Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Левашенко А.Д., Коваль А.А.

Определение подходов к регулированию персональных данных в России с учетом задачи развития цифровой экономики

Москва 2020

Аннотация В работе проведён анализ правоотношений, связанных с оборотом персональных данных в условиях цифровизации экономики. В рамках исследованию решаются задачи определения наиболее оптимального подхода к регулированию режима персональных данных, в части улучшения правоотношений субъекта персональных данных и оператора данных, статуса и объёма прав каждого из участников работы с персональными данными. Работа закладывает основы для разработки проблемы соотношения прав субъекта персональных данных и практики их коммерциализации в условиях развития цифровой экономики, а также использования новых методов и технологий защиты неприкосновенности частной жизни человека в условиях технологического развития. В результате исследования сформулированы предложения по совершенствованию законодательства о персональных данных в России на основе анализа стандартов ОЭСР и законодательства стран-членов и партнеров Организации.

Ключевые слова: персональные данные, информация, цифровизация экономики, ИКТ, конфиденциальность, неприкосновенность частной жизни

Левашенко А.Д. – руководитель Центра Россия-ОЭСР Российской академии народного хозяйства и государственной службы при Президенте РФ

Коваль А.А. – младший научный сотрудник Центра Россия-ОЭСР Российской академии народного хозяйства и государственной службы при Президенте РФ

Данная работа подготовлена на основе материалов научно-исследовательской работы, выполненной в соответствии с Государственным заданием РАНХиГС при Президенте Российской Федерации на 2020

Оглавление

1 ВВЕДЕНИЕ

Современное развитие цифровой экономики, в которой персональные приобретают новый экономический статус, ставит вопрос о переосмыслении правового регулирования правоотношений, связанных с оборотом персональных данных. Сегодня законодатели различных стран стремятся найти сбалансированный подход к том, чтобы сохранить ценности и информационные права человека, признанные ещё в прошлом веке, и одновременно обеспечить возможность использования экономического потенциала этих особых информационных ресурсов. Этот поиск выражается в модернизации международных стандартов защиты субъектов персональных данных, принятии новых законодательных актов, разработке компетентными органами тематических руководств по работе с данными.

Основной целью данного исследования является проведение анализа правоотношений, связанных с оборотом персональных данных в условиях цифровизации экономики, и формулирование предложений по совершенствованию законодательства о персональных данных в России на основе анализа стандартов ОЭСР и законодательства стран-членов и партнеров Организации.

Основными задачами данной работы являются определение значения персональных данных для развития цифровой экономики; анализ стандартов ОЭСР, Совета Европы и других международных организаций в сфере анализа и обработки персональных данных; анализ подходов государств-членов ОЭСР и партнеров Организации к регулированию персональных данных, и в частности, правил конфиденциальности на онлайн-платформах; формирование предложений для развития регулирования персональных данных в России на основе лучших международных практик.

Результаты данного исследования могут быть использованы в работе федеральных органов исполнительной власти в целях улучшения правового регулирования персональных данных и обеспечения правовых основ для цифровой экономики.

Научно-исследовательская работа обладает научной новизной, поскольку представляет результаты анализа последних правовых трендов, зарубежных нововведений и доктринальных предложений, которые служат опорой в разработке законопроектов в соответствующей сфере.

1 Значение персональных данных для развития цифровой экономики

Возрастающая роль данных в жизни общества и экономике. Рост взаимодействия между данными, алгоритмами и аналитикой больших данных, Интернетом вещей и людьми открывает огромные возможности для экономики. По оценкам ОЭСР, в 2015 году глобальный объем данных составил 8 зетабайт (8 триллионов гигабайт), что в 8 раз больше, чем в 2010 году. По прогнозам, к 2020 году этот объем увеличится в 40 раз, так как технологии, включая Интернет вещей, создают огромные новые наборы данных. Однако это также порождает проблемы, связанные с управлением данными, на национальном и международном уровнях. К ним относятся вопросы, связанные с управлением доступностью данных, удобством их использования, целостностью и безопасностью, с владением данными, их влиянием на торговлю и конкуренцию, последствиями для личной конфиденциальности и др. Использование цифровых технологий и данных лежит в основе цифровой трансформации во всех секторах экономики и общества, что означает, что любые политические решения в отношении данных могут иметь широкий эффект. Данные не являются новым явлением, но сейчас они растут беспрецедентными темпами. Люди записывают факты в виде символов, цифр и букв на протяжении тысячелетий. Новым является объем данных, производимых каждый день в результате распространения устройств, услуг и датчиков в экономике и обществе. Объем данных только увеличивается с их сбором и использованием, создавая широкие возможности для научного открытия и для улучшения существующих или изобретения новых продуктов и услуг.

Данные становятся ценными, когда они используются для улучшения социальных и экономических процессов, продуктов, организационных методов и рынков. Такие инновации, основанные на данных, лежат в основе многих новых бизнес-моделей, которые трансформируют рынки и сектора, от сельского хозяйства до транспорта и финансов, и стимулируют рост производительности. Использовать потенциал данных можно в случае, если обеспечена их доступность. Например, открытие доступа к научным данным, особенно когда исследования финансируются государством, может стимулировать сотрудничество, распространение, воспроизведение и применение результатов научных исследований. Инициативы «открытых государственных данных» могут стимулировать инновации и новые бизнес-модели.

Исследования показали, что компании, принимающие решения, основанные на данных, могут повысить производительность на 5-6%, при этом Европейская комиссия подсчитала, что «даже ограниченное использование решений для анализа больших

данных ведущими 100 производителями ЕС может ускорить экономический рост ЕС за счет дополнительного 1,9% к 2020 году». Данные также играют важную роль в развитии ИИ и машинного обучения, в котором цифровая программа выполняет роль лица, принимающего решения. ИИ обладает значительным потенциалом для экономического роста. Согласно одной из оценок, к 2030 году ИИ может увеличить ВВП на 10%.

Данные играют все более важную экономическую роль в поддержке международной торговли и сотрудничества. По данным Глобального института McKinsey, трансграничные потоки данных выросли в 45 раз с 2005 по 2014 год и составили 2,8 триллиона долларов (около 3,3%) мирового ВВП в 2014 году. Цифровизация увеличивает масштаб, объем и скорость торговли. Это позволяет компаниям предлагать новые продукты и услуги большему количеству клиентов по всему миру. В цифровую эпоху данные являются основой международной торговли, включая трансграничную торговлю услугами. Есть много причин, руководствуясь которыми страны регулируют потоки данных. Одной из них, несомненно, является защита неприкосновенности частной жизни физических лиц и их персональных данных. Страны также могут ограничивать поток данных или предписывать, чтобы данные хранились локально, для достижения других целей регулирования, таких как доступ к информации для целей проведения проверок. Ограничения на потоки данных могут также быть связаны с целью защиты информации, которая считается конфиденциальной с точки зрения национальной безопасности, или для того, чтобы службы национальной безопасности могли получать и просматривать соответствующие данные.

В торговых соглашениях все чаще появляются четкие положения, касающиеся трансграничных потоков данных. Такие положение нашли свое отражение, например, во Всеобъемлющем и прогрессивном соглашении о транстихоокеанском партнерстве (Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP) и Соглашении между США, Мексикой и Канадой (United States–Mexico–Canada Agreement, USMCA). В настоящее время ЕС также предлагает горизонтальные положения о трансграничных потоках данных и защите персональных данных в своих торговых соглашениях. Тем не менее, нет единого мнения о том, в какой степени меры защиты персональных данных должны подпадать под действие торговых соглашений. В условиях отсутствия согласованных на уровне международных соглашений требований страны применяют соответствующие меры в одностороннем порядке.

Таким образом, роль и значение данных сегодня невозможно недооценить. Они являются новым источником ценности в глобальной экономике.

2 Анализ стандартов ОЭСР, Совета Европы и других международных организаций в сфере анализа и обработки персональных данных

Определение персональных данных и степени идентифицируемости

Персональные данные впервые стали получать правовое регулирование в 1970 гг. Первые законы о защите данных появились в Швеции (1973), США (1974), Германии (1977), Франции, Австрии, Дании, Норвегии (1978), Люксембурге (1979). К персональным данным относят информацию, идентифицирующую или способную идентифицировать личность, субъект данных. Данная формулировка лежит в основе определений персональных данных в международных актах (Конвенция №108 Совета Европы о защите физических лиц в отношении автоматической обработки персональных данных; Рекомендация Совета, касающаяся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных 1980 г. (в ред. 2013 г.), региональных актах (Общий регламент ЕС о защите персональных данных 2016 г.), национальных законах (законы о защите данных в странах ЕС от 2018 г., отражающие и дополняющие положения регламента ЕС, Закон Бразилии об общей защите данных 2018 г.). Однако определения различаются и по юридической технике, и по степени детализации определения.

В ЕС к базовому определению приводятся перечисления отдельных идентификаторов и видов персональных данных. В соответствии с Регламентом ЕС (2016) персональными данными является «информация, относящаяся к идентифицированному или идентифицируемому физ. лицу (субъект данных). Субъект персональных данных может быть идентифицирован прямо или косвенно, в частности, на основе идентификационной информации, такой как имя, идентификационный номер, данные о местоположении, идентификаторы в интернете, например ID или информация об учетной записи пользователей, или посредством одного или нескольких показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физ. лица» (п.1 ст.4).

В Японском законе о защите персональной информации 2017 г. персональные данные определяют, как персональную информацию, помещённую в базу данных, а уже персональная информация означает информацию, относимую к личности по двум основаниям: личностное описание (имя, дата рождения) и идентификационный код.

В Китае, в соответствии с Законом о кибербезопасности 2017 г., квалификация в качестве персональных данных также привязывается к использованию технических

средств в работе с информацией, которая позволяет идентифицировать физическое лицо, включая имя, дату, рождения, биологические данные, адрес и номер телефона.

В Южной Корее, в соответствии с Законом о защите личной информации 2011 г., персональные данные определяются как «любая информация, которая относится к живому физическому лицу, которое идентифицируется или которое можно идентифицировать по этим данным, включая имя, регистрационный номер резидента и изображение, и т. д. (включая информацию, которая сама по себе не позволяет непосредственно идентифицировать конкретного человека, но это идентифицирует конкретного человека, когда это легко сочетается с другой информацией)».

Более распространено определение персональных данных без специальных содержательных указаний. Законопроект Индии 2019 г. о защите персональных данных определяет персональные данные, как «данные о физическом лице или относящиеся к нему, которые могут прямо или косвенно идентифицировать его с учетом любой характеристики, признака, атрибута или любой другой особенности личности такого физ. лица, или любой комбинации таких признаков, или любых сочетаний таких функций с любой другой информацией» (п. 28 ст. 3).

Однако регулирование персональных данных может происходить и без использования единого определения персональных данных, если законодательство страны о защите данных организовано по отраслевому принципу, как в США. На федеральном уровне действуют такие законы, как Закон о честной кредитной отчётности 1970 г., Закон о конфиденциальности 1974 г., Закон о конфиденциальности видео 1988 г., Закон о защите медицинских данных 1996 г., Закон о защите финансовых персональных данных 1999 г., Закон о защите персональных данных детей в интернете 2000 г. Параллельно действует разветвлённая система законов о персональных данных на уровне штатов, которые могут не совпадать между собой по содержанию.

В России, в соответствии с ФЗ «О персональных данных», персональные данные определяются как «любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных). Определение, данное российским законодателем, повторяет классическую структуру понятия персональных данных: «информация» и прямая или косвенная связь (отношение) к физическому лицу, т.е. идентификация. Избранный подход не ограничивает содержание персональных данных самым высоким уровнем идентифицируемости - «определённое лицо», но также включает в понятие информацию, относящуюся к потенциально «определяемому» лицу.

Определение «персональных данных» в зависимости от того идентифицирует информация или нет, в научной доктрине назвали бинарным подходом. Несмотря на его ясность и распространённость, подход критикуется с нескольких точек зрения.

Во-первых, подход технически не оправдан, поскольку неясен *порог идентификации*, когда неперсональные данные могут переходить в категорию персональных. Во-вторых, бинарный подход – слишком простая конструкция для выделения персональных данных. Таким образом, бинарный подход ограничивается не просто «идентифицируемостью» данных, а именно видимым свойством идентификации во внешней среде. В-третьих, сами по себе персональные данные настолько *разнообразны*, что могут отличаться по рискам, связанным с их сбором, обработкой и использованием.

