лучшего качества, но и необходима для социального развития, устанавливают дополнительные требования, направленные на совместимость собираемых данных, имеющих социальное значение. Модель взаимодействия более гармонична, т.к. позволяет формировать стимулы развития технологий обработки и сбора геопространственных данных.

Таким образом, в отношении отдельных категорий данных можно выделить как общие модели в целом, так и применительно к каждой из категорий. Сочетание выделенных моделей позволяет более детально охарактеризовать правовое регулирование отдельных категорий данных в странах проводимого исследования.

### 3.3 Модели правового регулирования информационного взаимодействия между различными государственными информационными системами

Общая цель правового регулирования информационного взаимодействия различных государственных информационных систем во всех исследуемых юрисдикциях состоит в создании единого информационного пространства в сфере публичного управления. Вместе с тем возможно выделить некоторые модели реализации названных целей,

отличающиеся принципами и методами организации информационного взаимодействия.

Ряду государств ЕС (Эстония, Франция, Германия и др.) присущ централизованный подход к организации информационного взаимодействия. Централизованная правовая модель характеризуется следующими признаками:

– общее правовое регулирование в сфере создания и администрирования государственных информационных систем (во Франции действует Хартия принципов взаимодействия государственных информационных систем[785], Декрет о государственной информационно-коммуникационной системе[786]; в Германии - Закон о продвижении электронного правительства[787], В Эстонии – Акт о публичной информации[788] и Принципы управления сервисами и информацией[789]),

– большая роль специализированных органов, координирующих взаимодействие между государственными информационными системами (во Франции функционируют Межведомственная дирекция по управлению национальными информационными системами – DINSIC, Генеральная дирекция цифрового развития и информационно-коммуникационных систем – DGNUM),

---

[785] Principes de mutualisation du SI de l'Etat. https://www.numerique.gouv.fr/uploads/201811-CSIC-Fiche_05-principes-mutualisation.pdf (дата обращения 14.08.2019).

[786] Décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'Etat. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029337021 (дата обращения 14.08.2019).

[787] Gesetz zur Förderung der elektronischen Verwaltung. URL: http://www.gesetze-im-internet.de/egovg/ (дата обращения 14.08.2019).

[788] Public Information Act. https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения 08.08.2019).

[789] Principles for Managing Services and Governing Information.: https://www.riigiteataja.ee/en/eli/507072017004/consolide (дата обращения: 14.08.2019).

– единая технологическая платформа взаимодействия государственных информационных систем (например, во Франции действует Единая система электронного межведомственного взаимодействия Франции - RIS[790], в Эстонии – X-road).

В некоторых юрисдикциях (например, в Австралии) реализована децентрализованная модель информационного взаимодействия. Для децентрализованной модели характерны следующие признаки:

– принятие на общегосударственном уровне стратегии информационного взаимодействия, закрепляющей лишь общие принципы взаимодействия информационных систем (в Австралии принята Национальная правительственная стратегия обмена информацией - NGISS791, которая не устанавливает единообразного подхода к обеспечению взаимодействия, а ограничивается общим подходом к обмену информацией на всех уровнях государственного управления),

– преимущественно отраслевой характер организации информационного взаимодействия,

– приоритет соглашений об информационном взаимодействии между участниками информационного взаимодействия перед административными методами организации взаимодействия (в Австралии обмен данными между многими ведомствами осуществляется в рамках Партнерства интеграции данных – DIPA792),

---

[790] Arrêté du 17 décembre 2012 portant création d'un service à compétence nationale dénommé « Réseau interministériel de l'Etat ». https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026792328&categorieLien=id (дата обращения: 01.09.2019).

[791] National Government Information Sharing Strategy. https://www.finance.gov.au/sites/default/files/ngiss.pdf (дата обращения: 01.09.2019).

[792] The Data Integration Partnership for Australia (DIPA). https://www.pmc.gov.au/public-data/data-integration-partnership-australia (дата обращения: 25.07.2019).

– проектный подход к организации взаимодействия информационных систем (например, в Австралии реализуется проект мульти-агентской интеграции данных (MADIP)[793] – партнерство шести государственных учреждений).

Технически взаимодействие информационных систем может быть также организовано по централизованной и децентрализованной модели. Обе модели взаимодействия информационных систем имеют как достоинства, так и слабые стороны[794]. Централизованная модель удобна для оперативного информационного взаимодействия, однако таит в себе более высокую степень уязвимости с точки зрения информационной безопасности. Децентрализованная модель, особенно на первый взгляд, в большей степени отвечает целям информационной безопасности (за счет распределённого хранения данных), но при этом предполагает технологические препятствия для информационного взаимодействия.

Третья, компромиссная модель предполагает координацию государственных информационных систем с централизованным хранением не всех данных, а только тех, которые необходимы для выполнения координирующей функции, в то время как основной массив данных хранится децентрализованно, но при этом обеспечивается доступ и переносимость данных (координационная модель). Такой подход является наиболее взвешенным, поскольку он позволяет оптимизировать риски информационной безопасности за счёт распределенного хранения данных,

[793] Multi-Agency Data Integration Project (MADIP). https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP (дата обращения: 25.07.2019).

[794] Научные дискуссии об оптимальности централизованного или децентрализованного хранения баз данных с чувствительной информацией ведутся уже более 40 лет. См., например, Turn R., Shapiro N., Juncosa M. Privacy and security in centralized vs. decentralized databank systems. Policy Sciences. 1976. Issue 1. P. 17–29. https://www.researchgate.net/publication/225826221_Privacy_and_security_in_centralized_vs_decentralized_databank_systems (дата обращения: 12.09.2019).

учитывать потребности отдельных публичных органов, при этом обеспечивает условия для координации их деятельности и оперативного обмена информацией между ними.

В большинстве исследуемых юрисдикций реализуется либо децентрализованная модель хранения данных (Австралия) либо третья, координационная модель (страны ЕС).

Примером организации информационного взаимодействия по координационной модели является подход, реализованный в Эстонии. Так, единая государственная информационная система данной страны состоит из баз данных, которые взаимодействуют со слоем обмена данными государственной информационной системы (то есть отдельных баз данных, администрируемых разными публичными органами), а также систем, поддерживающих ведение баз данных (support systems)[795]. Координационная модель предполагает действие интегрирующей платформы и подключенной к ней совокупности различных информационных систем (баз данных).

Таким образом, наиболее распространенная в зарубежных юрисдикциях модель правового регулирования взаимодействия государственных информационных систем предполагает наличие: общего нормативно-правового регулирования в сфере организации государственных информационных систем и управления данными публичного сектора; специализированных органов, координирующих деятельность по созданию и функционированию информационных систем. Оптимальная модель взаимодействия информационных систем не требует централизованного хранения данных, но предполагает наличие координирующей системы,

---

[795] К системам, поддерживающим ведение баз данных в государственной информационной системе, относятся: система классификаций; геодезическая система; система адресов; система мер безопасности для информационных систем; уровень обмена данными информационных систем; система управления государственной информационной системой

обеспечивающей техническое взаимодействие всех информационных систем, используемых в сфере публичного управления.

3.4 Обеспечение достоверности, актуальности и сохранности данных

Подход к правовому обеспечению информационной безопасности в различных странах имеет различия, которые позволяют выделить общие модели подхода к обеспечению достоверности, актуальности и сохранности данных. Выделяется две модели:

1) установление норм регулирования на государственном уровне,

2) государственно-частное регулирование.

Примером первой модели выступает Франция. В отличие от других стран Европейского союза, рассмотренных в рамках настоящего исследования, право Франции невозможно рассматривать в отрыве от права ЕС. Во французском праве положения многих директив ЕС во многом имплементированы их буквальным копированием. Право субъекта персональных данных на устранение в них противоречий во Франции рассматриваются в контексте общеевропейского права и не обладают дополнительной спецификой. Таким образом, французское право на нормативном уровне устанавливает правила устранения противоречий в режимах информации при предоставлении публичных данных иным лицам, оберегая как конфиденциальную публичную информацию, так и относящуюся к частным лицам. Одновременно, в связи с реформированием системы межведомственного взаимодействия, французская юрисдикция предпринимает попытки устранить дублирование сбора необходимой информации государственными органами. Французское право при этом в целом предполагает возможность невластного субъекта уточнить или исправить необходимые данные.

Вопросы подхода к выявлению и разрешению противоречий в данных, содержащихся в различных государственных информационных системах, и подхода к мониторингу и аудиту государственных информационных систем на предмет достоверности и иных показателей содержащихся в них данных в

рамках Сингапура тождественны. Аудит, обнаружение и исправление ошибок, корректировка неактуальной информации – элементы единого процесса управления данными и рисками, связанными с оборотом государственных данных. Как правило, государственные органы назначают сотрудников, ответственных за внутренний аудит, за обеспечение информационной безопасности.

В Эстонии отдельным актом[796] утверждена концепция базовых данных, которая заключается в признании авторитетного (эталонного) источника конкретной информации, хранящейся в различных базах данных. Если выявлено противоречие в данных, обрабатываемых в разных базах данных, приоритет остается за той информацией, которая содержится в первичной базе данных. Указанный Акт о публичной информации закрепляет обязанность держателя информации не поставлять заведомо ложную, неточную или неверную информацию и, в случае возникновения сомнений, обязательно проверять правильность и достоверность предоставленной информации. Также установлен запрет размещения устаревшей, неточной или вводящей в заблуждение информации на веб-сайте публичных органов.

Великобритания являет пример второй из указанных моделей. В данной стране противоречия с обеспечением достоверности, актуальности и сохранности данных возникают в первую очередь в сфере защиты персональных данных. Правовые противоречия, связанные с нарушением прав субъектов персональных данных, в частности, в отношении права на исправление неточных персональных данных (right to rectification) в государственной информационной системе должны решаться субъектами персональных данных и Информационным комиссаром. В частности, отношение ко второй модели подтверждает административная и судебная

[796] Public Information Act. https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения: 14.08.2019).

практика: по вопросу выявления и разрешения противоречий в отношении данных, находящихся в ведении государственных органов, она не так развита, как практика в отношении частных субъектов – контроллеров (операторов в российской системе терминологических координат).

3.5 Модели обеспечения конфиденциальности, целостности и доступности данных

Конфиденциальность, целостность и доступность данных образуют классическую триаду принципов информационной безопасности (confidentiality, integrity, accessibility – CIA[797]). В отличие от России, большинство зарубежных юрисдикций придерживаются узкого подхода к пониманию информационной безопасности.

Так, Доктрина информационной безопасности Российской Федерации[798] определяет информационную безопасность как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В зарубежной доктрине и зарубежных правовых актах распространен узкий подход к пониманию информационной безопасности, при котором информационная безопасность (information security, cyber security) охватывает главным образом вопросы защиты информации и

---

[797] См. Международные стандарты по управлению информационной безопасностью. https://www.iso.org/isoiec-27001-information-security.html (дата обращения: 10.08.2018).

[798] Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» СЗ N 50, ст. 7074 (далее – «Доктрина информационной безопасности»).

информационных систем в контексте обеспечения целостности, доступности и конфиденциальности информации. В таком контексте обеспечение информационной безопасности предполагает защиту информационных систем от несанкционированного доступа, искажения, модификации, уничтожения информации[799]. В правовых документах ЕС к информационной безопасности относят безопасность сетей и информационных систем, означающую их способность противодействовать любому действию, которое подвергает опасности доступность, аутентичность, целостность или конфиденциальность хранящейся, передаваемой или обрабатываемой в них информации[800].

В российском законодательстве подобная деятельность охватывается понятием «защита информации», которое раскрывается в статье 16 ФЗ «Об информации, информационных технологиях и о защите информации»[801]. В отечественной доктрине информационного права отмечается, что отношения по обеспечению информационной безопасности несправедливо сводить только к правоотношениям по защите информации[802].

Таким образом, в исследуемых юрисдикциях распространена модель ограничительного понимания конфиденциальности, целостности и доступности информации, которая предполагает защиту информационных

---

[799] См., например, определение информационной безопасности в Федеральном акте США «Об управлении информационной безопасностью».: https://www.law.cornell.edu/uscode/text/44/3542 (дата обращения: 02.09.2019).

[800] 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата обращения: 01.09.2019).

[801] СЗ РФ, 31.07.2006, N 31 (1 ч.), ст. 3448.

[802] Морозов А.В. и др. Организационно-правовое обеспечение информационной безопасности. М., 2013. С. 42.

систем от искажения, утечки информации, неправомерного доступа к информации и т.д.

В рамках обеспечения конфиденциальности, целостности и доступности большую роль играет защита критической информационной инфраструктуры (КИИ). Возможно выделить две основные модели регулирования безопасности КИИ в зависимости от непосредственного предмета регулирования: «объектную» (Германия) и «субъектно-деятельностную» (Франция, Сингапур и др.).

В законодательстве всех исследуемых юрисдикций прослеживаются сходные термины, аналогичные обязанности субъектов КИИ, идентичные полномочия компетентных органов в сфере обеспечения безопасности КИИ, установление административной и уголовной ответственности за нарушения в сфере КИИ. Указанное объясняется общей целью соответствующего регулирования – обеспечение безопасности КИИ.

Характерные особенности каждый из модели защиты КИИ таковы. «Объектная» модель характеризуется следующими особенностями:

– регулирование направлено непосредственно на объекты КИИ,

– наличие иерархически стройной системы регулирования в сфере КИИ,

– построение терминологического аппарата от определения КИИ и ее объектов,

– установление четких критериев категорирования через формирование «пороговых значений»,

– конкретное закрепление обязанностей субъектов,

– ограниченное количество уполномоченных органов с четко-определенной компетенцией.

Указанный подход позволяет, с одной стороны, упорядочить гражданский оборот (новый собственник объекта понимает, к какой категории он относится и какие обязанности на него будут возложены), с другой − упрощает государственным органам контроль за владельцами

таких объектов даже в тех случаях, если последние неправильно осуществили категорирование.

Вместе с тем указанному подходу недостает гибкости в части установления требований к безопасности конкретного объекта.

Среди особенностей «субъектно-деятельностной» модели необходимо отметить:

– регулирование деятельности субъектов в сфере КИИ,

– разрозненность нормативно-правового регулирования в сфере безопасности КИИ,

– построение терминологического аппарата от определения жизненно-важных услуг (сервисов),

– гибкость в вопросах категорирования, риск-ориентированный подход,

– множество регуляторов в разных сферах КИИ.

Субъектно-деятельностная модель регулирования является более гибкой (например, конкретный объект КИИ может принадлежать конкретному лицу, но не использоваться, следовательно, ущерб объекту не окажет существенного влияния, соответственно нет необходимости в принятии специальных мер безопасности). В данной модели имеет значение хозяйственная деятельность субъекта в той или иной сфере и возможный ущерб такой значимой деятельности от компьютерного инцидента. Указанная модель предусматривает большую степень самостоятельности субъектов и, как правило, предполагает риск-ориентированный подход (когда субъект в каждом случае выносит решение о соразмерности принимаемых мер киберугрозам).

На практике реализуются смешанные модели к регулированию критической информационной инфраструктуры, когда требования предъявляются как к объектам, так и к субъектам КИИ. Однако в смешанной модели в качестве системообразующего элемента преобладает либо объектный, либо субъектно-деятельностный подход, который определяет

логику законодательства, терминологический аппарат и т.п. Например, в России законодательство в сфере КИИ построено по смешанной модели, но с преобладанием объектного подхода.

При обеспечении доступа к данным из государственных систем здравоохранения операторами систем принимаются меры по обеспечению конфиденциальности информации ограниченного доступа и защите персональных данных. Например, в Эстонии Акт о публичной информации[803] выделяет категорию информации ограниченного доступа (restricted information). Руководитель публичного органа может огранить доступ к конкретной информации и классифицировать ее как информацию для внутреннего использования (information intended for internal use) в соответствии с установленными основаниями (см. § 35). Отнесение данных к информации ограниченного доступа, в том числе к персональным данным, может быть основанием для отказа в доступе к данным третьим лицам. При этом любое лицо может оспорить ограничение доступа к информации, если такое ограничение нарушает его права или свободы. В целом подход к обеспечению конфиденциальности данных, обрабатываемых в государственных информационных системах, единообразен во всех исследуемых юрисдикциях.

Во всех исследуемых юрисдикциях на нормативно-правовом уровне закреплена система мер по защите государственных информационных систем. Например, во Франции агентство, отвечающее за национальную кибербезопасность (ANSSI)[804], устанавливает правила и политику защиты государственных информационных систем, а также осуществляет

---

[803] https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения 08.08.2019).

[804] The National Cybersecurity Agency of France: https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/ (дата обращения: 01.11.2019).

мониторинг и контроль за принятием предписанных мер безопасности[805]. В Эстонии аналогичная система мер разработана Агентством по информационным системам (RIA)[806]. Система мер безопасности информационных систем, утвержденная правительством, предполагает дифференциацию принимаемых мер безопасности в зависимости от определяемого уровня, класса и подкласса безопасности[807]. Отдельно разработаны правила оценки рисков информационной безопасности[808]. В некоторых странах, например в Австралии, правительство разработало общие руководящие правила безопасности информационных систем не только в сфере публичного управления, но и в частном секторе[809].

3.6 Гармонизация данных и унификация форматов представления информации и технологий информационного обмена

Унификация технологий информационного обмена и форматов предоставления информации (форматов файлов) является необходимым элементом повышения эффективности операций как в системе

---

[805] См. Cyberwiser. France https://www.cyberwiser.eu/france-fr (дата обращения: 01.11.2019).

[806] Агентство по информационным системам Эстонии координирует разработку и администрирование информационных систем, обеспечивая интероперабельность государственных информационной системы, организует деятельность, связанную с информационной безопасностью, противодействует киберинцидентам в компьютерных системах. The Information System Authority (RIA) https://www.ria.ee/en/cyber-security/supervision.html (дата обращения: 01.11.2019).

[807] The system of security measures for information systems https://www.ria.ee/sites/default/files/content-editors/ISKE/regulation-the-system-of-security-measures-for-information-systems-2007-12-20.pdf (дата обращения: 01.11.2019).

[808] Requirements for risk analysis of network and information systems and description of security measures https://www.ria.ee/sites/default/files/content-editors/KIIK/requirements-for-risk-analysis.pdf (дата обращения: 01.11.2019).

[809] Australian Government Information Security Manual https://www.cyber.gov.au/sites/default/files/2019-05/Australian%20Government%20Information%20Security%20Manual%20%28MAY19%29.pdf (дата обращения: 01.11.2019).

межведомственного взаимодействия, так и в системе орган публичной власти – невластный субъект (юридические и физические лица).

Для целей анализа и обобщения подходов к указанному вопросу по исследуемым юрисдикциям предлагается использовать следующие критерии:

– установление конкретных форматов на основании общего акта (содержащего принципы регулирования сферы стандартизации)/ установление конкретных форматов без соответствующего акта,

– назначение единого ответственного органа по стандартизации/ децентрализованная система стандартизации,

– акцент на технологиях информационного обмена (процесс) / акцент на форматах предоставления информации или форматах файлов (результат),

– установление единых форматов внутренних и внешних информационных обменов / установление единых форматов исключительно для целей внешних обменов информацией.

