Юридический вестник ДГУ. 2022. Т. 44, № 4.
Law Herald of DSU, 2022, vol. 44, no. 4.

Научная статья
УДК/UDC 340
DOI: 10.21779/2224-0241-2022-44-4-34-41

Теоретико-правовые аспекты права на анонимность в сети Интернет

Р. В. Федоров
Институт технологий управления ФГБОУ ВО «МИРЭА – Российский технологический университет», г. Москва, Российская Федерация,
roman-fedorof@ya.ru, ORCID ID: 0000-0003-4926-6814

Аннотация. Статья посвящена анализу сети Интернет в качестве глобальной цифровой информационной среды, которой пользуется практически все человечество. Проблема необходимости идентификации/анонимности в сети является дискуссионной. Автор статьи ищет ответы на связанные с этим вопросы: как используется анонимность в сети? насколько анонимным является пользователь Интернета и как он может достичь анонимности? каковы плюсы и минусы анонимности в сети? насколько эффективно правовое регулирование анонимности специально нормативными правовыми актами? следует ли международному сообществу установить общую директиву о том, как регулировать вопросы анонимности в государствах-членах? Также затрагивается проблема доксинга в Интернете. Методологической основой работы стали методы комплексного анализа правовых явлений процедур и процессов, общенаучные и частнонаучные методы познания.

Ключевые слова: теория идентификации, анонимность, интернет, сеть, анонимизация, доксинг, цифровая анонимность.

Для цитирования: Федоров Р. В. Теоретико-правовые аспекты права на анонимность в сети Интернет // Юридический вестник ДГУ. 2022. Т. 44, № 4. С. 34–41. DOI: 10.21779/2224-0241-2022-44-4-34-41

Original article

Theoretical and legal aspects of the right to anonymity on the Internet

Roman V. Fedorov
Institute of Management Technologies of the MIREA – Russian Technological University, Moscow, Russian Federation
roman-fedorof@ya.ru, ORCID ID: 0000-0003-4926-6814

Abstract. The article is devoted to the analysis of the Internet as a global digital information environment, which is used by almost all mankind. The problem of the need for identification/anonymity in the network is debatable. The author of the article is looking for answers to related questions: how is anonymity used online? How anonymous is an Internet user and how can he achieve anonymity? What are the pros and cons of anonymity on the web? How effective is the legal regulation of anonymity specifically by regulatory legal acts? Should the international community establish a general directive on how anonymity issues should be regulated in Member States? The problem of boxing on the Internet is also touched upon. The methodological basis of the work was the methods of complex analysis of legal phenomena of procedures and processes, general scientific and private scientific methods of cognition.

Keywords: identification theory, anonymity, Internet, network, anonymization, boxing, digital anonymity.

For citation: Fedorov R. V. Theoretical and legal aspects of the right to anonymity on the Internet. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2022, vol. 44, no. 4, pp. 34–41. DOI: 10.21779/2224-0241-2022-44-4-34-41 (In Russ.).

В современном мире коммуникативные возможности Интернета используются в политике, государственной деятельности, науке, образовании и экономике. Анонимность означает, что реальный автор сообщения не показывается [1]. В теории информационного права анонимность рассматривается как антипод идентификации в паре «идентификация-анонимность». То есть анонимность следует рассматривать как неидентификацию субъекта отношения. В рамках процесса идентификации можно выделить три элемента (переменные): субъект идентификации (идентифицирующее лицо), объект идентификации (идентифицируемое лицо), идентификаторы объекта идентификации. При этом анонимность в разных общественных отношениях всегда имеет свою степень (в зависимости от возможностей субъекта идентификации по доступу к идентификаторам объекта идентификации), а

идентификаторы в сети Интернет дополнены возможностью идентификации устройства (смартфона, компьютера), с которого было осуществлено действие в сети [2].

Анонимность в сети является основной целью в компьютерных сетях, построенных на основе анонимных прокси-серверов. Существует круг лиц, которые хотели бы пользоваться возможностями глобальных сетей и при этом скрывать свой IP-адрес и другие идентификаторы.

