Правовые режимы информации в эпоху больших данных: сравнительно-правовое исследование

Skolkovo

Москва, 2021

УДК 349:681
ББК 67
П 685

Правовые режимы информации в эпоху больших данных: сравнительно-правовое исследование. — М.: Издательская группа «Закон», 2021. — 156 с.

ISBN 978-5-904208-21-9

Подготовлено на базе сравнительно-правового анализа подходов к правовому режиму данных, создаваемых пользователями сети Интернет, и принципов их сбора, хранения и обработки, проведенного Национальным исследовательским университетом «Высшая школа экономики», а также научно-практического анализа международного опыта регулирования сбора, обработки и результатов обработки массивов больших данных, в том числе обезличенных пользовательских данных, выполненного ООО «Институт исследований интернета».

Рассматриваются также предложения по регулированию для Российской Федерации с учетом странового, международного опыта и российского рынка.

Научный редактор — заведующий лабораторией правовой информатики и кибернетики МГУ имени М.В. Ломоносова к.ю.н. **Николай Андреевич Дмитрик.**

Выражаем благодарность всем экспертам, принимавшим активное участие на разных этапах работы над исследованием и книгой, и в частности:
д.ю.н. И.Ю. Богдановской,
к.ю.н. А.И. Савельеву,
к.ю.н. К.Ю. Голубу,
Е.А. Мешковой,
И.Ю. Левовой и команде ООО «Институт исследований интернета».

Уважаемый читатель!

В основу этой книги были положены исследования, выполненные по заказу Фонда «Сколково» Национальным исследовательским университетом «Высшая школа экономики» («Сравнительно-правовой анализ подходов к правовому режиму данных, создаваемых пользователями сети Интернет, и принципов их сбора, хранения и обработки») и Институтом исследований интернета («Анализ международного опыта регулирования сбора, обработки и результатов обработки массивов больших данных, в том числе обезличенных пользовательских данных»).

Главным содержанием книги является сравнительный анализ режимов регулирования персональных и иных данных в России, а также в Европейском союзе, США и странах Азии.

По итогам анализа отмечаются не только различия в режимах, но и общие закономерности, обусловленные сходством проблем, с которыми самые разные общества сталкиваются в период цифровой трансформации. Эти проблемы сводятся прежде всего к поиску пути для адекватной регуляторной коррекции не всегда справедливого распределения выгод и негативных экстерналий цифровизации общественной жизни в ситуации нарастающего дисбаланса технологических возможностей локомотивов цифровой экономики, государства и отдельных граждан.

Вместе с тем названная общая проблема может иметь и уже находит в различных странах целый ряд разновекторных решений в привязке к не всегда взаимно совместимым концепциям и правовым институтам.

В связи с этим книга описывает различные подходы и инициативы, предлагаемые как в России, так и за рубежом, в том числе касающиеся выделения правовых режимов обезличенных и неперсональных данных, совершенствования законодательства о тайнах, общедоступной информации и появления новой терминологии, включая понятия наподобие «принципалы данных», «целостность контекста» или «персональные данные, разрешенные субъектом персональных данных для распространения».

Изучение имеющихся подходов и инициатив представляется полезным и важным для возможного совершенствования в России правового регулирования информации в эпоху больших данных.

На обложке книги — портрет Готфрида Вильгельма Лейбница, отца математической комбинаторики, дифференциального и интегрального исчисления. Труды Лейбница в области алгебры и математической логики внесли вклад не только в развитие этих дисциплин, но и в создание математического аппарата с двоичной системой счисления, заложив тем самым основы для разработки машинного моделирования и нынешних технологий работы с большими данными.

А.Л. Тюльканов,

специальный советник
по цифровому развитию
в Совете Европы

Оглавление

...Одно только плохо — что каждая вещь сварена сама по себе. То ли дело куча всяких огрызков и объедков! Бывало, перемешаешь их хорошенько, они пропитаются соком и проскакивают не в пример легче...

Марк Твен.
Приключения Гекльберри Финна

Методика исследования

Эпоха больших данных характеризуется тем, что каждые два года объем существующей в мире информации удваивается[1]. Подключенные к сети Интернет автомобили, индустриальные объекты и другие устройства Интернета вещей (*Internet of Things, IoT*) генерируют огромные объемы данных. В частности, один лишь автономный автомобиль способен генерировать около 4000 гигабайт данных в день[2]. По оценкам *International Data Corporation* (*IDC*), к 2025 г. общий объем данных может составить 180 зеттабайт[3]. К 2022 г. взаимодействие между пользователями и устройствами будет персонализированным, при этом 30% коммуникаций между клиентами и продавцами будет ос-

---

[1] См.: The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. EMC Digital Universe with Research & Analysis by IDC, April 2014. URL: https://www.iotjournaal.nl/wp-content/uploads/2017/01/idc-digital-universe-2014.pdf.

[2] См.: *Nelson P.* Just One Autonomous Car Will Use 4,000 GB of Data/Day // Network World. 2016. 7 Dec. URL: https://www.networkworld.com/article/3147892/one-autonomous-car-will-use-4000-gb-of-dataday.html.

[3] См.: Data Age 2025: The Evolution of Data to Life-Critical. IDC White Paper. April 2017. URL: https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf.

новано на обработке геолокационных данных (в отличие от 4% в 2017 г.)[4]. Такого рода информационный взрыв породил популярное сравнение данных с нефтью XXI в. Как пишет *The Economist*, в XXI в. данные сыграют ту же роль, что нефть в XX в., а именно станут «главным фактором роста и перемен... Данные, изменяя рынки, требуют новых подходов в правовом регулировании»[5].

Под большими данными обычно понимается некий набор «подрывных» технологий[6] работы с данными. Встречаются следующие определения этого термина:

— «большие данные объединяют техники и технологии, которые извлекают смысл из данных на экстремальном пределе практичности» (консалтинговая компания *Forrester*)[7];

— согласно отчету Института *McKinsey* «Большие данные: новый рубеж инноваций, конкуренции и производительности»[8] этот термин относится к наборам данных, размер которых превосходит возможности типичных баз данных по формированию, хранению, анализу информации и управлению ею;

---

[4] См.: Predicts 2018: Analytics and BI Strategy // Gartner. 2018. 26 March. URL: https://www.gartner.com/en/documents/3869863/predicts-2018-analytics-and-bi-strategy0.

[5] Fuel of the Future: Data Is Giving Rise to a New Economy // Economist. 2017. 6 May. URL: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

[6] Disruptive technology. URL: https://dictionary.cambridge.org/dictionary/english/disruptive-technology.

[7] *Abo A.-M.* Developing Data Analytics to Improve Services in a Mechanical Engineering Company // Uden L., Fuenzaliza Oshee D., Ting I.-H., Liberona D., eds. Knowledge Management in Organizations. 9th International Conference, KMO 2014. N.Y., 2014. P. 100.

[8] Big Data: The Next Frontier for Innovation, Competition, and Productivity. McKinsey Global Institute, May 2011. URL: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation.

— в правовых актах Эстонии большие данные определяются как собираемые и обрабатываемые наборы данных, которые характеризуются множественностью форматов данных и скоростью их возникновения и обработки;

— в Нидерландах под ними понимается сбор максимально возможного объема информации, хранение их в больших базах данных, комбинирование данных в различных целях и применение алгоритмов для поиска корреляций между данными и получения новой информации[9];

— в документах Международной организации стандартизации большие данные определены как большие массивы данных, главным образом в части таких характеристик, как объем, разнообразие, скорость изменения, которые требуют масштабируемой инфраструктуры для эффективного хранения, обработки и анализа[10];

— в Методических рекомендациях по организационной защите физическим лицом своих персональных данных, размещенных на сайте Роскомнадзора, под большими данными понимается обозначение подходов, инструментов и методов распределенной обработки полуструктурированных и неструктурированных данных самого разного типа и огромных объемов. В отличие от традиционных баз данных большие данные не относятся к структурированным, хранятся децентрализованно и слабо связаны между собой[11].

---

[9] Подходы к определению больших данных в Эстонии и Нидерландах изложены на основании сравнительно-правового исследования: *Sloot B., van der, Schendel S., van.* Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study // JIPITEC. 2016. Vol. 7. Iss. 2. URL: https://www.jipitec.eu/issues/jipitec-7-2-2016/4438.

[10] См.: ISO/IEC TR 20547-5:2018 «Information technology — Big data reference architecture».

[11] См.: http://www.pd.rkn.gov.ru/library/p195/.

Однако даже из приведенных определений нельзя не заметить, что речь идет не столько о новых *технологиях*, сколько о новых *подходах*. Большие данные обрабатываются тогда, когда это дает коммерческие преимущества: увеличивает число заказов или пользователей, позволяет уменьшать издержки, в том числе запасы и иные издержки на планирование и т.п. В связи с этим главный вопрос, связанный с возможным правовым режимом больших данных, звучит так: *насколько добросовестным является поведение тех, кто обрабатывает большие данные и извлекает из этого выгоду*? С учетом того, что, еще раз отметим, речь идет не столько о технологии, сколько о поведении людей и его рамках, насколько оправданно вторжение в веками формировавшиеся правовые режимы тайн, общедоступной и персональной информации в целях слияния данных и поиска связей для их обработки?

Дискуссия о возможном регулировании больших данных ведется и в России. Как и везде, она находится на начальном этапе, и настоящее исследование представляет собой неотъемлемую часть этой дискуссии. Подготовленные в инициативном порядке законопроекты, в частности законопроект Минцифры России[12], не были поддержаны бизнесом и экспертами, потому что они не достигают цели, ради которой разрабатывались. В научных исследованиях сделан вывод, что такие принципы, как ограничение обработки персональных данных заранее определенными целями, ограничение объема собираемых и обрабатываемых данных минимально необходимым объемом, осуществление обработки данных на

[12] См.: С поправкой на большие данные: бизнес раскритиковал законопроект Минкомсвязи // Коммерсантъ. 2020. 21 февр. URL: https://www.kommersant.ru/doc/4261592.

основе информированного согласия, являются несовместимыми с природой технологии больших данных, обусловливающей те преимущества, которые эта технология несет в себе[13]. Правовая природа технологии больших данных, напомним, предопределена поиском связей в ходе их обработки — этим большие данные отличаются от «просто информации», в ходе обработки которой поиск связей не является самоцелью.

Законодательство большинства стран так или иначе регулирует оборот данных уже много лет. Даже если не брать в расчет существующее более трехсот лет законодательство об авторском праве, все равно уже более ста лет законодательно регулируются отдельные виды тайн, более пятидесяти лет регулируется оборот персональных данных, четверть века назад возникло право *sui generis* на содержание баз данных, более двадцати лет охраняются правовые средства защиты авторского права и смежных прав, контролирующие доступ к информации... Все эти правовые институты так или иначе опосредуют отношения по созданию, обработке, использованию, передаче разного рода информации. Наступление эпохи больших данных требует провести ревизию перечисленных правовых институтов, чтобы ответить на вопросы, чем эти институты, возможно, мешают современному информационному обществу и где есть место для какого-то нового регулирования.

Чтобы ответить на эти вопросы, необходимо систематизировать существующие подходы к регулированию оборота данных. Это позволит выявить пробелы в регулировании, а также возможные противоречия как меж-

[13] См.: *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.

ду разными правовыми институтами, применяемыми в рамках тех или иных правоотношений, так и между устаревшим правовым регулированием и новыми или обновившимися общественными отношениями. Право как универсальный регулятор общественных отношений всегда ограничено в доступных ему инструментах, а потому для классификации можно использовать давно сложившийся подход, учитывающий предмет и метод правового регулирования. **Предметом** для целей настоящего исследования будут выступать отдельные **виды данных** либо отношений по их формированию, обработке, использованию и передаче; **методом** — виды императивного или диспозитивного регулирования, запретов, ограничений, правонаделений, дозволений и обязанностей, а также характерный для правоотношений в информационной сфере метод фактической возможности, или *lex informatica*[14].

При таком подходе регулирование можно разбить на три категории: 1) собственно регулирование *оборота* данных; 2) регулирование *доступа* к ним как своего рода прекурсора возможного оборота; 3) обезличивание данных. К **первой категории** относятся прежде всего институт персональных данных и аналогичные институты, опосредующие оборот данных в странах общего права (где нет законодательства о персональных данных), а также институты неперсональных (индустриальных) данных. **Вторая категория** предполагает деление информации на информацию ограниченного доступа и общедоступную информацию, что обусловливается разным набором методов регулирования (запрет — дозволение; в меньшей степени императивный — диспозитивный методы).

[14] См.: *Дмитрик Н.А.* Цифровая трансформация: правовое измерение // Правоведение. 2019. Т. 63. № 1. С. 31–32.

Внутри правового режима общедоступной информации отдельно — по методу — выделяется правовой режим открытых данных, поскольку применительно к нему особо четко проявляется метод фактической возможности, когда данные не просто юридически доступны, но и фактически могут использоваться в силу их публикации, в том числе в машиночитаемом виде. **Третья категория** связана с применением не столько правовых, сколько технических методов разрыва связи данных с теми лицами, к которым они относятся. Разрыв информационной и технической связи одновременно означает и разрыв правовой связи, поскольку такие лица больше не могут заявлять свои права на относящиеся к ним данные.

Необходимо отметить, что настоящее исследование не имело перед собой цели рассмотреть правовые аспекты **интеллектуальной собственности**, хотя они тоже регулируют *оборот* определенных форм данных, ограничивая юридическую, а в рамках технических средств защиты авторского права и фактическую возможность *доступа* к ним. Интеллектуальная собственность является самостоятельным измерением вселенной данных, требующим отдельного изучения.

Помимо классификации подходов к регулированию оборота данных, в исследовании обращается внимание на **цели и задачи регулирования**, т.е. те или иные проблемы, которые пытаются решить законодатели, применяя соответствующие подходы. *Формально* такие цели и задачи уже закреплены в законодательстве в виде:

— права на неприкосновенность частной жизни и контроля информации о себе (для персональных данных и тайны частной жизни);

— свободы слова и свободы доступа к информации (для общедоступной информации);

— права на неприкосновенность коммуникаций (для тайны связи);

— неприкосновенности собственности (для коммерческой тайны);

— конституционного запрета монополистической деятельности (для неперсональных данных).

Для целей *функционального* анализа, т.е. для анализа фактических проблем и их правовых решений, в качестве рабочей гипотезы в настоящем исследовании предполагается, что регулирование оборота данных должно быть направлено на устранение дисбаланса прав и интересов сторон информационных правоотношений, возникающего в силу того, что *фактически* доступные одной из сторон информационные технологии создают для нее возможности, нарушающие ранее существовавший при реализации права баланс. Например, обработка сведений о месте нахождения абонента (сведений геолокации) в сфере оказания услуг связи для целей, непосредственно не относящихся к оказанию услуг связи по договору, заключенному между оператором связи и абонентом, нарушает изначальный баланс интересов оператора и абонента.

В целом такой подход обусловил структуру настоящего исследования и позволил определить место для возможного нового регулирования в уже сложившейся системе права.

Данные, относящиеся к физическому лицу, и иные данные

Режим персональных данных

Режим персональных данных в Европейском союзе

Европейский союз (а точнее, земля Гессен, ФРГ) — родина правового института персональных данных, здесь он зародился и здесь до настоящего времени находится его главный идейный центр. С 2018 г. регулирование персональных данных осуществляется на уровне Регламента Европейского парламента и Совета Европейского союза от 27.04.2016 № 2016/679 «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и об отмене Директивы № 95/46/ЕС (Общие правила защиты данных)» (*General Data Protection Regulation, GDPR*). В связи с вступлением в силу *GDPR* регулирование персональных данных унифицировано и не допускает отступлений на уровне государств — членов Европейского союза (далее также — ЕС, Союз).

Под **персональными данными** в *GDPR* понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъекту персональных данных), при этом идентифицируемое лицо — это лицо, которое может быть иденти-

фицировано прямо либо косвенно посредством ссылки на идентификационный номер, данные о местоположении, онлайн-идентификатор или один либо несколько специфичных факторов, касающихся его физической, психологической, генетической, ментальной, экономической, культурной либо социальной идентичности (ст. 4 *GDPR*). В отличие от ранее закрепленной в Директиве дефиниции персональных данных дефиниция *GDPR* прямо называет онлайн-идентификаторы в качестве разновидности персональных данных.

К группе специальных категорий персональных данных помимо прежних категорий также отнесены генетические данные и биометрические данные, используемые для идентификации физического лица (ст. 9 *GDPR*).

Европейский подход к понятию персональных данных можно выразить следующим образом: персональными данными является (1) любая информация, на основании которой можно определить конкретное физическое лицо (прямая идентификация), а также (2) любая информация *X*, на основании которой самой по себе нельзя определить конкретное физическое лицо, но при этом оператор (обработчик) (а) с разумной вероятностью, зависящей от наличия законного основания и пропорциональности требуемых трудовых, временны́х и материальных затрат, может использовать информацию *Y*, в совокупности с которой информация *X* позволит определить конкретное физическое лицо, (б) принимая во внимание технический прогресс и изменение возможностей обработчика (оператора).

В связи с вступлением в силу 25 мая 2018 г. *GDPR* в странах Европейского союза начали действовать унифицированные **правила обработки** персональных данных. В *GDPR* сохраняются базовые принципы обработки

персональных данных, ранее заложенные в Директиве Европейского парламента и Совета ЕС от 24.10.1995 № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных» и Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981). В рамках этого подхода предполагается закрытый перечень оснований (случаев) обработки персональных данных. К таким основаниям относятся согласие субъекта данных и иные случаи, прямо предусмотренные законом.

GDPR предъявляет следующие требования к согласию субъекта:

— согласие должно быть выражено в форме заявления или конкретного подтверждающего действия (*by a statement or by a clear affirmative action*) (ст. 4 (11)). Молчание, заранее проставленные галочки, нереализация права на отзыв согласия, иные формы молчаливого согласия не соответствуют требованиям, предъявляемым к согласию (п. 32 Преамбулы);

— согласие должно быть свободным (*freely given*). В связи с этим, если исполнение договора или предоставление услуги поставлено в зависимость от дачи согласия на обработку персональных данных, необходимо принимать во внимание, являются ли запрошенные в форме согласия способы обработки необходимыми для исполнения договора (ст. 7 (4)). Если имеет место существенный дисбаланс переговорных возможностей, например если оператор является органом власти, устанавливается презумпция вынужденного (несвободного) характера согласия. Согласие не считается данным свободно, если у лица нет разумного выбора или существует возможность наступления негативных послед-

ствий в случае отказа или последующего отзыва согласия (п. 42, 43 Преамбулы);

— положения об обработке данных, с которыми выражает согласие субъект персональных данных, должны быть отделены от других положений, регламентирующих транзакцию (ст. 7 (2)). Таким образом, эти условия не должны являться составной частью более общего документа, например пользовательского соглашения, в котором, помимо прочего, указаны условия приобретения товара, включающие в себя положения о доставке, оплате, порядке рассмотрения споров и т.п.);

— возможность отзыва согласия на обработку персональных данных должна быть такой же легкой, как и процесс дачи согласия. При этом субъект должен быть проинформирован о наличии права на отзыв согласия до его предоставления (ст. 7 (3));

— *GDPR* не предусматривает возможности получения ретроспективного согласия на обработку персональных данных.

Основания обработки обычных персональных данных без согласия субъекта в целом аналогичны основаниям, закрепленным ранее в Директиве 1995 г. Вместе с тем в *GDPR* расширены основания обработки специальных категорий персональных данных без согласия их субъекта. По-прежнему присутствуют такие основания, как (1) необходимость обработки данных (а) для целей исполнения договора с участием субъекта или в связи с его заключением; (б) для целей соблюдения обязанностей, возложенных на оператора законодательством; (в) для защиты жизненно важных интересов субъекта или третьих лиц; (г) для исполнения полномочий, возложенных на оператора законом, или для выполнения задач, имеющих публичный интерес; (2) наличие законного инте-

реса оператора или третьего лица, если при этом не нарушаются права и свободы субъекта, в частности когда таким субъектом является ребенок (ст. 6 *GDPR*).

При этом категория «законный интерес оператора» является наиболее интересной для обработки больших данных. Преамбула *GDPR* в п. 47 прямо упомянула в качестве возможного примера обработки данных по указанному основанию прямой маркетинг. Отмечается, что обработка данных для целей применения в приложениях аналитики или искусственного интеллекта на основании согласия субъекта является проблематичной, поскольку обозначить заранее цели такой обработки с достаточной степенью конкретности практически невозможно. Кроме того, *GDPR* не содержит никакой «дедушкиной» оговорки, легитимирующей использование ранее накопленных массивов данных[15]. Для решения этих вопросов как раз и должно использоваться основание «законный интерес оператора» в совокупности с псевдонимизацией данных как средства защиты интересов субъекта персональных данных, чтобы такие интересы не превалировали над законным интересом оператора[16].

Применительно к специальным категориям персональных данных *GDPR* в ст. 9 закрепляет следующие основания для обработки без согласия субъекта:

1) необходимость исполнения обязанностей оператора в сфере трудоустройства, социальной защиты в части, предусмотренной национальным или общеевропейским законодательством;

---

[15] См.: New Requirements for Legal Analytics & Artificial Intelligence under the GDPR // Anonos. May 2018. URL: https://www.lexology.com/library/detail.aspx?g=df98ae80-48ba-47e6-be61-25a76f4b9557.

[16] Ibid.

2) защита жизненно важных интересов субъекта или третьих лиц, если субъект не может дать согласие в силу физического или психического состояния;

3) осуществление законной деятельности некоммерческой организацией в отношении своих членов;

4) общедоступность данных, если они сделаны таковыми субъектом;

5) установление, осуществление или защита юридических требований;

6) реализация существенного публичного интереса с соблюдением требований пропорциональности и при наличии гарантий, установленных национальным или общеевропейским законодательством;

7) осуществление профилактической или трудовой медицины с целью оценки способности работника к работе, постановки диагноза, предоставления услуг здравоохранения, лечения или управления системой здравоохранения в соответствии с требованиями национального или общеевропейского законодательства;

8) реализация публичного интереса в сфере здравоохранения, включая защиту от серьезных трансграничных угроз здоровью, обеспечение высоких стандартов качества и безопасности здравоохранения, медицинских продуктов и устройств, если обработка осуществляется на основании закона с принятием мер защиты прав и свобод субъекта персональных данных, в особенности мер защиты профессиональной тайны;

9) архивирование в публичном интересе, для научных, исторических или статистических целей в соответствии со ст. 89 (1) (обеспечение принципа минимизации: если достижение цели обработки возможно без идентификации субъектов, то необходимо принять меры к обезли-

чиванию, псевдонимизации данных[17] и т.п.), при этом обработка не должна умалять существо права на защиту персональных данных и должна происходить с принятием мер защиты фундаментальных прав и интересов субъекта персональных данных.

Режим персональных данных в США

В регуляторных актах США не используется **понятие** «персональные данные», вместо него, как правило, применяют термины «персонально идентифицирующая информация» (*personally identifiable information*) или «персональная информация» (*personal information*). Для США характерен секторальный подход к защите такого рода информации, вследствие чего соответствующие законы приняты в различных сферах. Среди них государственное управление[18], здравоохранение[19], прокат видеофильмов[20], финансовые услуги[21], защита данных автовладельцев[22], защита частной жизни детей в онлайновой среде[23] и др. Закон о защите неприкосновенности частной жизни (*US Privacy Act* 1974) имеет ограниченную сферу применения и касается вопросов обработки персональной информации граждан США или лиц, имеющих постоянное место жительства в США, федеральными органами исполнительной вла-

[17] О подходах европейского законодателя к обезличиванию данных см. раздел «Обезличивание данных» настоящего исследования.

[18] The Privacy Act of 1974.

[19] The US Health Insurance Portability and Accountability Act of 1996.

[20] The US Video Privacy Protection Act of 1988.

[21] The US Financial Services Modernization Act of 1999.

[22] The US Drivers Privacy Protection Act of 1994.

[23] The Children's Online Privacy Protection Act of 1998.

сти[24]. На коммерческий сектор он не распространяется. Как следствие, единого определения персональных данных (персонально идентифицирующей информации) в законодательстве США нет.

Всего можно выделить три основных подхода законодательства США к определению понятия «персональные данные»: 1) тавтологический; 2) основанный на публичности информации; 3) основанный на перечислении видов данных.

Первый подход можно встретить, например, в Законе о защите частной жизни в сфере видеопроката (*The US Video Privacy Protection Act of* 1988), согласно которому «персональная идентифицирующая информация — любая информация, которая определяет лицо»[25]. Соответствующий статус, таким образом, приобретает любая информация о лице, если она связана с предметной областью закона: приобретением экземпляров видеофильмов в аренду или в собственность у профессиональных продавцов.

