РОССИЙСКОЕ ПРАВО: ИСТОРИЯ И СОВРЕМЕННОСТЬ

УДК 34.09
ББК 67.0

ПРОБЛЕМА «КРАЖИ ЛИЧНОСТИ» В РОССИЙСКОМ ПРАВЕ

А. А. Васильев, В. В. Мухопад
Алтайский государственный университет (Барнаул, Россия)

В рамках компьютеризации, роботизации всех сфер общественной жизни все острее встает вопрос о внедрении данных технологий в сферу правотворческой и правоприменительной деятельности. Данное явление уже широко развивается за рубежом и приобрело собственное устойчивое наименование — «legal tech». Однако, несмотря на свежесть и актуальность данной идеи, имеются серьезные противоречия, связанные с процедурой претворения ее в жизнь. Поскольку все сферы жизни сегодня прочно проходят оцифровку, неминуемо столкновение индивидов с процедурой «цифровой идентификации» — фиксирования своего пребывания на сайте, иначе пользователь остается неавторизированным, а значит, «невидимым» для создания отношений, в том числе в рамках правового поля.

В статье рассматривается проблема кражи персональных данных граждан посредством интернета, которая получила в юридической науке название «кража личности». Проводится анализ превентивных мер, осуществляемых в различных государствах. Авторы рассматривают теории защиты персональных данных и предлагают меры по совершенствованию правового поля. Приводятся данные зарубежных исследований, рассматривается такая категория, как «право на забвение», и возможность ее реализации в российской действительности. Предлагаются решения пробельных аспектов защиты персональных данных.

Ключевые слова: персональные данные, кража личности, идентификация, правовой статус, право на забвение.

THE PROBLEM OF “IDENTITY THEFT” IN RUSSIAN LAW

A. A. Vasilev, V. V. Mukhopad
Altay State University (Barnaul, Russia)

All spheres of society are being computerized and robotized. Legislation and the application of law are no exception. This phenomenon has been developing abroad for a long time. It has acquired its own stable name — “legal tech”. However, it is not easy to implement this idea. The introduction of a procedure for “digital identification” of people to record their presence on the site is inevitable. Otherwise, the user remains unauthorized, which means “invisible” to other users. This makes it impossible to conclude contracts on the Internet.

The article describes the problem of theft of personal data of citizens via the Internet, which is called “identity theft”in legal science. The analysis of preventive measures in different countries is carried out. The authors consider the theories of personal data protection and propose measures to improve the legal

framework. This category is considered as the “right to be forgotten” and the possibility of its implementation in Russian reality. We offer solutions to the gap aspects of personal data protection.

Keywords: personal data, identity theft, identification, legal status, right to be forgotten.

Doi: https://doi.org/10.14258/ralj(2020)3.1

Современные характеристики сети Интернет ни технически, ни юридически не обеспечивают достоверности идентификации пользователя. Учетная запись в любом сервисе, будь то электронная почта, социальная сеть или блог, даже если она содержит публично отображаемые имя и фотографию (особенно в сетях, где регистрация пользователя производится путем входа через аккаунты Facebook, Gmail и прочие, при которых данные из одной сети переносятся в другую), вовсе не обязательно создана или предоставлена именно этим лицом. Иными словами, правовая коммуникация интернет-пользователей всегда опосредована: двух лиц перманентно разделяет средство связи (компьютер, телефон или иной гаджет).

Итак, есть основания полагать, что за именем и изображением пользователя не всегда скрывается сам пользователь. Не исключено, что данный аккаунт управляется совершенно другим человеком, а цели, ради которых он это осуществляет, нередко могут противоречить нормам не только права, но и морали.

В литературе это явление получило название *identity theft* («кража личности»): при этом лицо, совершившее «кражу», снимает с себя и накладывает на потерпевшего ответственность за последствия своих действий.

Наиболее распространенным видом «кражи личности» в России признается так называемый фишинг (происходит от англ. *fish* — выуживание, вылавливание) — один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям, данным лицевых счетов и банковских карт (фишинг на сайтах, покупки на интернет-площадках, фишинговые приложения, телефонный фишинг и др.).

