**Концепция регулирования и защиты персональных данных с учётом развития информационных технологий**

I. Введение

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

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

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

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

Регулирование отношений в сфере персональных данных в Российской Федерации традиционно проводится с опозданием в сравнении с Европейским Союзом, модель регулирования которого была взята за основу в России, в связи с чем требуется новый подход к регулированию персональных данных в Российской Федерации для того, чтобы обеспечить и защиту прав субъектов персональных данных, и выполнение международных обязательств Российской Федерации в данной сфере.

II. Цели и задачи регулирования

Законодательство о защите персональных данных представляет собой практическое средство обеспечения одного из важнейших конституционных прав человека и гражданина - права на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23 Конституции Российской Федерации). Так как права и свободы человека и гражданина являются непосредственно действующими и определяют смысл и содержание федеральных законов и иных нормативных правовых актов (статья 18 Конституции РФ), то основной целью регулирования должна быть защита тех данных, использование которых позволяет лицу, получившему такие данные, вмешаться в частную жизнь индивида (в том числе с помощью устройств связи и средств телекоммуникации) без согласия соответствующего индивида.

Достижению поставленной цели должно способствовать решение следующих задач:

1) изменение подхода к определению персональных данных в целях возможности отнесения к персональным данным информации, позволяющей вмешиваться в частную жизнь физического лица с ее помощью;

2) установление требований к порядку обработки информация, которая не является персональными данными, но в результате обработки которой (в том числе автоматизированной) возможно получить персональные данные;

3) изменение подходов к административной, уголовной и гражданско-правовой ответственности за нарушение законодательства о защите персональных данных ;

4) установление требований к оператору персональных данных по раскрытию информации об утечках персональных данных;

5) наделение уполномоченного органа по защите прав субъектов персональных данных в Российской Федерации дополнительными контрольно-надзорными полномочиями;

6) создание системы доверительного управления персональными данными на основе единого средства идентификации и аутентификации физических лиц.

III. Направления реформирования сферы персональных данных

Для решения поставленных задач целесообразно осуществить реформирование законодательства в сфере персональных данных по следующим направлениям.

Во-первых, необходимо уточнить понятие персональных данных путем введения в определение персональных данных условия о вмешательстве в частную жизнь физического лица с помощью соответствующих данных.

Существующее в настоящий момент в Российской Федерации определение персональных данных является максимально абстрактным и общим: персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Подобная дефиниция персональных данных затрудняет применение этого термина на практике, так как, с одной стороны, позволяет любую информацию, создаваемую человеком или о человеке, рассматривать как персональные данные (со всеми вытекающими последствиями в виде необходимости соблюдать требования, предъявляемые операторам персональных данных), а с другой стороны, не позволяет, исходя из буквального толкования, применять нормы о персональных данных к случаям, когда с помощью данных идентифицируется не конкретное лицо, а устройство (компьютер, мобильный телефон и т.д.), которым пользуется физическое лицо.

В связи с изложенным необходимо в законодательстве дать общее определение персональных данных с приведением примеров (используя оборот «в том числе»), что позволит, с одной стороны, конкретизировать абстрактный термин, а с другой стороны, не замыкаться на закрытом перечне данных

Во-вторых, в целях обеспечения баланса интересов физических лиц – субъектов персональных данных и организаций, оказывающих различные услуги с использованием информационно-телекоммуникационной сети «Интернет», необходимо установить особые требования к порядку обработки информация, которая сама по себе не позволяет идентифицировать физическое лицо или его персональные характеристики (персональные данные специальных категорий), то есть не является персональными данными, но в результате обработки которой (в том числе автоматизированной) возможно получить персональные данные.

Такая информация должна обрабатываться без учета требований, установленных законодательством о персональных данных (например, требований о регистрации в качестве оператора персональных данных и т.п.), но с учетом специально установленных требований к обработке такой информации, которые необходимо изложить в Федеральном законе «Об информации, информационных технологиях и о защите информации». Однако результаты обработки такой информации могут обрабатываться[[1]](#footnote-1) только с соблюдением требований законодательства о защите персональных данных, в том числе о получении предварительного согласия физического лица на обработку данных.

