

УДК 34.096

[https://doi.org/10.34680/BENEFICIUM.2019.2\(31\).70-83](https://doi.org/10.34680/BENEFICIUM.2019.2(31).70-83)

МЕХАНИЗМЫ ЗАЩИТЫ ПРАВ ГРАЖДАН ПРИ ИСПОЛЬЗОВАНИИ ИМИ ТЕЛЕФОННЫХ СРЕДСТВ СВЯЗИ

ЛАПТЕВА Е.В.

Гуманитарный университет, г. Екатеринбург, Россия

Статья посвящена исследованию проблемы незаконного использования персональных данных абонентов сотовых операторов связи телефонными мошенниками, в частности, выявлению пробелов российского законодательства в обеспечении адекватной защиты прав субъектов персональных данных. Установлены факты приобретения баз персональных данных абонентов, зарегистрированных на территории г. Санкт-Петербурга и Ленинградской области, г. Екатеринбурга и Свердловской области недобросовестными медицинскими коммерческими организациями в целях увеличения собственных доходов посредством телефонных обзвонов (телефонного фишинга) граждан. Проблема состоит в том, что де-юре положения Федерального закона «О персональных данных» от 27.07.2006 г. №152-ФЗ (Закон №152-ФЗ), Федерального закона «О связи» от 07.07.2003 г. №126-ФЗ (Закон №126-ФЗ), Федерального закона «О рекламе» от 13.03.2006 г. №38-ФЗ (Закон №38-ФЗ) и других нормативно-правовых актов, призванных обеспечить защиту персональных данных граждан России, не распространяются на использование их телефонных номеров менеджерами call-центров, поскольку последние получают для обзвона уже «обезличенный» список телефонных номеров, а позиция Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций такова, что «номер телефона без указания на его владельца не является информацией, на основании которой это лицо (субъекта персональных данных) можно однозначно идентифицировать». Необоснованные и назойливые телефонные звонки нарушают неприкосновенность частной жизни и способны причинить значительный финансовый и моральный вред субъектам персональных данных. Таким образом, автор приходит к выводу о необходимости внесения поправок в Закон №152-ФЗ и Закон №38-ФЗ с тем, чтобы номера телефонов абонентов были признаны персональными данными, а также введения новой статьи в Закон №126-ФЗ под номером 44.2 с названием «Обзвоны по сети подвижной радиотелефонной связи» (по аналогии со ст. 44.1 «Рассылка по сети подвижной радиотелефонной связи») для

Образец цитирования:

Лаптева Е.В. (2019). Механизмы защиты прав граждан при использовании ими телефонных средств связи. *BENEFICIUM*. 2019. 2(31): 70-83. doi: [https://doi.org/10.34680/BENEFICIUM.2019.2\(31\).70-83](https://doi.org/10.34680/BENEFICIUM.2019.2(31).70-83)

For citation:

Lapteva E.V. (2019). Mechanisms for Protecting the Rights of Citizens when Using Telephone Communications. *BENEFICIUM*. 2019. 2(31): 70-83. (In Russ.) doi: [https://doi.org/10.34680/BENEFICIUM.2019.2\(31\).70-83](https://doi.org/10.34680/BENEFICIUM.2019.2(31).70-83)

унификации российского права и усиления правовых возможностей защиты частной жизни граждан от телефонных террористов.

Ключевые слова: вмешательство в частную жизнь; использование персональных данных; нарушение прав граждан; незаконная реклама; телефонные мошенники; телефонный спам; телефонный террор; телефонный фишинг; Федеральный закон «О персональных данных».

MECHANISMS FOR PROTECTING THE RIGHTS OF CITIZENS WHEN USING TELEPHONE COMMUNICATIONS

LAPTEVA E.V.

