УДК 342.7 + 340.64:004 056.53 Вестник УрФО № 1(19) / 2016, стр. 61–67

Жарова А. К.

О СООТНОШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ С IP АДРЕСОМ. РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ

В статье рассматриваются юридические вопросы определения человека и его деятельности в Интернете по создаваемому им персональному профилю. Демонстрируется роль IP-адреса как информации, соответствующей персональным данным для идентификации человека. Сравниваются зарубежные законодательные и юридические практики, направленные на решение проблемы выявления критериев, позволяющих установить личность человека в Интернете с российской законодательной и юридической практикой. Изучаются правовые вопросы, возникающие при использовании идентификационной информации третьими лицами. В заключение автор предлагает дополнить понятие «персональные данные», определенное Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», идентификационной информацией – IP-адресом и другой технологической информацией, на основании которой возможно определить физическое лицо в сети Интернет.

Ключевые слова: *IP, идентификация человека, персональные данные, правовое регулирование.*

Zharova A. K.

ON THE RELATION OF PERSONAL DATA WITH THE IP ADDRESS. A STUDY RUSSIAN'S AND FOREIGN EXPERIENCE

In the article deals the legal questions of identification of person and his activities on the Internet. A role of identification information such as IP address on the Internet was demonstrated. The link between the IP address and personal information was determined. Foreign laws and legal practices aimed at the detection of identification criteria to establish a person's identity on the Internet with the Russian laws and legal practices were compared.

The author proposed to add in the concept of "personal data" that was defined by the Federal Law of 27.07.2006 No 152-FZ "On personal data" the identification information which are IP address and other system information on the basis of which it is possible to identify an individual on the Internet.

Keywords: *The IP, human identification, personal data, legal regulation.*

Введение

Вопрос о признаках, присущих человеку, с развитием информационных телекоммуникационных (ИТ) технологий, встает перед исследователями с новой силой. Привычное восприятие человека как общественного существа, обладающего сознанием, разумом, субъектообщественной исторической деятельностью и культурой, меняется под воздействием ИТ-технологий. Например, в сети Интернет используются технологии, которые имитируют интеллект, деятельность и сознание [12; 13], т. е. те признаки, которые были всегда присущи только человеку. Имитация человеческой деятельности аватарами[1] в Интернете описывают Реза Этемад-Сажади и Лассаад Чачем в своей статье [5].

Задолго до активной информатизации ГК РФ определил признаки, свойственные гражданско-правовой деятельности человека. Так, ГК РФ определяет, что гражданин приобретает и осуществляет права и обязанности под своим именем, которое включает фамилию и собственно имя, а также отчество, если иное не вытекает из закона или национального обычая (ст. 19 ГК РФ). Однако применение информационных технологий позволяет человеку, участвующему в интернет-отношениях, утрачивать признаки гражданских отношений, определенные законом. Такие интернет-отношения характеризуются иными, отличными от законодательно определенных признаков. Например, им свойственны виртуальность и анонимность, т. к. сами участники этих отношений виртуальны и анонимны. Анонимность (от греч. *anonymos* – безымянный). В «Толковом словаре русского языка» под анонимным физическим лицом понимается неизвестный, не подписавший своего имени [24]. Анонимность трактуется различными авторами по-разному, так, П. А. Кабанов ставит знак равенства между анонимным и деперсонифицированным лицом, «о которых ничего не известно и/или их трудно идентифицировать, либо само государство не сообщает сведения о них» [15]. Н. Н. Федосеева определяет анонимность как характеристику киберпространства, подрывающую традиционное развитие и применение права в связи с тем, что пользователь Интернета может создать киберличность или образ, совершенно не соответствующий его реальной или физической идентичности и, тем самым, уклониться от юридической ответственности [23]. В. М. Елин пишет, что в России пока еще не выработаны правовые признаки и методы определения физического лица [10; 11].

Хотя с технологической точки зрения анонимность в сети – это достаточно условное состояние, поскольку пользователь, выходящий в Интернет формально, хоть и анонимен[2], но фактически с первой активации ссылки пользователем все его действия фиксируются и обрабатываются аппаратно-программными механизмами различных провайдеров. В соответствии со ст. 10.1 ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [27] данная информация фиксируется провайдером, предоставляющим доступ в Интернет, и она хранится не менее 6 месяцев у него на сервере.

