

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 области³.

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. Храпцовой: 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 чем-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, уполномоченным 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 субъекта 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-

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru