Научная статья
УДК 343.3/7.

МЕХАНИЗМ ПРОТИВОДЕЙСТВИЯ БЕСКОНТРОЛЬНОМУ РАСПРОСТРАНЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ, СПОСОБСТВУЮЩЕМУ СОВЕРШЕНИЮ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ НА ПРАВА И ЗАКОННЫЕ ИНТЕРЕСЫ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Алла Васильевна Ендольцева[1], Юлия Владимировна Ендольцева[2]
[1] Московский университет МВД России имени В. Я. Кикотя, Москва, Россия
[2] Всероссийский научно-исследовательский институт МВД России, Москва, Россия
[1] allaend2015@mail.ru, [2] sivelllinn@gmail.com

Аннотация. В настоящей статье авторы отмечают, что основой правового механизма противодействия бесконтрольному распространению персональных данных и их незаконному использованию является предупреждение таких противоправных деяний. Особенностью превентивных мер в данном случае является то, что они представляют собой совокупность различных методов противодействия, прежде всего технических, организационных, правовых, включая также воспитательные, образовательные и другие меры. Авторы акцентировали свое внимание на изменениях, внесенных в последние годы в Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», предложениях других ученых, направленных на его дальнейшее совершенствование, обозначили собственное видение по развитию уголовно-правового противодействия совершению преступлений, связанных с незаконными действиями по собиранию, распространению и использованию персональных данных.

Ключевые слова: персональные данные, субъект персональных данных, распространение персональных данных, бесконтрольное распространение, защита персональных данных.

Для цитирования: Ендольцева А. В., Ендольцева Ю. В. Механизм противодействия бесконтрольному распространению персональных данных, способствующему совершению преступных посягательств на права и законные интересы субъектов персональных данных // Вестник Уфимского юридического института МВД России. 2023. № 3 (101). С. 67–73.

Original Article

MECHANISM TO COUNTER THE UNCONTROLLED DISSEMINATION OF PERSONAL DATA FACILITATING THE COMMISSION OF CRIMINAL INFRINGEMENTS OF RIGHTS AND LEGITIMATE INTERESTS OF PERSONAL DATA SUBJECTS

Alla V. Endoltseva[1], Yulia V. Endoltseva[2]
[1] Moscow University of the Ministry of Internal Affairs of Russia
named after V. Ya. Kikot, Moscow, Russia
[2] National Research Institute of the Ministry of Internal Affairs of Russia, Moscow, Russia
[1] allaend2015@mail.ru, [2] sivelllinn@gmail.com

Abstract. In this article the authors note that the basis of the legal mechanism to counter the uncontrolled dissemination of personal data and their illegal use is the prevention of such illegal acts. The peculiarity of preventive measures in this case is that they consist of a combination of different methods of counteraction, primarily technical, organizational, legal, including also educational, educational and other measures. The authors focused on the changes made in recent years to the Federal Law of July 27, 2006 No. 152-FZ "On Personal Data", proposals of other scientists aimed at its further improvement, outlined their own vision for the development of criminal legal action to prevent the commission of offences related to unlawful actions to collect, disseminate and use personal data.

© Ендольцева А. В., Ендольцева Ю. В., 2023

Keywords: personal data, subject of personal data, dissemination of personal data, uncontrolled dissemination, protection of personal data.

For citation: Endoltseva A. V., Endoltseva Yu. V. Mechanism to counter the uncontrolled dissemination of personal data facilitating the commission of criminal infringements of rights and legitimate interests of personal data subjects // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2023. No 3 (101). P. 67–73. (In Russ.)

В главе 2 Конституции Российской Федерации «Права и свободы человека и гражданина» закреплены важные положения, обуславливающие необходимость государственной защиты персональных данных, отыскания способов и средств противодействия их бесконтрольному распространению и незаконному использованию:

1) «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» (ст. 23);

2) «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» (ч. 1 ст. 24);

3) «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ч. 4 ст. 29);

4) «Каждый имеет право на возмещение государством вреда, причиненного незаконными действиями (или бездействием) органов государственной власти или их должностных лиц» (ст. 53).

В соответствии с этими постулатами любое незаконное посягательство на частную жизнь каждого человека, находящегося на территории Российской Федерации, в том числе незаконное собирание, распространение, хищение информации о лице и использование ее в преступных целях, влечет за собой юридическую ответственность, установленную законодательством Российской Федерации. А если данные правонарушения были следствием незаконных действий (бездействия) органов государственной власти и их должностных лиц, то, помимо ответственности, Конституция гарантирует также и возмещение государством вреда потерпевшему.

Основой правового механизма противодействия противоправным действиям, в том числе бесконтрольному распространению персональных данных и их незаконному использованию, являются превентивные меры, направленные на предупреждение общественно опасных деяний.