Для описания отношений анонимного человека в Интернете, выберем термин «виртуальное лицо». Виртуальное лицо – это участник юридически значимых отношений, возникающих в Интернете, в который погружается реальный субъект с персональными данными, не соответствующими действительности. Связано это с тем, что виртуальные люди не имеют свойственных человеку признаков, на основании которых другие участники интернет-отношений могли бы быть уверенными, что деятельность осуществляется именно от конкретного лица. С точки зрения права виртуальные лица необходимо рассматривать как неподлинные, а их активность как имитационную.

Преодоление анонимности рассматривается многими государствами через реализацию процедуры идентификации человека в Интернете. Особенно остро стоит вопрос об идентификации человека при оказании государственных услуг и юридического разрешения правонарушений в Интернете. Однако идентификация возможна только на основании технологических и организационно-правовых процедур, применяя которые мы можем быть уверены, что вступаем в интернет-отношения с определенным человеком.

[1] Небольшое изображение, используемое в сети Интернет пользователями для своей персонализации или определения каких-либо сетевых сервисов.

[2] Единственная привязка – это его IP-адрес. Но и здесь необходимо учитывать, что пользователь, применяя аппаратно-программное обеспечение, может создавать динамический IP, или IP может принадлежать многим пользователям.

Соотношение технологических и правовых процедур идентификации человека

Как уже было сказано выше, состояние анонимности в Интернете – это условность. Лицо неизвестно участникам отношений, но все действия данного лица фиксируются аппаратно-программными технологиями провайдеров. Полученная информация хранится от 6 месяцев до 3 лет. Так, ст. 10.1 ФЗ «Об информации, информационных технологиях и о защите информации» определяет обязанность организатора распространения информации в Интернете «хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение шести месяцев с момента окончания осуществления таких действий, а также предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации в случаях, установленных федеральными законами».

Данное требование к хранению информации было определено ранее п. 12. Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность. В данном пункте указывается, что «оператор связи обязан своевременно обновлять информацию, содержащуюся в базах данных, об абонентах оператора связи и оказанных им услугах связи. Указанная информация должна храниться оператором связи в течение 3 лет….» [22]

Сохраняемая информация может содержать данные о IP-адресе выхода в Интернет, IP-страницы сайта, может сохраняться и содержание информации, т. е. деятельность человека в сети Интернет определяется через совокупность IP-адресов: интернет-зоны, технологии, посредством которой человек вышел в Сеть, и др. информации.

Применение в качестве подтверждения личности человека логинов, паролей, IP-адресов, паспортных и других данных реализуется в постановлении Правительства РФ «Об использовании Федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"» [21].

Однако все было бы достаточно просто, если бы и в этом процессе не существовала проблема. Проблема связана с тем, что разработаны программные технологии, которые позволяют менять IP-адрес, например, возможно создавать динамические, или «невидимые», или нераспознаваемые IP-адреса. Кроме того, возможно совпадение IP-адресов, именно по этой причине мировым сообществом осуществляется переход с протокола IPV4 на IPV6.

На решение данной проблемы косвенно указывала Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии» [7], в которой определена необходимость развивать применение протокола следующего поколения IPv6, благодаря которому субъектам государства будет облегчен доступ к формирующимся государственным услугам. Для этого Декларация призывает объединить усилия государств-участниц с целью формирования единого информационного пространства.

Переход на систему IPv6 связан с тем, что система IPv4 построена таким образом, что возможно появление схожих IP-адресов. Именно по этой причине мировое сообщество организует переход с протокола IPv4[3] на IPv6[4]. Но, по данным 2015 г., IPv6 протоколом пользуется всего 10% населения [6].

О реализации информационной безопасности при переходе на IPV6 пишет Марко Россини: «Дальнейшее развитие компьютерных технологий и интернет-правил, такие как введение нового интернет-протокола IPv6, также может облегчить идентификацию» [3].

А. В. Незнамов предлагает применять систему доменных имен для решения вопроса идентификации. Он пишет, что «обусловленность многих интернет-отношений использованием системы доменных имен является более значимым признаком, а проблема идентификации субъектов отношений может быть объединена с проблемой неопределенности местоположения сторон» [18]. Хотелось бы отметить, что данное видение сужает суще-

[3] Четвёртая версия IP-протокола, первая широко используемая версия.

[4] Новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в Интернете, за счёт длины адреса 128 бит вместо 32. Протокол был разработан IET.

ствующую проблему идентификации человека, сводя ее только к доменным именам. Кроме того, система доменных имен основана также на структуре IP-адресов.

