



ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ
по запросу Общества с ограниченной ответственностью
«Системы корпоративной аналитики» от 15.06.2022

Санкт-Петербург

07 июля 2022 г.

Адресат: Общество с ограниченной ответственностью «Системы корпоративной аналитики» (ООО «СКА»).

Экспертная организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет».

Место нахождения: Россия, 199034, Санкт-Петербург, Университетская наб. д.7-9.
Тел: +7 (812) 328-20-00
Эл. почта: spbu@spbu.ru
сайт: spbu.ru

Информационные материалы, представленные для проведения исследования: Не представлены.

Общие положения

Ответственность за подготовку информационных материалов, предоставленных для экспертного исследования (далее – исходные материалы), несет лицо, направившее запрос. Эксперт отвечает за выражение профессионального мнения по поставленным перед ним вопросам в соответствии с законодательством Российской Федерации.

Экспертное исследование проведено в соответствии с законодательством РФ, внутренними правилами, действующими в СПбГУ. Экспертное исследование было спланировано, проведено с учетом обеспечения разумной уверенности в полноте и достоверности исходных материалов для выражения экспертного суждения и, в том числе, включало в себя: а) изучение доказательств, подтверждающих значение и раскрытие информации в предоставленных исходных материалах; б) оценку принципов и методов создания исходных материалов; в) определение главных оценочных значений, представленных в исходных материалах; г) оценку общего представления об исходных материалах.

Датой экспертного заключения является дата окончания экспертного исследования. По изменениям состава и содержания исходных материалов, которые могут иметь место после окончания экспертного исследования, экспертная организация ответственности не несет.



Вопросы, поставленные перед экспертной организацией

Экспертное исследование направлено на выражение мнения во всех существенных отношениях по поставленным перед экспертной организацией вопросам:

- 1) Какие источники информации, содержащие персональные данные, могут использоваться для систематизации и аналитики данных?
- 2) Какие источники информации, содержащие персональные данные, запрещены к использованию законодательством Российской Федерации?
- 3) Правомерно ли использование (сбор, обработка, хранение) персональных данных, содержащихся в различных каналах мессенджера Telegram (Телеграм) и агрегируемых Телеграм-ботами?
- 4) Правомерно ли использование информации (сбор, обработка, хранение), содержащей персональные данные, находящейся в Даркнете?
- 5) Правомерно ли использование информации, содержащей персональные данные, размещенной в сети Интернет (Даркнет) в связи с утечкой из каких-либо организаций, учреждений (государственных, коммерческих и т.д.)?
- 6) В рамках договорных отношений с Заказчиком Исполнитель оказывает услуги, в том числе по проверке физических лиц, что подразумевает сбор, обработку и хранение персональных данных в отношении них. По условиям договора Заказчик обязан получить согласие на обработку персональных данных на каждое проверяемое физическое лицо и направить в адрес Исполнителя выверенные списки физических лиц, подлежащих проверке. Какая ответственность предусмотрена для Исполнителя, если Заказчиком согласие на обработку персональных данных получено не было, но Заказчик уведомил Исполнителя о получении такого согласия?

Перечень научных и иных источников, использованных для ответа на поставленный(е) вопрос (вопросы):

- 1) Гражданский кодекс Российской Федерации;
- 2) Кодекс Российской Федерации об административных правонарушениях;
- 3) Уголовный кодекс Российской Федерации;
- 4) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 5) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 6) Определение Второго кассационного суда общей юрисдикции от 13.07.2021 № 88-15635/2021, 2-1712/2020;
- 7) Постановление Девятого арбитражного апелляционного суда от 08.07.2021 № 09АП-31545/2021-ГК по делу № А40-18827/17;
- 8) Решение судьи Таганского районного суда города Москвы от 01.07.2021 № 2-2418/2021;
- 9) Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е издание, переработанное и дополненное. Издательство «Статут». – 2021;



10) Ширманов В.А. Критический анализ ст. 10.1 Федерального закона «О персональных данных», предложение новой редакции статьи // Право и экономика. 2022. № 2. С. 52 - 58.