В соответствии с пунктом 2 статьи 2 Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» профилактика правонарушений есть совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения.

Незаконное получение, распространение и использование персональных данных являются одной из причин роста совершаемых правонарушений и преступлений в различных сферах общества. На основе изученной литературы и практических случаев можно сделать выводы о целях противоправного получения персональных данных:

– с помощью персональных данных можно получить доступ к аккаунтам и устройствам конкретного пользователя для использования их в своих, в том числе (и чаще всего) преступных целях;

– с помощью персональных данных можно более точно составить фишинговое письмо, что увеличит вероятность выполнения потерпевшим желаемых злоумышленником действий;

– персональные данные могут быть использованы как средство совершения многих преступлений, а также иных правонарушений.

Способами получения персональных данных злоумышленниками являются:

– взлом баз данных различных организаций и государственных органов, органов местного самоуправления и т. д.;

– фишинговые рассылки;

– инсайдерские утечки;

– поиск в браузерах и социальных сетях открытых персональных данных;

– покупка персональных данных в Даркнете и др.

Сложность состоит в том, что перечень персональных данных является открытым. Это означает, что к ним можно отнести любые сведения, так или иначе относящиеся к конкретному человеку, позволяющие его идентифицировать. Вместе с тем можно выделить основные категории персональных данных:

– общая информация о личности (ФИО, дата рождения, место рождения, пол, образование, место работы, ИНН, СНИЛС и т. д.);

– специальная информация о личности (раса, национальность, религия, состояние здоровья и т. д.). Обработка данных сведений возможна в исключительных случаях с письменного согласия субъекта;

– биометрические данные лица (ДНК, отпечатки пальцев, сетчатка глаза и т. д.).

В последние годы в законодательство Российской Федерации были внесены изменения, касающиеся распространения персональных данных, поскольку ранее регулировались лишь вопросы, связанные с обработкой персональных данных. В Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ № 152) в 2020 г. было введено понятие персональных данных, разрешенных субъектом персональных данных к распространению, регламентированы особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения. Обобщая нововведения, отметим, что теперь для распространения персональных данных, помимо общего согласия на обработку, нужно получать отдельное согласие на их распространение. Без такого согласия любое распространение персональных данных признается незаконным. Требования к содержанию данного согласия установлены Приказом Роскомнадзора от 24 февраля 2021 г. № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». Еще одним важным нововведением является то, что согласие на распространение персональных данных прекращает действовать с момента, когда оператор получил требование об отмене согласия. При этом субъект персональных данных вправе обратиться не только к оператору, но и к любому лицу, которому было дано согласие на распространение, а также к другим лицам, которые получили право обрабатывать эти данные в будущем. Данные нововведения усилили защиту персональных данных лиц от их бесконтрольного и массового распространения в открытых источниках, что позволяет предупреждать их незаконное использование.

Для дальнейшего усиления защиты персональных данных необходимо применять совокупные способы и методы.

Основной метод защиты персональных данных – это, несомненно, технический. Речь идет о совершенствовании программ мероприятий по защите программного обеспечения от несанкционированного доступа. Для данного направления необходимо привлечение IT-специалистов, которые в результате своих специальных познаний могут моделировать угрозы, определять степень защищенности персональных данных и, конечно, обеспечивать их безопасность путем своевременной разработки и совершенствования технических возможностей защиты. Это важно потому, что вопросы защиты персональных данных во многом зависят от объективного технического обеспечения информационной безопасности [1].

Для разработки механизма технического противодействия бесконтрольного и незаконного распространения персональных данных и, как следствие, предотвращения совершения преступлений и правонарушений, совершаемых с помощью использо-

вания персональных данных, необходимо развивать направление политики в данной области, которое, как мы видим, в настоящее время становится одним из приоритетных. Сюда можно отнести и различные социальные льготы для специалистов, в том числе возможность получения бесплатного образования в данной сфере, обеспечение производственных практик, помощь в дальнейшем трудоустройстве на территории Российской Федерации с достойным уровнем оплаты труда, организацию курсов повышения квалификации и пр.

Кроме того, с учетом быстрого технического прогресса, внедрения цифровизации в бытовую жизнь граждан, в предоставление государственных, образовательных и медицинских услуг, судопроизводство и т. д., где вся система цифровизации строится на обработке персональных данных, необходимо повышать уровень технического просвещения как обычных граждан, так и должностных лиц. В первую очередь этого можно достичь путем предоставления образовательных услуг (от начального образования человека до отдельных дополнительных курсов и курсов повышения квалификации). Данные возможности должны быть доступны даже для малообеспеченных слоев населения. Возможность получения таких специальных познаний, а также знание цели их получения – защиты персональных данных, предотвращения совершения деяний, запрещенных законом, должны быть в свободном доступе для всех граждан, и как можно шире распространены всеми возможными способами (с использованием СМИ, сети Интернет, упоминания в кинофильмах, сериалах, телепередачах, рекламных роликах и стендах, телефонных средствах связи и т. д.).