Соотношение персональных данных в Интернет с идентификационными данными

В целях определения основных проблем в области идентификации человека в Интернете и разработки законодательных предложений для разрешения выявленных проблем в 2015 г. Управление делами Президента РФ сформулировало следующие направления исследований в области информационной безопасности в Интернете: исследование систем доверительного управления информацией, определение и защита персональных данных при трансграничной передаче таких данных, прав субъекта данных, определение требований к институту доверительного управления информацией (в том числе персональной) и др. [17].

Персональные данные п. 1. ст. 3 определены Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [28] как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Однако необходимо определиться с перечнем данных в сети Интернет, которые могут идентифицировать человека. Например, могут ли псевдоним, никнайм[5] или IP-адрес рассматриваться как данные, на основании которых можно определить человека.

В процессе исследования, проводимого Рабочей группой по защите персональных данных в Великобритании [4], возникли дебаты о соотношении персональных данных и IP-адреса. Так, высказывалось мнение, что все IP-адреса должны считаться персональными данными, а не только те, которые могут быть рассмотрены с другой информацией, помогающей идентифицировать конкретного индивидуума.

Тем не менее Федеральный уполномоченный по защите данных и председатель Рабочей группы заключил, что в Великобритании отношение к IP-адресам как к персональной информации остается на усмотрение Информационного комиссара и Судов. Подводя итог, он сообщил, что в том случае, где идентификация человека возможна по IP-адресу, IP должен считаться персональными данными. Однако он также заявил, что все IP-адреса, обрабатываемые компаниями должны рассматриваться как персональные данные. В конечном счете, только Суд решает данный вопрос [4].

В настоящее время Парламент Великобритании рассматривает поправки к дефиниции «Персональные данные», которую предлагается расширить так, чтобы в нее попали IP-адреса и «cookie»[6], как информация, позволяющая определить человека. Предлагается следующее определение: «персональные данные – данные, с помощью которых человек может быть идентифицирован прямо или косвенно на основании средств, которые могут быть использованы контроллером данных, в том числе применительно к идентификационным номерам, данным о местоположении, онлайн идентификаторам...» [2].

Уполномоченный по конфиденциальности в Гонконге высказал суждение, что к персональным данным не может относиться IP-адрес [1]. Уполномоченный написал в своем докладе: «IP-адрес сам по себе не подпадает под определение “персональных данных”». В руках провайдера IP-адрес становится персональными данными в сочетании с другой информацией, которая удерживается – которая будет включать имя и адрес клиента. В руках оператора сайта информация может стать персональными данными через пользовательский профиль.

На территории РФ нет единого понимания соотношения персональных данных с идентификационной информацией в Интернете. Н. Кудряшова пишет, что данные, такие как результаты предыдущих рекламных кампаний – обращение человека к страницам других сайтов, его просмотры и другая деятельность в рамках онлайн-ресурсов составляют данные, которые сами по себе не содержат сведений об определенном лице, но в силу закона могут быть признаны персональными данными. Например, если IP-адреса из лог-файлов сервера привязаны к физическим лицам, то информация о запросах с этих IP-адресов представляет собой персональные данные. Если же для определения человека, к которому относятся те или иные характеристики пользовательского профиля, необходимо воспользоваться дополнительной информацией, то такие данные могут считаться обезличенными.

[5] Nickname – кличка, прозвище. В Интернете используется как имя собственное, которое человек выбирает и присваивает себе сам для возможности других лиц обратиться к нему.

[6] Системная информация, отправляемая вебсервером и хранимая на компьютере пользователя.

А. А. Иванов считает, что при разработке Федерального закона от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» [26] допущена ошибка, т. к. в «перечне ресурсов, находящихся под угрозой, не упомянуты такие специфические средства Интернета, как иностранные доменные имена, DNS-адреса и статические IP, при получении которых также передаются персональные данные» [14].

Н. В. Власовой, С. А. Грачевой, М. А. Мещеряковой предлагалось предусмотреть проверку информации, представленной потенциальным пользователем, в том числе по IP-адресу при регистрации в социальных сетях [9].

Российское законодательство признает в качестве персональных данных IP-адрес. Например, в Постановлении Центральной избирательной комиссии РФ от 3 ноября 2003 г. № 49/463-4 «О Перечне персональных данных и иной конфиденциальной информации, обрабатываемой в комплексах средств автоматизации Государственной автоматизированной системы Российской Федерации "Выборы" и организации доступа к этим сведениям к персональным данным и иной конфиденциальной информации, обрабатываемой в комплексах средств автоматизации Государственной автоматизированной системы Российской Федерации "Выборы"» отнесен IP [20].

