ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

НОВАЯ ПАРАДИГМА **ЗАЩИТЫ И УПРАВЛЕНИЯ ПЕРСОНАЛЬНЫМИ ДАННЫМИ**

в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет

Под редакцией директора Института проблем правового регулирования НИУ ВШЭ, канд. юрид. наук А.С. Дупан (Гутниковой)

Издательский дом Высшей школы экономики
Москва 2016

УДК 342.7: 004.738.5.056.5
ББК 67.404.3
Н72

Под редакцией А.С. Дупан (Гутниковой)

Авторский коллектив:

директор Института проблем правового регулирования НИУ ВШЭ, канд. юрид. наук *А.С. Дупан* (*Гутникова*) (подразд. 1.11, гл. 3, подразд. 5.1.3, 5.2, 5.8, 6.1 (совместно с *С.В. Титовой*), 6.4, 6.5, гл. 8 (совместно с *А.Б. Жулиным*));

заместитель заведующего кафедрой инновации и бизнеса в сфере ИТ факультета бизнес-информатики НИУ ВШЭ, канд. юрид. наук, доцент *А.К. Жарова* (подразд. 1.3, 1.7);

заместитель заведующего кафедрой информационной безопасности факультета бизнеса и менеджмента НИУ ВШЭ, канд. пед. наук *В.М. Елин* (подразд. 1.10);

директор Центра анализа деятельности органов исполнительной власти ИГМУ НИУ ВШЭ, канд. экон. наук *А.Б. Жулин* (гл. 8 совместно с *А.С. Дупан* (*Гутниковой*));

научный сотрудник Института проблем правового регулирования НИУ ВШЭ *Ю.С. Бикбулатова* (подразд. 1.1, 2.1.2, 2.2.1 (совместно с *Т.И. Бикбулатовым*), 5.1.4, 5.7, гл. 7);

научный сотрудник Института проблем правового регулирования НИУ ВШЭ *Т.И. Бикбулатов* (подразд. 1.2, 1.9, 2.2.1 (совместно с *Ю.С. Бикбулатовой*));

аналитик Института проблем правового регулирования НИУ ВШЭ *С.В. Титова* (подразд. 1.5, 1.6, 1.8, 2.1.1, 2.1.3, 2.2.2, 2.3, 5.1, 5.1.1, 5.1.2, 5.3–5.6, 6.1 (совместно с *А.С. Дупан* (*Гутниковой*), 6.2, 6.3);

адвокат Германии (Германия, Kollegienwall, 24, 49074 Osnabrück) *Д. Римша* (подразд. 1.4).

ISBN 978-5-7598-1386-6

Содержание

Предисловие 11

1. НОВЫЕ ПОДХОДЫ К РЕГУЛИРОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕВРОПЕ, США И В ИНЫХ ЗАРУБЕЖНЫХ СТРАНАХ 13

1.1. Европейский союз 13
1.1.1. Регулирование 13
1.1.2. Определение персональных данных 14
1.1.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 20
1.1.4. Ответственность за нарушения в области персональных данных и запрет на передачу данных третьим лицам 24
1.1.5. Режим защиты персональных данных при обработке больших данных, позволяющих при сопоставлении получать персональные данные 25
1.1.6. Регулирование порядка анализа результатов обработки данных (метаданных) 27
1.1.7. Правовое обеспечение защиты данных 27
1.1.8. Регулирование вопроса о наследовании прав на персональные данные 30
1.1.9. Уполномоченный орган по защите субъектов персональных данных и его функции 31
1.1.10. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 34
1.1.11. Порядок трансграничной передачи персональных данных 35
1.2. Совет Европы 49
1.2.1. Регулирование 49
1.2.2. Определение персональных данных 53
1.2.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 54
1.2.4. Ответственность за нарушения в области персональных данных и запрет на передачу данных третьим лицам 56

1.2.5. Режим защиты персональных данных при обработке больших данных, позволяющих при сопоставлении получать персональные данные 58
1.2.6. Регулирование порядка анализа результатов обработки данных (метаданных) 59
1.2.7. Уполномоченный орган по защите субъектов персональных данных и его функции 60
1.2.8. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 61
1.2.9. Трансграничная передача данных 62
1.3. Великобритания 62
1.3.1. Регулирование 62
1.3.2. Определение персональных данных 65
1.3.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 66
1.3.4. Ответственность за нарушения в области персональных данных и запрет на передачу данных третьим лицам 67
1.3.5. Регулирование порядка анализа результатов обработки данных (метаданных) 69
1.3.6. Правовое обеспечение защиты данных 71
1.3.7. Системы удаленного распределенного управления данными и их регламентация в национальном законодательстве 72
1.3.8. Уполномоченный орган по защите субъектов персональных данных и его функции 77
1.3.9. Трансграничная передача данных 78
1.4. Германия 78
1.4.1. Регулирование 78
1.4.2. Определение персональных данных 83
1.4.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 85
1.4.4. Ответственность за нарушения в области персональных данных и запрет на передачу данных третьим лицам 86
1.4.5. Правовое обеспечение защиты данных 87
1.4.6. Регулирование вопроса о наследовании прав на персональные данные 88
1.4.7. Уполномоченный орган по защите субъектов персональных данных и его функции 89

1.5. Нидерланды 89
1.5.1. Регулирование 89
1.5.2. Определение персональных данных 90
1.5.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 91
1.5.4. Ответственность за нарушения в области персональных данных и запрет на передачу данных третьим лицам 94
1.5.5. Регулирование порядка анализа результатов обработки данных (метаданных) 95
1.5.6. Правовое обеспечение защиты данных 97
1.5.7. Уполномоченный орган по защите субъектов персональных данных и его функции 98
1.5.8. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 99
1.6. Япония 99
1.6.1. Регулирование 99
1.6.2. Определение персональных данных 102
1.6.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 103
1.6.4. Ответственность за нарушения в области персональных данных и запрет на передачу данных третьим лицам 104
1.6.5. Правовое обеспечение защиты данных 105
1.6.6. Режим регулирования персональных данных, отнесенных к государственной тайне 106
1.6.7. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 106
1.7. Аргентина 106
1.7.1. Регулирование 106
1.7.2. Определение персональных данных 110
1.7.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 111
1.7.4. Ответственность за нарушения, связанные с персональными данными, и регулирование передачи персональных данных третьим лицам 112
1.7.5. Правовое обеспечение защиты данных 116
1.7.6. Системы удаленного распределенного управления данными и их регламентация в национальном законодательстве 119

1.7.7. Уполномоченный орган по защите субъектов персональных данных и его функции 120
1.7.8. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 121
1.7.9. Трансграничная передача данных 121
1.8. Бразилия 122
1.8.1. Регулирование 122
1.8.2. Определение персональных данных 125
1.8.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 126
1.8.4. Ответственность за нарушения в сфере персональных данных и порядок передачи данных третьим лицам 127
1.8.5. Правовое обеспечение защиты данных 128
1.8.6. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 128
1.9. Китай 129
1.9.1. Регулирование 129
1.9.2. Определение персональных данных 134
1.9.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 135
1.9.4. Ответственность за нарушения в области персональных данных и порядок доступа к данным третьих лиц 136
1.9.5. Правовое обеспечение защиты данных 137
1.9.6. Уполномоченный орган по защите субъектов персональных данных и его функции 137
1.9.7. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 138
1.9.8. Трансграничная передача данных 138
1.10. Соединенные Штаты Америки 139
1.10.1. Регулирование 141
1.10.2. Определение персональных данных 148
1.10.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 152
1.10.4. Ответственность за нарушения в области персональных данных и порядок передачи данных третьим лицам 153

1.10.5. Режим защиты персональных данных при обработке больших данных, позволяющих при сопоставлении получать персональные данные 154
1.10.6. Уполномоченный орган по защите субъектов персональных данных и его функции 158
1.10.7. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы 159
1.10.8. Анализ законопроектов США в области персональных данных 160
1.11. Сингапур 163
1.11.1. Регулирование 163
1.11.2. Определение персональных данных 164
1.11.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных 165
1.11.4. Ответственность за нарушения в области персональных данных и порядок передачи данных третьим лицам 167
1.11.5. Правовое обеспечение защиты данных 168
1.11.6. Регулирование вопроса о наследовании прав на персональные данные 169
1.11.7. Системы удаленного распределенного управления данными и их регламентация в национальном законодательстве 169
1.11.8. Уполномоченный орган по защите субъектов персональных данных и его функции 170
1.11.9. Трансграничная передача персональных данных 171

2. «ПРАВО БЫТЬ ЗАБЫТЫМ» В МЕЖДУНАРОДНОМ, ЗАРУБЕЖНОМ И РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ 172

2.1. Международное регулирование 172
2.1.1. Общее регулирование 172
2.1.2. Регулирование в рамках проекта Регламента 173
2.1.3. Перспективы регулирования «права быть забытым» 175
2.2. Зарубежное регулирование 177
2.2.1. Регулирование в отдельных странах 177
2.2.2. Судебная практика по «праву быть забытым» 179
2.3. Российское регулирование 181

3. СУЩЕСТВУЮЩИЕ МОДЕЛИ РЕГУЛИРОВАНИЯ ПРАВОВОГО ИНСТИТУТА ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕЖДУНАРОДНО-ПРАВОВЫХ И НАЦИОНАЛЬНЫХ ЗАРУБЕЖНЫХ ПРАВОВЫХ ИСТОЧНИКАХ 189

3.1. Регулирование 189

3.2. Определение персональных данных 192

3.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных..... 197

3.4. Ответственность за несанкционированные действия с персональными данными..... 200

3.5. Порядок передачи персональных данных третьим лицам 203

3.6. Режим защиты персональных данных при обработке больших данных, позволяющих при сопоставлении получать персональные данные 207

3.7. Регулирование порядка анализа результатов обработки данных (метаданных) 210

3.8. Правовое обеспечение защиты персональных данных 211

3.9. Регулирование вопроса о наследовании прав на персональные данные 213

3.10. Системы удаленного распределенного управления данными и их регламентация в национальном законодательстве..... 214

3.11. Уполномоченный орган по защите субъектов персональных данных и его функции 216

3.12. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы..... 218

4. УСЛОВИЯ СБОРА, ХРАНЕНИЯ, ИСПОЛЬЗОВАНИЯ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ КРУПНЕЙШИМИ КОМПАНИЯМИ, ОКАЗЫВАЮЩИМИ УСЛУГИ В ОБЛАСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, В ТОМ ЧИСЛЕ В ИНТЕРНЕТЕ 220

4.1. Собираемые персональные данные 220

4.2. Предоставление персональных данных третьим лицам..... 222

4.3. Использование полученных персональных данных 223
4.4. Доступ к персональным данным и управление ими 223
4.5. Использование файлов cookie и аналогичных технологий 225
4.6. Защита персональных данных 228
4.7. Трансграничная передача персональных данных 229