Основные принципы регулирования отношений субъектов данных (которые еще не являются персональными данными, но обработка которых позволит получить персональные данные) и операторов данных должны быть описаны в Федеральном законе «Об информации, информационных технологиях и о защите информации», где необходимо:

1. определить понятие «профилирование» как особый вид деятельности, связанный с обработкой информации, касающейся физических лиц (не обязательно персональных данных);
2. предусмотреть, что оператор информационной системы, оператор связи, провайдер хостинга, которые собирают данные пользователей системы/средств связи/вычислительных мощностей в целях профилирования, должны до начала сбора и обработки данных представить пользователям информацию о сборе данных для профилирования, о целях проведения профилирования, о категориях персональных данных, которые могут быть получены в результате профилирования, об операторе данных и (или) его представителе, о наличии надлежащих гарантий безопасности обработки данных, категории лиц или органов, которым могут быть переданы персональные данные, полученные в результате профилирования, и в каких целях, длительность хранения данных, предполагаемые последствия присвоения профиля субъекту данных, о возможности или невозможности отказаться от сбора и обработки данных в целях профилирования без ущерба для качества предоставления соответствующей услуги;

3) установить, что оператор информационной системы, оператор связи, провайдер хостинга не имеют право ограничивать доступ к услугам или ухудшать качество услуг в случае отказа пользователя от обработки данных в целях профилирования за исключением случаев, если такой сбор, обработка или хранение данных предусмотрены законом.

В-третьих, необходимо решить важную проблему создания механизмов обеспечения выполнения требований, установленных законодательством о персональных данных, к числу которых относятся, прежде всего, меры ответственности.

В зарубежных странах установлена очень серьезная ответственность за нарушения в области персональных данных, причем указанные нарушения криминализированы.

В Российской Федерации административное наказание за нарушения в области персональных данных (ст.13.11 КоАП РФ нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)) влечет предупреждение или наложение административного штрафа на граждан в размере от 300 до 500 рублей; на должностных лиц - от 500 до 1000 рублей; на юридических лиц - от 5000 до 10 000 рублей.

Уголовная ответственность за данные нарушения в принципе не установлена (исключение составляет незаконное использование персональных данных для внесения сведения в единый государственный реестр юридических лиц).

Указанная ситуация не создает стимулов для компаний предпринимать все меры по защите персональных данных (а особенности при обработке больших данных в целях создания персонализированной рекламы), так как возможные риски совершенно не соотносимы с возможными прибылями.

В связи с изложенным необходимо:

1. увеличить административную ответственность за нарушения в области персональных данных (хотя бы на том же уровне, который установлен за незаконное использование иностранной рабочей силы),
2. установить уголовную ответственность за нарушения в области законодательства о защите персональных данных, причем ответственность должна возникать непосредственно за нарушения и не быть связана с размером причиненного вреда;
3. усовершенствовать модель привлечения к гражданско-правовой ответственности за нарушения в области персональных данных.

Так как при нарушении в области персональных данных имущественный вред практически недоказуем, а размер морального вреда всегда определяется по усмотрению суда, необходимо установить в Гражданском кодексе РФ возможность взыскания компенсации за нарушения в области персональных данных (по аналогии с тем, как в статье 1301 Гражданского кодекса РФ установлено, что в случаях нарушения исключительного права на произведение автор или иной правообладатель наряду с использованием других применимых способов защиты и мер ответственности, установленных ГК РФ ([статьи 1250](consultantplus://offline/ref=E8B43849461C167CC2DE451A0AFBD14BBB355C419D9E18DF5CFFABC27FE0120FC8C0E19550dAyEJ), [1252](consultantplus://offline/ref=E8B43849461C167CC2DE451A0AFBD14BBB355C419D9E18DF5CFFABC27FE0120FC8C0E19550ACB307dBy6J) и [1253](consultantplus://offline/ref=E8B43849461C167CC2DE451A0AFBD14BBB355C419D9E18DF5CFFABC27FE0120FC8C0E19552dAyAJ)), вправе в соответствии с [пунктом 3 статьи 1252](consultantplus://offline/ref=E8B43849461C167CC2DE451A0AFBD14BBB355C419D9E18DF5CFFABC27FE0120FC8C0E19550ACB306dBy4J) настоящего Кодекса требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации в размере от десяти тысяч рублей до пяти миллионов рублей, определяемом по усмотрению суда исходя из характера нарушения).