Humanitarian University, Ekaterinburg, Russia

The article is devoted to the study of the problem of the illegal use of personal data of subscribers of cellular telecom operators by telephone scammers, in particular, the identification of gaps in Russian legislation in ensuring adequate protection of the rights of personal data subjects. The facts of the acquisition of personal databases of subscribers registered in the territory of St. Petersburg and the Leningrad Region, of Yekaterinburg and the Sverdlovsk Region by unscrupulous medical commercial organizations in order to increase their own income through telephone calls (phishing) of citizens were established. The problem is that de jure the provisions of the Federal Law «On Personal Data» dated July 27, 2006 No. 152-ФЗ (Law No. 152-ФЗ), the Federal Law «On Communications» dated July 07, 2003 No. 126-ФЗ (Law No. 126-ФЗ), Federal Law «On Advertising» dated March 13, 2006 No. 38-ФЗ (Law No. 38-ФЗ) and other regulatory acts designed to protect the personal data of Russian citizens do not apply the use of their telephone numbers by call-center managers, since the latter receive an «impersonal» list of telephone numbers for calling, and the Federal oversight supervision in the field of communications, information technology and mass communications is such that «the phone number without indicating its owner is not information on the basis of which this person (the subject of personal data) can be unambiguously identified». Unreasonable and intrusive phone calls violate privacy and are capable of causing significant financial and moral harm to personal data subjects. Thus, the author comes to the conclusion that it is necessary to amend Law No. 152-ФЗ and Law No. 38-ФЗ so that the phone numbers of subscribers are recognized as personal data, as well as introduce a new article in Law No. 126-ФЗ under number 44.2 s the title «Ringing on a mobile radiotelephone communication network» (similar to Article 44.1 «Distribution on a mobile radiotelephone communication network») to unify Russian law and strengthen legal capabilities to protect citizens' private lives from telephone terrorists.

Keywords: privacy interference; the use of personal data; violation of citizens' rights; illegal advertising; telephone scammers; telephone spam; telephone terror; telephone phishing; Federal Law «On Personal Data».

Тенденции современного развития информационно-коммуникационных технологий ставят перед российской правовой системой задачу эффективной защиты прав и свобод граждан в сфере обработки и использования персональных данных.

Основным нормативным актом, направленным на защиту персональных данных россиян, является Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» (Закон №152-ФЗ) [Собрание законодательства Российской Федерации, 2019]. Согласно ст. 2 Закона №152-ФЗ, его целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Для достижения цели Закон №152-ФЗ дает понятие персональных данных и устанавливает требования к порядку их сбора, обработки и хранения, распространения и использования. Законодательство Российской Федерации предусматривает установление административной, уголовной и гражданско-правовой ответственности в отношении лиц, нарушивших требования Закона №152-ФЗ.

Казалось бы, проблема защиты персональных данных граждан России решена. Однако, в условиях ужесточения рыночной конкуренции между производителями разнообразных товаров и услуг, с одной стороны, и расширения их возможностей по использованию прогресса в сфере информационно-коммуникационных технологий – с другой, появляются новые формы воздействия, в том числе незаконного, на потенциальных потребителей с использованием баз их персональных данных. В данной статье речь пойдет об одной из таких форм – телефонном обзвоне (фишинге, телемаркетинге).

В настоящее время практически у каждого жителя России имеется мобильный телефон, смартфон, планшет, ноутбук либо компьютер, которые включены в общемировое информационное пространство посредством телекоммуникационных сетей и Интернет. В связи с этим нарастает проблема защиты личной конфиденциальной информации от рассекречивания и формирования нелегальных баз данных о номерах телефонов, адресах электронной почты, аккаунтах в социальных сетях и других персональных данных для незаконного коммерческого использования. Недобросовестные коммерческие организации покупают такие базы данных в своих корыстных интересах – для привлечения новых клиентов посредством телефонных обзвонков, – чем фактически нарушают Закон №152-ФЗ. Однако, проблема в том, что де-юре положения Закона №152-ФЗ не распространяются на использование списков телефонных номеров граждан как персональных баз данных.

Необоснованные и назойливые телефонные звонки нарушают неприкосновенность частной жизни граждан по всему миру и способны причинить значительный финансовый и моральный вред, прежде всего, наиболее доверчивым и уязвимым их категориям (пенсионеры, инвалиды, матери-одиночки, многодетные матери), оценить реальный размер которого не представляется возможным из-за отсутствия международных исследований по данной проблеме [Choi, Lee&Chun, 2017]. Телефонное мошенничество процветает в том числе и потому, что телефонный канал намного более безопа-

сен, чем большинство других каналов связи, из-за доступности Интернет-телефонии. Автоматизированные IP-звонки могут быть сделаны без непосредственного участия человека и без ограничений по охвату территории с целью скрыть телефонный номер вызывающего абонента, что делает затруднительным выявление личности телефонных мошенников [Marzuoli, Kingravi, Dewey & Pienta, 2016].