5. ЗАРУБЕЖНЫЙ ОПЫТ В ОБЛАСТИ СОЗДАНИЯ СИСТЕМ ДОВЕРИТЕЛЬНОГО УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ, ОПРЕДЕЛЕНИЯ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРОВЕДЕНИИ ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ И ОКАЗАНИИ АНАЛОГИЧНЫХ УСЛУГ ДОВЕРЕННЫМИ ЛИЦАМИ (ДОВЕРЕННЫЕ СЕРВИСЫ) 231

5.1. Страны Европейского союза. 231
5.1.1. Франция 237
5.1.2. Нидерланды 244
5.1.3. Эстония 248
5.1.4. Великобритания 260
5.2. Сингапур 269
5.2.1. Система доверенных сервисов в Сингапуре 269
5.2.2. Государственное регулирование доверенных сервисов. Присоединение к Национальной системе аутентификации частных компаний 276
5.2.3. Подходы к регулированию создания доверенных системы и управления персональными данными и иной информацией 278
5.2.4. IT-стандарты 279
5.3. Индия 280
5.4. Канада 284
5.5. Китай 292
5.6. ОАЭ 295
5.7. Соединенные Штаты Америки 298
5.8. Сравнение моделей доверительного управления информацией (доверенных сервисов идентификации и аутентификации) в зарубежных странах 301

6. АНАЛИЗ ПОНЯТИЙ СФЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ. ВОЗМОЖНЫЕ ПУТИ РАЗВИТИЯ СФЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ 305

6.1. Понятие «персональные данные». Правовой режим данных, не являющихся персональными данными, обработка которых позволяет получить персональные данные 305

6.2. Оператор персональных данных 311

6.3. Субъект персональных данных 312

6.4. Механизмы обеспечения выполнения требований, установленных законодательством о защите персональных данных 312

6.4.1. Совершенствование механизма ответственности за нарушения в области персональных данных 312

6.4.2. Механизм информирования уполномоченного органа об инцидентах 314

6.5. Корректировка действующего законодательства в части полномочий уполномоченного органа по защите прав субъектов персональных данных 315

7. О ВОЗМОЖНОСТИ СОСТАВЛЕНИЯ МАТРИЦЫ СООТНЕСЕНИЯ ОБЕЗЛИЧЕННЫХ СВЕДЕНИЙ, СОВОКУПНОСТЬ ОБОБЩЕНИЯ И СОПОСТАВЛЕНИЯ КОТОРЫХ МОЖЕТ СТАТЬ ПЕРСОНАЛЬНЫМИ ДАННЫМИ 318

8. КОНЦЕПЦИЯ РЕГУЛИРОВАНИЯ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ С УЧЕТОМ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 331

Предисловие

Свободный обмен информацией лежит в основе современной экономики. В то же время все более широкое использование и передача персональных данных создают повышенные риски с точки зрения неприкосновенности частной жизни. Постоянно трансформирующиеся способы и подходы обработки данных изменяют и категории рисков нарушения прав вовлеченных в формирующиеся правоотношения субъектов, что, в свою очередь, требует корректировки или даже полного изменения системы государственного регулирования данной сферы.

В контексте колоссально ускоряющихся темпов развития информационных технологий требуется выработка новой модели регулирования обработки персональных данных, которая, во-первых, обеспечила бы их адекватную защиту, а во-вторых, соответствовала бы принципу свободного обмена информацией.

Как и в любой другой сфере, где тесно переплетены право и технологии, подходы, меры государственного регулирования персональных данных нельзя признать сформированными в полной мере ни в одном государстве. Происходящее в настоящее время изменение подхода регулирования защиты персональных данных в различных странах мира обусловлено как общей тенденцией реформирования законодательства информационной отрасли в условиях цифровой эпохи отношений, так и особой политической ситуацией.

Система защиты персональных данных в Европейском союзе (как имеющая место в настоящий момент, так и планируемая к вступлению в силу после принятия нового генерального регламента) представляет собой комплексный стремящийся к сбалансированности механизм, выработка которого осуществлялась достаточно длительный период. Данная система не исчерпывается только законодательными актами, будучи детализируемой в многочисленных документах правового, технического, организационного характера (решения, резолюции, соглашения, документы и пр.).

Регулирование отношений в сфере персональных данных в Российской Федерации традиционно проводится с опозданием в срав-

нении с Европейским союзом, модель регулирования которого была взята за основу в России. В связи с этим требуется новый подход к регулированию персональных данных в Российской Федерации, основанный на изучении опыта зарубежных стран, чтобы обеспечить и защиту прав субъектов персональных данных, и выполнение международных обязательств Российской Федерации в данной сфере.

1. НОВЫЕ ПОДХОДЫ К РЕГУЛИРОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕВРОПЕ, США И В ИНЫХ ЗАРУБЕЖНЫХ СТРАНАХ

1.1. Европейский союз

1.1.1. Регулирование

На наднациональном уровне регулирование персональных данных включает следующие основные для данной сферы правовые акты:

1) Директиву Европейского союза от 24 октября 1995 г. № 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных (далее — Директива 95/46/ЕС);

2) Регламент Европейского союза № 45/2001 о защите персональных данных при их обработке органами и учреждениями Европейского союза, который отразил основные положения Директивы 1995 г.;

3) Директиву ЕС от 8 июня 2000 г. № 2000/31/ЕС о некоторых правовых аспектах информационных услуг на внутреннем рынке, в частности, об электронной коммерции.

25 января 2012 г. Европейской комиссией был опубликован проект Регламента Европейского союза о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных (далее — проект Регламента)[1]. 15 июня 2015 г. после более чем трехлетнего периода Советом Европейского союза был согласован законопроект о защите персональных данных. Начало процесса трехсторонних переговоров между Еврокомиссией, Европарламентом и Советом, известного как «трилог» (trilogue), было положено в июне

[1] Доработанная редакция проекта Регламента была опубликована 30 июня 2014 г. в Интернете для публичного доступа по адресу: URL: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011028%202014%20INIT.

2015 г. Как отметила Европейская комиссия в своем заявлении, «есть совместное желание достичь окончательного соглашения к концу 2015 г.»[2]. Новый порядок защиты персональных данных в Европейском союзе вступит в силу в 2017 г. и заменит устаревшие и нередко критично различающиеся нормативные правовые акты государств в этой области[3].

Проект Директивы Европейского парламента и Совета Европейского союза о защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или судебного преследования уголовных преступлений или исполнения уголовных наказаний и свободного движения таких данных (далее — проект Директивы), как и вышеупомянутый проект Регламента, является частью глобальной реформы защиты персональных данных граждан Евросоюза, который должен заменить Директиву Европейского союза от 24 октября 1995 г. № 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных.

1.1.2. Определение персональных данных

Пункт (а) ст. 2 Директивы 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных определяет персональные данные как любую информацию, относящуюся к определенному или определяемому физическому лицу («субъекту данных»). При этом определяемым является лицо, которое может быть определено прямо или косвенно, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Приведенное определение схоже с определением персональных данных, установленным п. 1 ст. 3 российского Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — За-

---

[2] *Ashford W.* EU Data Protection Regulation to be finalised by end of 2015. URL: http://www.computerweekly.com/news/4500248164/EU-Data-Protection-Regulation-to-be-finalised-by-end-of-2015

[3] *Эшфорд У.* Закон Евросоюза о защите персональных данных будет окончательно готов к концу 2015 г. URL: http://www.computerweekly.com/news/4500248164/EU-Data-Protection-Regulation-to-be-finalised-by-end-of-2015. Пер. Н. Храмцовской: URL: http://rusrim.blogspot.ru/2015/06/201519. html.

кон № 152-ФЗ, Закон о персональных данных), если рассматривать его в совокупности с определением субъекта данных. Представляется, что дефиниция «персональные данные» должна анализироваться в данном случае именно так (совокупно), поскольку характеристики данных, которые способны идентифицировать лицо (идентификационный номер либо один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности), содержатся именно в определении субъекта данных.

Проект Регламента в п. 1 ст. 4 дополняет перечень идентификаторов, с помощью которых возможно определение личности конкретного физического лица. В частности, перечень ранее установленных идентификаторов дополнен именем субъекта персональных данных, сведениями о месте его нахождения и онлайн-идентификаторами (id).

Такого рода дополнения в российском законодательстве пока не предвидятся.

За счет последующего пояснения в п. 1 ст. 4 Директивы понятия «субъект данных», определяющего виды информации, при помощи которых лицо может быть установлено (идентификационный номер либо один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности), персональные данные возможно условно группировать. Но дефиницию, представленную в Директиве 95/46/ЕС о защите физических лиц при обработке персональных данных и свободном перемещении таких данных, нельзя признать конкретной, поскольку перечисление видов персональных данных (ФИО, пол, дата рождения и пр.) данным актом не закреплено.

В то же время, как отмечалось выше, проект Регламента называет конкретные виды персональных данных: имя субъекта персональных данных, сведения о месте его нахождения и онлайн-идентификатор (id). В случае принятия данной редакции ст. 4 проекта Регламента определение персональных данных в ЕС будет иметь смешанный характер.

Последующий текст Директивы выделяет отдельную специальную категорию данных. В российском законе они соответствуют специальным персональным данным. Так, раздел 3 Директивы в ст. 8 запрещает обработку персональных данных, раскрывающих расовое или

этническое происхождение, политические взгляды, религиозные или философские убеждения, членство в профсоюзах, и обработку данных, касающихся состояния здоровья или сексуальной жизни. Таким образом, персональные данные также могут быть сгруппированы в перечисленные категории.

В проекте Регламента к специальным чувствительным категориям персональных данных также отнесены «генетические данные» (все личные данные, относящиеся к генетическим особенностям человека, наследуемым или приобретенным, полученным в результате анализа биологического материала человека), «биометрические данные» (любые личные данные, полученные в результате специфичной технической обработки, касающиеся физических, физиологических или поведенческих характеристик человека, которые позволяют подтвердить или подтверждают уникальную идентификацию конкретного лица, например, изображений лиц или дактилоскопические данные), «данные о здоровье» (данные, связанные с физическим или психическим здоровьем индивида, раскрывающие информацию о его состоянии здоровья).

