

|  |
| --- |
| **ОБЩЕРОССИЙСКАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ****«АССОЦИАЦИЯ ЮРИСТОВ РОССИИ»****МОСКОВСКОЕ ОТДЕЛЕНИЕ****Комиссия по правовому обеспечению Цифровой экономики** |
| 119991, г. Москва, ГСП-1, Ленинские горы, д. 1, стр. 13, 4 учебный корпус МГУ имени М.В. Ломоносова, Юридический факультет, ауд. 611 а тел.: +7 (499) 706-00-06, доб. 148; e-mail: digitallaw@alrf.msk.ru<http://www.alrf.msk.ru> |

|  |  |
| --- | --- |
| «05» марта 2020 года | г. Москва |

**ЗАКЛЮЧЕНИЕ ПО ВОПРОСУ «КОМПЕНСАЦИЯ СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК НОВЫЙ МЕХАНИЗМ ЗАЩИТЫ ПРАВ ГРАЖДАН ОТ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ»**

«27» февраля 2020 года в Университете имени О.Е. Кутафина (МГЮА) состоялось заседание Комиссии по правовому обеспечению цифровой экономики Московского отделения АЮР (далее - «Комиссия») по теме «Компенсация субъектам персональных данных как новый механизм защиты прав граждан от нарушений законодательства о персональных данных». В заседании и дискуссии приняли участие члены Комиссии, представители Государственной Думы Федерального Собрания Российской Федерации, международных и российских ассоциаций, органов государственной власти, члены Ассоциации юристов России, представители бизнеса и научного сообщества.

По результатам заседания Комиссия считает целесообразным опубликовать заключение с описанием ключевых проблем и предложений по вопросам, затронутым в докладах и рабочей дискуссии.

**ВВЕДЕНИЕ**

В последнее время в России и в мире участились случаи утечки персональных данных. Почти две трети медицинских организаций столкнулись с утечкой данных. Половина из них скрывает факт происшествия. Эксперты считают, что проблема заключается в нехватке квалифицированных кадров и слабой цифровой грамотности персонала. Однако большинство опрошенных представителей медучреждений сообщили, что виновниками инцидентов стали собственные сотрудники. При этом эксперты InfoWatch отмечают, что «низкий уровень информатизации в медицине можно считать скорее плюсом в сложившихся условиях — потому что развитие цифровых хранилищ потребует эволюции информационной безопасности»[[1]](#footnote-1). Существенная доля утечек персональных данных пользователей происходит в финансовой сфере[[2]](#footnote-2). Так, например, в октябре 2019 года СМИ сообщали об утечке данных 60 млн кредитных карт, принадлежащих клиентам Сбербанка[[3]](#footnote-3). Причем упущения операторов по работе с персональными данными встречаются не только в онлайн-сфере. В качестве примера можно привести широко обсуждавшийся в СМИ случай, когда мешки с документами "Сбербанка" лежали среди строительного мусора в частном секторе Ижевска на обочине дороги: копии паспортов, трудовых книжек, справок о доходах, заявления на получение кредитов, анкеты, с информацией о собственности клиента, его долговых обязательствах и зарплатных картах с номерами счетов[[4]](#footnote-4).

Зарубежные организации также подвержены рискам утечек персональных данных. Например, более 419 миллионов записей пользователей социальной сети Facebook оказались в свободном доступе. В сеть утекли телефонные номера, имена пользователей, а также их пол и страна нахождения пользователя[[5]](#footnote-5). В 2017 г. произошла крупная утечка персональных данных, содержащих имена, номера социального страхования, данные кредитных карт и пр., из одного из крупнейших кредитных бюро США – компании Equifax, затронувшая 143 млн. граждан США[[6]](#footnote-6). Компания Microsoft рассказала о возможной утечке информации из базы данных поддержки клиентов. По словам корпорации, инцидент произошёл в декабре 2019 года. Из-за ошибки сотрудников база находилась в Сети незащищенной с 05 по 31 декабря[[7]](#footnote-7).