По данным исследования компании InfoWatch (цит. по: [1]), в 2019 г. число «краж личностей» в мире за год составило более 13,7 млрд. При этом любое интернет-взаимодействие с органами власти (через портал «Госуслуги», официальные сайты органов государственной власти), медицинскими учреждениями требует ввода личных данных.

В большинстве стран право на защиту персональных данных признается фундаментальным, конституционным, вытекающим из права на неприкосновенность частной жизни [2, p. 135]. Так, закон о конфиденциальности и безопасности персональных данных, принятый в 2014 г. в США, предупреждает изъятие личной информации, обеспечивает конфиденциальность и возлагает на правоохранительные органы обязанность по выявлению, пресечению и профилактике правонарушений данной категории [3]. Также данный закон впервые предусматривает наказание в виде пяти лет лишения свободы для тех, кто умышленно нарушает безопасность личной информации. Например, в Бразилии, стране-рекордсмену по количеству интернет-пользователей, правками, внесенными в закон о защите персональных данных, предусмотрена личная ответственность компаний и частных лиц, занимающихся автоматизированной обработкой персональных данных.

В европейских государствах сложилось единое правовое регулирование защиты персональной информации. Отметим, что необходимость принятия законов о защите персональных данных была обусловлена факторами развития внешнеторговых связей. Например, принятие в 1998 г. Закона «О защите информации» в Великобритании было вызвано требованиями Директивы о защите информации Европейского союза и ратификацией Советом Европы Конвенции «О защите физических лиц в отношении автоматизированной обработки данных личного характера» и Европейской конвенции «О защите прав и основных свобод человека».

Закон «О защите информации» Великобритании предусматривает защиту информации частных лиц, которая хранится в компьютерных банках данных, от неправомерного доступа и некорректного использования, а также учетных записей государственных учреждений и частных структур, в которых содержится персональная информация о частном лице. В целях обеспечения такой защиты в Великобритании действует информационный ресурс — Регистратор защиты данных, который содержит

меры ответственности, в основном гражданско-правового характера, при использовании недостоверной информации и причинения ущерба частному лицу. Кроме того, работа по охране персональных данных проводится независимым агентством Великобритании — Комиссариатом по защите информации. Закон устанавливает санкцию в виде штрафа в размере до пятисот тысяч фунтов стерлингов за «утечку информации персонального характера» [4].

Во Франции правовое регулирование безопасности хранения персональных данных обеспечивается Законом «Об обработке данных, файлах данных и индивидуальных свободах» [5]. Данным актом вводится уголовная ответственность за незаконный сбор и хранение персональной информации, предусматривающая лишение свободы на срок до пяти лет.

Примечательно, что вразрез с официальной политикой государств по защите персональных данных, их сокрытия и недопустимости распространения без согласия владельца, зарубежными учеными предлагаются иные способы, противоположные, защиты названного права. Так, Л. Лопаки, ученый из Калифорнийского университета, основывает свои умозаключения на теории идентификации человека, предложенной профессором Р. Кларком. Согласно данной теории, вся человеческая идентификация соответствует одной модели — не совокупности качественных и количественных характеристик, а результатам сопоставления характеристик одного человека с другим человеком в наблюдении по поводу того, один ли это человек. Из этой теории следует, что персональные данные, используемые для идентификации в системе, такие как номер полиса СНИЛС, девичья фамилия матери, дата рождения и прочие, должны быть известны широкому кругу лиц, участвующих в какой-либо интернет-среде или социальной сети.

Авторы теории опираются на то, что такие персональные данные используются индивидом широко в большинстве интернет-отношений, следовательно, глупо полагать, что данная информация может оставаться секретной. Сторонники данного подхода считают, что политика засекречивания персональных данных с целью недопущения их использования в преступных целях третьими лицами обречена на провал.