Обработку специальных категорий персональных данных о расовой принадлежности, об этническом происхождении, о политических мнениях, о религии, о философских позициях, о членстве в профсоюзе, генетических данных, данных о состоянии здоровья или сексуальной жизни проектом Регламента предлагается запретить, однако допускаются исключения (если субъект персональных данных дал явное согласие на обработку персональных данных, обработка необходима в целях выполнения обязательств в области трудового права, обработка необходима, чтобы защитить жизненные интересы субъекта персональных данных или другого человека, обработка необходима для исполнения задач в рамках общественного интереса, социальной защиты, обработка персональных данных относительно здоровья необходима в целях профилактической или профессиональной медицины, медицинского диагноза, определения условий ухода или лечения и т.д.). Кроме того, обработка специальных категорий персональных данных может осуществляться в том случае, если она необходима для решения задач в области архивного дела в интересах общества, в исторических, статистических или научных целях. При этом обработка персональных данных, касающихся судимости и преступлений или связанных с обеспечением безопасно-

сти, может выполняться только под контролем официальных должностных лиц органов власти.

Также персональные данные предлагается различать по точности и надежности. В частности, проект Директивы разделяет персональные данные, основанные на фактах, и персональные данные субъективно оценочного характера.

Отметим, что вопросы о необходимости пересмотра концепции понимания персональных данных поднимаются все чаще как в ЕС, так и за его пределами. Эксперты отмечают, что граница между понятиями «персональные данные» (personally identifiable information, PII) и «неперсональные данные» (non-PII) постепенно размывается. Такое наблюдение подтолкнуло специалистов Международной ассоциации IAPP (далее — IAPP) к изучению того, что же именно входит в понятие «персональные данные», как с развитием технологий меняются официальные определения этих терминов.

В качестве отправной точки были взяты действующие официальные определения персональных данных. Действительно ли «персональные данные» — это «все данные о субъекте персональных данных»? Должны ли данные прямо идентифицировать субъекта персональных данных? Ответы на эти и многие другие вопросы можно получить, изучив определения персональных данных в законодательстве разных стран. Специалисты IAPP проверили соответствующие определения в 36 законах о защите данных 30 стран и пришли к следующим выводам. В упомянутых выше 36 законах используются разные формулировки. В некоторых странах, например в США, понятие персональных данных сформулировано относительно узко, и для его определения зачастую просто перечисляют конкретные элементы персональных данных. В то же время в других странах, особенно в странах Евросоюза, идет тенденция к более широкому толкованию термина «персональные данные». Несмотря на эти различия, в законодательстве этих стран, как и в Российской Федерации, используется типичная формулировка типа «персональные данные — это данные или информация, относящиеся к субъекту персональных данных, который можно идентифицировать». Также во всех странах используется одна и та же формулировка, иногда с небольшими изменениями, что «персональные данные — это данные, которые позволяют прямо или косвенно идентифицировать субъекта персональных данных».

Несмотря на схожесть формулировок, законы по-разному трактуют то, что действительно подпадает под их защиту. В одних странах прямо перечисляют состав персональных данных, в других ограничиваются более гибким (нечетким) определением. Несмотря на то что конкретные формулировки дают больше уверенности, они чаще подвергаются критике за свою инертность и невозможность следовать за современным развитием технологий. Гибкие формулировки, в свою очередь, позволяют адаптироваться к будущим изменениям, но при этом создают неопределенность.

По этим законам данные, которые не входят в состав персональных данных, считаются «неперсональными данными». Такой статус лишает их если не полностью, то большей части защиты со стороны закона. Эта концепция часто применялась в отношении собранных данных и только недавно стала применяться к «обезличенным» данным, из которых намеренно была удалена идентифицирующая информация.

В целях толкования разного рода неточностей в применении законодательства о персональных данных Рабочая группа 29-й статьи при ЕС подготовила Мнение 4/2007 (European Union Article 29 Working Party's Opinion 4/2007, далее — Группа и Мнение соответственно) о понятии персональных данных, расширяющее правила его толкования. Рабочая группа проанализировала типы данных или информации; отношения между данными и их субъектом; понятие идентифицируемости субъекта; субъекты персональных данных, подпадающие под защиту законодательства.

В рамках данного анализа наиболее интересны аспекты, связанные с идентификацией. Законы о приватности включают такие формулировки, как «ссылающийся на», «относящийся к», «о», «касающийся» субъекта персональных данных или человека. Разница между этими формулировками невелика, так как они так или иначе устанавливают связь между данными и их субъектом.

В Мнении Группы сообщается, что, вероятно, основная работа по установлению связей между персональными данными и субъектом персональных данных сводится к трем элементам — содержанию, задачам и интерпретации результатов.

Содержание данных, пожалуй, самый очевидный из этих трех элементов, так как оно раскрывает информацию о субъекте. Это могут быть его медицинская карта, реквизиты из договора или трудовая

книжка. Такая информация, по своей сути, относится к конкретному лицу.

Рассматривая задачи, можно обнаружить, что данные, которые никак не попадают в категорию персональных данных, — например, детализация корпоративных звонков — могут все же являться таковыми, если используются для наблюдения за действиями сотрудника. В этом случае Группа рассматривала такие данные, как персональные данные, относящиеся к сотруднику, делающему звонки, и к лицу, которому звонил данный сотрудник. И наконец, рассматривая интерпретацию результатов, можно утверждать, что даже данные, которые не относятся к определенному лицу,т.е. без элемента «содержание», и которые не используются для получения информации об определенном лице,т.е. даже без элемента «задачи», все равно могут являться персональными данными, затрагивающими права и интересы человека. Например, спутниковая система навигации, которая используется исключительно в целях обеспечения эффективности работы диспетчерской службы такси или службы доставки, может содержать персональные данные, так как данные о местонахождении потенциально могут быть использованы для мониторинга за поведением и передвижением водителей.

Группой, по-видимому, было оставлено пространство для маневров при рассмотрении того, что может являться персональными данными, чтобы со временем сузить или расширить это понятие.

Также требует освещения вопрос, рассмотренный Группой в анализе, касающийся требования идентификации субъекта данных. С этой точки зрения наблюдается единая позиция большинства стран. Ни один из законов не требует, чтобы лицо действительно было идентифицировано. Они либо оставляют такую возможность, используя термин identifiable (поддающийся идентификации), или конкретизируют, что данные являются персональными данными, если по ним можно идентифицировать субъекта персональных данных, либо с их помощью субъект персональных данных поддается идентификации. Таким образом, даже малейшая возможность идентификации лица может быть достаточной для того, чтобы отнести данные к персональным данным.

В то же время ни один из этих законов не требует, чтобы субъекта персональных данных можно было напрямую идентифицировать по этим данным. И хотя почти половина официальных определений

персональных данных ничего не говорят на этот счет, многие все же констатируют, что возможность даже косвенной идентификации субъекта является достаточной для того, чтобы их защищать. Это, по сути, означает, что данные, находящиеся в чьем-либо распоряжении, даже если они никого не идентифицируют, подлежат обращению как с персональными данными ровно до тех пор, пока они в сочетании с другой доступной информацией могут использоваться для идентификации их субъекта. Стоит понимать, что определение того, насколько субъект персональных данных поддается идентификации, может сильно зависеть от текущих обстоятельств, и то, что не поддается идентификации сегодня, может ей поддаваться уже через несколько лет, что, в свою очередь, может перевести такие данные в категорию персональных данных.

В качестве примера, предложенного Группой, приводится газетная статья о преступлении, в которой раскрываются определенные подробности преступления, но не называется ничьих имен. Поскольку имеется общедоступная информация — будь то информация из судебных протоколов или статьи из других газет, — имеется возможность установить личности задействованных лиц. Таким образом, по мнению Группы, даже если статья не указывает данные участников, все равно будет считаться, что в ней содержатся персональные данные.

1.1.3. Субъекты отношений в области обеспечения конфиденциальности персональных данных

Пункт (а) ст. 2 Директивы 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных определяет субъекта данных как лицо, которое может быть определено (прямо или косвенно, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности). Как отмечалось выше, проект Регламента дополняет это определение, конкретизируя перечень идентификаторов, дополнив его именем субъекта персональных данных, сведениями о месте его нахождения и онлайн-идентификаторами (id). В российском законе данный термин поясняется косвенно через определение персональных данных.

Проектом Директивы устанавливаются различия между субъектами данных. Отдельными категориями выделяются подозреваемые

в подготовке или совершении уголовного преступления, лица, осужденные за уголовные преступления, жертвы и потенциальные жертвы уголовного преступления, третьи стороны по уголовным преступлениям (свидетели и лица, которые могут представить информацию по правонарушению), а также лица, которых нельзя отнести ни к одной из перечисленных выше категорий.

Права субъекта персональных данных обеспечиваются предоставлением ему юридической возможности контролировать обращение со своими данными. Очевидно, что права субъекта данных корреспондируют обязанностям и ответственности операторов и обработчиков, поэтому будут рассмотрены совместно.

Пункт (d) ст. 2 Директивы 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных определяет оператора данных как физическое или юридическое лицо, государственный орган, агентство или любой другой орган, который самостоятельно или совместно с другими определяет цели и способы обработки персональных данных; когда цели и способы обработки определены законодательством или подзаконными актами на национальном уровне или уровне ЕС, оператор или конкретные критерии его назначения могут быть установлены национальным законодательством или законодательством ЕС.

Пункт (e) ст. 2 Директивы 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных устанавливает, что «обработчик» означает физическое или юридическое лицо, государственный орган, агентство или любой другой орган, который обрабатывает персональные данные от имени оператора.

Пункт (g) ст. 2 Директивы 95/46/ЕС закрепляет, что под получателем персональных данных следует понимать физическое или юридическое лицо, государственный орган, агентство или любой другой орган, являющийся или не являющийся третьим лицом, которому раскрывают данные; несмотря на это, органы власти, которые могут получать данные в рамках частного запроса, не рассматриваются как получатели.

Пункт (g) ст. 2 Директивы 95/46/ЕС определяет «третье лицо» как физическое или юридическое лицо, государственный орган, агентство или любой другой орган, который не является субъектом данных, оператором, обработчиком и лицом, управомоченным об-

рабатывать данные под прямым руководством оператора или обработчика.

Права субъекта данных, обязанности оператора и обработчика

Статья 17 Директивы 95/46/ЕС устанавливает, что оператор должен осуществлять надлежащие технические и организационные меры для защиты персональных данных от случайного или неправомерного разрушения либо случайной потери, изменения, несанкционированного раскрытия или доступа, в частности, когда обработка включает передачу данных по сети, и от всех иных неправомерных форм обработки.

Пункт 2 ст. 17 Директивы 95/46/ЕС устанавливает, что оператор должен, когда обработка осуществляется от его имени, выбирать обработчика, предоставляющего достаточные гарантии в отношении мер технической безопасности и организационных мер, регулирующих осуществляемую обработку, и должен обеспечить соблюдение этих мер.