Все нормативные правовые акты использованы в редакциях, действующих на дату составления экспертного заключения.

Перечень понятий, использованных в ходе исследования (в соответствии с перечисленными в Экспертном заключении научными и иными источниками):

1) *Даркнет (DarkNet)* – скрытая сеть, соединения которой устанавливаются с использованием нестандартных протоколов и портов.

2) *Лицо, осуществляющее обработку персональных данных по поручению оператора* – лицо, привлеченное оператором для осуществления обработки персональных данных в интересах соответствующего оператора.

3) *Обработка 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.

4) *Общедоступная информация* – общеизвестные сведения и иная информация, доступ к которой не ограничен.

5) *Оператор* – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

6) *Охраняемая база данных* – база данных, создание которой (включая обработку или представление соответствующих материалов) требует существенных финансовых, материальных, организационных или иных затрат. При отсутствии доказательств иного базой данных, создание которой требует существенных затрат, признается база данных, содержащая не менее десяти тысяч самостоятельных информационных элементов (материалов), составляющих содержание базы данных.

7) *Персональные данные, разрешенные субъектом персональных данных для распространения* – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

8) *Распространение персональных данных* – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.



Содержание исследования

1. Допустимые источники получения персональных данных

Одним из принципов российского информационного законодательства является недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия¹.

Закон прямо запрещает требовать от гражданина предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и *получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами*. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных². В свою очередь, Федеральный закон «О персональных данных» обязывает операторов обрабатывать персональные данные на законной основе³ и только в предусмотренных законом случаях⁴.

Систематическое толкование приведенных выше норм позволяет констатировать, что любые операции по обработке персональных данных (в том числе, их распространение, сбор, запись, систематизация и накопление) могут осуществляться только с согласия субъекта персональных данных или при наличии других *оснований, предусмотренных законом*.

Общие основания для обработки персональных данных перечислены в части 1 статьи 6 Федерального закона «О персональных данных». В ряде случаев перечень допустимых оснований обработки персональных данных уточняется специальными нормами закона, которые могут содержать более узкий перечень оснований для обработки отдельных видов данных (например, специальных категорий персональных данных⁵ или биометрических данных⁶) или устанавливать дополнительные условия для их обработки (например, требовать оформления согласия на обработку персональных данных в письменной форме⁷).

Независимо от того, о каких видах данных идет речь, наличие оснований для обработки персональных данных оценивается применительно к действиям каждого конкретного субъекта (оператора). Например, если определенное лицо осуществляет распространение данных с использованием сайта в сети «Интернет», а другое лицо использует распространяемые на сайте данные для рассылки рекламы, каждый из указанных субъектов должен иметь *собственное* основание для обработки персональных данных. Если у владельца сайта имеется основание для распространения персональных данных, это само по себе не означает правомерность использования этих данных любым заинтересованным лицом. Получатель данных должен доказать наличие у него основания для извлечения и последующего использования персональных данных, которые он получает через сайт (например, наличие согласия субъекта на использование его данных данным оператором либо иное основание обработки данных, предусмотренное законом).

¹ Пункт 7 части 1 статьи 3 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

² Части 8 и 9 статьи 9 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

³ Часть 1 статьи 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

⁴ Часть 1 статьи 6 и статья 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

⁵ Часть 2 статьи 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

⁶ Часть 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

⁷ Часть 4 статьи 12 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».



Необходимо подчеркнуть, что с 01.03.2021 общедоступность персональных данных (то есть размещение персональных данных в источнике, фактически открытом для всеобщего доступа с согласия субъекта персональных данных) более не является основанием, достаточным для обработки персональных данных любым заинтересованным оператором. Норма, предусматривавшая соответствующее основание для обработки персональных данных (пункт 10 статьи 6 Федерального закона «О персональных данных»), была исключена из закона. Одновременно, названный закон был дополнен статьей 10.1, посвященной обработке персональных данных, разрешенных субъектом персональных данных для распространения. В контексте потенциального сбора персональных данных, размещенных в открытых источниках, наиболее важное значение имеют следующие правила (части 2 и 3 статьи 10.1 Федерального закона «О персональных данных» соответственно):

(а) В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия на их распространение обязанность предоставить доказательства законности последующей обработки таких персональных данных лежит на каждом лице, осуществившем их обработку.