Второй подход характеризуется определением персональных данных через указание на то, что соответствующая информация не является публичной. Например, Закон Грэмма — Лича — Блайли 1999 г. (*Gramm — Leach — Bliley Act of* 1999) относит к персональной фи-

[24] Overview of the Privacy Act 1974. US Department of Justice. URL: https://www.justice.gov/opcl/definitions.

[25] 18 U.S.C. § 2710 (a)–(b). Данный Закон запрещает прокатным организациям и продавцам видеопродукции предоставлять третьим лицам информацию о том, какие видеофильмы арендовало и приобретало лицо, без его письменного согласия. Закон был принят в ответ на появление компрометирующих материалов, касающихся взятых в видеопрокате фильмов, в отношении кандидата на пост судьи Верховного суда. В настоящее время Закон получил новое дыхание в связи с развитием социальных сетей и онлайн-сервисов типа *Netflix*, которые широко используют систему рекомендаций.

нансовой информации любые сведения финансового характера, которые не являются публичными[26]. Закон не определяет, что такое публичные сведения, однако по контексту к ним относятся общедоступные данные (*public domain*).

Третий подход основан на перечислении определенных категорий данных, относящихся к персональной информации. Он наиболее типичен для законодательства США в указанной сфере. Так, в соответствии с Законом о защите частной жизни детей в онлайновой среде к персональным данным несовершеннолетнего относятся: имя и фамилия, адрес проживания, адрес электронной почты или идентификатор в мессенджере, номер телефона, номер карты социального страхования, онлайн-идентификатор (уникальный идентификатор в *cookie*-файле, *IP*-адрес, уникальный номер устройства и т.п.), аудио, фото и видео, содержащие изображение или голос несовершеннолетнего, геолокационная информация, позволяющая идентифицировать улицу или город местонахождения лица, любая иная информация, которую оператор собирает о несовершеннолетнем или его законном представителе и соединяет с одним из вышеуказанных видов данных[27].

В США действуют не только федеральные законы в сфере защиты частной жизни, но и законы штатов. В настоящее время в каждом штате (за исключением Алабамы и Южной Дакоты) существуют законы о защите частной жизни, которые содержат обязанность по уведомлению субъекта об утечках данных и иных инцидентах с ними (*breach notification rules*) и, соответственно, понятие таких данных, на которые распространяется

[26] 15 U.S.C. § 6809 (4) (A).

[27] The Children's Online Privacy Protection Rule of 2013. § 312.2.

эта обязанность[28]. В этих законах понятие персональной идентифицирующей информации основано на третьем подходе и включает в себя сочетание имени и одного из идентификаторов: 1) номер карточки социального страхования; 2) номер водительского удостоверения; 3) иной идентификатор, используемый государством; 4) номер счета или банковской карты[29]. Некоторые штаты, например Техас, к числу идентификаторов добавляют также дату рождения, биометрические данные, девичью фамилию матери, уникальные электронные идентификаторы, используемые в сети Интернет, данные о состоянии здоровья[30].

Закон о защите частной жизни потребителей Калифорнии (*California Consumer Privacy Act*), вступивший в силу 1 января 2020 г.[31], в секции 1798.140 (*o*) определил персональную информацию как любую информацию, которая идентифицирует, относится, описывает или может быть ассоциирована или связана прямо либо косвенно с конкретным потребителем или домовладением. К персональным данным относятся в том числе описание физических характеристик лица, номер телефона, номер страхового полиса, сведения о стаже работы, номер счета, номер кредитной карты и иная финансовая информация, медицинские данные и данные, связанные со страхованием здоровья; особо защищаемые сведения для целей применения антидискриминационных политик (сведения о расовой, национальной принадлежности, возрасте для лиц старше 40 лет, религиозных, политических взглядах, сексуаль-

[28] См.: *Pomerantz F.J.* Auto Insurance Telematics — Data Privacy And Ownership // FORC Journal. 2015. Vol. 26. Ed. 3.

[29] См., напр.: Code of Virginia Ann. § 18.2–186.6 (A).

[30] Texas Business & Commercial Code Ann. § 521.002 (a) (1).

[31] См.: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

ной жизни, сведения о состоянии здоровья, в том числе о беременности, о прохождении военной службы, генетическая информация и др.[32]); коммерческая информация, включая сведения о личной собственности, приобретенных или планируемых к приобретению товарах и услугах. Понятие «персональная информация» не включает в себя публично доступную информацию, т.е. ту, которая законно доступна из записей в государственных органах. Информация не является публично доступной, если она используется для целей, которые несовместимы с целями, для которых она была собрана и предоставляется государственными органами. Понятие публично доступной информации не охватывает биометрическую информацию, собранную бизнесом без ведома потребителя, а также агрегированную информацию о потребителе и обезличенные данные.

Фрагментарный подход законодательства США к дефиниции персональной информации выступает предметом критики. Высказываются предложения о необходимости выработки унифицированного подхода и расширении этого понятия как минимум за счет включения в него биометрических данных и данных, полученных с сенсоров устройств Интернета вещей, используемых индивидами[33].

Для законодательства США нетипично использование общего понятия обработки персональной информации, характерного для европейского права. Вместо этого в правовом акте регламентируются **правила осущест-**

[32] См.: Protected Classes. URL: https://www.senate.ca.gov/content/protected-classes.

[33] См.: *Peppet S.* Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent // Texas Law Review. 2014. Vol. 93. P. 148.

вления конкретных видов деятельности с данными, сопряженные с определенными рисками для субъектов данных.

По общему правилу обработка персональной информации по законодательству США не требует получения предварительного согласия в явной форме. Достаточно уведомления (*notice*) на веб-сайте или в приложении о параметрах такой обработки, которое в совокупности с последующим использованием соответствующего веб-сайта или приложения рассматривается как подразумеваемое согласие (модель *opt-out*)[34].

Получение предварительного выраженного согласия (модель *opt-in*) используется в ограниченном количестве случаев, в частности если обработка касается чувствительной информации — о здоровье, кредитной истории, сведений о студентах, персональных данных в Интернете о детях младше 13 лет, геолокационных данных, данных об использовании телекоммуникаций и др.

Существенный интерес с точки зрения требований, предъявляемых законом к коммерциализации персональных данных, представляет вышеуказанный Закон Калифорнии о защите частной жизни потребителей 2018 г., поскольку он может стать моделью для федерального законодательства и нормотворчества других штатов.

Во-первых, он возлагает ряд информационных обязанностей по отношению к потребителю. В частности, в политике конфиденциальности[35] и по верифицированному запросу потребителя должна быть предоставлена

[34] Data Protection Laws of the World. United States. Collection and Processing. URL: https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=US.

[35] Требования к наличию политики конфиденциальности и порядку ее предоставления на веб-сайте были установлены в Калифорнии еще в 2004 г. и содержатся в *California Online Privacy Protection Act of* 2003.

информация об обрабатываемых данных, источниках получения данных, целях обработки, категориях получателей данных (секции 1798.110, 1798.115).

Во-вторых, продажа персональных данных потребителей по общему правилу возможна на условии подразумеваемого согласия с учетом того, что потребителю дана возможность отказа (*opt-out*). В отношении персональных данных лиц, которым не исполнилось 16 лет, необходимо получение предварительного явного согласия на продажу данных (*opt-in*), которое несовершеннолетний в возрасте от 13 до 16 лет дает самостоятельно, в остальных случаях — его законный представитель (секция 1798.120). При этом оператор должен заранее предупредить потребителя о возможности продажи его данных третьим лицам, а также обеспечить наличие на домашней интернет-странице оператора кнопки *Do Not Sell My Personal Information*, которая должна быть доступна без предварительной регистрации. В случае если речь идет о мобильном приложении, соответствующая кнопка должна быть на странице с загрузкой такого приложения. Отказ потребителя имеет силу не менее 12 месяцев с момента его совершения.

В-третьих, потребитель имеет право (о котором оператор должен заблаговременно его проинформировать) требовать от оператора удаления на основании верифицированного требования собранной и обрабатываемой информации, за исключением случаев, когда соответствующая информация необходима оператору для совершения установленного перечня действий (секция 1798.105 (*d*)).

В-четвертых, закон прямо запрещает дискриминационные практики в отношении потребителей, которые реализовали свои права по нему, в частности отказ в предостав-

лении товара или услуги; установление иных цен на них; предоставление услуг или товаров иного качества или в ином объеме. Однако если иная цена или качество товаров или услуг находится в непосредственной взаимосвязи с ценностью предоставленных потребителем данных, то соответствующая практика может быть признана законной. Программы лояльности, в рамках которых потребителю предлагаются скидки, товары или услуги иного качества как компенсация за предоставленные персональные данные, не запрещены как таковые, но требуют предварительного получения явного согласия на них от потребителя с предоставлением всех существенных условий программы. При этом такое согласие может быть отозвано в любой момент (секция 1798.125).

В-пятых, продажа, использование, обмен обезличенными данными или агрегированной информацией о потребителях не ограничивается законом (секция 1798.145 (*a*) (5)). Равно как закон не распространяется на обработку данных резидентов Калифорнии в связи с их деятельностью за пределами Калифорнии (например, когда они находятся в отпуске или командировке в другом штате или стране) (секция 1798.145 (*a*) (6)).

Все положения закона, касающиеся прав потребителей, носят императивный характер и не могут быть изменены или отменены договором (секция 1798.192). Это, по мнению исследователей, заметно уменьшает вероятность признания потребителя собственником таких данных, поскольку его возможности по распоряжению ими существенно ограничены, и снижает коммерческую ценность таких данных[36].

[36] См.: *Determann L.* No One Owns Data (February 14, 2018). UC Hastings Research Paper No. 265. P. 30–31. URL: https://ssrn.com/abstract=3123957.

Режим персональных данных в праве стран Азии

Законодательство **Сингапура** о защите персональных данных представлено Законом Сингапура о персональных данных 2012 г. (*Personal Data Protection Act, PDPA*), вступившим в силу 2 июля 2014 г., а также двумя специальными законами, посвященными банковской тайне (ст. 47 *Banking Act* 1970) и биомедицинским исследованиям (ст. 25 *Human Biomedical Research Act* 2015).

По **определению** *PDPA*, персональными данными признаются сведения о физическом лице безотносительно их достоверности, если оно может быть идентифицировано либо на основании самих этих данных, либо на основании этих данных в совокупности с другой информацией, к которой оператор имеет или может получить доступ (секция 2)[37].

Положения *PDPA* не распространяются: 1) на контактные деловые данные; 2) персональные данные, отраженные в записи, существующей более 100 лет; 3) персональные данные лиц, умерших более 10 лет назад.

К контактным деловым данным относится информация, которая с учетом существующих обычаев может относиться к таковой (ФИО, должность, рабочий номер телефона, рабочий адрес электронной почты) и при этом предоставляется именно в контексте бизнес-отношений. Интересен спор, рассмотренный Комиссией по защите персональных данных Сингапура применительно к контактным данным таксистов, которые предоставлялись пассажирам платформой-агрегатором через приложение, посредством которого осуществлялся вызов. Таксисты возражали против раскрытия их мо-

[37] См.: https://sso.agc.gov.sg/Act/PDPA2012.

бильных телефонов пассажирам, однако Комиссия сочла, что в этом случае речь идет о контактных деловых данных, поэтому нарушений Закона о персональных данных нет[38].

В **Южной Корее** Закон о защите персональной информации (*Personal Information Protection Act, PIPA*) определяет персональные данные как информацию, относящуюся к живому физическому лицу, посредством которой данное физическое лицо может быть идентифицировано на основании самой этой информации либо при ее незатрудненном комбинировании с другой информацией (ст. 2.1).

Закон Южной Кореи о развитии информационно-телекоммуникационных сетей и защите информации (*IT Network Act*) закрепляет аналогичное определение персональных данных, но этот акт применяется только к персональной информации пользователей (пользовательской информации), к которым относятся все физические лица, использующие телекоммуникационные услуги, оказываемые провайдерами онлайн-сервисов (это могут быть как операторы связи, так и интернет-сервисы)[39].

Пункт 1 ст. 2 Акта **Японии** о защите персональной информации (*Amended Act on the Protection of Personal Information*, *APPI*) после изменений, внесенных в 2015 г., определяет персональную информацию как информацию о живом физическом лице, которая позволяет идентифицировать его по имени, дате рождения

[38] См.: *YongQuan B.* Data Privacy Law in Singapore: the Personal Data Protection Act 2012 // International Data Privacy Law. 2017. Vol. 7. No. 4. P. 299.

[39] Act on Promotion of Information and Communication Network Utilisation and Information Protection. URL: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf.

или другому содержащемуся в ней описанию (включая голос или данные о поведении), а также информацию, которая позволяет оператору идентифицировать физическое лицо посредством простого обращения к другой информации. Кроме того, к персональной информации прямо отнесена информация, представляющая собой «персональный идентифицирующий код», например номера и данные, предназначенные для использования с устройством, полученные путем преобразования сведений о теле человека (биометрические данные), а также номера документов или иные идентификаторы, уникальные для человека и по которым его можно определить (ст. 1).

Особенность понятийного аппарата японского законодательства заключается в том, что оно различает персональную информацию (см. выше) и персональные данные, которые понимают как персональную информацию, содержащуюся в базе данных оператора, которая трактуется достаточно широко (адресная книга почтовой программы, файлы с данными об *ID* пользователей и транзакциях, совершенных ими, оцифрованные данные визитных карточек, доступные для использования сотрудниками компании, и т.п.)[40].

К чувствительным персональным данным по законодательству Японии относятся данные о расе, вероучении, социальном статусе, медицинской истории; сведения о жертве преступления; любая другая информация, на основании которой физическое лицо может подвергнуться дискриминации (для передачи таких данных третьим лицам требуется предварительное

[40] См.: Baker McKenzie. Global Privacy and Information Management Handbook 2018. P. 444. URL: https://www.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en.

согласие субъекта, подразумеваемое согласие *opt-out* неприменимо)[41].

Что касается **обработки** персональных данных, то законодательства азиатских стран устанавливают следующие правила.

В **Южной Корее** оператор персональных данных в соответствии с *PIPA* и провайдер информационного сервиса в соответствии с *IT Network Act* перед началом обработки персональных данных обязаны сообщить субъекту информацию, касающуюся предстоящей обработки (цель, виды обрабатываемых данных, период хранения данных и др.), а также получить предварительное согласие. Согласие на обработку специальных категорий персональных данных должно быть получено отдельно. Согласие на обработку персональных данных лица моложе 14 лет должно быть получено у его законного представителя.

Обработка персональных данных без согласия субъекта в соответствии с *PIPA* допускается в случаях, когда она:

— прямо разрешается каким-либо законом либо необходима для выполнения обязанностей, предусмотренных законом или подзаконным актом;

— необходима для выполнения функций публичного органа или организации;

— осуществляется в целях заключения и исполнения договора с субъектом персональных данных;

— необходима в целях обеспечения физической безопасности либо материальных интересов субъекта персональных данных или третьих лиц в ситуации, когда невозможно получить согласие на обработку персональных данных;

---

[41] См.: Baker McKenzie. Global Privacy and Information Management Handbook 2018. P. 444.

— необходима в целях реализации законных интересов оператора и это с очевидностью превышает по своему значению право субъекта персональных данных на выражение согласия.

Обработка персональных данных без получения согласия субъекта по *IT Network Act* допускается, когда:

— персональные данные необходимы для исполнения договора об оказании *IT*-услуг, но существуют очевидные трудности в получении согласия по экономическим либо техническим причинам;

— обработка необходима для расчетов за оказанные *IT*-услуги;

— обработка персональных данных без согласия субъекта предусмотрена положениями *IT Network Act* либо другого акта.

В **Японии** в соответствии с *APPI* коммерческий оператор (*business operator*) обязан заранее определить цель обработки персональных данных и в дальнейшем не выходить за ее пределы без дополнительного согласия субъекта персональных данных. Цель обработки может быть объявлена публично (например, размещена на веб-сайте оператора) либо непосредственно донесена до субъекта персональных данных (например, указана в контракте между оператором и субъектом).

Передача третьим лицам персональных данных возможна без согласия субъекта, т.е. по модели *opt-out*, однако при условии предварительного согласования с регулятором — Комиссией по защите персональных данных[42]. Подобный подход неприменим к чувствительным персональным данным, где требуется предварительное согласие субъекта на их передачу третьим лицам.

[42] Ibid. P. 441.

Без согласия субъекта (даже по модели *opt-out*) данные могут быть переданы третьим лицам для целей:

— исполнения закона;

— защиты собственности, жизни и здоровья субъекта или третьих лиц;

— защиты общественного здравоохранения (например, для предотвращения эпидемий).

Закон о персональных данных Японии не регулирует вопросы, связанные с использованием данных для рекламных рассылок. Однако в соответствии с Законом Японии о регулировании передачи электронной почты для получения рекламных рассылок необходимо предварительное согласие субъекта.

В соответствии с Законом о защите персональных данных **Сингапура** 2012 г. (*Personal Data Protection Act, PDPA*) и разъяснениями Комиссии Сингапура по защите данных, посвященными вопросам оборота данных[43], обработка персональных данных, в том числе посредством их передачи третьим лицам, может осуществляться с согласия субъекта либо в предусмотренных законом случаях без такого согласия.

Особенностью сингапурского подхода к согласию является то, что он различает явное и подразумеваемое согласие. Явное согласие имеет место, когда субъект совершает действие, свидетельствующее о том, что он принимает предоставленные ему условия обработки. Например, продолжает использовать такси после прочтения при посадке в автомобиль соответствующего текстового уведомления на подголовнике перед пассажирским сиде-

[43] См.: PDPC Guide to Data Sharing. URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf.

ньем или прослушивания голосового уведомления о том, что все происходящее записывается[44].

Подразумеваемое согласие представляет собой конклюдентную форму его предоставления и имеет место в тех случаях, когда лицо добровольно предоставляет оператору свои данные и оператор использует их для тех целей, которые соответствуют разумным ожиданиям субъекта. В этом случае отсутствует предварительное уведомление субъекта о целях обработки. Второй пример подразумеваемого согласия можно наблюдать, когда субъект дал согласие на передачу данных другому лицу для определенной цели, что одновременно предполагает согласие субъекта на сбор и обработку таким другим лицом полученных данных в объеме, необходимом для достижения цели передачи (ст. 13 *PDPA*).

Персональные данные могут передаваться так называемому посреднику (*intermediary*), который осуществляет фактическую обработку данных по поручению оператора. В терминологии европейского законодательства такое лицо было бы признано обработчиком (*data processor*). В отличие от европейского подхода для передачи персональных данных посреднику сингапурское законодательство не предписывает обязательное получение согласия их субъекта.

При определении адекватного основания для передачи персональных данных третьим лицам (не посредникам) согласно разъяснениям Комиссии нужно принимать во внимание следующие факторы:

— цели использования;

[44] PDPC Advisory Guidelines on In-Vehicle Recordings by Transport Services for Hire. 9 April 2018. URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/Advisory-Guidelines-on-In-Vehicle-Recordings_Updated-22-May-2018.pdf?la=en.

— потенциальные выгоды;

— риски для субъектов персональных данных.

Если цели использования персональных данных третьим лицом соответствуют тем целям, для которых субъект давал согласие (например, на использование данных в целях их анализа, при этом данные передаются аналитическому центру), получать дополнительное согласие для такой передачи не требуется.

Кроме того, не требуется получать согласие при передаче третьим лицам обезличенных данных, поскольку по законодательству Сингапура обезличенные данные[45] не признаются персональными данными и на их обработку не распространяются требования к защите персональных данных.

Без согласия субъекта персональных данных третьим лицам могут передаваться данные при наличии специальных оснований — исключений. Широкий перечень таких оснований представлен в приложениях к *PDPA* и включает следующие случаи:

— передача необходима в любых целях в интересах субъекта персональных данных, если согласие на такую передачу не может быть своевременно получено;

— передача необходима в любых чрезвычайных ситуациях, угрожающих жизни, здоровью либо безопасности субъекта персональных данных или иного лица;

— персональные данные являются общедоступными;

— передача персональных данных необходима в государственных интересах;

— передача необходима для расследований и судебных разбирательств;

[45] О подходе к определению обезличенных данных в Сингапуре см. раздел «Обезличивание данных».

— персональные данные передаются публичной организации и такая передача необходима в публичном интересе;

— передача необходима для целей оценки;

— передача необходима в целях погашения долга субъекта персональных данных перед оператором либо долга оператора перед субъектом персональных данных;

— передача необходима в целях оказания юридических услуг в отношениях между оператором и субъектом персональных данных;

— передача осуществляется в целях подготовки кредитных отчетов;

— информация об обучающихся передается образовательной организацией публичным структурам для целей управления в сфере образования;

— информация о пациентах передается лицензированной медицинской организацией публичным структурам для целей управления в сфере здравоохранения;

— передача осуществляется официальному представителю уполномоченного правоприменительного органа на основании письменного распоряжения руководителя органа, подтверждающего необходимость предоставления персональных данных в целях исполнения обязанностей такого официального лица;

— передача персональных данных лица, получившего увечья, больного или умершего лица осуществляется ближайшему родственнику или другу лица; и др.

В *B*2*B*-отношениях персональные данные могут передаваться другой стороне коммерческой транзакции без согласия субъекта при условии, что они необходимы для осуществления данной транзакции и стороны вступают в соглашение о допустимости использования

персональных данных только в целях осуществления транзакции.

Субъект персональных данных по законодательству Сингапура может в любой момент отозвать согласие на обработку, если данные обрабатываются в соответствии с ранее выраженным согласием либо на основании подразумеваемого согласия.

Режим персональных данных в России

Определение персональных данных, содержащееся в действующем российском законодательстве («любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»), соответствует положениям Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, существующему европейскому регулированию и тенденциям развития законодательства в этой области, демонстрируемым в законодательстве отдельных азиатских стран.

Такой подход к дефиниции персональных данных характеризуется гибкостью, позволяющей обеспечить охват этой категорией новых видов данных о физических лицах, которые могут возникать с развитием технологий или появлением новых бизнес-моделей, без необходимости каждый раз вносить изменения в закон. Он позволяет охватить регулированием практику линкования различных массивов данных между собой с целью создания профайлов пользователей, поскольку такие практики сопряжены с рядом рисков для физических лиц (дискриминация, манипулирование, *identity theft*, т.е. кража личности, и др.).

Недостатком этого подхода является неопределенность, которая в ряде случаев не позволяет операторам с достаточной точностью сделать вывод об относимости тех или иных данных к категории персональных. Это создает риски избирательного правоприменения, а также дополнительные трансакционные издержки, поскольку операторы в стремлении обезопасить себя выбирают наиболее консервативное толкование, относя спорные данные к категории персональных.

Что касается оснований **обработки** персональных данных в России, то здесь нельзя не отметить недостаточный потенциал использования специальных оснований для обработки персональных данных в отсутствие согласия субъекта.

Во-первых, положения, применимые к «обычным» типам данным (ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»; далее — Закон о персональных данных), не синхронизированы с положениями, применимыми к специальной категории персональных данных: отсутствует возможность обработки специальных категорий данных без согласия субъекта, если она «осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных». Это не позволяет расширить возможности применения технологий искусственного интеллекта на медицинские и околомедицинские данные (например, данные с фитнес-браслетов, которые могут быть отнесены к специальным категориям как характеризующие здоровье субъекта). В настоящее время в отсутствие таких положений обработка подобных данных в аналитических целях возможна на основании письменного согласия, что трудно-реализуемо в условиях большого количества субъектов

и множества различных сценариев и целей аналитики, которые могут меняться достаточно оперативно.

Во-вторых, не предусмотрена возможность обработки особой категории персональных данных — агрегированной информации о потребителях — в аналитических, научных, статистических и иных исследовательских целях. Такое основание позволит использовать агрегированную информацию для целей совершенствования онлайн-сервисов без необходимости получения отдельного согласия на это. Кроме того, это позволит передавать такие массивы третьим лицам за вознаграждение или без такового, создавая условия для формирования легального рынка этих данных.

В-третьих, в силу косности правоприменительной практики почти не используются положения, касающиеся обработки данных в законном интересе оператора.

Необходимо отметить чрезмерно формальный подход к получению согласия субъекта, а также проблемы с получением оператором согласия на обработку данных через третьих лиц (например, операторами связи с привлечением банков и наоборот), обусловленные чрезмерно формальным толкованием закона, который прямо не предусматривает такую возможность, но и не запрещает ее. Также важным является вопрос об организационно-технических условиях для обеспечения удобного и эффективного способа предоставления и отзыва согласий в цифровой среде. То, что сейчас делается посредством письменных согласий или их суррогатов, вполне может осуществляться в режиме реального времени в цифровой среде с использованием специализированных программных решений и платформ. Проблема с выполнением требований к согласию во многом порождена технологическими реалиями, поэтому было

бы наиболее адекватно решать ее также посредством технологии.

В рамках перечисленных выше проблем с обработкой персональных данных в России реализуется трехэтапный подход к совершенствованию регулирования в сфере персональных данных.