Проект Регламента предусматривает получение персональных данных не только от субъекта персональных данных, право на доступ субъекта к собранным персональным данным, право субъекта на исправление и удаление его персональных данных. Проект Регламента устанавливает, что оператор обработки данных обязан стереть персональные данные без неоправданной задержки. Проект Регламента также устанавливает право на мобильность персональных данных.

Проектом Регламента субъект персональных данных наделяется правом возразить на аргументированных основаниях в отношении обработки своих персональных данных. Оператор обработки данных должен прекратить такую обработку, если не докажет, что имеются законные основания, которые выше интересов и аргументов субъекта персональных данных.

Оператор обработки данных обязуется согласно проекту Регламента обеспечивать получение однозначного согласия субъекта персональных данных на обработку его данных. Причем субъект данных должен иметь право отозвать согласие в любое время. Какое бы согласие ни было необходимо для обработки данных, проект Регламента указывает, что оно должно быть дано однозначно, а не подразумеваться.

Оператор должен обеспечить необходимые технические и организационные меры в соответствии с проектом Директивы 95/46/ЕС таким образом, чтобы гарантировать защиту прав субъекта данных.

Оператору следует выбирать обработчика исходя из достаточности гарантий при осуществлении технических и организационных мер, соответствующих требованиям проекта Директивы и обеспечивающих защиту персональных данных.

Оператор обработки персональных данных должен предоставлять субъекту персональных данных сведения о том, где и когда его персональные данные были собраны. В дополнение к указанным сведениям оператор обработки данных должен предоставить субъекту персональных данных информацию о целях обработки персональных данных, о получателях или категориях получателей персональных данных, уведомлять о намерениях передачи персональных данных за пределы Европейского союза или в международную организацию, а также информировать о наличии права субъекта персональных данных обращаться к оператору с просьбой исправить или удалить персональные данные, ограничить или исключить их обработку, обращаться в уполномоченный надзорный орган и т.д.

Отметим при этом, что проект Директивы предусматривает право государств — членов ЕС принимать законодательные меры, отлагающие, ограничивающие или опускающие обязательства по предоставлению информации субъекту данных в той степени и так долго, как, к примеру, частичное или полное ограничение прав субъекта данных является необходимым и соразмерным мерам в демократическом обществе, с должным вниманием к законным интересам соответствующего человека, включая случаи:

1) исключения препятствий по официальным или юридическим запросам, расследованиям или процедурам;

2) исключения нанесения ущерба при предотвращении, обнаружении, расследовании и судебном преследовании уголовных преступлений или для исполнения уголовных наказаний;

3) защиты общественной безопасности;

4) защиты национальной безопасности;

5) защиты прав и свобод других лиц.

При этом государствам — членам ЕС предоставляется право определить категории обработки данных, которые могут полностью или частично подпадать под перечисленные выше категории.

Проект Регламента устанавливает, что по общему правилу обработка персональных данных не требует идентификации. Так, если цели, с которыми оператор обработки персональных данных обраба-

тывает данные, не требуют идентификации субъекта персональных данных оператором, то оператор не должен запрашивать дополнительную информацию и осуществлять дополнительную обработку персональных данных.

Обработчик данных обязуется обеспечить письменное уведомление субъекта данных о любом отказе или об ограничении доступа, о причинах отказа и о возможностях его обжалования в надзорном или судебном органе.

Проект Регламента предусматривает также право субъектов персональных данных подать жалобу в надзорный орган, право юридических лиц и субъектов персональных данных на судебную защиту против надзорного органа, право субъекта персональных данных подать в суд на оператора и обработчика персональных данных, право любой персоны на компенсацию за несоответствующую обработку принадлежащих ей персональных данных.

1.1.4. Ответственность за нарушения в области персональных данных и запрет на передачу данных третьим лицам

В Европейском союзе установлена ответственность как за раскрытие персональных данных неограниченному кругу лиц, так и за раскрытие данных конкретным третьим лицам (ст. 16, 17 Директивы 95/46/ЕС), а также предусмотрена ответственность за непринятие мер по защите персональных данных (ст. 23 Директивы 95/46/ЕС).

Статья 16 Директивы 95/46/ЕС устанавливает принципиальное требование конфиденциальности обработки персональных данных. Любое лицо, действующее под руководством оператора или обработчика, включая самого обработчика, которое имеет доступ к персональным данным, не может их обрабатывать, кроме как по поручению оператора, если оно не обязано это делать по закону.

Статья 17 Директивы 95/46/ЕС устанавливает, что оператор должен осуществлять надлежащие технические и организационные меры для защиты персональных данных от случайного или неправомерного разрушения, либо от случайной потери, изменения, несанкционированного раскрытия или доступа, в частности, когда обработка включает передачу данных по сети, и от всех иных неправомерных форм обработки.

Проект Регламента устанавливает запрет передачи персональных данных третьим лицам, осуществляющим предпринимательскую дея-

тельность. Кроме того, устанавливается, что доступ к персональным данным не продается и не предоставляется по подписке.

1.1.5. Режим защиты персональных данных при обработке больших данных, позволяющих при сопоставлении получать персональные данные

Данная сфера правоотношений не регулируется специальными нормами права. Между тем она является предметом особого внимания европейских регуляторов. Так, 16 сентября 2014 г. Рабочей группой по защите физических лиц при обработке персональных данных WP29 было опубликовано Заявление EC14/EN WP 221 о влиянии развития больших данных на защиту физических лиц в отношении обработки их персональных данных. В частности, указывается, что вызовы, бросаемые технологиями «больших данных», требуют инновационного подхода к толкованию и применению базовых принципов законодательства о персональных данных, а также их дальнейшего совершенствования, хотя, по их мнению, на данном этапе рано говорить о том, что эти принципы абсолютно не действуют в новых реалиях.

В рамках проекта новых Рекомендаций Y.3600 МСЭ-Т «Требования и технические возможности использования облачных вычислений для обработки больших данных» (далее — Рекомендации) при определении требований, технических возможностей и вариантов использования облачных вычислений для обработки больших данных не устанавливаются специфические требования к защите персональных данных при обработке больших данных в облачной среде, однако определяется конкретный субъект, который обеспечивает защиту всех данных, в том числе персональных данных, в целом при обработке больших данных в облачной среде.

Таким субъектом является провайдер облачного сервиса / провайдер инфраструктуры или приложений для анализа больших данных.

Рекомендации устанавливают, что провайдер облачного сервиса / провайдер инфраструктуры или приложений для больших данных обеспечивает защиту данных таким образом, что защищенные данные не будут собираться, храниться ненадлежащим лицом и передаваться ненадлежащему лицу.

При этом Рекомендации не определяют, кто является ненадлежащим лицом, в связи с чем однозначно сделать вывод о том, что Рекомендации запрещают передачу данных третьим лицам, нельзя.

При установлении требования к анализу данных в облачной среде Рекомендации устанавливают рекомендательную (необязательную) норму, чтобы провайдер облачного сервиса / провайдер приложений для больших данных обеспечивал анализ поведения пользователей. Это включает анализ информации, связанной с пользователями, собранной в реальном времени, в том числе информации о поведении пользователей, средовой информации и проанализированной информации из накопленных о пользователе сведений в хранилище данных провайдера облачного сервиса / провайдера приложения для больших данных. При этом сбор информации должен осуществляться на основании предварительно данного согласия пользователя.

Рекомендации устанавливают следующие обязательные требования к безопасности и защите данных:

1) провайдер облачного сервиса / провайдер инфраструктуры больших данных должен обеспечивать защиту данных при сборе данных, при хранении данных, при передаче данных и обработке данных с помощью механизмов безопасности;

2) провайдер облачного сервиса / провайдер приложения для больших данных должен удалять связанные данные и аналитические результаты в соответствии с требованиями клиента облачного сервиса или по запросу клиента облачного сервиса.

Рекомендации устанавливают следующие факультативные требования к безопасности и защите данных:

1) провайдер облачного сервиса может поддерживать возможность имплементации политики защиты и безопасности данных и аналитических результатов клиента облачного сервиса;

2) провайдер облачного сервиса / провайдер инфраструктуры больших данных может обеспечивать резервирование данных и ведение журнала транзакций.

Технические возможности облачных вычислений по обеспечению безопасности и защиты данных при обработке больших данных включают следующее:

1) контроль доступа, что означает возможность управления правами сторон по контролю или влиянию на связанную с ними информацию;

2) контроль политики, что означает возможность для управления политикой защиты данных и безопасности;

3) безопасность данных, что означает возможность применять различные механизмы безопасности, связанные с хранением, сетями

и сервисами, в том числе административные, операционные и технические меры.

1.1.6. Регулирование порядка анализа результатов обработки данных (метаданных)

В ЕС уделяется особое внимание регулированию обработки «метаданных» (так называемых «информации об информации»): данных о трафике, геолокационных данных и т.п.

В частности, 8 апреля 2014 г. Суд ЕС вынес решение по объединенным делам C-293/12 и C-594/12, отменив Директиву 2006/24/ЕС Европейского парламента и Совета от 15 марта 2006 г. о сохранении данных, генерируемых или обрабатываемых в ходе оказания общедоступных услуг электронной коммуникации или функционирования публичных коммуникационных сетей (так называемая Data Retention Directive). Данная Директива, в сущности, распространяла свое действие на обработку «данных о данных», т.е. метаданных. Основанием для признания Директивы не имеющей юридической силы с даты ее принятия послужило то, что содержание Директивы фактически противоречит важному принципу европейского права: ограничение основополагающих прав граждан допустимо лишь при условии соблюдения принципа пропорциональности[4]. Таким образом, расширенный сбор и долгосрочное хранение метаданных были признаны незаконными.

Также ограничены сроки хранения — 6 месяцев для поисковых запросов[5] — и установлено требование об обеспечении самоуничтожения данных по прошествии определенного срока техническими средствами (privacy by design).

1.1.7. Правовое обеспечение защиты данных

Если обобщить положения нормативных правовых актов, то ими устанавливаются ограничения на сбор данных: ex ante и ex post.

Положения ex ante устанавливают необходимость уведомления о целях, для которых необходима передача данных, а также согласова-

---

[4] См. подробнее: *Тарасов Д.А.* Суд Евросоюза отменил обязанность провайдеров хранить сведения о коммуникациях клиентов. URL: http://lexdigital.ru/2014/110/.

[5] Opinion 1/2008 on data protection issues related to search engines. EU Article 29 Data Protection Working Party, 00737/EN WP 148. April 2008.