Распространенным вариантом анонимности является псевдоанонимность, когда указывается другое имя субъекта. Псевдоним порой держится в строжайшей тайне, иногда настоящее имя псевдонима известно, например, Марк Твен – псевдоним Сэмюэля Клеменса или Эд Макбейн – псевдоним Эвана Хантера, чье первоначальное имя было Сальваторе А. Ломбино. Человек может даже использовать несколько псевдонимов для различных видов общения.

Если сравнивать псевдоним и полную анонимность, то можно выделить следующее преимущество. Псевдоним можно распознать и определить, что совершенно разные сообщения написаны одним и тем же человеком. Если индивид хочет стать анонимом, то есть некий недостаток, который свидетельствует о том, что при объединении информации во многих сообщениях от одного и того же человека может облегчить выяснение того, кто скрывается за псевдонимом.

Феномен анонимности не был изобретен вместе с Интернетом. Анонимность и псевдоанонимность существовали на протяжении всей истории. Например, Уильям Шекспир, вероятно, является псевдонимом, а настоящее имя этого знаменитого автора неизвестно и, вероятно, уже никогда не будет раскрыто. Анонимность используется во многих целях. Например, известный человек может использовать псевдоним для написания сообщений в том случае, когда он не хочет, чтобы предубеждение людей о реальном авторе сказывалось на восприятии сообщения.

Кроме того, другие люди могут захотеть скрыть определенную информацию о себе, чтобы добиться более объективной оценки своих сообщений. Например, в истории распространенным фактом было использование женщинами мужских псевдонимов, а иудеи применяли псевдонимы в тех обществах, где их религия подвергалась преследованиям.

Анонимность часто используется для защиты частной жизни людей, например, при сообщении результатов научного исследования, при описании отдельных случаев. Во многих странах даже существуют законы, защищающие анонимность в определенных обстоятельствах.

Анонимность имеет как положительные, так и отрицательные мотивы, то же самое можно сказать и о целях анонимности. То есть для одного человека анонимность может стать желательной и востребованной, а для другого, напротив, – нежелательной [3].

В сети в соответствии с принципом свободы выражения мнений и правом на неприкосновенность частной жизни использование анонимности является законным. Пользователи могут захотеть получить доступ к данным и просматривать их анонимно, чтобы их личные данные не могли быть записаны и использованы без их ведома. Поставщики контента в Интернете могут пожелать сохранить анонимность в законных целях, например, когда лицо, страдающее зависимостью, такой как алкоголь или наркотики, болезнь или инвалидность, желает поделиться опытом с другими, не раскрывая своей личности, или когда лицо желает сообщить о преступлении, не опасаясь возмездия. При этом законопослушный пользователь не должен быть обязан оправдывать анонимное использование.

Однако анонимность может также использоваться теми, кто совершает противозаконные действия. В этом случае анонимность не должна использоваться как прикрытие для ухода преступников от ответственности.

Закон должен допускать анонимность и псевдоанонимность в Интернете. Однако закон может потребовать, чтобы реальная личность, стоящая за анонимными сообщениями, была доступна для идентификации, но если это так, то только в полном соответствии с условиями политики конфиденциальности веб-сервера, распространяющего сообщение.

Каждый сайт, который допускает анонимность, должен публиковать политику конфиденциальности, в которой объясняется, в каких случаях они будут предоставлять уполномоченным субъектам возможность идентификации пользователей. Безусловно, что администрация сайта, в свою очередь, должна придерживаться собственной политики конфиденциальности и не искать настоящее имя пользователя за псевдонимом, за исключением случаев, указанных в политике конфиденциальности [4].

Интернет во всех его проявлениях, в том числе и в формате социальных сетей, прочно и надежно вошел в нашу повседневную жизнь. При помощи социальных сетей можно не только развлекаться и общаться в свободной форме, но и решать достаточно серьезные вопросы: с помощью сетевых инструментов заключать сделки и вести эффективную торговлю, например, с помощью следующих сетевых платформ: Вконтакте, Telegram, WhatsApp, Facebook.