На экспертном уровне формируется подход разграничения персональных данных по видам идентифицируемости. Так, в стандарт ISO/IEC 19944:2017, разработанном совместно Международной организацией по стандартизации и Международной электротехнической комиссии, различается 5 степеней идентифицируемости данных. Таким образом, степень идентифицируемости информации может быть градуирована по уровню удаленности конечных данных от их персонального носителя.

Так как удалённость обработанных данных от субъекта этих данных определяется процессом их обработки, то представляется необходимым провести разграничение применяемых методов обработки данных по критерию достигаемой удалённости. В соответствии с международными стандартами ISO следует разграничить 1) идентифицированные данные (identified data); 2) псевдонимизированные данные (preudonymised data); 3) несвязанные псевдонимизированные данные (unlinked pseudonymised data); 4) анонимизированные данные (anonymized data); 5) агрегированные данные (aggregated data).

Персональные данные как объект гражданских прав

Применительно к персональным данным можно видеть, что персональные данные действительно составляют объект личного интереса конкретных лиц, которые вправе распоряжаться своими данными и это право защищается законом. В этом контексте под введением в право собственности (propertization) понималось получение контроля над персональными данными.

Очевидная проблема заключается в том, что при передаче персональных данных, их носитель не утрачивает связи с идентификаторами в этих данных, он по-прежнему ими идентифицируется. Кроме того, данные являются неисчерпаемым ресурсом. Передавая сведения, лицо может утратить контроль над данными в той форме, в которой они были переданы, однако эти же данные он может распространять и передавать другим лицам, в

иной форме и иным образом. В случае персональных данных не возникает ситуации отчуждения объекта, обременённого иными имущественными правами. Право на персональные данные всегда свободно от претензий третьих лиц. Есть аргумент, исключающий легитимную возможность «propertization», в силу того, что информационная неприкосновенность личности является общественным благом, а значит, попытки её отчуждения у личности нарушает общественный порядок. Значит, контроль над данными может быть только у субъекта данных. Значит, он не неотчуждаем. Следовательно, право на персональные данные нельзя считать полноценным правом собственности в общепринятом его понимании.

Если рассматривать персональные данные как нематериальные ценности, то в России их правовой режим подпадает под нормы гражданского законодательства. В соответствии со ст.128 ГК РФ в число объектов гражданских прав входят нематериальные блага. Нематериальные блага являются необоротоспособными в силу того, что они привязаны к личности. Следовательно, они не могут переходить к другим лицам. Однако их можно предоставлять для пользования.

В то же время персональные данные могут рассматриваться и в качестве разновидности иного объекта гражданских отношений – информации. Некоторые юристы приходят к тому умозаключению, что российский законодатель наделил персональные данные необоротоспособным характером, когда с 1 января 2008 г. из числа объектов гражданских прав, поименованных в ст.128 ГК, была исключена «информация». По законодательному определению персональные данные относятся именно к понятию информации. Определение персональных данных как информации не делает их автоматически оборотоспособными объектами гражданских прав, но при этом не исключает их возможность быть объектом гражданских отношений.

В целом приходится констатировать неопределённость в правовом статусе персональных данных как объекта гражданских прав. На данный момент российский законодатель придерживается европейского подхода в понимании того, что персональными данными нельзя торговать в силу принципа неприкосновенности частной жизни. Таким образом, персональные данные неотчуждаемы, поскольку составляют содержание неотчуждаемых прав человека. В дискуссии российских авторов отмечается, что такой подход к защите персональных данных, который бы включал консенсуальное условие, экономически более выгоден бизнесу, чем коммерциализация данных. Бизнес заинтересован в работе с полными релевантными персональными данными. Экономические выгоды от работы с полноценными данными покрывают издержки исполнения обязательств по работе с персональными данными.

В мире уже появилась законодательная практика по коммерциализации данных. С начала 2019 г. вступил в силу Закон штата Вермонт (США) о регулировании информационных брокеров. Согласно законодательному определению, информационным брокером считается компания, одно или несколько подразделений компании, которые открыто собирают, продают или предоставляют лицензии третьим сторонам на личную информацию потребителя, с которым компания не имеет прямых отношений. Информационные брокеры должны ежегодно регистрироваться у Секретаря штата, а также отчитываться о соблюдении минимальных стандартов обеспечения защиты персональных данных. Таким образом, законодатель штата Вермонт выводит коммерческий оборот персональных данных из теневой экономики и требует обязательного соблюдения гарантий защиты персональных данных.

Статус и режим обезличенных данных

Обезличивание данных имеет экономическое и правовое значение в современных условиях. В Руководящих принципах ОЭСР по защите неприкосновенности частной жизни и трансграничной передачи персональных данных отмечалось, что широкое и новаторское использование персональных данных приносит значительные экономические и социальные блага, но вместе с тем увеличивает риски для неприкосновенности частной жизни. Масштабный сбор и обработка персональных данных необходимы для развития общества. В программном документе ОЭСР по торговле и трансграничной передаче данных 2019 г. отмечается рост и потребность в потоках данных. Для многонациональных компаний передача данных – это основа каждодневных операций. В данных условиях технологии обезличивания позволяют минимизировать риски, возрастающие вместе с наращиванием потоков данных. Экономическая ценность обезличивания выражается в том, что оно освобождает от необходимости делать выбор между экономическими преимуществами обмена данными и соблюдением прав человека. Обезличивание снимает препятствия к взаимовыгодной работе с данными.

Обезличивание данных – один из способов их защиты. Степень «обезличивания» данных может определять какая степень правовой и технической защиты необходима и какой должен быть уровень контроля доступа. Чем меньше данные связаны с личностью, т.е. достаточно обезличены, тем свободнее может быть оборот этих данных. Выделяют несколько способов предотвращения раскрытия персональной информации:

1) сокращённый сбор данных (reduced data collection),

2) шифрование (cryptography),

3) де-идентификация (псевдонимизация, анонимизация),

4) функциональное разделение (unlinkability/ functional separation),

5) добавление шумов и дезинформация.

В доктрине самым надёжным способом считается *сокращённый сбор данных*, поскольку, если нет данных, информация и не может быть извлечена. Принцип минимизации сбора должен позволять субъектам данных ограничивать или отказываться от предоставления данных. Метод упоминается в национальных руководствах по де-идентификации исполнительных органов, уполномоченных по защите данных, например, в руководстве Корейского агентства по вопросам интернета и безопасности Министерства внутренних дел и безопасности.

Помимо технических различий способов защиты данных, можно столкнуться с терминологическими отличиями самого понятия «обезличивания». Например, русскоязычный термин «обезличенные» данные равно применим при переводе терминов «anonymized data», «pseudonymized data», «de-identified data». В Общем регламенте ЕС по защите данных (General Data Protection Regulation, GDPR) вводится термин «pseudonymization». «Псевдонимизация» не тождественна понятию «анонимизации» персональных данных. Как отмечается в документе Рабочей группы ЕС по защите личности в отношении обработки персональных данных, «pseudonymysed» данные не могут приравниваться к «anonymised» данным, поскольку они оставляют возможность выделить субъекта данных и установить связь с ним иных данных». Понятие «de-identification» выступает родовым для «pseudonymization» и «anonymization», поскольку указывает не результат, а только суть процесса – снятие возможности идентификации.

В ФЗ «О персональных данных» 2006 г. используется термин обезличивание, как «действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных». Очевидно, что термин «обезличивание» был введён для описания процесса, который в Регламенте ЕС обозначен термином «pseudonymization». Этот подход неточен, поскольку термин «обезличивание» как устранение связи данных с лицом, может включать в себя устранение с помощью замены и устранение без возможности восстановления связи.

Подходы на получение согласия на обработку данных

Согласие субъекта персональных данных служит правовым основанием обработки его данных. Эксперты ОЭСР выделяют проблему реализации действующего общепринятого подхода к получению согласия субъекта персональных данных в аспекте проведения медицинских научно-исследовательских работ с вовлечением большого количества данных. При сборе данных для целей научно-исследовательских работ, прежде всего в области медицины, получение информированного согласия означает, что субъект

данных осведомлён и понимает цели исследований, для которых собираются его данные. Однако в условиях создания новых форм биомедицинских исследований, когда используются большие массивы данных из различных источников, реализация общепризнанного стандарта работы с персональными данными, как получение согласие субъекта данных, становится затруднительной. Например, в случае биобанков, где сосредоточены множество исследователей и исследовательских проектов, сложно получить прямое согласие на все цели возможных исследований в будущем.

На данный момент самым распространённым подходом к согласию субъекта персональных данных, применяемом научными центрами, является получение широкого единовременного согласия («one-time general consent» или «broad consent»). Это значит, что субъект персональных данных даёт согласие на работу со своими данными с целью медицинского исследования, без указания конкретных исследовательских проектов. Данный подход позволяет удовлетворить интересы субъектов персональных данных в том, чтобы контролировать использование их данным третьими лицами, и вместе с тем, освобождает организации от необходимости получения неоднократного согласия. Не следует понимать широкое согласие, как согласие на использование данных любым образом третьими лицами, порядок получения такого согласия не освобождает от указания характера собираемой информации, хранения, обработки и будущего использования персональных данных.

Возможно получать согласие субъекта данных не для целей исследования в целом, а так называемое пошаговое согласие («tiered" или «step-by-step consent»). Такой подход был принят в Имперском Колледже для проведения исследования по предотвращению деменции и других возрастных нейродегенеративных заболеваний при участии 20 000 волонтёров. Участник медицинских исследований может изначально выразить согласие на использование собранных данных, с тем, чтобы к нему больше не обращались из организации, или наоборот, заявить своё осторожное отношение к использованию персональных данных и согласию на рассмотрение вопроса о даче своего повторного согласия. И таким образом, круг лиц, к которым нужно обращаться за повторным согласием, значительно сужается. Но такой способ работает на локальном уровне — на уровне одного или нескольких научных институтов. Однако, чем больше массив данных, тем более затратно получать повторное согласие каждого субъекта.

В правовой доктрине также предлагаются модели "адаптивной" или "динамичной" формы получения согласия (adaptive/ dynamic consent). В соответствии с таким подходом, лица, участвующие в медицинских исследованиях, и дававшие согласие на работу со своими медицинскими данными, могут получать запросы о повторном согласии на новое

направление использования персональных данных через интернет-коммуникационные сети (мессенджеры, социальные сети и др.). Такая модель называется “динамичной” поскольку она позволяет устанавливать контакт с субъектом данных в любое время в удобной форме. Преимуществом динамичной модели является то, что субъект также получает возможность в любое время отозвать своё согласие или изменить условия своего согласия, и при этом быть уверенным, что его последующие шаги, связанные с ранее выданным согласие на сбор и обработку данных, будут учтены. Таким образом, в сфере научно-исследовательской деятельности возможно использовать 4 подхода к согласию субъекта персональных данных.

Определение статуса обработчика и контролера данных

Рекомендация о руководящих принципах защиты конфиденциальности и трансграничных потоков персональных данных (2013 г.) определяет «контролера данных» как «сторону, которая в соответствии с национальным законодательством компетентна принимать решение о содержании и использовании (персональных и не персональных) данных независимо от того, кем (стороной или ее агентом) была собрана, обработана или распространена данная информация». Их иногда считают «владельцами данных», даже если они не имеют законных прав собственности на данные, которыми они управляют. По этой причине их иногда также называют «хранителями данных» (data stewards). Владельцы данных могут хранить как данные из частного сектора, так и государственного. Владельцами данных могут быть не только организации. Субъект данных, контролирующий свои персональные данные и имеющий возможность обмениваться ими с заинтересованными лицами, также может считаться владельцем данных. Стоит отметить, что контроль владельца данных не безграничен. После того, как данные будут доступны или переданы, если не будут приняты конкретные меры по управлению данными и их обработке, эти данные выйдут за пределы информационной системы исходного контролера данных и, таким образом, выйдут из-под его/ее контроля. То же самое относится и к лицам, которые предоставляют свои данные и дают свое согласие на их повторное использование и передачу. Владельцы данных не могут контролировать, каким образом их данные используются повторно.

Помимо контролера персональных данных также выделяют «обработчика данных» (processor). Общий регламент по защите данных (General Data Protection Regulation, GDPR) строго разграничивает контролеров и обработчиков данных, поскольку от роли субъекта данных зависят их обязанности и объем ответственности.