Первый этап реализован принятием Федерального закона от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» (далее — Закон № 519-ФЗ), положения которого урегулировали персональные данные, разрешенные их субъектом для распространения, дали определение понятию такой категории и установили особенности их обработки. В числе особенностей обозначено, что молчание или бездействие субъекта ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом для распространения, а также то, что в случае несоблюдения положений ст. 10.1 Закона № 519-ФЗ субъект вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных им для распространения, к любому лицу, обрабатывающему эти данные, или заявить такое требование в суд.

Второй этап находится в стадии реализации. Законопроект № 992331-7 «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения порядка обработки персональных данных)» принят в первом чтении 16.02.2021. Законопроект предусматривает возможность предоставления согласия на обработку персональных данных в письменной форме, требования к которому перечислены в ч. 4 ст. 9 Закона о персональных данных (получение у субъекта персональных данных согласия в письменной форме обяза-

тельно в случаях, указанных в ст. 10, 11, 12, 16 Закона о персональных данных, и иных случаях, установленных федеральными законами), одновременно в нескольких целях, а также нескольким лицам, осуществляющим обработку персональных данных по поручению оператора персональных данных. При этом если обработка персональных данных осуществляется в нескольких целях, в отношении каждой цели должны быть указаны сведения в соответствии с п. 5–8 ч. 4 ст. 9 Закона о персональных данных. В случаях возникновения необходимости обработки персональных данных в дополнительных целях (отличных от первоначальных целей сбора) законопроектом предусмотрена возможность обработки таких данных при условии получения согласия субъекта персональных данных или в иных случаях, перечисленных в ч. 1 ст. 6 Закона о персональных данных, но без проведения процедур сбора персональных данных.

Для обеспечения защиты прав граждан при уничтожении персональных данных законопроектом предусмотрена обязанность использовать средства защиты информации, в составе которых реализована функция уничтожения информации и которые прошли в установленном порядке процедуру соответствия, проведенную ФСБ России или ФСТЭК России. В части установления порядка обезличивания персональных данных законопроектом предлагается уточнить полномочия Роскомнадзора по утверждению требований и методов обезличивания. Регламентация требований и методов по обезличиванию персональных данных на уровне нормативного акта Роскомнадзора с учетом развития информационных технологий позволит оперативно вносить необходимые изменения и дополнения в существующую методологию обезличивания.

Третий этап планируется к реализации через исполнение Федерального закона от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» и соответствующих законов-спутников:

— в соответствии с п. 9.1 ст. 6, ч. 1 ст. 10 Закона о персональных данных в экспериментальном правовом режиме (ЭПР) обрабатываются обезличенные персональные данные с вариативностью методик обезличивания;

— федеральный уполномоченный орган по контролю за обработкой персональных данных готов оценивать реализацию программ ЭПР, достижение целей программ ЭПР, установленные риски в программах ЭПР, достижение допустимых уровней рисков в ходе реализации ЭПР, а в случаях достижения недопустимых уровней рисков в экспериментах с обезличенными персональными данными оценивать ущерб, нанесенный гражданам, обществу, государству;

— по итогам достижения положительных результатов ЭПР федеральные уполномоченные органы готовы совместно с бизнесом и экспертами выступить инициаторами внесения изменений в Закон о персональных данных, устанавливающих разумные послабления в режимах обработки информации.

Промежуточные выводы

Российское регулирование в сфере персональных данных как по подходам к определению их содержания, так и в части оснований и условий их обработки соответствует европейским стандартам. Широкий подход к понятию персональных данных в ЕС нередко объясняется тем, что он направлен не столько на регулирование сбора

таких данных, сколько на регулирование установления корреляций между ними, что делает его оправданным и для российской действительности. Преимущество существующего в российском законодательстве варианта определения заключается в сохранении гибкости формулировки, а вместе с ней и стабильности такой дефиниции, поскольку она сможет охватывать новые виды персональных данных, появляющиеся по мере развития технологий, без необходимости внесения изменений в законодательство. Кроме того, сохраняется соответствие требованиям Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и совместимость с европейским правом, что важно для обеспечения трансграничного обмена данными с компаниями, ведущими бизнес в странах Европейского союза.

В России требуется дальнейшее совершенствование механизмов применения различных оснований обработки персональных данных. Здесь стоит иметь в виду опыт стран Тихоокеанского региона: отдельные штаты США, такие как Калифорния, идут по пути экспансивного подхода к персональным данным, охватывая все новые виды коммерчески ценной информации, относящейся к физическим лицам, а Япония придерживается более точечного подхода, включив в последних изменениях в законодательство биометрические данные в состав персональных данных. Подобная экспансия характеризуется расширением перечня оснований для обработки персональных данных без согласия субъекта, а в некоторых юрисдикциях также и либерализацией требований к согласию. При этом необходимо понимать, что ЕС и США занимают принципиально разные позиции в отношении оснований для обработки персональных данных. Если

в ЕС требуется наличие легитимирующего основания для такой обработки (принцип «запрещена по умолчанию»), то в США обработка данных персонального характера разрешена по умолчанию, за исключением случаев, когда она должна осуществляться в соответствии со специальными требованиями закона в целях минимизации возможных рисков субъектов. Это различие обусловлено принципиально разными подходами к природе персональных данных: в ЕС они рассматриваются как продолжение личности, в связи с чем регулируются через призму обеспечения фундаментальных прав и свобод; в США информация — это в первую очередь товар (*commodity*), в отношении которого может возникать законный интерес, требующий балансировки с другими правами (на свободу слова, на осуществление предпринимательской деятельности и др.).

Сбалансированный подход к основаниям обработки персональных данных демонстрирует Сингапур, который тяготеет к европейскому подходу, однако предоставляет достаточный простор для обеспечения гибкости операторов при обработке данных (концепция подразумеваемого согласия). Кроме того, там реализована возможность получения оператором от административного органа специального разрешения на исключение из-под действия закона отдельных видов обработки данных, что не свойственно ни США, ни ЕС. Во многом это связано с характерными для азиатского общества принципами коммунитаризма (приоритета общественных интересов над частными).

Решение выявленных в настоящем разделе исследования задач развития законодательства в сфере персональных данных требует от российского законодателя и правоприменителей стратегического многоэтапного

подхода к регулированию, основные элементы которого были описаны выше. Особое значение в этой ситуации приобретает экспериментальное регулирование, которое позволит оценить преимущества и недостатки того или иного правового режима обработки данных на ранней стадии, до распространения его на все сферы деятельности и отрасли экономики России.

Индустриальные и иные неперсональные данные

Режим неперсональных данных в Европейском союзе

В Европейском союзе в настоящее время проходит реформа, направленная на обеспечение единообразного правового регулирования в сфере обработки персональных и неперсональных данных с использованием сети Интернет и их свободного перемещения в ЕС. Рамкой реформы выступает стратегия Европейской комиссии по формированию Цифрового единого рынка (*Digital Single Market*, *DSM*) в целях обеспечения наилучшего возможного доступа к онлайн-миру для физических и юридических лиц. *DSM* — это такой рынок, на котором обеспечивается свободное перемещение людей, услуг и капитала и где физические и юридические лица могут беспрепятственно получать доступ и участвовать в онлайн-деятельности в условиях честной конкуренции, а также гарантируется высокий уровень защиты потребительских и персональных данных независимо от гражданства или места жительства[46].

[46] Shaping the Digital Single Market. URL: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.

Результатами реформы уже стали два Регламента: рассмотренный выше *GDPR* и Регламент по неперсональным данным[47]. Такое разделение обусловлено тем, что реформа правового регулирования обработки персональных данных осуществлена и в ней уже заложены принципы единого цифрового рынка и свободного перемещения данных в ЕС. **Все остальные группы данных подпадают под второй регламент, комплементарный к *GDPR***. Так как создание европейской экономики данных является частью стратегии Цифрового единого рынка, проводимая реформа направлена на то, чтобы максимально эффективно использовать потенциал цифровых данных в интересах экономики и общества. Именно поэтому и разработано новое рамочное регулирование об обеспечении свободного перемещения неперсональных данных в ЕС.

Понятие «*данные, не являющиеся персональными*» является новым для законодательства государств — членов ЕС. Выбор персональных и неперсональных данных как принципиально важных элементов регулирования оборота данных на территории ЕС обусловлен следующими причинами. С точки зрения экономики к данным может применяться различная классификация, в частности по отраслям (промышленные, аграрные, финансовые), по степени обработки или объему данных (неупорядоченные, упорядоченные, базы данных, массивы данных, большие данные). Юридически значимая классификация базируется не на отраслевых признаках данных, а на применяемых к данным правовых режимах. С правовой

[47] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807.

точки зрения для цифровой экономики наибольшее значение имеют как персональные данные, так и данные, не являющиеся персональными, прежде всего индустриальные (промышленные) данные, которые генерируют счетчики, робототехника.

Основным источником данных, не являющихся персональными, является Интернет вещей. К неперсональным данным относятся также обезличенные данные. Персональные и неперсональные данные составляют основной массив больших данных и, как следствие, обладают наиболее высокой коммерческой ценностью. Анализ больших пользовательских данных активно используется в электронной коммерции и рекламе. Анализ данных точного земледелия — для планирования высева, расчета норм внесения удобрений и средств защиты растений; промышленные данные — для повышения эффективности работы и обслуживания станков и оборудования.

В процессе развития цифровой экономики требуется создавать благоприятные правовые условия обороту данных, генерируемых без участия человека (данных Интернета вещей, индустриального Интернета; далее также — индустриальные данные). Включение таких данных в широкий оборот и использование их в разных секторах экономики (транспорт, энергетика, здравоохранение и т.п.) позволит улучшать качество услуг, создавать новые продукты, повышать эффективность управленческих процессов.

В контексте правового обеспечения оборота данных, генерируемых без непосредственного участия человека, актуальными являются две ключевые задачи — определение прав субъектов, организовавших генерацию и сбор таких данных, в отношении этих данных (баз дан-

ных), а также обеспечение недискриминационного доступа третьих лиц к этим данным.

В правовой[48] и экономической[49] литературе, а также в стратегических документах[50] Европейского союза приведены результаты анализа возможных правовых моделей регулирования отношений в сфере оборота индустриальных данных, а также изложены рекомендации по дальнейшему решению проблем свободного обмена этими данными.

В Европейском союзе был проведен ряд исследований[51], посвященных изучению препятствий для свободного передвижения данных внутри интеграционного объединения (как цифрового единого рынка), и ключевыми названы такие препятствия:

— неоправданные ограничения локализации данных государственными органами государств-членов;

— правовая неопределенность в отношении законодательства, применимого к трансграничному хранению и обработке данных;

— отсутствие доверия к трансграничному хранению и обработке данных, связанное с обеспокоенностью вла-

---

[48] См.: *Drexl J.* Designing Competitive Markets for Industrial Data — between Propertisation and Access (October 31, 2016). Max Planck Institute for Innovation & Competition Research Paper No. 16-13. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2862975.

[49] См.: *Duch-Brown N.*, *Martens B.*, *Mueller-Langer F.* The Economics of Ownership, Access and Trade in Digital Data (February 17, 2017). JRC Digital Economy Working Paper 2017-01. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914144.

[50] См.: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «Building a European Data Economy». URL: https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy.

[51] См.: Measuring the Economic Impact of Cloud Computing in Europe — Study Report. 2017. URL: https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe.

стей государств-членов относительно доступности данных в контрольных целях;

— трудности в смене поставщиков услуг (таких, как облачные).

Кроме того, следует заключить, что очевидным препятствием является отсутствие единых обязательных требований в европейском и национальных законодательствах, а также соответствующих прав, обязанностей и ответственности субъектов.

В результате Регламент о свободном обороте неперсональных данных направлен на устранение препятствий на пути свободного перемещения неличных данных[52]. Хотя законодательство ЕС и так устанавливает принцип свободного перемещения в отношении персональных данных внутри ЕС, новый Регламент дополняет и представляет всеобъемлющий и последовательный **подход к свободному перемещению всех данных в ЕС**, в частности:

— свободное перемещение неличных данных через границы: каждая организация должна иметь возможность хранить и обрабатывать данные в любом месте Европейского союза;

— доступность данных для регулирующего контроля: государственные органы сохраняют доступ к данным, когда они находятся в другом государстве-члене или когда они хранятся или обрабатываются в облаке;

— простая смена поставщиков облачных сервисов для профессиональных пользователей. Комиссия начала содействовать саморегулированию в этой области, побуждая интернет-посредников разрабатывать кодексы пове-

[52] См.: Free Flow of Non-Personal Data. URL: https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data.

дения в отношении условий, при которых пользователи могут передавать данные между поставщиками облачных услуг и обратно в собственные *IT*-среды;

— полная согласованность и синергия с пакетом кибербезопасности и разъяснение того, что любые требования безопасности, которые уже применяются к предприятиям, хранящим и обрабатывающим данные, будут продолжать действовать, когда данные хранятся или обрабатываются за пределами ЕС.

Данные должны быть доступны для повторного использования в максимально возможной степени в качестве основного источника инноваций и роста. Меры, объявленные в документе «На пути к общему европейскому пространству данных»[53], охватывают разные типы данных и поэтому имеют свою специфику:

— внесение изменений в Директиву Европейского парламента и Совета ЕС от 17.11.2003 № 2003/98/*EC* о повторном использовании информации в государственном секторе (Директива *PSI, the Directive on the re-use of public sector information*[54]);

— обновление Рекомендации 2012 г. о доступе и сохранности научной информации (*Recommendation on access to and preservation of scientific information*[55]);

— Руководство по обмену данными частного сектора между компаниями и органами государственного сектора в общественно значимых целях (*Guidance on sharing pri-*

[53] Building a European Data Economy. URL: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[54] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Re-Use of Public Sector Information // Official Journal L 345. 2003

[55] Recommendation on Access to and Preservation of Scientific Information. URL: https://ec.europa.eu/digital-single-market/en/news/recommendation-access-and-preservation-scientific-information.

vate sector data among companies and with public sector bodies for public interest purposes[56]).

Режим неперсональных данных в США

В настоящее время в США отсутствуют специальные законы, посвященные регулированию неперсональных данных самих по себе. В то же время некоторые положения ранее принятых законов потенциально применимы к указанной категории данных. Наиболее актуальным является Закон о мошенничестве и злоупотреблениях с использованием компьютеров (*U.S. Computer Fraud and Abuse Act, CFAA*). Он запрещает доступ к информации, содержащейся на компьютере, без согласия его владельца или с превышением полученной от него авторизации[57]. При этом понятие «компьютер» понимается достаточно широко, охватывая любое устройство, способное хранить и обрабатывать данные с высокой скоростью (18 *U.S.C.* § 1030 (*e*) (1)). Этот Закон обязывает производителей устройств Интернета вещей, которые хотят получать любые данные с них (беспилотные автомобили, смартфоны, носимые устройства и т.п.), получить согласие их владельца на это.

Необходимость регулирования неперсональных данных активно обсуждается в США, однако преимущественно с позиций информационной безопасности. В частности, предложены законопроекты по регулированию оборота неперсональных данных в отдельных секторах экономики, а именно в отношении «умных» авто-

[56] Guidance on Sharing Private Sector Data among Companies and with Public Sector Bodies for Public Interest Purposes. URL: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[57] 18 *U.S.C.* § 1030 (*a*) (2) (*c*).

мобилей (*Security and Privacy in Your Car (SPY Car) Act*)[58] и использования технологий обработки таких данных на воздушных судах и системах наземного обслуживания воздушных судов (*Cybersecurity Standards for Aircraft to Improve Resilience (Cyber AIR) Act*)[59].

Первый проект носит предварительный характер, он не устанавливает регуляторные положения, а предписывает уполномоченным структурам разработать правила (организационные и технические меры, «лучшие практики») для обеспечения информационной безопасности в сфере использования «умных» автомобилей. Вторым проектом предлагается, в частности, закрепить обязательство по уведомлению о попытках кибератак и совершенных инцидентах, использованию полученных сведений для выявления уязвимостей в системах управления воздушными судами и разработки наилучших практик и стандартов по предотвращению последующих инцидентов.

Есть и противники прямого законодательного регулирования неперсональных данных. Такую точку зрения выразила глава Федеральной торговой комиссии США (*FTC*)[60]. Она отражает взгляды участников рынка, настроенных против специального законодательного регулирования из опасения, что оно чрезмерно повысит ответственность производителей Интернета вещей, лишит их свободы действий и станет тормозом на пути технологических нововведений. Интернет вещей на текущем эта-

[58] *S.* 680 — SPY Car Act of 2017. URL: https://www.congress.gov/bill/115th-congress/senate-bill/680/text.

[59] *S.* 679 — Cyber AIR Act. URL: https://www.congress.gov/bill/115th-congress/senate-bill/679/.

[60] См.: Acting Federal Trade Commission Head: Internet of Things Should Self-Regulate. URL: https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation.

пе, по их мнению, является сферой, которая должна быть саморегулируемой.

Несмотря на отсутствие специального законодательного регулирования, Федеральная торговая комиссия может осуществлять регулятивные полномочия в этой сфере на основании п. 5 Акта о Комиссии, дающего ей право во внесудебном порядке противодействовать «несправедливой» (*unfair*) или «обманной» (*deceptive*) практике.

Предлагаемый режим неперсональных данных в Индии

Экспертный комитет, созданный Министерством электроники и информационных технологий Индии (*MeitY*), в 2019 г. разработал систему регулирования и использования неперсональных данных, отраженную в отчете комитета экспертов[61]. В нем говорится, что «мир наводнен данными» и их необходимо регулировать, чтобы создать экономическую ценность для страны и граждан. Комитет экспертов предлагает отдельный «новый национальный закон» для регулирования неперсональных данных, а также создание уполномоченного органа по неперсональным данным.

Среди задач, которые были возложены на Комитет, было определение того, что именно означает «неперсональные данные». Согласно отчету, когда данные не являются персональными данными, как они определены в законопроекте о защите персональных данных, или данные более не содержат никакой личной идентифицирующей информации (*PII*), они считаются неперсональными.

---

[61] См.: https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.

Отчет называет два вида неперсональных данных:

1) любые данные, которые не связаны с идентифицированным или идентифицируемым физическим лицом, например данные о погодных условиях;

2) персональные данные, которые были анонимизированы.

Комитет определил три категории неперсональных данных: публичные, коммунальные (или данные сообщества) и частные, а также сформулировал новую концепцию «чувствительности неперсональных данных», поскольку даже неперсональные данные могут быть чувствительными в случаях, если:

— они касаются национальной безопасности или стратегических интересов;

— это конфиденциальная информация или коммерческая тайна;

— анонимные данные несут в себе риск повторной идентификации.

Комитет стремился изложить аргументы в пользу регулирования данных, используя в качестве отправной точки природу данных как экономического блага. Комитет рекомендует, чтобы правила и положения были необходимы для управления данными таким образом, чтобы это привело к «созданию экономической ценности от использования данных, и генерированию экономических выгод для граждан и общин в Индии и раскрытию огромного потенциала социально-экономической ценности данных».

В отчете определены четыре ключевые роли, связанные с неперсональными данными: принципал данных, хранитель данных, доверительные управляющие (попечители) данными и трасты данных.

Принципалы данных — это физические лица, к которым относятся данные (в том числе после обезличива-

ния). Как правило, в этом случае речь идет о некоторых сводных или обобщенных данных, например сведениях о количестве избирателей. Если данные относятся к компаниям или иным сообществам, то принципалами данных считаются они.

Хранители данных — это те, кто осуществляет сбор, хранение, обработку, использование и т.д. данных таким образом, чтобы это отвечало наилучшим интересам принципалов данных. Правительство или частные компании, таким образом, могут быть хранителями данных, в то время как отдельные граждане, к которым относятся данные, будут принципалами. В отчете отмечается, что хранитель данных также может рассматриваться как доверенное лицо, подчиняющееся определенным указаниям и контролю и действующее в соответствии с интересами принципала данных / группы / сообщества. Такие «наилучшие интересы» сообщества должны быть направлены или доведены до сведения хранителей данных попечителями от имени основного сообщества данных. Это может быть сделано в форме рекомендаций по данным, рекомендуемых требований к практике обработки данных, руководящих принципов и т.д., но всегда нужно учитывать каноны наилучших интересов принципалов данных.

Хранители данных несут «обязанность заботиться» о заинтересованном сообществе в отношении обработки связанных с ним неперсональных данных. Это понятие представляет собой общий набор обязательств, которые со временем могут быть уточнены в нормативных положениях, практике, правилах, законодательстве и т.д. Отчет предполагает некоторые такие обязанности в отношении стандартов и требований анонимизации, протоколов и средств безопасного обмена данными и др.

Принципалы данных / сообщество будут осуществлять свои права на данные через соответствующего доверительного управляющего данными сообщества. В случае данных сообщества, в отличие от персональных данных, где физическое лицо может непосредственно осуществлять контроль над ними, возникает концепция доверительного управляющего данными сообщества. Такой доверительный управляющий будет осуществлять права от имени сообщества. Принципы и руководящие указания относительно того, кто может быть надлежащим доверительным управляющим в контексте данных группы/сообщества, будут изложены в упомянутом рамочном законодательстве. В общем он должен быть самым близким и наиболее подходящим представительным органом для соответствующего сообщества. Для большого количества данных сообщества соответствующий государственный орган или орган сообщества может выступать в качестве доверительного управляющего данными. Например, Министерство здравоохранения и благосостояния семьи, Правительство Индии могут быть доверительными управляющими данными о диабете среди индийских граждан, а объединения граждан (НПО), зарегистрированные в населенном пункте Уайтфилд в Бангалоре, могут быть доверенными лицами по данным управления твердыми отходами в Уайтфилде. Доверительные управляющие могут требовать от хранителей данных поделиться данными или, наоборот, не делиться ими с другими хранителями в зависимости от того, что больше соответствует интересам принципалов данных.

Наконец, трасты данных — это институциональные структуры, включающие определенные правила и протоколы для хранения и совместного использования на-

бора данных. Трасты данных могут содержать данные из нескольких источников, хранителей и т.д. и относиться к конкретному сектору либо набору цифровых или информационных услуг. Хранители данных могут добровольно делиться данными в этих трастах, поскольку многие частные организации могут выступить с предложением поделиться данными, хранящимися у них. Еще одним важным источником данных, объединенных в эти общие трасты, будут общественные организации, производящие и хранящие различные публичные данные.

Подобная идеалистическая структура, предлагаемая в отчете, уже вызвала критику. В нем часто и похвально отмечается важность действий в наилучших интересах субъекта данных, но не объясняется, что это означает. Также неясна предполагаемая докладом связь между хранителем и принципалом данных[62]. Неопределенность создает также порядок доступа правительства к данным. В отчете предполагается, что правительство может собирать и использовать неперсональные данные «в целях национальной безопасности, правоохранительной деятельности, правовых или нормативных целях». Отмечается, что такая широкая формулировка может подстегнуть озабоченность по поводу государственного надзора и потенциально отбить у потребителей желание делиться данными с правительством или бизнесом, задерживая инновации и рост[63].

Хотя комитет, состоящий из представителей сферы технологий, принадлежащих к правительственному, го-

[62] См.: *Sircar S.* Non-Personal Data: What the Govt Proposes & Why It Needs Reworking. URL: https://www.thequint.com/explainers/non-personal-data-meity-report-raises-more-questions-than-answers.

[63] Ibid.

сударственному и частному секторам, обсуждал этот вопрос в течение более девяти месяцев, в отчете не упоминаются какие-либо консультации с другими экспертами. «Очевидно, что это не было сделано в процессе общественных консультаций, поскольку это, по-видимому, создает новые правила и экономику, которая не имеет никакого сходства с состоянием данных в мире или требованиями индийского общества», — сказал Миши Чоудхари, технологический юрист и основатель компании *SFLC.in*. «Он замкнут в слишком узкой перспективе и не задает никаких междисциплинарных вопросов», — добавляет эксперт. Чоудхари указывает, что «вопиюще удивительной частью» является то, что связь фреймворка с Законом об авторском праве, Законом о коммерческой тайне или любыми другими законами вообще не обсуждалась, за исключением упоминания ожидающего рассмотрения законопроекта о защите персональных данных[64].

Предлагаемые режимы неперсональных данных в иных странах Азии

Дискуссии о необходимости специального регулирования отдельных аспектов оборота неперсональных данных ведутся в **Сингапуре**, что обусловлено реализацией подпрограммы «Национальная умная сенсорная платформа» (*Smart Nation Sensor Platform*) в рамках государственной программы «Умная нация»[65]. Отмечается, в частности, необходимость развития открытых стандартов в сфере Интернета вещей и избегания «огороженных садов», разбиваемых частными *IT*-компаниями, стремя-

[64] Ibid.

[65] См.: https://www.smartnation.sg.