Действие общего акта, устанавливающего принципы в сфере информационного обмена, является характерной чертой большинства исследуемых правопорядков, в частности, Великобритании, Франции, Германии, Эстонии.

Единый ответственный орган стандартизации (в контексте форматов представления информации) существует также в большинстве проанализированных правопорядков, в частности, в Великобритании, Франции, Германии, Эстонии, ЕС.

Регулирование в исследуемой области в основном решает проблемы унификации процессов обмена информацией в Австралии и Германии.

Регулирование в исследуемой области в основном решает проблемы унификации форматов файлов в Великобритании, Франции, Эстонии, ЕС.

Единые информационные стандарты действуют для внутренних и внешних отношений в большинстве проанализированных юрисдикций, за исключением Франции. Для внутренних нужд органы власти во Франции могут свободно определять, какие нормы и стандарты будут применяться.

Одновременно, рекомендуется следовать предлагаемым стандартам по умолчанию. В остальных случаях положения стандартов являются обязательными для органов власти.

Из рассмотренных критериев можно выделить следующие возможные классификации по вопросу гармонизации данных и унификации форматов представления информации и технологий информационного обмена:

– по централизации процессов информационной стандартизации: юрисдикции с централизованным / децентрализованным подходом (критерий 1,2).,

– по комплексности подходов: юрисдикции с комплексным / фрагментарным подходами в исследуемой информационной сфере (критерий 3,4).

Из сказанного следует, что большинство исследуемых юрисдикций придерживаются централизованного подхода к гармонизации данных и унификации форматов представления информации и технологий информационного обмена (установление конкретных форматов на основании общих принципов).

Также стоит отметить, что большинство юрисдикций отличаются комплексным подходом к стандартизации форматов. Вместе с тем существуют различия.

Так, для одних систем характерно регулирование вопросов стандартизации информационного обмена (Австралия, Германия), а для других – вопросов стандартизации форматов файлов (ЕС, Великобритания, Франция, Эстония).

Следовательно, если целью является выявление различных моделей, необходимо выделить условно-«процессуальную» и условно-«форматную» модели гармонизации данных и унификации форматов представления информации и технологий информационного обмена.

3.7 Модели подходов к мониторингу и аудиту государственных информационных систем на предмет достоверности и иных качественных показателей содержащихся в них данных

В анализируемых странах реализуются различные формы контроля публичных органов и подведомственных им организаций. В зависимости от органов, осуществляющих мониторинг и аудит государственных систем, выделяются три основные модели:

1) осуществление аудита/мониторинга единым государственным органом,

2) ответственность каждого отдельного государственного органа за аудит/мониторинг в подведомственной сфере,

3) смешанная модель.

Первая модель подразумевает деятельность государственного органа, осуществляющего аудит и мониторинг государственных систем. Осуществление контрольно-надзорной функции осуществляется только этим органом, то есть проверка происходит исключительно на общегосударственном уровне.

Примером такой модели выступает Германия. Полномочиями по контролю и аудиту соблюдения законодательства о защите данных наделен Федеральный комиссар защиты данных и свободы информации.

В Великобритании Информационный комиссар проводит аудит в области соблюдения законодательства о персональных данных и свободы информации. Планирование аудита основывается на риск-ориентированном подходе, который предполагает выявление контроллеров (операторов, в терминологии отечественного законодательства в области персональных данных) и секторов с потенциально-высоким риском нарушений. По общему правилу аудит не является карательной мерой, следовательно, обычно никаких принудительных санкций за несоответствия не накладывается. Сферы проверки выбираются исходя из направлений деятельности органа публичной власти и не являются одинаковыми для различных органов.

В Эстонии субъектами, осуществляющими надзор за соблюдением требований Акта о публичной информации, является Инспекция защиты данных, вышестоящие над держателями данных органы; Министерство экономики и коммуникаций. Инспекция по защите данных осуществляет надзор за деятельностью держателей данных. Надзорные меры могут осуществляться как на основании правонарушений, так и по собственной инициативе Инспекции. Инспекция проверяет порядок исполнения обязанностей по предоставлению информации по запросу, по раскрытию информации, в том числе полноту размещаемой информации на веб-сайте. Инспекция может давать рекомендации по имплементации требований Акта о публичной информации.

Вторая модель представляет собой расширенный вариант первой. Наличие государственного органа, ответственного за мониторинг и аудит, не означает, что исключительно данный орган и подведомственные ему организации осуществляют аналогичные проверки. Такой орган в большей степени является главным контрольным органом, он назначает сотрудников, ответственных за внутренний аудит, и наделяет их полномочиями.

Сингапур – пример второй рассматриваемой модели. Внутри агентства государственных технологий (орган, ответственный за цифровизацию систем) действует комитет по рискам и аудиту. Данный комитет занимается определением и оперативным устранением рисков оборота государственных данных, методиками работы с противоречиями внутри ГИСов и т.д. Однако каждый государственный орган самостоятельно управляет своими данными и/или отвечает за свой сектор данных внутри общей инфраструктуры, определяет процедуры проверки корректности данных, устранения ошибок, проверки систем и распределение ответственности за нарушения с вендорами информационных компонентов. Например, Министерство здравоохранения самостоятельно управляет ошибками и утечками данных. Как правило, государственные органы назначают сотрудников, ответственных за внутренний аудит, обеспечение информационной безопасности. Ошибки в

информационных системах устраняются самостоятельно ответственными сотрудниками, обнаружившими такие ошибки, или же по заявлениям/информации, поступающей извне.

Во Франции реализуются различные формы контроля публичных органов и подведомственных им организаций. Особый акцент сделан на квалифицированный министерский внутренний аудит. В стране организована система профессионального внутреннего аудита для каждого министерства. Под руководством министра, ответственного за реформирование государства, создается Комитет гармонизации внутреннего аудита (CHAIE), который объединяет лиц ответственных за внутренний аудит каждого министерства, представителей генерального директора публичных финансов, генерального директора бюджета, а также лиц, назначенных постановлением Премьер-министра. CHAIE утверждает нормативные акты внутреннего аудита, а также ежегодно проверяет политику аудита в каждом министерстве и дает рекомендации. Кроме того, создается министерская миссия внутреннего аудита, которая проводит глубокий анализ возможных рисков, готовит для утверждения Комитетом программу внутреннего аудита.

В отношении информационных систем также могут реализовываться формы внешнего и смешанного контроля. Декретом председателя совета министров установлены меры внешнего экономического и финансового контроля (CGefI). Внутри CGefI выделена миссия аудита, которая участвует как во внутреннем министерском контроле (смешанный контроль), так и во внешнем.

В связи с активным развитием государственных информационных систем и цифровизацией управления, деятельность каждого из министерств по созданию и развитию информационных систем в соответствии с его полномочиями подлежит также внешней координации. Межведомственная дирекция по управлению национальными информационными системами (DINSIC) имеет полномочия мониторинга развития государственных информационных систем в форме предварительного одобрения проектов

развития и создания государственных информационных систем, утверждаемых каждым министерством в соответствии с его компетенцией. Таким образом, контроль над государственными информационными системами осуществляется во Франции в следующих формах: внутренней, внешней и смешанной (предварительного согласования). При этом отдельный акцент во французском праве сделан на квалифицированном постоянном внутреннем министерском аудите.

3.8 Монетизация данных, их продажа и оказание платных услуг с их использованием

Данные, в том числе находящиеся в государственных информационных системах, имеют большую ценность. Причем ценность данных может проявляться как в явном виде (в связи с возможностью получения прямого дохода от использования данных третьими лицами), так и косвенно (ценность проявляется в пользе, приносимой экономике, обществу, государству и т.п.).

Исследование зарубежного опыта показывает, что подходы в правовом регулировании монетизации публичных данных в анализируемых странах во многом схожи.

Во всех анализируемых странах принят национальный централизованный правовой акт, устанавливающий возможность повторного использования государственных данных третьими лицами (на уровне Европейского союза также действует наднациональное регулирование данного аспекта в виде Директивы 2003/98/ЕС о повторном использовании информации публичного сектора). Основной целью данного законодательства является создание условий для развития новых услуг, бизнес-моделей, основанных на повторном использовании публичных данных, что позволяет ускорять экономический рост стран, содействовать социальной активности. Соответственно использование публичных данных возможно в коммерческих и некоммерческих целях.

В результате анализа национального и наднационального законодательства выявлены следующие общие черты в подходах к монетизации данных публичного сектора:

– установление предельного размера платы за доступ к публичным данным, при этом размер платы или порядок ее определения подлежат публикации,

– утверждение специального положения отдельных категорий субъектов (библиотек, архивов, музеев, образовательных учреждений), а также исключений из общего подхода для доступа к данным в определенных целях (например, исследовательских),

– предоставление доступа к данным на основании соглашений, определяющих порядок и ограничения использования данных, а также возможный контроль за их использованием (по общему правилу данные предоставляются на основании лицензии Creative Commons),

– обеспечение равного доступа к данным и недопустимость эксклюзивных соглашений.

При этом выделяются следующие подходы к установлению платы за доступ к данным: 1) бесплатное предоставление данных, 2) установление платы в размере расходов, понесенных органом в связи с деятельностью по предоставлению данных, 3) установление платы в размере издержек государственного органа с минимальной наценкой, 4) утверждение дифференцированного подхода к определению стоимости доступа к данным.

Первый подход является наиболее распространенным. В основной своей массе данные государственного сектора для последующего использования предоставляются бесплатно. Это объясняется в первую очередь тем, что во многих странах в настоящее время реализуется концепция электронного (открытого) правительства. Открытые данные способствуют повышению прозрачности деятельности органов власти стран различного уровня. Кроме того, открытые данные играют важную роль в развитии государства (с точки зрения экономики, социальной сферы,

политики и пр.), т.е. само государство заинтересовано в облегчении доступа граждан, организаций к публичным данным. Для достижения этой цели государственные органы публикуют информацию в доступных форматах, предлагают удобные инструменты использования данных (в том числе API открытых платформ), используют стандартные лицензии.

Реже применяется второй подход. Законодательством Европейского союза и отдельных стран государственным органам дано право взимать плату за предоставление публичных данных в размере, необходимом для покрытия издержек, понесенных в связи со сбором, оцифровкой, воспроизведением, предоставлением данных. При этом могут устанавливаться способы расчета возмещения. В частности, на сайте ETALAB[810] французского Межведомственного управления цифровых и информационных систем и коммуникаций государства приведены таблица с уточнением расчета максимального размера возмещения. Примеры данного подхода можно найти и в правовом регулировании других государств. Применение такого подхода призвано обеспечивать баланс интересов государственных органов (при несении им затрат) и интересов субъектов, реализующих свое право на доступ к информации.

Третий подход предполагает установление платы за пользование публичными данными с применением минимальной наценки к сумме расходов, понесенных государственным органом при предоставлении таких данных третьим лицам. Данный подход легализован в Германии, где законом «О повторном использовании информации государственного сектора» (IWG)[811] предусмотрена возможность применять разумную норму прибыли к сумме расходов, понесенных государственным органом. При этом плата взимается в соответствии с правилами бухгалтерского учета, применимым к

[810] https://www.etalab.gouv.fr/ (дата обращения 12 09 2019)
[811] IWG. https://www.gesetze-im-internet.de/iwg/ (дата обращения: 02.08.2019)

соответствующим органам государственного сектора. Несмотря на то, что данный подход на практике не применяется, наблюдаются тенденции к его популяризации. Так, Еврокомиссией реализуются различные инициативы по пересмотру Директивы о повторном использовании информации государственного сектора. В частности по заказу Еврокомиссии в 2018 г. проведено исследование, результаты которого содержатся в Позиционной бумаге LAPSI n. 1 «Принципы, регулирующие взимание платы за повторное использование информации государственного сектора»[812], основной целью которого было расширение возможностей взимания платы за использование публичных данных сверх «компенсационной» суммы.

Четвертый подход (применение дифференцированной платы за использование данных публичного сектора) виден на примере Австралии, где внедрена практика коммерческого доступа к микроданным (Microdata). Помимо этого в Австралии внедрена Система по взиманию платы Правительством (Фреймворк)[813], устанавливающая рекомендации по определению размера платы в зависимости от субъектов, запрашивающих данные, и целей обработки данных. В частности, выделяются категории платы:

– плата неправительственному сектору в целях возмещения издержек, связанных с регулирующей деятельностью, в рамках которой правительство выполняет публичные функции по управлению рисками, стремится контролировать или влиять на поведение деятелей неправительственного сектора,

---

[812] Позиционная бумага LAPSI n. 1: Принципы, регулирующие взимание платы за повторное использование информации государственного сектора http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8342 (дата обращения 10.08.2019).

[813] Australian Government Charging Framework (the Charging Framework). https://www.finance.gov.au/resource-management/charging-framework/ (дата обращения 02.08.2019).

– плата в рамках коммерческой деятельности, когда государство участвует на рынке товаров/услуг и пользователь обладает определенной свободой действий,

– плата за предоставление конкретных прав или доступов к государственным информационным ресурсам.

Таким образом, в настоящий момент правовое регулирование монетизация данных в разных странах проходит этап активного развития, внедряются разнообразные подходы к формированию условий и порядка определения платы за использование данных государственного сектора.

3.9 Модели использования специальных финансовых и юридических инструментов для создания «маркетплейсов» на основе данных

На сегодняшний день сложились три основные модели регулирования отношений, связанных с созданием и функционированием «маркетплейсов» на основе данных.

Рассматриваемым моделям присущи как общие, так и особенные признаки.

К общим признакам, присущим всем моделям, следует отнести отсутствие «маркетплейса» на основе данных как самостоятельной правовой категории. По этой причине ни в одном из исследованных правопорядков не выявлено специального регулирования отношений, связанных с созданием и функционированием такого рода «маркетплейсов», а также специальных норм, направленных на защиту прав потребителей и обеспечение конкуренции на подобных площадках обмена данными.

К особенностям рассматриваемых моделей можно отнести наличие или отсутствие специального регулирования цифровых (онлайн) платформ, одной из разновидностей которых являются «маркетплейсы» на основе данных.

Так, лишь в одной юрисдикции (Франция) законодательство содержит определение цифровых (онлайн) платформ, а также определяет налоговый статус операторов таких платформ. Кроме того, в данном правопорядке

отдельно урегулированы обязательства операторов платформ в отношениях, возникающих с их потребителями. Таким образом, не выделяя «маркетплейсы» данных в самостоятельную правовую категорию, есть основания полагать, что в рамках данной модели их правовое регулирование подпадает под регулирование цифровых платформ.

Вторая модель, реализованная в большинстве рассмотренных правопорядков (Великобритания, Эстония, Австралия, ЕС) характеризуется тем, что на отношения, связанные с деятельностью маркетплейсов, распространяется действующее регулирование «традиционных» отношений. Прежде всего речь идет о нормах конкурентного права (например, создание условий для равного доступа частных субъектов к соответствующему ресурсу, запрет на дискриминацию, запрет на злоупотребление доминирующим положением на рынке и пр.). Также к «маркетплейсам» на основе данных будет применимо общее законодательство о защите прав потребителей, некоторые положения законодательства об открытых данных (в части гарантий недискриминационного доступа к данным государственного сектора), законодательство о защите персональных данных, а также законодательство о кибербезопасности.

Кроме того, в ЕС определены принципы деятельности цифровых платформ, которые также могут быть распространены на деятельность «маркетплейсов» на основе данных (одинаковые условия для сопоставимых цифровых сервисов; предотвращение распространения нелегального контента установление доверия, обеспечение прозрачности и добросовестности и другие). Это сближает подход ЕС с французской моделью.

В остальных странах не выявлено специального регулирования «маркетплейсов» на основе данных. В Сингапуре при отсутствии специальных нормативных актов регулирование обмена данными происходит в рамках регулятивных «песочниц», учреждаемых и функционирующих под управлением государственных структур. В Германии

идея обмена данными через цифровые платформы реализована лишь применительно к открытым данным публичного сектора.

В завершение следует указать, что существует определенная терминологическая специфика, в соответствии с которой в ряде стран (Великобритания, Австралия, Франция, Эстония) под маркетплейсом данных традиционно понимают электронные площадки (Digital Marketplace, Marketplace), предназначенные для размещения, поиска и управления закупками цифровых продуктов, сервисов, в том числе, облачных сервисов для правительственных нужд

3.10 Лицензирование, сертификация или установления иных требований к лицам, претендующим на доступ к данным, содержащимся в государственных информационных системах

Доступ к данным, содержащимся в государственных информационных системах, может разделяться на несколько моделей в зависимости от категорирующего признака:

1) по категории лица, претендующего на доступ к данным, содержащимся в государственных информационных системах – доступ для граждан и доступ для юридических лиц,

2) по типу информации, доступ к которой запрашивается – доступ к открытым данным или данным ограниченного доступа,

3) по целям доступа – для осуществления (помощи в осуществлении) публичной функции или для коммерческого использования.