Необходимость введения специальной гражданско-правовой ответственности за нарушения в области персональных данных наряду с административной и уголовной ответственностью необходима, так как в рамках административной и уголовной ответственности субъект персональных данных не получает никакого возмещения (а только тратит время на жалобы в уполномоченные органы), тогда как в рамках гражданско-правовой ответственности возмещение может получить сам субъект данных. Это позволит гражданам осознать ценность своих персональных данных и самим отслеживать случаи их нарушения. Последствием активной политики граждан в отношении своих персональных данных станет повышение внимания компаний к соблюдению требований законодательства о защите персональных данных.

В-четвертых, необходимо внедрить в российскую практику информирование операторами данных уполномоченного органа об инцидентах с обрабатываемыми персональными данными.

Важным механизмом повышения ответственности операторов персональных данных и обработчиков данных за обеспечение конфиденциальности персональных данных является существующий в зарубежных странах (Нидерланды, Германия, Великобритания, Япония) механизм информирования уполномоченного органа об инцидентах (утечках, нарушениях и т.п.), произошедших с персональными данными, сопровождающийся установлением серьезной административной ответственности за невыполнение данной обязанности.

В Российской Федерации законодательство в принципе не содержит никаких требований к оператору по раскрытию информации об утечках персональных данных, что не позволяет установить объективную картину достаточности принимаемых мер по защите персональных данных.

В связи с изложенным необходимо дополнить Федеральный закон «О персональных данных» новой статьей, устанавливающей обязанность оператора уведомлять уполномоченный орган обо всех инцидентах с персональными данными, дав определение инцидента (любое несанкционированное предоставление (в том числе доступ) или распространение персональных данных), а также в определенных случаях уведомлять об этом субъекта персональных данных. Требования к порядку направления уведомления и его содержанию может установить уполномоченный орган (данное полномочие целесообразно возложить на него законом).

В-пятых, ряд корректировок необходимо внести в положения Федерального закона №152-ФЗ о полномочиях уполномоченного органа по защите прав субъектов персональных данных в Российской Федерации.

Полномочия уполномоченного органа по защите прав субъектов персональных данных в Российской Федерации (Роскомнадзор) установлены статьей 23 Федерального закона №152-ФЗ. Анализ указанных полномочий позволяет говорить о том, что в сфере персональных данных и взаимодействия с операторами персональных данных контрольно-надзорные полномочия Роскомндазора являются необходимыми и достаточными для осуществления необходимой защиты прав субъектов персональных данных и соответствуют объему полномочий аналогичных органов государственной власти зарубежных стран.

Вместе с тем в настоящее время существенно возросла потребность в регулировании отношений, непосредственно не связанных с обработкой персональных данных (в понимании Федерального закона №152-ФЗ), но приводящих к вмешательству в частную жизнь физического лица. И применительно к данным отношениям полномочий Роскомнадзора, перечисленных в статье 23 Федерального закона №152-ФЗ, будет явно недостаточно.

Соответственно, в том случае, если понятие «персональные данные» будет скорректировано, а также будут установлены обязанности операторов, обрабатывающих данные, непосредственно не являющиеся персональными данными, но позволяющие получить персональные данные в ходе обработки, то потребуется скорректировать и полномочия Роскомнадзора в целях распространения их на новых субъектов (операторов поисковых систем, операторов почтовых сервисов и т.д.).