Обработчик данных (processor) – физическое или юридическое лицо, государственный орган, учреждение или другое лицо, обрабатывающее персональные

данные по поручению оператора персональных данных. Обработчик данных не может привлечь другого обработчика без предварительного письменного разрешения контролера. Согласно п. 3 ст. 28 GDPR, если обработка данных осуществляется от имени контролера, контролер и обработчик данных должны заключить договор (или другой юридический акт), в котором указываются предмет договора и продолжительность, характер и цель обработки, тип персональных данных и категории субъектов данных, обязанности и права контролера. Обработчик должен всегда действовать в соответствии с документированными инструкциями контролера, соблюдать требования GDPR, обеспечивать соблюдение конфиденциальности лицами, имеющими право на обработку данных/доступ к таким данным и др. Как контролер, так и обработчик должны вести учет обработки данных, осуществляемой под их ответственностью.

Определение статуса пользователя данных

Согласно отчету ОЭСР «Расширение доступа к данным и обмена ими: согласование рисков и преимуществ повторного использования данных в разных обществах», одними из основных действующих лиц в сфере персональных данных являются пользователи данных (data user). Пользователями данных могут быть различные лица. Например, согласно вышеуказанному отчету ОЭСР, пользователями данных могут быть:

– потребители, которые имеют прямой доступ к данным о них, которые контролируются предприятиями;

– граждане, которые получают доступ к данным государственного сектора, предоставляемым правительствами в рамках своих инициатив по открытым данным;

– исследователи, которые получают доступ к научным данным, доступным через открытый научный проект;

– предприятия, которые получают доступ к данным, например, через партнерства в области данных, открытые данные или инициативы по переносимости данных.

В соответствии с типологией действующих лиц на рынке персональных данных, сформулированной в отчете Всемирного банка «Information and Communications for Development 2018: Data-Driven Development», пользователями данных являются предприятия, которые покупают продукты агрегаторов данных (или брокеров). Агрегаторы данных или брокеры данных собирают персональные данные из публичных и частных источников с целью их дальнейшей продажи. Одним из самых известных брокеров данных является Bloomberg.

В некоторых случаях различные пользователи могут использовать одни и те же данные, но в различных целях. Например, общедоступные данные предоставляются через открытые данные гражданам для наблюдения за деятельностью государственного сектора (прозрачность), ученым в исследовательских целях и предприятиям для создания новых коммерческих возможностей. Взаимодействие с пользователями данных может быть в интересах владельцев данных, готовых делиться своими данными.

Пользователи данных несут ответственность за создание социальной и экономической ценности обмена данными. Персональные данные могут представлять финансовую ценность для пользователей данных. Например, в случае, когда персональные данные продаются маркетинговым компаниям. Используя рекламу в качестве источника дохода, организации обычно предоставляют людям - производителям данных - бесплатный доступ к их услугам, либо по низкой стоимости. К таким пользователям относят социальные сети, поисковые системы, информационные и новостные порталы. Стоит отметить, что прежде чем передать персональные данные другой компании, компания-владелец данных должна «продемонстрировать», что данные были изначально получены в соответствии с GDPR (в случае с компаниями, в отношении деятельности которых применяется европейское законодательство) и компания вправе использовать такие данные в коммерческих целях для рекламы. В Калифорнии, согласно закону о защите данных потребителя (California Consumer Protection Act, CCPA), субъект данных вправе отказать в продаже своих персональных данных. Согласно разделу 1798.120 CCPA, потребитель вправе в любое время обратиться к предприятию (business), которое продает персональную информацию о потребителе третьим лицам, с требованием не продавать персональные данные потребителя. Такое право отказа называется «right to opt out».

Определение статуса посредника данных

В большинстве случаев конечные пользователи данных, потребители и компании, получают обработанную информацию с добавленной стоимостью. Такая информация является результатом деятельности посредников данных. Посредниками данных признаются лица, которые способствуют обмену данных. Благодаря обмену данными персональные данные могут быть повторно использованы потенциальными пользователями данных. Существуют разные виды посредников данных: хранилище или банк данных (data repositories), брокеры данных (data brokers), рынки данных (data marketplaces), системы управления личной информацией и хранилища персональных данных (personal information management systems and personal data stores), доверенные

третьи лица (trusted third parties). Самыми популярными являются банк или хранилище данных (data repositories) и брокеры данных (data brokers).

Хранилище или банк данных (Research) data repositories). Банк данных служит преимущественно общественным благам, и используется, например, научным сообществом в качестве архива или библиотеки данных. Основной задачей хранилищ данных является сохранение данных в качестве источника знаний для общества. Таким образом, они выполняют ту же функцию, что и традиционные библиотеки или архивы. Хранилища данных особенно важны для науки, поскольку сохранение данных и политика открытых данных становятся все более распространенными и значимыми, особенно в контексте открытой науки.

Брокеры данных (Data brokers). Брокерами данных, в основном, являются коммерческие организации. Основная цель брокеров данных заключается в сборе и агрегировании данных, включая личные данные. Брокеры данных, такие как Bloomberg, Медиалаборатория РИА Новости, РБК и др., используют различные источники данных, которые используются для услуг, связанных с данными. Приспосабливая свои услуги для различных целей, брокеры данных продают продукты различным типам клиентов. Некоторые брокеры данных также анализируют свои наборы данных, чтобы предоставлять своим клиентам информационные и разведывательные услуги в разных сферах для различных целей, включая проверку личности человека, маркетинг продукта и обнаружение мошенничества.

Рынки данных (Data marketplaces). В последние годы также появились «рынки данных» (data marketplaces) – онлайн-платформы, на которых размещаются данные от различных издателей и которые предлагают данные заинтересованным сторонам, система управления персональной информацией/хранилище персональных данных, которые служат потребителям для управления совместным использованием их персональных данных. Одним из важных отличительных факторов между брокерами данных и поставщиками рынка данных является то, что брокеры данных активно участвуют в сборе дополнительных данных и их агрегации, тогда как поставщики рынка данных являются пассивными посредниками, через которых контролеры данных, включая брокеров, могут предлагать свои наборы данных. Несмотря на рост числа посредников данных, не существует единого рынка данных, где организации и частные лица могли бы продавать или обмениваться данными непосредственно друг с другом. Таким образом, могут существовать различные бизнес-модели.

Системы управления личной информацией и хранилища данных (Personal information management systems and personal data stores). Системы управления личной

информацией и хранилища персональных данных являются платформами, предоставляющими субъектам данных (потребителям) больший контроль над своими личными данными и, таким образом, позволяющими восстановить пользовательское посредничество (user agency), в том числе в контексте Интернета вещей. Поэтому концепция систем управления личной информацией и хранилищ персональных данных получает большое внимание в качестве движущей силы переносимости данных, поскольку они могут функционировать как централизованная инфраструктура данных, позволяющая отдельным лицам управлять своими личными данными. Примером системы управления персональной информацией и хранилищами персональных данных в туризме является Omotenashi, приложение в Японии, которое может собирать существующую личную информацию из социальных сетей, которой можно поделиться с местным бизнесом (при условии согласия пользователя).

Доверенные третьи лица (Trusted third parties). Доверенные третьи лица могут способствовать обмену данными и их повторному использованию. Такими посредниками могут быть различные платформы и организации. Крупные поставщики данных могут либо назначить существующую доверенную организацию, либо создать новую доверенную организацию и платформу для выполнения функций посредника данных. В качестве примера можно привести Платформу больших данных для судов (Ship Big Data Platform), которая была создана Японской морской ассоциацией и объединяет, и предоставляет различные наборы данных от данных о погоде до данных о судне, включая информацию о правах собственности на судно, операторах и траектории.

2.7 Переносимость данных

Переносимость данных (portability of data) означает возможность передачи данных, собранных и обрабатываемых одним оператором, другому оператору по воле субъекта этих персональных данных. Возможность переноса данных входит в круг прав субъекта осуществлять контроль над собранными данными, в т.ч. передавать и использовать повторно эти данные на различных онлайн-платформах. Ценность переносимости данных выражается в трёх аспектах. Во-первых, пользователи могут эффективно распоряжаться своими данными независимо от того, кем и как они были собраны и обработаны. Во-вторых, провайдеры платформ могут снизить порог входа на рынок услуг, для которых необходимы персональные данные пользователей, поскольку они могут получать доступ к целому комплексу данных простым переносом. В-третьих, переносимость данных способствует практике повторного использования собранных данных, повышает конкуренцию и эффективность цифровых платформ.

С технической точки зрения переносимость данных часто сопряжена с проблемой операционной совместимости данных (interoperability), с правовой точки зрения переносимость данных требует законодательно закреплённой гарантии субъектам персональных данных, что их собранные данные остаются в их распоряжении, они всегда могут быть как отозваны, так и перенесены.

Преимущества обеспечения переносимости данных. Во-первых, переносимость данных обеспечивает укрепление конкуренции в цифровой экономике среди провайдеров платформ за счёт корректировки информационной асимметрии среди поставщиков товаров, услуг и их потребителей; посредством ограничения расходов на перенос данных и снижения барьеров для входа на рынок. На высококонкурентном рынке эффективно устанавливаются оптимальные условия для пользователей, например, оптимизируется цена товаров и услуг.

Во-вторых, переносимость данных создаёт возможности для развития инноваций, работающих на основе баз данных. Поддержка инноваций способствует появлению новых продуктов на цифровом рынке, расширению существующих рынков и их содержательной диверсификации. В странах ОЭСР известны частные, публичные и смешанные практики по обеспечению переноса данных. Например, в Великобритании в 2012 г. была запущена инициатива Midata, в соответствии с которой все британские компании, обслуживающие физических лиц (коммунальные услуги, магазины, web-сервисы и др.) должны обеспечить доступ своим потребителям к истории их транзакций в читаемом формате. Введение программы стимулировало развитие новаторских подходов на потребительском рынке и распространение сервисов по сравнению цен среди провайдеров платформ.

В-третьих, переносимость данных способствует движению потока данных и обмену данными (data sharing). Эксперты ОЭСР отмечают, что содействие обмену данными может выражаться в том, как возрастает доверие пользователей к концепции сбора персональных данных как таковой. Пользователи могут быть уверены, что, передавая данные, они не утрачивают контроль над ними, и, как следствие, возрастает мотивация к передаче своих данных. Увеличивается обмен данными, поскольку имея возможность эффективного контроля за своими данными, пользователи могут спокойно принимать решения, как и кому могут передаваться и данные.

В-четвёртых, обеспечение права на перенос данных является условием информационного самоопределения субъектов персональных данных. Стоит подчеркнуть, что переносимость данных составляет неотъемлемую часть принципа участия субъекта персональных данных (individual participation principle) в соответствии с Руководством ОЭСР по защите неприкосновенности частной жизни и трансграничной передаче данных.

Право участия означает право физического лица запрашивать от организации сведения о наличии в базе данных организаций информации о себе и другие сопутствующие шаги (п.13). Способность субъекта данных скачивать персональные данные, собранные оператором данных повышает транспарентность информационной среды и позволяет субъекту персональных данных принимать взвешенное решение о необходимости внесения исправления в персональные данные или их удаления. Наконец, возможность переноса данных позволяет субъекту выбирать оператора данных с лучшими технологиями по управлению или по обеспечению безопасности данных. В этом смысле перенос данных позволяет оградить субъекта персональных данных от проблем утраты данных или их недоступности.

Эксперты ОЭСР выделяют ряд вопросов обеспечения переносимости данных.

1. Определение переносимости данных. Персональные данные не являются однородными, они различаются по содержанию, по потенциальной экономической ценности, по субъектам. В связи с этим приходится говорить о нескольких типах данных. Физические лица часто обращаются к переносу данных социальных сетей для различных сервисов. Организации могут быть заинтересованы в переносе технических данных, собранных с использованием технологий Интернета вещей, или рейтинговых данных, которые обычно используются в электронной коммерции. Возникает вопрос о том, является ли принцип переносимости данных универсальным или он ограничен конкретными типами данных.

2. Техническое обеспечение переносимости данных – операционная совместимость. Одна из самых часто встречающихся проблем переноса данных – операционная несовместимость. Эта техническая неполадка возникает из-за отсутствия единых стандартов в образовании систем обработки данных. Даже когда используются общие машиночитаемые форматы, операционная совместимость не гарантирована. Поэтому на практике складывается ситуация, когда право на перенос данных субъект персональных данных осуществляет лишь частично, субъект может скачать машиночитаемую цифровую копию его данных, собранных у одного оператора, но не может их использовать у другого оператора.