Именно по этой причине пристальное внимание было приковано к социальным сетям не только в государственных структурах всех форматов, но и со стороны криминальных элементов. Данный формат общения предоставляет чрезвычайно широкие возможности для отслеживания человека. Исходя из этого, большинство организа-

ций стараются сохранить анонимность пользователей VK, Telegram, WhatsApp. В таких социальных сетях есть вероятность встретиться с мошенниками и прочими криминальными элементами. Правительство Российской Федерации в рамках закона ведет борьбу с анонимностью в социальных сетях и, соответственно, в самом Интернете. В качестве примера можно привести Постановление Правительства Российской Федерации от 27.10.2018 г. № 1279 "Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети "Интернет" организатором сервиса обмена мгновенными сообщениями" [5]. Также анонимность может потребоваться законопослушным гражданам.

Часто люди обходят запреты социальных сетей и из-за своей неопытности и невнимательности публикуют и размещают материалы, запрещенные правилами многих социальных сетей, то есть человек делает это непреднамеренно. За неправомерные действия администрация сайтов и социальных сетей может (а иногда, это становится их обязанностью) заблокировать аккаунт или ограничить доступ к таким материалам.

В настоящее время социальные сети активно ведут борьбу со спамом, вирусной рекламой, на законодательном уровне предпринимаются попытки перевода сетевых взаимоотношений в правовое поле. Интернет представляет собой хаос человеческих мыслей, в котором, однако, можно найти много интересного. Именно поэтому большинство людей не хотят оставлять свои персональные данные в сети. Ведь из-за необдуманной авторизации на непонятном и неизвестном сайте можно попасть в ловушку или наткнуться на аферистов и мошенников. Сейчас имеется возможность использовать виртуальные адреса компании и оставаться анонимным в сети, по крайней мере, для обычных людей.

Чувство вседозволенности и безнаказанности возникает, когда индивид публикует информацию, скрывая свое имя под никнеймом или псевдонимом, то есть безлично, тогда он не беспокоится за идентификацию личности и начинает писать и говорить то, чего никогда не позволил бы себе при личном общении. В современном интернет-общении обвинения и оскорбления становятся обычным и привычным явлением.

Эксперты могут столкнуться с самой главной ошибкой – с непониманием пользователями принципа работы сети, возникает ошибочное представление о том, что при использовании логина «из латинских букв» человек становится анонимным, но если посмотреть глубже, то конфиденциальность в данном случае весьма призрачна.

Использование виртуальных номеров является одним из оптимальных решений в возникшей ситуации, это может обеспечить действительно максимальную защиту своих персональных данных и иной информации, а также пригодиться для более эффективного выполнения своих профессиональные обязанностей. Однако в Комитете Государственной Думы по информационной политике, информационным технологиям и связи не согласны с такой позицией. В качестве примера можно привести законопроект № 978343-7 «О внесении изменения в статью 45 Федерального закона "О связи"» [6].

В современной России борьба с анонимностью достаточно распространенное явление. Можно выделить: блокировку доменов, инициативы по контролю сообщений в социальных сетях. Многие пользователи понимают, что сейчас можно реально пострадать за свои высказывания в сети Интернет. Тем не менее, все чаще появляются новости о том, что кто-то опять был осужден за репост во «ВКонтакте» или переписку в Твиттере, что свидетельствует о низком уровне правовой культуры и правосознания граждан, а также о наличии ложной уверенности в собственной анонимности. Однако необходимо понимать, что это не проблема сетевой идентификации, а следствие качества конкретных законов и их реализации в нашей стране [7].

Существует много причин для использования анонимной технологии. Пользователи, которые хотят анонимности, обычно делают это, поскольку они не хотят, чтобы их идентифицировали как издателя (отправителя) или читателя (получателя) информации. Общие причины включают в себя:

- цензуру на местном, организационном или национальном уровне;

- личные предпочтения конфиденциальности, такие как предотвращение отслеживания или интеллектуального анализа данных;

- страх возмездия [8].

Но когда дело доходит до обсуждения сущности и назначения анонимности, зачастую люди считают: «Если вы не делаете ничего плохого, то вам и бояться нечего». Существует предположение, что только люди, занимающиеся противоправной или аморальной деятельностью, хотели бы, чтобы их личность была защищена.