(б) В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующей обработки таких персональных данных лежит на каждом лице, осуществившем их обработку.

Указанные нормы позволяют сделать следующий вывод: независимо от события, в результате которого персональные данные оказались доступны неопределенному кругу лиц (в результате раскрытия самим субъектом персональных данных или в результате совершения правонарушения, приведшего к «утечке» данных), заинтересованный оператор *вправе* осуществлять их обработку, *если* докажет наличие у него законных оснований для такой обработки. Хотя приведенные выше правила вызывают критику в научно-практической литературе, поскольку вступают в некоторое противоречие с принципом законности обработки персональных данных⁸, в настоящее время они сформулированы достаточно однозначно. Соответственно, если персональные данные оказались в открытом доступе в результате неправомерных действий, но при этом заинтересованный в их обработке оператор, например, имеет согласие на использование указанных данных (пункт 1 части 1 статьи 6 Федерального закона «О персональных данных»), обработка персональных данных таким оператором является правомерной.

В российской судебной практике встречаются решения, в которых распространение персональных данных через чат-боты в приложении Телеграм или в иных открытых источниках признается незаконным по причине отсутствия правового основания для такого распространения⁹. В то же время исследование судебной практики не позволило обнаружить судебные решения, свидетельствующие о привлечении к ответственности лиц, использующих такие источники для сбора персональных данных *при наличии на то правового основания* (например, согласия субъекта персональных данных).

⁸ Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е издание, переработанное и дополненное. Издательство «Статут». – 2021. С. 468; Ширманов В.А. Критический анализ ст. 10.1 Федерального закона «О персональных данных», предложение новой редакции статьи // Право и экономика. 2022. № 2. С. 52 - 58.

⁹ Решение судьи Таганского районного суда города Москвы от 01.07.2021 № 2-2418/2021; Определение Второго кассационного суда общей юрисдикции от 13.07.2021 № 88-15635/2021, 2-1712/2020.



Отдельно следует отметить, что правомерное извлечение персональных данных из открытых источников предполагает соблюдение оператором законодательства об интеллектуальной собственности. В соответствии с российским законодательством информационный массив, доступный в сети «Интернет», может являться охраняемой базой данных. В таком случае, составителю соответствующей базы данных принадлежит исключительное право на её использование, и любое иное лицо не вправе без разрешения правообладателя осуществлять перенос существенной части составляющих ее материалов на другой информационный носитель с использованием любых технических средств и в любой форме¹⁰. Кроме того, не допускается неоднократное извлечение или использование материалов, составляющих несущественную часть базы данных, если такие действия противоречат нормальному использованию базы данных и ущемляют необоснованным образом законные интересы изготовителя базы данных¹¹.

В российской судебной практике имеют место прецеденты, в рамках которых действия по извлечению материалов из открытых баз данных были признаны нарушением интеллектуальных прав её изготовителей. Наиболее значимым из них является спор ООО «Дабл» против ООО «В Контакте». Хотя рассмотрение соответствующего дела еще не завершено, последний судебный акт, принятый по делу на дату составления настоящего заключения, содержит выводы о незаконности действий компании, которая без согласия администрации социальной сети использовала для аналитических целей данные профилей пользователей¹². Подходы, выработанные судебными органами в рамках рассмотрения данного спора, предположительно окажут определяющее влияние на рассмотрение схожих споров в будущем.

2. Риски неполучения согласия на обработку персональных данных

При наличии согласия субъекта оператор вправе привлечь для обработки его данных третье лицо, обрабатывающее персональные данные по поручению оператора¹³. При этом в силу прямого указания закона такое третье лицо освобождается от обязанности получать согласие субъекта на обработку его персональных данных – соответствующая обязанность возлагается на оператора¹⁴. Как следствие, если лицо (например, исполнитель по договору оказания услуг) действует на основании надлежащим образом оформленного поручения оператора (заказчика) на обработку персональных данных, такое лицо не может быть привлечено к ответственности в случае отсутствия согласия субъекта персональных данных на обработку его данных.