3. Затратность обеспечения переносимости данных. Перенос данных не должен требовать у субъекта персональных данных покрытия расходов на его обеспечение. Однако создание инфраструктуры, которая бы обеспечивала переносимость данных является очень затратным. В связи с этим для малых и средних компаний обеспечение переносимости данных является непомерно тяжёлой задачей, тогда как переносимость данных входит в число базовых законодательных требований ко всем операторам данных.

4. Обеспечение безопасности и ответственности. Эксперты ОЭСР ставят вопросы о том, какие обязанности несут операторы данных при переносе данных в другую систему; могут ли операторы данных нести ответственность за неправильное обращение с данными субъектом персональных данных; кто из операторов ответственен за безопасность процесса передачи данных; кто и на каком этапе осуществляет контроль или определённый вид контроля за переносимыми данными.

5. Обеспечение защиты персональных данных. Перенос данных, как и другие действия операторов с данными, подпадает под режим защиты персональных данных. Вместе с тем, при переносе данные подвержены трём видам рисков нарушения их сохранности или связанных с ними прав. Во-первых, есть риск манипуляций в установлении связи между субъектом данных, хранящихся у оператора, и лицом, запрашивающим данные. Во-вторых, процедура идентификации данных с лицом, их запрашивающим, может требовать снятия некоторых установок встроенной системы обеспечения защиты (восстановление идентификаторов), это значит, что в какой-то момент оператор работает с данными не в обезличенном, а в «восстановленном» виде. В-третьих, переносимость данных может затронуть интересы третьих лиц, которых касается переносимая информация от одного оператора к другому.

6. Необходимость защиты от злоупотребления принципом переносимости данных. Перенос данных – это, прежде всего, право субъекта персональных данных, и уже в качестве коррелирующего элемента к нему устанавливается обязанность оператора обеспечить перенос. Переносимость данных должна обеспечиваться прежде всего в интересах субъекта.

Право на забвение

Право на забвение/ право на удаление данных (Right to be forgotten/ Right to erasure) заключается в том, что субъект персональных данных обладает правом на удаление своих данных, собранных и обрабатываемых оператором данных. В международно-правовой доктрине данное право считается правом нового поколения информационных прав в сфере персональных данных. Выделение права на удаление данных – это ответная тенденция на скорость появления и распространения информации в современном информационном обществе. Можно видеть, что классические международные документы по регулированию прав субъектов персональных данных не выделяли право на забвение отдельно. Традиционное управление своими персональными данными после их сбора для обработки для конкретной цели подразумевало возможность запроса удаления персональных данных, однако только под некоторыми условиями, такими как неправомерность сбора и обработки данных.

Конвенция Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г. предусматривала в числе дополнительных гарантий субъекту персональных данных обеспечение субъектам персональных данных «возможность добиваться в случае необходимости исправления или уничтожения таких данных, если они подвергались обработке в нарушение норм внутреннего законодательства, воплощающего основополагающие принципы конвенции» (п. c, ст.8). В мае 2018 г. был принят Протокол (CETS No. 223), предусматривающий поправки к Конвенции. В модернизированной версии документа положение по уничтожению данных представляется уже на новом уровне. Теперь право на забвение помещено в число прав субъектов персональных данных: «запрашивать выполнение бесплатно и без промедлений исправления или удаления его данных, если его данные обрабатываются или были обработаны в нарушение положений настоящей Конвенции» (п. e ст. G).

Уведомление о нарушении данных

Согласно определению GDPR (ст. 4), нарушение данных (Data breach) – это нарушение безопасности, приводящее к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к персональным данным, переданным, сохраненным или обработанным иным образом. В рамках существующей нормативно-правовой базы требования об уведомлении значительно различаются в разных странах ОЭСР: они могут быть отраслевыми (например, в США необходимо направить уведомление в случае нарушений медицинской информации, информации финансовых учреждений и др.), обязательными (Германия, Великобритания, Канада) или добровольными (Новая Зеландия, Сингапур, Гонконг, Швейцария) и могут зависеть от типа и размера инцидента цифровой безопасности или типа затронутых данных.

В некоторых юрисдикциях действуют требования к контролерам об уведомлении субъектов данных и/или компетентных органов о нарушении персональных данных. Правило об обязательном уведомлении о нарушении данных применяется в странах, в которых действует GDPR, в 5 странах, в которых не действует GDPR, а также в 16 штатах США. При этом данное требование может быть установлено как на национальном уровне, так и на местном уровне (например, в США), и применяться в разных секторах.

Так, в ЕС требование об обязательном уведомлении о нарушении персональных данных применятся в соответствии с GDPR и распространяется на государственный и частный секторы. Так, согласно ст. 33 GDPR, в случае нарушения персональных данных, контролер обязан уведомить компетентный орган в течение 72 часов после того, как ему стало известно о нарушении. В США в 14 штатах требование об уведомлении о

нарушении персональных данных распространяется на все сектора. В 2 штатах США существуют исключения и специальные требования для определенных секторов, таких как сектор здравоохранения и банковский сектор, которые должны соответствовать Закону о мобильности и подотчётности медицинского страхования 1996 г. и Закону о финансовой модернизации 1999 г., соответственно.

Обязательность уведомления о нарушении персональных данных обуславливается тем, что сообщения о случаях нарушения безопасности данных негативно влияют на репутацию контролеров, и последние могут быть не заинтересованы в уведомлении субъектов о нарушениях безопасности данных. В отчете ОЭСР «Рамочная концепция защиты персональных данных» отмечается, что требование об уведомлении компетентных органов о каждом нарушении безопасности данных может привести к чрезмерной нагрузке контролеров и компетентных органов. Кроме того, постоянные уведомления могут понизить внимательность и заинтересованность субъектов данных к таким сообщениям.

Подходы к доступу и контролю данных

ОЭСР выделяет три наиболее распространённых подхода к доступу и обмену данными: открытые данные, рынки данных и переносимость данных. Открытые данные представляют собой наиболее ярко выраженный подход к повышению доступности данных. Режим открытых данных применяется в первую очередь государственным сектором (например, data.gov, data.gov.uk, data.gov.fr, data.go.jp) и НКО. Согласно отчёту ОЭСР, открытые данные могут быть определены как «данные, которые могут быть получены и использованы повторно без технических или правовых ограничений».

ОЭСР разработан ряд инструментов, содержащих руководство и лучшие практики по таким вопросам, как открытость данных, прозрачность, вовлечение заинтересованных сторон, права на интеллектуальную собственность и ценообразование в отношении данных. Так, в отношении режима открытых исследовательских данных ОЭСР в 2006 году разработаны Принципы и руководство по доступу к исследовательским данным из государственного финансирования, содержащие рекомендации по государственной политике в сфере науки, а также рекомендации для органов, осуществляющих финансирование исследований, по обеспечению доступа к исследовательским данным. В отношении информации государственного сектора ОЭСР в 2008 году разработана Рекомендация по улучшению доступа и более эффективному использованию данных государственного сектора. В 2009 году ОЭСР разработала Руководство по человеческим био-банкам и базам данных генетических исследований. Данным Руководством установлены, среди прочего, принципы и лучшие практики по предоставлению доступа к

материалам, хранящимся в человеческих биологических банках и к базам данных о генетических исследованиях (human biobanks and genetic research databases, HBGRD). В 2014 году ОЭСР разработала Рекомендацию по стратегиям цифрового правительства, устанавливающую набор требований к принимаемым государствами стратегиям, которые в долгосрочной перспективе призваны обеспечить переход к цифровому правительству. Также, в 2016 году ОЭСР принята Рекомендация по управлению данными в сфере здравоохранения. Целью Рекомендации также является усиление гармонизации между системами управления данными в сфере здравоохранения разных стран для того, чтобы больше стран могли извлечь пользу из статистического и исследовательского использования данных для общественного блага, а также участвовать в межгосударственных статистических и исследовательских проектах, обеспечивая при этом защиту тайны частной жизни и безопасность данных.

Перечисленные выше Рекомендации содержат ряд инструментов для обеспечения режима открытости данных. В отношении открытости данных ОЭСР выделяет следующие инструменты:

1) Нормативное установление презумпции открытости данных и механизмов её реализации

Данный инструмент предполагает максимизацию доступности данных государственного сектора для их использования и повторного использования на основе презумпции открытости как базового правила для обеспечения доступности и повторного использования. Также, открытость предполагает определение оснований для отказа или ограничения в доступе к таким данным (в исключительных целях – таких, как интересы национальной безопасности, неприкосновенности личной жизни, защита частных интересов, например, если может быть нарушено авторское право). Рекомендациями ОЭСР по улучшению доступа и более эффективному использованию данных государственного сектора предусмотрено установление принципов режима открытого доступа или презумпции открытости в качестве базового правила открытых данных.

2) Нормативное установление стандартов и критериев доступности и прозрачных условий для повторного использования данных

ОЭСР рекомендует поощрять недискриминационный, развитый доступ и условия для повторного использования информации государственного сектора, не допускать предоставления эксклюзивного доступа и устранять избыточные ограничения на способы доступа к информации, а также её использования, повторного использования сбора и распространения. ОЭСР устанавливает следующие критерии доступности данных:

- Возможность получения доступа к данным в дезагрегированной форме и в электронном виде при условии признания права на доступ к данным в электронном виде.
- Доступность данных в удобной и модифицируемой форме.
- Обеспечение поисковой доступности данных – например, посредством создания государственных и общественных каталогов данных, реестров информационных активов. В качестве технических инструментов обнаружения и повторного использования данных могут выступать, например, метаданные и инструменты семантической разметки данных – такие, как микроформаты.

Механизмы контроля доступа к данным

В 1992 г. ОЭСР приняла Руководство по безопасности информационных систем. Данное Руководство было заменено в 2002 и в 2015, в настоящее время действует Рекомендация по управлению рисками цифровой безопасности для экономического и социального благополучия, с 2019 г. её дополняет Рекомендация по цифровой безопасности критических видов деятельности. Для целей данных документов «риск цифровой безопасности» определен как категория риска, связанная с использованием, развитием и управлением цифровой средой в рамках любой деятельности. Этот риск может возникнуть в результате сочетания угроз и уязвимостей в цифровой среде и может помешать достижению экономических и социальных целей, нарушая конфиденциальность, целостность и доступность осуществления тех или иных видов деятельности и среды для их осуществления. Риск цифровой безопасности по своей природе динамичен, он включает аспекты, связанные с цифровой и физической средой, людьми, участвующими в деятельности, и поддерживающими ее организационными процессами.

Основные принципы управления цифровыми рисками включают:

1. Осведомленность, навыки и расширение возможностей. Все заинтересованные стороны (органы власти, государственные и частные организации, частные лица, которые прямо или косвенно полагаются на использование цифровой среды при осуществлении экономической и социальной деятельности) должны понимать риски цифровой безопасности и способы управления ими.

2. Ответственность. Все заинтересованные стороны должны нести ответственность за управление рисками цифровой безопасности.

3. Права человека и основные ценности. Управление рисками цифровой безопасности должно осуществляться в соответствии с такими ценностями, как, например, свобода выражения мнений, свободна движения информации,

конфиденциальность информации, тайна переписки, защита персональных данных, открытость и непредвзятость.

4. Сотрудничество. Все заинтересованные стороны должны осуществлять сотрудничество между собой, в том числе на международном уровне, в области управления рисками цифровой безопасности.

5. Цикличность оценки рисков и принятия мер. Руководители и лица, принимающие решения, должны обеспечивать принятие мер по управлению рисками цифровой безопасности на основе постоянной оценки рисков.

6. Меры безопасности. Руководители и лица, принимающие решения, должны обеспечивать принятие мер безопасности, адекватных рискам и соизмеримых с ними. Выбор, внедрение и улучшение мер безопасности должны основываться на оценке рисков и быть направлены на их снижение до приемлемого уровня.

7. Инновации. Руководители и лица, ответственные за принятие решений, должны учитывать необходимость внедрения инноваций как неотъемлемой части мер по снижению рисков цифровой безопасности.

8. Готовность и непрерывность деятельности. Необходимо планирование мер по профилактике и снижению негативных последствий инцидентов в сфере безопасности и по обеспечению бесперебойности осуществления защищаемой деятельности.

3 Анализ подходов государств-членов ОЭСР и партнеров Организации к регулированию персональных данных

Регулирование обезличенных данных в странах ОЭСР и партнерах Организации

Персональные данные, утратившие свойства идентифицируемости, выходят из-под правового регулирования персональных данных. Поэтому обезличенные данные не являются персональными данными. Соответственно, работа с обезличенными данными не подлежит соблюдению требований по защите персональных данных. Однако такая схема разграничения сферы регулирования действительна, если под идентифицируемостью мы пониманием наличие в персональных данных идентификаторов. При таком подходе обезличенными данными будут считаться и анонимизированные, и псевдонимизированные, т.е. восстановимые данные. Учитывая проблему незащищённости обезличенных персональных данных в случае их восстановления, законодатели вносят уточнения о распространении режима защиты персональных данных на такие случаи.