С другой стороны, есть много веских причин заботиться об анонимности, особенно в социальных сетях. Неспособность сохранить свою личность в тайне, когда это необходимо, может вызвать серьезные проблемы. Вот некоторые причины, по которым можно остаться анонимным в Интернете, и почему анонимность в Интернете важна.

1. Защита личных данных. Иногда у человека нет желания, чтобы кто-то знал, кто он на самом деле. Существует уровень социальной безопасности, который приходит с анонимностью, что может быть действительно важно для интровертов в онлайн-сообществах.

2. Личные домогательства. Анонимность в Интернете также играет важную роль в свободе выражения мнений. Одна из самых удивительных

особенностей Интернета заключается в том, что анонимность предоставляет возможность говорить тем, кого активно заставляют молчать. Всё это позволяет таким людям говорить и не опасаться последствий.

3. Деликатные вопросы. Существует следующая категория людей, которым важна и выгодна анонимность. Многие нуждаются в информации по определенной теме, но они не желают, чтобы их поймали на поиске данной информации, например, человек может задать свои вопросы в онлайн-сообществе, не раскрывая своей личности и не рискуя преждевременным разоблачением.

4. Медицинские вопросы становятся достаточно чувствительной областью. Очень часто молодые люди сталкиваются с проблемой «а вдруг меня осудят или не поймут». В современном мире много молодых девушек, которые забеременели и хотят обратиться за медицинской помощью, но в то же время хотят скрыть это от родителей, т.е. сохранить свою тайну.

Список можно продолжать до бесконечности: люди, которые борются с проблемами психического здоровья, люди, которые изменяют в отношениях, люди, которым нужен совет по разводу, те, кто занимается юридическими вопросами и не хотят разоблачения себя или своего клиента и т.д.

Таким образом, можно сказать, что в современных реалиях сеть Интернет является основным пространством обмена мнениями между людьми. Тысячи форумов, сайтов по интересам и страниц в социальных сетях являются площадками для обсуждения всевозможных проблем или событий. Но страх открытого изложения своей позиции из-за возможного осуждения, который присущ подавляющему числу людей, породил потребность в сокрытии своей личности. При этом анонимность в информационном пространстве практически невозможно регулировать без серьезных ограничений граждан в их правах и свободах. Она, с одной стороны, может породить среду активного поиска лучших путей развития общества и государства, а с другой стороны – среду деятельности преступников. Уровень социальной ответственности можно изменить, если заменить все обезличенные аватарки и профили с использованным псевдонимом на конкретного человека с его именем. Это позволит направить беседу в благоприятное русло, а мнение каждого человека оценить соразмерно его реальным достижениям и опыту.

Интернет-сервисы, программы электронной почты уже широко используются в нашей стране как для частного, так и для делового общения. Однако при каждом доступе происходит утечка большого количества информации, относящейся к конкретным пользователям. Следовательно, использование популярных интернет-сервисов приводит к угрозам конфиденциальности пользователей, поскольку эти данные могут быть получены злоумышленниками или собраны поставщиками услуг для создания профилей пользователей. Для борьбы с такими угрозами были введены сервисы анонимайзера, специально предназначенные для анонимной электронной почты и сетевых новостей. Но доступные сервисы анонимизации имеют множество недостатков и не обеспечивают требуемой степени анонимности для пользователей Интернета. Это происходит, главным образом, потому, что эти услуги были реализованы довольно разрозненно, без систематического анализа. В результате законодатель решил радикально устранить эту проблему, внеся изменения в Федеральный закон "Об информации, информационных технологиях и о защите информации" [9]. Данные изменения также являются дискуссионными с точки зрения теории права, однако это станет предметом другой научной статьи.

Еще одной проблемой, связанной с анонимностью в сети Интернет, является так называемый «доксинг» (или «doxxing»). Этот термин означает свободное опубликование персональных данных в сети, таких как адрес места жительства, логины и пароли ученых записей сайта госуслуг или личного кабинета налогоплательщика, внутренняя корпоративная переписка, интимные фотографии знаменитостей или обычных людей. При этом такие данные уже могут быть опубликованы в сети самим пользователем (например, в социальных сетях). Жертвой доксинга может стать любой пользователь сети, все, что для этого нужно – заинтересовать другого человека в таких данных.