Однако несмотря на то, что Закон и большинство исследователей сходятся во мнении, что IP-адрес должен быть отнесен к персональным данным, можно привести пример российской судебной практики, указывающий иное. Федеральный арбитражный суд Московского округа постановил [19], что под тайной связи понимается именно тайна информации, содержащейся в сообщении, а не информация о владельце IP-адреса, с которого произошло обращение к сайту.

Суть дела была в следующем: в связи с проведением камеральной проверки в отношении возможного неправомерного использования инсайдерской информации и манипулирования рынком обыкновенных именных акций ОАО «СМЗ» в адрес общества направлено предписание о предоставлении документов от 30.05.2012 № 12-ОП-10/23 808, в соответствии с которым заявитель в течение пяти рабочих дней с даты получения Предписания обязан предоставить ФСФР России: информацию о лице, использовавшем 07.03.2012 в 18:00:56 IP-адрес 46.73.66.221 при соединении с сетью Интернет, с приложением подтверждающих документов; договоры о предоставлении услуг, заключенные обществом с лицом, указанным в пункте 1 данного предписания, со всеми приложениями и дополнениями.

В указанный в предписании срок информация и документы в адрес ФСФР не поступили. Общество сообщило административному органу 19.06.2012 об отказе в предоставлении информации, содержащей персональные данные физического лица, ввиду отсутствия письменного согласия абонента на предоставление таких данных третьим лицам.

Данные обстоятельства послужили основанием для привлечения общества к ответственности по ч. 9 ст. 19.5 КоАП РФ. Суд постановил, что в соответствии со ст. 63 Федерального закона от 07.07.2003 № 126-ФЗ (ред. от 13.07.2015) «О связи» на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Таким образом, под тайной связи понимается именно тайна информации, содержащейся в сообщении, а не информация о владельце IP-адреса, с которого произошло обращение к сайту.

Данный вывод судом корреспондируется со ст. 6, 7, 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [28].

Заключение

В 2007 году А. А. Тедеев приводил слова М. А. Федотова, что «правовая наука находится на пороге появления нового метода правового регулирования, связанного с функционированием права в телекоммуникационных сетях с использованием новых информационных и коммуникационных технологий. Традиционные представления о методах правового регулирования, которые позволяют нам вычленять традиционные отрасли права, как то: административное право, гражданское право, конституционное (или государственное) право, уголовно-процессуальное право и т. д., применить в данном случае мы не сможем.

Но если представить, что телекоммуникационные сети типа Интернета – это не просто новое средство коммуникации, а новая сфера обитания человеческой цивилизации, новая сфера человеческой активности и новая сфера применения права, то мы поймем, что информационное право будет иметь свой особый метод правового регулирования, ибо он в первую очередь будет осуществляться в телекоммуникационных сетях, в киберпространстве. Иными словами, человек будет не просто пользоваться телекоммуникационными сетями, он будет вступать в правовые отношения, испытывать на себе правовое регулирование через телекоммуникационные сети» [25].

Таким образом, исследование узкой сферы отношений, связанных с соотношением персональных данных и IP-адреса, позволяет подтвердить мысль А. А. Тедеева и М. А. Федотова Регулирование отношений теми правовыми нормами, которые основаны на понимании отношений без учета специфики информационных технологий в настоящий период развития, дает сбой.

Подводя итог, можно обобщить, что IP-адрес указывает территориальную принадлежность, провайдера, технологию человека, вышедшего в Интернет, географическое место выхода в Интернет и др. информацию.

Деятельность человека в Интернете представлена набором цифровых данных, которые содержат его атрибуты, предпочтения и особые его черты, включающие в том числе и IP. Цифровая идентичность человека представлена в виде набора признаков виртуального субъекта, зафиксированных в виде электронных записей.

Однако, несмотря на отрытый перечень персональных данных, в России вопрос о возможности отнесения таких данных к персональным на уровне Федерального закона все еще остается неопределенным.

В связи с этим верным решением было бы внесение предложения о включение в понятие «персональные данные», определенное Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», идентификационной информации – IP-адрес и другой технологической информации, на основании которой возможно определить физическое лицо в сети Интернет.

Примечания

1. Hong Kong clears Yahoo! of privacy breach over jailed journalist // URL: http://www.out-law.com/page-7880 (дата обращения: 10.02.2016).

2. Data protection Act // Legislation. gov.uk. URL: http://www.legislation.gov.uk/all?title=The%20Data%20Protection%20Act (дата обращения: 10.02.2016).