ние любого дальнейшего использования данных (исключая случаи, когда оно осуществляется с согласия субъекта данных или иным образом в соответствии с действующим законодательством и соответствуют четким целям). Положения ex post нацелены на постоянный контроль обеспечения надежности данных (в том числе уведомление о факте обработки таких данных, о доступе к ним и о возможности внесения исправлений в поврежденные/неточные сведения личного характера). В эту же категорию следует отнести группу норм, устанавливающих порядок хранения и обработки данных, включая процедуры защиты от утери уничтожения и несанкционированного раскрытия. Любое использование или раскрытие должно быть зарегистрировано, а в случае любого несанкционированного использования или раскрытия субъект данных должен быть уведомлен об этом.

Итак, к превентивной мере можно отнести требование ст. 17 Директивы 95/46/ЕС к оператору по осуществлению надлежащих технических и организационных мер для защиты персональных данных от случайного или неправомерного разрушения либо от случайной потери, от изменения, несанкционированного раскрытия или доступа, в частности, когда обработка включает передачу данных по сети, и от всех иных неправомерных форм обработки.

Далее, превентивной мерой являются требования раздела IX Директивы 95/46/ЕС, касающиеся обязательств уведомить надзорный орган. Так, согласно ст. 18 оператор или его представитель, если таковой имеется, должен уведомить надзорный орган перед осуществлением любой полностью или частично автоматизированной операции по обработке или последовательности таких операций, предназначенных, чтобы служить одной цели или нескольким связанным целям (данное требование действует с исключениями).

К информации, которая предоставляется при уведомлении, относятся, как минимум:

1) наименование и адрес оператора и его представителя, если таковой имеется;

2) цель или цели обработки;

3) описание категории или категорий субъектов данных и данных или категорий данных, относящихся к ним;

4) информация о получателях или о категориях получателей, которым могут раскрываться данные;

5) информация о предполагаемой передаче данных в третьи страны;

6) общее описание, позволяющее осуществить предварительную оценку целесообразности мер, принятых для обеспечения безопасности обработки.

Статья 20 Директивы 95/46/ЕС также описывает такую меру, как предварительная проверка. Государства — члены ЕС определяют операции по обработке, которые могут создавать конкретные риски для прав и свобод субъектов данных, и проверяют контролируемость и прогнозируемость хода проведения таких операций. Такие предварительные проверки осуществляются надзорным органом вслед за получением уведомления от оператора или служащего, занимающегося защитой данных, который в случае сомнения должен проконсультироваться с надзорным органом.

Статьей 22 Директивы 95/46/ЕС оговариваются средства защиты прав. Так, без ущерба для какого-либо административного средства правовой защиты, которое может предусматриваться до обращения в судебный орган, inter alia, обеспечивается право любого лица на судебную защиту от любого нарушения прав, гарантированных ему национальным законодательством, применимым к осуществляемой обработке.

При этом устанавливается, что любое лицо, которое понесло ущерб в результате неправомерной операции по обработке или какого-либо иного действия, имеет право получить компенсацию от оператора за понесенный ущерб. Оператор может быть полностью или частично освобожден от такой ответственности, если он докажет, что не несет ответственности за событие, вызвавшее ущерб.

Кстати, новые правила позволят пользователям требовать компенсации, например, за незаконное предоставление или за потерю их данных (например, в результате несанкционированной их обработки). Более того, пострадавшие смогут выступать в группе и организовать коллективный иск.

Более жесткие санкции — одно из самых важных изменений. По новым правилам штрафы могут достигать 100 млн евро или 5% дохода (в зависимости от того, какая сумма будет выше), что значительно превышает текущие суммы (в Великобритании максимальное наказание в настоящее время составляет 500 тыс. фунтов).

При трансграничной передаче данных, выходящей за рамки стандартной процедуры, требуется получение прямого разрешения субъ-

екта данных. Форма получения согласия не регламентируется, оно лишь должно быть однозначным. Кроме того, закрепление гарантий защиты данных в соглашении имеет место в рамках процедур трансграничной передачи данных Model Clauses, когда конкретные гарантии закреплены стандартными договорными условиями.

1.1.8. Регулирование вопроса о наследовании прав на персональные данные

На нормативно-правовом уровне данный вопрос не урегулирован. Между тем в ЕС развит рынок услуг, связанных с менеджментом персональных данных, в том числе в случае смерти субъекта данных. Так, под цифровым наследованием понимается процесс передачи персональных данных в цифровом виде, цифровых активов и прав бенефициарам[6]. Процесс состоит из составления перечня существующих цифровых активов и прав, включения их в наследственную массу (по желанию завещателя) и установления порядка реализации прав на них у будущих наследников. Такими активами могут быть аккаунты в Google, Apple, Microsoft и Facebook, на различных форумах, в блогах, на личных веб-сайтах и реквизиты для дистанционного банковского обслуживания. В отличие от физических активов, цифровые активы эфемерны и подвержены постоянному изменению. Цифровое наследование может представлять собой проблему для наследников данных в силу сложной структуры, даже запутанности, и может повлечь для них нежелательные правовые последствия. С учетом того что пользователи могут иметь в среднем около 25 аккаунтов, ситуация действительно сложна с точки зрения как составления перечня активов, так и дальнейшей реализации наследственных прав[7]. В данном случае имеет место нотариальный цифровой менеджмент. Существуют также различные опции, согласуемые оператором данных, провайдерами информационных ресурсов, субъектом данных, касательно порядка обращения с данными, порядка и условий их предоставления, направления иным лицам и иные действия, которые тоже условно относятся к менеджменту персональных данных, в сущности — к управлению

---

[6] *Niekerk A.J. van*. The Strategic Management of Media Assets; A Methodological Approach. Allied Academies, New Orleans Congress, 2006.

[7] *Rosen R.J.* The Government Would Like You to Write a 'Social Media Will' // The Atlantic. Retrieved 4 June 2013.

правами на персональные данные (в ряде случаев осуществляемому доверенными лицами).

1.1.9. Уполномоченный орган по защите субъектов персональных данных и его функции

Статья 28 действующей Директивы 95/46/ЕС устанавливает, что каждое государство — член ЕС предусматривает, что один или несколько государственных органов ответственны за контроль применения на их территории норм, регулирующих порядок обработки персональных данных. Эти органы имеют полную независимость при осуществлении возложенных на них функций.

В каждой стране, входящей в состав Европейского союза, должно быть не менее одного независимого надзорного органа по защите данных. Предполагается, что эти органы будут сотрудничать между собой и с Европейской комиссией в целях реализации Регламента. Данные органы обеспечиваются соответствующими государствами кадровыми, техническими и финансовыми ресурсами, помещениями и инфраструктурой, необходимой для эффективного выполнения своих обязанностей, за счет государственного бюджета, однако такое обеспечение не должно влиять на самостоятельность принимаемых решений и независимость надзорного органа по защите.

В соответствии с п. 6 ст. 28 Директивы 95/46/ЕС независимо от национального права, применимого к соответствующей обработке, каждый надзорный орган должен иметь возможность осуществлять на территории своего государства — члена ЕС полномочия, предоставленные ему в соответствии с Директивой 95/46/ЕС. При этом каждому такому органу может быть предложено осуществлять свои полномочия органом другого государства — члена ЕС.

Независимые надзорные органы по защите данных в соответствии с проектом Регламента получают больше полномочий, чтобы иметь возможность лучше контролировать соблюдение правил Европейского союза внутри собственной страны.

Кроме контроля реализации проекта Регламента, к их задачам отнесены:

1) повышение осведомленности общественности о рисках, правилах, гарантиях и правах в отношении обработки персональных данных, при этом особое внимание должно уделяться обработке персональных данных детей;

2) разработка рекомендаций для национальных парламентов, правительств и других учреждений, органов по совершенствованию законодательных и административных мер, связанных с защитой прав граждан и их свобод в отношении обработки персональных данных;

3) работа с запросами субъектов персональных данных и при необходимости сотрудничество с надзорными органами других государств — членов Европейского союза в целях подготовки ответов на запросы;

4) расследования, инициированные жалобами субъектов персональных данных, органов власти, организаций, информирование заявителей о ходе такого расследования, а также самостоятельные расследования по вопросам защиты персональных данных;

5) сотрудничество, в том числе обмен информацией, и оказание взаимной помощи другим надзорным органам с целью обеспечения согласованности и применения Регламента;

6) мониторинг развития информационно-коммуникационных технологий, коммерческой практики и иных событий, оказывающих влияние на защиту персональных данных;

7) определение и утверждение требований к защите персональных данных;

8) содействие созданию механизмов сертификации защиты данных, пломб защиты данных и специальных знаков;

9) проведение регулярного мониторинга подтверждения проведенных сертификаций и др.

Одновременно каждое государство — член Европейского союза должно обеспечить ряд следственных полномочий собственного надзорного органа, необходимых для защиты персональных данных, полномочий по выдаче предписаний по устранению правонарушений, консультативных полномочий. Данные органы будут наделены правом наложения штрафов на компании, нарушающие законодательство Европейского союза по защите персональных данных. При принятии решения о размере административного штрафа в каждом конкретном случае необходимо учитывать сущность, тяжесть и продолжительность нарушения, умышленный или неосторожный характер правонарушения, число субъектов персональных данных, пострадавших от правонарушения, меры, принимаемые оператором или обработчиком персональных данных для уменьшения ущерба субъектов персональных данных, все предыдущие нарушения оператора

персональных данных, любые другие отягчающие или смягчающие вину правонарушителя факторы.

Надзорные органы взаимодействуют друг с другом в режиме, необходимом для исполнения своих обязанностей, в частности, обмениваясь всей полезной информацией.

Кроме того, в ЕС можно выделить совещательный тип взаимодействия надзорных органов. Так, на основании ст. 29 Директивы 95/46/ЕС функционирует достаточно влиятельная Рабочая группа по защите физических лиц при обработке персональных данных. Рабочая группа состоит из представителя надзорного органа или органов, назначенного от каждого из государств — членов ЕС, и представителя органа или органов, созданных в интересах институций и органов ЕС, а также представителя Европейской комиссии.

Европейский инспектор по защите данных (European Data Protection Supervisor) также является лицом, уполномоченным на защиту персональных данных в Европейском союзе[8] (далее — инспектор). Деятельность инспектора регламентирована разделом 8 Регламента от 18 декабря 2000 г. № 45/2001 «О защите физических лиц при обработке персональных данных, осуществляемой учреждениями и органами сообщества, и о свободном обращении таких данных».

Акты, принимаемые инспектором, в сущности, относятся к категории так называемого гибкого права (soft law), которые, хотя и не обладают характеристиками нормативно-правовых актов, в достаточной степени оказывают влияние на формирующиеся правоотношения. Инспектором могут быть использованы следующие инструменты: официальные отчеты, выражающие позицию инспектора по определенному вопросу; мнения; результаты проведенных исследований, например, позиционный документ о передаче персональных данных в третьи страны (The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies) от 14 июля 2014 г.)[9], или, например, Мнение-рекомендации инспектора (EDPS Recommendations on the Directive for Data Protection in the Police and

---

[8] Официальный сайт Европейского инспектора по защите данных (European Data Protection Supervisor). URL: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/cache/offonce?lang=en.