При этом мотивы доксинга могут быть самыми разными: а именно – правомерными и социально полезными, например, разоблачение преступника и привлечение его к юридической ответственности, а также и противоправными, например, запугивание, унижение, вымогательство. Зачастую жертвы доксинга имеют серьезные основания опасаться за свою жизнь [10], либо становятся объектом насмешек и издевательств со стороны других пользователей, что также может привести, например, к попыткам самоубийства [11]. При этом особенностью Интернета является то, что информацию в сети разместить достаточно просто, а вот удалить её будет намного сложнее, в связи с сохранением резервных копий на серверах сайтов, а также возможностью скачивания изображений (скриншотов) такой информации и т.п. В результате процедуры доксинга может пострадать честь человека (например, известного футболиста) или деловая репутация компании.

Исследователи проводят параллель между доксингом и сексуальными домогательствами в сети (онлайн-харассмент), при этом они отмечают следующие факторы, способствующие онлайн-харассмену: во-первых, анонимность домогателей, во-вторых, усиление домогательств в случае передачи видеороликов или изображений от жертвы,

в-третьих, трудности удаления компрометирующего контента из сети [12].

Несмотря на указанные выше негативные аспекты доксинга, иногда его рассматривают и как средство разоблачения преступников, или как инструмент гражданского протеста. Например, коррупционные правонарушения правительственных чиновников в Китае являются объектом поиска так называемой «Поисковой Системы Человеческой Плоти» («Human Flesh Search Engine»), которая представляет собой пользователей Китайского Интернета, проводящих частные и общественные расследования по фактам взяточничества и злоупотреблений должностных лиц. Например, официальное расследование против двух муниципальных служащих было инициировано на основании анонимно опубликованных в Интернете документов об их командировочных расходах, из которых было видно нецелевое расходование денежных средств [13].

По проблеме доксинга имеется интересное исследование Дэвида Дугласа, который классифицирует доксинг на следующие виды: делигитимация (раскрытие личной интимной информации), таргетирование (раскрытие персональной информации о неясных или запутанных обстоятельствах, связанных с конкретным случаем) и деанонимизация (раскрытие персональных данных, позволяющих идентифицировать ранее анонимного или псевдонимного лица) [14]. Обоснованным видится мнение Дугласа, что доксинг может быть признан допустимым только в общественных интересах (для разоблачения правонарушителей) и только в той мере, какая минимально необходима в целях выявления факта совершения противоправного деяния. Превышение объема раскрываемой информации, а также использование доксинга для угроз или унижения недопустимы.

Термин «доксинг» возник в 90-е годы, им обозначалась одна из форм мести в хакерском сообществе, когда в компетентные органы анонимно подбрасывались документы, раскрывающие личность преступника (хакера) и обстоятельства совершения преступления (взлома) [15]. Оксфордский британский и Всемирный словарь английского языка дает следующее определение доксингу: «поиск и опубликование личной или идентифицирующей информации о человеке во всемирной сети, как правило со злым умыслом». То есть доксинг не всегда рассматривается как негативное явление. Зачастую доксингом занимаются журналисты, преследуя цель раскрытия анонимных/псевдонимных личностей в общественных интересах. Хотя в большинстве случаев преобладает мнение, что журналисты не имеют права опубликовывать персональную информацию без согласия лица.

Возвращаясь к проблеме анонимности отметим, что в результате доксинга устраняется некоторая доля анонимности определенного человека. Эта степень анонимности зависит от количества известных идентификаторов. Такими идентификаторами (с позиции Гари Маркса) являются:

Официальное имя (Ф.И.О. физического лица)	Имя, под которым лицо известно в официальных государственных структурах
Место нахождения	Информация о месте жительства или временного пребывания лица, а также сведения о контактном номере телефона
Псевдоним, связанный с официальным именем или местом нахождения	Имя или код, под которым лицо известно в информационной системе (например, номер банковского счета), связанное с ФИО. или адресом места жительства
Псевдоним, не связанный с официальным именем или местом нахождения	по причинам политики использования персональных данных (например, анонимная медицинская запись); в случае, когда иные люди не знаю, что это псевдоним, а пользователь таким образом маскируется (обманывает)
Паттерн (образ действия)	Лицо может быть распознано по своим регулярным (повторяющимся) публичным действиям или привычкам (например, ходить в один и тот же магазин в определенное время)
Социальная категоризация	Сведения, на основании которых лицо может быть отнесено к той или иной стереотипизированной категории (стиль одежды, акцент, внешность и т.п.)
Символы правомочности	Вещи или знания, благодаря которым лицо может быть распознано как обладающие отдельными правомочиями (служебное удостоверение, пароль, билет на самолет)