Необходимо отметить некоторые сходные тенденции, прослеживаемые во всех анализируемых юрисдикциях:

– создание государственных программ и инициатив в сфере унификации принципов работы с данными и упрощения доступа к государственным данным. Например, в Сингапуре действует программа

Digital Government Transformation и специальный государственный орган по исполнению программы – Government Technology Agency; в Великобритании реализуются программы Government Transformation Strategy[814] и UK Digital Strategy[815], во Франции - программа трансформации публичной службы Франции до 2022 г.[816] и т.д.,

– открытие большой части информации через общедоступные источники, единые порталы открытых/государственных данных посредством использования открытых протоколов (например, API). Таким порталом является, GOV.UK, который дает возможность через сервис Gov.uk Registers, извлекать структурированные наборы данных, находящихся в ведении государственных органов, в форматах CSV и ODS, с использованием API[817]. Кроме того, Data.gov.au[818] является центральным источником открытых правительственных данных (Open government data) Австралии, которые также размещаются в машиночитаемом виде с использованием API. Такие порталы функционируют и во многих других государствах, например, в Соединенных Штатах[819], КНР[820] и т.д. Доступ к подобным данным, находящимся в государственных информационных системах, не требует дополнительных условий, сертификации и т.д. Такие сведения открыты для физических и юридических лиц как для коммерческого, так и для некоммерческого использования,

---

[814] https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020 (дата обращения 19 08 2019)

[815] https://www.gov.uk/government/publications/uk-digital-strategy (дата обращения 20 05 2019)

[816] ACTION PUBLIQUE 2022 : UN PROGRAMME POUR ACCÉLÉRER LA TRANSFORMATION DU SERVICE PUBLIC. https://www.modernisation.gouv.fr/action-publique-2022/comprendre/action-publique-2022-un-programme-pour-accelerer-la-transformation-du-service-public (дата обращения 07 06 2019)

[817] https://www.gov.uk (дата обращения 10 11 2019)

[818] https://data.gov.au 9 (дата обращения 5 06 2019)

[819] https://www.data.gov (дата обращения 24 09 2019)

[820] http://data.stats.gov.cn/english/ ( дата обращения 31 10 2019)

– проведение технологической ревизии, активизация работы по стандартизации в сфере работы с данными, создание специализированных органов и/или должностных лиц, ответственных за работу IT систем. Так, в Великобритании на Цифровую правительственную службу возложен набор обязанностей, среди которых: разработка и поддержка совместимых, понятных, высококачественных сервисов, основанных на лучших практиках и рекомендациях; установка и применение стандартов цифровых услуг; разработка и поддержка общих платформ, сервисов, услуг и инструментов и т.д.[821] с учётом требований стандартов в сфере обработки данных, установленных уполномоченным органом − Советом стандартизации (Open Standards Board)[822]. В Китае разработка стандартов ведётся крайне активно и динамично. В 2018 году в КНР введен Национальный стандарт по технологиям информационной безопасности «Требования безопасности персональных данных» (National Standard of the People's Republic of China for Information Security Technology – Personal Data Security Specification)[823], который уже находится в процессе обновления. В Германии Закон о повышении безопасности систем информационных технологий от 7 июля 2015 г. (IT-Sicherheitsgesetz) создал единую правовую базу для обеспечения кибербезопасности. Закон устанавливает минимальные стандарты ИТ и требования к отчетности операторов критически важных инфраструктур (включая энергетику, водоснабжение, здравоохранение,

[821] Government ICT Strategy - Strategic Implementation Plan 2011. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266169/govt-ict-sip.pdf (дата обращения 16 11 2019)

[822] https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice. Policy paper: Open Standards principles, 2018. https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles 9 (дата обращения 22 07 2019)

[823] https://www.chinalawtranslate.com/en/persona-information-security-standards/ (дата обращения 23 10 2019)

телекоммуникации)[824]. Разработкой международных стандартов занимается также Международная организация стандартизации[825]. Со временем многие подготовленные ею стандарты становятся обязательными для применения отдельными государственными органами и частными организациями.

Относительно круга лиц, претендующих на доступ к данным, содержащимся в государственных информационных системах, необходимо отметить следующее. Как правило, для рядовых граждан (пользователей) не устанавливается специальных требований по доступу к информации. Иногда для получения сведений из государственных информационных систем гражданину необходимо обратиться в государственный орган с запросом об информации и уплатить пошлину (например, такой порядок закреплен Актом о свободе информации Великобритании[826]) или же обратиться напрямую на портал государственных данных (например, govdata в Германии). К юридическим лицам, запрашивающим информацию, законом могут предъявляться дополнительные требования в зависимости от характера запрашиваемой информации, канала передачи данных и целей такой передачи.

Государственные органы и их подведомственные организации, как правило, придерживаются специальных стандартов, разработанных для оборота государственных данных. Особенно стоит отметить ряд стандартов Великобритании, которые являются обязательными к использованию государственными органами: Руководство по обмену с государственными

---

[824] IT-Sicherheitsgesetz. https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1565384375246 (дата обращения 05 10 2019)

[825] https://www.iso.org/ru/home.html (дата обращения 01 11 2019)

[826] http://www.legislation.gov.uk/ukpga/2000/36/contents. В Шотландии в силу особенностей ее правовой системы принят отдельный Акт о свободе информации в Шотландии (Freedom of Information (Scotland) Act 2002) http://www.legislation.gov.uk/asp/2002/13/contents (дата обращения 30 10 2019)

документами[827], Руководство по просмотру государственных документов [828], Руководство по обмену информацией о киберугрозах[829], Руководство по стандарту кросс-платформенной кодировки [830]. Также органами государственной власти активно используются международные стандарты, например Руководство по обмену данными о местоположении[831], Руководство по постоянным идентификаторам[832], стандарты Международной организации по стандартизации[833].

Таким образом, лица, претендующие на доступ к государственным данным, обязаны соблюдать все требования государственных органов, для соблюдения интероперабельности данных и беспрепятственной работы информационных систем.

---

[827] Guidance: Sharing or collaborating with government documents, 2019: https://www.gov.uk/government/publications/open-standards-for-government/sharing-or-collaborating-with-government-documents (дата обращения 12 11 2019)

[828] Guidance: Viewing government documents, 2019. https://www.gov.uk/government/publications/open-standards-for-government/viewing-government-documents (дата обращения 12 11 2019)

[829] Guidance: Exchanging Cyber Threat intelligence, 2019. https://www.gov.uk/government/publications/open-standards-for-government/exchanging-cyber-threat-intelligence (дата обращения 12 11 2019)

[830] Guidance: Cross platform character encoding profile, 2019. https://www.gov.uk/government/publications/open-standards-for-government/cross-platform-character-encoding-profile (дата обращения 14 11 2019)

[831] Guidance: Exchange of location point, 2019. URL: https://www.gov.uk/government/publications/open-standards-for-government/exchange-of-location-point (дата обращения 06 11 2019)

[832] Guidance: Persistent resolvable identifiers, 2019. https://www.gov.uk/government/publications/open-standards-for-government/persistent-resolvable-identifiers (дата обращения 14 11 2019)

833 Например, общие рекомендации ISO MEMBER DATA PROTECTION POLICY (URL: https://www.iso.org/iso-member-data-protection-policy.html) (дата обращения 26 11 2019); ISO/TS 8000-1:2011 Data quality https://www.iso.org/standard/50798.html (дата обращения 14 11 2019)

Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data (https://www.iso.org/standard/52955.html); ISO/IEC TS 20748-4:2019 (дата обращения 10 11 2019)

Information technology for learning, education and training — Learning analytics interoperability — Part 4: Privacy and data protection policies https://www.iso.org/standard/74379.html (дата обращения 10 11 2019)

Однако для некоторых видов информации и для некоторых видов деятельности создаются дополнительные требования, нацеленные на повышение уровня защищённости данных ограниченного доступа. Зачастую такие требования сопутствуют механизмам лицензирования отдельных видов деятельности. Так, деятельность в сфере здравоохранения является лицензируемой в большинстве юрисдикций, поэтому деятельность по обработке медицинской информации также требует дополнительных гарантий безопасности, например, аккредитации[834]. Кроме того, деятельность по раскрытию финансовой и трейдерской информации также подлежит дополнительной авторизации. Например, Правила оказания услуг по представлению данных Великобритании (2017 г.) предъявляют подобные требования финансовым организациям[835].

3.11 Выводы

Исследование зарубежного опыта правового регулирования управления данными на примере ряда государств, занимающих ведущие места в международных рейтингах, показывает, что при поступательном развитии информационного общества и внедрении ИКТ в многие сферы жизни человечества проблема оборота данных требует правового разрешения, и различные правовые культуры, не отказываясь полностью от традиций, формируют новые подходы к ней. Подходы выражаются в правовом регулировании прежде всего отдельных категорий (персональных данных, открытых, общедоступных данных).

Общим является принятие законодательства в сфере организации государственных информационных систем и управления данными

[834] https://www.natlawreview.com/article/france-issues-new-rules-accreditation-health-data-hosting-services-providers (дата обращения 14 11 2019)

[835] http://www.legislation.gov.uk/uksi/2017/699/pdfs/uksi_20170699_en.pdf (дата обращения 17 11 2019)

публичного сектора. В проводимых многими юрисдикциями реформах государственного аппарата явственно прослеживаются тенденции перехода от отраслевого принципа к межведомственному, наделения межведомственных органов контрольными полномочиями. В зависимости от органов, осуществляющих мониторинг и аудит государственных систем, выделяются три основные модели:

– осуществление аудита/мониторинга единым государственным органом,

– ответственность каждого отдельного государственного органа за аудит/мониторинг в подведомственной сфере,

– смешанная модель.

Опыт государств с федеративным устройством показывает, что требуется нормативное обеспечение взаимодействия органов разного уровня власти.

В настоящий момент правовое регулирование монетизации данных в разных странах проходит этап активного развития, в том числе внедряются разнообразные подходы к формированию условий и порядка определения платы за использование данных государственного сектора. При этом определились следующие подходы к установлению платы за доступ к данным: 1) бесплатное предоставление данных, 2) установление платы в размере расходов, понесенных органом в связи с осуществлением деятельности по предоставлению данных, 3) установление платы в размере издержек государственного органа с минимальной наценкой, 4) утверждение дифференцированного подхода к определению стоимости доступа к данным.

# ЗАКЛЮЧЕНИЕ

Для исследования зарубежного опыта правового регулирования управления данными был проведен анализ рейтингов зарубежных государств в области цифровой экономики по различными системам рейтингования, по результатам которого отобраны такие страны, как США, Австралия, Великобритания, Германия, Франция, Эстония, Норвегия, Сингапур, Китай, Республика Корея.

В ходе исследования была установлена полнота охвата правовым регулированием различных вопросов управления данными и фактическое наличие соответствующих источников права для последующего анализа зарубежного законодательства. Определен круг зарубежных государств, в которых правовое регулирование управления данными представляется наиболее развитым и достаточным для дальнейшего детального исследования: Великобритания, Австралия, Сингапур, Франция, Германия, Эстония.

Как показал анализ законодательства в европейских государствах со сложившимся правовым регулированием и правовыми традициями в публично-правовой сфере, вопросы управления данными в нем являются логичным продолжением развития публичного права. В азиатских странах, а также таких государствах, как например Австралия, публичное право находится на начальном этапе своего формирования (публично правовые споры, судебные способы их решения, споры гражданин-государство), зато сформировался сильный государственный аппарат, который позволяет решать вопросы управления данными административными методами. С учетом наличия у Российской Федерации международно-правовых обязательств как члена Совета Европы, а также близости российской правовой системы к романо-германскому праву, в первую очередь были рассмотрены модели правового регулирования в области управления данными, которые сформированы в законодательстве государств-членов Европейского союза, таких как Франция, Германия, Эстония.

Анализ правового регулирования в указанных государствах показывает наличие тенденции к большей конкретизации правового режима публичных данных, в том числе включенных в информационные системы, включая вопросы их повторного использования и монетизации (предоставления их за плату или их использования для оказания платных услуг), а также расширения случаев, при которых такие данные подлежат размещению в информационно-телекоммуникационной сети «Интернет» в форме открытых данных. При этом публичные данные и иные аналоги данного термина (например, информация публичного сектора) понимаются по-разному в различных национальных юрисдикциях, например, могут быть ограничены только данными государственных органов, или также охватывать данные различных государственных учреждений. Наряду с развитием правового режима публичных данных также происходит конкретизация правового режима персональных данных, включая потребительские данные как одной из их разновидности. Также существует тенденция к принятию законов, регулирующих на системной основе вопросы наделения государственных данных статусом «эталонных» или «базовых», разработки порядка выявления и устранения противоречий в данных, обрабатываемых в разных государственных базах данных и информационных системах, и взаимодействия между различными государственными информационными системами.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 CEN/TC 434 - Electronic Invoicing. — URL: https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:1883209,25&cs=126F1BDBC8D6D6141F550EB578B4A9CF4 (дата обращения: 21.08.2019)

2 Charalabidis Y. et al. The World of Open Data. Concepts, Methods, Tools and Experiences. Springer International Publishing AG, part of Springer Nature, 2018. P. 2

3 Gartner IT Glossary. — URL: https://blogs.gartner.com/it-glossary/ (дата обращения: 02.08.2019)

4 IMD World Competitiveness Center. IMD World Digital Competitiveness Ranking 2018. — URL: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2018/ (дата обращения 01.08.2019)

5 International Covenant on Civil and Political Rights. — URL: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (дата обращения: 02.08.2019)

6 International Electrotechnical Commission. Electropedia: The World's Online Electrotechnical Vocabulary. — URL: http://www.electropedia.org/iev/iev.nsf/6d6bdd8667c378f7c12581fa003d80e7?OpenForm (дата обращения: 02.08.2019)

7 ISO 10159:2011 «Health informatics — Messages and communication — Web access reference manifest»

8 ISO 10789:2011 «Space systems — Programme management — Information and documentation management»

9 ISO 13008:2012 «Information and documentation — Digital records conversion and migration process»

10 ISO 13527:2010 «Space data and information transfer systems — XML formatted data unit (XFDU) structure and construction rules»

11 ISO 14641:2018 «Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications»

12 ISO 18542-2:2014 «Road vehicles — Standardized repair and maintenance information (RMI) terminology — Part 2: Standardized process implementation requirements, Registration Authority»

13 ISO 22857:2013 «Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data»

14 ISO 26262-1:2011 «Road vehicles — Functional safety — Part 1: Vocabulary»

15 ISO 5127:2017 «Information and documentation. Foundation and vocabulary»

16 ISO 55000:2014 «Asset management — Overview, principles and terminology»

17 ISO 8000-2:2017 «Data quality — Part 2: Vocabulary»

18 ISO MEMBER DATA PROTECTION POLICY. — URL: https://www.iso.org/iso-member-data-protection-policy.html (дата обращения: 02.08.2019)

19 ISO/IEC 15944-10:2013 «Information technology — Business operational view — Part 10: IT-enabled coded domains as semantic components in business transactions»

20 ISO/IEC 25012:2008 «Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model»

21 ISO/IEC 27000:2014 «Information technology — Security techniques — Information security management systems — Overview and vocabulary»

22 ISO/IEC 27001:2013 «Preview Information technology. Security techniques. Information security management systems. Requirements»

23 ISO/IEC 27032:2012 «Information technology — Security techniques — Guidelines for cybersecurity»

24 ISO/IEC 29110-4-3:2018 «Systems and software engineering — Lifecycle profiles for very small entities (VSEs) — Part 4-3: Service delivery — Profile specification»

25 ISO/IEC 8824-2:2015 «Information technology — Abstract Syntax Notation One (ASN.1): Information object specification — Part 2:»

26 ISO/IEC TS 20748-4:2019 «Information technology for learning, education and training — Learning analytics interoperability — Part 4: Privacy and data protection policies»

27 ISO/TS 19475-3:2018 «Document management — Minimum requirements for the storage of documents — Part 3: Disposal»

28 ISO/TS 27790:2009 «Health informatics — Document registry framework»

29 ISO/TS 8000-1:2011 «Data quality»

30 Kirby, Michael. 1999. Privacy protection, a new beginning: OECD principles 20 years on. Privacy Law & Policy Reporter, 6(3) . — URL: http://www5.austlii.edu.au/au/journals/PrivLawPRpr/1999/41.html (дата обращения: 02.08.2019)

31 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. — URL: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (дата обращения: 02.08.2019)

32 The Fletcher School, Tufts University. Digital Planet 2017. How competitiveness and trust in digital economies vary across the world. . — URL: https://sites.tufts.edu/digitalplanet/files/2017/05/Digital_Planet_2017_FINAL.pdf (дата обращения 01.08.2019)

33 Turn, R., Shapiro, N.Z. & Juncosa, M.L. Privacy and security in centralized vs. decentralized databank systems. Policy Sciences (1976), Volume 7, Issue 1. – pp 17–29. — URL: https://www.researchgate.net/publication/225826221_Privacy_and_security_in_centralized_vs_decentralized_databank_systems (дата обращения: 12.09.2019)

34 UNITED NATIONS. UN E-Government Survey 2018. — URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018 (дата обращения 01.08.2019)

35 Watts, D., Casanovas P. Privacy and Data Protection in Australia: a Critical overview (extended abstract). — URL: https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf (дата обращения: 02.08.2019)

36 World Economic Forum. The Global Information Technology Report 2016. Innovating in the Digital Economy. — URL: http://reports.weforum.org/global-information-technology-report-2016/ (дата обращения 01.08.2019)

37 Богдановская И.Ю. Источники права на современном этапе развития «общего права». Диссертация на соискание ученой степени доктора юридических наук. Москва, 2007 г.

38 Журавленко Н. И. Организация защиты информации в развитых зарубежных странах: учебное пособие / Н. И. Журавленко. – Уфа : РИЦ БашГУ, 2014. С. 162

39 Ковалева Н.В. Природа и функции технико-юридических норм // Государство и право. 2016. № 11. С. 5-12

40 Конвенция о защите прав человека и основных свобод. URL: https://www.echr.coe.int/Documents/Convention_RUS.pdf

41 Малько А. В., Солдаткина О. Л. ИНФОРМАЦИОННО-ПРАВОВАЯ ПОЛИТИКА В СОВРЕМЕННОМ ОБЩЕСТВЕ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ //Сравнительная политика. – 2019. – Т. 10. – №. 1. С. 51

42 Организационно-правовое обеспечение информационной безопасности: монография / А. В. Морозов, Т. А. Полякова; РПА Минюста России. — М.: РПА Минюста России, 2013. – С. 42

43 Словарь терминов ITIL. Версия 1.0 от 29.07.2011. — URL: http://www.itsmforum.ru/upload/medialibrary/937/937554807eac2bc6ce4b3b5bbeedb840.pdf (дата обращения: 02.08.2019).

44 Сорокина А. Э. Охрана коммерческой тайны по законодательству зарубежных стран (на примере Великобритании и Германии) //Вестник Московского университета МВД России. – 2013. – №. 1.С. 62

Источники в разрезе Российской Федерации:

45 А.М. Прохоров: Большой энциклопедический словарь. 2-е изд., перераб. и доп.