щимися «запереть» пользователей в своих автономных экосистемах[66].

В настоящее время в Сингапуре внедрено пять стандартов, касающихся Интернета вещей: 1) стандарт в области сенсорных сетей в зонах публичного доступа; 2) стандарт в области сенсорных сетей в домовладениях; 3) стандарт эталонной архитектуры Интернета вещей; 4) стандарт совместимости данных и услуг Интернета вещей; 5) Рекомендации по безопасности в области Интернета вещей[67].

Таким образом, несмотря на перспективы дальнейшего развития Интернета вещей, правовые модели в этой сфере только разрабатываются. На современном этапе все же приоритетным остается техническое регулирование.

Схожая ситуация характерна для Японии. Национальный центр кибербезопасности при Правительстве Японии в 2016 г. опубликовал Общие принципы обеспечения безопасности *IoT*-систем[68]. В соответствии с названным документом ключевым направлением развития систем *IoT* является реализация принципа *Security by Design*. Предлагается двухступенчатый подход к реализации этого принципа: 1) определение общих требований к разработке, внедрению и функционированию *IoT*-систем; 2) определение секторальных требований с учетом специфики отдельных секторов. В документе отмечается необходимость определения фундамен-

---

[66] См.: Government's Duty to Set Open Standards for Internet of Things Deployment: Vivian Balakrishnan. URL: https://www.channelnewsasia.com/news/singapore/government-s-duty-to-set-open-standards-for-internet-of-things-10062284.

[67] См.: https://www.imda.gov.sg/itsc/technical-committees/internet-of-things-technical-committee-iottc.

[68] См.: General Framework for Secure IoT Systems. URL: https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf.

тальных требований к *IoT*-системам и последующей их регулярной адаптации к постоянно развивающимся технологиям.

Базовыми вопросами информационной безопасности, которые должны быть урегулированы на уровне законодательства, стандартов и саморегулирования, названы:

— определение *IoT*-систем и их классификация с учетом рисков информационной безопасности;

— обеспечение конфиденциальности, целостности и доступности информации в *IoT*-системах;

— обеспечение отказоустойчивости *IoT*-систем в случае нарушений информационной безопасности, в том числе обеспечение безопасности, целостности, доступности и конфиденциальности при реализации физических угроз и хакерских атаках, включая возможность оперативного восстановления сервисов;

— разграничение ответственности в сфере Интернета вещей и решение вопросов управления данными, в том числе вопросов, касающихся владения данными в *IoT*-системах.

В качестве иных вопросов, требующих регулирования, в документе упоминаются координация *IoT*-систем, расширение области полезного использования данных (*data utilization*), а также вопросы сертификации устройств в сфере *IoT*.

Промежуточные выводы

В настоящее время правовой режим оборота неперсональных данных только начинает складываться. Действующее законодательство есть только в Европейском союзе, однако и оно было принято совсем недавно, что не позволяет делать выводы о его успешности.

Законодательство о неперсональных данных призвано дополнить существующее регулирование оборота персональных данных и создать условия для безопасного оборота тех и других данных на формируемых цифровых единых рынках. Возможными препятствиями для этого остаются требования локализации, а также отсутствие технической возможности переносить данные, что приводит к возникновению «огороженных садов» и зависимости от конкретных поставщиков и операторов. Также среди проблем необходимо назвать интересы тех лиц, которые создают данные или к которым данные относятся, а следовательно, необходимы механизмы трансляции этих интересов в отношении лиц, обрабатывающих персональные данные. Дискуссия о возможности таких механизмов и их структуре ведется, но в настоящее время эффективное решение пока не найдено.

Тайны

Тайна частной жизни

В смысле, заложенном в ст. 12 Всеобщей декларации прав человека, тайна частной жизни не является тайной: Декларация запрещает произвольное вмешательство в личную и семейную жизнь, подразумевая под этим определенную сферу отношений, а не вид сведений. Эта формулировка дословно воспроизводится и в ст. 17 Международного пакта о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.), а в ст. 8 Конвенции о защите прав человека и основных свобод *ETS* № 005 (Рим, 4 ноября 1950 г.) вообще говорится о праве на уважение личной и семейной жизни.

В таком ключе неприкосновенность частной жизни понимается в **США** (где этот институт возник в конце XIX в.).

Лицо, необоснованно и серьезно нарушающее интерес другого лица в сохранении его поведения в неизвестности или в недоступности его облика для публики, несет ответственность.

Право на приватность нарушается путем:

— необоснованного вторжения в чужое уединение или частные дела;

— эксплуатации чужого имени или облика;

— необоснованной огласки чужой частной жизни;

— огласки, необоснованно показывающей другое лицо в неблагоприятном свете перед публикой[69].

---

[69] См.: *Prosser W.L.* Privacy // California Law Review. 1960. Vol. 48. No. 3. P. 389 (приводится по: *Дмитрик Н.А.* Истоки, смысл и перспективы института персональных данных // Вестник гражданского права. 2020. № 3. С. 49).

В США законы о тех или иных аспектах приватности действуют как на федеральном уровне, так и на уровне штатов. Например, только в Калифорнии принято более 25 правовых актов о запрете вторжения в частную жизнь в отдельных сферах.

Европейский суд по правам человека расширительно трактует рассматриваемое понятие, называя «частную жизнь» емкой категорией, которой невозможно дать исчерпывающее определение[70]. Эта категория шире, чем право на личную жизнь, и она касается таких сфер, внутри которых каждый человек волен развивать это понятие и наполнять его смыслом. В 1992 г. Суд заявил, что «было бы непозволительно ограничить понятие личной, частной жизни «внутренним кругом», в котором отдельный человек может жить жизнью, которую он выбирает, и исключить из нее внешний мир, не входящий в этот круг. Уважение к личной, частной жизни должно также включать определенный набор прав для установления и развития взаимоотношений с другими аспектами жизни человека»[71]. Частная жизнь с точки зрения Европейского суда по правам человека включает в себя физическую и психологическую неприкосновенность[72].

В практике европейских судов, прежде всего в **ФРГ**, недопустимость вторжения в частную жизнь обосновывается не только юридическими, но и экономическими

---

[70] См.: решение ЕСПЧ от 25.03.1993 по делу «Костелло-Робертс против Соединенного Королевства» (Costello-Roberts v. UK, жалоба № 13134/87).

[71] Решение ЕСПЧ от 16.12.1992 по делу «Нимиц против Германии» (Niemietz v. Germany, жалоба № 13710/88).

[72] См.: постановление ЕСПЧ от 24.04.2004 по делу «фон Ганновер (Принцесса Ганноверская) против Германии» (Von Hannover v. Germany, жалоба № 59320/00).

доводами. Долгий опыт рассмотрения дел о контроле правообладателями частного использования интеллектуальной собственности (например, контроле домашнего копирования фонограмм, документов и т.п.) еще в середине XX в. привел к формированию судебной практики, признающей экономическую нецелесообразность такого контроля[73]. Поэтому неприкосновенность частной жизни рассматривается не только как юридическое явление, но и как фактическое: вторжение в нее не только не является допустимым, но и в значительной степени невозможно, потому что сколько-нибудь длительный контроль частной жизни приводит к непоправимым экономическим и социальным последствиям.

Конституция Российской Федерации наделяет частную жизнь дуалистической охраной: ст. 23 говорит о праве на неприкосновенность частной жизни, личную и семейную тайну, ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Согласно позиции Конституционного Суда РФ право на неприкосновенность частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о себе; препятствовать разглашению сведений личного, интимного характера; в понятие «частная жизнь» включается область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит общественному и государственному контролю, если она не носит про-

[73] См. об этом: *Кувыркова А.Ю.* Осуществление исключительных интеллектуальных смежных прав: дис. ... канд. юрид. наук. М., 2010. С. 47; *Дмитрик Н.А.* Пределы правового регулирования в цифровую эпоху // Информационное общество. 2018. № 3. С. 55–56.

тивоправного характера[74]. При этом тайну личной жизни, семейную тайну определяет само лицо[75]. Соответственно, лишь само лицо вправе определить, какие именно сведения, имеющие отношение к его частной жизни, должны оставаться в тайне, а потому и сбор, хранение, использование и распространение такой информации, не доверенной никому, не допускается без согласия этого лица, как того требует Конституция РФ.

Как отмечает Конституционный Суд РФ, предполагается, что реализация другого конституционного права — права каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29 Конституции РФ) — возможна только в порядке, установленном законом, и что федеральный законодатель правомочен определить законные способы получения информации[76]. Следовательно, сбор или распространение информации о частной жизни лица допускается лишь в предусмотренном законом порядке и лишь в отношении сведений, которые уже официально кому-либо доверены самим лицом и в законном порядке собраны, хранятся, используются и могут распространяться. Иное приводило бы к произвольному, не основанному на законе вторжению в сферу частной жизни лица, право на неприкосновенность которой гарантируется Конституцией РФ, сужало бы понятие частной жизни и объем гарантий ее защиты.

---

[74] См.: определения КС РФ от 09.06.2005 № 248-О, от 26.01.2010 № 158-О-О и от 27.05.2010 № 644-О-О.

[75] См.: постановление КС РФ от 16.06.2015 № 15-П; апелляционное определение Алтайского краевого суда от 18.11.2015 по делу № 33-11032/2015.

[76] См.: постановление КС РФ от 31.03.2011 № 3-П.

Тайна связи

Формально тайна связи (коммуникаций) является единственной тайной, упомянутой на уровне таких международных документов, как Всеобщая декларация прав человека и Международный пакт о гражданских и политических правах, — в тех же статьях, которые устанавливают неприкосновенность частной жизни. Поскольку указанные документы не уточняют, какие сведения составляют тайну коммуникаций и на кого распространяются обязанности по ее сохранению, это решается на уровне национального законодательства или законодательства межгосударственных объединений.

Уважение к тайне корреспонденции прямо закреплено в ст. 8 **Европейской конвенции о защите прав человека и основных свобод** и ст. 7 Хартии Европейского союза об основных правах.

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

1) Директива Европейского парламента и Совета ЕС от 12.07.2002 № 2002/58/ЕС «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)» (далее — Директива *ePrivacy*);

2) проект Регламента Европейского парламента и Совета ЕС в отношении уважения частной жизни и защиты персональных данных в секторе электронных средств связи взамен Директивы № 2002/58/ЕС[77] (далее — Регламент *ePrivacy*).

---

[77] См.: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN.

В настоящий момент применяется Директива *ePrivacy*, однако в силу развития технологий и неактуальности ряда положений, а также необходимости приведения регулирования в соответствие с *GDPR* очевидно, что в ближайшем будущем будет принят новый акт, положения которого будут базироваться на Регламенте *ePrivacy*, поэтому мы полагаем необходимым привести основные нормы и этого документа тоже. Кроме того, как было отмечено в официальной позиции Европейского инспектора по защите данных[78], Регламент *ePrivacy* является одной из ключевых инициатив в рамках развития Стратегии Цифрового единого рынка[79], которая призвана обеспечить высокий уровень защиты для граждан и участников рынка на территории всего ЕС. Регламент будет иметь прямое действие на территории ЕС и применяться ко всем типам коммуникаций, включая мессенджеры, платформы, *IP*-телефонию (*VOIP*), коммуникации в рамках Интернета вещей (*IoT*, *M2M*) и т.д.

В соответствии с п. 1 ст. 5 Директивы *ePrivacy* конфиденциальность передаваемых сообщений и относящихся к ним данных трафика предполагает установление запрета государствами — участниками ЕС на «прослушивание, несанкционированное подключение, хранение или другие виды перехвата или слежки за сообщениями и относящимися к ним данными трафика лицами, не являющимися пользователями, без согласия заинтересованных пользователей». Аналогичное положение содержится и в ст. 5 Регламента *ePrivacy*. Режим

[78] См.: EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). URL: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf.

[79] См.: Digital Single Market. URL: https://ec.europa.eu/commission/priorities/digital-single-market_en.

конфиденциальности означает, что информация, которой обмениваются стороны при участии внешнего провайдера, включая информацию о времени отправки, отправителе и адресате, не должна быть известна кому-либо, кроме сторон.

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

Регламент *ePrivacy* в целом сохраняет этот подход, но использует иную терминологию, подразделяя данные на метаданные (*electronic communications metadata*) и содержание данных электронной связи (*electronic communications content*), которые в совокупности образуют данные электронной связи (*electronic communications data*) (ст. 4). Данные электронной связи определяются максимально широко и технологически нейтрально с целью охватить любую информацию, включая содержание передаваемых данных и информацию, касающуюся пользователей, обрабатываемую для целей передачи данных (включая данные об отправителе и адресате, их

местонахождении, дате, времени, продолжительности и типе коммуникации).

Таким образом, предметом охраны являются любые данные, передаваемые посредством сетей связи общего пользования и общедоступных услуг электронной связи, за исключением тех, которые предназначаются для потенциально неограниченного круга лиц и передаются в рамках широкого оповещения общественности по сети электронной связи.

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

Директива *ePrivacy* закрепляет, что обработка сообщений и трафика без согласия пользователей не допускается, за исключением случаев, установленных национальным законодательством в целях обеспечения национальной безопасности, расследования преступлений и т.д. Это, однако, не исключает возможность технического хранения данных, необходимого для передачи сообщения с соблюдением требований конфи-

денциальности. Дополнительно в Директиве говорится, что «установленные требования не должны затрагивать законодательно разрешенную запись сообщений и относящихся к ним данных трафика, когда такая запись производится в ходе законной деловой практики для целей представления доказательства совершения коммерческой сделки или осуществления любого другого делового взаимодействия» (ст. 5). Также прямо разрешается обработка данных трафика, необходимых для формирования счетов абонента за пользование связью и межсоединение в течение определенного промежутка времени (ст. 6 Директивы *ePrivacy*).

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

Согласно Директиве для обработки данных трафика в целях продвижения услуг электронных коммуникаций или дополнительных услуг провайдером общедоступных услуг электронной связи требуется получить предварительное согласие лица. Данные трафика подлежат удалению или анонимизации после достижения цели передачи сообщения. Третьи лица, действующие под руководством провайдеров, могут осуществлять обработку данных трафика в пределах, необходимых для управления трафиком или биллингом, рассмотрения требований клиентов, обнаружения случаев мошенничества, продвижения услуг электронной связи или предоставления дополнительных услуг при условии соблюдения установленных требований (п. 5 ст. 6 Директивы *ePrivacy*). Иные случаи привлечения третьих лиц и передачи им данных в Директиве *ePrivacy* прямо не урегулированы. Аналогично отсутствуют специальные положения о трансграничной передаче сведений и передаче сведений третьим лицам без согласия пользователей. Соответственно, в этой части применяются положения *GDPR*. На это прямо указывается в ст. 7 Регламента *ePrivacy*, в соответствии с которой содержание данных электронной связи может быть записано или иным образом сохранено пользователем или третьим лицом, которому пользователем поручены запись, хранение или иная обработка данных в соответствии с *GDPR*.

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

Право на тайну связи в **США** благодаря правоприменительной практике стало выводиться из Четвертой

поправки[80], и прослушивание телефонных разговоров без постановления суда стало трактоваться как ее нарушение (*Katz v. United States*). Право на тайну связи регламентируется следующими федеральными законами США: Закон о свободе информации (*the Freedom of Information Act of* 1996); Закон о частной жизни (*the Privacy Act of* 1974); Закон о конфиденциальности электронных сообщений (*the Electronic Communications Privacy Act, ECPA*), Закон о защите личных данных водителя (*the Driver's Privacy Protection Act of* 1994); Закон Меган (*Megan's Law of* 1999), Закон о борьбе с компьютерными мошенничеством и противоправным поведением (*the Computer Fraud and Abuse Act, CFAA*) и различные разделы Закона о связи (*the Communications Act*). *ECPA* и *CFAA* регулируют перехват электронных сообщений и несанкционированный доступ к компьютерам. Закон о содействии правоохранительным органам (*CALEA*), введенный в 1994 г., предусматривает, что все телекоммуникационное оборудование должно быть спроектировано таким образом, чтобы государственные органы США, наделенные соответствующими полномочиями, могли бы перехватить и прослушать телефонные разговоры[81]. Федеральная комиссия по связи США (*FCC*) является основным регулятором, следящим за соблюдением положений о конфиденциальности информации, относимой к тайне связи, в некоторой части разделяя компетенцию с Федеральной торговой комиссией (*FTC*).

---

[80] См.: *Kerr S.O.* Applying the Fourth Amendment to the Internet: A General Approach // Stanford Law Review. 2010. Vol. 62. Iss. 4. P. 1005–1050.

[81] См.: *Horniak V.* Privacy of Communication — Ethics and Technology. URL: http://www.idt.mdh.se/utbildning/exjobb/files/TR0390.pdf.

Правовая система США предполагает регулирование рассматриваемого вопроса на уровне штатов. *ECPA* не содержит дефиниции, позволяющей отграничить сведения, составляющие тайну связи, однако, например, Калифорнийский закон о конфиденциальности электронных сообщений (*CECPA*) говорит следующее: «Информация об электронной связи» включает в себя любую информацию об электронной коммуникации или использовании электронного коммуникационного сервиса, включая сведения о содержании, отправителе, получателе, местонахождении обоих в момент связи, *IP*-адресе и т.д., но не ограничиваясь ими»[82]. При этом Закон разделяет информацию об электронной связи и информацию об абоненте. Под последней понимаются имя, адрес, телефонный номер, адрес электронной почты или иная контактная информация, доступная провайдеру, идентификатор или номер абонента, продолжительность оказания услуг, виды услуг, предоставляемых или предоставленных абоненту.

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

Передачу сведений, составляющих тайну связи, в США регламентируют три акта: Закон о частной жизни (*Privacy Act*), Закон о конфиденциальности электронных сообщений (*ECPA*) и Закон о связи (*Communica-*

[82] Electronic Communications Privacy Act (Section 1546). URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB178.

tions Act of 1934). Первый устанавливает ограничение на распространение, разглашение и допуск государственных органов к информации, относимой к персональным данным. Второй нормативно-правовой акт запрещает провайдеру услуг электронной связи раскрывать содержание сообщений, которые он хранит и/или передает, и ограничивает раскрытие таких данных государственным органам (но не частным лицам). Третий нормативно-правовой акт ограничивает использование и разглашение пользовательской сетевой информации (*CPNI*) поставщиками телекоммуникационных услуг и предоставляет право доступа к таковой для самих пользователей — физических лиц[83].

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

В **России** понятие «тайна связи» определяется в ст. 23 Конституции, ст. 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» (далее — Закон о связи), ст. 15 Федерального закона от 17.07.1999 № 176-ФЗ «О почтовой связи» (далее — Закон о почтовой связи), в соответствии с которыми тайна связи означает тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электросвязи и по сетям почтовой связи.

В законодательстве принципы формирования сведений, составляющих тайну связи, не определены. Согласно применимым нормативным правовым актам, правовым

[83] См.: *Stevens G.* Privacy Protections for Personal Information Online. URL: https://fas.org/sgp/crs/misc/R41756.pdf.

позициям КС РФ и судебной практике других судов тайну связи составляют:

1) содержание любых сообщений, вне зависимости от средства передачи (через сети почтовой связи, посредством электросвязи, через Интернет), в том числе любые вложения, документы, информация, приложенные к таким сообщениям (ст. 63 Закона о связи, ст. 15 Закона о почтовой связи, постановление КС РФ от 26.10.2017 № 25-П);

2) содержание телефонных переговоров, а именно любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры (определение КС РФ от 02.10.2003 № 345-О);

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

4) сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях, т.е. технологическая, техническая информация, включая метаданные (ст. 63 Закона о связи). Интересно, что изначально тайной связи охранялось только содержание самих сообщений. Постепенно состав сведений расширяется практикой и начинает включать разного рода метаданные[84].

В российской судебной практике прослеживается разделение между информацией, составляющей тайну связи, и информацией о пользователях услугами связи, в особенности если запрос такой информации не вызван сообщениями, переданными такими пользователями. Как правило, суды и иные государственные органы не относят к тайне связи сведения об абонентах и оказывае-

[84] См.: *Терещенко Л.К.* Отдельные вопросы, возникающие в судебной практике при применении норм о тайне связи // Комментарий судебной практики / отв. ред. К.Б. Ярошенко. М., 2016. С. 145–153.

мых услугах, например ФИО абонентов, информацию о подключениях к интернет-ресурсам и т.д.[85]

При этом и в данном случае, как показывает складывающаяся судебная практика, основным определяющим критерием отнесения той или иной информации к тайне связи является отсутствие или наличие связи такой информации с коммуникациями пользователей. Если персональная информация абонентов / пользователей услуг связи запрашивается по причине, обусловленной коммуникациями абонентов/пользователей (например, детализация звонков), то такая информация может быть отнесена к тайне связи.

Закон о связи предусматривает, что предоставление третьим лицам сведений об абоненте может осуществляться только с их согласия, за исключением случаев предоставления органам, осуществляющим оперативно-разыскные действия, и ФСБ. При этом специальных правил и норм, определяющих порядок передачи (в том числе трансграничной) сведений, составляющих тайну связи, коммерческим организациям, законодательством не установлено.

Банковская тайна

По общему правилу в странах **Европейского союза** сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также государственным органам в случаях, предусмотренных законом, в частности в рамках противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

[85] См., напр.: постановления Курганского областного суда от 10.08.2015 № 4А-178/2015; Восьмого ААС от 12.10.2016 по делу № А70-5136/2016.

(далее — *AML/CFT*). В целом же вопрос установления режима банковской тайны и его пределов решается в каждом государстве — участнике ЕС самостоятельно. На практике это ведет к трудностям, например при несовпадении оснований и условий раскрытия сведений, составляющих банковскую тайну, в различных государствах в рамках мероприятий по *AML/CFT*.

Банковская тайна не является абсолютной. В качестве иллюстрации можно привести дело № C-580/13, позиция по которому была выражена в том числе на уровне Европейского суда[86]. Суть дела состояла в том, что правообладатель товарного знака *Davidoff Hot Water*, проведя закупку товара под данным товарным знаком, обнаружил, что товар является контрафактным. Правообладатель запросил данные о продавце у оператора платформы, однако продавец отрицал нарушение прав на товарный знак. Впоследствии правообладатель обратился к банку продавца с просьбой раскрыть данные владельца счета. Однако банк отказал, сославшись на действие банковской тайны. Истец настаивал на своем праве получить такую информацию на основе ст. 8 Директивы Европейского парламента и Совета ЕС от 29.04.2004 № 2004/48 об обеспечении прав на интеллектуальную собственность, согласно которой государства — члены ЕС должны обеспечить, чтобы при защите прав на интеллектуальную собственность компетентные органы могли предоставить правообладателям по их запросам необходимую информацию в отношении товаров и услуг, нарушающих их права. При этом такая информация включает

[86] Opinion of Mr Advocate General Cruz Villalón delivered on 16.04.2015. Case C-580/13 Coty Germany GmbH v. Stadtsparkasse Magdeburg. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A62013CC0580.

в том числе имена и адреса производителей, дистрибьюторов, поставщиков (п. 2 ст. 8 Директивы). Кроме того, указанное выше право не ограничивает положения, касающиеся защиты конфиденциальности источников информации или обработки персональных данных. Вопрос заключался в том, должна ли ст. 8 (3) Директивы толковаться как ограничивающая национальные положения, позволяющие банковским учреждениям со ссылкой на банковскую тайну отказывать в предоставлении информации в соответствии со ст. 8 (1) Директивы. Европейский суд ответил на данный вопрос утвердительно, отметив, однако, что при этом национальный суд должен оценить законность ограничения таких прав.

В результате в указанном деле Федеральный суд Германии, руководствуясь позицией Европейского суда, вынес решение о том, что банковская тайна может быть ограничена, а ее пределы должны толковаться исходя из баланса интересов[87].

В отсутствие законодательного определения банковской тайны факт отнесения той или иной информации к ней подлежит исследованию в каждом конкретном деле. Состав сведений, составляющих банковскую тайну, также не определен законодательно. В связи с этим можно сказать, что принцип формирования банковской тайны является открытым.

На уровне ЕС в актах различного уровня имеются положения о необходимости сохранения сотрудниками финансовых и надзорных учреждений служебной тайны в отношении сведений, которые стали им известны.

[87] Bundesgerichtshof Urteil vom 21.10.2015 I ZR 51/12. URL: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2015&anz=179&pos=0&nr=74346&linked=urt&Blank=1&file=dokument.pdf.

В ст. 37 Устава Европейского центрального банка[88] (далее — ЕЦБ) содержатся положения о том, что члены руководящих органов и персонал ЕЦБ и национальных центральных банков даже после прекращения своих функций обязаны не разглашать информацию, которая по своему характеру охватывается профессиональной тайной. Эта обязанность распространяет силу на лиц, которые имеют доступ к данным, подпадающим под действие законодательства Евросоюза, предписывающего хранить тайну.