Масштабная серия обысков, проведенных Главным следственным управлением Следственного комитета Российской Федерации в пяти медицинских центрах г. Санкт-Петербурга в сентябре 2019 г., выявила преступную схему привлечения пациентов на «бесплатное обследование» через назойливые телефонные звонки, после чего «диагносты» с помощью «чудо-оборудования» выявляли страшное заболевание и обещали эффективное лечение, но уже за деньги, в том числе путем заключения кредитных договоров. Счет обманутых пациентов исчисляется многими десятками [Балагаев, 2019]. Отмечается, что подобные медицинские центры действовали по франшизе в каждом российском городе с численностью населения более 100 тыс. человек и свернули свою криминальную деятельность только после череды громких уголовных дел, возбужденных по ст. 159 «Мошенничество» Уголовного кодекса Российской Федерации (УК РФ) [Министерство внутренних дел Российской Федерации, 2019].

Так, в г. Екатеринбурге и Свердловской области сотрудники данных фирм начинали свой обман с тотального телефонного обзвона всех жителей региона в возрасте от 30 и до 74 лет без их письменного согласия по заранее купленным базам телефонных номеров с приглашением пройти бесплатную диагностику в рамках государственной программы диспансеризации по полису ОМС. Такие звонки поступали гражданам многократно и непрерывно на протяжении последних трех лет. Имеются данные о подтвержденных звонках одному человеку, которому сотрудники call-центра данной сети медицинских центров позвонили за два года более 10 раз на разные номера мобильных телефонов, причем иногда они называли абонента по имени, рассчитывая, тем самым, расположить к себе собеседника и настроить его на более доверительную беседу [Бесплатное обследование в многопрофильном медцентре GLOBALMED, 2019]. По такого рода правонарушениям некоторыми гражданами были поданы обращения в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) по Свердловской области, на что были получены разъяснения о том, что номера телефонов не являются персональными данными и в силу этого не подпадают под механизмы правовой защиты, которые прописаны в Законе №152-ФЗ, а на осуществление оперативно-розыскных действий и установление фактов, имеющих юридическое значение, Управление Роскомнадзора не уполномочено, поэтому в случае нарушения Закона №152-ФЗ необходимо обращаться в правоохранительные органы или суд с соответствующим заявлением.

С данной позицией Управления Роскомнадзора вряд ли можно согласиться по следующим соображениям. В соответствии со ст. 3 Закона №152-ФЗ

персональные данные – это любая информация, относящаяся прямо или **косвенно** к определенному или **определяемому физическому лицу** (субъекту персональных данных). Таким образом, Закон №152-ФЗ в целом дает очень широкую трактовку персональным данным, однако контролирующий орган трактует их несколько уже, чем создает правовой вакуум, который способствует незаконному использованию номеров телефонов абонентов, а следовательно, нарушению неприкосновенности частной жизни граждан, а также расширению мошеннической деятельности во всех сферах экономики.

Обычно телефонные мошенники покупают базы номеров телефонов со всеми персональными данными граждан, но затем, уходя от ответственности, автоматизировано ранжируют потенциальных клиентов по заданным критериям, удаляют из имеющихся баз паспортные данные (ФИО, дату рождения, адрес и т.д.) и распечатывают списки. Менеджеры call-центров видят на бумажных носителях уже одни только цифры телефонных номеров и обзванивают граждан «вслепую». В данном случае следует согласиться с позицией Управления Роскомнадзора, что «номер телефона без указания на его владельца не является информацией, на основании которой это лицо (субъекта персональных данных) можно однозначно идентифицировать».

Однако, на наш взгляд, данный подход неприемлем. Российская Федерация еще в 1981 г. подписала «Конвенцию о защите физических лиц при автоматизированной обработке персональных данных» (Конвенция), в соответствии с которой «персональные данные» означают **любую информацию** об определенном или поддающемся определению физическом лице («субъекте данных») [Конвенция о защите физических лиц при автоматизированной обработке персональных данных, 1981]. Также как и «Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [Регламент Европейского Парламента и Совета, 2016], Конвенция запрещает любую обработку персональных данных без согласия субъекта этих данных, а именно: сбор, запись, упорядочение, структурирование, хранение, адаптацию, изменение, извлечение, консультирование, использование, раскрытие, передачу, распространение, ограничение, уничтожение или разрушение. Несовершенство российской нормативно-правовой базы в отношении правовой защиты персональных данных вызвано недооценкой важности поддержания уважения к личности человека путем создания благоприятной атмосферы невмешательства в его частную жизнь в связи с узким истолкованием законодателями самого понятия «частная жизнь», при котором к последней относится не широкая сфера всевозможной жизнедеятельности, связанной с личностью гражданина, а узкий спектр интимных, бытовых и семейных отношений, непосредственно не связанных с правовой сферой [Проскурякова, 2016].