46 ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения»

47 ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения»

48 ГОСТ 2.053-2013 «Единая система конструкторской документации. Электронная структура изделия. Общие положения»

49 ГОСТ 2.611-2011 «Единая система конструкторской документации. Электронный каталог изделий. Общие положения»

50 ГОСТ 2.612-2011 «Единая система конструкторской документации. Электронный формуляр. Общие положения»

51 ГОСТ 20886-85 «Организация данных в системах обработки данных. Термины и определения»

52 ГОСТ 22487-77 «Проектирование автоматизированное. Термины и определения»

53 ГОСТ 25868-91 «Оборудование периферийное систем обработки информации. Термины и определения»

54 ГОСТ 26553-85 «Обслуживание средств вычислительной техники централизованное комплексное. Термины и определения»

55 ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»

56 ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры»

57 ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»

58 ГОСТ 34.320-96 «Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы»

59 ГОСТ 34.321-96 «Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными»

60 ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»

61 ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»

62 ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем»

63 ГОСТ 7.0-99 «Система стандартов по информации, библиотечному и издательскому делу. Информационно-библиотечная деятельность, библиография. Термины и определения»

64 ГОСТ 7.70-2003 «Система стандартов по информации, библиотечному и издательскому делу. Описание баз данных и машиночитаемых информационных массивов. Состав и обозначение характеристик»

65 ГОСТ 7.73-96 «Система стандартов по информации, библиотечному и издательскому делу. Поиск и распространение информации. Термины и определения»

66 ГОСТ ISO 22745-11-2017 «Системы промышленной автоматизации и интеграция. Открытые технические словари и их применение к основным данным. Часть 11. Руководящие принципы по формулированию терминологии»

67 ГОСТ ISO 9000-2011 «Системы менеджмента качества. Основные положения и словарь»

68 ГОСТ Р 22.0.02-2016 «Безопасность в чрезвычайных ситуациях. Термины и определения»

69 ГОСТ Р 22.0.05-94 «Безопасность в чрезвычайных ситуациях. Техногенные чрезвычайные ситуации. Термины и определения»

70 ГОСТ Р 43.2.2-2009 «Информационное обеспечение техники и операторской деятельности. Язык операторской деятельности. Общие положения по применению»

71 ГОСТ Р 50646-2012 «Услуги населению. Термины и определения»

72 ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

73 ГОСТ Р 50779.11-2000 «Статистические методы. Статистическое управление качеством. Термины и определения»

74 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

75 ГОСТ Р 51170-98 «Качество служебной информации. Термины и определения»

76 ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»

77 ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

78 ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»

79 ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения»

80 ГОСТ Р 51904-2002 «Программное обеспечение встроенных систем. Общие требования к разработке и документированию»

81 ГОСТ Р 52292-2004 «Информационная технология. Электронный обмен информацией. Термины и определения»

82 ГОСТ Р 52438-2005 «Географические информационные системы. Термины и определения»

83 ГОСТ Р 52573-2006 «Географическая информация. Метаданные»

84 ГОСТ Р 52591-2006 «Система передачи данных пользователя в цифровом телевизионном формате. Основные параметры»

85 ГОСТ Р 52653-2006 «Информационно-коммуникационные технологии в образовании. Термины и определения»

86 ГОСТ Р 52872-2012 «Интернет-ресурсы. Требования доступности для инвалидов по зрению»

87 ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»

88 ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»

89 ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования»

90 ГОСТ Р 53339-2009 «Данные пространственные базовые. Общие требования»

91 ГОСТ Р 53801-2010 «Связь федеральная. Термины и определения»

92 ГОСТ Р 54097-2010 «Ресурсосбережение. Наилучшие доступные технологии. Методология идентификации»

93 ГОСТ Р 55062-2012 «Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения»

94 ГОСТ Р 56174-2014 «Информационные технологии. Архитектура служб открытой Грид-среды. Термины и определения»

95 ГОСТ Р 56214-2014 «Качество данных. Часть 1. Обзор»

96 ГОСТ Р 56272-2014 «Системы промышленной автоматизации и интеграция. Интеграция данных жизненного цикла перерабатывающих предприятий, включая нефтяные и газовые производственные предприятия. Часть 8. Практические методы интеграции распределенных систем: практическая реализация сетевого языка онтологий (OWL)»

97 ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»

98 ГОСТ Р 56875-2016 «Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий»

99 ГОСТ Р 57100-2016 «Системная и программная инженерия. Описание архитектуры»

100 ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем»

101 ГОСТ Р 57773-2017 «Пространственные данные. Качество данных»

102 ГОСТ Р 7.0.10-2010 «Система стандартов по информации, библиотечному и издательскому делу. Набор элементов метаданных «Дублинское ядро»»

103 ГОСТ Р 7.0.83-2013 «Система стандартов по информации, библиотечному и издательскому делу. Электронные издания. Основные виды и выходные сведения»

104 ГОСТ Р ИСО 10303-1-99 «Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 1. Общие представления и основополагающие принципы»

105 ГОСТ Р ИСО 15188-2012 «Принципы управления проектами стандартизации терминологии»

106 ГОСТ Р ИСО 15489-1-2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования»

107 ГОСТ Р ИСО 15926-2-2010 «Системы промышленной автоматизации и интеграция. Интеграция данных жизненного цикла для перерабатывающих предприятий, включая нефтяные и газовые производственные предприятия. Часть 2. Модель данных»

108 ГОСТ Р ИСО 19439-2008 «Интеграция предприятия. Основа моделирования предприятия»

109 ГОСТ Р ИСО 21500-2014 «Руководство по проектному менеджменту»

110 ГОСТ Р ИСО 23081-1-2008 «Система стандартов по информации, библиотечному и издательскому делу. Процессы управления документами. Метаданные для документов. Часть 1. Принципы

111 ГОСТ Р ИСО 8000-2-2014 «Качество данных. Часть 2. Словарь»

112 ГОСТ Р ИСО 9000-2015 «Системы менеджмента качества. Основные положения и словарь»

113 ГОСТ Р ИСО 9241-110-2009 «Эргономика взаимодействия человек-система. Часть 110. Принципы организации диалога»

114 ГОСТ Р ИСО 9241-210-2012 «Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем»

115 ГОСТ Р ИСО/МЭК 11179-1-2010 «Информационная технология. Регистры метаданных (РМД). Часть 1. Основные положения»

116 ГОСТ Р ИСО/МЭК 11179-3-2012 «Информационная технология. Регистры метаданных (РМД). Часть 3. Метамодель регистра и основные атрибуты»

117 ГОСТ Р ИСО/МЭК 19762-1-2011 «Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь. Часть 1. Общие термины в области АИСД»

118 ГОСТ Р ИСО/МЭК 20000-1-2013 «Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами»

119 ГОСТ Р ИСО/МЭК 2382-23-2004 «Информационная технология. Словарь. Часть 23. Обработка текста»

120 ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

121 ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

122 ГОСТ Р ИСО/МЭК 33001-2017 «Информационные технологии. Оценка процесса. Понятия и терминология»

123 ГОСТ Р ИСО/МЭК 9834-3-2009 «Информационная технология. Взаимосвязь открытых систем. Процедуры действий уполномоченных по регистрации ВОС. Часть 3. Регистрация дуг дерева идентификатора объекта, расположенных ниже дуги, администрируемой совместно ИСО и МСЭ-Т»

124 ГОСТ Р ИСО/МЭК ТО 10032-2007 «Эталонная модель управления данными»

125 ГОСТ Р ИСО/ТС 14048-2009 «Экологический менеджмент. Оценка жизненного цикла. Формат документирования данных»

126 ГОСТ Р ИСО/ТС 18308-2008 «Информатизация здоровья. Требования к архитектуре электронного учета здоровья»

127 ГОСТ Р 55022-2012 «Информационная технология. Спецификация языка описания представления задач (JSDL). Версия 1.0»

128 ГОСТ Р ИСО/МЭК 29361-2012 «Информационная технология. Интероперабельность сетевых услуг. Базовый профиль WS-1. Версия 1.1»

129 Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ // СЗ РФ. 2005. № 1 (Часть I). Ст. 16

130 Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ

131 Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ

132 Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 25.12.2006. № 52 (1 ч.), ст. 5496

133 Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // СЗ РФ. 03.08.1998. № 31, ст. 3824

134 Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. 07.01.2002. № 1 (ч. 1), ст. 1

135 Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 17.06.1996. № 25, ст. 2954

136 Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014)

137 Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. С. 8220-8235

138 Закон Российской Федерации от 27.12.1991 N 2124-1 «О средствах массовой информации»

139 Закон Российской Федерации от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей» // СЗ РФ, 1996. № 3. Ст. 140

140 Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ// СЗ РФ. 2002. № 1 (Часть I). Ст. 1

141 Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»

142 Модельный информационный кодекс для государств - участников СНГ (принят в г. Санкт-Петербурге 23.11.2012 Постановлением 38-6 на 38-м пленарном заседании Межпарламентской Ассамблеи государств - участников СНГ, обладает рекомендательным статусом)

143 Определение Московского городского суда от 26 января 2016 г. № 33а-598/2016

144 Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации». — URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения 51.08.2019)

145 Положение Банка России от 06.08.2015 N 483-П «О порядке расчета величины кредитного риска на основе внутренних рейтингов» (вместе с «Требованиями к качеству данных, используемых банками для создания и применения моделей количественной оценки кредитного риска для целей расчета нормативов достаточности капитала») (Зарегистрировано в Минюсте России 25.09.2015 N 38996)

146 Постановление Конституционного Суда Российской Федерации от 26.10.2017 № 25-П

147 Постановление Правительства Москвы от 14.06.2005 N 439-ПП «О дальнейшем проведении работ по созданию Московского городского портала» (вместе с «Концепцией Системы городских порталов», «Функциональными требованиями к Московскому городскому порталу (МГП) в сети Интернет») (утратил силу)

148 Постановление Правительства Российской Федерации от 01.06.2016 N 487 «О первоочередных мерах, направленных на создание государственной информационной системы «Единая информационная среда в сфере систематизации и кодирования информации» (вместе с «Правилами

создания, изменения, ведения и применения отдельных информационных ресурсов») (утратил силу)

149 Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. 2012. № 45. Ст. 6257

150 Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» // СЗ РФ. 2012. № 7. Ст. 863

151 Постановление Правительства Российской Федерации от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» // СЗ РФ. 2019. № 23. Ст. 2963

152 Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» // СЗ РФ. 2005. № 30 (Часть II). Ст. 3165

153 Постановление Правительства Российской Федерации от 06.07.2015 № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2015. № 28. Ст. 4240

154 Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // СЗ РФ. 2015. № 28. Ст. 4241

155 Постановление Правительства Российской Федерации от 07.06.2019 № 733 «Об общероссийских классификаторах технико-экономической и социальной информации» (вместе с «Правилами разработки, ведения, изменения и применения общероссийских классификаторов технико-экономической и социальной информации»)

156 Постановление Правительства Российской Федерации от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» // СЗ РФ. 2010. № 38. Ст. 4823

157 Постановление Правительства Российской Федерации от 09.10.2014 № 1037 «О внесении изменения в Положение о единой системе межведомственного электронного взаимодействия»

158 Постановление Правительства Российской Федерации от 10.07.2013 № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // СЗ РФ. 2013. № 30 (Часть II). Ст. 4108

159 Постановление Правительства Российской Федерации от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе» // СЗ РФ. 2012. № 25. Ст. 3380

160 Постановление Правительства Российской Федерации от 14.09.2012 N 928 «О базовых государственных информационных ресурсах» (вместе с «Требованиями к порядку формирования, актуализации и использования базовых государственных информационных ресурсов», «Правилами формирования, актуализации и использования реестра базовых государственных информационных ресурсов») (утратил силу)

161 Постановление Правительства Российской Федерации от 14.11.2015 № 1235 «О федеральной государственной информационной системе координации информатизации» // СЗ РФ. № 47. Ст. 6599

162 Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

163 Постановление Правительства Российской Федерации от 24.10.2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» // СЗ РФ. 2011. № 44. Ст. 6274

164 Постановление Правительства Российской Федерации от 25.12.2014 № 1494 «Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия» // СЗ РФ. 2015. № 1 (Часть II). Ст. 284

165 Постановление Правительства Российской Федерации от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления

государственных и муниципальных услуг в электронной форме» // СЗ РФ. 2011. № 49 (Часть IV). Ст. 7284

166 Постановление Правительства Российской Федерации от 29.12.2008 № 1057 «Об утверждении Положения о межведомственной интегрированной автоматизированной информационной системе федеральных органов исполнительной власти, осуществляющих контроль в пунктах пропуска через государственную границу Российской Федерации»

167 Постановление Правительства Российской Федерации от 30.01.2016 № 48 «О федеральной государственной информационной системе «Единый фонд геологической информации о недрах» // СЗ РФ. 2016. № 6. Ст. 844

168 Постановление Правительства Российской Федерации от 10.07.2013 № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных»// СЗ РФ. 29.07.2013. № 30 (часть II), ст. 4107

169 Постановление Правительства Российской Федерации от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» // СЗ РФ. 30.11.2009. № 48, ст. 5832

170 Постановление Правительства Российской Федерации от 26.10.2019 № 1377 «Об утверждении Регламента информационного взаимодействия федерального фонда данных дистанционного зондирования Земли из космоса и федерального фонда пространственных данных» // СЗ РФ. 04.11.2019. № 44, ст. 6211

171 Постановление Правительства Российской Федерации от 15.06.2009 № 477 «Об утверждении Правил делопроизводства в федеральных органах исполнительной власти» // СЗ РФ. 22.06.2009. № 25, ст. 3060

172 Постановление Правительства Российской Федерации от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // СЗ РФ. 09.06.2008. № 23, ст. 2708

173 Постановление Правительства Российской Федерации от 24.10.2011 № 860 «Об утверждении Правил взимания платы за предоставление информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 31.10.2011. № 44, ст. 6273

174 Постановление Правительства Российской Федерации от 17.08.2016 № 806 «О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 29.08.2016. № 35, ст. 5326

175 Постановление Правительства Российской Федерации от 08.06.2011 № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» // СЗ РФ. 13.06.2011. № 24, ст. 3503

176 Постановление Правительства Российской Федерации от 22.12.2012 № 1382 «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» // СЗ РФ. 31.12.2012. № 53 (ч. 2), ст. 7938

177 ПР 50.1.024-2005 «Основные положения и порядок проведения работ по разработке, ведению и применению общероссийских классификаторов»

178 Приказ Минкомсвязи России от 19.01.2015 N 7 «Об утверждении Положения о федеральной государственной информационной системе

«Единая система нормативной справочной информации», а также Перечня нормативной справочной информации, подлежащей размещению в федеральной государственной информационной системе «Единая система нормативной справочной информации» (Зарегистрировано в Минюсте России 20.05.2015 N 37343)

179 Приказ Минэкономразвития России № 412, МВД России № 645, Министра обороны Российской Федерации № 1183, Минюста России № 216, МЧС России № 422, Минздравсоцразвития России № 782н, Минкомсвязи России № 120, ФСБ России № 425, ФСКН России № 370, ФТС России № 1638, ФМС России № 264, ФНС России № ММВ-7-6/437а от 03.09.2010 «О функционировании государственной информационной системы «Правоохранительный портал Российской Федерации». — URL: http://legalacts.ru/doc/prikaz-minekonomrazvitija-rf-n-412-mvd-rf (дата обращения 51.08.2019)

180 Приказ Минэкономразвития России от 05.06.2018 № 286 «Об утверждении формата предоставления сведений годовой бухгалтерской (финансовой) отчетности юридических лиц Федеральной службой государственной статистики в рамках межведомственного информационного взаимодействия» // Официальный интернет-портал правовой информации. — URL: http://www.pravo.gov.ru. 2018 rf (дата обращения 51.08.2019)

181 Приказ Минкомсвязи России от 30.12.2016 № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий» // СПС «КонсультантПлюс»

182 Приказ Минкомсвязи России от 31.05.2013 № 127 «Об утверждении методических указаний по осуществлению учета

информационных систем и компонентов информационно-телекоммуникационной инфраструктуры» // «Российская газета». № 255, 13.11.2013

183 Приказ Минэнерго России от 03.08.2015 № 536 «Об утверждении требований к технологиям информационного взаимодействия в интеграционном сегменте государственной информационной системы топливно-энергетического комплекса, в том числе к форматам представления информации в рамках данного сегмента государственной информационной системы топливно-энергетического комплекса» // Официальный интернет-портал правовой информации. — URL: http://www.pravo.gov.ru. 2015 (дата обращения 51.08.2019)

184 Приказ Росстата от 07.07.2011 № 313 «Об утверждении Унифицированного формата транспортного сообщения при обмене электронными документами между территориальными органами Росстата и респондентами». — URL: http://gks.ru (дата обращения 51.08.2019)

185 Приказ Росстата от 17.04.2018 № 179 «Об утверждении порядка сбора сведений о населении в электронной форме, определяющего требования к программному обеспечению, техническим средствам, включая носители информации, каналам связи, средствам защиты и форматам представления данных в электронной форме» // Официальный интернет-портал правовой информации. — URL: http://www.pravo.gov.ru. 2018 (дата обращения 51.08.2019)

186 Приказ ФСБ России от 13.11.1999 № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2000. № 3

187 Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах» // Российская газета. 2013. № 136

188 Проект ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»

189 Р 50.1.028-2001 «Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования»

190 Р 50.1.031-2001 «Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Часть 1. Стадии жизненного цикла продукции»

191 Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»

192 Распоряжение ОАО «РЖД» от 24 марта 2017 г. № 543р. http://www.consultant.ru/document/cons_doc_LAW_218604

193 Распоряжение Правительства Российской Федерации от 10.07.2013 № 1187-р «О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных» // СЗ РФ. 2013. № 30, ст. 4128

194 Распоряжение Правительства РФ от 25.12.2013 № 2516-р «Об утверждении Концепции развития механизмов предоставления государственных и муниципальных услуг в электронном виде» // СЗ РФ. 13.01.2014. № 2 (часть II), ст. 155

195 Распоряжение Правительства Российской Федерации от 02.10.2009 № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти»

196 Распоряжение Правительства Российской Федерации от 03.06.2019 № 1189-р «Об утверждении Концепции создания и

функционирования национальной системы управления данными и плана мероприятий дорожную карту») по созданию национальной системы управления данными на 2019 - 2021 годы» // СЗ РФ. 2019. № 23. Ст. 3041

197 Распоряжение Правительства Российской Федерации от 23.01.2015 № 96-р «О перечне сведений, предусмотренных частью 8 статьи 71 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. 2015. № 5. Ст. 865

198 Распоряжение Правительства Российской Федерации от 28.08.2019 № 1911-р «Об утверждении Концепции создания государственной единой облачной платформы»

199 Распоряжение Правительства Российской Федерации от 28.12.2018 N 2963-р «Об утверждении Концепции создания и функционирования в Российской Федерации системы маркировки товаров средствами идентификации и прослеживаемости движения товаров»

200 Распоряжение Правительства Российской Федерации от 29.06.2012 № 1123-р «О перечне сведений, находящихся в распоряжении государственных органов субъектов РФ, органов местного самоуправления, территориальных государственных внебюджетных фондов» // СЗ РФ. 2012. № 28. Ст. 3924

201 Решение Высшего Евразийского экономического совета от 11.10.2017 N 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года»

202 Решение Коллегии Евразийской экономической комиссии от 09.06.2015 N 63 «О Методике анализа, оптимизации, гармонизации и описания общих процессов в рамках Евразийского экономического союза»

203 Решение Коллегии Евразийской экономической комиссии от 26.12.2017 N 190 «Об утверждении Положения о модели данных Евразийского экономического союза»

204 Руководящий документ ФСТЭК России «Защита от НСД. Термины и определения»

205 СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения»

206 Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954

207 Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074

208 Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СЗ РФ. 2018. № 20. Ст. 2817

209 Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»

210 Указ Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // СЗ РФ. 2015. № 21. Ст. 3092

211 Федеральный закон от 03.12.2011 № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса» // СЗ РФ. 2011. № 49 (Часть IV). Ст. 7060

212 Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // СЗ РФ. 2013. № 14. Ст. 1652

213 Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

214 Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете» // СЗ РФ. 2011. № 50. Ст. 7344

215 Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. Ст. 2895

216 Федеральный закон от 08.11.2007 № 257-ФЗ «Об автомобильных дорогах и о дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2007. № 46. Ст. 5553

217 Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009. № 7. Ст. 776

218 Федеральный закон от 09.07.1999 № 160-ФЗ «Об иностранных инвестициях в Российской Федерации» // СЗ РФ. 1999. № 28. Ст. 3493

219 Федеральный закон от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости» // СЗ РФ. 2015. № 29 (Часть I). Ст. 4344