Положения об установлении режима служебной тайны содержатся во многих директивах, регулирующих различные аспекты банковской деятельности. Например, в Директиве Европейского парламента и Совета ЕС от 26.06.2013 № 2013/36/ЕС о доступе к осуществлению деятельности кредитными организациями и пруденциальном надзоре за кредитными организациями и инвестиционными компаниями, вносящей изменения в Директиву № 2002/87/ЕС и отменяющей Директивы № 2006/48/ЕС и № 2006/49/ЕС, установлено, что «на всех лиц, которые работают в компетентных органах, а также на аудиторов и экспертов, действующих от имени компетентных органов, распространяется обязательство по соблюдению профессиональной тайны. Конфиденциальная информация, которую такие лица, аудиторы или эксперты могут получать в ходе осуществления их обязанностей, может быть раскрыта только в краткой или обобщенной форме, препятствующей идентификации отдельной кредитной организации, без ущерба случаям, к которым применяется уголовное законодательство».

[88] Протокол об Уставе Европейской системы центральных банков и Европейского центрального банка (в ред. Лиссабонского договора от 13.12.2007). URL: http://eulaw.ru/treaties/protoc/4.

Разрешается обмен информацией с контролирующими и некоторыми иными органами в установленных случаях. В равной степени к сфере банковского дела применимы требования законодательства об обработке персональных данных.

Таким образом, можно сказать, что на уровне ЕС банковская тайна обеспечивается преимущественно за счет установления режима служебной тайны для работников соответствующих кредитных и контролирующих структур и режима обработки персональных данных клиентов. Особое внимание уделяется регулированию на уровне ЕС единообразных для всех государств-участников правил по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Пределы раскрытия банковской тайны при расследовании *AML/CFT* преступлений определяет Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (Варшава, 16.05.2005). В соответствии с ее ст. 7 каждая сторона принимает законодательные и иные необходимые меры, предоставляющие компетентным органам полномочия принимать решения об истребовании/изъятии банковских, финансовых или коммерческих документов в целях выполнения действий, предусмотренных Конвенцией. Сторона не вправе отказаться выполнять положения этой статьи на основании банковской тайны. В целях идентификации и отслеживания доходов, сбора соответствующих доказательств допускается наблюдение, перехват телекоммуникационных сообщений, доступ к компьютерным системам и постановления о представлении конкретных документов. В соответствии с рекомендациями Группы

разработки финансовых мер борьбы с отмыванием денег (ФАТФ) законодательство о защите банковской тайны не должно препятствовать реализации рекомендаций[89] ФАТФ.

В **США** нормативными правовыми актами федерального уровня, которые предметом своего регулирования имеют банковскую тайну и составляющие ее сведения, являются Закон о праве на финансовую тайну (*RFPA*)[90], Закон о банковской тайне (*BSA*), Закон о добросовестном предоставлении кредитной информации (*FCRA*)[91], Закон Грэмма — Лича — Блайли (*GLBA*)[92].

GLBA регулирует сбор, использование, защиту и раскрытие (передачу) финансовыми организациями непубличной личной информации потребителей. Целью Закона является ограничение передачи такой информации и установление обязанности по уведомлению потребителей об обработке персональных данных.

Перечисленные выше нормативно-правовые акты, впрочем, не содержат понятия банковской тайны.

Так как США относится к семье общего права, для них характерно явление прецедента как одного из видов нормотворчества, поэтому во многом статутное право не закрепляет принципов формирования состава сведений, относимых к понятию банковской тайны. Та или

---

[89] Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения: Рекомендации ФАТФ. Февраль 2012. URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Russian.pdf.

[90] The Right to Financial Privacy Act. URL: https://www.gpo.gov/fdsys/pkg/CFR-2011-title31-vol1/pdf/CFR-2011-title31-vol1-part14.pdf.

[91] The Fair Credit Reporting Act. URL: https://www.gpo.gov/fdsys/pkg/CFR-2011-title16-vol1/pdf/CFR-2011-title16-vol1-chapI-subchapF.pdf.

[92] The Gramm — Leach — Bliley Act. URL: https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

иная информация понимается в качестве относящейся к банковской тайне исходя из конкретного рассматриваемого случая, а критерием формирования является отнесение признаков той или иной информации под конкретное нормативно-правовое регулирование.

На сегодняшний день вышеназванный *GLBA* содержит определение понятия «непубличная персональная информация»[93], под которой понимается финансовая информация, относящаяся к определенному потребителю (физическому лицу), (1) предоставленная потребителем финансовой организации, (2) сформированная в результате любой сделки с потребителем или любой услуги, выполняемой для потребителя, или (3) полученная финансовой организацией иным способом.

Банковскую тайну составляют: 1) сведения о клиентах кредитной организации и о корреспондентах клиентов; 2) сведения об операциях, счетах и вкладах клиентов и корреспондентов; 3) иная информация, содержащаяся в записях (*records*) финансовой организации.

Согласно рекомендациям Экспертного совета по финансовым институтам (*FFIEC*) к чувствительной информации потребителя относятся: имя, адрес или номер телефона в сочетании с номером социального страхования, номером кредитной или дебетовой карты либо личным идентификационным номером или паролем, которые позволят получить доступ к банковскому счету потребителя. Чувствительная информация о потребителе также включает любую комбинацию, позволяющую кому-либо войти в систему или получить доступ к учетной записи потребителя, например имя

[93] 15 U.S.C. § 6809 (4). URL: https://www.law.cornell.edu/uscode/text/15/6809.

пользователя и пароль или пароль и номер учетной записи[94].

Ввиду секторального подхода законодательного регулирования в США сведения, составляющие банковскую тайну, могут одновременно охраняться как иные виды тайн или иметь статус информации ограниченного доступа по иным основаниям: например, сведения о денежных переводах одновременно охраняются как тайна связи; сведения о вкладах, счетах, операциях по счету и иная подобная информация — как тайна частной жизни; сведения о клиенте и его корреспонденте — как персональные данные; кроме того, банковская и налоговая тайна из-за схожих предметов регулирования пересекаются во многих случаях.

GLBA устанавливает (1) обязанность ввести риск-ориентированную внутреннюю программу информационной безопасности в финансовой организации, (2) обязанность уведомлять потребителей о передаче их информации в некоторых ситуациях, содержит (3) норму о пассивном согласии (*opt-out*), при соблюдении которой согласие потребителя на передачу сведений предполагается, пока потребитель не ответит на запрос отказом.

Финансовая организация, рассматривающая передачу данных из неамериканской юрисдикции в США, должна учитывать, что записи, содержащие финансовую информацию (*financial records*), подлежат учету и контролю со стороны широкого круга американских регулирующих и правоохранительных органов.

---

[94] См.: Final Guidance on Response Programs Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. April 1, 2005. URL: https://www.fdic.gov/news/news/financial/2005/fil2705.html.

В законодательстве США имеется перечень случаев, при которых сведения могут передаваться без уведомления:

1) финансовая организация может раскрывать непубличную личную информацию потребителей в соответствии с требованиями федеральных законов или законов штатов, правилами и другими применимыми правовыми нормами;

2) финансовое учреждение может раскрывать непубличную личную информацию потребителей для ответа на запрос в рамках гражданского, уголовного расследования, а также по запросам суда либо федеральных, государственных или местных органов власти и для других целей, предусмотренных законом;

3) финансовое учреждение может раскрывать непубличную личную информацию потребителей для защиты или предотвращения фактического или потенциального мошенничества, несанкционированных трансакций и иных запрещенных законом действий;

4) в той мере, в какой это разрешено или требуется в соответствии с нормами закона и в соответствии с Законом о праве на финансовую неприкосновенность 1978 г. (*RFPA*), финансовое учреждение может раскрывать непубличную личную информацию правоохранительным органам для расследования по вопросам, касающимся общественной безопасности.

GLBA не запрещает передачу финансовой информации, относящейся к конкретному лицу, в адрес аффилированных компаний. Однако Закон о добросовестном предоставлении кредитной информации (*FCRA*) указывает, что такая передача аффилированным компаниям *в целях маркетинга* должна раскрываться потребителям по установленной процедуре: 1) факт передачи должен

быть четко и явно раскрыт потребителю в письменной форме или, если потребитель согласен, в электронном виде в кратком уведомлении; 2) потребителю должна быть предоставлена разумная возможность и разумный и простой способ отказаться от передачи этой информации; 3) потребитель не должен отказаться от такой передачи (*opt-out*).

Кроме того, передача сведений может осуществляться в адрес третьих лиц (неаффилированных компаний) также в рамках процедуры *opt-out*[95]. Финансовая организация не имеет права раскрывать никому, кроме агентства по предоставлению отчетности, номер счета или код доступа от счета кредитной карты, депозитного счета и т.д. любому не аффилированному с финансовой организацией лицу для использования в телемаркетинге, прямом маркетинге или другом виде маркетинга, осуществляемого посредством электронной почты.

Согласие *opt-out* неприменимо к третьим лицам (неаффилированным компаниям), если (1) между ним и финансовой организацией заключен контракт о признании и хранении этой информации как конфиденциальной, т.е. третье лицо не может использовать такую информацию для раскрытия ее иным лицам[96], *или* если (2) третье неаффилированное лицо исполняет функцию финансовой организации от ее имени.

Наконец, требования к уведомлению и *opt-out* также неприменимы к поставщикам услуг (обслуживающим компаниям) и к проектам совместного маркетинга, если (1) третье неаффилированное лицо исполняет функцию

[95] 15 U.S.C. § 6802 (b). URL: https://www.law.cornell.edu/uscode/text/15/6802.

[96] См.: A Legal Guide to Privacy and Data Security. URL: https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf.

финансовой организации от ее имени и если (2) финансовая организация раскрывает сведения о потребителе этим третьим лицам, поскольку это необходимо для осуществления, администрирования или принудительного исполнения трансакции, на осуществление которой потребитель дал разрешение.

Субъект данных (потребитель) не имеет права требовать изменения, удаления, доступа, добавления персональных данных, хранимых в финансовой организации[97].

В **России** банковская тайна включает сведения об операциях, о счетах и вкладах клиентов кредитных организаций и корреспондентов клиентов, а также иные сведения, устанавливаемые кредитной организацией, если это не противоречит федеральному закону (ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»; далее — Закон о банках и банковской деятельности). В отличие от иных видов тайн состав сведений, составляющих банковскую тайну, определен в достаточной степени и не содержит оценочных и описательных категорий, которые бы требовали дополнительного толкования.

КС РФ рассматривает банковскую тайну как частный случай тайны личной жизни. Соответственно, ее ограничение возможно только на условиях и в порядке, которые закреплены в ст. 55 Конституции РФ, т.е. только на основании федеральных законов. Конституционный Суд высказал важные правовые позиции по вопросу соотношения банковской тайны и тайны личной жизни[98].

---

[97] 15 U.S.C. § 6801–6809. URL: https://www.notarylearningcenter.com/pdf/GrammLeachBliley.pdf.

[98] См.: постановление КС РФ от 14.05.2003 № 8-П; определение КС РФ от 14.12.2004 № 453-О.

Предусмотренные в законе отступления от банковской тайны не могут быть произвольными. Такие отступления (в частности, предоставление банками, иными кредитными организациями и их служащими сведений о счетах и вкладах и операциях по счету, а также сведений о клиентах государственным органам и их должностным лицам) должны отвечать требованиям справедливости, быть адекватными, соразмерными и необходимыми для защиты конституционно значимых ценностей, в том числе частных и публичных прав и интересов граждан, не затрагивать существо соответствующих конституционных прав, т.е. не ограничивать пределы и применение основного содержания закрепляющих эти права конституционных положений, и могут быть оправданы лишь необходимостью обеспечения указанных в ч. 3 ст. 55 Конституции РФ целей защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов других лиц и общественной безопасности.

Порядок предоставления сведений, составляющих банковскую тайну, урегулирован в ст. 26 Закона о банках и банковской деятельности. В основном эта статья предусматривает случаи и условия предоставления таких сведений различным государственным органам и организациям для исполнения их функций. Среди таких органов налоговые органы, Пенсионный фонд РФ, суды, Фонд социального страхования РФ и т.д. В этой статье прямо закреплена возможность предоставления сведений, составляющих банковскую тайну, в головную кредитную организацию (управляющую компанию) банковского холдинга, аудиторским организациям. В литературе случаи предоставления банковской тайны по порядку и

форме принято делить следующим образом: а) по специальным запросам государственных органов; б) в составе отчетной и иной обязательной документации; в) в порядке уведомления, в силу предписания закона комитету по финансовым рынкам[99]. Каких-либо специальных условий передачи сведений названным организациям Закон о банках и банковской деятельности не содержит (помимо головных организаций, расположенных на территории иностранных государств).

Коммерческая тайна

Правовой режим коммерческой тайны[100] распространяется на сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, у которых нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. То есть информация, составляющая коммерческую тайну, должна соответствовать нескольким требованиям: 1) иметь коммерческую ценность в силу неизвестности ее третьим лицам; 2) у третьих лиц не должно быть свободного доступа к этой информации; 3) в отношении нее должен быть введен режим коммерческой тайны (в том числе предпри-

[99] См., напр.: *Селивановский А.С.* Банковская тайна: состояние и проблемы. URL: http://selivanovsky.ru/pages/bankovskaya_tajna/.

[100] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

няты действия к ее защите от несанкционированного доступа).

Коммерческая ценность индустриальных данных далеко не обязательно связана с фактом неизвестности ее третьим лицам. У третьих лиц может быть как минимум опосредованный доступ к этим данным (например, возможность сбора данных о транспортных потоках, о температуре, влажности и т.п. с помощью аналогичных устройств). Защита индустриальных данных посредством введения режима коммерческой тайны и мер противодействия несанкционированному доступу возможна, но в ряде случаев может потребовать значительных затрат. Кроме того, следует учитывать ограниченный характер охраны коммерческой тайны, которая не распространяется на случаи честного (законного) использования в коммерческих целях (в отличие от интеллектуальной собственности охрана коммерческой тайны не имеет исключительного характера).

Регулированию этого вида тайн в **Европейском союзе** посвящена Директива Европейского парламента и Совета ЕС от 08.06.2016 № 2016/943 о защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия (далее — Директива № 2016/943). Государства — члены ЕС должны были до 9 июня 2018 г. привести свое национальное законодательство в соответствие с положениями Директивы № 2016/943. При этом они вправе предусмотреть дополнительные способы защиты коммерческой тайны.

Как отмечено в преамбуле Директивы, «коммерческая тайна играет важную роль в деле защиты обмена знаниями между субъектами предпринимательской деятельности, включающими в себя, в частности, малые и средние пред-

приятия (*SMEs*), а также исследовательские учреждения в пределах и за рамками внутреннего рынка, в области исследований, разработок и инноваций. Коммерческая тайна является одной из наиболее общераспространенных форм защиты бизнесом результатов интеллектуальной деятельности и инновационного ноу-хау, однако в то же время коммерческая тайна является наименее защищенной с помощью средств имеющейся правовой базы Союза от незаконного приобретения, использования или раскрытия третьими лицами».

Определение коммерческой тайны содержится в ст. 2 Директивы № 2016/943: в частности, коммерческая тайна обозначает информацию, отвечающую всем нижеперечисленным требованиям:

а) она является секретной в том смысле, что полностью или в части не является общеизвестной или общедоступной для круга лиц, обычно имеющих дело с такого рода информацией;

б) она обладает коммерческой ценностью, так как недоступна третьим лицам;

в) владельцем информации были предприняты необходимые меры для сохранения ее в тайне.

В преамбуле Директивы № 2016/943 отмечено, что такое определение коммерческой тайны охватывает ноу-хау, деловую информацию и техническую информацию, в случае если эта информация соответствует установленным требованиям, и ее владелец вправе сохранить ее в секрете. Виды информации, которые могут составлять коммерческую тайну, не могут быть ограничены. «Под определение коммерческой тайны не подпадает обычная информация и опыт, полученный сотрудниками в ходе обычного выполнения ими их трудовых обязанностей, а также из определения исключается общеизвестная информация

или информация, к которой имеется свободный доступ лиц, в кругу которых принято иметь дело с такого рода информацией. Примечательно, что ни на информацию, охраняемую в качестве коммерческой тайны, ни на ноу-хау не устанавливается никаких исключительных прав». Таким образом, должна сохраняться возможность для самостоятельного выявления одних и тех же ноу-хау или информации.

Использование или разглашение коммерческой тайны может осуществляться исключительно с согласия ее обладателя. Нарушителем, а значит, и ответчиком может быть любое лицо, которое приобрело информацию, составляющую коммерческую тайну, незаконно, в частности путем несанкционированного доступа, присвоения, копирования документов, предметов, материалов, веществ или электронных файлов, либо нарушило соглашение о конфиденциальности, либо нарушило договорное или любое другое обязательство по ограничению использования коммерческой тайны (п. 2, 3 ст. 4 Директивы № 2016/943). Обязательство по сохранению конфиденциальности информации накладывается на всех участников судебного разбирательства по вопросу незаконного приобретения, использования или раскрытия коммерческой тайны.

Приобретение, использование и раскрытие коммерческой тайны в случаях, разрешенных законодательством, должно расцениваться как правомерное. В частности, это относится к приобретению и раскрытию коммерческой тайны в контексте осуществления прав представителей работников на получение информации, консультаций, в ходе коллективной защиты прав работников и работодателей, а также к приобретению или раскрытию коммерческой тайны при проведении обязательного аудита.

В соответствии с Директивой № 2016/943 государства — члены ЕС обязаны обеспечить, чтобы за раскрытие коммерческой тайны и иные правонарушения компетентные судебные органы могли применить к нарушившей стороне «одну или более из нижеуказанных мер:

(*a*) прекращение или, в зависимости от ситуации, запрет использования или раскрытия коммерческой тайны;

(*b*) запрет на производство, предложение, размещение на рынке или использование контрафактных товаров или импорт, экспорт или хранение контрафактных товаров для указанных целей;

(*c*) принятие в отношении контрафактных товаров надлежащих корректировочных мер (изъятие с рынка контрафактных товаров, лишение контрафактных товаров их контрафактных качеств, уничтожение контрафактных товаров);

(*d*) уничтожение полностью или частично любого документа, объекта, материала, вещества или электронного файла, содержащего или воплощающего собой коммерческую тайну, или, если применимо, передача заявителю полностью или частично любых из указанных документов, объектов, материалов, веществ или электронных файлов».

Вместо перечисленных мер суды должны при определенных условиях иметь право взыскать денежную компенсацию (если лицо добросовестно приобрело коммерческую тайну, но только позднее узнало, что информация была получена из источников, использующих соответствующую коммерческую тайну незаконно) либо возместить владельцу коммерческой тайны ущерб в размере, равном действительному ущербу, причиненному в результате незаконного приобретения, использования или раскрытия коммерческой тайны.

В **США** коммерческая тайна (*trade secrets*) регулируется как на федеральном уровне, так и законами отдельных штатов, ориентирующимися на Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС) и Модельный закон о коммерческой тайне 1985 г. (*Uniform Trade Secrets Act of* 1985)[101]. При этом в ст. 39 (2) ТРИПС охрана коммерческой тайны понимается как защита информации, которая на законных основаниях контролируется юридическим или физическим лицом и которая:

а) является конфиденциальной, поскольку в целом либо в конкретном сочетании или расположении ее компонентов не является известной или легко доступной лицам, принадлежащим определенному кругу, обычно имеющему дело с подобным видом информации;

б) имеет коммерческую ценность;

в) в конкретных обстоятельствах была подвергнута определенным мерам охраны лицом, контролирующим эту информацию на законных основаниях, в целях сохранения ее секретности.

Эти положения воспроизведены и в Модельном законе 1985 г., в соответствии с которым коммерческая тайна:

1) приобретает независимую экономическую ценность, фактическую или потенциальную, поскольку она не является общеизвестной и не может быть легко установлена надлежащими средствами другими лицами, которые могут получить экономическую ценность от ее раскрытия или использования;

---

[101] См.: Office of Policy and External Affairs United States Patent and Trademark Office. Trade Secrets Protection in the U.S. URL: https://www.nist.gov/system/files/documents/mep/marinaslides.pdf.

2) представляет собой предмет усилий, которые являются разумными в данных обстоятельствах для сохранения ее секретности.

Федеральный закон о защите коммерческой тайны 2016 г. создал исковую защиту коммерческой тайны на федеральном уровне, дав сторонам споров выбор между локализованными спорами в соответствии с законами штата или спорами в соответствии с этим Федеральным законом, рассматриваемыми в федеральных судах. Хотя законы штатов различаются, между ними есть сходство, поскольку почти все штаты приняли ту или иную форму Модельного закона 1985 г.

Суды могут защищать коммерческую тайну, запрещая неправомерное присвоение, предписывая сторонам, незаконно присвоившим коммерческую тайну, принимать меры для ее сохранения, а также принимая решение о принудительном роялти. Суды также могут присуждать убытки, судебные издержки и разумные гонорары адвокатов. Эта защита очень ограничена, поскольку владелец коммерческой тайны защищен только от несанкционированного раскрытия и использования, которое называется незаконным присвоением. Если владелец коммерческой тайны не соблюдает секретность или если информация самостоятельно обнаруживается, разглашается или иным образом становится общеизвестной, защита коммерческой тайны утрачивается. Срок действия коммерческой тайны не истекает, поэтому защита продолжается до обнаружения или утраты[102].

В **России** существует дуалистический режим охраны информации, составляющей коммерческую тайну. С од-

[102] См.: Trade Secret Policy. URL: https://www.uspto.gov/ip-policy/trade-secret-policy.

ной стороны, она охраняется в режиме тайны в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», с другой — как разновидность интеллектуальной собственности (секрет производства) в соответствии с четвертой частью ГК РФ. Таким образом, в России понятия «секрет производства» и «информация, составляющая коммерческую тайну» максимально близки по содержанию, о чем свидетельствуют их легальные определения.

В качестве условия правовой охраны информации закон требует, чтобы лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании (обладатель информации), ограничило доступ к ней и установило в отношении нее режим коммерческой тайны. С фактическим ограничением доступа к информации (так называемая фактическая монополия) закон связывает юридическое ограничение возможности использования информации (исключительное право, т.е. юридическая монополия).

Обладателю секрета производства принадлежит исключительное право использования его любым не противоречащим закону способом (исключительное право на секрет производства), в том числе при изготовлении изделий и реализации экономических и организационных решений. Обладатель секрета производства может распоряжаться указанным исключительным правом. Лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета производства, приобретает самостоятельное исключительное право на этот секрет производства.

Режим коммерческой тайны не исключает доступа к соответствующей информации органов государственной власти, иных государственных органов, органов местного самоуправления. Мотивированное требование соответствующего органа о предоставлении информации, составляющей коммерческую тайну, должно быть подписано уполномоченным должностным лицом, содержать цель и правовое основание затребования информации, составляющей коммерческую тайну, а также срок ее предоставления, если иное не установлено федеральными законами. Органы государственной власти, иные государственные органы, органы местного самоуправления обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им ее обладателями.

В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

Предоставление права использования секрета производства осуществляется по лицензионному договору или договору об отчуждении исключительного права. При этом обе стороны договора (как обладатель, так и получатель секрета производства) обязаны сохранять конфиденциальность секрета производства в течение всего срока действия лицензионного договора.

Ответственность за нарушение исключительного права на секрет производства связана как с незаконным использованием секрета производства, так и с неправомерным получением таких сведений или с их разглашением (если у нарушителя существовала обязанность сохранять конфи-

денциальность секрета производства). Ответственность связана с обязанностью нарушителя возместить убытки, причиненные нарушением исключительного права на секрет производства, если иная ответственность не предусмотрена законом или договором с этим лицом. Лицо, которое использовало секрет производства и не знало и не должно было знать о том, что использование незаконно, в том числе в связи с тем, что оно получило доступ к секрету производства случайно или по ошибке, не несет ответственности.

Исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание. С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей.

Промежуточные выводы

В таких юрисдикциях, как США и Европа, сложилась система тайн, выстроенных как по отраслевому (банковская тайна, тайна связи) признаку, так и по предметному (коммерческая тайна, тайна частной жизни). Эти правовые режимы имеют долгую историю своего развития и направлены на защиту важнейших интересов лиц, к которым они относятся. Основанием для установления режима тайны во всех случаях является то, что разглашение информации, составляющей ту или иную тайну, способно причинить вред тому лицу, к которому относится тайна (принципалу тайны).

В целом аналогичная система тайн выстроена в Российской Федерации, что обусловливается участием России в базовых международных договорах по

правам человека, по обмену информацией между государствами, а также по защите интеллектуальной собственности.

В Российской Федерации в рамках реализации национальной программы «Цифровая экономика РФ» периодически ведутся дискуссии об изъятии технологической, технической информации из тайны связи. Центром компетенций по нормативному регулированию цифровой среды (Фонд «Сколково») предлагается внести следующие изменения в действующий Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (далее — Закон о связи).