[9] The transfer of personal data to third countries and international organisations by EU institutions and bodies, 14 July 2014. URL: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Papers

Justice Sectors[10]) от 28 октября 2015 г. На официальном сайте инспектора по защите данных ЕС представлены все материалы по множеству актуальных вопросов.

Необходимо также отметить деятельность Европейского агентства по сетевой и информационной безопасности — ENISA (European Network and Information Security Agency) (агентство ЕС, созданное с целью повышения эффективности функционирования внутреннего рынка, оно выступает в роли консультанта и центра передовых технологий в сфере сетевой и информационной безопасности для стран — членов ЕС и институтов ЕС и содействует развитию связей между странами — членами ЕС, институтами ЕС, хозяйствующими субъектами и частным бизнесом).

При возникновении споров надзорных органов окончательное мнение по существу спорных вопросов будет формировать Европейский совет по защите данных. Данный Совет учреждается во исполнение проекта Регламента. Планируется, что его состав будет представлен руководителями национальных надзорных органов по защите персональных данных и инспектором Совета.

1.1.10. Регулирование таргетированной (адресной, основанной на персональных данных и запросах лица) рекламы

Согласно ст. 19 проекта Регламента субъект персональных данных наделяется правом возразить на аргументированных основаниях в отношении обработки своих персональных данных. Оператор обработки данных должен прекратить такую обработку, если не докажет, что имеются законные основания, которые выше интересов и аргументов субъекта персональных данных. При обработке персональных данных в целях прямого маркетинга субъект персональных данных должен иметь право возразить в любой момент против обработки своих персональных данных. Информация о данном праве должна предоставляться субъекту персональных данных предельно понятно и отдельно от любых других сведений. Если субъект персональных данных против обработки собственных персональных данных в целях прямого

[10] EDPS recommendations on the Directive for data protection in the police and justice sectors. URL: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/OpinionsC

маркетинга, персональные данные больше не могут обрабатываться в указанных целях.

1.1.11. Порядок трансграничной передачи персональных данных

Статьей 25 Директивы не в качестве исключения, а в качестве правила устанавливается, что государства — члены ЕС могут разрешить передачу в третью страну персональных данных, только если соответствующая третья страна обеспечивает достаточный уровень защиты. Необходимо оговориться о критериях и порядке оценки уровня защиты при составлении перечня стран для беспрепятственного обмена данными согласно Директиве 95/46/ЕС.

Согласно п. 2 ст. 25 достаточность уровня защиты, предоставляемого третьей страной, оценивается в свете всех обстоятельств, связанных с операцией по передаче или с последовательностью операций по передаче данных. Особое внимание уделяется характеру данных, цели и продолжительности предлагаемой операции или операций по обработке, стране происхождения и стране конечного назначения, законодательным правилам — как общим, так и отраслевым, — действующим в соответствующей третьей стране, а также профессиональным правилам и мерам безопасности, соблюдаемым в этой стране.

Однако иных нормативных документов, разъясняющих вышеуказанное положение об определении «адекватности» или «неадекватности» стран для передачи персональных данных, не принято. Методологические критерии для оценки режима передачи персональных данных изложены в документе рекомендательного характера, адресованном непосредственно публичным органам власти по вопросу понимания органами ЕС и странами — участницами ЕС критериев определения «адекватности» или «неадекватности» стран при передаче персональных данных, содержащихся в Директиве 95/46/ЕС и в других международных правовых актах. Рабочая группа по защите частных лиц в связи с обработкой персональных данных, созданная на основании Директивы 95/46/ЕС (ст. 29), издала руководящие принципы в помощь осуществления оценки:

1) WP 4 (5020/97) «Рабочий документ, содержащий первые ориентиры относительно передачи персональных данных третьим странам — возможные пути продвижения в оценке соответствия», документ для обсуждения, принятый Рабочей группой 26 июня 1997 г.;

2) WP 7 (5057/97) «Оценка саморегулирования отрасли: в каких случаях она вносит значимый вклад в уровень защиты данных в третьей стране?», рабочий документ, принятый Рабочей группой 14 января 1998 г.;

3) WP 9 (3005/98) «Предварительные мнения относительно использования договорных положений в контексте передачи персональных данных третьим странам», рабочий документ, принятый Рабочей группой 22 апреля 1998 г.;

4) WP 12 «Передачи персональных данных третьим странам: применение статей 25 и 26 Директивы ЕС о защите данных», рабочий документ, принятый Рабочей группой 24 июля 1998 г.[11]

Если обобщить критерии признания стран как предоставляющих адекватный уровень защиты данных, то можно заключить, что к таковым может быть отнесено государство, в котором действуют соответствующие нормы права, сформирован уполномоченный орган, а также обеспечивается правовая защита граждан в сфере персональных данных.

Следует отметить, что мнения Рабочей группы фактически легализуются в результате принятия Европейской комиссией решений по квалификации уровня защиты данных в тех или иных странах в соответствии с рекомендуемыми критериями. Решение, основанное на документе рекомендательного характера, становится правовым актом, имеющим юридическую силу (к примеру, Решение 11/2011 об адекватности уровня безопасности персональных данных в Новой Зеландии от 4 апреля 2011 г. и т.д.). Критерии «адекватности» сформировали важную отправную точку для принятия решений Европейской комиссии по адекватности режимов третьих стран.

В результате проведенной оценки составляется перечень государств, обеспечивающих адекватный уровень защиты данных согласно

---

[11] WP 4 (5020/97) «Рабочий документ, содержащий первые ориентиры относительно передачи персональных данных третьим странам — возможные пути продвижения в оценке соответствия» от 26 июня 1997 г.; WP 7 (5057/97) «Оценка саморегулирования отрасли: в каких случаях она вносит значимый вклад в уровень защиты данных в третьей стране?» от 14 января 1998 г.; WP 9 (3005/98) «Предварительные мнения относительно использования договорных положений в контексте передачи персональных данных третьим странам» от 22 апреля 1998 г.; WP 12 «Передачи персональных данных третьим странам: применение статей 25 и 26 Директивы ЕС о защите данных» от 24 июля 1998 г. // Интернет-источник: URL: europa.eu.int/comm/internal_markt/en/media.dataprot/wpdocs/wp12/en.

но Директиве 95/46/ЕС. Оговаривается, что государства — члены ЕС и Европейская комиссия должны уведомлять друг друга о случаях несоответствия уровня защиты данных в стране декларируемому. Причем в случае последующего выявления недостаточного уровня защиты данных при их обработке Европейской комиссией государства — члены ЕС должны принять меры по предотвращению любой передачи данных того же типа в соответствующую третью страну. Либо, напротив, третья страна в силу ее внутреннего законодательства или международных обязательств может быть признана Европейской комиссией как обеспечивающая достаточный уровень защиты.

Между тем Директивой устанавливается ряд исключений из описанного общего принципа передачи данных только в страны, уровень защиты данных в которых признан адекватным (ст. 26).

Прежде всего стоит перечислить фиксированные исключения, согласно которым передача или последовательность передач персональных данных в третью страну, не обеспечивающую достаточный уровень защиты по смыслу Директивы, может совершаться при условии, что:

1) субъект данных однозначно дал свое согласие на предполагаемую передачу данных;

2) передача необходима для исполнения договора между субъектом данных и оператором или для осуществления преддоговорных мер, принимаемых по просьбе субъекта данных;

3) передача необходима для заключения или исполнения договора, заключенного в интересах субъекта данных между оператором и третьим лицом;

4) передача необходима или требуется на основании закона в связи с особой общественной важностью данных либо для установления, осуществления или защиты правовых требований;

5) передача необходима в целях защиты жизненно важных интересов субъекта данных;

6) или передача осуществляется из реестра, который в соответствии с законами или подзаконными актами предназначен для предоставления информации общественности и который открыт для доступа как общественности в целом, так и любого лица, могущего продемонстрировать законный интерес, в той мере, в какой в конкретном случае выполняются условия, установленные законодательством о доступе.

Но особую значимость в условиях принятия и опыта применения положений Директивы сыграли оговорки о возможных средствах обеспечения безопасности данных при передаче за пределы ЕС.

Так, в соответствии с п. 2 ст. 26 государство — член ЕС может разрешить передачу или последовательность передач персональных данных в третью страну, которая не обеспечивает достаточный уровень защиты, когда оператор представляет достаточные гарантии в отношении защиты частной жизни и основных прав и свобод физических лиц; такие гарантии могут, в частности, следовать из соответствующих условий договора. При этом Европейская комиссия может признать отдельные стандартные договорные условия в качестве достаточных гарантий достаточной защиты персональных данных.

Данные оговорки действительно обладают колоссальной значимостью, в том числе ввиду следующих обстоятельств. Несмотря на то что Соединенные Штаты Америки, как и Европейский союз, декларируют аналогичные принципы защиты персональных данных, практикуемые ими подходы регулирования отношений и защиты прав весьма отличны. А именно, в Соединенных Штатах Америки имеет место секторальный подход, базирующийся на комбинации законодательного регулирования, иных форм публичного регулирования и саморегулирования. Между тем подход защиты персональных данных, практикуемый Европейским союзом, подразумевает по большей части законодательное регулирование указанной сферы отношений. При этом на уровне закона устанавливается необходимость создания независимых государственных органов по защите данных, регистрации баз данных этими учреждениями, а в некоторых случаях — получения предварительного одобрения любой обработки персональных данных. Наличие подобных регулятивных отличий обусловило проблематичность участия американских обработчиков данных в уже сложившихся на тот момент правоотношениях. С принятием Директивы 95/46/ЕС, потребовавшей составления перечня стран, предоставляющих адекватный уровень защиты данных при их обработке, США (как и другие государства, оказавшиеся в аналогичной ситуации), которые не признаны такой страной, могли фактически выпасть из экономических отношений.

В связи с возникшей ситуацией необходимы были поиск нового подхода в международном сотрудничестве, обеспечение условий для преодоления указанных отличий правовых моделей регулирования, а также создание рациональных и экономически эффективных инстру-

ментов, позволяющих американским обработчикам данных соответствовать на достаточном уровне требованиям Директивы. Так, Департаментом торговли США в сотрудничестве с Европейской комиссией был разработан подход, отраженный в так называемых «Принципах защиты конфиденциальности персональных данных» / «Принципах безопасной гавани для тайны частной жизни»[12] (Safe Harbor Privacy Principles, далее — «Принципы», Safe Harbor)[13]. Указанные принципы соответствия требованиям информационной безопасности ЕС были приняты Министерством торговли США и, по сути, являются ответом на Директиву 95/46/ЕС. Будучи инициированы США, они приобрели дееспособность в отношениях по поводу передачи данных с ЕС особой волей ЕС. На тот момент указанное специальное Решение стало разрешением дискуссии между ЕС и США о принципах достаточности уровня защиты персональных данных: в 2000 г. Комиссией ЕС было принято специальное Решение от 26 июля 2000 г. № 2000/520/ЕС[14], в котором описаны условия передачи данных в США. Именно этим документом они признаны как обеспечивающие необходимую защиту.