220 Федеральный закон от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2015. № 29 (Часть I). Ст. 4350

221 Федеральный закон от 14.03.2009 № 31-ФЗ «О государственной регистрации прав на воздушные суда и сделок с ними» // СЗ РФ. 2009. № 11. Ст. 1260

222 Федеральный закон от 15.07.1995 № 101-ФЗ «О международных договорах Российской Федерации»

223 Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» (утратил силу)

224 Федеральный закон от 21.07.2005 № 115-ФЗ «О концессионных соглашениях» // СЗ РФ. 2005. № 30 (Часть II). Ст. 3126

225 Федеральный закон от 21.07.2014 № 209-ФЗ «О государственной информационной системе жилищно-коммунального хозяйства» // СЗ РФ. 2014. № 30 (Часть I). Ст. 4210

226 Федеральный закон от 21.11.2011 № 325-ФЗ «Об организованных торгах» // СЗ РФ. 2011. № 48. Ст. 6726

227 Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг» // СЗ РФ. 1996. № 17. Ст. 1918

228 Федеральный закон от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» // СЗ РФ. 2003. № 21. Ст. 1957

229 Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СЗ РФ. 2008. № 52 (Часть I). Ст. 6217

230 Федеральный закон от 23.11.2009 № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2009. № 48. Ст. 5711

231 Федеральный закон от 26.06.2008 № 102-ФЗ «Об обеспечении единства измерений»

232 Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции» // СЗ РФ. № 31 (Часть I). Ст. 3434

233 Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

234 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Часть I). Ст. 212

235 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (Часть I). Ст. 3451

236 Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. 2010. № 31. Ст. 4179

237 Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // СЗ РФ. 2002. № 52 (Часть I). Ст. 5140

238 Федеральный закон от 28.12.2013 № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный

закон «Об общих принципах организации местного самоуправления в Российской Федерации» // Официальный интернет-портал правовой информации. — URL: http://www.pravo.gov.ru. 2013 (дата обращения 51.08.2019)

239 Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации»

240 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283

241 Федеральный закон от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»

242 Федеральный закон от 30.12.2015 № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2016. № 1. Ст. 51

243 Федеральный закон от 31.12.2014 № 488-ФЗ «О промышленной политике в Российской Федерации» // СЗ РФ. 2015. № 1 (Часть I). Ст. 41

244 Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // СЗ РФ. 25.03.2019. № 12, ст. 1224

245 Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» // СЗ РФ. 25.10.2004. № 43, ст. 4169

246 Федеральный закон от 28.12.2009 № 381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации» // СЗ РФ. 04.01.2010. № 1, ст. 2

247 Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СЗ РФ. 05.02.1996. № 6, ст. 492

248 Функциональные и технические требования к Федеральной государственной системе «Единая информационная платформа Национальной системы управления данными»

249 Цифровые платформы. Подходы к определению и типизации // Цифровая экономика. — URL: https://files.data-economy.ru/digital_platforms.pdf (дата обращения 51.08.2019)

250 Типовые условия использования общедоступной информации, размещаемой в информационно-телекоммуникационной сети «Интернет» в форме открытых данных (утв. протоколом заочного голосования Правительственной комиссии по координации деятельности открытого правительства от 19.09.2016 № 6) // СПС «КонсультантПлюс»

251 Постановление Правительства Саратовской области от 14.07.2007 № 227-Пр «О согласовании проектов технических заданий для осуществления закупок товаров, работ, услуг для обеспечения государственных нужд Саратовской области по вопросам, связанным с созданием, приобретением и развитием информационных систем органов исполнительной власти области и подведомственных им учреждений» // «Саратовская областная газета», официальное приложение. № 52, 22.06.2007

Источники в разрезе Европейского Союза:

252 Commission Delegated Regulation (EU) 2018/815 of 17 December 2018 supplementing Directive 2004/109/EC of the European Parliament and of the Council with regard to regulatory technical standards on the specification of a single electronic reporting format. — URL: http://data.europa.eu/eli/reg_del/2019/815/oj (дата обращения: 02.08.2019)

253 Commission notice — Guidelines on recommended standard licences, datasets and charging for the reuse of documents № 2014/C 240/01, 24.07.2014. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2014.240.01.0001.01.ENG (дата обращения: 02.08.2019)

254 Commission Regulation (EC) No 1205/2008 of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata (Text with EEA relevance) . — URL: http://data.europa.eu/eli/reg/2008/1205/oj (дата обращения: 02.08.2019)

255 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Open data an engine for innovation, growth and transparent governance. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011DC0882 (дата обращения 10.08.2019)

256 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, Brussels, 25.5.2016, COM(2016) 288 final. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1466514160026&uri=CELEX:52016DC0288 (дата обращения: 02.08.2019)

257 Consolidated version of the Treaty on the Functioning of the European Union - PART THREE: UNION POLICIES AND INTERNAL ACTIONS - TITLE VIII: ECONOMIC AND MONETARY POLICY - Chapter 1: Economic policy - Article 126 (ex Article 104 TEC) . — URL: http://data.europa.eu/eli/treaty/tfeu_2008/art_126/oj (дата обращения: 02.08.2019)

258 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32003R0001 (дата обращения: 02.08.2019)

259 Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) . — URL: http://data.europa.eu/eli/reg/2004/139/oj (дата обращения: 02.08.2019)

260 CRISTINA DOS SANTOS & ELEONORA BASSI; CÉCILE DE TERWAGNE, MANUEL FERNÁDEZ SALMERÓN, POLONA TEPINA, BART VAN DER SLOOT. LAPSI POLICY RECOMMENDATION N. 4 PRIVACY AND PERSONAL DATA PROTECTION. — URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8366 (дата обращения: 02.08.2019)

261 Definition of Annex Themes and Scope (D 2.3, Version 3.0), 2008. — URL: https://inspire.ec.europa.eu/documents/definition-annex-themes-and-scope-d-23-version-30 (дата обращения: 02.08.2019)

262 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. — URL: http://data.europa.eu/eli/dir/2016/1148/oj (дата обращения 10.08.2019)

263 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943 (дата обращения: 05.08.2019)

264 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. — URL: http://data.europa.eu/eli/dir/2019/1024/oj (дата обращения 10.08.2019)

265 Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003L0004 (дата обращения: 05.08.2019)

266 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. — URL:

https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003L0098 (дата обращения: 05.08.2019)

267 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. — URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32003L0098 (дата обращения: 14.08.2019)

268 Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC. — URL: http://data.europa.eu/eli/dir/2004/109/oj (дата обращения: 02.08.2019)

269 Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE). — URL: http://data.europa.eu/eli/dir/2007/2/oj (дата обращения 10.08.2019)

270 Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information. — URL: https://eur-lex.europa.eu/eli/dir/2013/37/oj (дата обращения 10.08.2019)

271 Elements of a data value chain strategy, Last update: 8 November 2013. — URL: https://ec.europa.eu/digital-single-market/en/news/elements-data-value-chain-strategy (дата обращения: 02.08.2019)

272 ESEF Reporting Manual. Preparation of Annual Financial Reports in Inline XBRL. — URL: https://www.esma.europa.eu/sites/default/files/library/esma32-60-254_esef_reporting_manual.pdf (дата обращения: 02.08.2019)

273 European Commission. Commission notice — Guidelines on recommended standard licences, datasets and charging for the reuse of documents. — URL: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=uriserv:OJ.C_.2014.240.01.0001.01.ENG (дата обращения 10.08.2019)

274 European Commission. D 3.3 Quarterly Stories (Story 3). Update of the European Data Market SMART 2016/0063. — URL: http://datalandscape.eu/sites/default/files/report/D3.3_Data_Monetization_10.10.2018_GM.PDF (дата обращения: 02.08.2019)

275 European Commission. D2.6 Second Interim Report. THE EUROPEAN DATA MARKET MONITORING TOOL: KEY FACTS & FIGURES, FIRST POLICY CONCLUSIONS, DATA LANDSCAPE AND QUANTIFIED STORIES. — URL: http://datalandscape.eu/sites/default/files/report/D2.6_EDM_Second_Interim_Report_28.06.2019.pdf (дата обращения: 02.08.2019)

276 European Commission. Digital Economy and Society Index 2018 Report. — URL: https://digital-agenda-data.eu/charts/desi-composite#chart={%22indicator%22:%22desi_sliders%22,%22breakdown%22:{%22desi_1_conn%22:5,%22desi_2_hc%22:5,%22desi_3_ui%22:3,%22desi_4_idt%22:4,%22desi_5_dps%22:3},%22unit-measure%22:%22pc_desi_sliders%22,%22time-period%22:%222018%22} (дата обращения 01.08.2019)

277 European Commission. Document L:2017:239:TOC. — URL: https://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=3&year=2017&number=6100&version=ALL (дата обращения: 02.08.2019)

278 European Commission. Impact Assessment on the review of the Directive 2003/98/EC on the reuse of public sector information. — URL: https://ec.europa.eu/digital-single-market/en/news/impact-assessment-review-directive-200398ec-reuse-public-sector-information (дата обращения: 02.08.2019)

279 European commission. Regulations, Directives and other acts. — URL: https://europa.eu/european-union/eu-law/legal-acts_en (дата обращения 10.08.2019)

280 European Commission. Staff Working Document - Guidance on sharing private sector data in the European data economy. — URL: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy (дата обращения: 02.08.2019)

281 European Commission. Synopsis report of the public consultation on the revision of the Directive on the reuse of public sector information. 25th April, 2018. — URL: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-revision-directive-reuse-public-sector-information (дата обращения 10.08.2019)

282 European Commission. The European Data Flow Monitoring Initiative. — URL: https://ec.europa.eu/digital-single-market/en/european-data-flow-monitoring-initiative (дата обращения: 02.08.2019)

283 EUROPOL INFORMATION SYSTEM. — URL: https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system (дата обращения: 02.08.2019)

284 Impact Assessment on the review of the Directive 2003/98/EC on the reuse of public sector information. — URL: https://ec.europa.eu/digital-single-market/en/news/impact-assessment-review-directive-200398ec-reuse-public-sector-information (дата обращения: 02.08.2019)

285 INSPIRE Generic Conceptual Model, Version 3.4, 2014. — URL: https://inspire.ec.europa.eu/documents/inspire-generic-conceptual-model (дата обращения: 02.08.2019)

286 MARCO RICOLFI. AND JOSEF DREXL, MIREILLE VAN EECHOUD, KATLEEN JANSSEN, MARIA TERESA MAGGIOLINO, FEDERICO MORANDO, CRISTIANA SAPPA, PAUL TORREMANS, PAUL UHLIR (AND RAIMONDO IEMMA – EVPSI AND MARC DE VRIES). LAPSI POSITION PAPER NO 1: THE «PRINCIPLES GOVERNING CHARGING» FOR RE-USE OF PUBLIC SECTOR INFORMATION. — URL:

http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8342 (дата обращения: 02.08.2019)

287 MARCO RICOLFI. LAPSI CONCEPTUAL FRAMEWORK NO 1 CHARGING POLICY: A CONCEPTUAL FRAMEWORK FOR EU GUIDANCE TO THE MEMBER STATES — URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8345 (дата обращения: 02.08.2019)

288 MARIATERESA MAGGIOLINO, JOSEF DREXL, KATLEEN JANSSEN. LAPSI POLICY RECOMMENDATION N. 1 THE COMPETITION LAW ISSUES OF THE RE-USE OF PUBLIC SECTOR INFORMATION (PSI) — URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=8349 (дата обращения: 02.08.2019)

289 Methodology for the development of data specifications: baseline version (D 2.6, Version 3.0), 2008. — URL: https://inspire.ec.europa.eu/documents/methodology-development-data-specifications-baseline-version-d-26-version-30 (дата обращения: 02.08.2019)

290 Open Data Monitor. — URL: https://opendatamonitor.eu (дата обращения 25.08.2019)

291 Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009R0223 (дата обращения 25.08.2019)

292 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: https://gdpr-info.eu/ (дата обращения 10.08.2019)

293 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. — URL: http://data.europa.eu/eli/reg/2016/794/oj (дата обращения: 02.08.2019)

294 Regulation (EU) 2017/1951 of the European Parliament and of the Council of 25 October 2017 amending Regulation (EU) No 99/2013 on the European statistical programme 2013-17, by extending it to 2020. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.284.01.0001.01.ENG (дата обращения 25.08.2019)

295 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725 (дата обращения 10.08.2019)

296 Regulation (EU) No 99/2013 of the European Parliament and of the Council of 15 January 2013 on the European statistical programme 2013-17. — URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1409068106403&uri=CELEX:32013R0099 (дата обращения 25.08.2019)

297 TARGET consolidation: what is it? . — URL: https://www.ecb.europa.eu/paym/target/consolidation/html/index.en.html (дата обращения: 02.08.2019)

298 Technical Guidance for the implementation of INSPIRE Download Services, 2013. — URL: https://inspire.ec.europa.eu/documents/technical-

guidance-implementation-inspire-download-services (дата обращения: 02.08.2019)

299 Technical Guidelines. — URL: https://inspire.ec.europa.eu/Technical-guidelines3 (дата обращения: 02.08.2019)

300 What is TARGET Instant Payment Settlement (TIPS)? . — URL: https://www.ecb.europa.eu/paym/target/tips/html/index.en.html (дата обращения: 02.08.2019)

301 What is TARGET2? . — URL: https://www.ecb.europa.eu/paym/target/target2/html/index.en.html (дата обращения: 02.08.2019)

302 Отчет Еврокомиссии об инструментах мониторинга рынка данных SMART 2016/0063 от 28.06.2019. — URL: http://datalandscape.eu/sites/default/files/report/D2.6_EDM_Second_Interim_Report_28.06.2019.pdf (дата обращения: 02.08.2019)

Источники в разрезе Германии:

303 Akteneinsichts- und Informationszugangsgesetz (AIG). — URL: http://bravors.brandenburg.de/gesetze/aig (дата обращения: 02.08.2019)

304 Andre Meister. Anna Biselli. IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll. — URL: https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 (дата обращения: 02.08.2019)

305 Bayerisches Datenschutzgesetz (BayDSG). — URL: https://www.gesetze-bayern.de/(X(1)S(nzjymmxxpbdihomdbanqlx0f))/Content/Document/BayDSG/true?AspxAutoDetectCookieSupport=1 (дата обращения: 02.08.2019)

306 Bundesamt für Sicherheit in der Informationstechnik. Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen. — URL:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=6 (дата обращения: 02.08.2019)

307 Bundesdatenschutzgesetz. — URL: https://www.gesetze-im-internet.de/bdsg_2018/index.html (дата обращения 17.08.2019)

308 Cyber-Sicherheitsstragie für Deutschland. — URL: http://www.bmi.bund.de/cybersicherheitsstrategie/ (дата обращения: 02.08.2019)

309 Das Datenportal für Deutschland. — URL: https://www.govdata.de/ (дата обращения: 15.08.2019)

310 Das Digitalisierungsprogramm des IT-Planungsrates. — URL: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/21_Sitzung/18_Anlage1_Digitalisierungsprogramm.html?nn=9693774 (дата обращения: 02.08.2019)

311 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. — URL: https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 (дата обращения 20.08.2019)

312 Federal Data Protection Act (BDSG). — URL: https://www.gesetze-im-internet.de/englisch_bdsg/ (дата обращения: 02.08.2019)

313 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG). — URL: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (дата обращения: 02.08.2019)

314 Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik. — URL: http://www.gesetze-im-internet.de/stug/ (дата обращения: 02.08.2019)

315 Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen. — URL: https://www.gesetze-im-internet.de/iwg/ (дата обращения: 10.08.2019)

316 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). — URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1565384375246 (дата обращения: 02.08.2019)

317 Gesetz zur Förderung der elektronischen Verwaltung. — URL: http://www.gesetze-im-internet.de/egovg/ (дата обращения 14.08.2019)

318 Gesetz zur Regelung des Zugangs zu Informationen des Bundes. — URL: http://www.gesetze-im-internet.de/ifg/ (дата обращения 11.08.2019)

319 Hamburgisches Datenschutzgesetz (HmbDSG). — URL: http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&st=lr&doc.id=jlr-DSGHA2018rahmen (дата обращения: 02.08.2019)

320 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG). — URL: http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?xid=8074311,1 (дата обращения: 02.08.2019)

321 IT-Staatsvertrag über die Errichtung des IT-Planungsrats. — URL: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/ITPlanungsrat/Staatsvertrag/Staatsvertrag.html?nn=6839036 (дата обращения: 02.08.2019)

322 Kooperationsgruppe «Informationssicherheit des IT-PLR». Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung. — Stand 19.02.2013. — URL: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.pdf?__blob=publicationFile&v=2 (дата обращения: 02.08.2019)

323 Nationale E-Government-Strategie. — URL: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/NEGS/NEGS_Fortschreibung.html?nn=6839038 (дата обращения 13.08.2019)

324 Projekt Zukunft. — URL: https://projektzukunft.berlin.de/ (дата обращения 17.08.2019)

325 SITZUNG DES IT-PLANUNGSRATS VOM 5. OKTOBER 2017. ENTSCHEIDUNG 2017/39. STANDARD FÜR DEN AUSTAUSCH VON AKTEN, VORGÄNGEN UND DOKUMENTEN. — URL: https://www.it-planungsrat.de/SharedDocs/Entscheidungen/DE/2017/Entscheidung_2017_39.html?nn=10144556 (дата обращения 11.08.2019)

326 Standardisierungsagenda. — URL: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.pdf?__blob=publicationFile&v=2 (дата обращения 14.08.2019)

327 STANDARDISIERUNGSAGENDA. — URL: http://www.xoev.de/sixcms/media.php/13/Standardisierungsagenda.pdf (дата обращения: 02.08.2019)

328 Standards des IT-Planungsrats. — URL: https://www.it-planungsrat.de/DE/Standards/Standards_node.html (дата обращения: 02.08.2019)

329 Telekommunikationsgesetz. — URL: https://www.gesetze-im-internet.de/tkg_2004/index.html (дата обращения: 10.08.2019)

330 Telemediengesetz. — URL: https://www.gesetze-im-internet.de/tmg/ (дата обращения: 02.08.2019)

331 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz. — URL: https://www.gesetze-im-internet.de/bsi-kritisv/ (дата обращения: 02.08.2019)

332 Verordnung zur Übermittlung von Meldedaten in Berlin (MeldDÜV BE). — URL: http://gesetze.berlin.de/jportal/?quelle=jlink&query=MeldD%C3%9CV+BE+%C2%A7+8&psml=bsbeprod.psml&max=true (дата обращения: 17.08.2019)

333 Источники в разрезе Франции:

334 ACTION PUBLIQUE 2022 : UN PROGRAMME POUR ACCÉLÉRER LA TRANSFORMATION DU SERVICE PUBLIC. — URL: https://www.modernisation.gouv.fr/action-publique-2022/comprendre/action-publique-2022-un-programme-pour-accelerer-la-transformation-du-service-public (дата обращения 10.08.2019)