Помимо человеческого фактора причиной утечек могут выступать и используемые операторами персональных данных (далее – операторы) программно-технические средства. Как отмечается, «неожиданные крупные утечки паролей к почтовым ящикам «Яндекса» и Mail.ru стали результатами взлома через уязвимости в бесплатном ПО, которое используют крупнейшие российские интернет-компании»[[8]](#footnote-8).

Аналогичные случаи имеют широкое распространение на практике и их число только растет. Однако и из приведенных примеров достаточно для иллюстрации факта того, что значительной части утечек можно было бы предотвратить, если бы операторы более внимательно относились к вопросам защиты персональных данных. То же самое справедливо и применительно к иным видам нарушений персональных данных.

Одной из проблем существующего в России правового режима персональных данных является отсутствие эффективных *частноправовых* механизмов защиты прав субъектов персональных данных. Особенностью таких механизмов, отличающих их от административно-правовых является возможность субъекта защищать свое право через суд, определяя судьбу инициированного процесса по своему усмотрению с присуждением в случае выигрыша взысканных сумм самому субъекту, а не бюджету, как это имеет место в случае с административными штрафами. Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных» (далее - Закон о персональных данных; 152-ФЗ) в настоящее время предусматривает, что субъект имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке (ч. 2 ст. 17). Однако указанные меры на практике практически не используются в силу своей неэффективности.

**Взыскание убытков в качестве средства защиты прав субъектов персональных данных.**

Для того, чтобы взыскать убытки, субъекту персональных данных необходимо доказать не только факт нарушения, но и размер таких убытков, а также причинно-следственную связь между допущенным оператором нарушением и такими убытками. Это сделать гражданину практически невозможно. Многие негативные последствия нарушений прав субъектов персональных данных носят нематериальный характер и, как правило, отдалены во времени от самого нарушения. Например, когда разглашение чувствительных персональных данных (например, о состоянии здоровья) может повлечь дискриминацию на работе или в иных социальных группах. Либо когда недостоверные или неточные данные были впоследствии включены в профайл гражданина и используются для определения его платежеспособности, что, например, повлекло ухудшение кредитной истории лица, невозможность заключения кредитного договора. Не говоря уже о рисках совершения мошеннических действий, таких как последующего оформления кредита или юридического лица на гражданина по ксерокопии паспорта, полученной оператором в нарушение закона или выступившей предметом утечки.

Кроме того, в ряде случаев субъект просто не может обосновать наличие причинно-следственной связи между нарушением и убытками как того требует гражданское законодательство, поскольку информационные процессы, связанные с обработкой данных, достаточно сложны и в них вовлечено множество участников, значительная часть из которых невидима для субъекта. Как следствие, субъект просто не знает, кем, в каком объеме и для каких целей обрабатываются его данные, после того как они «ушли» от первоначального оператора.

Проводить при указанных особенностях отношений, связанных с нарушениями прав субъектов персональных данных, аналогию с традиционными подходами гражданского права, выработанными без учета специфики современных информационных процессов, - неправильно. Однако именно такая аналогия и предполагается в ч. 2 ст. 17 Закона о персональных данных, которая без каких-либо изъятий и особенностей распространяет положения о возмещении убытков на отношения, связанные с нарушением прав субъектов персональных данных. Не удивительно, что за более чем 10 лет существования данной нормы, так и не появилось судебной практики по ее применению.

**Взыскание морального ущерба в качестве средства защиты прав субъектов персональных данных.**

Помимо возмещения убытков, ч. 2 ст. 17 Закона о персональных данных предусматривает возможность заявления требования о компенсации морального вреда. Данный способ защиты в большей степени учитывает особенности отношений, возникающих в сфере обработки персональных данных, чем возмещение убытков, однако и он не обладает достаточной эффективностью. Проблема все в той же необходимости установления судом факта наличия морального вреда и причинно-следственной связи между нарушением и таким вредом[[9]](#footnote-9). Кроме того, как известно, моральный вред российскими судами если и взыскивается, то в крайне незначительных объемах (средний размер за нарушение прав субъектов персональных данных варьируется от 500 руб. до 5 000 руб.)[[10]](#footnote-10).