Итак, соглашение было одобрено в 2000 г., это позволило избежать перерывов в сформировавшихся отношениях, предполагающих обработку данных, а также лишило основания для привлечения к ответственности американских обработчиков, как осуществляющих свою деятельность в нарушение Директивы (так как относились к категории стран с неадекватным уровнем защиты данных). Проведение сертификации обработчиков данных согласно положениям Соглашения Safe Harbor предоставляет гарантии для ЕС в адекватном уровне защиты обрабатываемых данных (в соответствии с Директивой), на более конкретизированном уровне — при их обработке конкретными американскими компаниями, прошедшими сертификацию.

Таким образом, Соглашение Safe Harbor обеспечило удовлетворение интересов обеих сторон. В частности, в случае участия в Программе Safe Harbor американские обработчики данных получали следующие преимущества:

---

[12] Safe Harbor Privacy Principles. URL: http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm

[13] Международное и зарубежное финансовое регулирование: институты, сделки, инфраструктура. В 2 ч. / под ред. А.В. Шамраева. М.: КноРус; ЦИПСиР, 2014. Ч. 2.

[14] Official Journal L 215. 25.08.2000. P. 0007–0047.

1) все 28 государств — членов ЕС придерживаются определенных Европейской комиссией критериев адекватности уровня обработки данных;

2) участвующий в Программе Safe Harbor обработчик данных будет рассматриваться как соответствующий требованиям адекватной обработки данных согласно Директиве;

3) требование о получении предварительного одобрения трансграничной передачи данных будет отменено в отношении участвующего в Программе Safe Harbor обработчика или будет осуществляться автоматически;

4) требования Соглашения возможны к исполнению с минимальными ресурсозатратами, экономически эффективны, что особенно значимо для малых и средних предприятий.

Лицо, передающее данные американскому обработчику, приобретало гарантии соответствия данного обработчика критериям адекватной защиты данных только в том случае, если он участвует в Программе Safe Harbor, т.е. в данном случае осуществляется привязка к соответствию стандартов обработки данных уровню безопасности, обеспечиваемому конкретным лицом, а не всем государством. Проверку участия конкретного обработчика можно было осуществить путем просмотра списка Safe Harbor организаций, который находится в публичном доступе на сайте Министерства торговли США[15].

Наряду со странами — членами ЕС члены Европейского экономического союза (Исландия, Лихтенштейн и Норвегия) также признавали организации, сертифицированные по программе Safe Harbor, как обеспечивающие достаточный уровень конфиденциальности для передачи данных из своих стран в США. Швейцария заключила почти аналогичное соглашение (соглашение Safe Harbor между Швейцарией и США) с Министерством торговли США для передачи данных из Швейцарии в США на законном основании. Кроме того, разрешена свободная передача данных из ЕС в ряд других стран (например, в Канаду и Аргентину), принявших всесторонние законы о конфиденциальности данных.

Итак, на протяжении 15 лет обмен данными между ЕС и США регламентировался указанным договором, известным как Соглашение о «безопасной гавани», что позволяло тысячам компаний Европейского

---

[15] URL: http://safeharbor.export.gov/list.aspx

союза и США обмениваться электронными данными, вести бизнес и передавать информацию в упрощенном порядке, без дорогостоящих мер защиты. Но уже после выявления первых чрезвычайных случаев нарушения принципов трансграничной передачи данных высказывались мнения о необходимости приостановлении действия Соглашения Safe Harbor и договора о международной банковской системе обмена информацией и совершения платежей SWIFT[16], который предоставляет США возможность доступа к банковским данным граждан ЕС, изначально Европейским парламентом даже были выдвинуты такие требования[17].

Между тем Федеральная торговая комиссия США (FTC) объявила, что примет меры против американских компаний, которые нарушили европейские законы о конфиденциальности, собирая данные о жителях стран ЕС без их ведома (в пресс-релизе FTC названы 12 американских компаний, включая Apperian, Atlanta Falcons Football Club, Baker Tilly Virchow Krause, BitTorrent, Charles River Laboratories International, DataMotion, DDC Laboratories, Level 3 Communications, PDB Sports, Reynolds Consumer Products Inc., Receivable Management Services Corporation, Tennessee Football, нарушивших договор U.S.–EU Safe-Harbor Agreement при сборе персональных данных), а также начнет переработку принципов разведывательной деятельности США. В частности, комиссия заявила, что вышеуказанные компании вводили в заблуждение людей путем использования просроченных сертификационных знаков для подтверждения законности своей деятельности[18].

Европейская комиссия, в свою очередь, заявила, что Соглашение Safe Harbor не будет приостановлено, однако был выдвинут ряд требований к США[19].

В ноябре 2013 г. Комиссия ЕС изложила меры, которые необходимо принять с целью осуществления дальнейших передач данных

---

[16] *Eecke P. van*. URL: http://www.jdsupra.com/legalnews/europe-eu-commissioner-reding-introduc-85150/; http://europa.eu/rapid/press-release_SPEECH-14-62_en.pdf (пер. Н. Храмцовской) // URL: http://rusrim.blogspot.ru/2013/11/blog-post_15.html.

[17] ЕП требует расторгнуть договоры ЕС с США об обмене данными. URL: http://www.warandpeace.ru/ru/news/view/87751/.

[18] *Мироненко В.* FTC сообщила о санкциях для нарушителей законов ЕС о конфиденциальности // Daily digital digest. URL: http://www.3dnews.ru/797428.

[19] *Baker J.* EU will not suspend safe harbor data privacy agreement with the US // PC World. 2013. No. 11.

между США и ЕС (IP/13/1116)[20]. Ключевым инструментом указанных мер выбрано развитие программы-инструмента Safe Harbor, а также деятельность рабочей группы ЕС–США MEMO/13/1059 по защите персональных данных, которая была создана в июле 2013 г.[21]

Помимо указанных предложений реформирования европейского законодательства о персональных данных, были обозначены 13 направлений совершенствования реализации Программы Safe Harbor, которые требуют значительного финансирования, в связи с этим решение вопроса о действии Соглашения назначено на лето 2014 г. Эти направления фактически являются ответом на выявленные рабочей группой ЕС–США 2013 г. угрозы, несоответствия и риски. Среди них:

блок 1 — прозрачность:

1) политика безопасности должна быть опубликована сертифицированными компаниями в режиме открытого доступа в полном объеме;

2) каждая политика безопасности должна содержать активную ссылку на сайт Министерства торговли США (конкретное место с указанием на действительность сертификации);

3) должны также публиковаться детализированные данные о наличии у сертифицированной компании договорных отношений, связанных с процессом обработки данных;

4) Министерством торговли США должен быть опубликован «черный список» компаний, которые не участвуют в Программе;

блок 2 — правоприменение:

1) проверки на соответствие уровня безопасности данных, обеспечиваемых компанией, принципам Safe Harbor и опубликованной политике безопасности должны проводиться постоянно после получения сертификата (достаточно глубокие ревизии);

2) при выявлении нарушений должна быть запланирована подобная проверка через год;

3) в случае возникновения любых сомнений в безопасности данных Министерство торговли США должно информировать ЕС;

---

[20] European Commission calls on the U.S. to restore trust in EU-U.S. data flows // Пресс-релиз Европейской комиссии от 27 ноября 2013 г. URL: http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

[21] Rebuilding Trust in EU-US Data Flows. COM(2013) 846 final // Документ Европейской комиссии от 27 ноября 2013 г. URL: http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

4) должно быть осуществлено следствие по случаям фальсификации участия в Программе;

блок 3 — процедуры альтернативного разрешения споров:

1) должны активно использоваться процедуры альтернативного разрешения споров, в силу чего в политике безопасности должна присутствовать активная ссылка на соответствующий орган;

2) процедуры альтернативного разрешения споров должны быть доступными и незатратными;

3) Министерство торговли США должно проводить постоянный контроль за реализацией процедур альтернативного разрешения споров;

блок 4 — доступ публичных органов США:

1) в политике конфиденциальности должны подробно указываться положения законодательства США, влияющие на реализацию прав вовлеченных субъектов;

2) исключения из политики конфиденциальности в пользу национальной безопасности должны быть крайне ограниченной мерой, применяемой строго пропорционально реальной необходимости.

Между тем вопреки обозначенным планам и ожиданиям 6 октября 2015 г. высший орган судебной власти Евросоюза признал недействительным существующее законодательство о трансатлантической передаче данных. Европейский суд заключил, что Facebook не обеспечивает адекватную защиту персональных данных жителей ЕС, и постановил провести дальнейшее расследование.

В Европейский суд в Люксембурге обратился пользователь Facebook австрийский юрист Макс Шремс. Он потребовал, чтобы Facebook не передавал его личные данные на серверы в США, так как сеть не может гарантировать защиту этой информации. Свою просьбу он мотивировал тем, что, согласно информации Эдварда Сноудена, такие крупнейшие компании, как Google, Apple, Facebook, сотрудничают с американским Агентством национальной безопасности. Первоначально жалоба была подана в Ирландии, где находится европейская штаб-квартира компании Facebook. Но там иск был отклонен, поэтому австриец обратился к высшей судебной инстанции Евросоюза.

Суд занял принципиальную позицию, сделав вывод, что договор о трансатлантической передаче данных нарушает право европейцев жаловаться на использование их личных данных в коммерческих целях различными мультинациональными компаниями. Защита права

на неприкосновенность личной жизни в США во многом отличается от защиты этого права в Европе.

Таким образом, ответ на жалобу Шремса касается не только Facebook, он затрагивает тысячи других компаний, деятельность которых осуществляется в рамках Соглашения Safe Harbour как инструмента передачи данных на законной основе[22].

Также большие ставки делались на реформирование правозащитных процедур и мер обеспечения гарантий. В частности, планировалось развитие и усиленное использование уже сформированных инструментов взаимной правовой помощи (Mutual Legal Assistance) и отраслевых соглашений по вопросам обмена данными.

Особо рассматривались вопросы Рамочного соглашения IP/10/1661 «О защите информации в области полицейского и судебного сотрудничества»[23]. С 18 ноября 2013 г. США реализуются меры по предоставлению гражданам ЕС права на судебную защиту.