Действующая ст. 63 Закона о связи является архаичной, так как ее положения не позволяют работникам операторов связи осуществлять «осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи» (ч. 3); получать «сведения о передаваемых по сетям электросвязи сообщениях» (ч. 4).

Осмотр вложений, ознакомление с информацией, передаваемой по сетям электросвязи, получение сведений о передаваемых по сетям электросвязи сообщениях работниками оператора связи в информационном, постиндустриальном обществе в условиях цифровой трансформации при современном уровне развития информационно-коммуникационных технологий являются непосредственными компонентами технологического цикла оказания услуг связи физическим и юридическим лицам операторами. Осмотр вложений, равно как ознакомление с информацией, получение сведений о передаваемых по сетям электросвязи сообщениях в нынешних реалиях означают получение работниками оператора связи технической, служебной информации об элек-

тронных сообщениях, содержащейся в информационных системах оператора связи, обеспечивающих функционирование инфраструктуры сетей связи. При этом такая информация не относится к содержанию сообщений. Поэтому в ч. 3, 4 ст. 63 Закона о связи необходимы соответствующие уточнения, представленные в законопроекте.

Определение КС РФ от 02.10.2003 № 345-О: «Право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает **комплекс действий по защите информации**, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются **любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры,** включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи (т.е. детализация переговоров); **для доступа к указанным сведениям** (выделено нами. — *Ред.*) органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования статьи 23 (часть 2) Конституции Российской Федерации о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения». Аналогичная позиция подтверждена в определении КС РФ от 21.10.2008 № 528-О-О.

Предлагаемые изменения в соответствии с приведенными положениями КС РФ к тайне связи относят три компонента:

— содержание сообщений;

— доступ к содержанию (с последующим ознакомлением);

— сообщения пользователей услуг связи, передаваемые с помощью пользовательского оборудования (оконечного оборудования) или телефонной аппаратуры.

При этом такие изменения затрагивают:

— сведения средств связи оператора связи, не являющихся оконечным оборудованием и содержащих данные об объемах и стоимости оказанных услуг связи;

— сведения радиоэлектронных средств оператора связи, с помощью которых осуществляется подключение пользовательского оборудования абонента к сети подвижной радиотелефонной связи, указывающие положение пользовательского оборудования абонента относительно радиоэлектронных средств.

Эти сведения не являются тайной связи по критериям, установленным в Конституции Российской Федерации и положениях Конституционного Суда, так как при современном уровне развития технологий у операторов связи существуют средства связи, не являющиеся оконечным оборудованием, а также радиоэлектронные средства оператора связи, с помощью которых осуществляется подключение пользовательского оборудования абонента к сети, с информацией о местоположении пользовательского оборудования абонента относительно инфраструктуры и сооружений сети связи операторов связи.

Принятие предлагаемых изменений позволит:

— уточнить в ст. 63 Закона о связи архаичные нормы, не соответствующие текущим реалиям;

— упорядочить нормы ст. 63 Закона о связи в целях применения, соответствующего положениям Конституции РФ и позициям Конституционного Суда РФ;

— определить трехкомпонентную защиту тайны связи пользователей услугами связи, физических и юридических лиц, а следовательно, обеспечить их информационную безопасность;

— операторам связи на законном основании пользоваться служебной, технической, технологической информацией, содержащейся в информационных системах, предназначенных для функционирования инфраструктуры связи и сетей связи.

Предлагаемые изменения окажут положительное влияние на развитие оказания услуг связи в Российской Федерации, придадут им бóльшую прозрачность и однозначность правоприменения.

При формировании предлагаемых изменений Центром компетенций по нормативному регулированию цифровой среды (Фонд «Сколково») проводилась методическая и консультативная работа совместно с ИЗиСП и Минцифрой России.

Общедоступная информация

Свобода доступа к информации

В зарубежных странах общедоступность информации является не столько элементом правового режима самой информации, сколько следствием реализации базового права человека на доступ к информации[103], предусмотренного ст. 19 Всеобщей декларации прав человека и ст. 19 Международного пакта о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.).

В **США** по общему правилу вся информация, находящаяся в открытом доступе, в том числе сведения персонального характера, может быть использована без ограничений, за исключением случаев, указанных в законе (принцип «разрешено по умолчанию, если иное не установлено законом»). Это основано на Первой поправке к Конституции США о защите свободы слова. Открытый характер сети Интернет подчеркнут в решениях Верховного суда США. В частности, им был признан неконституционным закон Северной Каролины, называвший правонарушением использование лицом, осужденным за преступления сексуальной направленности, социальных сетей вроде *Facebook* или *Twitter*. Верховный суд отметил, что «в настоящее время социальные сети явля-

[103] См.: OECD. Right to Access Information. URL: https://www.oecd.org/mena/governance/right-to-access-information-2018.pdf.

ются источником получения сведений о происходящем в мире, изучения вакансий на работу; общения в современном публичном пространстве и изучения достижений человеческой мысли и знаний»[104].

Свободе слова могут быть противопоставлены другие права и свободы, например неприкосновенность частной жизни, защита коммерческой тайны, секретной информации и т.п. Нахождение баланса между ними в каждом конкретном случае относится к полномочиям законодателей или судов. Ограничения на свободное использование публично доступной информации, как правило, обусловлены необходимостью защиты определенных субъектов. Типичный пример — требование *Children's Online Privacy Protection Act* о получении согласия от несовершеннолетнего или его законного представителя при осознанном сборе данных о таком лице (*knowingly collect personal information from children*). Таким образом, несмотря на возможный общедоступный характер такой информации (размещение ее в социальной сети), если она касается несовершеннолетнего, требуется выполнение определенных формальностей.

Другой пример касается сферы трудовых отношений. Ряд штатов США приняли законы, запрещающие сотрудникам кадровых служб и рекрутерам использовать информацию, содержащуюся в социальных сетях, для принятия решений о трудоустройстве, продвижении по службе и т.п., за исключением случаев, когда такие данные необходимы для расследования трудовых правонарушений[105]. По общему правилу для получения доступа

[104] Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

[105] *Deschenaux J.* State Laws Ban Access to Workers' Social Media Accounts. URL: https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/states-social-media.aspx.

к такого рода данным необходимо согласие субъекта. Эти законы имеют в своей основе стремление минимизировать риски дискриминации по различным защищенным классам (сведениям о расовой, национальной принадлежности, религиозных, политических взглядах, сексуальной жизни, здоровье и др.).

Когда тот или иной правовой акт США использует широкий подход к ограничениям для защиты определенных лиц (например, Закон Калифорнии «О защите неприкосновенности частной жизни в цифровой среде» 2018 г., Закон Грэмма — Лича — Блайли 1999 г.), делается соответствующее изъятие в отношении публично доступной информации, которое является адекватным с учетом контекста соответствующего закона. Так, в упомянутом Законе Калифорнии указано, что понятие персональной информации не включает в себя публично доступную информацию, т.е. «информацию, которая законно доступна из записей в государственных органах. Информация не является публично доступной, если она используется для целей, которые несовместимы с целями, для которых она была собрана и предоставляется государственными органами».

Равным образом свобода слова охраняется и в **Европейском союзе:** ст. 10 Конвенции о защите прав человека и основных свобод *ETS* № 005 предусматривает свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ. Как неоднократно указывал Европейский суд по правам человека, ст. 10 не только обязывает прессу сообщать информацию и идеи, представляющие общественный интерес, но и гарантирует право общественности быть информирован-

ной должным образом[106]. Однако это право связано не только с сообщениями, передаваемыми средствами массовой информации[107].

В то же время ч. 2 ст. 10 Конвенции допускает ограничения свободы слова, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия. В частности, законодательство ЕС о персональных данных устанавливает разрешительный порядок доступа к ним, что противопоставляет правовой режим персональных данных свободе слова.

Баланс между интересом лица контролировать данные о себе и общественным интересом в доступе к информации обеспечивается работой сложного правового механизма, учитывающего цели обработки и их совместимость с первоначальными целями сбора данных, а также волю субъекта на обработку данных и ограничение (или отсутствие ограничений) на доступ к ним. В силу этого обработка общедоступных специальных категорий персональных данных (ст. 9 *GDPR*) возможна только тогда, когда сам субъект явно выраженным образом сделал эти

---

[106] См.: *Сальвиа М., де.* Прецеденты Европейского суда по правам человека. Руководящие принципы судебной практики, относящиеся к Европейской конвенции о защите прав и основных свобод. Судебная практика с 1960 по 2002 г. СПб., 2004. С. 631, 634, 659.

[107] См.: *Эктумаев А.Б.* Свобода слова в решениях Европейского суда по правам человека // Вестник Пермского университета. Юридические науки. 2011. Вып. 3. С. 54–58.

данные публично доступными (*manifestly made public by the data subject*). В разъяснениях рабочей группы ст. 29 указано, что явно выраженное опубликование должно пониматься в узком смысле, когда субъект осознает и предупрежден о доступности его персональных данных любому лицу, включая государственные органы[108]. При этом рабочая группа делает акцент на соблюдении принципа необходимости в обработке специальных категорий персональных данных и наличии серьезных оснований (*solid justifications*) для такой обработки.

Идея о том, что баланс между доступом к информации и защитой персональных данных определяется совместимостью целей обработки (первоначальных и новых), находит свое закрепление и в законодательстве неевропейских государств. Так, Комиссией по защите персональных данных **Гонконга** были разработаны руководящие правила по использованию общедоступных персональных данных[109]. В них указано, что возможность доступа к персональным данным из открытого источника не подразумевает наличие бланкетного согласия субъекта персональных данных на их обработку в любых целях. Если первоначальная цель явно обозначена самим субъектом персональных данных либо оператором (например, в политике обработки персональных данных), следует руководствоваться ею. Если же цель явно не обозначена, то следует применить тест «разумных ожиданий»: при оценке допустимости обработки общедоступных персональных данных необходимо

[108] См.: Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680). URL: https://ec.europa.eu/newsroom/article29/items/610178.

[109] См.: Guidance on Use of Personal Data Obtained from the Public Domain. URL: https://www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf.

определить, посчитало ли бы обычное физическое лицо в имеющихся обстоятельствах неприемлемой обработку его общедоступных персональных данных в новых целях, в которых предполагается их обработка.

В законодательстве **Сингапура** общедоступные персональные данные (*publicly available personal data*) определяются как «персональные данные, доступные неопределенному кругу лиц (*generally available to the public*) и включающие в себя персональные данные, которые возможно наблюдать с помощью разумно ожидаемых средств (*can be observed by reasonably expected means*) в месте или на событии, где появляется физическое лицо, которое открыто для посещения неопределенным кругом лиц»[110]. Общедоступные данные могут собираться, передаваться и использоваться без согласия субъекта персональных данных, однако в соответствии с официальными разъяснениями государственного органа Сингапура в сфере защиты персональных данных необходимо различать ситуации, когда данные доступны для членов интернет-сообщества и при этом членство в таком сообществе открыто и может быть получено без существенных усилий (посредством несложной регистрации), и ситуации, когда персональные данные сообщаются узкому кругу лиц (семье, друзьям) либо случайно сообщаются незнакомому лицу. Таким образом, если информация из профайла социальной сети доступна всем членам этой социальной сети, то такая информация является общественно доступной. Если информация доступна ограниченному кругу лиц из списка друзей и на размещаемый контент установлены ограничения по его

[110] Статья 2 Акта о защите персональных данных Сингапура. URL: https://sso.agc.gov.sg/Act/PDPA2012.

дальнейшему распространению (репосту), то она не может признаваться общественно доступными данными[111].

В **России** помимо аналогичных положений Конституции о свободе слова (ч. 4 ст. 28) и соответствующих им положений законодательства о массовой информации существуют особые правовые режимы общедоступной информации (согласно ст. 7 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации) к ней относятся общеизвестные сведения и иная информация, доступ к которой не ограничен) и персональных данных, разрешенных субъектом персональных данных для распространения (ст. 10.1 Закона о персональных данных). Правда, содержание первого из названных правовых режимов в законе не раскрывается, что приводит к неопределенности на практике, а второй правовой режим фактически делает распространение персональных данных чрезмерно затруднительным. Применительно к общедоступной информации указано лишь, что она может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения этой информации. Таким образом, эта норма хотя и устанавливает презумпцию общедоступности информации, но делает затруднительным определение круга ограничений на использование информации, а также отнесение ее к общедоступной.

---

[111] См.: Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Singapore). URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf.

Доступ к государственной информации и открытые данные

До принятия в **США** ключевого акта — Закона о свободе информации (*Freedom of Information Act, FOIA*) федеральные агентства были свободны в своем решении о публикации документов. Это положение, закрепленное разделом 3 Акта об административных процедурах 1946 г., серьезно затрудняло доступ общественности к информации о государстве, его планах и процедурах. Вступивший в силу с 1967 г. Закон о свободе информации предусмотрел полное или частичное обнародование информации и документов Правительства США и применяется только к документам органов исполнительной власти. Он внес важный вклад в развитие информационного общества. Согласно этому Закону гражданин США может запросить у любого федерального ведомства страны любые документы, кроме тех, что входят в исключения (национальная оборона, правоохранительные органы, финансовые и личные документы — всего 9 пунктов исключений), а государственное учреждение будет обязано удовлетворить этот запрос. В случае если учреждение не предоставляет запрашиваемую информацию, при этом она у него есть, местный суд имеет право в принудительном порядке эту информацию извлечь и передать гражданину. Интересы частных лиц в ограничении доступа к информации о них, находящейся в распоряжении федеральных агентств, сбалансированы Законом о неприкосновенности частной жизни (*Privacy Act*) 1974 г.

С развитием информационно-коммуникационных технологий положения Закона о свободе информации были дополнены (Закон о свободе электронной информации 1996 г., Закон о разрешении на информацию 2002 г.).

Последующие поправки установили обязанность федеральных агентств отчитываться о состоянии доступа к информации перед Министерством юстиции. В США информация о разрабатываемом правовом акте должна быть доступна публике, в частности публиковаться в Федеральном реестре. Это делается с целью привлечения к обсуждению заинтересованных лиц. Закон США о свободе информации в редакции 1996 г. устанавливает, что запрос, в котором содержится информация, имеющая общественный интерес, является приоритетным и на него должен быть дан ответ в кратчайший срок.

В **Европейском союзе** ст. 42 Хартии по правам человека гарантирует право на доступ к документации институтов ЕС: «Каждый гражданин Союза и каждое физическое или юридическое лицо, живущее или имеющее офис, зарегистрированный в государстве — члене Союза, имеет право на доступ к документации Европейского парламента, Совета Европы и Европейской комиссии. Государства — члены Совета Европы гарантируют право каждого на доступ по запросу к официальной документации, находящейся в компетенции публичной власти». Отличительной чертой европейских законов является регулирование запроса о получении информации. Совет Европы рекомендует, чтобы требования к запросам в государственные органы были минимальны, что уберет ненужные препятствия на пути к получению информации. Законы некоторых стран требуют конкретизации запрашиваемой информации или содержат требование, по которому гражданин имеет право только на получение информации, непосредственно затрагивающей его права и свободы, а организация — информации, непосредственно касающейся прав и обязанностей ее самой.

Современное законодательство признает разнообразные формы запроса. Многие законы допускают, что можно запрашивать информацию в любой разумной форме (электронной форме, печатной копии, аудио- или видеоформате, доступном с помощью обычных технических средств). Доминирует письменное обращение, но допускается и его электронная форма. Закон Бельгии о праве доступа к административным документам допускает письменное обращение в органы исполнительной власти и в суды. В зарубежных странах в практику входит назначение чиновников, которые помогают в написании запроса, что в конечном счете облегчает его понимание.

Также различаются формы ответов. Законодательство почти всех государств устанавливает требования к содержанию ответа. В Бельгии ответ должен включать информацию о процедуре обжалования и указание на чиновника, который его готовил. Закон также устанавливает право лица требовать разъяснений в связи с ответом. Все законы требуют, чтобы государственный орган информировал лицо, обратившееся с запросом, об отклонении запроса, направлял письменный отказ и в ясной форме объяснял основания отказа. Обратившееся лицо в зависимости от этого может принять решение о дальнейшем обжаловании.

С 2003 г. действует Директива Европейского парламента и Совета ЕС от 17.11.2003 № 2003/98/ЕС об использовании информации публичного сектора (*Public Sector Information (PSI) Directive*)[112]. Устанавливая предмет своего регулирования, она закрепляет, что публичные органы должны делать документы доступными в ориги-

[112] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32003L0098.

нальном (*pre-existing*) формате и на оригинальном языке, а также, когда это возможно, в открытом (*open format*)[113], машиночитаемом формате (*machine-readable format*)[114] вместе с метаданными. При этом формат и метаданные по возможности должны соответствовать формальным открытым стандартам (*formal open standards*[115]). В 2013 г. в Директиву были внесены дополнения, касающиеся доступа к информации музеев, библиотек и архивов. Директива об использовании информации публичного сектора задала новый стандарт доступа к данным — **открытые данные**[116]. Это понятие раскрывается через ряд признаков: данные должны существовать в цифровом формате; быть доступными в онлайновом режиме; быть в машиночитаемом формате; быть бесплатно доступны любому лицу. Такая информация в зарубежном праве не должна иметь правовых ограничений (быть *openly licensed*)[117].

---

[113] Под открытым форматом в Директиве понимается файловый формат, который основан на независимой платформе и является публично доступным без каких-либо ограничений, препятствующих использованию документа.

[114] Машиночитаемый формат определяется как файловый формат, структурированный таким образом, чтобы программа могла легко идентифицировать, распознать и извлечь конкретные данные, включая конкретные утверждения фактов и их внутреннюю структуру.

[115] Формальный открытый стандарт означает стандарт, который изложен в письменном виде, детализирует спецификации для требований по обеспечению интероперабельности программ.

[116] *Zuiderwijk A., Janssen M.* Barriers and Development Directions for the Publication and Usage of Open Data: A Socio-Technical View // Gascó-Hernández M., ed. Open Government, Public Administration and Information Technology. Vol. 4. N.Y., 2014. P. 115–135.

[117] *Kučera J., Chlapek D., Nečaský M.* Open Government Data Catalogs: Current Approaches and Quality Perspective. Technology-Enabled Innovation for Democracy, Government and Governance, Lecture Notes in Computer Science. Berlin — Heidelberg, 2013. P. 152–166; *Reiche K.J., Höfig E.* Implementation of Metadata Quality Metrics and Application on Public Government Data. COMPSAC Workshops. 2013. P. 236–241.

В настоящее время во многих странах вырабатываются модели правового регулирования открытых публичных данных. Законодательство о таких данных продолжает традиции, заложенные законодательством о свободе информации и общедоступных данных органов публичной власти, принятом во второй половине прошлого века. Законы об общедоступных и открытых данных различаются по содержанию. По сути, законы об открытых данных — новый этап законодательного обеспечения транспарентности (прозрачности). В отличие от законов предыдущего поколения, которые в основном определяли доступ к информации в ответ на запрос (ответное открытие доступа), большинство ныне действующих законов об открытых данных предполагают предупредительное раскрытие (открытие доступа без запроса).

Законы об открытых данных существенно отличаются от законов первого поколения. Они не содержат процедуры запросов, не устанавливают пошлин. Речь идет о расширении права на доступ к информации. Правовое регулирование исходит из особенностей оборота открытых данных различными субъектами в публичной и частноправовой сферах. На современном этапе формируется модель публичных (государственных) данных. Законы об открытых данных определяют правовую основу более широкого подхода к данным. Они действуют в совокупности с другими законами — о свободе информации, о доступе к информации, об архивах. На практике разрабатываются руководящие принципы, которые направлены на определение разграничения открытых данных (какие данные должны стать открытыми; как их преобразовывать в открытые; как реализовывать эти меры).

Законы об открытых данных позволяют не только модернизировать и расширять доступ к информации. Они

призваны сделать доступной публичную информацию, не содержащую тайны, причем в удобном формате, с размещением машиночитаемых наборов информации на государственных официальных сайтах.

Концепция открытых данных в последние годы активно развивается в странах Азии[118]. В одних странах (например, в Японии, Сингапуре, Малайзии и др.) правовой базой для оборота открытых данных являются законодательство о доступе к информации о деятельности государственных органов и государственные программы в сфере развития концепции открытых данных. В других странах, например в Южной Корее[119], принимаются специальные законы об открытых данных.

Закон **Южной Кореи** об открытых данных устанавливает обязанность всех государственных структур (*national institutions*), за исключением оправданных случаев, предоставлять открытые данные и обеспечивать их использование. Данные должны быть в удобном пользователям формате. Закон предусматривает координацию взаимодействия всех структур в сфере открытых данных, механизмы совершенствования системы открытых данных и стандартов предоставления информации, а также повышение квалификации государственных служащих в области культуры открытых данных (*open data culture*)[120].

В **Сингапуре** не принят отдельный закон об открытых данных, однако действуют государственные программы по стимулированию оборота открытых публичных

[118] См.: Open Data in Asia. URL: https://knowledgedialogues.files.wordpress.com/2014/07/open-data-asia-09-2014.pdf.

[119] См.: Open Data Law (South Korea). URL: http://www.law.go.kr/lsEfInfoP.do?lsiSeq=142444#.

[120] См.: Open Data: An Introductory, Practical Guide for Solutions. URL: http://www.uraia.org/documents/10/1580_arquivoB.pdf.

данных. В частности, в Сингапуре работает портал открытых данных *Data.gov.sg*. Также получила распространение лицензия на использование открытых данных[121]. Она дает право использовать данные на территории всего мира, без ограничения срока, безвозмездно и на неисключительных условиях. Данные могут использоваться различными способами как в коммерческих, так и в некоммерческих целях. Лицензиат имеет возможность передавать данные по сублицензии.

Предусмотрен ряд ограничений на использование открытых данных. В частности, лицензия не дает права свободно использовать размещенные в базах открытых данных персональные данные, товарные знаки, объекты патентных прав. Использование открытых данных не должно подразумевать поддержку деятельности лицензиата государственными органами. Лицензия также содержит дополнительные условия, касающиеся указания на источник данных (*attribution*); освобождения от ответственности за качество, точность и иные характеристики информации (*disclaimers*); возложения ответственности на лицензиата при поступлении претензий от третьих лиц (*indemnities*); информации о принадлежности интеллектуальных прав на базы данных (права принадлежат государственным структурам); права лицензиара прекратить действие лицензии при нарушении условий; вопросов применимого права.

Законы об открытых данных принимаются и в других странах. В **Дубае** действует Закон об открытых данных от 2015 г. № 26 (*Open Data Law*), регулирующий распространение и обмен открытыми данными в эмирате. Это одна из первых на всем Ближнем Востоке инициатив регулиро-

[121] См.: Singapore Open Data Licence. URL: https://data.gov.sg/open-data-licence#about.

вания открытых данных. Цель Закона — способствовать превращению Дубая в «умный город». Среди задач Закона — увеличивать прозрачность и эффективность правительственных служб; продвигать творческие и инновационные навыки; упрощать доступ к правительственным базам данных для личных, исследовательских и коммерческих целей; содействовать распространению данных и обмену ими с использованием электронных платформ, обзоров и других средств; вырабатывать критерии и правила обмена данными, в том числе в сфере технических протоколов.

Закон об открытых данных регулирует использование и распределение «данных Дубая», которые определяются как все данные, относящиеся к Дубаю и доступные провайдерам данных. «Данные» означают любой набор систематизированной или бессистемной информации, фактов, концепций, инструкций, наблюдений или мер в любой форме, которые собраны, произведены или обработаны провайдерами данных. Провайдеры данных — любое правительственное учреждение (включая власти, осуществляющие надзор над зонами специального развития и свободными зонами) или другое лицо, указанное компетентными органами. Сфера применения закона может быть очень широкой — она зависит от подхода компетентных органов к классификации лиц в качестве провайдеров данных.

Статья 10 Закона Дубая об открытых данных гласит, что провайдеры данных обязаны обновлять оборудование и сотрудничать в сфере обмена данных с «фундаментальной инфраструктурой», к которой относятся *IT*-системы, органы защиты данных и их безопасности, электронные платформы и другие системы, определяемые компетентными органами. Закон не касается распределения неиз-

бежных финансовых издержек между провайдерами данных и государственными органами.

Органы власти Дубая обязаны классифицировать свои данные в соответствии с официальным справочником о «данных Дубая» (который должен быть издан); готовить план-график обмена данными (который должен быть утвержден вышестоящими органами ОАЭ); выявлять опасности, могущие возникнуть при обмене данными.

«Данные Дубая» разделены на две категории: 1) открытые данные, публикуемые без ограничений или с минимальными ограничениями; 2) данные, которыми могут обмениваться провайдеры данных на условиях и по критериям компетентных органов. Оценить классификацию невозможно до обнародования соответствующих ограничений и критериев.