Описанное выше правило применяется только к лицам, выполняющим функции обработки персональных данных *по поручению* оператора. Если речь идет об отношениях между двумя независимыми операторами (то есть двумя лицами, каждое из которых обрабатывает персональные данные *в собственных интересах*), каждое из указанных лиц должно иметь основания для обработки персональных данных. Так, если в случае спора первый из двух операторов не сможет предъявить доказательства наличия согласия на обработку персональных данных по причине нарушения договора другим оператором (например, если второй оператор обязался перед первым, что получит согласие субъекта, но нарушил это обязательство), в таком случае первый оператор будет нести ответственность за обработку персональных данных без правового основания.

¹⁰ Пункт 1 статьи 1334 Гражданского кодекса РФ.

¹¹ Пункт 3 статьи 1335.1 Гражданского кодекса РФ.

¹² Постановление Девятого арбитражного апелляционного суда от 08.07.2021 № 09АП-31545/2021-ГК по делу № А40-18827/17.

¹³ Часть 3 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

¹⁴ Часть 4 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».



Административная ответственность за обработку персональных данных в отсутствие правовых оснований дифференцирована в зависимости от того, какие требования нарушены оператором¹⁵:

(а) по общему правилу, если юридическое лицо обрабатывает персональные данные без правового основания, оно может быть подвергнуто административному штрафу в размере от шестидесяти тысяч до ста тысяч рублей, а его должностные лица – в размере от десяти тысяч до двадцати тысяч рублей;

(б) если юридическое лицо могло обрабатывать персональные данные только на основании письменной согласия субъекта, но не получило его, оно может быть подвергнуто административному штрафу в размере от тридцати тысяч до ста пятидесяти тысяч рублей, а его должностные лица – в размере от двадцати тысяч до сорока тысяч рублей.

Анализ правоприменительной практики показывает, что в случае незаконной обработки персональных данных в деятельности юридического лица применение к должностным лицам организации мер уголовной ответственности (статья 137 Уголовного кодекса РФ) не практикуется, хотя и является теоретически возможным.

Выводы

В настоящее время российское законодательство о персональных данных не содержит запрета на систематизацию и иное использование персональных данных, извлеченных из каких-либо источников (в том числе, баз данных, сформированных в результате неправомерного доступа к информации). В то же время, оператор, использующий персональные данные из любых источников, должен иметь законное основание для обработки персональных данных, предусмотренное статьей 6 Федерального закона «О персональных данных», либо специальными нормами закона, которые уточняют перечень оснований для обработки отдельных категорий персональных данных. Кроме того, оператор должен убедиться, что извлечение материалов из открытых источников не приведет к нарушению интеллектуальных прав изготовителя соответствующей базы данных.

В тех случаях, когда обработка персональных данных осуществляется исполнителем в интересах заказчика (в частности, для целей оказания заказчику тех или иных услуг, прямо предполагающих обработку персональных данных), такие отношения по своему содержанию являются обработкой персональных данных по поручению. В таком случае стороны должны заключить письменное соглашение о поручении обработки персональных данных, соответствующее требованиям части 3 статьи 6 Федерального закона «О персональных данных» (может быть интегрировано в состав основного договора об оказании услуг).

При условии заключения соглашения о поручении обработки персональных данных ответственность за получение согласия на обработку персональных данных будет нести оператор (заказчик услуг). В силу прямого указания закона лицо, осуществляющее обработку персональных данных по поручению оператора (исполнитель), не может подлежать административной ответственности за неполучение согласия субъекта на обработку его данных.

¹⁵ Части 1-2.1 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.



Заключение

Вопрос 1: Какие источники информации, содержащие персональные данные, могут использоваться для систематизации и аналитики данных?

Ответ на вопрос 1: В целях осуществления систематизации и аналитики персональных данных оператор может использовать любые источники информации, при условии (а) наличия у оператора правового основания для обработки соответствующего состава персональных данных теми способами, которые применяет оператор; (б) соблюдения оператором норм законодательства об интеллектуальной собственности (если база данных, из которой осуществляется извлечение сведений, охраняется законодательством о смежных правах).