Завершается работа над зонтичным соглашением США и ЕС о защите персональных данных для совместной борьбы с терроризмом от 8 сентября 2015 г. Документ позволит защитить персональные данные, которыми обмениваются полиция, судебные органы и частные компании в ходе расследований.

Зонтичное соглашение в качестве основы полагает всестороннюю структурную высокоуровневую защиту при взаимодействии США и ЕС в сфере правоохранения. Соглашение касается всех персональных данных (например, имена, адреса, досье), которые подвергаются трансграничной передаче между ЕС и США в целях предотвращения, обнаружения, расследования и судебного преследования уголовных преступлений, включая терроризм. Текст соглашения полностью разработан, однако требуется провести ряд процедур для вступления его в силу. В частности, должен быть принят американский закон о компенсациях, затем американские власти публикуют соответствующее решение касательно зонтичного соглашения, которое в итоге утверждается властью ЕС.

---

[22] Европейский суд решил, что Facebook не защищает данные пользователей // Русская служба RFI. Франция. URL: http://informburo.dn.ua/cgi-bin/iburo/start.cgi?info58=7431

[23] Рамочное соглашение IP/10/1661 «О защите информации в области полицейского и судебного сотрудничества».

Основной целью документа является создание одинакового режима: граждане ЕС будут иметь те же самые судебные права, как и американские граждане, в случае правонарушений в сфере персональных данных. В настоящий момент если данные граждан ЕС переданы американским правоохранительным органам и если эти данные неправильно или незаконно обработаны, граждане ЕС — нерезиденты США не могут получить компенсацию в американских судах (в отличие от американских граждан, которые имеют право требовать компенсацию в европейских судах).

На практике этот инструмент может работать следующим образом. Например, имя гражданина ЕС попадает в базу данных как лица, подозреваемого в совершении преступления. В дальнейшем лицо оправдано. Между тем его данные могут находиться в своего рода «черном списке», что препятствует, к примеру, получению визы. Если соглашение будет принято, то гражданин ЕС сможет обратиться с требованием удалить сведения о себе из баз данных и получить компенсацию.

Это соглашение дополняет существующее регулирование правоотношений ЕС и США в сфере персональных данных, создавая четкие, согласованные правила защиты данных и устанавливая высокий уровень защиты, в частности:

1) ограничение на использование данных — персональные данные не могут обрабатываться вне согласованных с субъектом данных целей;

2) любая передача данных за пределы США, в не входящую в ЕС страну или международную организацию должна быть подвергнута предварительному согласованию с компетентным органом страны, которая первоначально передала личные данные;

3) личные данные не могут храниться дольше, чем необходимо;

4) субъект данных должен быть наделен правом получения доступа к своим данным, возможностью инициировать их исправление;

5) в случае нарушения условий защиты информации должно быть направлено уведомление о нарушении компетентному органу и в соответствующих случаях субъекту данных.

В случае если органам власти США необходимо передать данные третьей стране или международной организации, следует получить предварительное согласие правоохранительных органов ЕС, изначально передавших данные.

Также относительно трансграничной передачи данных в ЕС функционирует такой инструмент, как стандартные договорные условия

(Model Clauses). Гарантии, требуемые ч. 2 ст. 26 Директивы, в частности, могут вытекать из соответствующих договорных условий.

В рамках данного положения Европейской комиссией было принято Решение от 15 июня 2001 г. № 2001/497/ЕС «О стандартных договорных условиях относительно передачи персональных данных третьим странам согласно Директиве 95/46/ЕС». Этот документ адресован государствам — членам ЕС и в отличие от принятых ранее непосредственно устанавливает несколько стандартных вариантов-наборов условий для обеспечения адекватного уровня защиты данных. Операторы данных могут выбрать любой из вариантов, но при этом они не имеют права изменять условия или комбинировать отдельные условия либо комплекты.

Стандартные договорные условия становятся действительными для конкретных субъектов с момента их согласования сторонами. При этом они будут обязательными для исполнения не только организациями, являющимися сторонами договора, но и субъектами данных, в частности, в случаях, когда субъекты данных несут ущерб вследствие нарушения положений договора. Условия своим предметом имеют только вопросы защиты данных. Субъекты отношений могут дополнить соглашения иными положениями, в частности, условиями о взаимной помощи в случаях споров с субъектом данных или с контролирующим органом, которые они считают имеющими прямое отношение к договору. Правом, подлежащим к применению (по общему правилу), является законодательство государства — члена ЕС, в котором учрежден экспортер данных (лицо, осуществляющее передачу данных).

Согласно ст. 1 Решения стандартные договорные условия (в случае их согласования сторонами) расцениваются как достаточные гарантии в отношении защиты неприкосновенности частной жизни и основных прав и свобод физических лиц и в отношении осуществления соответствующих прав согласно требованиям, предусмотренным в ст. 26 (2) Директивы.

Резолюции Европейского парламента 2011/2025 (INI) от 6 июля 2011 г. о комплексном подходе к защите персональных данных в Европейском союзе провозгласили преемственность основных принципов Директивы 95/46/ЕС, но при этом — необходимость значительной доработки отдельных норм касательно трансграничной передачи данных[24].

---

[24] См.: Personal data protection in the European. Union European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the Eu-

Итак, что касается проектного внутреннего регулирования в ЕС, то регулированию особенностей передачи персональных данных странам, не входящим в Европейский союз, посвящена отдельная глава проекта Регламента. Передача персональных данных за пределы Европейского союза или в международную организацию может осуществляться в случае наличия решения Европейской комиссии о том, что страна или организация, получающая персональные данные, обеспечивает адекватный уровень защиты персональных данных. При оценке адекватности уровня защиты персональных данных Европейская комиссия принимает во внимание:

1) верховенство закона, уважение прав человека и основных свобод, соответствующего законодательства, как общего, так и отраслевого, правил защиты данных и мер безопасности, в том числе правил дальнейшей передачи персональных данных в иные страны или международные организации, а также существование эффективных и действенных механизмов защиты субъектов персональных данных, включая административную и судебную правовую защиту;

2) существование и эффективное функционирование одного или нескольких независимых надзорных органов в данной стране или в стране, в которой учреждена международная организация, ответственных за обеспечение соблюдения правил защиты данных, включая необходимые полномочия для оказания помощи и консультирования субъектов персональных данных при осуществлении их прав и сотрудничестве с надзорными органами Европейского союза и государств-членов;

3) международные обязательства стран, расположенных за пределами Европейского союза, или международных организаций, вытекающие из их участия в многосторонних или региональных системах, в частности, в отношении защиты персональных данных.

---

ropean Union (2011/2025 (INI)) // Official Journal C 033 E. 05.02.2013. P. 0101–0110; Directive of the European Parliament and of the Council 2012/0010 (COD) on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Brussels, 25.01.2012 (проект); Resolution of the 85th Conference of the Data Protection Commissioners of the Federal Government and the Bremerhaven on 13–14 March 2013 «Europe must strengthen data protection».

Европейский совет по защите данных может представлять Европейской комиссии мнение для оценки адекватности уровня защиты персональных данных в стране, расположенной за пределами Европейского союза, или в международной организации.

Решение Европейской комиссии может быть отозвано при изменении обстоятельств, влияющих на защиту персональных данных в стране, расположенной за пределами Европейского союза, или в международной организации.

Европейская комиссия должна опубликовать в официальном журнале Европейского союза список стран, территорий, секторов экономической деятельности и международных организаций, в отношении которых были приняты решения об адекватности защиты персональных данных.

В отсутствие решения Европейской комиссии об адекватности защиты данных передача персональных данных возможна при условии надлежащих гарантий оператора персональных данных и (или) обработчика персональных данных.

Во многом реформа сконцентрирована на предоставлении субъектам персональных данных инструментов контроля с одновременным упрощением передачи данных в пределах Европы.

В частности, предусмотрены гораздо более серьезные меры ответственности в случае незаконной передачи данных за пределы ЕС. Так, в случае получения организацией (к примеру, облачным провайдером, социальной сетью, поисковой системой) запроса от третьей страны о предоставлении обрабатываемых на территории ЕС персональных данных выдача таких данных допускается исключительно с разрешения национального органа по защите персональных данных и при условии обязательного информирования субъекта персональных данных о таком запросе.

Кроме того, предложено внедрить очень серьезные санкции в случае нарушения указанного порядка, а именно: штраф организациям, незаконно предоставляющим сведения, в размере до 100 млн евро или до 5% их годового оборота в мировом масштабе, т.е. даже выше, чем было изначально предложено Европейской комиссией (в размере до 1 млн евро или до 2% годового оборота в мировом масштабе).

В открытом доступе информация по вопросу регулирования персональных данных, отнесенных к государственной тайне, в ЕС не размещена.

Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет [Текст] / А. С. Дупан (Гутникова), А. Б. Жулин, А. К. Жарова и др. ; под ред. А. С. Дупан (Гутниковой) ; Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2016. — 344 с. — 1000 экз. — ISBN 978-5-7598-1386-6 (в обл.).

Н72

В монографии представлено исследование актуальных проблем регулирования отношений по оказанию услуг операторами доверенных сервисов (прежде всего идентификация и аутентификация лиц при электронном взаимодействии) и по доверительному управлению информацией на международном уровне, в зарубежных странах и в Российской Федерации, а также проблем защиты персональных данных в Интернете, в том числе в условиях применения новых методов обработки больших массивов данных и использования технологии облачных вычислений.

Книга адресована сотрудникам государственных органов, осуществляющих регулирование информационных отношений и (или) обеспечивающих защиту персональных данных, и компаний, являющихся операторами доверенных сервисов, оказывающих услуги по обработке больших массивов данных, предоставляющих услуги с помощью Интернета, а также операторам персональных данных. Она будет интересной и при изучении курса информационного права в учреждениях высшего образования.

УДК 342.7: 004.738.5.056.5
ББК 67.404.3

Научное издание

Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет

Зав. редакцией *Е.А. Бережнова*
Художественный редактор *А.М. Павлов*
Компьютерная верстка и графика: *О.А. Быстрова*
Корректор *Н.В. Андрианова*

Подписано в печать 16.05.2016. Формат 60×88 1/16
Гарнитура Newton. Усл. печ. л. 20,9. Уч.-изд. л. 18,0
Тираж 1000 экз. Изд. № 2032

Национальный исследовательский университет «Высшая школа экономики»
101000, Москва, ул. Мясницкая, 20
Тел./факс: (499) 611-15-52

Отпечатано в ОАО «Первая Образцовая типография»
Филиал «Чеховский Печатный Двор»
142300, Московская обл., г. Чехов, ул. Полиграфистов, д. 1
www.chpd.ru, e-mail: sales@chpd.ru, тел.: 8 (495) 988-63-76, тел./факс: 8 (496) 726-54-10