335 Arrêté du 17 décembre 2012 portant création d'un service à compétence nationale dénommé «Réseau interministériel de l'Etat». — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026792328&categorieLien=id (дата обращения 10.08.2019)

336 Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité. — URL: https://www.legifrance.gouv.fr/eli/arrete/2016/4/20/PRMJ1526716A/jo/texte (дата обращения 10.08.2019)

337 Cadre stratégique SI Etat, 2013. — URL: https://references.modernisation.gouv.fr/sites/default/files/03%20-%20Cadre%20strat%C3%A9gique%20SI%20Etat%20-%20version%201.0%20F%C3%A9vrier%202013.pdf (дата обращения 10.08.2019)

338 CGefI, Rapport d’activité, 2018. — URL: https://www.economie.gouv.fr/files/2018-Rapport-d-activite-CGefi_0.pdf (дата обращения 10.08.2019)

339 CGU du service FranceConnect pour les Utilisateurs. — URL: https://franceconnect.gouv.fr/cgu (дата обращения 10.08.2019)

340 Code de la consommation. — URL: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=9D9EE6F8EC8E205D245C1AB7970BF19C.tplgfr30s_2?cidTexte=LEGITEXT000006069565&dateTexte=20170223 (дата обращения 10.08.2019)

341 Code de la route. — URL: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=72937776B1BC54575C2A628ED8BF4EB1.tplgfr25s_3?idSectionTA=LEGISCTA000006143842&cidText

e=LEGITEXT000006074228&dateTexte=20190903 (дата обращения 10.08.2019)

342 Code des relations entre le public et l'administration - Article D323-2-2. — URL: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000034504993&cidTexte=LEGITEXT000031366350&dateTexte=29991231 (дата обращения 10.08.2019)

343 Code des relations entre le public et l'administration. — URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000031366350 (дата обращения 10.08.2019)

344 Code général des impôts. — URL: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000037526190&cidTexte=LEGITEXT000006069577&dateTexte=20181231 (дата обращения 10.08.2019)

345 Conditions d’utilisation. — URL: https://www.data.gouv.fr/fr/terms/ (дата обращения 10.08.2019)

346 Conformant Licenses. — URL: http://opendefinition.org/licenses/ (дата обращения 10.08.2019)

347 Conseil d'État. 10ème - 9ème chambres réunies. N° 389806. ECLI:FR:CECHR:2017:389806.20170208. lecture du mercredi 8 février 2017. [Source numérique] . — URL: https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000034017890&fastReqId=453311552&fastPos=1 (date d’accès – 12.05.2019)

348 Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information». — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212 (дата обращения 10.08.2019)

349 Décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'Etat. — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029337021 (дата обращения 10.08.2019)

350 Décret n° 2015-1165 du 21 septembre 2015 relatif à la direction interministérielle de la transformation publique et à la direction interministérielle du numérique et du système d'information et de communication de l'Etat. — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031194412&categorieLien=cid (дата обращения 10.08.2019)

351 Décret n° 2016-1617 du 29 novembre 2016 relatif aux catégories d'informations publiques de l'Etat et de ses établissements publics administratifs susceptibles d'être soumises au paiement d'une redevance de réutilisation. — URL: https://www.legifrance.gouv.fr/eli/decret/2016/11/29/PRMJ1630605D/jo/texte (дата обращения 10.08.2019)

352 Décret n° 2017-1434 du 29 septembre 2017 relatif aux obligations d'information des opérateurs de plateformes numériques. — URL: . — URL: https://www.legifrance.gouv.fr/eli/decret/2017/9/29/ECOC1716647D/jo/texte (дата обращения 10.08.2019)

353 Décret n° 2017-1435 du 29 septembre 2017 relatif à la fixation d'un seuil de connexions à partir duquel les opérateurs de plateformes en ligne élaborent et diffusent des bonnes pratiques pour renforcer la loyauté, la clarté et la transparence des informations transmises aux consommateurs. — URL: https://www.legifrance.gouv.fr/eli/decret/2017/9/29/ECOC1716648D/jo/texte (дата обращения 10.08.2019)

354 Décret n° 2017-1584 du 20 novembre 2017 relatif à la direction interministérielle de la transformation publique et à la direction interministérielle du numérique et du système d'information et de communication de l'Etat. — URL: https://www.legifrance.gouv.fr/eli/decret/2017/11/20/PRMX1732385D/jo/texte (дата обращения 10.08.2019)

355 Décret n° 2017-331 du 14 mars 2017 relatif au service public de mise à disposition des données de référence. — URL: https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=C49A75316B5545B2041F83902D900816.tplgfr34s_2?cidTexte=JORFTEXT000034194946&idArticle=LEGIARTI000034195955&dateTexte=20170316 (дата обращения 10.08.2019)

356 Décret n°55-733 du 26 mai 1955 relatif au contrôle économique et financier de l'Etat. — URL: . — URL: https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4F994518EBDD70B55684DB74A2EB10D7.tpdjo02v_2?cidTexte=LEGITEXT000006060746&dateTexte=20120727 (дата обращения 10.08.2019)

357 Décret no 2011-775 du 28 juin 2011 relatif à l'audit interne dans l'administration. — URL: https://www.legifrance.gouv.fr/jo_pdf.do?numJO=0&dateJO=20110630&numTexte=50&pageDebut=&pageFin (дата обращения 10.08.2019)

358 France Issues New Rules for the Accreditation of Health Data Hosting Services Providers. — URL: https://www.natlawreview.com/article/france-issues-new-rules-accreditation-health-data-hosting-services-providers (дата обращения 10.08.2019)

359 Gazier A., Les personnes morales de droit public (les personnes publiques) // Fiche de niveau 2. Institutions administratives, 29 décembre 2007. — URL: http://france-jus.ru/les-personnes-morales-de-droit-public-les-personnespubliques/ (дата доступа – 19.09.2019)

360 L'ensemble des textes de référence fondant l'institution, ses missions et services, depuis sa création en janvier 2010. — URL: https://www.dila.premier-ministre.gouv.fr/institution/presentation/textes-fondateurs (дата обращения 10.08.2019)

361 La circulaire du Premier ministre du 30 juin 2011 sur la mise en oeuvre de l'audit interne dans l'administration. — URL:

https://www2.economie.gouv.fr/files/CirculairePM-30-06-2011_0.pdf (дата обращения 10.08.2019)

362 La DINSIC. — URL: https://www.numerique.gouv.fr/dinsic/ (дата обращения 10.08.2019)

363 La réutilisation des données du système d'immatriculation des véhicules. — URL: https://www.interieur.gouv.fr/Repertoire-des-informations-publiques/La-reutilisation-des-donnees-du-systeme-d-immatriculation-des-vehicules (дата обращения 10.08.2019)

364 LA SOUS-DIRECTION OPÉRATIONS (SDO) . — URL: https://www.ssi.gouv.fr/agence/organisation/les-sous-directions/centre-operationnel-de-la-securite-des-systemes-dinformation-cossi/ (дата обращения 10.08.2019)

365 Le Conseil Constitutionnel, Décision n° 2012-652 DC du 22 mars 2012 // ORF n°0075 du 28 mars 2012 page 5607, texte n° 6. [Source Electronique]. — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582452 (дата обращения 10.08.2019)

366 Le contrôle des systèmes d’information dans les organismes publics. — URL: https://www.economie.gouv.fr/cgefi/controle-des-systemes-dinformation-dans-organismes-publics (дата обращения 10.08.2019)

367 Licence Ouverte V 2.0. — URL: https://www.etalab.gouv.fr/wp-content/uploads/2017/04/ETALAB-Licence-Ouverte-v2.0.pdf (дата обращения 10.08.2019)

368 Licences de réutilisation. — URL: https://www.data.gouv.fr/fr/licences (дата обращения 10.08.2019)

369 LOI n° 2012-410 du 27 mars 2012 relative à la protection de l'identité // JORF n°0075 du 28 mars 2012 page 5604, texte n° 2.— URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411&dateTexte=20170503 (дата обращения 10.08.2019)

370 LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique. — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id (дата обращения 10.08.2019)

371 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 (дата обращения 10.08.2019)

372 Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics. — URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030920376&categorieLien=id (дата обращения 10.08.2019)

373 Principes de mutualisation du SI de l'Etat. — URL: https://www.numerique.gouv.fr/uploads/201811-CSIC-Fiche_05-principes-mutualisation.pdf (дата обращения 14.08.2019)

374 Projets informatiques de l'Etat : retrouvez l'ensemble des avis conformes émis par la DINSIC. — URL: https://www.numerique.gouv.fr/publications/avis-conformes/ (дата обращения 10.08.2019)

375 Redevances. — URL: https://www.data.gouv.fr/fr/Redevances (дата обращения 10.08.2019)

376 Référentiel Général d'Accessibilité pour les Administrations, RGAA 3 2017. — URL: https://references.modernisation.gouv.fr/sites/default/files/RGAA-3-2017-Referentiel-Technique.pdf (дата обращения 10.08.2019)

377 Référentiel Général d'Interopérabilité V2 version, 2015. — URL: https://references.modernisation.gouv.fr/sites/default/files/Referentiel_General_Interoperabilite_V2.pdf (дата обращения 10.08.2019)

378 RIPMEF - Conditions de réutilisation. — URL: https://www.economie.gouv.fr/cedef/repertoire-des-informations-publiques-des-ministeres-economiques-et-financiers-conditions (дата обращения 10.08.2019)

Источники в разрезе Норвегии:

379 Digital agenda for Norway in brief. ICT for a simpler everyday life and increased productivity. — URL: https://www.regjeringen.no/contentassets/07b212c03fee4d0a94234b101c5b8ef0/en-gb/pdfs/digital_agenda_for_norway_in_brief.pdf (дата обращения 08.08.2019)

380 Digital Agenda for Norway. ICT for Growth and Value Creation. — URL: https://www.regjeringen.no/contentassets/4339bb2154bd4b829f1d147bb2b26da8/en-gb/pdfs/stm201220130023000engpdfs.pdf (дата обращения 08.08.2019)

381 Digital Government Factsheet 2019. Norvey. — URL: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Norway_2019.pdf (дата обращения 08.08.2019)

382 Digitalisation for Development. Digital strategy for Norwegian development policy. — URL: https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/utvpolitikk/digital_strategynew.pdf (дата обращения 08.08.2019)

383 Freedom of Information Act. — URL: https://app.uio.no/ub/ujur/oversatte-lover/data/lov-20060519-016-eng.pdf (дата обращения 08.08.2019)

384 National Cyber Security Strategy for Norway. — URL: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf (дата обращения 08.08.2019)

385 National geospatial strategy towards 2025. — URL: https://www.regjeringen.no/contentassets/6e470654c95d411e8b1925849ec4918d/en-gb/pdfs/en_nasjonal_geodatastrategi.pdf (дата обращения 08.08.2019)

386 Personal Data Act. — URL: http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan033937.pdf (дата обращения 08.08.2019)

387 Public Administration Act. — URL: https://app.uio.no/ub/ujur/oversatte-lover/data/lov-19670210-000-eng.pdf (дата обращения 08.08.2019)

388 Strategy. Norway as a data centre nation. — URL: https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/strategier/strategi-nfd-eng-nett-uu.pdf (дата обращения 08.08.2019)

Источники в разрезе Эстонии:

389 Access to electricity and gas smart meter data in Estonia powered by X-Road technology. — URL: https://x-road.global/access-to-electricity-and-gas-smart-meter-data-in-estonia (дата обращения: 09.09.2019)

390 Accounting Act. — URL: https://www.riigiteataja.ee/en/eli/517012017005/consolide (дата обращения: 21.08.2019)

391 Charte Internet de l'Etat, 2012. — URL: https://references.modernisation.gouv.fr/sites/default/files/Charte_Internet_de_l%27Etat_v1.0.pdf (дата обращения: 09.09.2019)

392 Cybersecurity Act. — URL: https://www.riigiteataja.ee/en/eli/523052018003/consolide (дата обращения 08.08.2019)

393 Digital Agenda 2020 for Estonia. — URL: https://www.mkm.ee/sites/default/files/digitalagenda2020_final_final.pdf (дата обращения 08.08.2019)

394 Digital Government Factsheet 2019. Estonia. — URL: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Estonia_2019.pdf (дата обращения 08.08.2019)

395 eInvoicing in Estonia. — URL: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eInvoicing+in+Estonia (дата обращения: 21.08.2019)

396 Electricity data exchange. — URL: https://elering.ee/en/data-exchange (дата обращения: 09.09.2019)

397 Estonian Centre for Standardisation. — URL: https://www.evs.ee/ (дата обращения: 21.08.2019)

398 Estonian Open Government Data Portal. — URL: https://opendata.riik.ee/en/ (дата обращения: 02.09.2019)

399 European Interoperability Framework. — URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf (дата обращения: 07.08.2019)

400 Interoperability of the State Information System. . — URL: https://www.mkm.ee/sites/default/files/interoperability-framework_2011.doc (дата обращения 08.08.2019)

401 Introducing Marketplace. — URL: https://riigipilv.ee/blog-and-news/introducing-marketplace (дата обращения: 09.09.2019)

402 Licence of open data by Estonian Land Board. — URL: Режим доступа: https://geoportaal.maaamet.ee/eng/Ordering-Data/Open-Data-for-download/Estonian-Topographic-Database-p618.html?plugin_act=litsents (дата обращения: 02.09.2019)

403 Personal Data Protection Act. — URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide (дата обращения 14.08.2019)

404 Principles for Managing Services and Governing Information. — URL: https://www.riigiteataja.ee/en/eli/507072017004/consolide (дата обращения 08.08.2019)

405 Public Information Act. — URL: https://www.riigiteataja.ee/en/eli/514112013001/consolide (дата обращения 08.08.2019)

406 Requirements for the accessibility of websites and mobile applications, and the rules for publishing information describing accessibility. —

URL: https://www.riigiteataja.ee/en/eli/ee/EVIM/reg/512042019003/consolide (дата обращения 14.08.2019)

407 State Infocommunication Foundation. — URL: http://riks.ee/609.html (дата обращения: 09.09.2019)

408 State Secrets and Classified Information of Foreign States Act. — URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042019009/consolide (дата обращения 08.08.2019)

409 Tax Information Exchange Act. — URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/501042019004/consolide (дата обращения 08.08.2019)

410 The Estonian Government Cloud. — URL: https://e-estonia.com/solutions/e-governance/government-cloud/ (дата обращения: 09.09.2019)

411 The requirements for the conversion of the documents preserved in electronic form into electronic databases allowing excess to legible information. — URL: https://www.riigiteataja.ee/en/eli/ee/RHM/reg/524092014007/consolide (дата обращения: 21.08.2019)

Источники в разрезе США:

412 44 U.S. Code § 3542 - Definitions. — URL: https://www.law.cornell.edu/uscode/text/44/3542 (дата обращения 08.08.2019)

413 AB-375 Privacy: personal information: businesses (California Consumer Privacy Act of 2018)

414 Cable Communications Policy Act of 1984. — URL: https://www.congress.gov/bill/98th-congress/senate-bill/66 (дата обращения 08.08.2019)

415 Children's Online Privacy Protection Act of 1998. — URL: https://searchcompliance.techtarget.com/definition/COPPA-Childrens-Online-Privacy-Protection-Act (дата обращения 08.08.2019)

416 CIRCULAR NO. A-130. — URL: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf (дата обращения 08.08.2019)

417 Confidential Information Protection and Statistical Efficiency Act of 2002. — URL: https://www.eia.gov/cipsea/cipsea.pdf (дата обращения 08.08.2019)

418 Cross-Agency Priority (CAP) . — URL: https://www.performance.gov/CAP/leveragingdata/ (дата обращения 08.08.2019)

419 Current Federal Information Processing Standards. — URL: https://www.nist.gov/itl/current-fips (дата обращения 08.08.2019)

420 Driver's Privacy Protection Act of 1994. — URL: https://www.law.cornell.edu/uscode/text/18/2721 (дата обращения 08.08.2019)

421 EDUCATION CODE – EDC (ARTICLE 1. Regional Data-Processing Centers [10500 - 10507])

422 E-Government Act of 2002. — URL: https://www.congress.gov/bill/107th-congress/house-bill/2458) (дата обращения 08.08.2019)

423 Evidence Act of 2018. — URL: https://www.congress.gov/bill/115th-congress/house-bill/4174 (дата обращения 08.08.2019)

424 Fair and Accurate Credit Transactions Act of 2003. — URL: https://www.congress.gov/108/plaws/publ159/PLAW-108publ159.pdf (дата обращения 08.08.2019)

425 Fair Credit Reporting Act. — URL: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (дата обращения 08.08.2019)

426 Family Educational Rights and Privacy Act. — URL: https://uscode.house.gov/view.xhtml?req=(title:20%20section:1232g%20edition:prelim) (дата обращения 08.08.2019)

427 Federal Data Strategy. — URL: https://strategy.data.gov (дата обращения 08.08.2019)

428 Federal Information Security Modernization Act of 2002. — URL: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf (дата обращения 08.08.2019)

429 Federal Policy on Standards. — URL: https://www.nist.gov/standardsgov/what-we-do/federal-policy-standards (дата обращения 08.08.2019)

430 Freedom of Information Act in a form showing all amendments to the statute made by the «FOIA Improvement Act of 2016». — URL: https://www.foia.gov/foia-statute.html (дата обращения 08.08.2019)

431 Freedom of Information Act. — URL: https://www.congress.gov/114/bills/s337/BILLS-114s337enr.xml (дата обращения 08.08.2019)

432 GOVERNMENT CODE – GOV (ARTICLE 1. General Provisions [68500 - 68530])

433 Gramm–Leach–Bliley Act. — URL: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (дата обращения 08.08.2019)

434 HEALTH AND SAFETY CODE – HSC (ARTICLE 1. General Provisions [40400 - 40408], CHAPTER 8.5. Health Care Cost Transparency Database [127671 - 127674])

435 Health Insurance Portability and Accountability Act. — URL: http://counsel.cua.edu/fedlaw/Hipaa.cfm (дата обращения 08.08.2019)

436 Identity Theft and Assumption Deterrence Act. — URL: https://www.congress.gov/bill/105th-congress/house-bill/3601 (дата обращения 08.08.2019)

437 Memorandum on Open Data Policy. Managing Information as an Asset («the Open Data Memorandum», also known as M-13-13). May 9, 2013. — URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf (дата обращения 08.08.2019)

438 Open, Public, Electronic, and Necessary Government Data Act. — URL: https://www.congress.gov/bill/115th-congress/senate-bill/760?q=%7B%22search%22%3A%5B%22Open+Government+Data+Act%22%5D%7D&s=1&r=1 (дата обращения 08.08.2019)