Значение обезличивания на примере медицинских персональных данных. Сбор персональных данных может быть необходим даже не ради дальнейшей работы с

конкретным физическим лицом, а для работы с содержанием данных. Это случай сбора медицинских показателей для проведения оценки системы здравоохранения, состояния здоровья населения, контроля за распространением заболеваний и др. Персональные медицинские сведения могут включать диагнозы пациентов, результаты анализов, выписываемые рецепты, медицинские истории, назначаемые виды лечения и др.

Распространённая во многих странах ОЭСР система сбора медицинских данных основана на использовании электронных медицинских карт (electronic health record, EHR). Медицинские карты не только собирают полные данные о пациенте и его медицинской истории, но также включают электронные медицинские записи (electronic medical records, EMR). Однако не все государства предполагают вторичное использование данных медицинских карт для целей анализа состояния здравоохранения или состояния здоровья населения. На 2016 г. готовность к введению национальных баз медицинских данных выражали Польша, Исландия, Новая Зеландия, США, Великобритания (Англия и Шотландия, Скандинавские страны, тогда как Австрия, Франция, Греция, Япония, Мексика и Швейцария выражали сомнение относительно такой возможности. Одна из причин отказа некоторых стран от идеи широкого использования данных медицинских карт – это недостаточная техническая проработанность систем HER.

Во Франции действует Национальная Комиссия по информации и свободам (Commission Nationale de l'Informatique et des Libertés, CNIL), которая определяет порядок работы публичных институтов с персональными данными. В Великобритании передача данных Канала исследовательских данных клинической практики (Clinical Practice Research Datalink, CPRD) подлежит одобрению Независимого научного консультационного комитета (Independent Scientific Advisory Committee, ISAC). В то же время в некоторых странах принята концепция «открытой публичной базы данных» (open government data) в отношении медицинских данных. Например, в США действуют платформы HealthData.gov и Национальный центр статистики о здоровье (National Center for Health Statistics, https://www.cdc.gov/nchs/), в австралийском штате Квинсленд Queensland Health (https://www.health.qld.gov.au/).

Регулирование получения согласия в странах ОЭСР и партнерах Организации

Европейский союз. В преамбуле Регламента ЕС о персональных данных 2016 г. (п.32) устанавливается, что согласие должно быть выраженно свободно (freely given), быть информированным (informed), конкретным (specific) в значении целенаправленности его предоставления, и должно прямо демонстрировать намерение в утвердительной форме (unambiguous indication).

Согласие должно быть выражено свободно. Свободно выраженное согласие значит, что субъект персональных данных не вынуждается к даче согласия внешними условиями, а принимает самостоятельное решение о распоряжении своими персональными данными.

Согласие должно быть информированным. Это значит, что субъект персональных данных знает, кто является контролёром данных, какие действия будут осуществляться с его данными, какова цель обработки данных, также субъект данных должен быть осведомлён о своей возможности отзыва данного согласия и каким образом осуществить отзыв. Информированность предполагает понимание субъектом персональных данных на что он даёт своё согласие.

Согласие должно быть конкретным. Это значит, что согласие даётся на обработку данных для конкретной цели. Если сбор данных осуществляется для нескольких целей, согласие должно быть получено для каждой из этих целей, причём должно соблюдаться право дать согласие на конкретную цель, не давая согласия на другие цели.

Согласие должно быть в утвердительной форме. Это значит, что согласие не должно быть двусмысленным, вызывать сомнения относительно наличия согласия на обработку данных в выраженной воле субъекта персональных данных.

Относительно минимального возраста для дачи согласия на обработку данных, Регламент ЕС устанавливает планку 16 лет (п.1 ст.8). Устанавливается, что это правило не должно противоречить общему договорному праву государств членов, утверждая тем самым право государств снижать планку, но не ниже 13 лет. Согласие должно быть ясным и утвердительным, и может предоставляться в устной или письменной, включая электронную, формах

США. В США отраслевое законодательство о персональных данных не использует понятие «согласия» субъекта на обработку персональных данных. Тем не менее, правовая конструкция волевого решения о предоставлении своих данных физическим лицом закрепляется понятием «разрешения» (authorization). Так, Законом о мобильности и подотчётности медицинского страхования 1996 г. (Health Insurance Portability and Accountability, HIPPA) устанавливается, что в целях защиты информации о здоровье использование и раскрытие собираемой информации может производиться только с письменного согласия лица, причём лицо всегда может отозвать своё согласие.

Южная Корея. В Южной Корее Закон о защите персональной информации специально не выделяет характеристики действительного согласия, но они выводятся из содержания отдельных положений. Согласие на обработку персональных данных рассматривается как одно из охраняемых прав субъекта персональных данных (ст.4). Форма выражения согласия Законом не оговаривается.

Индия. Законопроект Индии о защите персональных данных 2019 представляет конкретный перечень характеристик согласия, при выполнении которых оно признаётся действительным. Согласие должно быть свободным (в соответствии со стандартом свободной воли, установленном Закон Индии о договорах 1872 г.); информированным; конкретным, в смысле того, чтобы субъект данных мог определить объём своего согласия в части цели обработки данных; ясным, в смысле того, что согласие должно прямо указываться в утвердительной форме; согласие действительно, если может быть отменено с такой же лёгкостью, как было дано.

Регулирование порядка сбора и обработки данных в отсутствии согласия. Следует заметить, что каждый из выше рассмотренных подходов основан на том, что предполагается получение согласия самого субъекта персональных данных. Однако обработка данных в медицинских целях возможна и без согласия персональных данных в определённых законодательством случаях.

В Великобритании обработка персональных данных для исследований и статистики подпадает под исключения из общих правил о согласии (schedule 3 Закона о защите персональных данных 2018). При этом предусматривается, чтобы у субъектов персональных данных была возможность возразить против использования их данных для этих целей или отозвать их согласие на обработку данных в принципе.

В других странах принято более строгое регулирование или есть национальные специфические ограничения. В Израиле идентифицируемые персональные данные считаются конфиденциальными и не могут передаваться третьим лицам. Предусматривается два исключения: 1) если субъект дал своё согласие на обработку своих персональных данных; это правило применимо и для тяжело больных, поэтому дополнительно устанавливается право дачи согласия на обработку персональных данных больного для членов его семьи; 2) если есть законодательно установленное обязательство о передаче информации. Например, государство в праве обращаться в медицинские учреждения для получения медицинских данных независимо от согласия субъекта данных.

Регулирование статуса обработчика и контролера данных в странах ОЭСР и партнерах Организации

GDPR также выделяет такую категорию лиц, как «joint controllers» - совместные контролеры или со-контролеры. В отношении любого процесса обработки, более чем один объект может быть контролером (исходя из того, что более чем один объект может принимать решения о целях, для которых и посредством которых эти данные обрабатываются). Ст. 26 GDPR признают совместных контролеров как двух или более

контролеров, совместно определяющих цели и средства обработки. Совместные контролеры должны посредством «договоренности» между ними распределить обязанности по соблюдению защиты данных (например, должно быть согласовано, какой контролер должен отвечать за предоставление четкой информации субъекту данных). Краткое изложение соглашения должно быть доступно субъекту данных. Кроме того, в соглашении должно быть установлено кто из контролеров является «контактным центром» для обращения субъектов данных.

С 1 января 2020 г. В Калифорнии вступил в силу Закон Калифорнии о защите персональных данных потребителей (CCPA). Предполагается, что CCPA является аналогом GDPR. CCPA не содержит терминов «контролер» и «обработчик», но вводит аналогичные по содержанию термины «бизнес» (или «предприятие») и «поставщик услуг». В Сингапуре действует аналогичное GDPR законодательство о защите персональных данных – Personal Data Protection Act (PDPA) 2012. Однако вместо понятий «контролер» и «обработчик» PDPA использует понятие «организация» и «посредник данных» («data intermediary») соответственно.

Регулирование статуса посредника данных в странах ОЭСР и партнерах Организации

В странах ОЭСР доверенная третья сторона выступает своего рода гарантом обеспечения безопасности предоставленных данных, механизмом подтверждения надежности конечного пользователя данных. При этом под надежностью конечного пользователя следует подразумевать соблюдение принципов защиты персональных данных при их использовании и обработке.

Например, в США в настоящее время рынок посредников данных строго не регламентирован. Однако предпринимались попытки регулирования деятельности брокера данных. В 2014 г. США был предложен Законопроект об ответственности и прозрачности брокера данных (в 2017 г. передан на рассмотрение комитетам), который направлен на ограничение деятельности посредников персональных данных. В 2018 г. в штате Вермонт был принят Закон о регулировании брокеров данных. В 2019 г. в Сенате США был предложен Законопроект о списке брокеров данных (Data Broker List Act of 2019), устанавливающий требование к брокерам данных о регистрации в национальном реестре, контролируемым Федеральной торговой комиссией (FTC), а также об обеспечении защиты персональных данных. Создание национального реестра предоставит субъектам данных бóльшую степень контроля над личной информацией.

Регулирование переносимости данных в странах ОЭСР и партнерах Организации

Национальные подходы к обеспечению переносимости данных. Правовое регулирование переносимости данных – это нововведение Регламента ЕС 2016 г. о защите персональных данных. Поэтому в более раннем законодательстве стран, не входящих в ЕС, понятие переносимости данных не встречается. В соответствии со ст.20 Регламента право на переносимость данных определяется как право субъекта «получить относящиеся к нему персональные данные, которые он предоставил контролеру, в структурированном, универсальном и машиночитаемом формате и передать их другому контролеру беспрепятственно со стороны контролера, которому были предоставлены персональные данные». Переносимость данных возможна при соблюдении двух условий (пп. a,b п.1 ст.20). Во-первых, можно запрашивать перенос только тех данных, обработка которых основывается на согласии субъекта. Следовательно, право на переносимость данных не распространяется на данные, собранные и обработанные в рамках исключений из правила об обязательном получении согласия субъекта. Во-вторых, данные подлежат переносу, только если их обработка осуществляется при помощи автоматизированных средств.

Положения Регламент ЕС о переносимости включают уточнение, что «право на переносимость не должно применяться для обработки, необходимой для выполнения задачи, осуществляемой в рамках общественного интереса или при исполнении официальных полномочий, возложенных на контролёра» (п.3 ст.20). Данное положение направлено на защиту интересов контролёров данных: контролёры не должны обременяться дополнительными обязательствами, помимо тех, которые следуют из права субъекта персональных данных свободно распоряжаться своими данными.

В США переносимость данных не закрепляется в федеральном законодательстве о персональных данных, однако есть практика на уровне штатов. С 2020 г. вступил в силу Закон штата Калифорния о неприкосновенности частной жизни потребителя (California Consumer Privacy Act 2018, CCPA). Право на переносимость данных по сравнению с аналогичными положениями Регламента ЕС отличается дополнительными гарантиями по управлению персональными данными, переданными оператору в части коммерческого использования данных.

В Канаде право на переносимость данных закрепляется в числе 10 принципов Цифровой Хартии в форме принципа транспарентности, переносимости и системной совместимости. В Бразилии право на переносимость данных закрепляется в ст.18 Закона об обеспечении неприкосновенности частной жизни в числе прав субъекта персональных данных, которые могут быть осуществлены посредством запроса к контролёру данных. В Таиланде с 27 мая 2020 г. вступает в силу Закон о защите персональных данных,

основанный на положениях Регламента ЕС и предусматривающий право на переносимость данных. Закон был принят в 2019 г. с введением 1-летнего переходного периода для того, чтобы контролёры и обработчики данных смогли подготовиться к выполнению новых обязательств.

Регулирование права на забвение в странах ОЭСР и партнерах Организации

Право на забвение было изначально сформировано судебной практикой и впоследствии закреплено на основе базовых судебных положений с учётом экспертных комментариев. Так, включение права на забвение в Регламент ЕС о защите персональных данных стало результатом разрешения Европейским Судом дела испанского гражданина Марио Костеха против компании Google. Основываясь на положениях Директивы 95/46ЕС и главы 8 Хартии Европейского союза по правам человека, Суд признал обязательство Google удалить указанные ссылки на домене Google.es.