В-шестых, необходимо создать в Российской Федерации систему доверительного управления персональными данными, основанную на едином национальном средстве идентификации и аутентификации, которое не является удостоверением личности. Применение указанного средства будет являться обязательным при взаимодействии в электронной форме с государственными и муниципальными органами и поощряемым к применению в частных сферах (такая модель создана и успешно применяется в Великобритании и Сингапуре).

Сохранение существующей сейчас системы управления персональными данными, основанной на множественности средств идентификации и аутентификации и различии указанных средств для публичной и частной сфер, нецелесообразно, так как, с одной стороны, является препятствием для развития систем электронного взаимодействия (в связи с наличием множественности различных паролей и иных средств идентификации и аутентификации у граждан), а с другой стороны, требует от граждан предоставления персональных данных значительному числу лиц при прохождении процедур аутентификации и идентификации (создание профилей, аккаунтов, личных кабинетов и т.п.), что приводит к неоправданному расширению числа операторов персональных данных одного конкретного физического лица.

Внедрение системы доверительного управления информации, основанной на едином средстве идентификации и аутентификации гражданина, потребует законодательной регламентации единого средства аутентификации и идентификации на территории Российской Федерации и установления требований об использовании данного средства при оказании государственных и муниципальных услуг, а также установления требований к оператору данного единого средства аутентификации и идентификации.

Основой для создания системы доверительного управления информации может стать федеральная государственная информационная система "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (ЕСИА).

В настоящее врем альтернатив ЕСИА среди государственных информационных систем в качестве систем доверительного управления информацией, применимых, в том числе для исключения трансграничной передачи персональных (личных) данных и допускающих подключение неограниченного количества потребителей нет как по уровню зрелости, так и по достигнутым результатам.

Действующее законодательство закрепляет уникальность ЕСИА в России как государственной системы – поставщика идентификации, в связи с чем замена ЕСИА означает необходимость повторения функционала ЕСИА хотя бы в части интеграции с электронными сервисами, зарегистрированными в СМЭВ. Кроме того, использование иных государственных информационных систем как основы для создания системы доверительного управления информацией невозможно по следующим информационно-технологическим причинам:

1) в иных ГИС отсутствует защищенная инфраструктура (по типу К-1) хранения персональных данных с максимально возможной моделью угроз, при которой сохранность данных обеспечивается даже при нарушении целостности системы;

2) в иных ГИС отсутствует автоматизированная настройка прав доступа сторонних порталов к персональным данным, в соответствии с типом соглашения, заключенным с пользователем, типом подтверждения пользователем своих персональных данных, в том числе сторонних порталов органов государственной власти субъектов РФ.

Вместе с тем использование ЕСИА как системы доверительного управления информацией, в том числе персональными данными, потребует решения следующих вопросов:

1) создание сервиса выдачи СКПЭП для ИС и приложений на ГОСТ-алгоритмах (серия 28147), для чего необходимо определить критерии выдачи сертификатов. Сервис может располагаться как в ЕСИА, так и в удостоверяющих центрах. Цель появления сервиса - усиление контроля над владельцами ИС, особенно за нерезидентами РФ;

2) разрешение регистрирования в ЕСИА зарубежных компаний либо без необходимости указания ОГРН, либо с необходимостью указания аналога. При этом должна быть обеспечена интеграция с международными реестрами юридических лиц;

3) разрешение регистрирования ФЛ с неподтвержденной учетной записью;

4) создание в составе ЕСИА программного продукта обезличивающего персональные данные, т.е. позволяющего осуществлять связывание хранящихся и обрабатываемых сведений с конкретным физическим лицом — фамилии, имени и отчества, с набором идентификаторов (токеном). Данные, связывающие идентификационную информацию с токенами, не будут покидать пределов Российской Федерации и храниться в ЕСИА, все технические средства которой находятся на территории России.

1. Обработка персональных данных в соответствии с Федеральным законом «О персональных данных» - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [↑](#footnote-ref-1)