Каждый человек, покупая sim-карту с определенным номером телефона, предоставляет сотовым операторам связи все свои персональные данные; поэтому номера телефонов неразрывно привязаны к этим данным, косвенно относясь к определенному физическому лицу (субъекту персональных дан-

ных). Если кто-то звонит абоненту на его мобильный телефон, то он должен осознавать, кому именно он звонит и с какой целью, т.к. номер мобильного телефона – это уникальный индивидуальный набор цифр, который напрямую связан с личностью конкретного частного лица, защищенного Законом №152-ФЗ, и всеми другими его персональными данными, отделить от которых этот номер фактически невозможно. Номера телефонов позволяют точно идентифицировать личность человека, таким образом, их использование злоумышленниками может негативно отразиться на неприкосновенности частной жизни, а обработку и хранение подобной информации без согласия лица, которому она принадлежит, нельзя назвать нейтральными или незначительными [Бембеева, 2018]. В обществе сложилось негласное правило, по которому не принято передавать номера телефонов третьим, даже хорошо знакомым, лицам без разрешения пользователей этих номеров. Граждане осознают, что, набирая номер телефона определенного абонента, происходит вторжение в его частную жизнь, нарушение его спокойствия, привлечение внимания, расходование его личного времени и моральных сил. Считается, что нужно сначала предупредить абонента о том, что кто-то интересуется его номером телефона, узнать, дает ли он на передачу данной информации свое согласие, и лишь затем сообщать персональный номер мобильного телефона другим людям. Таким образом, психологическая почва для внесения поправок в действующее законодательство уже подготовлена: российское общество готово воспринимать сложившуюся практику обращения частных номеров телефонов в виде регламентированного закона.

Для устранения пробелов в области законодательства необходимо внести изменения в Закон №152-ФЗ с тем, чтобы номера телефонов были признаны персональными данными и защищались этим законом наравне с другими персональными данными граждан, а их незаконный оборот мог бы повлечь ответственность, предусмотренную действующим деликтным законодательством. Обработка персональных данных разрешена только с согласия субъекта персональных данных, причем в письменной форме (п. 4 ст. 9 Закона №152-ФЗ). В случае, если правонарушители не предъявляют доказательства наличия такого согласия, то граждане смогут не только наказывать нарушителей спокойствия, но и взыскивать с них денежные средства в гражданских судах в качестве компенсации морального вреда (ст. 17 и ст. 24 Закона №152-ФЗ). Это позволит оперативно пресекать возможности из преступных побуждений осуществлять массовые звонки гражданам в целях продвижения своих товаров и услуг.

Здесь следует отметить, что реклама по телефону запрещена (ст. 18 Федерального закона «О рекламе» от 13.03.2006 г. №38-ФЗ (Закон №38-ФЗ)) [Собрание законодательства Российской Федерации, 2019]; Федеральная антимонопольная служба России следит за этим, наказывая нарушителей по ст. 14.7 и ст. 14.8 Федерального закона «О защите конкуренции» от 26.07.2006 г. №135-ФЗ [Собрание законодательства Российской Федерации, 2019]. Однако, мошенники нашли лазейки и в этих законах и успешно пользуются ими в

погоне за сверхприбылями. Состав данного правонарушения включает следующие элементы:

1) объект – общественные отношения, право на неприкосновенность частной жизни;

2) объективная сторона – использование номеров телефонов граждан в целях незаконной рекламы и приглашения для последующего совершения мошеннических действий;

3) субъект – вменяемые лица старше 18 лет, нарушающие закон о персональных данных;

4) субъективная сторона – виновные имеют прямой умысел и осознают общественную опасность своих действий по незаконному использованию персональных данных граждан в своих корыстных интересах, поскольку они получают за это заработную плату, предвидят причинение морального и материального вреда обзваниваемым гражданам, т.к. абоненты часто возмущаются, просят их больше не беспокоить и даже ругаются на сотрудников call-центра нецензурной бранью, однако виновные пренебрегают мнением граждан и желают наступления негативных последствий.