В качестве альтернативного решения ученые предлагают создание системы, с помощью которой лица, обеспокоенные гипотетической кражей личных данных, могут зарегистрировать эти данные в государственном органе (учреждении), а последний обеспечит защищенность имени, персональных данных и несекретной контактной информации путем опубликования их на сайте открытого доступа. Таким образом, организации, получившие, например заявление лица о выдаче кредита или иным образом контактирующие с персональными данными индивида посредством интернета, будут иметь возможность связаться с действительным владельцем персональных данных, чтобы убедиться, что именно он является контрагентом, заявителем или адресантом.

По мнению сторонников данной теории, таким способом организации будут освобождены от ответственности за неправильную идентификацию, а лица — носители персональных данных — смогут контролировать процесс своей собственной идентификации, особенно в кредитных операциях, без существенной потери конфиденциальности [6].

Анализ практического опыта зарубежных стран, касающегося защиты персональных данных, позволяет заключить, что одним из неопровержимых достоинств является наличие специализированных органов, предоставляющих защиту персональных данных субъектов информационного взаимодействия, что позволяет создать более качественный механизм ее обеспечения.

Мы полагаем, что данная идея вполне логична, поскольку создание всеобщей базы данных будет сопряжено с возможностью проверки намерений стороны при заключении соглашений в интернете в телефонном разговоре. Однако, анализируя данные положения с учетом российской действительности, видим, во-первых, что нет никакой гарантии защиты этой базы от утечки персональных данных посредством стороннего взлома, кибер-атаки и т. д. Во-вторых, в гражданско-правовых отношениях одна из сторон может являться более слабой в силу характера правоотношения (выдача кредита, микрозайма, ссуды и т. д.). В таком случае организация-контрагент может быть не заинтересована в уточнении идентификации личности. Также следует отметить, что для крупных организаций (масс-маркеты, банковские холдинги и др.), которые заключают большое количество соглашений ежедневно, обзвон контрагентов может существенно замедлить исполнение сделки, потребует дополнительных ресурсов, затормозит развитие интернет-продаж и оказание интернет-услуг.

Еще одним вопросом защиты персональных данных является реализация лицом-владельцем персональных данных так называемого права на забвение. Данное право появилось от английского *right to be forgotten*, которое изначально было закреплено в 1995 г. в Директиве № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [7]. Положениями данного документа определено, что государства — члены Европейского союза гарантируют каждому субъекту персональных данных право требовать от оператора исправления, стирания или блокирования данных, обработка которых не соответствует нормам, за исключением случаев, когда это невозможно или повлечет за собой несоразмерные усилия. А в Хартии Европейского союза «Об основных правах» от 2007 г. было введено право каждого получать доступ к собранным в отношении него данным и добиваться устранения в них ошибок [8].

В отечественном законодательстве отсылка к праву на забвение содержится в Федеральном законе «Об информации, информационных технологиях и о защите информации» [9]. В частности, оператор поисковой системы по требованию гражданина обязан прекратить выдачу сведений об указателе страницы сайта в интернете, позволяющих получить доступ к информации о заявителе. Примечательно, что об удалении непосредственно данных речи не идет. С одной стороны, это логично, поскольку с технической точки зрения удаление информации из интернета является неосуществимым в силу возможности ее многократного копирования и сохранения на разных устройствах.

В качестве оснований для осуществления права на забвение (точнее будет использование формулировки «право на удаление данных») перечисляются следующие:

1) информация распространяется с нарушением законодательства РФ. При этом закон не содержит ориентировочного перечня таких нарушений, следовательно, расширительное толкование данной нормы требует включения наработок судебной практики. В противном случае возможно двоякое толкование юридических фактов, влекущих применение данного пункта.

Интересна при этом широко обсуждаемая позиция Московского городского суда, который указал, что «лицо, оказывающее услуги по хранению информации и обеспечению доступа к ней, не несет гражданско-правовой ответственности за распространение информации, если оно не могло знать о незаконности такого распространения» [10]. Таким образом, вопрос грани «законного» и «незаконного» распространения информации остается открытым;

2) информация является недостоверной;

3) информация является неактуальной;

4) информация является утратившей значение для заявителя в силу последующих событий или действий заявителя.