Как следствие, сейчас гражданин лишен возможности эффективно защищать и восстанавливать свои нарушенные права в суде, поскольку он не только не может выполнить предъявляемые к нему требования по доказыванию соответствующих обстоятельств, но и даже в случае успеха получает слишком незначительные суммы. Это, в свою очередь, влечет отсутствие интереса со стороны практикующих судебных представителей к такого рода спорам и адекватного профессионального представительства граждан в судах по таким спорам. Граждане, не имея эффективного процесса защиты их прав, лишены стимулов к тому, чтобы повышать свою информированность в сфере защиты персональных данных и рассматривают законодательство о персональных данных как искусственную конструкцию, которая создает иллюзию защиты.

В настоящее время единственным более-менее работоспособным механизмом защиты является административный – посредством обращения в Роскомнадзор соответствующей жалобой. Однако ресурсов Роскомнадзора не хватает для реагирования на все допущенные нарушения. С другой стороны, операторы больше заинтересованы в том, чтобы выполнить букву закона и его формальности, чем в выстраивании эффективной защиты персональных данных. Существующие административные штрафы за нарушение прав субъектов персональных данных в размере до 75 000 руб. (ст. 13.11 КоАП РФ) не создают достаточных финансовых стимулов для операторов по принятию необходимых мер по соблюдению законодательства о персональных данных. Вместе с тем, когда затраты на исполнение требований закона существенно превышают издержки, связанные с его нарушением, законодательство перестает быть эффективным. Данную ситуацию не исправить лишь повышением административных штрафов, для этого необходимо создать условия, при которых, операторы несли бы непосредственную ответственность перед субъектами за каждый случай нарушения их прав, которой в настоящее время по факту нет.

Существующая ситуация противоречит национальной программе «Цифровая экономика», предполагающей ответственный подход граждан к распоряжению своими данными, с одной стороны, и ответственный подход операторов к их обработке и защите для обеспечения доверия к внедряемым цифровым сервисам. Доверие является одним из ключевых условий развития инноваций, основанных на обработке данных[[11]](#footnote-11). По данным исследовательской компании *Gartner,* опасения пользователей относительно сохранности своих данных влекут самоцензурирование и сокращение количества выкладываемых в сеть данных, а также использование альтернативных способов защиты данных (*VPN*, плагины к браузерам и пр.)[[12]](#footnote-12). Это, в свою очередь, может повлечь сокращение и ухудшение качества данных, необходимых для адекватной персонализации сервисов. О негативном влиянии отсутствия доверия на развитие технологий машинного обучения говорится и в материалах Мирового экономического форума[[13]](#footnote-13). Недавнее исследование ВЦИОМ демонстрирует, что большинство граждан выражают озабоченность непрозрачными механизмами использования их данных в социальных сетях[[14]](#footnote-14).

Кроме того, существующая ситуация с отсутствием эффективных частноправовых механизмов защиты прав субъектов персональных данных не отвечает требованиям международного права. Ряд международных соглашений предусматривают обязанность государства обеспечить эффективные средства правовой защиты лиц, пострадавших от нарушения их фундаментальных прав и свобод. В частности, согласно международным документам ООН, государства обязаны не только обеспечивать подотчетность и средства правовой защиты в случае нарушений прав человека, совершенных государственными субъектами, но и принимать надлежащие меры для обеспечения доступа пострадавших от связанных с предпринимательской деятельностью нарушений прав человека к эффективным средствам правовой защиты[[15]](#footnote-15). Аналогичные положения о необходимости обеспечения эффективных средств защиты прав граждан от нарушений их фундаментальных свобод содержатся и в ст. 13 Европейской конвенции о защите прав человека и основных свобод. При этом указанные положения имеют непосредственное отношение к правам субъектов персональных данных, поскольку законодательство о персональных данных имеет одной из своих главных целей защиту фундаментального права на неприкосновенность частной жизни (ст. 2 Закона о персональных данных). В пояснительном протоколе к Модернизированной конвенции Совета Европы № 108, подписанной Российской Федерацией 10 октября 2018 г., отмечается, что санкции за нарушение законодательства о персональных данных должны быть «эффективными, пропорциональными или дестимулирующими» по отношению к соответствующему поведению нарушителя, «такими же должны быть и средства правовой защиты субъектов»[[16]](#footnote-16).