Лицам, нарушившим требования Закона №152-ФЗ, в зависимости от конкретных обстоятельств и серьезности деяния может грозить административная, уголовная и гражданско-правовая ответственность [Добрикова, 2019]. Таким образом, если бы в Законе №152-ФЗ было четко указано, что номера телефонов (как мобильных, так и домашних) являются персональными данными, то стало бы возможным применение к правонарушителям различных видов ответственности в соответствии с имеющимся законодательством (табл. 1).

Таблица 1. Виды ответственности за нарушение Закона №152-ФЗ (в отношении использования персональных данных)

Вид ответственности	Нарушение	Санкция	Норма
Административная	Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных	Предупреждение или административный штраф: <ul style="list-style-type: none"> • на граждан – от 1 до 3 тыс. рублей; • на должностных лиц – от 5 до 10 тыс. рублей; • на юридических лиц – от 30 до 50 тыс. рублей 	Ч. 1 ст. 13.11 КоАП РФ ¹
	Обработка персональных данных без письменного согласия субъекта, когда это	Административный штраф: <ul style="list-style-type: none"> • на граждан – от 3 до 5 тыс. рублей; 	Ч. 2 ст. 13.11 КоАП

¹ Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. №195-ФЗ.

	необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие	<ul style="list-style-type: none"> • на должностных лиц – от 10 до 20 тыс. рублей; • на юридических лиц – от 15 до 75 тыс. рублей 	РФ
	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключаящих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них	Административный штраф: <ul style="list-style-type: none"> • на граждан – от 700 рублей до 2 тыс. рублей; • на должностных лиц – от 4 до 10 тыс. рублей; • на индивидуальных предпринимателей – от 10 до 20 тыс. рублей; на юридических лиц – от 25 до 50 тыс. рублей 	Ч. 6 ст. 13.11 КоАП РФ
Уголовная	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ	Штраф до 200 тыс. рублей, либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо принудительные работы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арест на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет)	Ст. 137 УК РФ
	Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование	Штраф до 200 тыс. рублей, либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок	Ст. 272 УК РФ
Гражданско-правовая	Причинение лицу убытков в результате нарушения правил обработки его персональных	Возмещение убытков	ст. 15 ГК РФ ¹

¹Гражданский кодекс Российской Федерации от 30.11.1994 г. №51-ФЗ.

	данных		
	Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных	Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков)	ст. 24 Закона №152-ФЗ, ст. 151 ГК РФ

В отчете Роскомнадзора о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2017-2018 гг. сообщается, что в 2017 г. проведено 875 плановых проверок, при этом нарушения были выявлены в 70.6% случаев; в 2018 г. – 832 плановых проверки, из которых в 668 обнаружены нарушения (табл. 2). Кроме того, процент выявленных нарушений вырос и по внеплановым проверкам (с 30% до 33%).

Таблица 2 – Данные отчетов Роскомнадзора о деятельности Уполномоченного органа по защите прав субъектов персональных данных [Отчет Роскомнадзора, 2019]

Показатель		2017 г.	2018 г.
Количество проведенных плановых проверок	ед.	875	832
Количество проведенных плановых проверок, по которым выявлены нарушения	ед.	618	668
	%	70.6	80.3

Полученные в ходе проверок данные свидетельствуют о необходимости ужесточения российского законодательства в области защиты персональных данных как в плане увеличения размера отдельных административных штрафов и усиления уголовного наказания, так и, и прежде всего, в плане расширения нормативно-правовых оснований привлечения к ответственности путем устранения имеющихся пробелов в законодательстве. При этом контролирующий орган ссылается на ключевой принцип законодательства в области персональных данных, в том числе международного права, – принцип, по которому обработка персональных данных должна ограничиваться достижением конкретных и законных целей. Если сам субъект не дал согласие на обработку своих персональных данных, то их обработка операторами является незаконной. Снизить риск нарушения прав субъектов персональных данных – задача контролирующих органов [Терещенко, 2018].

Если Закон №152-ФЗ станет полноценным, т.е. включающим номера телефонов граждан в объект защиты, возникнет необходимость привлечения к ответственности и тех лиц, которые незаконно предоставляют базы телефонных номеров недобросовестным фирмам, а ими, вероятно, являются операторы телефонной связи. Сейчас они не несут никакой ответственности за эти свои действия, поэтому должным образом не заботятся о безопасности баз с персональными данными своих абонентов. Точно также возникнет ответственность и у тех юридических и физических лиц, которые в настоящее время незаконно приобретают эти базы и безнаказанно используют в своих ко-

рыстных интересах. При этом, очевидно, что сотрудники таких call-центров должны привлекаться к ответственности наравне с фирмами-работодателями, поскольку они сознательно выбирают работу, на которой будут вынуждены нарушать права других граждан. Именно поэтому, подобные нелегальные call-центры не имеют опознавательных знаков и расположены в потаенных местах, где их нелегко обнаружить правоохранительным органам; следовательно, все осознают преступный характер обращения чужих номеров телефонов.