Рабочая группа по защите данных разработала Руководство по имплементации судебного решения Суда ЕС, в котором разъясняются детали осуществления права на забвение. Рабочая группа составила перечень критериев, на которые могут опираться компетентные органы для проверки соблюдения режима защиты персональных данных.

1) Относится ли поисковый результат к конкретному физическому лицу.

2) Является ли субъект персональных данных публичным лицом/ играет ли роль в публичной жизни.

3) Является ли субъект персональных данных несовершеннолетним.

4) Являются ли данные точными.

5) Является ли информация актуальной и имеет ли информация значение для публичного интереса в доступе к этой информации.

6) Является ли информация чувствительной по смыслу действующего законодательства.

7) Хранится ли информация дольше необходимого для достижений цели обработки.

8) Причиняет ли обработка данных вред субъекту этих данных.

9) Ведёт ли результат поиска к информации, которая подвергает субъекта персональных данных какому-либо риску.

10) В каком контексте была опубликована информация.

11) Были ли оригинальные сведения опубликованы для целей журналистской профессиональной деятельности.

12) Имеет ли сайт размещения информации юридическое полномочие или обязательство делать персональные данные публично доступными.

13) Касаются ли персональные данные деяния, преследуемого в уголовном порядке.

Законодательное регулирование ЕС. Право на забвение закрепляется в Регламенте ЕС о защите персональных данных. В соответствии со ст.17 субъект данных имеет право запрашивать незамедлительное удаление его данных у контролёра данных, и контролёр должен незамедлительно выполнить обязательство по удалению, если для этого есть одно из прямо установленных оснований.

Регламент ЕС предусматривает обязательство контролёра, получившего запрос на удаление данных по одному из оснований, оповещать об удалении данных другие организации в двух случаях. Во-первых, предупреждение обязательно, если персональные данные были раскрыты третьим лицам. Во-вторых, предупреждение требуется, если данные были опубликованы в интернет-среде (например, в социальных сетях, на сайтах, форумах). В п.66 преамбулы устанавливается, что контролёр данных должен проинформировать иных контролёров-реципиентов данных о полученном запросе на удаление ссылок, копий или точных повторений персональных данных.

Индия. Право на забвение предлагается к закреплению в законопроекте о защите персональных данных 2019 г. Примечательно, что право на забвение (ст.20) перечисляется наравне с правом на внесение исправлений и удаление данных (ст.18), тогда как в Регламенте ЕС прямо указывается взаимозаменяемость терминов «право на удаление» и «право на забвение». В Индии между этими видами прав субъекта персональных данных проводится содержательная разница. Право на внесение исправлений и удаление используется для улучшения качества персональных данных или оптимизации распоряжения данными (удаление данных после достижения цели).

США. В федеральном законодательстве США нет нормативного закрепления права на удаление данных. Однако право на удаление данных ребёнка получило законодательное закрепление в 2015 г. в Законе штата Калифорния о защите неприкосновенности частной жизни ребёнка в Интернете. Также право на забвение было включено в Закон о неприкосновенности частной жизни потребителя 2018 г. (California Consumer Privacy Act, CCPA).

Южная Корея. В Южной Корее законодательство о персональных данных прямо не устанавливает право на забвение, однако осуществление этого права частично регламентируется Корейской Комиссией коммуникаций в сфере интернета. В 2016 г. Комиссия выпустила Руководство по праву на ограничение доступа по запросу в отношении индивидуальных интернет-публикаций.

Сингапур. В Сингапуре нет прямого законодательного закрепления права на забвения. Однако сингапурские правоведы рассматривают вопрос о том, что право на забвение уже присутствует в национальном законодательстве в форме обязательства об ограничении хранения данных (retention limitation obligation).

Регулирование уведомления о нарушениях в отношении данных в странах ОЭСР и партнерах Организации

В странах, предъявляющих требование к контролерам данных об уведомлении нарушения персональных данных, устанавливается ответственность за несоблюдение данного требования. Например, п.4 ст.83 GDPR, за нарушение требования об уведомлении налагается административные штрафы в размере до 10 млн евро или до 2% от общего годового оборота за предыдущий финансовый год, в зависимости от того, что выше.

В Австралии несоблюдение требования об уведомлении нарушения персональных медицинских данных влечет штраф размером 2100 долл. США.

В Индии в настоящее время штраф за несоблюдение правил об уведомлении о нарушении персональных данных составляет не более 1300 долл. США, однако законодатели планируют увеличить сумму штрафа с принятием нового Закона о защите персональных данных.

В некоторых странах ведется отчетность о фактах нарушения персональных данных. ОЭСР считает, что наличие базы данных, консолидирующей все зарегистрированные в стране уведомления о нарушении персональных данных, позволит осуществлять внутренний мониторинг, анализ таких нарушений и проводить расследования. Такие централизованные базы данных есть в 28 странах, участвующих в опросе, и в 9 штатах США.

Подходы к доступу и контролю данных в странах ОЭСР и партнерах Организации

В США Административно-бюджетным управлением в 2009 году принята Директива открытого правительства, базовыми принципами которой являются принципы прозрачности, участия и сотрудничества. ОЭСР отмечает, что на основании данной директивы были приняты ведомственные планы (Open Government Plan) и составлялись руководства, в том числе по реализации презумпции открытости. Департаментом юстиции США разработано, постоянно обновляется и дополняется подробное Руководство по применению режима открытых данных.

В Великобритании Закон о свободе информации был принят в 2000 году. Законом, в частности, регулируются отношения по раскрытию сведений государственного сектора по запросу, основания для отказа в таком раскрытии, обязанности органов власти по

разработке схем публикации сведений и по самой такой публикации. Правительством и органами власти Великобритании приняты стратегии по открытости данных.

В ряде стран ОЭСР (Дания, Франция, Германия, Корея, Великобритания) данные государственного сектора распространяются по открытой лицензии, то есть, хотя данные признаются объектами интеллектуальной собственности, они доступны неопределённому кругу лиц по договору простой лицензии.

В качестве лучших практик управления данными в госсекторе ОЭСР выделены следующие инициативы: наличие портала отрытого правительства (Австрия), наличие плана действий, стратегии по обеспечению открытости власти (Канада), создание единой электронной системы доступа к государственным услугам (Италия, Словения), создание платформы для сотрудничества и обсуждения действий, результатов деятельности органов власти с заинтересованными сторонами (Колумбия), специальный портал по законодательству (Польша).

Кроме того, в 2011 г. была создана международная инициатива по открытому правительству – Партнерство для открытого правительства. В 2019 году 49 из 78 присоединившихся государств совместно создают планы действий по созданию открытого правительства. Также, Партнерством разработан Инструментарий, содержащий лучшие практики по созданию открытого правительства.

Регулирование механизмов контроля доступа к данным в странах ОЭСР и партнерах Организации

1 мая 2018 года правительство Австралии обязалось реформировать свою национальную структуру управления данными путем разработки нового законодательства о хранении и извлечении данных. Управление национального уполномоченного по данным (NDC) обеспечивает надзор и регулирование новой системы обмена и публикации данных, включая мониторинг и отчетность о работе системы и обеспечении соблюдения сопутствующего законодательства. Также действует Партнерство по интеграции данных для Австралии (DIPA), скоординированная инициатива в рамках всей государственной службы Австралии, направленная на максимальное использование и ценность огромных государственных данных, позволяющая рентабельно и своевременно анализировать уже имеющиеся данные, обеспечивая при этом безопасное использование данных в безопасных и контролируемых средах.

В апреле 2018 года правительство Дании создало Экспертную группу по этике данных с целью разработки рекомендаций по обеспечению доверия граждан к цифровой экономике. В экспертную группу вошли высокопоставленные представители крупных, средних и малых компаний. Его цель состояла в том, чтобы разработать рекомендации,

которые защитят доверие потребителей, не создавая ненужного бремени для компаний и не подавляя инновации. Правительство Дании также сотрудничает с отраслевыми органами, чтобы изучить возможность создания «национального знака» цифровой безопасности и ответственного использования данных, которая повысит прозрачность и упростит для потребителей выбор компаний, продуктов и решений, соответствующих требованиям. определенные стандарты безопасности данных и этики. В более долгосрочной перспективе эти инициативы можно вывести на международный уровень, поскольку большинство проблем, связанных с данными, по своей природе являются международными.

4 Формирование предложений для развития регулирования персональных данных в России на основе лучших международных практик

Предложения по совершенствованию подходов к определению понятия персональных данных, а также к статусу и режиму их обезличивания

Ввиду стремительного развития цифровой экономики и технологий, основанных на работе с данными необходимо пересмотреть базовое регулирование персональных данных, начиная с определения объёма понятия персональных данных в ФЗ «О персональных данных».

1) В соответствии с действующим законодательством, персональные данные определяются как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Для обеспечения ясности содержания понятия, следует ввести понятие «идентификатора» в терминологию российского права и дополнить законодательное определение перечислением примеров идентификаторов, делающих информацию относимой к определенному или определяемому лицу. Например, могут быть названы имя, номер удостоверения личности (паспорта, служебного удостоверения, иного удостоверяющего личность документа); изображение; контактные данные; сведения о местоположении; цифровые идентификаторы, как IP-адрес; описание признаков, характерные для физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности указанного физического лица; индивидуальная информация как коды, подписи, голосовые записи.

2) Необходимо ввести в определение разграничение уровней идентифицируемости данных, в соответствии с международными стандартами. Например, в соответствии со стандартом ISO/IEC 19944:2017 персональные данные могут быть разграничены на основе применяемых методов обработки персональных данных на 5 категорий: 1)

идентифицированные данные; 2) псевдонимизированные данные; 3) несвязанные псевдонимизированные данные; 4) анонимизированные данные; 5) агрегированные данные.

3) Необходимо внести ясность в квалификацию персональных данных как объект гражданских прав. Необходимо указать, что персональные данные, как информация, которая может быть объектом публичных, гражданских и иных правоотношений, могут признаваться оборотоспособными в той степени, насколько это не противоречит правовому режиму их защиты. Таким образом, российской законодатель может подготовить правовую основу для регулирования деятельности информационных посредников в развивающейся цифровой экономике.

Регулирование обезличивания данных в России. ФЗ-152 «О персональных данных» не устанавливает статус обезличенных данных как таковых, а указывает только на процесс обезличивания, в результате которого данные утрачивают высокую степень идентифицируемости.

В соответствии со п.9 ст.3 первой редакции от 27.07.2006 процесс обезличивания данных определялся как «действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных». При формулировании данного определения законодатель полагался на представление о процессе обезличивания как о процессе безвозвратного удаления идентификаторов. Такая формулировка не вызывала правовых вопросов поскольку была обусловлена сугубо техническими факторами. Законодатель не предполагал возможности ре-идентификации данных. Исходя из представления о надёжности процесса обезличивания законодатель не предусматривал необходимости обеспечения конфиденциальности обезличенных персональных данных, Поэтому в первоначальной редакции 2006 г. ФЗ содержал п. 2 ст. 7, которым устанавливалось, что обеспечения конфиденциальности персональных данных не требуется в случае обезличивания персональных данных и в отношении общедоступных персональных данных.Однако совершенствование технологий и отдельные прецеденты в международной практике доказали, что обезличенные данные могут быть восстановлены.

В условиях современных информационных технологий, данные каждого пользователя сети Интернет потенциально или непосредственно размещены в открытом доступе и могут служить дополнительной информацией для восстановления данных. Однако новое определение оставляет неопределённость в отношении того, можно ли считать обезличенные данные по-прежнему персональными ввиду потенциальной возможности восстановления удалённых идентификаторов; или, если их режим

меняется, то каким образом. Задача может быть разрешена путём разграничения персональных данных по уровню обезличивания, поскольку на основе этого разграничения может проведено установление правил вовлечения данных в оборот.

С этой целью 18 сентября 2019 г. Министерство цифрового развития, связи и массовых коммуникаций РФ представило поправки в ФЗ «О персональных данных». Предлагается дополнить закон новыми понятиями «обезличенные персональные данные» и «обезличенные данные». Тем самым Министерство намерено развести порядок и условия обработки этих двух категорий данных. В соответствии с проектом поправок в закон: «9.1) обезличенные персональные данные – информация, которая в результате обезличивания персональных данных не позволяет без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных». Данное определение указывает на то, что данные претерпели изменения таким образом, что степень их идентифицируемости перешла из уровня «прямой» в уровень «потенциальной». Следовательно, можно предположить, что возможен переход и к нулевому уровню идентифицируемости. В связи с этим предлагается выделить категорию «обезличенных данных».