Таким образом, проблема обеспечения наличия в законодательстве адекватных средств защиты субъектов персональных данных от нарушений может также рассматриваться и через призму неукоснительного исполнения принятых на себя Российской Федерацией международных обязательств. При этом уровень эффективности защиты субъектов персональных данных, в частности, средств предоставляемой им защиты является одним из ключевых факторов, принимаемых во внимание Европейской комиссией при принятии решения о признании страны, обеспечивающей адекватный уровень защиты прав субъектов персональных данных[[17]](#footnote-17).

**Предлагаемое решение**

 Целесообразно введение *нового* инструмента защиты прав субъектов персональных данных, который бы учитывал особенности нематериального характера персональных данных, сложности информационных процессов, связанных с их обработкой и проблемы, связанные с доказыванием фактов наступления неблагоприятных последствий и установлением причинно-следственной связи.

В качестве правовой модели здесь могла бы послужить такая мера ответственности, как компенсация за нарушение исключительного права, предусмотренная статьей 1301 Гражданского Кодекса РФ. Такая компенсация подлежит взысканию при наличии доказанного факта нарушения. При этом, в ходе рассмотрения таких споров у суда сохраняется достаточно большая гибкость при определении размера компенсации с учетом характера нарушения, его наступивших или возможных последствий, необходимости обеспечения превентивного эффекта и других релевантных факторов.

**Преимущества данного предложения:**

Появляется сильный аргумент в пользу сбалансированности разрабатываемого для целей реализации национальной программы «Цифровая экономика» нового регулирования. Как демонстрируют обсуждения, которые проходят в Сколково, АНО «Цифровая экономика» и других площадках, на них в основном идет речь именно о либерализации действующего законодательства, посредством «снятия барьеров» для операторов персональных данных. Как следствие, подготовленные изменения носят исключительно прооператорскую направленность, без глубокой проработки возможных рисков, связанных с использованием новых информационных технологий для обработки персональных данных.

При этом для операторов, осуществляющих коммерческую деятельность, основной целью выступает получение прибыли, а защита прав персональных данных граждан представляет собой лишь издержки. Поэтому о рисках, возникающих у граждан в связи с обработкой их данных, говорить если и принято, то только в контексте возможных издержек и влияния на прибыль. Предлагаемый механизм создает дополнительные издержки в случае несоблюдения операторами законодательства о персональных данных и финансовый стимул для ответственного, а не формального построения соответствующей требованиям законодательства о персональных данных системы защиты.

Например, в случае массовых «утечек» персональных данных, которые периодически происходят по вине крупных операторов (МТС[[18]](#footnote-18), Мегафон[[19]](#footnote-19), Сбербанк[[20]](#footnote-20) и т.д.) субъекты персональных данных, права которых были нарушены, могут объединиться для подачи коллективного иска к виновному лицу. Именно с целью защиты прав граждан при наличии массовых правонарушений Федеральным законом от 18.07.2019 № 191-ФЗ в Гражданский процессуальный кодекс РФ (далее – «ГПК РФ») была введена гл. 22.3, предусматривающая возможность подачи коллективных исков. Это процессуальное средство защиты применительно к спорам, связанным с крупной «утечкой» персональных данных, позволит большому количеству субъектов защитить свои права и взыскать с оператора такую компенсацию, размер которой превысит выгоду оператора от неправомерной продажи персональных данных или от отсутствия затрат на обеспечение надлежащего хранения и надежной обработки персональных данных. Кроме того, установленная ч. 4 ст. 30 ГПК РФ исключительная подсудность для таких исков позволит в рамках одного суда по месту нахождения оператора персональных данных сформировать системообразующую судебную практику и судейский состав, способный квалифицированно разрешать споры, связанные с нарушением прав граждан как субъектов персональных данных.