439 PENAL CODE – PEN (CHAPTER 11. Street Terrorism Enforcement and Prevention Act [186.20 - 186.36])

440 Privacy Act of 1974. — URL: https://www.justice.gov/opcl/privacy-act-1974 (дата обращения 08.08.2019)

441 The Data Incubator Project. — URL: https://strategy.data.gov/incubator/ (дата обращения 08.08.2019)

442 United States Senate. FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK. STAFF REPORT. — URL: https://www.hsgac.senate.gov/imo/media/doc/2019-06-25%20PSI%20Staff%20Report%20-%20Federal%20Cybersecurity%20Updated.pdf (дата обращения 08.08.2019)

443 WATER CODE – WAT (CHAPTER 1. General Provisions [12400 - 12402])

Источники в разрезе Великобритании:

444 «Openness by design» Information Commissioner's Office The Information Commissioner's strategic plan 2019/20 – 2021/22. — URL: https://ico.org.uk/media/about-the-ico/documents/2615190/openness_by_-design_strategy_201906.pdf (дата обращения: 05.08.2019)

445 A guide to ICO audits 2018. — URL: https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf (дата обращения: 05.08.2019)

446 Big Brother Watch and others v. The United Kingdom (2018) . — URL: https://hudoc.echr.coe.int/eng#{"itemid":["001-186048"]} (дата обращения: 05.08.2019)

447 BS 10012 - The standard for a personal information management system (PIMS) . — URL: https://www.itgovernance.co.uk/bs10012_pims (дата обращения: 05.08.2019)

448 Catt v. the United Kingdom (2019) . — URL: https://hudoc.echr.coe.int/eng#{"itemid":["001-189424"]} (дата обращения: 05.08.2019)

449 Competition Act 1998. — URL: http://www.legislation.gov.uk/ukpga/1998/41/contents (дата обращения: 05.08.2019)

450 Copyright, Designs and Patents Act 1988. — URL: http://www.legislation.gov.uk/ukpga/1988/48/contents (дата обращения: 05.08.2019); Copyright and Rights in Databases Regulations 1997. URL: http://www.legislation.gov.uk/uksi/1997/3032/contents/made (дата обращения: 05.08.2019)

451 Data Protection Act 2018. — URL: http://www.legislation.gov.uk/ukpga/2018/12/contents (дата обращения: 05.08.2019)

452 Digital Marketplace. — URL: https://www.digitalmarketplace.service.gov.uk (дата обращения: 05.08.2019)

453 DIRECTGOV 2010 and beyond: revolution not evolution. — URL: https://www.gov.uk/government/publications/directgov-2010-and-beyond-revolution-not-evolution-a-report-by-martha-lane-fox (дата обращения: 05.08.2019)

454 FINANCIAL SERVICES AND MARKETS. The Data Reporting Services Regulations 2017. — URL: http://www.legislation.gov.uk/uksi/2017/699/pdfs/uksi_20170699_en.pdf (дата обращения: 05.08.2019)

455 Freedom of Information (Scotland) Act 2002. — URL: http://www.legislation.gov.uk/asp/2002/13/contents (дата обращения: 05.08.2019)

456 Gianclaudio Malgieri, Trade Secrets v Personal Data: a possible solution for balancing rights, International Data Privacy Law, Volume 6, Issue 2, May 2016, Pages 107

457 Government Digital Service. — URL: https://gds.blog.gov.uk (дата обращения: 05.08.2019)

458 Government ICT Strategy - Strategic Implementation Plan 2011. — URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266169/govt-ict-sip.pdf (дата обращения: 05.08.2019)

459 Government ICT Strategy 2011. — URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-government-government-ict-strategy_0.pdf (дата обращения: 05.08.2019)

460 Government Transformation Strategy 2017 to 2020. — URL: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020 (дата обращения: 05.08.2019)

461 Guidance on the implementation of the Re-use of Public Sector Information Regulations 2015 for re-users. — URL: http://www.nationalarchives.gov.uk/documents/information-management/psi-implementation-guidance-re-users.pdf (дата обращения: 05.08.2019)

462 Guidance. Buying and selling on the Digital Marketplace. — URL: https://www.gov.uk/guidance/buying-and-selling-on-the-digital-marketplace (дата обращения: 05.08.2019)

463 Guidance. Cross platform character encoding profile, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/cross-platform-character-encoding-profile (дата обращения: 05.08.2019)

464 Guidance. Exchange of location point, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/exchange-of-location-point (дата обращения: 05.08.2019)

465 Guidance. Exchanging Cyber Threat intelligence, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/exchanging-cyber-threat-intelligence (дата обращения: 05.08.2019)

466 Guidance. Open contracting data, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/open-contracting-data-standard-profile (дата обращения: 05.08.2019)

467 Guidance. Persistent resolvable identifiers, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/persistent-resolvable-identifiers (дата обращения: 05.08.2019)

468 Guidance. Publishing grant data, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/data-standard-for-grant-making (дата обращения: 05.08.2019)

469 Guidance. Publishing vacancies, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/publishing-vacancies-online-standards-profile--2 (дата обращения: 05.08.2019)

470 Guidance. Sharing or collaborating with government documents, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/sharing-or-collaborating-with-government-documents (дата обращения: 05.08.2019)

471 Guidance. Technology Code of Practice, 2019. — URL: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice (дата обращения: 05.08.2019)

472 Guidance. Viewing government documents, 2019. — URL: https://www.gov.uk/government/publications/open-standards-for-government/viewing-government-documents (дата обращения: 05.08.2019)

473 HMRC enforcement notice (10 May 2019) . — URL: https://ico.org.uk/action-weve-taken/enforcement/hmrc/ (дата обращения: 05.08.2019)

474 Igbal Safarov (2019) Institutional Dimensions of Open Government Data Implementation: Evidence from the Netherlands, Sweden, and the UK, Public Performance & Management Review, 42:2, 305-328

475 IICSA monetary penalty notice (18 July 2018) . — URL: https://ico.org.uk/action-weve-taken/enforcement/independent-inquiry-into-child-sexual-abuse/ (дата обращения: 05.08.2019)

476 Information Commissioner's Office. Official website. — URL: https://ico.org.uk (дата обращения: 05.08.2019)

477 Information Principles 2011. — URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266284/Information_Principles_UK_Public_Sector_final.pdf (дата обращения: 05.08.2019)

478 Information Rights Strategic Plan 2017-2021. — URL: https://ico.org.uk/media/about-the-ico/documents/2014134/20170413icoinformationrightsstrategicplan2017to2021v10.pdf (дата обращения: 05.08.2019)

479 Lancashire Police data protection audit report 2019. — URL: https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2615173/lancashire-police-exec-summary-201905.pdf (дата обращения: 05.08.2019)

480 Legal Ombudsman data protection audit report 2019. — URL: https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2615063/legal-ombudsman-executive-summary.pdf (дата обращения: 05.08.2019)

481 Liddle, C., & McMenemy, D. (2015). A Scottish freedom of information regime for a denationalised environment: rhetorical or authentically practical?. Information & Communications Technology Law, 24(3), 234

482 Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000. — URL:

http://www.nationalarchives.gov.uk/documents/information-management/foi-section-46-code-of-practice.pdf (дата обращения: 05.08.2019)

483 NHS England data protection audit report 2019. — URL: https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2614990/nhs-england-audit-es-201901.pdf (дата обращения: 05.08.2019)

484 Official Secrets Act 1989. — URL: http://www.legislation.gov.uk/ukpga/1989/6/contents (дата обращения: 05.08.2019)

485 oneTRANSPORT Data Marketplace website. — URL: https://onetransport.io (дата обращения: 05.08.2019)

486 Open Government License for public sector information. — URL: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ (дата обращения: 05.08.2019)

487 Open Standards Board. — URL: https://www.gov.uk/government/groups/open-standards-board

488 Open Standards Principles. — URL: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (дата обращения: 05.08.2019)

489 Policy paper. Government Transformation Strategy 2017 to 2020. — URL: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020 (дата обращения: 05.08.2019)

490 Policy paper. Open Data: unleashing the potential. — URL: https://www.gov.uk/government/publications/open-data-white-paper-unleashing-the-potential (дата обращения: 05.08.2019)

491 Policy paper. Open Standards principles, 2018. — URL: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (дата обращения: 05.08.2019)

492 Policy paper. Open Standards principles. — URL: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles (дата обращения: 05.08.2019)

493 Policy paper. UK Digital Strategy. — URL: https://www.gov.uk/government/publications/uk-digital-strategy (дата обращения: 05.08.2019)

494 Protection of Freedoms Act 2012. — URL: http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted (дата обращения: 05.08.2019)

495 Public Services Network (PSN) . — URL: https://www.gov.uk/government/groups/public-services-network (дата обращения: 05.08.2019)

496 Rachel Montagnon, The Trade Secrets Directive – consistency of approach required, with or without Brexit, Journal of Intellectual Property Law & Practice, Volume 11, Issue 9, September 2016, Pages 643–644

497 Regulatory Action Policy, 2018. — URL: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf (дата обращения: 05.08.2019)

498 Resource and Infrastructure Strategic Plan 2017 – 2021. — URL: https://ico.org.uk/media/about-the-ico/documents/2172792/resourceandinfrastructurestrategicplan27112017.pdf (дата обращения: 05.08.2019)

499 Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part I of the Freedom of Information Act 2000. — URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/722476/Secretary_of_State_for_Constitutional_Affairs__Code_of_Practice.pdf (дата обращения: 05.08.2019)

500 Secretary of State for the Home Department & Anor v TLU & Anor [2018] EWCA Civ 2217 (15 June 2018) . — URL: http://www.bailii.org/ew/cases/EWCA/Civ/2018/2217.html (дата обращения: 05.08.2019)

501 Secretary of State for Justice enforcement notice (21 December 2017) . — URL: https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-justice/ (дата обращения: 05.08.2019)

502 Technology Strategy 2018-2021. — URL: https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf (дата обращения: 05.08.2019)

503 The Central Government sector monitoring report, 2009. — URL: https://ico.org.uk/media/action-weve-taken/monitoring/2795/central-government-sector-monitoring-report.pdf (дата обращения: 05.08.2019)

504 The Copyright and Rights in Databases Regulations 1997. — URL: http://www.legislation.gov.uk/uksi/1997/3032/contents/made (дата обращения: 05.08.2019)

505 The Environmental Information (Scotland) Regulations 2004. — URL: http://www.legislation.gov.uk/ssi/2004/520/contents/made (дата обращения: 05.08.2019)

506 The Network and Information Systems Regulations 2018. — URL: http://www.legislation.gov.uk/uksi/2018/506/contents (дата обращения: 05.08.2019)

507 The Re-use of Public Sector Information Regulations 2015. — URL: http://www.legislation.gov.uk/uksi/2015/1415/contents/made (дата обращения: 05.08.2019)

508 The Trade Secrets (Enforcement, etc.) Regulations 2018. — URL: http://www.legislation.gov.uk/uksi/2018/597/contents/made (дата обращения: 05.08.2019)

509 UK Digital Strategy 2017. — URL: https://www.gov.uk/government/publications/uk-digital-strategy (дата обращения: 05.08.2019)

510 Шамсутдинов Р. Р. Сравнительный анализ правовой защиты государственной тайны в Российской Федерации и в Великобритании //Символ науки. – 2016. – №. 12-3. С. 134

Источники в разрезе Австралии:

511 1406.0.55.003 - Responsible Use of ABS Microdata, User Guide. — URL: https://www.abs.gov.au/ausstats/abs@.nsf/mf/1406.0.55.003 (дата обращения: 05.08.2019)

512 ABS Pricing Policy. — URL: https://www.abs.gov.au/websitedbs/D3310114.nsf/51c9a3d36edfd0dfca256acb00118404/12bb13b927110e44ca2569a80013bec1!OpenDocument (дата обращения: 05.08.2019)

513 Architecture Overview. — URL: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-architecture-overview.pdf (дата обращения: 05.08.2019)

514 Attribute Profile. — URL: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-attribute-profile.pdf (дата обращения: 05.08.2019)

515 Audit Practice Statement. — URL: https://audit.wa.gov.au/wp-content/uploads/2018/07/AuditPracStatement-July2018.pdf (дата обращения: 05.08.2019)

516 Auditor General Act 2006. — URL: https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_4780.pdf/$FILE/Auditor%20General%20Act%202006%20-%20%5B00-00-02%5D.pdf?OpenElement (дата обращения: 05.08.2019)

517 Auditor-General Act 1997. — URL: https://www.legislation.gov.au/Details/C2018C00036 (дата обращения: 05.08.2019)

518 Australian Auditing Standards. — URL: https://www.auasb.gov.au/Pronouncements/Australian-Auditing-Standards.aspx (дата обращения: 05.08.2019)

519 Australian Government Charging Framework (the Charging Framework) . — URL: https://www.finance.gov.au/resource-management/charging-framework/ (дата обращения 02.08.2019)

520 Australian Government Public Data Policy Statement. — URL: https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf (дата обращения: 05.08.2019)

521 Australian Government Recordkeeping Metadata Standard. — URL: http://www.naa.gov.au/Images/AGRkMS-Version-2.2-June-2015_tcm16-93990.pdf (дата обращения: 05.08.2019)

522 Australian Information Commissioner Act 2010. — URL: https://www.legislation.gov.au/Details/C2010A00052 (дата обращения: 05.08.2019)

523 Australian National Audit Office Auditing Standards 2018. — URL: https://www.legislation.gov.au/Details/F2018L00179 (дата обращения: 05.08.2019)

524 CDR design – complete documentation (August 2019) . — URL: https://treasury.gov.au/consumer-data-right

525 Census and Statistics Act 1905. — URL: https://www.legislation.gov.au/Details/C2016C01005 (дата обращения: 05.08.2019)

526 Charter of Fundamental Rights of the European Union. — URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (дата обращения: 05.08.2019)

527 Competition Act 1998. — URL: http://www.legislation.gov.uk/ukpga/1998/41/contents (дата обращения: 05.08.2019)

528 Content Guide. URL: https://guides.service.gov.au/content-guide/ (дата обращения: 05.08.2019)

529 Content Strategy Guide. — URL: https://guides.service.gov.au/content-strategy/ (дата обращения: 30.08.2019)

530 Creative Commons licensing. — URL: https://www.abs.gov.au/websitedbs/D3310114.nsf/4a256353001af3ed4b2562bb00121564/8b2bdbc1d45a10b1ca25751d000d9b03?opendocument? (дата обращения: 05.08.2019)

531 Data sharing technology unlocks analytics insights for ANZ. — URL: https://www.datarepublic.com/case-study-anz (дата обращения: 05.08.2019)

532 DATA61.SCIRO.Regulation as a Platform. — URL: https://data61.csiro.au/en/Our-Work/Future-Cities/Optimising-service-delivery/RaaP (дата обращения: 05.08.2019)

533 Data-matching Program (Assistance and Tax) Act 1990. — URL: https://www.legislation.gov.au/Series/C2004A04095 (дата обращения: 05.08.2019)

534 De-identification and the Privacy Act. — URL: https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/ (дата обращения: 05.08.2019)

535 Digital Service Platforms Strategy. — URL: https://www.dta.gov.au/book/export/html/769 (дата обращения: 30.08.2019)

536 Digital Service Standard. — URL: https://www.dta.gov.au/help-and-advice/about-digital-service-standard (дата обращения: 05.08.2019)

537 Digital Transformation Strategy. — URL: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-transformation-strategy/digital-transformation-strategy.pdf (дата обращения: 05.08.2019)

538 External audit: IT Capability and Resourcing. Report by the Independent Auditor. — URL: https://www.anao.gov.au/files/external-audit-it-capability-and-resourcing-pdf (дата обращения: 05.08.2019)

539 Flipchart and List of Commonwealth entities and companies. — URL: https://www.finance.gov.au/resource-management/governance/#flipchart (дата обращения: 05.08.2019)

540 Freedom of Information (Prescribed Authorities, Principal Officers and Annual Report) Regulations 2017. — URL: https://www.legislation.gov.au/Details/F2017L01676 (дата обращения: 05.08.2019)

541 Freedom of Information Act 1982. — URL: https://www.legislation.gov.au/Details/C2019C00198 (дата обращения: 05.08.2019)

542 Guide to Data Analytics and the Australian Privacy Principles. — URL: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/ (дата обращения: 05.08.2019)

543 Guide to privacy regulatory action. — URL: https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/ (дата обращения: 05.08.2019)

544 Guide to Securing Personal Information. — URL: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/#appendix-b-additional-resources (дата обращения: 05.08.2019)

545 Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982. — URL: https://www.oaic.gov.au/assets/freedom-of-information/guidance-and-advice/foi-guidelines/foi-guidelines-combined-january-2019.pdf (дата обращения: 05.08.2019)

546 Guidelines on Data Matching in Australian Government Administration. — URL: https://www.oaic.gov.au/privacy/guidance-and-advice/guidelines-on-data-matching-in-australian-government-administration/ (дата обращения: 05.08.2019)

547 Healthcare Identifiers Act 2010. — URL: https://www.legislation.gov.au/Series/C2010A00072 (дата обращения: 05.08.2019)

548 How to use data.gov.au. — URL: https://toolkit.data.gov.au/How_to_use_data.gov.au.html (дата обращения: 05.08.2019)

549 Human Rights Act 1998. — URL: https://www.legislation.gov.uk/ukpga/1998/42/contents (дата обращения: 05.08.2019)

550 Information security. Core requirements. — URL: https://www.protectivesecurity.gov.au/information/Pages/default.aspx (дата обращения: 05.08.2019)

551 Information Systems Audit Report 2019. — URL: https://audit.wa.gov.au/wp-content/uploads/2019/05/IS-Report-2019.pdf (дата обращения: 05.08.2019)

552 LOCAL GOVERNMENT ACT 1995 - SECT 7.12A. — URL: http://classic.austlii.edu.au/au/legis/wa/consol_act/lga1995182/s7.12a.html (дата обращения: 05.08.2019)

553 Location Index (Loc-I). — URL: http://locationindex.org/ (дата обращения: 05.08.2019)

554 Magda Documentation. — URL: https://magda.io/docs/

555 Mobile privacy: a better practice guide for mobile app developers. — URL: https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/#appendix-b-resources (дата обращения: 05.08.2019)

556 Multi-Agency Data Integration Project (MADIP). — URL: https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP (дата обращения: 05.08.2019)

557 Multi-Agency Data Integration Project (MADIP). — URL: https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP (дата обращения: 05.08.2019)

558 My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016. — URL: https://www.legislation.gov.au/Details/F2016L00360 (дата обращения: 05.08.2019)

559 My Health Records Act 2012. — URL: https://www.legislation.gov.au/Series/C2012A00063 (дата обращения: 05.08.2019)

560 My Health Records Regulation 2012. — URL: https://www.legislation.gov.au/Details/F2019C00520 (дата обращения: 05.08.2019)

561 My Health Records Rule 2016. — URL: https://www.legislation.gov.au/Details/F2016L00095 (дата обращения: 05.08.2019)

562 National Government Information Sharing Strategy. — URL: https://www.finance.gov.au/sites/default/files/ngiss.pdf (дата обращения: 01.09.2019)