В феврале 2020 г. Минкомсвязи внёс очередной законопроект о регулировании больших данных. Предлагается внести поправки в ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»: добавить определения понятий «большие данные», «оператор больших данных», «обработка больших данных», добавить положения о регулировании обработки больших данных, контролю и надзору за обработкой и оборотом больших данных. Положения законопроекта уже получили ряд критических замечаний от юристов и компаний, которых непосредственно затрагивают предложенные поправки. Эксперты обращают внимание на нецелесообразность попытки дать законодательное определение «большим данным», поскольку там этот термин является образным понятием, а не конкретным техническим термином. Неудачным представляется и определение оператора больших данных, которое сформулировано настолько широко, что под него подпадает любое лицо, каким-либо образом причастное к обработке любой информации. Считается, что законопроект может противоречить задачам Национальной стратегии развития искусственного интеллекта на период до 2030 г., поскольку будет создавать избыточное регулирование, которое станет сдерживающим фактором в развитии технологий. Ни в одной из стран ОЭСР не принято специальное регулирование Больших данных.

Основная проблема законопроекта, предусматривающего разграничение обезличенных персональных данных и обезличенных данных, заключается в

практическом аспекте такого разграничения. Не предусматривается, каковы критерии определения того, что процесс обезличивания обеспечил нужный уровень идентифицируемости данных, для того чтобы их относить к той или иной категории. Как вариант, возможно разграничить данные по методам их обезличивания. С переходом к разграничению на обезличенные персональные и обезличенные данные Роскомнадзору следует выделить для сопоставления свойство «восстановимости». В условиях постоянного технического развития Роскомнадзору следует расширить обзор возможных методов обезличивания, а также сформулировать критерии, по которым определяется свойство обезличенных данных для тех методов, которые не учтены в обзоре.

Предложения по совершенствованию подходов к получению согласия

В России согласие субъекта регламентируется в ст.9 ФЗ «О персональных данных». Устанавливается, что субъект данных даёт своё согласие «свободно, своей волей и в своём интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным». При этом в тексте закона не указывается, что согласие должно быть «ясным», «прямым», и с этой точки зрения, нормы российского законодательство устанавливают стандарт согласия субъекта ниже, чем Регламент ЕС.

Хотя согласно п.1 ст.9 согласие на обработку ПД может быть дано в любой позволяющей подтвердить факт его получения форме, в законе оговаривается, что в законодательно установленных случаях становится обязательной письменная форма согласия на обработку персональных данных, которая должна содержать собственноручную подпись субъекта, или электронную подпись в случае электронного документа (п.4 ст.9 ФЗ).

В отличие от большинства законов/ актов о персональных данных в российском законе нет прямого указания на возраст для правомерной дачи согласия на обработку персональных данных, что вызывает сомнения в кругах правоведов о порядке получения согласия несовершеннолетнего с 14 до 18 лет. Также российский законодатель не устанавливает правил о порядке отзыва согласия, помимо закрепления самого права на отзыв (п.2 ст.9). Это значит, что российский субъект персональных данных не пользуется гарантией столь же простой процедуры отзыва, как процедуры дачи согласия. Таким образом, можно видеть, что многие положения законодательства о защите персональных данных остаются неясными, и требуют уточняющих дополнений.

В России понятия «информированности» и «сознательности» различаются, тогда как в рамках европейского подхода информированность подразумевает под собой осознание полученной информации. В связи с этим рекомендуется дополнить п.1 ст.9

примечанием о том, что «конкретное согласие означает согласие субъекта на обработку для конкретной цели в степени или объёмах, определённых субъектом».

В российском законодательстве нет уточнения относительно ясности предоставляемого согласия, однако это является существенным фактом в случае спорной ситуации, так как этот критерий тесно взаимосвязан с критерием «информированности», «осознанности». Рекомендуется изменить формулировку «согласие может быть дано в любой позволяющей подтвердить факт его получения форме» на «согласие в утвердительной форме» (п.1 ст.9). Также следует дополнить п.4 ст.9 уточнением о том, что «согласие предоставляется после получения всей необходимой информации, изложенной в доступной для понимания, ясной форме».

Представляется малоэффективным положение о праве на отзыв своего согласия на обработку персональных данных, без указания условия его осуществления. Для этого следует включить в п.2 ст.9 уточнение о том, что «процедура отзыва данного согласия должна быть не более сложной, чем процедура предоставления согласия». Также следует указать точный возрастной порог для самостоятельного осуществления права дачи согласия субъектом персональных данных, поскольку это позволит избежать образования противоречивой судебной практики.

Следует отметить, что российское законодательство предусматривает значительное количество исключений из общих правил о получении согласия субъекта персональных данных по сравнению с другими странами. В связи с этим рекомендуется внести поправки в ФЗ «О персональных данных», а именно сократить число условий для обработки персональных данных путём замены пунктов 2, 3, 3.1, 4, 11 пунктом об обработке персональных данных для выполнения функций государства в публичных интересах. Также внести в п.7 дополнение об обработке персональных данных для правомерных целей исследований в сфере медицины и здравоохранения.

Предложения по развитию подходов к статусу оператора данных

В российском законодательстве о защите персональных данных есть только понятие «оператор» персональных данных. Практика стран склоняется к разделению категорий контролера и обработчика, разграничивая их права и обязанности, а также степень ответственности. Кроме того, к процессу определения целей обработки и контроля применяют отличные от процесса обработки данных принципы защиты данных. Поскольку лицо, определяющее цели обработки, и лицо, непосредственно осуществляющее обработку данных, чаще всего не являются одним и тем же лицом, представляется необходимым установить обязанности и ответственность каждого из них.

Представляется, что в российском законодательстве о персональных данных необходимо разграничить категорию лиц, осуществляющих контроль и обработку данных. Поскольку, как правило, контролирующее лицо нанимает другое лицо для осуществления обработки данных.

Предложения по развитию подходов к статусу посредника данных

С учетом передовой практики стран-членов ОЭСР и партнеров Организации в России представляется необходимым регламентировать деятельность посредников данных. В частности, посредники данных должны соблюдать принципы защиты персональных данных при обработке и передаче информации. Также предполагается, что реестр посредников данных обеспечит прозрачность деятельности компаний, обрабатывающих данные, а также расширит возможности субъектов данных в отношении контроля и управления персональными данными.

Предложения для России:

1) Минкомсвязи сформировать рекомендации для посредников данных, включающие требования о соблюдении принципов защиты персональных данных.

2) Внести изменения в ст. 3 ФЗ «О персональных данных», установив понятие «посредники данных»:

«12) Посредники данных – это лица, осуществляющие сбор, обработку и хранение персональных данных, с целью последующей передачи пользователям персональных данных, третьим лицам».

Предложения по развитию подходов к переносимости данных

Переносимость данных в России. ФЗ «О персональных данных» не предусматривает права на переносимость данных. С экономической точки зрения отсутствие переносимости персональных данных тормозит развитие цифровой экономики. Во-первых, в отсутствие возможности субъекта персональных данных свободно переносить свои данные высока вероятность образования информационной асимметрии между субъектами и поставщиками товаров и услуг. Во-вторых, при невозможности переноса данных субъекты несут большие затраты, сопряжённые со сменой поставщика или расширением круга поставщиков (switching costs). В-третьих, отсутствие переносимости данных приводит к низкой мотивации потребителей к предоставлению данных новым участникам рынка. Тем самым для новых компаний устанавливаются информационные барьеры входа на рынок.

Рекомендация для России. Переносимость данных может вводиться в российское право в два последовательных этапа: 1) законодательное закрепление права на

переносимость данных; 2) информационное сопровождение операторов данных и субъектов персональных данных об эффективной реализации нововведения.

Предложения по развитию регулирования права на забвение

Законодательное закрепление права на забвение в России отличается от положений Регламента ЕС по ряду параметров.

Во-первых, в России право на забвение затрагивает только операторов поисковых систем, а не всех операторов данных.

Во-вторых, закрепляется широкое действие такого основания для удаления данных, как незаконность обработки данных. В ст.10.3 устанавливается, что право действует в отношении «информации о заявителе, распространяемой с нарушением законодательства Российской Федерации». Следовательно, речь идёт о нарушении любых законов.

В-третьих, для осуществления права на забвение не предусматривается ограничений, которые бы обеспечивали законные интересы операторов поисковых систем и других операторов данных.

В-четвёртых, право ограничивается формальными признаками. Устанавливается, что требование заявителя должно содержать определённый набор сведений, включая паспортные данные, информацию ссылки на которую должны быть удалены, основание для прекращения выдачи ссылок. Такие требования представляются чрезмерными, поскольку они практически блокируют возможности осуществления права на забвение.

В-пятых, такой механизм осуществления права на забвение возлагает лишние обязательства на оператора данных. Устанавливается, что оператор вправе запрашивать уточняющую информацию в случае обнаружения неполноты сведений. Это значит, что оператор поисковой системы несёт лишнее бремя оценки полученного запроса.

Право на забвение следует сделать универсальным. Это значит, что сфера его действия не должна ограничиваться только ссылками в поисковых системах, но распространяться непосредственно на персональные данные в первоисточниках. Для этого необходимо закрепить право на забвение в ФЗ «О защите персональных данных» в виде отдельной статьи. Это позволит: 1) снять лишние обязательства с оператора данных по оценке достоверности информации; 2) снизить значение субъективной воли субъекта персональных данных для реализации права на забвение, что в свою очередь позволяет снизить число запросов; 3) обеспечить операторов данных ясными основаниями для определения наличия своего встречного обязательства по удалению указанных в запросе данных; 4) обеспечить операторам данных свободу принятия решения о порядке взаимодействия с субъектом персональных данных по вопросам реализации права на забвение.

Предложения по развитию подходов к уведомлениям о нарушениях в отношении данных

В России требование об уведомлении нарушения персональных данных законодательно не закреплено. Предполагается, что информирование о нарушениях безопасности данных уполномоченного органа и самого субъекта данных, повысит степень ответственности оператора данных за обеспечение соблюдения правил обработки данных.

Так, предлагается определить «инцидент» нарушения данных как несанкционированное предоставление и/или доступ, распространение персональных данных. Предполагается, что необходимо внести изменения в ФЗ «О персональных данных», определив в отношении какой информации следует применять требование к операторам об обязательном уведомлении в случае инцидента, связанным с обрабатываемыми данными.

Предложения по развитию подходов к доступу и контролю данных

1. Действующим федеральным законодательством не установлены критерии доступности и прозрачности условий для повторного использования данных, кроме машиночитаемости (размещения в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования). Как следствие, отсутствуют предусмотренные на уровне закона нормы, которым должен соответствовать режим открытости данных, в том числе данных государственного сектора в соответствии с ч.4 ст. 7 ФЗ «Об информации, информационных технологиях и о защите информации».

2. Данные государственного сектора в открытом доступе, несмотря на формальное выполнение правовых требований об обеспечении их доступности и машиночитаемости, не всегда пригодны для повторного использования.

Для решения указанных проблем предлагается внести в ФЗ «Об информации, информационных технологиях и о защите информации» дополнения в виде норм, устанавливающих стандарты и критерии доступности и прозрачных условий для повторного использования данных, такие, как соответствие открытых стандартов данных нуждам пользователя, гибкость данных, сохранение устойчивости издержек, совместимость стандартов с государственными ИС, интероперабельность, поддержка со стороны рынка и т.д., а также прозрачность процедур выбора открытых стандартов.

Проблема в сфере правового регулирования открытых данных в части перечней данных состоит в том, что такие перечни, несмотря на их открытость, ограничены и не учитывают одной из основных целей обеспечения государством открытого доступа к

данным государственного сектора: генерирования общественной стоимости данных. Как было указано выше, для обеспечения эффективного правового регулирования открытых данных необходима проактивность органов власти, то есть учёт текущих и будущих потребностей пользователей данных.

Для обеспечения такой проактивности в части создания перечней данных рекомендуется внести изменения в Перечень информации о деятельности госорганов и органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных, утвержденный Распоряжением Правительства РФ от 10.07.2013 № 1187-р, путем включения в него пункта о наборах данных, часто запрашиваемых пользователями данных. Критерий частоты запросов данных может устанавливаться Правительством РФ с учетом анализа запросов пользователей данных и выявления средних показателей частоты запросов за определённый период времени (например, за месяц или за год).