Используя классификацию Маркса, доксинг можно понимать, как публичное обнародование определенного типа знаний (идентификатора) об идентичности лица (объекта доксинга), которое устанавливает поддающуюся проверке связь между этим идентификатором и другими идентификаторами объекта идентификации. Возможность перепроверки результатов доксинга отличает его от других форм разоблачения, поскольку, как следует

из происхождения термина, он базируется на документальных доказательствах.

В России имеется ряд правовых норм, которые так или иначе описывают юридическую и техническую составляющую анонимности: различные взаимоотношения в Интернете, возложение ответственности за вред, причиненный такими действиями, но количество этих норм небольшое, и это связано с тем, что Интернет является всемирным феноменом и ограничить его можно разве что в Корейской Народно-Демократической Республике (Северной Корее), в которой Интернет доступен лишь для ряда организаций, получивших на это разрешение. По-другому отношениями в сети Интернет управлять сложно, будь то отношения обезличенные (анонимные) или же пользователи под своими именами. И с теоретической точки зрения можно сказать, что, если у лица есть доступ к всемирной паутине, значит, у него есть вероятность получения нужной информации из другой страны, которая также подключена к сети Интернет, правда, в ряде случаев для этого понадобятся различные хакерские действия [16]. Таким образом, страны могут воздействовать друг на друга путем установления определенных юридических ограничений и иными способами, чтобы это предотвратить, необходимы новые международные договоренности.

Государственная Дума приняла ряд поправок и дополнений в действующее законодательство в целях борьбы с такой важной глобальной проблемой, как терроризм, но новые права и обязанности обеспокоили общественность. «Пакет Яровой» был создан после масштабной катастрофы на борту российского самолёта над Синайским полуостровом, что подтолкнуло Россию к действиям. В пакете прописаны положения о привлечении несовершеннолетних с 14 лет к уголовной ответственности за участие в террористических группировках, уголовная ответственность также предусматривается за недонесение о каком-либо преступлении. Поправки включают в себя правило о том, что операторы мобильной связи обязаны хранить информацию о посещении веб-сайтов, записи звонков и сообщений на своих серверах и, в случае необходимости, предоставить эти данные правоохранительным органам. Общественный резонанс произошёл именно из-за этого, так как общественность посчитала, что данный проект нарушает право на личную жизнь (ст. 23 Конституции РФ).

В завершение нельзя не вспомнить о трагедии, произошедшей в 2021 году: 19-летний молодой человек ворвался в здание своей бывшей школы и расстрелял девятерых человек, из которых двое взрослых и семь детей, около двадцати человек были ранены и доставлены в больницы. Незадолго до стрельбы стрелок создал Telegram-канал, где говорил о том, что он Бог и сообщил о намерении убийства: «в мире не должно остаться живности, это ошибка вселенной» [17]. Со стороны правительства последовала незамедлительная реакция на данную ситуацию. Глава Государственной думы Вячеслав Володин в Telegram написал, что надо отказаться от анонимности в Интернете – это поможет снизить количество пропаганды насилия и экстремизма в Интернет-среде. Он отметил: «Мир сильно изменился за последние несколько десятилетий. Новые технологии, доступный всем Интернет принесли с собой не только прогресс, но и проблемы, ставшие серьёзной угрозой, особенно для детей. Их здоровья, психики. Даже жизни» [18].

Список источников

1. Толковый словарь русского языка : 72500 слов и 7500 фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова ; Российская АН, Ин-т рус. яз., Российский фонд культуры. 2-е изд., испр. и доп. Москва : Азъ, 1994. 907 с.

2. Правовые аспекты идентификации в Интернете. URL: http://igpran.ru/public/events/01-02.03.2013/Andruschenko.pdf (дата обращения: 16.09.2022).