Также необходимо дополнить ст. 2 Федерального закона от 07.07.2003 г. №126-ФЗ «О связи» (Закон №126-ФЗ) [Собрание законодательства Российской Федерации, 2019] определением нового термина «обзвоны» и ввести новую ст. 44.2 с названием «Обзвоны по сети подвижной радиотелефонной связи» по аналогии со ст. 44.1 «Рассылка по сети подвижной радиотелефонной связи» для унификации российского права и усиления правовых возможностей защиты граждан от телефонных мошенников, т.к. сейчас именно противоправные массовые звонки на телефонные номера граждан являются единственным социально-экономическим явлением никак не урегулированным законодательством Российской Федерации при том, что в соответствии со ст. 53 Закона №126-ФЗ сведения об абонентах, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются информацией ограниченного доступа и подлежат защите в соответствии с российским законодательством, а предоставление третьим лицам сведений об абонентах-гражданах не может осуществляться без их согласия.

Абоненты как пользователи услуг связи (п. 1 ст. 2 Закона №126-ФЗ) в настоящее время не защищены (п. 2 ст. 62 Закона №126-ФЗ) от наглых обзвонков недобросовестных коммерсантов и мошенников, поскольку данный закон даже не предусматривает определение этого термина и разъяснений по поводу незаконности применения такого метода донесения информации до абонентов как, например, это сделано в отношении рассылки смс-сообщений (п. 3 ст. 44.1 Закона №126-ФЗ).

Таким образом, гражданин России совершенно не защищен государством от вторжения в свою личную жизнь злоумышленников путем их навязчивых звонков на свой персональный телефон по причине несовершенства законодательства, а именно:

- не защищен Законом №152-ФЗ («О персональных данных»), т.к. «голые» абонентские номера телефонов, по которым злоумышленники совершают свои незаконные обзвоны, не являются персональными данными, в связи с тем, что телефонные номера являются персональными данными исключительно в совокупности с дополнительной информацией, позволяющей отнести их к конкретным физическим лицам (указание ФИО, даты рождения, адреса и т.д.);

- не защищен Законом №126-ФЗ («О связи»), т.к. данное противоправное явление вообще никаким образом не отражено в данном законе;

- не защищен Законом №38-ФЗ («О рекламе»), т.к. все, что не допускается делать ст. 18 данного закона, упирается в формулировки «абонента или

адресата», которые при детальном рассмотрении сведутся к их абонентским номерам, которые, в свою очередь, опять же не являются персональными данными, и значит их противоправное использование злоумышленниками не запрещается.

Следовательно, в настоящее время ни один российский закон не обеспечивает адекватную защиту прав субъектов персональных данных от посягательств мошенников путем навязчивых тотальных телефонных обзвонков с целью поиска потенциальных жертв обмана в связи с тем, что простые граждане без привлечения правоохранительных органов не имеют возможности самостоятельно выяснить откуда, каким образом и в каком объеме мошенники получили информацию с их абонентскими номерами телефонов и ведут их незаконную обработку без их письменного согласия, а сотрудники территориальных органов Министерства внутренних дел России не реагируют на заявления граждан об этом, не считая это правонарушением, также ссылаясь на непринадлежность телефонных номеров к персональным данным. Однако, именно с этого первого телефонного звонка и начинается обман потенциальных жертв мошенников, который, в конечном итоге, способен привести к потере не только последних денег и бесценного здоровья жертв телефонного фишинга, но и их доверия к власти и веры в справедливость.