Вопрос 2: Какие источники информации, содержащие персональные данные, запрещены к использованию законодательством Российской Федерации?

Ответ на вопрос 2: Российское законодательство не содержит запрета на извлечение персональных данных из определенных типов источников. Для целей определения правомерности обработки персональных данных важен не источник их получения, а наличие правового основания для их обработки, а также соблюдение прав правообладателей (если источник персональных данных охраняется в качестве объекта смежных прав).

Вопрос 3: Правомерно ли использование (сбор, обработка, хранение) персональных данных, содержащихся в различных каналах мессенджера Telegram (Телеграм) и агрегируемых Телеграм-ботами?

Ответ на вопрос 3: Факт использования для получения персональных данных каналов или чат-ботов мессенджера Telegram сам по себе не свидетельствует о правомерности или неправомерности извлечения персональных данных. Определяющим фактором для определения правомерности использования персональных данных является наличие правовых оснований для их обработки у лица, осуществляющего такое извлечение и последующее использование данных.

Вопрос 4: Правомерно ли использование информации (сбор, обработка, хранение), содержащей персональные данные, находящейся в Даркнете?

Ответ на вопрос 4: Факт использования для получения персональных данных телекоммуникационных сетей, относящихся к Даркнету, сам по себе не свидетельствует о правомерности или неправомерности извлечения персональных данных. Определяющим фактором для определения правомерности использования персональных данных является наличие правовых оснований для их обработки у лица, осуществляющего такое извлечение и последующее использование данных.

Вопрос 5: Правомерно ли использование информации, содержащей персональные данные, размещенной в сети Интернет (Даркнет) в связи с утечкой из каких-либо организаций, учреждений (государственных, коммерческих и т.д.)?

Ответ на вопрос 5: Факт использования для наполнения источника персональных данных информации, полученной незаконным путем, сам по себе не свидетельствует о правомерности или неправомерности извлечения персональных данных из соответствующего источника. Определяющим фактором для определения правомерности использования персональных данных является наличие правовых оснований для их обработки у лица, осуществляющего такое извлечение и последующее использование данных.



Вопрос 6: В рамках договорных отношений с Заказчиком Исполнитель оказывает услуги, в том числе по проверке физических лиц, что подразумевает сбор, обработку и хранение персональных данных в отношении них. По условиям договора Заказчик обязан получить согласие на обработку персональных данных на каждое проверяемое физическое лицо и направить в адрес Исполнителя выверенные списки физических лиц, подлежащих проверке. Какая ответственность предусмотрена для Исполнителя, если Заказчиком согласие на обработку персональных данных получено не было, но Заказчик уведомил Исполнителя о получении такого согласия?

Ответ на вопрос 6: Если обработка персональных данных осуществляется исполнителем в интересах заказчика (в частности, для целей оказания заказчику тех или иных услуг, прямо предполагающих обработку персональных данных), такие отношения по своему содержанию являются обработкой персональных данных по поручению. Заказчик при этом выступает оператором персональных данных, а исполнитель – лицом, обрабатывающим персональные данные по поручению оператора. В таком случае стороны должны заключить письменное соглашение о поручении обработки персональных данных, соответствующее требованиям части 3 статьи 6 Федерального закона «О персональных данных» (может быть интегрировано в состав основного договора об оказании услуг). При условии надлежащего заключения соглашения о поручении обработки персональных данных ответственность за получение согласия на обработку персональных данных несет оператор (заказчик услуг). В силу прямого указания закона лицо, осуществляющее обработку персональных данных по поручению оператора (исполнитель), не может подлежать административной ответственности за неполучение согласия субъекта на обработку его данных.

Исследование в объеме 9 страниц.

И.о. директора Центра экспертиз

А.В. Попов

В документе прошито, пронумеровано 9 (девять) листов.

И.о. директора Центра экспертиз А.В. Попов

Дата 04.04.2023