3. *Кирмайер М.* Информационные технологии. СПб.: Питер, 2017.

4. *Колисниченко Д.Н.* Анонимность и безопасность в Интернете. От «чайника» к пользователю / Д.Н. Колисниченко. М.: БХВ-Петербург, 2013.

5. Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети "Интернет" организатором сервиса обмена мгновенными сообщениями: постановление Правительства Российской Федерации от 27 окт. 2018 г. № 1279. URL: http://publication.pravo.gov.ru/Document/View/0001201811060001 (дата обращения: 16.09.2022).

6. Законопроект № 978343-7 О внесении изменения в статью 45 Федерального закона "О связи" URL: https://sozd.duma.gov.ru/bill/978343-7 (дата обращения: 16.09.2022).

7. *Бачавер А.А., Хломов К.Д.* Кибербуллинг: травля в пространстве современных технологий // Психология // Журнал Высшей школы экономики. 2014. № 3. С. 177-191.

8. МВД хочет получить доступ к данным пользователей анонимной сети Tor. URL: http://tass.ru/obschestvo/1338815 (дата обращения: 16.09.2022).

9. О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации": федеральный закон от 29 июля 2017 г. № 276-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_221230/ (дата обращения: 16.09.2022).

10. *Citron, D. K.* (2014). Hate crimes in cyberspace. Cambridge, MA: Harvard University Press.

11. *Solove, D. J*. (2007). The future of reputation: Gossip, rumor, and privacy on the internet. London: Yale University Press.

12. *Franks, M. A.* (2012). Sexual harassment 2.0. Maryland Law Review, 71, 655.

13. *Gao, L., & Stanyer, J.* (2014). Hunting corrupt officials online: The human flesh search engine and the search for justice in China. Information, Communication & Society, 17(7), 814–829.

14. *Douglas, D.M.* Doxing: a conceptual analysis. Ethics Inf Technol 18, 199–210 (2016).

15. *Honan, M.* (2014). What is doxing? Wired. http://www.wired.com/2014/03/doxing/ (дата обращения 16.09.2022)

16. Further TTPs associated with SVR cyber actors. URL: https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf (дата обращения 16.09.2022)

17. «Хочу, чтобы признали себя рабами»: найден блог предполагаемого стрелка из Казани. URL: https://www.5-tv.ru/news/342735/hocu-ctoby-priznali-seba-rabami-najden-blog-predpolagaemogo-strelka-izkazani/ (дата обращения: 16.09.2022)

18. Глава Госдумы потребовал обсудить запрет на анонимность в Интернете. URL: https://news-ru.turbopages.org/news.ru/s/society/glava-gosdumy-potreboval-obsudit-zapret-na-anonimnost-v-internete/ (дата обращения: 16.09.2022)

References

1. *Ozhegov S.I., Shvedova N.Yu.* Tolkovyj slovar' Ozhegova [Ozhegov's explanatory dictionary]. 1949. (In Russ.).

2. Pravovye aspekty identifikacii v Internete [Legal aspects of identification on the Internet]. (In Russ.). Available at: http://igpran.ru/public/events/01-02.03.2013/Andruschenko.pdf (accessed 16.09.2022).

3. *Kirmaier M*. Informacionnye tekhnologii [Information Technologies]. St. Petersburg: Peter, 2017. (In Russ.).

4. *Kolisnichenko D.N*. Anonimnost' i bezopasnost' v Internete. Ot «chajnika» k pol'zovatelyu [Anonymity and security on the Internet. From the "teapot" to the user]. Moscow: BHV-Petersburg, 2013. (In Russ.).

5. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 27.10.2018 № 1279 "Ob utverzhdenii Pravil identifikacii pol'zovatelej informacionno-telekommunikacionnoj seti "Internet" organizatorom servisa obmena mgnovennymi soobshcheniyami" [Decree of the Government of the Russian Federation No. 1279 dated 27.10.2018 "On Approval of the Rules for Identifying Users of the Internet Information and Telecommunications Network by the organizer of the instant messaging service"]. (In Russ.). Available at: http://publication.pravo.gov.ru/Document/View/0001201811060001 (accessed: 16.09.2022).