Статья 9 Закона Дубая об открытых данных запрещает провайдерам данных нарушать правила конфиденциальности и авторские права, что дает возможность коммерческим провайдерам данных сохранять контроль над своими базами. Эти положения нуждаются в дополнительном рассмотрении до начала применения Закона. Статья 13 гласит, что Закон не может противоречить законодательству о данных и что провайдеры данных при обмене ими обязаны уважать конфиденциальность и закрытость частной жизни пользователей.

Компетентным органом, проводящим в жизнь нормы Закона, является Комитет открытых данных Дубая, состоящий из служащих правительственных органов и функционирующий на временной основе. В дальнейшем для претворения норм Закона в жизнь планируется создать постоянный орган. Закон предусматривает, что неперсональные данные будут включены в оборот. В связи с этим критики Закона отмечают, что в нем следует

определить, какая информация является персональной и чувствительной.

В **России** доступ к информации о деятельности государственных органов осуществляется как путем направления запросов в соответствии с Федеральным законом от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», так и в форме открытых данных — на основе ст. 7 Закона об информации посредством обеспечения функционирования официальных сайтов государственных органов и органов местного самоуправления. Подзаконные акты, в том числе ведомственного характера, устанавливают к официальным сайтам технологические, программные и лингвистические требования в целях поддержания надлежащего уровня создания официальных сайтов, их развития и эксплуатации.

Промежуточные выводы

Презумпция общедоступности информации, вытекающая из базовых документов по правам человека, в большинстве юрисдикций не создает какого-то особого правового режима общедоступной информации.

Такой режим заявлен, но практически не раскрыт в законодательстве Российской Федерации.

Поскольку право на доступ к информации прежде всего ориентировано на государственную информацию, оно в значительной степени было развито в рамках законов о свободе информации и о доступе к информации о деятельности государственных органов. Такие законы действуют и успешно реализуются во многих странах мира, в том числе в России. На текущем этапе особую

значимость приобретает доступ к информации в форме открытых данных, т.е. в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования.

При обработке общедоступных данных, в особенности общедоступных персональных данных, принципиальное значение имеет вопрос о совместимости контекстов последующей обработки с контекстом, в котором данные были сделаны общедоступными. Также возможность доступа к информации, вытекающая из свободы слова, ограничивается неприкосновенностью частной жизни и иными правами, например закрепленным ст. 10.1 Закона о персональных данных безусловным правом субъекта запретить оператору передачу данных о себе. В некоторых случаях для пресечения возможных злоупотреблений со стороны владельцев платформы может быть использован инструментарий антимонопольного законодательства.

Обезличивание данных

Методы обезличивания

Как указывается в отчете Института исследований интернета, наиболее сложным вопросом, связанным с обезличиванием данных, является вопрос о том, каким образом можно убедиться в их успешном обезличивании[122]. Данные имеют ценность в силу того, что они связаны с тем или иным лицом, и обезличивание снижает их ценность, поскольку разрывает эту связь. Однако разрыв связи позволяет уменьшить риск вреда, который может быть причинен принципалу данных в случае распространения или иного использования относящихся к нему данных. Наконец, обезличивание позволяет разорвать и правовую связь лица и данных о нем: когда данные перестают быть связаны с лицом, это лицо больше не нуждается в установлении прав и гарантий в отношении таких данных. Поэтому применение обезличивания как технологии и как метода регулирования — это поиск баланса между достижением интересов всех перечисленных сторон. Государственные органы и иные организации в таких странах, как США, Великобритания, Южная Корея,

[122] См.: Анализ международного опыта регулирования сбора, обработки и результатов обработки массивов больших данных, в том числе обезличенных пользовательских данных, а также предложения по регулированию для Российской Федерации, с учетом странового, международного опыта и российского рынка. М., 2019. С. 4.

Япония, предприняли попытки определить этот баланс, дающий возможность для развития технологий больших данных без нарушения прав принципалов данных.

Различным аспектам обезличивания данных также посвящен ряд международных стандартов в сфере защиты конфиденциальности и персональной информации. В этом ряду особо выделяются три стандарта, выпущенные Международным институтом стандартизации (*International Organization for Standardization, ISO*) и Международной электротехнической комиссией (*International Electrotechnical Commission, IEC*): *ISO/IEC* 29100 и *ISO/IEC* 27018 устанавливают требования и выделяют методики по защите идентифицирующей информации (*PII*) в информационной и коммуникационной среде, в то время как *ISO/IEC* 20889 определяет стандарты обезличивания. Применительно к последнему документу важно отметить, что его целью является защита персональных данных физических лиц, однако термин «принципал данных», используемый в документе, относится также к организациям и устройствам (компьютерам).

Существует достаточно большое количество различных методов обезличивания данных[123]. Наиболее общим является их деление на статистические и криптографические.

Статистические методы обычно связаны с изменением структуры данных и применяются для обезличивания массивов данных либо для повышения эффективности обезличивания. Криптографические методы применяются для реализации мер безопасности, которые повы-

[123] Описание методов обезличивания приводится по: Анализ международного опыта регулирования сбора, обработки и результатов обработки массивов больших данных...

шают эффективность методов обезличивания, а также являются частью самих этих методов.

В настоящем разделе перечислены методы обезличивания, которые рекомендуются к применению органами по защите персональных данных в различных странах. Как правило, в документах по обезличиванию рассматриваются не все эти методы. Например, в Позиции рабочей группы статьи 29 (*Article* 29 *Working Party, Art.* 29 *WP*) по методам обезличивания 05/2014 (*Opinion of the Working Party on Anonymization Techniques*; далее также — Позиция 05/2014)[124] рассматриваются добавление шума, замена, *k*-анонимность, *l*-разнообразие и дифференцированная приватность. В Руководстве по обезличиванию персональных данных Южной Кореи основополагающим методом является *k*-анонимность, включающая в себя методы агрегации, подавления и маскирования. Криптографические методы описаны только в стандарте *ISO/IEC* 20889:2018 «Терминология, касающаяся способов повышения конфиденциальности и классификация методов обезличивания». Абсолютно все регуляторы рассматриваемых стран в сфере персональных данных едины во мнении, что применение какого-то одного метода обезличивания не гарантирует надежность соответствующего уровня обезличивания данных. Для достижения этой цели необходимо применять набор методов, выбор которых происходит отдельно для каждого случая и обусловливается различными факторами, такими как типы данных, содержащихся в исходном массиве, наличие других общедоступных данных, способ применения обезличенных данных, воз-

[124] См.: Opinion of the Working Party on Anonymization Techniques, Article 29 Working Party. URL: http://www.dataprotection.ro/servlet/ViewDocument?id=1085.

можные последствия повторной идентификации для субъекта и т.д.

Рассмотрим базовые **статистические методы обезличивания** данных.

1. Подавление (*suppression*): полное удаление значений атрибутов или их частичная замена на бессмысленное значение (как правило, используется знак *). Этот метод обычно применяется к персональным идентификаторам. К методам подавления относятся маскирование (*masking*), локальное подавление (*local suppression*), подавление записей (*record suppression*).

Маскирование состоит в удалении из массива всех прямых идентификаторов. Также метод потенциально удаляет некоторые или все дополнительные оставшиеся идентифицирующие атрибуты для всех записей в массиве.

Локальное подавление заключается в удалении отдельных значений атрибутов из выбранных записей, которые в комбинации с другими идентифицирующими атрибутами могут привести к идентификации субъекта. Обычно метод применяется для удаления редко встречающихся в массиве значений (или редких комбинаций значений) косвенных идентификаторов, которые остались в массиве после применения метода обобщения. Чаще всего локальное подавление применяется к категорийным значениям, в то время как обобщение применяется к числовым значениям.

Подавление записей включает в себя удаление записи или записей целиком. Обычно применяется к записям, которые содержат редкие комбинации атрибутов.

2. Обобщение (*generalization*): замена значений атрибутов более абстрактными значениями. Метод обычно применяется к квазиидентификаторам. К методам обобщения относятся округление (*rounding*), нисходящее и

восходящее кодирование (*top and bottom coding*), комбинирование набора атрибутов в один атрибут (*combining a set of attributes into a single attribute*), локальное обобщение (*local generalization*).

Округление включает в себя выбор базы для округления выбранного атрибута и последующего округления его значения в бóльшую или меньшую сторону до ближайшего кратного основания округления. Выбор округления в бóльшую или меньшую сторону определяется вероятностно на основе того, насколько близко значение находится к ближайшему кратному базы округления. Например, если основание округления равно 10, а значение равно 7, то 7 округляется до 10 с вероятностью 0,7 и округляется до 0 с вероятностью 0,3. Также возможно контролируемое округление, гарантирующее, что сумма округленных значений совпадает с округленным значением суммы исходных данных.

Нисходящее и восходящее кодирование. В ходе применения метода устанавливается порог для наибольшего (или наименьшего) значения, которое может принимать данный атрибут. Значения, которые выше (или ниже) порогового значения, заменяются одним значением, указывающим верхнюю (или нижнюю) категорию. Этот метод применим либо к непрерывным, либо к категорийным атрибутам и к порядковым числам. Например, конкретный размер дохода человека может быть заменен на «более 1000 долларов США».

Комбинирование набора атрибутов в один атрибут. Степень детализации информации, содержащейся в наборе выбранных (связанных) атрибутов, можно уменьшить, заменив их одним атрибутом, значение которого вычисляется путем применения определенной функции к значениям выбранных атрибутов в той же записи.

Локальное обобщение включает в себя обобщение конкретных значений атрибутов из выбранных записей. Этот метод используется, если значения таких атрибутов в сочетании с другими идентифицирующими атрибутами могут привести к идентификации субъекта данных. Обычно локальное обобщение применяется для удаления редких значений (или редких комбинаций значений) косвенных идентификаторов без изменения оставшихся значений этого атрибута во всех записях. Локальное обобщение обычно применяется к числовым значениям с целью увеличения количества записей с одинаковыми значениями идентифицирующих атрибутов.

3. Искажение (*randomization/perturbation*): замена значений атрибутов таким образом, что связь с изначальными данными устраняется при сохранении статистических свойств. Наиболее типичным методом с применением искажения является метод добавления шума (*noise addition*). К другим методам относятся метод замены/перестановки (*substitution/permutation*) и метод агрегации или микроагрегации (*aggregation/microaggregation*).

Метод добавления шума состоит в снижении точности персональных идентификаторов посредством внесения случайных статистически незначимых изменений в массив данных. Например, массив данных, содержащий данные о возрасте субъектов, может быть обезличен путем случайного добавления или вычитания числа от 1 до 10 из значений атрибута «возраст», а затем удаления значений имен. Это позволит указать в массиве средний возраст субъектов (в пределах погрешности), но не даст злоумышленнику узнать их реальные даты рождения.

Метод замены/перестановки состоит в перестановке персональных идентификаторов внутри таблицы или замене их на произвольные значения, взятые из того

же массива. Метод используется, если важно сохранить точное распределение каждого атрибута внутри массива данных. Перестановка может быть рассмотрена как частный случай добавления шума, при котором снижение точности значений атрибутов внутри массива данных происходит благодаря перемещению их с одной записи на другую. Такой обмен, с одной стороны, сохраняет диапазон и распределение значений, а с другой стороны, удаляет корреляцию между записями и субъектами данных.

Агрегация или микроагрегация заключается в обобщении персональных идентификаторов в группы или диапазоны и подстановке получившихся обобщенных значений на место персональных идентификаторов. Например, даты рождения конкретных субъектов могут быть обобщены по диапазону дат или сгруппированы по месяцу и году рождения. Числовые атрибуты могут быть обобщены по интервальным значениям, например по месяцу рождения, а значения имен субъектов удаляются.

4. Перестановка (*permutation*): разделение данных на группы и перестановка чувствительных значений внутри каждой группы. Таким образом устраняется связь между квазиидентификаторами и чувствительными данными.

Наиболее часто используемыми статистическими методами обезличивания на сегодняшний день являются метод *k*-анонимности, метод *l*-разнообразия, метод *t*-близости и метод дифференцированной приватности. Международный стандарт *ISO/IEC* 20889:2018 «Терминология, касающаяся способов повышения конфиденциальности и классификация методов обезличивания» (*Privacy enhancing de-identification terminology and classification of techniques*) относит эти методы к моделям, гарантирующим приватность (*formal privacy measurement*

models), т.е. формальным мерам по измерению уровня конфиденциальности, каждая из которых основана на различных методах обезличивания и имеет собственный подход к математическому вычислению уровня риска повторной идентификации (раздел 10 *ISO/IEC* 20889:2018).

Метод k-анонимности (*k-anonymity*). Процесс *k*-анонимизации начинается с удаления из массива данных всех явных персональных идентификаторов (имен и т.д.). Хотя после этого массив больше не содержит явных идентификаторов, в нем остаются квазиидентификаторы. Основная задача *k*-анонимности состоит в преобразовании массива таким образом, чтобы было невозможно установить связи между любыми записями в массиве и соответствующими субъектами. Конфиденциальность субъекта данных гарантируется за счет включения его в общую группу с как минимум *k* другими субъектами. При этом достигается состояние, при котором любая запись в полученном массиве данных неотличима по крайней мере от (k – 1) других записей в отношении определенного квазиидентификатора субъекта. Для этого персональные идентификаторы обобщаются так, чтобы они в равной степени соответствовали всем субъектам. Группа записей, которые неотличимы друг от друга, часто называется классом эквивалентности. Для обеспечения *k*-анонимности необходимо, чтобы каждый персональный идентификатор имел по крайней мере *k* вхождений в массив данных. Массив данных обладает *k*-анонимностью, если для каждого субъекта, данные которого попали в массив, имеется по меньшей мере k – 1 субъект, обладающий такими же значениями атрибутов.

Метод l-разнообразия (*l-diversity*). Метод является расширением метода *k*-анонимности. При его примене-

нии персональные идентификаторы сначала обобщаются в группы по принципу, аналогичному используемому в *k*-анонимности, а затем достигается состояние, при котором каждое из обобщенных значений атрибутов встречается в кластере как минимум *l* раз. При достижении этого состояния можно говорить о том, что чувствительные атрибуты «достаточным образом представлены» (*well-represented*). Тем самым предотвращается ситуация, при которой значения чувствительных атрибутов встречаются в кластере настолько редко, что это может привести к идентификации конкретных субъектов.

Метод t-близости (t-closeness). Это усовершенствованный вариант метода *l*-разнообразия, который направлен на сохранение изначального распределения атрибутов. Он эффективен, если для целей обработки необходимо, чтобы данные в массиве обезличенных данных были максимально приближены к данным в оригинальном массиве. Для этого к требованию, чтобы в каждом классе эквивалентности присутствовало по крайней мере *l* различных значений, добавляется требование, чтобы каждое значение было представлено столько раз, сколько это необходимо для того, чтобы отобразить исходное распределение каждого атрибута.

Метод дифференцированной приватности основан на введении в данные случайной информации (добавления шума), однако в отличие от других методов, использующих сходную технику, он применяется для создания обезличенного представления массива данных с одновременным сохранением массива исходных данных. Подобные обезличенные представления обычно генерируются посредством подмножества запросов для конкретного третьего лица. Подмножество включает в себя случайную информацию, которая добавляется в момент

выдачи ответа на запрос. Таким образом, метод позволяет обеспечить равную защиту конфиденциальности для каждого субъекта без необходимости удаления исходного массива данных. Описание метода дифференцированной приватности более простым языком может выглядеть следующим образом: допустим, существуют два идентичных массива данных, которые различаются только тем, что один из них содержит информацию, относящуюся к конкретному субъекту, а другой нет. Дифференциальная приватность гарантирует, что одинаковый статистический запрос и к одной, и к другой базе выдаст один и тот же результат с практически одинаковой вероятностью.

Далее рассмотрим **активные методы обезличивания данных с использованием криптографических средств защиты информации**.

Детерминированное шифрование (*deterministic encryption*) может использоваться для замены любых идентифицирующих или чувствительных атрибутов зашифрованным значением. Характерной чертой детерминированного шифрования является то, что два одинаковых значения, зашифрованных одним и тем же ключом шифрования, производят два одинаковых шифротекста. Это позволяет сохранять полезные свойства обезличенных данных. Результатом детерминированного шифрования являются микроданные, которые можно использовать для поиска соответствий и аналитики.

Сохраняющее порядок шифрование (*order-preserving encryption*), применяемое в ходе обезличивания, используется для замены любого идентификатора или чувствительного атрибута записью с зашифрованным значением. Свойством этого шифрования является сохранение порядка значений в шифротексте в случае примене-

ния к значениям одного и того же ключа шифрования. То есть если два значения расположены в определенном порядке, в таком же порядке будут расположены зашифрованные значения. Сохраняющее порядок шифрование предоставляет более высокий уровень полезности обезличенных данных, чем детерминированное шифрование, и не снижает качество данных.

Сохраняющее формат шифрование может быть применено не только к двоичным данным. В частности, для любого конечного набора символов, такого как десятичные цифры, сохраняющее формат шифрование преобразует данные, отформатированные в виде последовательности символов, таким образом, что зашифрованные данные имеют тот же формат, что и исходные данные, включая длину последовательности символов. Например, зашифрованный с помощью этого метода 9-значный номер социального страхования будет иметь вид последовательности девяти десятичных чисел. Сохраняющее формат шифрование применяется при обезличивании и псевдонимизации, а также как модифицированная техника шифрования в унаследованных приложениях, где традиционный режим шифрования невозможен.

Гомоморфное шифрование, или гомоморфный обмен ключами (*homomorphic secret sharing*), позволяет разделить ключ на части — определенные подмножества, которые можно использовать для восстановления ключа таким образом, что если одна и та же математическая операция выполняется для всех частей, используемых для восстановления ключа, то результат применения совпадает с результатом выполнения этой математической операции с оригинальным ключом. Как составная часть процесса обезличивания гомоморфное шифрование может быть применено для замены любого идентифициру-

ющего или чувствительного атрибута записью данных с одной или более частями, полученными в ходе применения алгоритма обмена сообщениями. В дальнейшем части могут быть распределены между несколькими лицами, число которых определяется реализацией схемы обмена ключами.

Подходы к обезличиванию и к использованию его результатов

Регуляторные подходы к обезличиванию и к использованию данных, полученных в результате обезличивания, отличаются в разных странах.

В **Европейском союзе** наиболее подробное руководство по различным методам обезличивания, а также преимуществам, недостаткам и степени безопасности с точки зрения возможности восстановления исходных данных каждого из них представлено в Позиции рабочей группы статьи 29 по методам обезличивания 05/2014.

Поскольку обезличивание также представляет собой обработку персональных данных, возникает вопрос о необходимости получения отдельного согласия субъекта персональных данных на осуществление такой обработки. Однако, по мнению рабочей группы ст. 29, поскольку цели обезличивания сопоставимы с изначальными целями обработки, получения отдельного согласия субъекта для обезличивания не требуется, при условии что обезличивание проводится так, как это описано в Позиции 05/2014. Обезличивание в том виде, в каком оно понимается рабочей группой, является предельным случаем де-идентификации. Более слабые варианты де-идентификации, такие как псевдонимизация, также признаются

в *GDPR* как меры по защите конфиденциальности, которые снижают риск для субъекта данных. В случае если при обработке данных с целью их де-идентификации могут потребоваться дополнительные правовые основания для обработки, контролер может сослаться на такие основания, как законный интерес.

В то время как обезличенные (анонимизированные) данные выводятся за рамки законодательства в сфере защиты персональных данных, псевдонимизированные данные являются персональными данными и не должны использоваться для обхода требований законодательства. При этом псевдонимизация признается хорошей практикой, обеспечивающей защиту интересов граждан. В Позиции 05/2014 подчеркивается, что для того чтобы данные соответствовали стандартам обезличивания и были признаны анонимизированными, они должны быть лишены всех элементов, на основании которых возможна повторная идентификация субъекта персональных данных. При этом процесс обезличивания должен быть необратимым.

Хорошими практиками обезличивания с точки зрения рабочей группы являются:

— постоянная переоценка рисков повторной идентификации, выявление новых рисков, оценка и соответствующая корректировка способов управления рисками;

— учет возможностей использования для повторной идентификации необезличенной части массива данных, особенно если возможна его комбинация с обезличенной частью, а также вероятна корреляция между различными атрибутами;

— оценка существующего контекста (например, происхождение данных, доступность публичных данных, наличие и качество контрольных механизмов и т.д.);

— раскрытие информации о методах, примененных для обезличивания;

— учет ограничений и возможных ошибок при применении различных методов обезличивания.

В правовых актах **США** в значении обезличивания используется термин «де-идентификация» (*de-identification*). При этом определение де-идентификации приводится лишь в некоторых законодательных актах США, хотя, как правило, акты по защите персональной информации содержат положения, свидетельствующие об их неприменимости к де-идентифицированным данным. Например, Закон о мобильности и подотчетности медицинского страхования (*Health Insurance Portability and Accountability Act, HIPAA*) не применяется к де-идентифицированным данным, если нет разумных оснований полагать, что информация может быть использована для идентификации физического лица.

Наиболее полные определения де-идентификации содержатся в *HIPAA* и в сопутствующем Правиле защиты конфиденциальности идентифицирующей информации о здоровье (*Standards for Privacy of Individually Identifiable Health Information, Privacy Rule*), а также в Калифорнийском законе о защите прав потребителей (*California Consumer Privacy Act, CCPA*). Определения обезличивания также можно найти в Руководстве Федеральной комиссии по связи (*Federal Communications Commission, FCC*) «Защита конфиденциальности потребителей широкополосных и других телекоммуникационных сервисов» (*Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*), а также в стандартах Национального института стандартов и технологий США (*National Institute of Standards and Technology, NIST*).

Согласно *CCPA* информация является де-идентифицированной, если она не может идентифицировать, быть отнесенной, описывать, быть ассоциированной или связанной, прямо или косвенно, с конкретным потребителем при условии, что бизнес, который использует обезличенную информацию:

— принял технические меры, предотвращающие повторную идентификацию пользователя, к которому данная информация может относиться;

— внедрил бизнес-процессы, которые явно запрещают повторную идентификацию информации;

— внедрил бизнес-процессы для предотвращения непреднамеренного раскрытия де-идентифицированной информации;

— не предпринимает попыток повторной идентификации информации.

В определениях де-идентификации в праве США, в отличие от европейского *GDPR*, нет четкого требования необратимости к процессу обезличивания. Вместо этого вводится требование к владельцам данных (или контролерам данных в терминологии *GDPR*) не предпринимать попыток к повторной идентификации данных и накладывать подобные ограничения в рамках контракта на тех лиц, которым раскрываются данные или предоставляется доступ к ним.

Дискуссия относительно обезличивания данных в **Южной Корее** началась вскоре после вступления в силу в 2011 г. упоминавшегося ранее Закона о защите персональной информации Южной Кореи (*Personal Information Protection Act, PIPA*). Несмотря на то, что в целом *PIPA* соответствует целям защиты конфиденциальности, высказывались опасения, что в некоторых аспектах Закон предъявляет чрезмерно строгие требования, не обе-

спечивая при этом должного уровня защиты данных. В ответ на эти опасения был проведен ряд публичных обсуждений, результатом которых стал выпуск руководств и разъяснений, которые, в частности, рассматривают вопрос обезличивания данных.

Руководство по обезличиванию персональных данных (*Guidelines for De-identification of Personal Data*)[125] представляет собой совместный документ ряда государственных органов, которые в различных аспектах отвечают за вопросы конфиденциальности данных: Управления по координации государственной политики, Министерства внутренних дел и безопасности, Министерства образования, науки и техники и Министерства здравоохранения и социального обеспечения. Руководство устанавливает стандарты обезличивания и дает рекомендации по управлению процессом. Основной целью Руководства является снятие жестких ограничений на обработку данных, которые замедляют рост рынка больших данных.

Согласно преамбуле Руководства данные, которые были обезличены адекватным способом в соответствии с руководящими принципами, установленными в документе, не являются персональными данными и могут использоваться в целях аналитики больших данных или в других целях без согласия субъекта персональных данных. Однако при этом необходимо учитывать, что повторная идентификация обезличенных данных может быть осуществлена, учитывая технологическое развитие и увеличение объемов доступных данных, поэтому бизнес должен принимать необходимые меры (как техно-

[125] См.: Guidelines for De-identification of Personal Data. URL: https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830764&fileSn=0.

логические, так и управленческие) для предотвращения повторной идентификации.

В процедуре обезличивания выделяют четыре последовательных шага:

1) предварительная оценка — выделение персональных данных из массива имеющихся данных;

2) обезличивание — удаление или замена некоторых или всех элементов персональных данных из массива данных, которые могут идентифицировать субъекта;

3) оценка адекватности принятых мер по обезличиванию посредством комбинирования обезличенных данных с другими доступными данными, которая должна проводиться группой выделенных экспертов по обезличиванию. Важным критерием в процессе оценки является понятие *k*-анонимности;

4) последующий контроль — мониторинг и предотвращение повторной идентификации данных. Если данные были обезличены адекватным образом, то они могут использоваться для аналитики и других целей. В то же время владелец данных обязан взять на себя обязанность предотвращать утечки данных и их незаконное использование.