Очевидно, что в перспективе внедрение нового способа защиты права будет способствовать «перезагрузке» законодательства о персональных данных, выработке более ответственного подхода субъектов к распоряжению своими данными и переносу рассмотрения многих спорных вопросов, связанных с использованием таких данных, с уровня «Роскомнадзор – оператор» на уровень «субъект — оператор». Субъекты, получив предлагаемый механизм защиты своих прав, смогут эффективно использовать существующие положения законодательства о персональных данных:

* взаимодействие с операторами посредством запросов о получении информации об обрабатываемых данных, их уточнении или удалении;
* уделение внимания политикам конфиденциальности,
* более ответственный подход к даче согласий на обработку их данных
* и пр.

Роскомнадзор, при этом сможет в большей степени сосредоточиться не столько на рассмотрении рутинных дел, сколько на стратегических вопросах и направлять практику. Кроме того, Роскомнадзор мог бы выступать в качестве эксперта в судебных процессах между субъектом и оператором, подобно тому, как сейчас это происходит в спорах между потребителями и предпринимателями, где уполномоченный государственный орган - Роспотребнадзор выступает не инициатором процесса, а лицом, обладающим экспертизой в вопросах, связанных с предметом спора, и участие которого способствует более тщательному рассмотрению дела.

Механизм взыскания компенсаций в пользу граждан является частноправовым, а не публично-правовым. В связи с этим взыскание такого рода компенсаций подчиняется иным правилам, нежели взыскание административных штрафов. Например, взыскание административного штрафа с иностранной компании, не имеющей присутствия или активов на территории Российской Федерации, является практически невозможным, поскольку признать и принудительно исполнить решение российского правоприменительного органа о наложении санкций невозможно принудительно исполнить за рубежом в силу существующих принципов международного права (за исключением случаев, когда имеется соответствующее международное соглашение, но таких соглашений у России с ключевыми западными и восточными юрисдикциями нет). В свою очередь, признание и принудительное исполнение решений по частноправовым отношениям возможно и без специального международного договора, а на основании принципов взаимности и международной вежливости. Учитывая, что ориентация законодательства и правоприменительной практики на защиту персональных данных субъектов является общемировым трендом, вероятность исполнения иностранным судом решения российского суда о взыскании в пользу физического лица компенсации за нарушение его прав, вынесенного в отношении иностранной компанией, имеет перспективы. Тем самым осуществляется выравнивание позиций российских компаний и иностранных организаций, осуществляющих деятельность в виртуальном пространстве Российской Федерации в части соблюдения требований российского законодательства.

Предлагаемое изменение будет способствовать усилению механизмов защиты чести, достоинства и деловой репутации граждан от соответствующих публикаций в сети Интернет. Информация, порочащая честь, достоинство и деловую репутацию физического лица, может рассматриваться как персональные данные. Соответственно, если такая информация будет размещаться на интернет-ресурсах без законного основания, это будет нарушать права лица как субъекта персональных данных и влечь соответствующую ответственность. Такая ответственность может быть усилена механизмом компенсации, который обеспечит более «зрелый» и внимательный подход интернет-ресурсов и платформ к рассмотрению требований граждан, связанных с удалением порочащей их честь, достоинство и деловую репутацию информации из сети Интернет. Принятие предлагаемых изменений также повлечет за собой снижение количества преступлений имущественного характера, совершаемых с использованием персональных данных граждан, за счет повышения качества предпринимаемых операторами мер по обеспечению комплаенса в области законодательства о персональных данных.

Предлагаемое изменение может положительно сказаться на имидже Российской Федерации и дать дополнительные аргументы при взаимодействии в рамках Совета Европы (имплементация в российское законодательство положений Модернизированной конвенции Совета Европы № 108 «О защите физических лиц при автоматизированной обработке персональных данных», подписанной РФ 10 октября 2018 г.) и при взаимодействии с основным торговым партнером РФ – Европейским Союзом при обсуждении вопроса о признании РФ страной, обеспечивающей адекватный уровень защиты прав субъектов персональных данных, что может существенно облегчить трансграничный обмен данными между странами ЕС и РФ.