Считаем, что данные положения должны быть закреплены на уровне подзаконных актов соответствующими указами Президента Российской Федерации, постановлениями Правительства Российской Федерации, приказами министерств и ведомств, а также локальными актами различных органов, организаций и объединений.

Данный метод должен работать в совокупности с организационным и юридическим (правовым) методом.

К организационным способам защиты можно отнести следующие действия:

– разработка локальных нормативных актов в области защиты персональных данных (положения о персональных данных, список работников, имеющих доступ к персональным данным, инструкции о служебном расследовании фактов разглашения персональных данных, инструктаж по защите персональных данных с указанием конкретных мер, необходимых для их защиты, журнал контроля использования персональных данных и т. д.);

– допуск к персональным данным только строго определенного внутренними локальными актами круга лиц;

– назначение ответственного работника за выполнение правовых норм в области защиты персональных данных;

– установление внутреннего контроля за соблюдением правил обработки персональных данных;

– ознакомление работников, обрабатывающих персональные данные, с нормативными правовыми актами и локальными актами в сфере защиты персональных данных и проведение периодических проверок знаний работников в данной области;

– обеспечение пропускного режима;

– размещение рабочих мест таким образом, чтобы сохранить конфиденциальность персональных данных;

– программная защита данных;

– проведение профилактических мероприятий по недопущению разглашения персональных данных и т. д.

Адекватное выстраивание процессов в организациях, осуществляющих обработку персональных данных на постоянной основе, создаст необходимые условия для объективной защиты персональных данных [2] (разработка и внедрение юридическими лицами (государственными органами, организациями и пр.), индивидуальными предпринимателями политики обработки персональных данных и их распространения,

положений о защите персональных данных, издание приказов о назначении ответственных лиц, осуществление контрольных мероприятий в данной сфере).

В любой организации и органе, чья работа связана в той или иной мере с обработкой персональных данных, должны быть составлены и распространены методические рекомендации о работе с персональными данными, а также со способами их защиты. Руководителями органов и организаций должны приглашаться соответствующие специалисты для проведения занятий по защите персональных данных. Данная обязанность работодателя также должна быть закреплена на законодательном уровне (в Трудовом кодексе Российской Федерации, а также в иных нормативных правовых актах в сфере трудоустройства).

В Трудовом кодексе Российской Федерации следует дополнить статью 57 «Содержание трудового договора» отдельным пунктом, в котором необходимо указать условие «об обязанности работника не разглашать ставшие известными в результате трудовой деятельности сведения о персональных данных лиц без их согласия, полученного в установленном законом порядке, кроме случаев выполнения возложенных законодательством Российской Федерации полномочий и обязанностей».

Кроме того, для должностных инструкций всех работников и сотрудников, с которыми заключаются трудовые договоры и служебные контракты, следует установить обязательность положений о недопустимости ознакомления с персональными данными, а также их разглашении без соответствующего доступа к ним и без согласия лиц (субъектов персональных данных). Помимо этого, в локальных нормативных актах органов и организаций должна быть обязательно прописана ответственность за нарушение данного положения, о чем под подпись должны быть ознакомлены все работники и сотрудники.

Такое же правило, по мнению авторов, должно быть установлено законом для всех гражданско-правовых договоров (договоры об оказании услуг, абонентские договоры и пр.).

Кроме того, при изучении литературы по исследуемой теме нас заинтересовали предложения некоторых авторов по защите персональных данных. Так, Е. Г. Дмитриева в своей статье «Проблемы защиты персональных данных в цифровом мире и пути их решения» предлагает дополнить ФЗ «О персональных данных» «требованием о том, что оператор должен разместить на сайте или платформе типовую форму, позволяющую отозвать согласие на обработку и распространение персональных данных в электронном виде непосредственно на самой платформе» [3, с. 20]. Таким положением целесообразно дополнить статью 18.1 ФЗ «О персональных данных». Заслуживают внимания ее предложения об ограничении на законодательном уровне сроков хранения персональных данных и проведении проверки за соблюдением этих сроков, по организации проведения внешних независимых проверок и расследований случаев утечки и неправомерного использования персональных данных, а также создание упрощенных внесудебных механизмов защиты граждан в случаях неправомерного использования персональных данных.

Мы предлагаем пути совершенствования уголовно-правовых мер по противодействию совершению преступлений, связанных с незаконным собиранием, распространением и использованием персональных данных.