Кроме того, следует отметить проблему отсутствия в российском законодательстве норм, предусматривающих установление режима типовой открытой лицензии для распространения данных государственного сектора, создаёт неясность для пользователей в вопросе условий использования открытых данных. Рекомендуется внести в ч.4 ГК РФ, в ФЗ «Об информации, информационных технологиях и о защите информации» и в ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» изменения, устанавливающие режим предоставления пользователям данных простой лицензии в упрощенном порядке (открытой лицензии), а также условий такой лицензии для открытых данных государственного сектора.

В России ФЗ «О персональных данных» закреплены принципы доступа граждан к публичной информации (открытость, достоверность, свобода поиска и т.п.), права пользователя информацией (на получение/на отказ от получения информации, механизмы обжалования действий и возмещения вреда), организационные аспекты обеспечения доступа к информации.

Проблема современного регулирования открытости данных в российском законодательстве заключается в качестве процесса публикации таких данных в открытом доступе. Как отмечалось выше, на уровне федерального законодательства (а именно, в Федеральном законе «Об информации, информационных технологиях и о защите информации») установлено требование к машиночитаемости открытых данных. Также, данным ФЗ установлены принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, к которым относятся, среди прочего, открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации,

достоверность информации и своевременность ее предоставления и неприкосновенность частной жизни. Технические требования к открытым данным установлены также упомянутыми выше Методическими рекомендациями, утвержденными протоколом заседания Правительственной комиссии по координации деятельности Открытого Правительства от 29 мая 2014 г. № 4.

В российском законодательстве отсутствует ряд базовых критериев открытого правительства, которыми создавались бы правовые условия для обеспечения нахождения в открытом доступе качественных, целостных, доступных для обнаружения и понимания данных. К таким критериям относятся создание условий для обнаружения таких данных, обеспечение интероперабельности и безопасности данных. Отсутствие таких критериев открытости правительства на уровне норм-принципов влечет за собой отсутствие внедрения указанных критериев в российскую правовую систему, результатом чего является низкое качество данных, недостаточная осведомлённость потенциальных пользователей о возможности получения таких данных и низкая степень вовлеченности пользователей в использование и повторное использование таких данных, чем, в свою очередь, обусловлена низкая общественная стоимость открытости данных государственного сектора в России. Исходя из изложенного, предлагается:

1) Внести изменение в раздел III Концепции открытости федеральных органов исполнительной власти, утверждённой Распоряжением Правительства РФ от 30 января 2014 г. № 93-р, дополнив его положениями о таких принципах открытости федеральных органов исполнительной власти, как создание условий для обнаружения таких данных, обеспечение интероперабельности и безопасности данных.

2) Внести изменение в ч.4 ст.7 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», дополнив её положениями, устанавливающими дополнительные критерии открытости общедоступных данных, публикуемых в сети «Интернет» государственными органами и органами местного самоуправления: создание условий для обнаружения таких данных, обеспечение интероперабельности и безопасности данных.

Предложения по развитию подходов к механизмам контроля доступа к данным

Загрузки. В российском праве предусмотрены возможности для использования загрузок, в частности, в сфере открытых данных государственного сектора. Так, например, Методических рекомендациях Правительственной комиссии по координации деятельности Открытого Правительства по публикации открытых данных государственными органами и органами местного самоуправления (далее – Методические

рекомендации) указана необходимость обеспечения возможности немедленной загрузки данных из опубликованного набора.

В части защиты персональных данных Федеральной службой по техническому и экспортному контролю (ФСТЭК России) утверждены требования для средств доверенной загрузки, применяемых в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Интерфейсы прикладного программирования (API). В Методических рекомендациях предоставление возможностей API рекомендуется в части публикации открытых данных через порталы государственных и муниципальных органов. Указано, что открытые данные на порталах должны размещаться в машиночитаемом виде либо в одном из машиночитаемых форматов (CSV, XML, JSON, RDF), либо в виде API. Также, даны методические рекомендации по использованию API, случаям его использования, методам API, адресам доступа и вызовов, форматам ответа и т.д.

В 2019 г. была разработана Концепция открытых API, в которой описаны подходы к разработке и внедрению открытых API, которые были определены совместно с участниками российского финансового рынка. В Концепции, среди прочего, перечислены принципы внедрения открытых API:

– Создание ценности: стандарты открытых API должны разрабатываться под конкретные кейсы и проекты, в которых на начальном этапе определены поставщики и потребители API, проведен детальный анализ пользовательского опыта.

– Единообразие: при создании открытых API должны использоваться единые стандарты данных и информационной безопасности.

– Развитие: открытые API должны быть расширяемыми, то есть дополняться новыми и позволять расширять функциональность существующих.

– Безопасность: внедрение стандартов открытых API требует соблюдения повышенных мер информационной безопасности, в том числе проведения аудита квалифицированными специалистами.

– Открытость: аккредитация участников среды открытых API не должна создавать избыточные барьеры для доступа к открытым API.

– Ответственность: должен быть разработан порядок разрешения споров. Будет принят набор правил, устанавливающих ответственность и полномочия участников среды открытых API.

– Обязательный или рекомендательный характер: установление обязательного или рекомендательного характера будет зависеть от экономического эффекта API.

Песочницы данных. Что касается песочниц данных, такой инструмент не предусмотрен российским правовым регулированием. Вместе с тем, ОЭСР называет данный инструмент в качестве наиболее перспективного с точки зрения контроля доступа к конфиденциальным данным. Таким образом, предусмотрение цифровых песочниц как инструмента контроля доступа к данным в российском правовом регулировании безопасности информации будет означать введение в российское правовое поле перспективного инструмента контроля доступа к конфиденциальным данным.

В указанной выше Концепции отмечается, что создание песочницы данных планируется на портале открытых API для финансовой сферы в качестве дополнительной функции портала. Следует также отметить, что песочницы данных активно применяются российскими компаниями и ассоциациями. Например, Лаборатория Касперского использует «песочницы» в своих программных продуктах для создания изолированной виртуальной среды и проверки исполняемых файлов с целью выявления вредоносного ПО.

В российском праве требования к инструментам контроля доступа к данным прямо не установлены на уровне федеральных законов. Установлены отдельные обязанности по обеспечению такого контроля обладателями информации и операторами информационных систем: как, ч.4 ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»

Рекомендации для России.

1) Формирование нормативных требований к обеспечению безопасности данных и контроля доступа к данным. Такие требования могут формироваться Минкомсвязью России в форме подзаконных актов, принимаемых для обеспечения выполнения положений ч.4 ст. 16 Федерального закона «Об информации, информационных технологиях и защите информации».

2) Принятие Минкомсвязью России методических рекомендаций по вопросам контроля доступа к данным с перечислением инструментов такого контроля, в том числе API и песочниц данных. Такие рекомендации должны содержать сведения об обеспечении безопасности доступа к данным, управлению рисками, связанными с предоставлением такого доступа, с учетом рекомендаций ОЭСР (в частности, Рекомендации по управлению рисками цифровой безопасности для экономического и социального благополучия, отчета о подходах к управлению данными 2020 г.) и международной практики (например, инициативы «Пяти безопасностей»).

3) Предусмотрение Банком России в стандарте по использованию открытых API для финансовой сферы необходимости цикличной оценки рисков безопасности в сфере контроля доступа к данным и принимаемых в соответствии с ними мер.

ВЫВОДЫ

Таким образом проанализированы доктринальные основания к пересмотру устаревшей концепции персональных данных и практики по совершенствованию статуса, объёма и содержания прав субъектов персональных данных на примере таких зарубежных юрисдикций, как ЕС, США, Сингапур, Южная Корея, Индия и др. Проведена оценка персональных данных как фактора для развития цифровой экономики, отдельных отраслей, сферы инноваций, международной торговли; проанализированы статистические показатели, подтверждающие экономическую значимость данных.

Реализован анализ стандартов ОЭСР, Совета Европы и других международных организаций, занимающихся правовыми и техническими вопросами обработки персональных данных. Исследованы причины происхождения кризиса бинарного подхода к пониманию персональных данных, такие как неясность порога идентификации, ограниченность и примитивность подхода, разнообразие и многоаспектность персональных данных, не поддающиеся однозначному делению в условиях развития технологий. Выявлены различия подходов к пониманию персональных данных, как объекта гражданских прав и как ценности в социально-правовом понимании.

Обозначена роль степени идентифицируемости данных в определении их правового статуса. Изучен правовой режим обезличенных данных, проведён сравнительный анализ различных технологий защиты персональных данных по содержанию процедур и их технической надёжности и национальные подходы к их классификации. Выявлена тенденция к различению обезличенных персональных данных и

обезличенных данных в зависимости от сохранения технической возможности восстановления удалённых идентификаторов.

Проведён анализ законодательных и доктринальных подходов к получению согласия на обработку персональных данных. Хотя классическим подходом к регулированию согласия выступает узкий/ целевой подход, динамичное развитие цифровой экономики требует обращения к более гибким способам обеспечения правового основания к обработке данных.

Исследовано положение отдельных участников оборота персональных данных. Определено содержание статуса пользователя данных, проанализирована проблема использования данных из открытых источников, а также выделены основания для использования данных без согласия их субъекта. Проведено различие в статусе обработчика и контролёра данных в европейском праве. Ввиду распространения коммерческого оборота данных значение приобретает роль посредника данных.

Практический интерес представляет анализ новых элементов правоспособности субъекта персональных данных, как право на перенос данных и право на забвение, а также такой механизм укрепления защиты персональных данных, как уведомление о нарушении. Несмотря на то, что новации, влекущие расширение прав и обязанностей участников оборота данных, отвечают потребностям развивающейся цифровой экономики, их имплементация в национальных правовых системах неоднозначна. Переносимость данных рассматривается как драйвер конкурентной экономики, поскольку решает проблему информационной асимметрии, способствует развитию инноваций, укреплению потока данных, обеспечивает возможность информационного самоопределения. Вместе с тем реализация права на перенос данных поднимает множество практических вопросов, как техническое обеспечение переноса данных, затраты на осуществление переноса, обеспечение безопасности переносимых данных и принятие ответственности за их сохранность.

По каждому из выделенных вопросов проведён анализ действующего российского законодательства, выявлены пробелы и иные сдерживающие факторы к развитию режима персональных данных в России, сформулированы рекомендации по его улучшению.

Выявлена необходимость обновления определения персональных данных. Необходимо ввести понятие «идентификатора», дополнить определение примерами идентификаторов, провести различение видов персональных данных по степени идентифицируемости на основе применяемых методов обработки данных. На основе анализа проекта Минкомсвязи о выделении категории обезличенных персональных данных, сделан вывод о целесообразности диверсификации категорий персональных

данных, и необходимости перехода к более детальному регулированию обезличенных персональных данных. Разработаны рекомендации по работе с новой категорией персональных данных. Для улучшения регулирования обезличивания данных необходима разработка практических рекомендаций компетентным органом по снижению рисков обезличивания данных с учётом развития технологий и лучших практик.

В части регулирования согласия на обработку персональных данных выявлено упущение в объяснении конкретности согласия. Рекомендуется внести дополнение о том, что «конкретное согласие означает согласие субъекта на обработку для конкретной цели в степени или объёмах, определённых субъектом». Необходимо указание точного возрастного порога дачи согласия. Также реализация самоопределения субъекта персональных данных предполагает свободное распоряжение своим согласием как в части его дачи, так и отзыва. Рекомендуется уточнить, что «процедура отзыва данного согласия должна быть не более сложной, чем процедура предоставления согласия».

В исследовании прав и обязанностей участников российского правового режима персональных данных выявлена необходимость их уточнения. Также необходима регламентация деятельности посредников данных. Необходимо сформировать рекомендации для посредников данных, включающие требования о соблюдении принципов защиты персональных данных.

Исследовано содержание прав субъектов персональных данных с учётом развития правового режима персональных данных в зарубежных странах. Выявлен законодательный пробел в части регулирования переносимости персональных данных. Необходимо закрепить право субъектов на переносимость данных с указанием принципов его использования, например, закрепить оговорку о неумалении остальных законодательно установленных прав субъекта персональных данных. Также составлены рекомендации по закреплению в российском законодательстве требования об уведомлении о нарушении персональных данных. Рекомендуется закрепить понятие «инцидент» и регламентировать порядок сообщения оператора данных о допущении нарушения, включая определения перечня обязательных сведений для уведомления. Сформированы предложения по развитию подходов к доступу и контролю данных, включая принцип информационной открытости органов государственной власти. Предлагается дополнить Концепцию открытости ФОИВ положениями о критериях открытого правительства и законодательство о защите информации положениями об обеспечении открытости общедоступных данных.