Руководство требует от компаний постоянного мониторинга возникновения риска повторной идентификации, что может быть связано с изменением внешних (появление новых технологий и доступа к новым видам данных) и внутренних обстоятельств (сбор дополнительных данных, внедрение новых систем, которые влияют на системы безопасности).

Также, в случае предоставления обезличенных данных третьим лицам, элементы управления рисков повторной идентификации должны быть внедрены в контрактные обязательства (запрет на попытки повторной иденти-

фикации, ограничение на дальнейшее предоставление и передачу полномочий, обязанность уведомления о возникновении риска повторной идентификации).

Если повторная идентификация произошла, то необходимо:

— прекратить обработку повторно идентифицированных данных;

— принять меры по защите таких данных от возможных утечек;

— незамедлительно уничтожить повторно идентифицированные данные либо (в случае необходимости их дальнейшего использования) повторно их обезличить.

Со стороны государственных органов необходимо создание системы поддержки для обеспечения безопасного использования обезличенных данных. В частности, нужна поддержка организаций среднего и малого бизнеса и стартапов для стимулирования использования ими технологий больших данных посредством проведения необходимых консультаций и профессиональных тренингов по обезличиванию.

В каждой отрасли экономики (Интернет, безопасность, финансы и кредитование, социальная поддержка) должно быть основано специализированное агентство, которое подчиняется соответствующему министерству и выполняет такие функции, как организация пула экспертов в сфере обезличивания, составление рекомендаций по применению методов обезличивания в соответствующей отрасли, оценка адекватности применяемых мер по обезличиванию, а также контроль за созданием комбинированных массивов данных, т.е. объединенных массивов, представленных различными организациями — контролерами данных.

В **Сингапуре** обязанности, возлагаемые на операторов персональных данных, не распространяются на обезличенные данные. Это отражено в Разъяснениях Комиссии по защите персональных данных Сингапура относительно защиты персональных данных в определенных случаях (*Advisory Guidelines on the Personal Data Protection Act for Selected Topics*)[126]. В них указывается, что обезличенные данные не являются персональными данными и к их сбору, обработке и раскрытию не применяются требования соответствующих частей Закона Сингапура о персональных данных.

Обезличивание в Разъяснениях определяется как процесс преобразования персональных данных в данные, которые не могут быть использованы для идентификации какого-либо лица как обратимым, так и необратимым способом. Обратимость обезличивания является важным фактором, который необходимо учитывать при оценке рисков повторной идентификации.

Данные не могут быть признаны обезличенными, если присутствует существенная возможность повторной идентификации субъекта, принимая во внимание (1) сами данные или данные в сочетании с другой информацией, к которой у организации есть или может быть доступ; (2) меры и гарантии (или отсутствие таковых), внедренные организацией для смягчения риска идентификации

Таким образом, существенным риском для повторной идентификации признается наличие или доступ к информации, позволяющей повторную идентификацию

[126] Advisory Guidelines on the Personal Data Protection Act for Selected Topics. URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-9-Oct-2019.pdf.

субъекта, у организации, проводящей обезличивание данных. Наличие такой информации у других операторов не принимается во внимание, в отличие от законодательства ЕС, в котором при анализе вероятности повторной идентификации учитываются возможности не столько конкретной организации (контролера данных), сколько любой абстрактной организации с учетом имеющихся возможностей и уровня развития технологий. Достаточно мягкие требования, предъявляемые к обезличиванию, необходимы для того, чтобы создать благоприятные условия для обработки данных в аналитических целях и сделать возможности их использования более широкими, чем в рамках требований режима по защите персональных данных.

Каждая организация должна выбирать методы обезличивания, наиболее подходящие в каждом конкретном случае[127]. При выборе методов обезличивания и необходимого уровня обезличивания организациям в Сингапуре рекомендуется принимать во внимание:

— цель обезличивания и необходимые полезные качества данных. Процесс обезличивания независимо от используемого метода снижает качество исходных данных. Поэтому организация должна определить приемлемый для нее уровень качества данных и постараться при этом снизить риск повторной идентификации. Рекомендуется оценивать качество не всего обезличенного массива, а только тех атрибутов, которые представляют наибольший интерес. Допускается, что к нему вообще могут быть не применены методы обезличивания, если его качество является критичным;

[127] См.: Guide to Basic Anonymization Techniques. URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.

— характеристики методов обезличивания. В зависимости от характеристик некоторые методы могут быть более подходящими в конкретной ситуации. Например, метод маскирования обычно применяется к прямым идентификаторам, а агрегация — к косвенным. Также важно учитывать, какое значение — непрерывное или дискретное — имеет атрибут, так как, например, техника искажения больше подходит для непрерывных значений;

— выводимая информация. Некоторая информация может быть получена из обезличенных данных путем вывода. Например, маскирование может скрыть персональные данные, но оно не скрывает их длину (количество знаков). В процессе обезличивания необходимо учитывать любую возможность вывода как перед, так и после применения соответствующих методов;

— обладание необходимыми знаниями. Методы обезличивания в основном уменьшают идентифицируемость одного или нескольких субъектов исходного массива данных до уровня риска, приемлемого для организации. Оценка идентифицируемости должна выполняться до и после применения методов обезличивания, что требует хорошего понимания предмета, к которому относятся данные. Оценка до процесса обезличивания гарантирует, что структура и информация, которую содержит атрибут, четко определены и понятны, а риск прямого и непрямого вывода из данных оценен (например, из атрибута «год рождения» можно косвенным образом вывести возраст). Оценка после процесса обезличивания позволяет установить остаточный риск повторной идентификации. Таким образом, правильный выбор методов обезличивания зависит от осведомленности о явной и неявной информации, содержащейся

в массиве данных, а также о количестве или типе информации, которую требуется обезличить;

— компетенции в методах и процессе обезличивания. Обезличивание является сложным процессом, поэтому оно должно осуществляться людьми, хорошо разбирающимися в его методах и принципах. Если в организации отсутствует сотрудник с необходимым уровнем компетенции, рекомендуется привлекать внешних экспертов;

— получатель данных. Такие факторы, как обладание получателей данных необходимыми знаниями, внедренные им меры контроля для ограничения доступа и предотвращения передачи данных несанкционированным лицам, играют важную роль в выборе методов обезличивания. В частности, то, как получатель планирует использовать данные, может наложить ограничения на применяемые методы обезличивания, так как полезные качества данных могут быть утеряны. При публичном выпуске данных следует соблюдать максимальные меры предосторожности и применять более сильные методы обезличивания по сравнению с передачей данных установленному получателю на основании контракта;

— инструменты. Из-за сложности методов и необходимости вычислений для обезличивания могут быть использованы готовые программные инструменты, однако при этом необходимо учитывать, что любой инструмент требует точности в постановке задачи, а также имеет свои ограничения, поэтому дополнительный контроль со стороны человека необходим в любом случае.

Понятие обезличенных данных в **России** не определено, однако в ст. 3 Закона о персональных данных вводится определение процесса обезличивания: «Обезличивание персональных данных — действия, в результате

которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных». Обезличивание является одним из видов обработки персональных данных. Поскольку в определении обезличивания заложена возможность повторной идентификации, можно заключить, что фактически обезличивание в этом случае совпадает с понятием псевдонимизации в терминах *GDPR*, т.е. является обратимым.

Обезличивание как альтернатива уничтожению применяется к персональным данным «по достижении целей обработки или в случае утраты необходимости в достижении этих целей» (п. 7 ст. 5 Закона о персональных данных). Обезличивание также является необходимым условием для обработки персональных данных в статистических или иных исследовательских целях (п. 9 ст. 6 Закона о персональных данных).

Требования и методы по обезличиванию персональных данных, установленные для государственных или муниципальных органов, осуществляющих обработку персональных данных (операторов персональных данных), приведены в приказе Роскомнадзора от 05.09.2013 № 996. Подробное описание требований и методов обезличивания содержится в Методических рекомендациях по применению этого приказа, утв. Роскомнадзором 13.12.2013. Документов, четко регламентирующих обезличивание данных и их последующую обработку коммерческими организациями, в российском законодательстве не существует.

Первая попытка регулирования сбора и обработки обезличенных данных в России была предпринята в октябре 2018 г., когда на рассмотрение был внесен законо-

проект о внесении изменений в Закон об информации (проект федерального закона № 571124-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»). Проектом вводились понятия «большие пользовательские данные» (БПД), которые определялись как совокупность не содержащей персональных данных обезличенной информации о физических лицах и их поведении, «собираемой из различных источников, в том числе сети Интернет, количество которых превышает тысячу сетевых адресов», а также «оператор БПД» и «обработка БПД». Оператор обязывался информировать пользователя о начале обработки связанных с ним БПД, получать согласие на обработку БПД третьими лицами, при работе с базой данных из более чем 100 тыс. сетевых адресов уведомлять Роскомнадзор об обработке БПД до начала такой обработки. Документом также предусматривалось создание реестра операторов БПД, который должен был вести Роскомнадзор.

Законопроект подвергся критике, в частности из-за смешения понятий «БПД» и «данные, прошедшие процедуру обезличивания», что приводило к конфликту с действующим законодательством. В результате нельзя будет разграничить упомянутые понятия, а это сделает невозможной обработку данных в статистических и иных целях без согласия их владельцев. В то же время сейчас обезличивание персональных данных рассматривается как условие введения данных в свободное обращение, гарантирующее соблюдение прав физических лиц благодаря разрыву связи между данными и конкретным субъектом. В ноябре 2018 г. законопроект был возвращен на доработку и в дальнейшем не вносился на повторное рассмотрение.

В конце 2019 г. Центром компетенций по нормативному регулированию цифровой среды (Фонд «Сколково») подготовлен законопроект о внесении изменений в Федеральный закон «О персональных данных». Законопроект был разработан во исполнение п. 01.01.003.002.001 Плана мероприятий по направлению «Нормативное регулирование» национальной программы «Цифровая экономика». Законопроектом предлагалось дополнить Закон о персональных данных понятиями «обезличенные персональные данные» и «обезличенные данные», а также установить порядок и условия их обработки. Обезличенные персональные данные в законопроекте определяются как информация, которая «в результате обезличивания персональных данных не позволяет без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных». Под обезличенными данными понимается «информация, которая в результате обезличивания не позволяет даже при использовании дополнительной информации определить ее принадлежность конкретному субъекту персональных данных». Таким образом, законопроект определял обезличенные данные как необратимо обезличенные данные, в то время как обезличенные персональные данные могут быть подвергнуты повторной идентификации. Похожее разграничение присутствует в *GDPR* в отношении понятий «обезличенные данные» и «псевдонимизированные данные». Определение требований к обезличиванию и описание методов обезличивания в законопроекте отнесены к компетенции Правительства РФ. Для обработки персональных данных в целях обезличивания, в том числе для последующей передачи обезличенных данных тре-

тьим лицам, вводится отдельное согласие субъекта персональных данных, но при этом предполагается отход от принципа «одна цель — одно согласие», т.е. согласие на обработку может быть дано одновременно на несколько целей.

На текущий момент этот законопроект не получил поддержки регуляторов и уполномоченных федеральных органов исполнительной власти. Вместе с тем существует понимание, в том числе со стороны бизнеса и экспертов, что в целях внедрения в Российской Федерации регламентированного оборота обезличенных персональных данных необходимо:

— решить юридическую проблему отнесения обезличенных данных к персональным данным;

— исходить из того, что государство каждый раз при возникновении определенных правоотношений независимо от псевдонимизации, обратимости персональных данных будет видеть риски для информационной безопасности, защиты прав и законных интересов субъектов персональных данных, связанные с повторной идентификацией, и каждый раз будет относить эти риски к персональным данным, прошедшим процедуру обезличивания;

— установить принцип вариативности методов обезличивания персональных данных;

— рассмотреть возможность (в связи с принципом вариативности методов обезличивания персональных данных) установления принципа вариативности методик обезличивания персональных данных, в том числе с учетом отраслевых сфер работы с данными (связь, здравоохранение, труд, образование, социальная защита).

Промежуточные выводы

Подход к регулированию больших данных, связанный с их обезличиванием и последующим использованием, является воплощением *lex informatica*, т.е. регулирования, сочетающего в себе технологические и правовые приемы. Главным достоинством этого подхода является его самобалансировка, основанная на управлении правовыми и информационными связями между лицом и данными о нем. Если существует информационная и технологическая связь, т.е. из совокупности данных можно установить лицо, к которому она относится, то возникает и правовая связь: лицо является принципалом данных и может заявить права на них, что повлечет ограничение прав для фактического обладателя совокупности данных.

При этом, как показывает опыт зарубежных стран, для эффективного применения методов обезличивания и последующего использования обезличенных данных должна быть выстроена правовая и организационно-техническая инфраструктура, включающая в себя как методические документы и руководства по обезличиванию, описывающие требования на основе лучших практик по обезличиванию данных, так и соответствующую систему органов и организаций, обеспечивающих методическую поддержку и контроль, в том числе контроль по обеспечению информационной безопасности, операторов, осуществляющих обезличивание и оборот данных.

Особого внимания требует переход данных из правового режима персональных данных (или иных, имеющих принципала данных: тайны, промышленных, общедоступных данных) в режим обезличенных данных.

Этот переход не должен сопровождаться избыточными требованиями, например необходимостью получения отдельного согласия субъекта данных на создание обезличенных данных, но при этом качество обезличивания должно контролироваться. Процесс обезличивания должен быть регламентирован.

Большинство из существующих в зарубежной практике стандартов и требований к обезличиванию данных основывается на методологии оценки рисков, суть которой состоит в выборе степени обезличивания данных в зависимости от степени риска повторной идентификации, которая, в свою очередь, зависит от контекста и, соответственно, может меняться. Обезличивание с использованием криптографических методов при этом рассматривается как способ повышения уровня конфиденциальности и снижения риска повторной идентификации, т.е. риска причинения вреда принципалу данных.

Выводы и рекомендации

Международные исследования по вопросам больших данных ставят под сомнение те выгоды, которые несут в себе эти технологии. В отчете Центра безопасности прорывных технологий (*CSET*) при Университете Джорджтауна[128] отмечается, что ценность имеют лишь очищенные, преобразованные, маркированные данные, оптимизированные для обучения нейросетей конкретными алгоритмами машинного обучения. При этом очистка и структурирование данных становятся все дороже как в денежном[129], так и в экологическом[130] измерении. В связи с этим аналогией с точки зрения задач и целей регулирования является промышленное производство. Интерес производителя заключается в том, чтобы минимизировать издержки, что достигается прежде всего за счет удешевления сырья, а также за счет сокращения всех расходов, не связанных напрямую с производством. Для производителя интересы источников сырья, а также вред для окружающей среды, вызванный производством,

---

[128] См.: Messier Than Oil: Assessing Data Advantage in Military AI. URL: https://cset.georgetown.edu/research/messier-than-oil-assessing-data-advantage-in-military-ai/.

[129] См.: The Cost of Training Machines Is Becoming a Problem. URL: https://www.economist.com/technology-quarterly/2020/06/11/the-cost-of-training-machines-is-becoming-a-problem.

[130] См.: Training a Single AI Model Can Emit As Much Carbon As Five Cars in Their Lifetimes. URL: https://www.technologyreview.com/2019/06/06/239031/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/.

являются экстерналиями[131]. Аналогично экстерналиями для лиц, занимающихся обработкой больших данных, являются интересы источников данных (индивидов, собственников устройств Интернета вещей и т.п.) и экологические последствия от работы средств вычислительной техники. Интернализация таких экстерналий и должна являться задачей законодательства.

Нельзя не отметить, что именно эту задачу (как указывалось, она заключается в устранении дисбаланса прав и интересов сторон информационных правоотношений) решают существующие и рассмотренные в рамках настоящего исследования институты персональных и неперсональных данных, тайн, общедоступной информации, в том числе открытых данных, каждый из них — в соответствии с собственным предметом и методом регулирования:

— институт персональных данных — закрепляя принципы и основания обработки, в том числе принцип ограниченности целей;

— институт неперсональных данных — стимулируя свободный оборот таких данных, минимизируя случаи локализации данных и поощряя переносимость данных.

В своей совокупности два названных института имеют целью обеспечение свободного оборота данных на соответствующем рынке, но с учетом интересов принципалов данных — индивидов, владельцев устройств Интернета

[131] Внешние эффекты (экстерналии) — это выгоды и издержки, не учитываемые в действующем рыночном механизме ценообразования и в стандартном механизме рыночного распределения ресурсов. Они существуют вне его, не отражаются в ценах, но затрагивают интересы третьих лиц, не участвующих в рыночной сделке, нанося им ущерб (отрицательный внешний эффект) или принося выгоду (положительный внешний эффект). Внешний эффект — это сбой в функционировании рыночной системы хозяйствования, когда рынок оказывается не в состоянии автоматически превратить внешние эффекты в частные издержки и выгоды (Глоссарий. URL: https://lpp.econ.msu.ru/glossary/Article.20110325_6258/).

вещей и иных лиц, чьи интересы затрагиваются обработкой конкретных данных.

Институты тайн также направлены на защиту принципалов данных, т.е. лиц, чьи интересы будут нарушены в случае неограниченного доступа к их информации. Тайны балансируют интересы принципалов доступа к информации, т.е. всех нас, кому нужна информация о деятельности государственных органов и иная затрагивающая нас информация. Методом регулирования обоих институтов является ограничение доступа к информации — институты тайн устанавливают такое ограничение, институт доступа к информации минимизирует случаи такого ограничения, институт открытых данных стимулирует фактическую (а не только юридическую) доступность информации.

Пристального внимания заслуживает возникшая необходимость изъятия некоторых сведений, составляющих тайны, например тайну связи, из правового режима тайн, обусловленная условиями цифровой трансформации, развитием технологий, появлением все большего объема технической, технологической информации, необходимой для оказания соответствующих услуг и сервисов, исполнения договорных обязательств.

Обработка больших данных, принося несомненную выгоду тем, кто ею занимается, создает экстерналии для принципалов данных и, более того, ставит под угрозу существующие механизмы интернализации экстерналий, т.е. механизмы балансировки интересов сторон информационных правоотношений. Эти механизмы, возможно, требуют модернизации вслед за изменившимися информационными технологиями, но они не могут быть разрушены к выгоде отдельных лиц. Здесь также возможна аналогия с промышленным производством и связанны-

ми с ним проблемами утилизации. В результате высоких темпов роста населения, объемов производства и потребления отходы деятельности человечества к началу XXI в. стали общемировой проблемой, представляющей угрозу окружающей среде и экологии планеты. Осознание кризисной ситуации с загрязнением окружающей среды привело к тому, что управление отходами превратилось в один из основных вопросов устойчивого развития городов и целых регионов[132].

Большие данные уже тоже сравнивают с мусором[133], а места их «захоронения» — с полигонами, которые приносят прибыль только их владельцам. Как и в случае с мусором, дешевле и экологичнее разделять объекты по классам в самом начале их жизненного цикла и сохранять это разделение, а не смешивать их на полигоне для того, чтобы потом пытаться извлечь ценность в буквальном смысле из кучи мусора. Такое смешение, помимо прочего, нарушает целостность контекста, являющуюся основой личности человека[134] (если речь идет о персональных данных), и в этом плане создает больше вреда, чем пользы. Цель — это юридический эвфемизм контекста. Отсюда и вопрос о совместимых и несовместимых целях обработки персональных данных, столь важный для эпохи больших данных. Совместимые цели обработки — те, что оставляют информацию внутри контекста.

---

[132] См.: *Прозорова А.С., Мусинова Н.Н.* Организация раздельного сбора и сортировки твердых бытовых отходов в городах России // Актуальные проблемы и перспективы развития государственного управления: сб. науч. ст. по материалам ежегодной междунар. науч.-практ. конф. от 25 ноября 2014 г. / под ред. С.Е. Прокофьева, О.В. Паниной, С.Г. Еремина. М., 2015.

[133] См.: Данные — это новый мусор. URL: https://expert.ru/2020/08/5/dannyie---eto-novyij-musor/.

[134] См.: *Nissenbaum H.* Privacy as Contextual Integrity // Washington Law Review. 2004. Vol. 79. Iss. 1. P. 119–158.

Несовместимые — связанные с перемещением информации в другой контекст (например, продажа товара вместо трудоустройства) либо с объединением информации из разных контекстов[135].

Как видно из проведенного анализа законодательства разных стран, именно такое понимание и заложено в существующих и проектируемых нормативных правовых актах. В зависимости от правовой системы речь может идти о разных правовых механизмах. В США это обеспечение баланса между свободой слова, защищаемой Первой поправкой, и интересами приватности и интеллектуальной собственности. В Европейском союзе это обеспечение оборота данных на цифровом едином рынке, сбалансированное правом тех, чьи интересы затрагиваются оборотом данных, на контроль целей их обработки. Индийские эксперты обозначили правовой статус принципалов данных и разрабатывают правовые механизмы учета их интересов при обработке данных. Законодатели иных азиатских стран создают условия для систем управления большими — преимущественно неперсональными — данными в целях обеспечения безопасности их обработки и учета мнений всех заинтересованных сторон. В любом случае большие данные как новое явление адресуются с использованием существующих правовых институтов. По всей видимости, этим путем следует идти российскому законодателю и правоприменительной практике.

В области **персональных данных** это требует совершенствования режима обезличенных данных, добавления новых оснований для обработки персональных данных без согласия субъекта, модернизации механиз-

[135] См.: *Дмитрик Н.А.* Истоки, смысл и перспективы института персональных данных. С. 67.

мов информирования субъектов и получения согласия субъекта, внедрения института оценки воздействия на обработку данных. В области **неперсональных данных** целесообразным является использование подходов, предложенных для ЕС[136], а именно:

1) повышение доступности анонимных индустриальных данных;

2) стимулирование обмена такими данными;

3) защита законных интересов субъектов, инвестирующих в продукты, генерирующие индустриальные данные;

4) защита конфиденциальных данных;

5) минимизация «запирающего» (*lock-in*) эффекта на рынке данных.

Для достижения обозначенных целей возможно применение следующих инструментов:

— разработка руководящих принципов по стимулированию оборота данных (*data sharing*) с целью внесения большей правовой определенности для участников рынка; руководящие принципы должны быть разработаны с учетом законодательства о защите конкуренции, о защите прав потребителей, о коммерческой тайне, об интеллектуальной собственности и др.;

— стимулирование развития технических решений для свободного обмена данными и связанных с ними стандартных договорных условий (возможно, существующих как в человекочитаемой, так и в машиночитаемой форме), по умолчанию способствующих более свободному обмену данными в *B2B*-секторе (*default contract rules*); учреждение

[136] См.: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «Building a European Data Economy». URL: https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy.

контроля над недобросовестными бизнес-практиками, отклоняющимися от согласованных (в том числе в рамках саморегулирования) принципов оборота данных;

— обеспечение свободного доступа публичных органов к данным, генерируемым без участия человека, при наличии общего интереса (g*eneral interest*), например в целях повышения качества государственного управления, здравоохранения, в научных, статистических целях и т.п.;

— закрепление права производителя данных, являющегося владельцем и пользователем устройства (*data producer's right*), использовать и предоставлять право использования данных, генерируемых этим устройством, с обязательным установлением ограничений такого права (например, возможности использования этих данных производителем устройства);

— обязательное предоставление доступа к некоторым данным в определенных случаях любому третьему лицу в обмен на вознаграждение на принципах добросовестности, разумности и недискриминационности (аналогия с принудительными лицензиями и другими формами использования объектов интеллектуальной собственности без согласия правообладателя, но с выплатой компенсации) с закреплением перечня оснований предоставления данных по такой схеме.

Все вышеперечисленные предложения целесообразно использовать при разработке российского подхода к правовому регулированию оборота информации в эпоху больших данных.

Правовые режимы информации в эпоху больших данных: сравнительно-правовое исследование

ООО «Издательская группа «ЗАКОН»

Ответственный редактор:
В.Б. Румак

Литературный редактор:
О.С. Розанова

Корректор:
Т.А. Казакова

Верстка:
О.Ю. Гранкин

Адрес ООО «Издательская группа «ЗАКОН»:
Россия, 107078, Москва, Красноворотский проезд,
д. 3, стр. 1, под. 2, офис 306

www.igzakon.ru
www. zakon.ru

ISBN 978-5-904208-21-9

9 785904 208219

Подписано в печать 12.12.2021
Формат 148 x 210
Бумага офсетная. Печать офсетная.
Тираж 500 экз.

Отпечатано в ООО «Буки Веди»
Россия, 115093, г. Москва, Партийный переулок, д. 1, корп. 58, стр. 2
info@bukivedi.com