Предлагаемое решение не требует затрат на его реализацию из федерального бюджета.

**Возможные негативные последствия:**

Новый вид ответственности по своей природе является частноправовым, поэтому будет сосуществовать наряду с административными штрафами, которые уже предусмотрены нормами административного законодательства, представляя собой дополнительное финансовое бремя издержки для операторов. Хотя в условиях незначительного размера административных штрафов, связанных с нарушениями прав субъектов персональных данных (до 75 000 руб.), данное бремя вряд ли можно считать сопоставимым с европейским (штрафы до 20 млн. Евро или до 4% общегодового мирового оборота компании);

Нельзя исключать возможных злоупотреблений правом со стороны субъектов, которые будут целенаправленно заниматься провоцированием операторов. Однако в смежной области, где подобные риски обозначались (законодательство о защите прав потребителей) - они так и не материализовались в каком-либо значительном объеме. Кроме того, даже при возникновении на начальном этапе внедрения рассматриваемого механизма, он впоследствии может быть скорректирован разъяснениями Верховного Суда Российской Федерации.

**Вариант возможной реализации обозначенного предложения**

Внесение изменений в действующий Закон о персональных данных приводится далее. При этом необходимо сделать несколько комментариев к его положениям

Во-первых, ответственность в виде компенсации наступает лишь при наличии вины оператора, поскольку положения части 3 предлагаемого проекта должны применяться в совокупности с уже имеющейся в части 1 данной статьи нормой о наступлении ответственности только в отношении лиц, «*виновных* в нарушении требований настоящего Федерального закона». Тем самым, у оператора сохраняется возможность освободиться от ответственности, если он докажет, что «при той степени заботливости и осмотрительности, какая от него требовалась по характеру обязательства и условиям оборота, принял все меры для надлежащего исполнения обязательства» (п. 1 ст. 401 Гражданского кодекса РФ). Например, если соответствующая утечка данных произошла по причинам, зависящим от самого субъекта (несоблюдение им элементарных правил информационной безопасности, в частности, неиспользование им систем антивирусной защиты, необновление используемого программного обеспечения, использование одного и того же пароля к различным аккаунтам и приложениям и пр.), либо же в результате действий особенно изощренных хакерских атак, то такой оператор освобождается от ответственности в форме выплаты компенсации за произошедшие в результате таких действий нарушения.

Во-вторых, ответственность в виде выплаты компенсаций наступает лишь за те виды нарушений, которые непосредственно затрагивают права субъекта (на что указывает используемая в тексте поправки формулировка - «за нарушение его прав»). Таким образом, формальные нарушения законодательства о персональных данных, например, неподача оператором уведомления в Роскомнадзор в порядке, предусмотренном ст. 22 152-ФЗ, для включения такого оператора в реестр, не будет являться основанием для требования компенсации, так как данный вид нарушения не затрагивает прав субъекта, а является нарушением в сфере порядка управления, о чем свидетельствует характер наступающей административной ответственности. В данном случае ответственность наступает не по ст. 13.11 КоАП РФ (нарушение законодательства Российской Федерации в области персональных данных), а по ст. 19.7 КоАП РФ (непредставление сведений (информации).

В-третьих, размер «вилки» компенсации взят по аналогии с предусмотренным в ст.1301 Гражданского кодекса РФ применительно к компенсациям за нарушение авторских прав в силу схожести проблем, возникающих при защите соответствующих прав. При этом данная «вилка» обладает достаточно высокой степенью гибкости, позволяя учитывать, как малозначительные, так и достаточно серьезные по своему характеру нарушения, которые отличаются особой опасностью и тяжестью вреда для граждан (например, в кредитно-финансовой сфере). Однако в целом размер данной «вилки» является обсуждаемым и может быть изменен в том числе для того, чтобы несколько минимизировать возможную явную несоразмерность существующих компенсаций морального вреда за наиболее тяжелые виды потерь (потеря кормильца, пожизненная инвалидность и пр.) и размеры компенсаций за нарушение прав субъектов персональных данных. В этом вопросе необходимо проявлять осмотрительность: в условиях мизерных компенсаций морального вреда важно не «опустить» компенсации в сфере персональных данных до их уровня, а наоборот – поднять первые до уровня вторых.