3. Marco Roscini. Cyber Operations and the Use of Force in International Law. — Oxford University Press. — P. 33

4. Protection of personal data // Justice. Building a European Area of justice. URL: http://ec.europa.eu/justice/data-protection/index_en.htm (дата обращения: 10.02.2016).

5. Reza Etemad-Sajadi, Lassaad Ghachem (2015) "The impact of hedonic and utilitarian value of online avatars on e-service quality" Computers in Human Behavior 52, 81–86.

6. Statistics// Google statistics. URL: https://www.google.com/intl/en/ipv6/statistics.html (дата обращения: 10.02.2016).

7. World Summit on the Information Society Declaration of Principles: Building the Information Society: a global challenge in the new Millennium // UN Documents Gathering a body of global agreements. URL: http://www.un-documents.net/wsis-dop.htm (дата обращения: 10.02.2016)

8. Zharova A. (2015) Influence of the principle of interoperability on legal regulation // International Journal of Law and Management. — Vol. 57, iss. 6.

9. Власова Н. В., Грачева С. А., Мещерякова М. А. и др. Правовое пространство и человек : монография /отв. ред. Ю. А. Тихомиров, Е. В. Пуляева, Н. И. Хлуденева. — М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, 2013.

10. Елин В. М. Значение гражданско-правовых механизмов защиты компьютерной информации в условиях информационного общества // Проблемы информационной безопасности. Компьютерные системы. — 2015. — № 1. — С. 74—82.

11. Елин В. М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. —2013. — № 2 (24). — С. 70—76.

12. Жарова А. К. Сущность и структура информационного противоборства// Государство и право. — 2009. — № 2. — С. 48—54.

13. Жарова А. К. Право и информационные конфликты в ИТ сфере. – М.: Янус К. 2016. — 435 с.

14. Иванов А. А. Хранение персональных данных за рубежом с точки зрения российского права // Закон. — 2015. — № 1.

15. Кабанов П. А. Криминологическая классификация жертв политических преступлений в современной российской криминальной политической виктимологии // Юридическое образование и наука. — 2007. — № 4. — С. 3.

16. Кудряшова Н. RTB-аукционы и защита персональных данных // эж-ЮРИСТ. — 2014. — № 41.

17. Научно-исследовательская работа «Подготовка предложений по повышению защищенности персональных данных». Распоряжение Администрации Президента Российской Федерации от 18 марта 2015 № 280.

18. Незнамов А. В. Особенности компетенции по рассмотрению интернет-споров / науч. ред. В. В. Ярков. — М.: Инфотропик Медиа, 2011. – Сер. «Гражданский и арбитражный процесс: новые имена & новые идеи». - Кн. 1. — 272 с.

19. Постановление Федерального арбитражного суда Московского округа от 12 марта 2013. № Ф05-1348/13 по делу № А40-112131/2012 // Гарант

20. Вестник Центральной избирательной комиссии Российской Федерации, 2003., № 21.

21. СЗ РФ. —2013. —№ 30 (ч. II). — Ст. 4108.

22. СЗ РФ. — 2005. — № 36. — Ст. 3704.

23. Сущность и проблемы электронного документооборота // Юрист. — 2008. — № 6.

24. Толковый словарь русского языка: в 4 т. / под ред. Д. Н. Ушакова. — М. – Т. 1., 1935. — С. 34.

25. См., например: Тедеев А. А. Особенности правового регулирования отношений в глобальных компьютерных сетях // Информационное право. — 2007. — № 2.

26. СЗ РФ. — 2014. — № 30. — Ст. 4243.

27. СЗ РФ. — 2006. — № 31 (1 ч.) — Ст. 3448.

28. СЗ РФ. — 2006. — № 31 (1 ч.). — Ст. 3451.

29. СЗ РФ. —2003. —№ 28. —Ст. 2895.

Жарова Анна Константиновна, к. ю. н., доцент, доцент кафедры инноваций и бизнеса в сфере ИТ НИУ ВШЭ, с. н. с. ИГП РАН, 105187, Москва, Кирпичная ул., 33. E-mail: alexmin@bk.ru

Zharova Anna K., Candidate of Juridical Sciences, Associate Professor, Associate Professor of Department of Innovation and Business in IT HSE., Senior Researcher of The Institute of State and Law of The Russian Academy of Sciences, Kirpichnaya 33 str., Moscow, 105187. E-mail: alexmin@bk.ru