Учитывая, что все больше видов преступлений совершаются с помощью незаконного использования персональных данных потерпевших или их близких лиц, полагаем, что назрела необходимость признать обстоятельством, усиливающим общественную опасность деяния, совершение преступления посредством использования персональных данных потерпевшего и (или) его близких родственников, родственников или близких лиц, и предлагаем дополнить часть 1 статьи 63 УК РФ «Обстоятельства, отягчающие наказание» таким самостоятельным пунктом.

Отмечая увеличение количества совершаемых преступлений посредством исполь-

зования персональных данных, зачастую полученных незаконным путем, или из открытых источников, где данная информация была размещена без соответствующего согласия субъекта персональных данных, считаем, что незаконное собирание и распространение персональных данных имеют большую общественную опасность и должны предусматриваться законом в виде квалифицированного состава преступления, в связи с чем предлагаем дополнить статью 137 УК РФ следующей частью:

«1.1. Незаконное собирание или распространение сведений о персональных данных лица без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации –

наказываются штрафом в размере до двухсот пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до четырех лет или без такового, либо арестом на срок до пяти месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до четырех лет.».

Отметим, что закрепления в уголовном законе понятия «частная жизнь» на данный момент нет, как и не существует закрепленного законом перечня персональных данных. Полагаем, что следует дополнить положения Постановления Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145 Уголовного кодекса Российской Федерации)». В целях обеспечения единообразного применения судами законодательства об ответственности за совершение данных преступлений в Постановлении Пленума Верховного Суда Российской Федерации следует прописать понятие частной жизни и понятие персональных данных, на которые следует ориентироваться судам при квалификации преступлений. Также в данном Постановлении следует указать перечень персональных данных, таких как: ФИО, дата и место рождения, гражданство, место регистрации, место проживания, СНИЛС, ИНН, образование, профессии, специальности, сведения о составе семьи, отношение к воинской обязанности, трудовая деятельность (в том числе стаж), наличие либо отсутствие судимости, состояние здоровья, биометрические данные и т. д.

Кроме того, учитывая активный рост совершения определенных видов преступлений, полагаем, что совершение преступлений посредством использования персональных данных потерпевшего и (или) его близких родственников, родственников или близких лиц необходимо закрепить в уголовном законе и как квалифицирующие составы, а именно:

– часть 2 статьи 158 «Кража» дополнить пунктом:

«е) посредством использования персональных данных потерпевшего и (или) его близких родственников, родственников или близких лиц, – …»;

– часть 2 статьи 159 «Мошенничество» УК РФ представить в виде:

«2. Мошенничество, совершенное группой лиц по предварительному сговору и (или) посредством использования персональных данных потерпевшего и (или) его близких родственников, родственников или близких лиц, а равно с причинением значительного ущерба гражданину, – …»;

– часть 2 статьи 163 «Вымогательство» дополнить пунктом:

«д) посредством использования персональных данных потерпевшего и (или) его близких родственников, родственников или близких лиц, – …».

В заключение сделаем вывод о том, что механизм противодействия бесконтрольному распространению персональных данных и незаконному их использованию будет работать только при совокупности подходов к его формированию. Необходимо разра-

ботать и обеспечить такой баланс методов противодействия, который совместит технические, организационные и правовые методы, не оставив в стороне воспитательные, образовательные, социально-экономические и другие меры.

СПИСОК ИСТОЧНИКОВ

1. Бражник Т. А. Правовые вопросы обеспечения информационной безопасности личности // Информационное право. 2018. № 4. С. 17–21.

2. Жемчугов Н. Защита персональных данных в цифровую эпоху: судебная практика в РФ и практические рекомендации // ЭЖ-Юрист. 2022. № 21 (1222).

3. Дмитриева Е. Г. Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. 2021. № 3. С. 18–23.

REFERENCES

1. Brazhnik T. A. Legal issues of information security of the person // Information Law. 2018. No 4. P. 17–21. (In Russ.).

2. Zhemchugov N. Protection of personal data in the digital age: judicial practice in the Russian Federation and practical recommendations // EJ-Lawyer. 2022. 21 (1222). (In Russ.).

3. Dmitrieva E. G. Problems of personal data protection in the digital world and ways of their solution // Law and business. 2021. No 3. P. 18–23. (In Russ.)

Информация об авторах:

А. В. Ендольцева, доктор юридических наук, профессор;

Ю. В. Ендольцева, кандидат юридических наук.

Information about the authors:

A. V. Endoltseva, Doctor of Law, Professor;

Yu. V. Endoltseva, Candidate of Law.

Статья поступила в редакцию 29.03.2023; одобрена после рецензирования 24.05.2023; принята к публикации 15.09.2023.

The article was submitted 29.03.2023; approved after reviewing 24.05.2023; accepted for publication 15.09.2023.