В отношении данных пунктов снова возникают резонные вопросы: какова процедура проверки достоверности, актуальности; кто вправе оценивать информацию по данным критериям; насколько объективной будет такая оценка и т. д.

На сегодняшний день оператор поисковой системы вправе сам определять достоверность, актуальность, значение информации и в течение 10 дней с момента обращения гражданина с требованием об удалении транслировать ему свое решение. В случае несогласия с решением оператора гражданин вправе обратиться в суд. Данное положение кажется нам не весьма корректным, поскольку порой даже сами суды не в силах оценить соответствие информации вышеуказанным критериям.

Также заслуживает внимания вопрос удаления информации, которая на момент ее размещения соответствовала всем критериям. В этом смысле авторы видят возможности субъектов «искажать» события. Соответственно, следует вести речь о столкновении частных интересов и общественной значимости. Ведь в случае безоговорочного удаления любых персональных данных по требованию правообладателя интерес в использовании поисковых систем может исчезнуть, как исчезнет и их основное предназначение. В позиции Суда Европейского союза по делу компании «Гугл Спейн СЛ» и «Гугл Инк.» против Испанского агентства по защите данных и Марио Костехи Гонсалеса отмечается, что «право на забвение» может быть предоставлено гражданину, только если отсутствует заинтересованность широкой общественности в доступе к данной информации; а также, если гражданин не является общественно значимой персоной [11].

Следовательно, защита персональных данных может быть ограничена в силу общественного интереса, общественной значимости данных конкретного субъекта, а также с точки зрения политической или исторической ценности информации. Сегодня российское законодательство данной ого-

ворки не содержит. Полагаем, что в случае увеличения количества рассмотрения подобного рода дел в судах формулировка правовой нормы может существенно измениться.

Кроме того, считаем важным восполнить правовой пробел и разрешить удаление информации об умершем человеке с соблюдением вышеотмеченных условий соответствия общественным интересам по требованию доверенных лиц или наследников. Особенно это касается значимых для родственников сведений о смерти, личных данных, страниц в социальных сетях.

Несомненно, что с учетом разработки touch ID, face ID, voice ID идентификация пользователя становится более надежной. Однако уже сегодня этих мер недостаточно. Кроме того, на большинстве государственных российских сайтов не предусматривается двухфакторной аутентификации с использованием кода подтверждения доступа, присылаемого в SMS.

Несмотря на то, что большинство государств уже приравняли IP-адреса к персональным данным, поскольку именно они позволяют идентифицировать устройство, с которого был осуществлен выход в интернет, российские суды пока прямо не заявляют о принятии данной позиции. Равно как не признаются на практике сегодня персональными данными и адреса электронной почты, а также фото лица при отсутствии иных данных, позволяющих его идентифицировать.

Пока суды относятся к вопросу весьма формально и считают личными данными следующие: фамилию, имя, отчество (ФИО), адрес и паспортные данные лица; размер задолженности по оплате коммунальных платежей; анкетные данные в заявлении на получение потребительского кредита; материалы пенсионного дела, трудового договора; информацию о привлечении к административной ответственности; сведения о зарегистрированных автомототранспортных средствах [12].

Нам кажется, что данный перечень требует значительного дополнения, как минимум, данными банковских счетов, логинов и электронных адресов, аккаунтов.

Полагаем, что следует определить особую правовую природу идентификационных данных и IP- и MAC-адресов как особой формы собственности, привязанной к конкретному лицу или устройству, посредством чего проблемы поиска нарушителя могут быть частично сняты. Думается, что в этой части гражданское законодательство должно быть дополнено новыми положениями.

Считаем, что проблема «кражи личности» должна решаться в рамках публичного права, с участием государства, поскольку введение лицом недостоверных, чужих данных направлено на введение в заблуждение не только владельцев сайта или контрагентов, но и, гипотетически, всех других пользователей.