В связи с вышеизложенным, полагаем, что законодательные органы обязаны принять соответствующие поправки в Закон №152-ФЗ, Закон №126-ФЗ, Закон №38-ФЗ и, тем самым, обеспечить граждан полноценной правовой базой в целях гарантирования защиты жизненно важных прав человека правоохранительными и контролирующими органами, а также в целях реализации прав каждого гражданина в гражданских судах Российской Федерации. Органам правопорядка стоит обратить особое внимание на тот факт, что насильственные преступления могут быть также разрушительны, как и насильственные, когда представляют собой посягательства на финансовое положение и психологическое благополучие граждан, оставляя их без средств к существованию и без уверенности в завтрашнем дне. Причем не имеет значения, будет ли в последующем совершен обман и хищение денег или не будет, но сам факт противоправного телефонного звонка на телефонный номер абонента должен вызывать ответственность, в том числе и потому, что наибольшей ценностью в перенасыщенный информационный век является право человека на спокойную частную жизнь без воздействия дополнительных факторов стресса из внешней среды.

Библиография

1. Аферисты заработали миллиард рублей, ставя пенсионерам липовые диагнозы (2019). Министерство внутренних дел Российской Федерации. URL: <https://мвд.рф/news/item/16952024/> (дата обращения: 26.09.2019).
2. Балагаев, Г. (2019). Помогите полиции! В Екатеринбурге следователи ищут потерпевших от центра «Глобал Мед». *Российская газета*. 17 сентября 2019. URL: <https://rg.ru/2019/09/17/reg-cfo/v-ekaterinburge-sledovateli-ishchut-poterpevshih-ot-centra-global-med.html> (дата обращения: 28.09.2019).

3. Бембеева, Б.С. (2018). Право на защиту персональных данных и различные категории персональных данных. *Право в сфере Интернета: Сборник статей, сер. «Анализ современного права»*, С. 48-61. – Москва: ООО «Издательство «СТАТУТ», 2018.

4. Бесплатное обследование в многопрофильном медцентре GLOBALMED (2019). Видеоресурс YouTube. URL: <https://youtu.be/qxL6aKa5yIk> (дата обращения: 13.10.2019).

5. Бочкарев, А. (2019). «Приема не будет»: после обысков в медцентрах «нашли» организованное преступное сообщество. Информационный портал Санкт-Петербурга «Мойка78». URL: <https://moika78.ru/news/2019-09-25/293331-priema-ne-budet-posle-obyskov-v-medtsentrah-nashli-prestupnoe-soobshhestvo/> (дата обращения: 26.09.2019).

6. Добрикова, Е. (2019). Ответственность за нарушение закона о персональных данных. Гарант: справ.-правовая система. URL: <https://www.garant.ru/actual/persona/otvetstvennost/> (дата обращения: 11.10.2019).

7. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981 г.) (1981). КонсультантПлюс: справ.-правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 25.10.2019).

8. Marzuoli A., Kingravi H.A., Dewey D. & Pienta R. (2016). Uncovering the Landscape of Fraud and Spam in the Telephony Channel. *15th IEEE International Conference on. IEEE*. 2016. pp. 853-858. (In Eng.).

9. Отчет Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2017-2018 гг. (2019). URL: https://rkn.gov.ru/docs/Otchet_o_deyatelnosti_Upolnomochennogo_organa.pdf (дата обращения: 25.10.2019).

10. Проскуракова, М.И. (2016). Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе. *Сравнительное конституционное обозрение*, 2016, №6(115), С. 84-98.

11. Регламент Европейского Парламента и Совета «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС (Общие правила защиты данных)» от 27 апреля 2016 г. (2016). URL: <https://ogdpr.eu/ru/gdpr-2016-679> (дата обращения: 25.10.2019).

12. Собрание законодательства Российской Федерации (2019). URL: <http://www.szrf.ru/szrf/oglavlenie.phtml?md=0&nb=100> (дата обращения: 5.10.2019).

13. Терещенко, Л.К. (2018). Государственный контроль в сфере защиты персональных данных. *Право. Журнал Высшей школы экономики*, 2018, №4, С. 142-161.

14. Choi K., Lee J.-l. & Chun Y.-T. (2017). Voice phishing fraud and its modus operandi. *Security Journal*, 2017, Vol. 30, №2: 454-466. (In Eng.).

References

1. Aferisty zarabotali milliard rubley, stavya pensioneram lipovyye diagnozy [Scammers have earned a billion rubles, giving pensioners fake diagnoses] (2019). The Ministry of Internal Affairs of the Russian Federation. (In Russ.). Retrieved September 26, 2019, from: <https://mvd.rf/news/item/16952024/>.