«24. Ответственность за нарушение требований настоящего Федерального закона

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.
2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.
3. **Субъект персональных данных вправе вместо возмещения убытков и (или компенсации морального вреда требовать от нарушителя выплаты компенсации за нарушение его прав. Компенсация подлежит взысканию при доказанности факта нарушения, совершенного оператором. При этом субъект персональных данных, обратившийся за выплатой компенсации, освобождается от необходимости доказывания размера причиненного ему таким нарушением имущественного или морального ущерба. Размер компенсации устанавливается судом в размере от десяти тысяч рублей до миллиона рублей, определяемом по усмотрению суда исходя из характера нарушения и иных обстоятельств дела с учетом требований разумности и справедливости.**

\*\*\*\*\*

*Координатор работы Комиссии* – Журавлев Александр Викторович, председатель Комиссии, управляющий партнер юридической компании «ЭБР».

*Куратор аналитической работы* Савельев Александр Иванович, заместитель председателя Комиссии, к.ю.н., доцент кафедры информационного права, старший научный сотрудник НИУ ВШЭ

**Докладчики и эксперты, чьи материалы использованы при подготовке настоящего заключения:**

Едидин Борис Александрович – член Комиссии, к.ю.н., заместитель генерального директора по правовым вопросам Института развития интернета (ИРИ).

Орехович Александра Владимировна – Член комиссии, директор по правовым инициативам Фонда развития интернет-инициатив (ФРИИ).

Третьяков Андрей Юрьевич – член МРО АЮР, управляющий партнер Questa Consulting.

Чирков Борис Аркадьевич – член МРО АЮР, аспирант им. М.В. Ломоносова, юрисконсульт отдела судебно-арбитражной практики Questa Consulting.

Погожев Дмитрий Валерьевич – член МРО АЮР, директор по правовым вопросам ООО «ПЕТЕР-СЕРВИС Спецтехнологии», оператор фискальных данных OFD.ru выпускник Moscow Digital School.

Липин Дмитрий Александрович - заместитель исполнительного директора-руководителя Аппарата Ассоциации юристов России.