Также полагаем необходимым, ориентируясь на опыт других государств, закрепить административную ответственность организаций — хранителей персональных данных, в том числе сайтов, банков и иных, за совершаемую в их базах данных кражу персональных данных, поскольку на сегодняшний день меры, предпринимаемые данными лицами, кажутся нам неэффективными в контексте развития цифровых технологий, а граждане, подвергшиеся «краже личности», не имеют возможности восстановить нарушенные права.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Количество утечек персональной информации выросло на треть. URL: https://guardinfo.online/2020/05/29/daanye-na-veter-kolichestvo-utechek-personalnoj-informacii-vyroslo-na-tret/.

2. Bouhadana I. Le droit au respect de la vie privee a l'ere du numerique dans le systeme francais // Эволюция государственных и правовых институтов в условиях развития информационного общества. М., 2012. С. 135–153.

3. Закон о конфиденциальности и безопасности персональных данных 2014 года. URL: http://www.congress.gov/bill/113thcongress/senate-bill/1897.

4. Великобритания. Защита персональных данных. URL: http://www.ucontrol.ru/new/137.

5. Act № 78–17 of 6 january 1978. On information technology, data files and civil liberties. URL: http://www.cnil.fr/fileadmin/documents/en/ACT78–17VA.pdf.

6. Lunn Lopucki. Human Identification theory and the identity theft problem. SSRN Electronic Journal. 2001. May. № 80 (1).

7. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных: Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза (принята в Люксембурге 24.10.1995) // Official Journal of the European Union. № L 281. 23.11.1995. С. 731.

8. Хартия Европейского союза об основных правах (2007/С 303/01) (Вместе с «Разъяснениями…» (2007/С 303/02)) (Принята в Страсбурге 12.12.2007) // СПС «КонсультантПлюс».

9. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

10. Апелляционное определение Московского городского суда от 08.02.2017 по делу № 33–5031/17 // СПС «КонсультантПлюс».

11. Google Spain SL and Google Inc. v. Agencia de Datos (AEPD) and Mario Costeja Gonzales [C-131/12CJEU] (Большая Палата) // Бюллетень Европейского суда по правам человека. Российское издание. 2014. N 9. С. 22–23.

12. Как суды и Роскомнадзор определяют, что является персональными данными, а что нет? URL: https://zakon.ru/blog/2020/5/24/-kak_sudy_i_roskomnadzor_rkn_opredelyayut_chto_yavlyaetsya_personalnymi_dannymi_a_cht_net.

УДК 342
ББК 67.400.7

АНТИКОРРУПЦИОННЫЕ МЕХАНИЗМЫ В РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ О МУНИЦИПАЛЬНОЙ СЛУЖБЕ

О. Л. Казанцева
Алтайский государственный университет (Барнаул, Россия)

Государственная политика последних десятилетий существенно продвинулась в формировании и законодательном закреплении антикоррупционных механизмов на муниципальной службе. Несмотря на меры, принимаемые государством по борьбе с коррупцией, ситуация в стране остается напряженной, злоупотребления публичной властью становятся системными, появляются новые формы и виды коррупции. Анализ действующего законодательства о муниципальной службе позволил сделать ряд выводов об имеющихся в этой сфере проблемах и предложить варианты их решения.

Ключевые слова: антикоррупционные механизмы, антикоррупционное законодательство, коррупция, муниципальная служба.

ANTI–CORRUPTION MECHANISMS IN RUSSIAN LEGISLATION ON MUNICIPAL SERVICE

O. L. Kazantseva
Altai State University (Barnaul, Russia)

The state policy of the last decades has made significant progress in the formation and legislative consolidation of anti-corruption mechanisms in the municipal service. Despite the measures taken by the state to combat corruption, the situation in the country remains tense, abuses of public power are becoming systemic, new forms and types of corruption appear. An analysis of the current legislation on municipal service made it possible to draw a number of conclusions about the existing problems in this area and propose options for their solution.

Keywords: anti-corruption mechanisms, anti-corruption legislation, corruption, municipal service.

Doi: https://doi.org/10.14258/ralj(2020)3.2