6. Zakonoproekt № 978343-7 O vnesenii izmeneniya v stat'yu 45 Federal'nogo zakona "O svyazi" [Draft Law No. 978343-7 On Amendments to Article 45 of the Federal Law "On Communications"]. (In Russ.). Available at: https://sozd.duma.gov.ru/bill/978343-7 (accessed: 11.05.2022).

7. *Bochaver A.A., Khlomov K.D*. Kiberbulling: travlya v prostranstve sovremennyh tekhnologij [Cyberbullying: harassment in the space of modern technologies]. Psihologiya. ZHurnal Vysshej shkoly ekonomiki. [Psychology. Journal of the Higher School of Economics], 2014, no. 3, pp. 177-191. (In Russ.).

8. MVD hochet poluchit' dostup k dannym pol'zovatelej anonimnoj seti Tor. [The Ministry of Internal Affairs wants to access the data of users of the anonymous Tor network]. (In Russ.). Available at: http://tass.ru/obschestvo/1338815 (accessed 16.09.2022).

9. Federal'nyj zakon o vnesenii izmenenij v federal'nyj zakon "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" ot 29 iyulya 2017 goda N 276-FZ [Federal Law on Amendments to the Federal Law "On Information, Information Technologies and Information Protection" dated July 29, 2017 N 276-FZ] (In Russ.). Available at: http://www.consultant.ru/document/cons_doc _LAW_221230/ (accessed: 16.09.2022).

10. *Citron, D. K*. (2014). Hate crimes in cyberspace. Cambridge, MA: Harvard University Press. (In Eng.)

11. *Solove, D. J*. (2007). The future of reputation: Gossip, rumor, and privacy on the internet. London: Yale University Press. (In Eng.)

12. *Franks, M. A.* (2012). Sexual harassment 2.0. Maryland Law Review, 71, p. 655. (In Eng.)

13. *Gao, L., & Stanyer, J.* (2014). Hunting corrupt officials online: The human flesh search engine and the search for justice in China. Information, Communication & Society, 17(7), pp. 814–829. (In Eng.)

14. *Douglas, D.M.* Doxing: a conceptual analysis. Ethics Inf Technol 18, pp. 199–210 (2016). (In Eng.)

15. *Honan M.* (2014). What is doxing? Wired. (In Eng.) Available at: http://www.wired.com/2014/03/doxing/ (accessed: 16.09.2022).

16. Further TTPs associated with SVR cyber actors. (In Eng.) Available at: https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf (accessed: 16.09.2022).

17. «Hochu, chtoby priznali sebya rabami»: najden blog predpolagaemogo strelka iz Kazani. ["I want them to recognize themselves as slaves": the blog of the alleged shooter from Kazan was found.] (In Russ.). Available at: https://www.5-tv.ru/news/342735/hocu-ctoby-priznali-seba-rabami-najden-blog-predpolagaemogo-strelka-izkazani/ (accessed: 16.09.2022).

18. Glava Gosdumy potreboval obsudit' zapret na anonimnost' v Internete. [The head of the State Duma demanded to discuss the ban on anonymity on the Internet.] (In Russ.). Available at: https://news-ru.turbopages.org/news.ru/s/society/glava-gosdumy-potreboval-obsudit-zapret-na-anonimnost-v-internete/ (accessed: 16.09.2022).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Федоров Роман Валерьевич, кандидат юридических наук, доцент кафедры государственного и административного права Института технологий управления ФГБОУ ВО «МИРЭА – Российский технологический уинверситет», г. Москва, Российская Федерация. *E-mail: roman-fedorof@ya.ru*

INFORMATION ABOUT THE AUTHOR

Fedorov Roman Valerievich, PhD in Law, Associate Professor of the Department of State and Administrative Law of the Institute of Management Technologies of the MIREA – Russian Technological University. *E-mail: roman-fedorof@ya.ru*

Поступила в редакцию 20.09.2022 г.; одобрена после рецензирования 18.11.2022 г.; принята к публикации 30.11.2022 г.

Received 20.09.2022; approved after reviewing 18.11.2022; accepted for publication 30.11.2022