2. Balagaev, G. (2019). Pomogite politzii! V Ekaterinburge sledovateli ishchut poterpevshikh ot tsentra «Global Med». [Help the police. In Yekaterinburg, investigators are looking for victims from the center «Global Med»]. *Rossiyskaya gazeta – RG.RU*. September 17, 2019. (In Russ.). Retrieved September 28, 2019, from: <https://rg.ru/2019/09/17/reg-cfo/v-ekaterinburge-sledovateli-ishchut-poterpevshih-ot-centra-global-med.html>.

3. Bembeeva, B.S. (2018). Pravonazashchitupersonal'nykhdannyykhirazlichnyyekategoriipersonal'nykhdannyykh [The right to protection of personal data and various categories of personal data]. *Pravo v sfere Interneta: Sbornikstatey, ser. «Analiz sovremennogo prava»* [Internet Law: Collection of articles, ser. «Analysis of modern law»], pp. 48-61. – Moskva: OOO «Izdatel'stvo «STATUT»» [Moscow: STATUT Publishing House LLC], 2018. (In Russ.).

4. Besplatnoe obsledovaniye v mnogoprofil'nom medtsentre GLOBALMED [Free examination at the GLOBALMED Multidisciplinary Medical Center] (2019). Video resource YouTube. (In Russ.). Retrieved October 13, 2019, from: <https://youtu.be/qxL6aKa5yIk>.

5. Bochkarev, A. (2019). «Priyema ne budet»: posle obyskov v medtsentrakh «nashli» organizovannoye prestupnoye soobshchestvo [«There will be no reception»: after searches in medical centers «found» an organized criminal community]. *Informatsionnyy portal Sankt-Peterburga «Moyka78»* [Information portal of St. Petersburg «Moyka78»]. (In Russ.). Retrieved September 26, 2019, from: <https://moika78.ru/news/2019-09-25/293331-priema-ne-budet-posle-obyskov-v-medtsentrah-nashli-prestupnoe-soobshchestvo/>.

6. Dobrikova, E. (2019). Otvetstvennost' za narusheniye zakona o personal'nykhdannyykh [Responsibility for violation of personal data law]. *Garant: legal reference system*. (In Russ.). Retrieved October 11, 2019, from: <https://www.garant.ru/actual/persona/otvetstvennost/>.

7. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28/01/1981) (1981). Council of Europe Portal. Retrieved October 25, 2019, from: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

8. Marzuoli A., Kingravi H.A., Dewey D. & Pienta R. (2016). Uncovering the Landscape of Fraud and Spam in the Telephony Channel. *15th IEEE International Conference on. IEEE*. 2016. pp. 853-858.

9. Otchet Federal'noi sluzhby po nadzoru v sfere svyazi, informatsionnykh tekhnologiy I massovykh kommunikatsiy (Roskomnadzor) o deyatel'nosti Upolnomochennogo organa po zashchite prav sub'ektov personal'nykh dannyykh

za 2017-2018 gg. [Report of the Federal Service for Supervision of Communications, Information Technologies and Mass Communications (Roskomnadzor) on the activities of the Authorized Body for the Protection of the Rights of Personal Data Subjects for 2017-2018] (2019). (In Russ.). Retrieved October 25, 2019, from: https://rkn.gov.ru/docs/Otchet_o_deyatelnosti_Upolnomochennogo_organa.pdf.

10. Proskuryakova, M.I. (2016). Personal'nyye dannyye: rossiiskaya i german-skayanatsional'nyye modeli konstitutsionno-pravovoyzashchity v sravnitel'noy perspektive [Personal data: Russian and German national models of constitutional protection in a comparative perspective]. *Sravnitel'noe Konstitutsionnoe Obozrenie [Comparative Constitutional Review]*, 2016, №6(115): 84-98. (In Russ.).

11. Regulation (EU) 2016/679 of the European Parliament and of the Council «On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)» of April 27, 2016 (2016). Retrieved October 25, 2019, from: <https://ogdpr.eu/en/gdpr-2016-679>.

12. Sobraniye zakonodatel'stva Rossiyskoy Federatsii [Collection of the legislation of the Russian Federation] (2019). (In Russ.). Retrieved October 5, 2019, from: <http://www.szrf.ru/szrf/oglavlenie.phtml?md=0&nb=100>.

13. Tereshchenko, L.K. (2018). State Control in Personal Data Protection. *Law. Journal of the Higher School of Economics*, 2018, №4: 142-161. (In Russ.).

14. Choi K., Lee J.-l. & Chun Y.-T. (2017). Voice phishing fraud and its modus operandi. *Security Journal*, 2017, Vol. 30, №2: 454-466.