563 National Health (Privacy) Rules 2018. — URL: https://www.legislation.gov.au/Details/F2018L01427 (дата обращения: 05.08.2019)

564 NationalMap. — URL: https://nationalmap.gov.au/ (дата обращения: 05.08.2019)

565 New Australian Government Data Sharing and Release Legislation: Issues paper for consultation. — URL: https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation (дата обращения: 05.08.2019)

566 New South Wales Government Open Data Policy supports Creative Commons licensing for government data and information. — URL: https://creativecommons.org.au/blog/2013/11/new-south-wales-government-open-data-policy-supports-creative-commons-licensing-for-government-data-and-information/ (дата обращения: 05.08.2019)

567 NSW Data Portal Tutorial. — URL: https://portal.data.nsw.gov.au/arcgis/apps/MapSeries/index.html?appid=86e47b08897642c9842c7b84d7dfd354 (дата обращения: 05.08.2019)

568 NSW. Open Data Policy. — URL: https://www.digital.nsw.gov.au/sites/default/files/NSW_Government_Open_Data_Policy_2016.pdf (дата обращения: 05.08.2019)

569 Open Data Toolkit. — URL: https://toolkit.data.gov.au/ (дата обращения: 05.08.2019)

570 Perfomance Audit Report. Information Technology at the Department of Health and Ageing. — URL: https://www.anao.gov.au/work/performance-audit/information-technology-department-health-and-ageing (дата обращения: 05.08.2019)

571 Performance Audit Report. Information Technology in the Department of Veterans' Affairs-Follow-up Audit. — URL: https://www.anao.gov.au/work/performance-audit/information-technology-department-veterans-affairs-follow-audit (дата обращения: 05.08.2019)

572 Planning. — URL: https://toolkit.data.gov.au/Planning.html (дата обращения: 05.08.2019)

573 Policies and Guidelines. — URL: https://dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/policies-and-guidelines; Toolkits. — URL: https://dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/toolkits (дата обращения: 05.08.2019)

574 Policy. — URL: https://toolkit.data.gov.au/Policy.html (дата обращения: 05.08.2019)

575 Prices. — URL: https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Microdata+prices (дата обращения: 05.08.2019)

576 Principles on open public sector information. — URL: https://www.oaic.gov.au/information-policy/information-policy-

resources/principles-on-open-public-sector-information (дата обращения: 05.08.2019)

577 Privacy Act 1988. — URL: https://www.legislation.gov.au/Details/C2019C00198 (дата обращения: 05.08.2019)

578 Productivity Commission 2017, Data Availability and Use, Report No. 82, Canberra.— URL: https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf (дата обращения: 05.08.2019)

579 Program Protocol. Matching of Centrelink and Medicare Data. — URL: https://www.humanservices.gov.au/sites/default/files/2019-matching-of-centrelink-and-medicare-data-protocol.pdf (дата обращения: 05.08.2019)

580 Public Governance, Performance and Accountability Act 2013 (PGPA Act). URL: https://www.legislation.gov.au/Series/C2013A00123 (дата обращения: 05.08.2019)

581 Public Governance, Performance and Accountability Act 2013. — URL: https://www.legislation.gov.au/Details/C2017C00269 (дата обращения: 05.08.2019)

582 Public Service Act 1999. — URL: https://www.deepl.com/translator#en/ru/Public%20Service%20Act%201999 (дата обращения: 05.08.2019)

583 Requirements for Australian Government websites. — URL: https://www.dta.gov.au/help-and-advice/guides-and-tools/requirements-australian-government-websites (дата обращения: 30.08.2019)

584 Review of ANAO better practice guides. — URL: https://www.anao.gov.au/work/better-practice-guide/review-anao-better-practice-guides (дата обращения: 05.08.2019)

585 Roadmap. — URL: https://www.dta.gov.au/digital-transformation-strategy/roadmap-page (дата обращения: 30.08.2019)

586 Secretary of State for the Home Department & Anor v TLU & Anor [2018] EWCA Civ 2217 (15 June 2018) . — URL:

http://www.bailii.org/ew/cases/EWCA/Civ/2018/2217.html (дата обращения: 05.08.2019)

587 Service Operations Testing Requirements. — URL: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/Trusted%20digital%20identity%20framework%202/Service%20Operations%20Testing%20Requirements.pdf (дата обращения: 05.08.2019)

588 Style Manual. — URL: https://www.dta.gov.au/our-projects/style-manual (дата обращения: 30.08.2019)

589 Systems Assurance and Data Analytics Group. Roles, requirements and responsibilities. — URL: https://www.anao.gov.au/careers/business-areas/systems-assurance-and-data-analytics-group (дата обращения: 05.08.2019)

590 Technical Integration Testing Requirements. — URL: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/Trusted%20digital%20identity%20framework%202/Technical%20Integration%20Testing%20Requirements.pdf (дата обращения: 05.08.2019)

591 Terms of Use. — URL: https://data.gov.au/page/about (дата обращения: 05.08.2019)

592 The Commonwelth. — URL: http://thecommonwealth.org/our-member-countries/australia (дата обращения: 05.08.2019)

593 The Confidentiality Information Series. — URL: https://www.abs.gov.au/ausstats/abs@.nsf/mf/1160.0 (дата обращения: 05.08.2019)

594 The Data Integration Partnership for Australia (DIPA) . — URL: https://www.pmc.gov.au/public-data/data-integration-partnership-australia (дата обращения: 05.08.2019)

595 The De-Identification Decision-Making Framework. — URL: https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS3 (дата обращения: 05.08.2019)

596 The Network and Information Systems Regulations 2018. — URL: http://www.legislation.gov.uk/uksi/2018/506/contents (дата обращения: 05.08.2019)

597 The Protective Security Policy Framework. — URL: https://www.protectivesecurity.gov.au/Pages/default.aspx (дата обращения: 05.08.2019)

598 Transparency Report. — URL: https://audit.wa.gov.au/wp-content/uploads/2018/05/Transparency-Report_May2018-3.pdf (дата обращения: 05.08.2019)

599 Treasury Laws Amendment (Consumer Data Right) Bill 2019. Division 3—Accreditation etc. Subdivision A—Accreditation process. — URL: https://www.legislation.gov.au/Details/C2019A00063 (дата обращения: 05.08.2019)

600 Trusted Digital Identity Framework. — URL: https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework (дата обращения: 05.08.2019)

601 Watts, D., Casanovas P. Privacy and Data Protection in Australia: a Critical overview (extended abstract) . — URL: https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf (дата обращения: 05.08.2019)

Источники в разрезе Сингапура:

602 Advisory Guidelines On Enforcement For Data Protection Provisions. — URL://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-enforcement-of-dp-provisions-(210416).pdf (дата обращения: 05.08.2019)

603 Advisory Guidelines On Key Concepts In The Personal Data Protection Act. — URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-

Files/Advisory-Guidelines/AG-on-Key-Concepts-in-the-PDPA-Revised-15-July-2019.pdf (дата обращения: 05.08.2019)

604 Advisory Guidelines On The Personal Data Protection Act For Selected Topics. — URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/FINAL-Advisory-Guidelines-on-PDPA-for-Selected-Topics-2-Jan-2019.pdf (дата обращения: 05.08.2019)

605 Banking Act 1970. — URL: https://sso.agc.gov.sg/Act/BA1970 (дата обращения: 05.08.2019)

606 CCS Guidelines on the Section 34 Prohibition 2016. — URL: https://www.cccs.gov.sg/-/media/custom/ccs/files/legislation/legislation-at-a-glance/cccs-guidelines/cccs-guidelines-on-the-section-34-prohibitions-2016.pdf (дата обращения: 05.08.2019)

607 Competition Act. — URL: https://sso.agc.gov.sg/Act/CA2004 (дата обращения: 05.08.2019)

608 Competition Commission of Singapore. Brief extracts from this paper may be reproduced for non-commercial use provided the source is acknowledged. — 2017. — URL: https://www.cccs.gov.sg/-/media/custom/ccs/files/media-and-publications/publications/occasional-paper/ccs-big-data-paper-16-aug-2017nonconfi-final.pdf (дата обращения: 05.08.2019)

609 Computer Misuse And Cybersecurity (Amendment) Act 2017. — URL: https://sso.agc.gov.sg/Acts-Supp/22-2017/Published/20170511?DocDate=20170511 (дата обращения: 05.08.2019)

610 Cybersecurity Act 2018 (Act. 9 of 2018) . — URL: https://sso.agc.gov.sg/Acts-Supp/9-2018/ (дата обращения: 05.08.2019)

611 Digital Government Blueprint) . — URL: https://www.smartnation.sg/docs/default-source/default-document-library/dgb_booklet_june2018.pdf (дата обращения: 05.08.2019)

612 Digital Government Transformation. — URL: https://www.tech.gov.sg/digital-government-transformation/ (дата обращения: 05.08.2019)

613 Digital Readiness Blueprint. — URL: https://www.mci.gov.sg/en/portfolios/digital-readiness/digital-readiness-blueprint (дата обращения: 05.08.2019)

614 Digital Service Standards. — URL: https://www.tech.gov.sg/files/digital-transformation/DSS%20for%20public%20release.pdf.pdf (дата обращения: 05.08.2019)

615 Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, pp. 25–26. — URL: https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6370_ems_ce513d68-7222-49f4-a2fe-67e1c2b32fed/upload_pdf/712911.pdf;fileType=application%2Fpdf (дата обращения: 05.08.2019)

616 Human Biomedical Research Act 2015. — URL: https://sso.agc.gov.sg/Act/HBRA2015 (дата обращения: 05.08.2019)

617 Inofocom Media development Authority. Guide to Data Sharing. — URL: https://www2.imda.gov.sg/-/media/Imda/Files/Industry-Development/Innovation/Guide-to-Data-Sharing-PowerPoint.pdf?la=en (дата обращения: 05.08.2019)

618 Ministry Family Digitalisation Guide. — URL: https://www.tech.gov.sg/files/digital-transformation/ministry-family-digitalisation-guide.pdf (дата обращения: 05.08.2019)

619 Monetary Authority of Singapore Act. — URL: https://sso.agc.gov.sg/Act/MASA1970#legis (дата обращения: 05.08.2019)

620 Monetary Authority of Singapore. CONSULTATION PAPER ON SANDBOX EXPRESS. P015 — 2018. — URL: https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/2018%20Nov%20Sandbox%20Express/Consultation%20Paper%20on%20Sandbox%20Express.pdf (дата обращения: 05.08.2019)

621 Official Secrets Act 2012. — URL: https://sso.agc.gov.sg/Act/OSA1935#pr1- (дата обращения: 05.08.2019)

622 PDPC Guide to Data Sharing. — URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/OtherGuides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf (дата обращения: 05.08.2019)

623 Personal Data Protection (Statutory Bodies) Notification 2013. — URL: https://sso.agc.gov.sg/SL/PDPA2012-S149-2013?DocDate=20180329 (дата обращения: 05.08.2019)

624 Personal Data Protection Act 2012 (PDPA). Personal Data Commission Singapore. — URL: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Enforcement-of-the-Act (дата обращения: 05.08.2019)

625 Private Hospitals and Medical Clinics Act. — URL: https://sso.agc.gov.sg/Act/PHMCA1980 (дата обращения: 05.08.2019)

626 Public Sector (Governance) Act 2018. Personal Data Commission Singapore. — URL: https://sso.agc.gov.sg/Acts-Supp/5-2018/Published/20180305?DocDate=20180305 (дата обращения: 05.08.2019)

627 Singapore Government Tech Stack. — URL: https://www.tech.gov.sg/products-and-services/singapore-government-tech-stack/?utm_medium=recommender_3&utm_source=aHR0cHM6Ly93d3cudGVjaC5nb3Yuc2cvZGlnaXRhbC1zdGFuZGFyZHMtYW5kLWd1aWRlcy8=&utm_content=aHR0cHM6Ly93d3cudGVjaC5nb3Yuc2cvcHJvZHVjdHMtYW5kLXNlcnZpY2VzL3NpbmdhcG9yZS1nb3Zlcm5tZW50LXRlY2gtc3RhY2sv (дата обращения: 05.08.2019)

628 Spam Control Act. — URL: https://sso.agc.gov.sg/Act/SCA2007 (дата обращения: 05.08.2019)

629 Telecoms Competition Code. — URL: https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/frameworks-and-policies/competition-management/telecom-competition-code/02-2012tccwef2july2014.pdf?la=en (дата обращения: 05.08.2019)

Источники в разрезе Китая:

630 General Office of the CPC Central Committee Opinions on Comprehensively Promoting Open Government. — URL: https://law.yale.edu/system/files/area/center/china/document/2016-2_en_jt_promoting_open_government_opinions.pdf (дата обращения: 02.08.2019)

631 Information security techniques - personal information security specifications (Draft for solicitation of comments. — URL: https://www.chinalawtranslate.com/%e4%bf%a1%e6%81%af%e5%ae%89%e5%85%a8%e6%8a%80%e6%9c%af%e3%80%80%e4%b8%aa%e4%ba%ba%e4%bf%a1%e6%81%af%e5%ae%89%e5%85%a8%e8%a7%84%e8%8c%83-%ef%bc%88%e5%be%81%e6%b1%82%e6%84%8f%e8%a7%81%e7%a8%bf%ef%bc%89/?lang=en#_Toc28802 (дата обращения: 02.08.2019)

632 Information security technology—Personal Information Security Specifications. — URL: https://www.chinalawtranslate.com/en/persona-information-security-standards/ (дата обращения:02.08.2019)

633 Measures for the Administration of Population Health Information (Trial Implementation). — URL: http://www.law.hku.hk/cprivacy/archives/175 (дата обращения: 31.10.2019)

634 Measures on Open Environmental Information (for Trial Implementation) . — URL: https://law.yale.edu/system/files/area/center/china/document/sepa_measures_on_open_environmental_information_trial.pdf (дата обращения: 02.08.2019)

635 Notice of the General Office of the State Council on Further Improving Secrecy Examination in Open Government Information Work. — URL: https://law.yale.edu/system/files/china-law-documents/2010_SCGO_Notice_on_Secerecy_Examination.docx (дата обращения: 02.08.2019)

636 Notice of the General Office of the State Council On Preparing Well for Implementing the Regulations of the People's Republic of China on Open

Government Information. — URL: https://law.yale.edu/system/files/documents/pdf/Intellectual_Life/CL--OGI-State_Council_Notice-English.pdf (дата обращения: 02.08.2019)

637 Notice of the General Office Secretariat Bureau of the State Council on Issuing the Open Government Information Catalog System Implementing Guide (Interim) . — URL: https://law.yale.edu/system/files/china-law-documents/ch_2009_SCGO_on_OGI_Catalgoue_System.docx (дата обращения: 02.08.2019)

638 Notice of the Ministry of Finance and the National Development and Reform Commission on Fees Collected for Providing Open Government Information and Other Relevant Issues. — URL: https://law.yale.edu/system/files/documents/pdf/Intellectual_Life/CL-OGI-Notice_MOF-English.pdf (дата обращения: 02.08.2019)

639 Notice of the National Development and Reform Commission and the Ministry of Finance on the Standards for Fees Collected by Administrative Organs for Providing Open Government Information upon Request and Other Relevant Issues. — URL: https://law.yale.edu/system/files/documents/pdf/Intellectual_Life/CL-OGI-NDRC_MOF_July08-English.pdf (дата обращения: 02.08.2019)

640 Opinions of the General Office of the State Council on Further Strengthening Open Government Information Responding to Social Concerns in order to Raise Government Credibility. — URL: https://law.yale.edu/system/files/china-law-documents/ch_2010_SCGO_Notice_on_Secrecy_Exam_in_OGI_Work.docx (дата обращения: 02.08.2019)

641 Opinions of the General Office of the State Council on Improving the Work of Disclosing Government Information Upon Request. — URL: https://law.yale.edu/system/files/documents/pdf/Intellectual_Life/CL-OGI_SCGO_Opinions_on_OGI_Request_2010_%28Eng%29.pdf (дата обращения: 02.08.2019)

642 Opinions of the General Office of the State Council on Various Issues of Implementing the Open Government Information Regulations of the People’s Republic of China. — URL: https://law.yale.edu/system/files/documents/pdf/Intellectual_Life/CL-OGI-State_Council_Opinions-English.pdf (дата обращения: 02.08.2019)

643 Regulation on medical records management in medical institutions. URL: http://en.nhc.gov.cn/2014-06/25/c_46464.htm (дата обращения: 31.10.2019)

644 Regulations of the Communist Party of China on Open Party Affairs (For Trial Implementation) . — URL: https://law.yale.edu/system/files/china-law-documents/horsley_eng._open_party_affairs_regulations.pdf (дата обращения: 02.08.2019)

645 Regulations of the People’s Republic of China on Open Government Information. — URL: https://law.yale.edu/system/files/documents/pdf/china/ogi_regulations_eng_jph_rev_9-11.pdf (дата обращения: 02.08.2019)

646 Surveying and Mapping Law of the People's Republic of China. — URL: http://extwprlegs1.fao.org/docs/pdf/chn173733.pdf (дата обращения: 31.10.2019)

647 The Cybersecurity Law of the People’s Republic of China. — URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (дата обращения:02.08.2019)

648 The Supreme People’s Court Provisions on Certain Questions Concerning the Trial of Open Government Information Administrative Cases. — URL: https://law.yale.edu/system/files/area/center/china/document/2011-8_en_spc_ogi_cases_provisions.pdf (дата обращения:02.08.2019)

649 Конституция Китайской Народной Республики 1982 г. — URL: https://legalns.com/download/books/cons/china.pdf (дата обращения: 31.10.2019)

Источники в разрезе Республики Кореи:

650 Act on Disclosure of Information by Public Agencies, 2014. — URL: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025690.pdf (дата обращения: 02.08.2019)

651 Act on promotion of information and communications Network Utilization and Data Protection, 2016. — URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG (дата обращения: 02.08.2019) (дата обращения: 02.08.2019)

652 Act on Promotion of the Provision and Use of Public Data, 2013. — URL: https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=37882 (дата обращения: 02.08.2019)

653 Act on the Protection of Information and Communications and Infrascture, 2001. — URL: http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43 (дата обращения: 02.08.2019)

654 Act on the Protection, Use, etc. of Location Information, 2016. — URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=43349&lang=ENG#targetText=The%20purpose%20of%20this%20Act,the%20promotion%20of%20public%20welfare (дата обращения: 02.08.2019)

655 Bioethics and Safety Act, 2005. — URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=33442&type=part&key=36 (дата обращения: 02.08.2019)

656 Electronic government act, 2001. — URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=45844&type=part&key=4 (дата обращения: 02.08.2019)

657 Military Secrets Protection Act, 1993. — URL: http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=35867&type=part&key=13 (дата обращения: 02.08.2019)

658 Personal Information Protection Act, 2011. — URL: http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf (дата обращения: 02.08.2019)

659 Spatial Data Industry Promotion Act, 2014. — URL: http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=32571&type=new&key= (дата обращения: 02.08.2019)