|  |  |
| --- | --- |
| **Председатель Комиссии** | **А.В. Журавлев** |

1. *Выжать любой ценой: медицинская отрасль лидирует по утечкам данных: Российские компании в области здравоохранения замалчивают инциденты со сливами информации о пациентах // Известия, 27.02.2020* [↑](#footnote-ref-1)
2. *Исследование InfoWatch утечек конфиденциальной информации из организаций финансового сегмента в 2019 г.* [↑](#footnote-ref-2)
3. *Клиенты Сбербанка попали на черный рынок. Утечка затронула владельцев кредитных карт // Коммерсант, 03.10.2019.* [↑](#footnote-ref-3)
4. *Личные данные клиентов Сбербанка выбросили на помойку в Зеленограде // Forbes.ru, 31.05.2013.* [↑](#footnote-ref-4)
5. *A huge database of Facebook users’ phone numbers found online // Techcrunch, 04.09.2019* [↑](#footnote-ref-5)
6. *The Equifax Data Breach: What to Do. Federal Trade Commission, 08.09.2017.* [↑](#footnote-ref-6)
7. [*https://www.anti-malware.ru/news/2020-01-23-1447/31801*](https://www.anti-malware.ru/news/2020-01-23-1447/31801) [↑](#footnote-ref-7)
8. *Дилер Google: «Яндекс» и Mail.ru взломаны через новую уязвимость // Известия, 09.09.2014.* [↑](#footnote-ref-8)
9. *«Суду следует также устанавливать, чем подтверждается факт причинения потерпевшему нравственных или физических страданий, при каких обстоятельствах и какими действиями (бездействием) они нанесены, степень вины причинителя, какие нравственные или физические страдания перенесены потерпевшим, в какой сумме он оценивает их компенсацию и другие обстоятельства, имеющие значение для разрешения конкретного спора» (Постановление Пленума Верховного Суда РФ от 20.12.1994 N 10 "Некоторые вопросы применения законодательства о компенсации морального вреда").* [↑](#footnote-ref-9)
10. *Напр.:.: решение Ленинского районного суда г. Новосибирска от 20.01.2015 по делу № 2-692/2015, Апелляционное определение Красноярского краевого суда от 29.06.2016 по делу № 33-8532/2016 и др.* [↑](#footnote-ref-10)
11. *OECD. Data-driven Innovation for Growth and Well-being. P. 58; OECD. Meeting the policy challenges of tomorrow’s digital economy. 2016. Данный тезис признается и российским правительством. Как отметил в ходе Парламентских слушаний «Большие данные и защита прав пользователей» заместитель Председателя Правительства РФ М. Акимов, «если не удастся создать атмосферу взаимного доверия, которое бы обеспечивало динамичное технологическое развитие с одной стороны, но с другой стороны — безусловно защищало бы права, базовые свободы и уверенность граждан в легальном, защищенном использовании их данных, если эту задачу решить не удастся, то обесценятся все иные: инфраструктурные, образовательные, технологические инициативы, которые содержатся в программе „Цифровая экономика“».* [↑](#footnote-ref-11)
12. *Gartner/Maverick Research: The Disappearing Customer. Published: 18 September 2017.* [↑](#footnote-ref-12)
13. *How to Prevent Discriminatory Outcomes in Machine Learning. WEF Global Future Council on Human Rights 2016–2018. White Paper. March 2018.*  [↑](#footnote-ref-13)
14. *Персональные данные в интернете: возможности и риски. Исследование ВЦИОМ. URL:* [*https://wciom.ru/index.php?id=236&uid=9401&fbclid=IwAR2\_IaebzcdZT6348Ojgfbh7vACNPiKOtM4g\_caYvc5TsmPs6WLmlwC8x1M*](https://wciom.ru/index.php?id=236&uid=9401&fbclid=IwAR2_IaebzcdZT6348Ojgfbh7vACNPiKOtM4g_caYvc5TsmPs6WLmlwC8x1M) [↑](#footnote-ref-14)
15. *См. раздел III Руководящих принципов предпринимательской деятельности в аспекте прав человека (одобрены Советом ООН по правам человека резолюцией от 16.06.2011 № 17/4). Аналогичные положения о необходимости обеспечения эффективных средств защиты прав граждан содержатся и в ст. 13 Европейской конвенции о защите прав человека и основных свобод.* [↑](#footnote-ref-15)
16. *Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 2018. P. 27.* [↑](#footnote-ref-16)
17. *«Оценивая уровень адекватности уровня защиты, Комиссия, помимо прочего, принимает во внимание следующие элементы… наличие эффективных и подлежащих правовой защите прав субъектов персональных данных, эффективных административных и судебных средств защиты прав субъектов» (ст. 45 (2)(а) GDPR).* [↑](#footnote-ref-17)
18. *«Стало известно об еще одной крупной утечке персональных данных абонентов сотовой связи. В интернете появились сведения о 1,6 млн абонентов МТС из Башкирии и Санкт-Петербурга», URL: https://rb.ru/article/iz-mts-utekli-personalnye-dannye-16-mln-abonentov/6804637.html* [↑](#footnote-ref-18)
19. *«Мегафон оштрафован на 30 тысяч рублей за утечку данных абонентов», URL:* [*https://www.securitylab.ru/news/407057.php*](https://www.securitylab.ru/news/407057.php) [↑](#footnote-ref-19)
20. *«У клиентов Сбербанка прослушали аудио. На теневых ресурсах снова продают их данные», URL: https://www.kommersant.ru/doc/4134949* [↑](#footnote-ref-20)