ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ

Научная статья
УДК 342.7
EDN: RPCHZR
doi: 10.21685/2307-9525-2023-11-2-7

ПУБЛИЧНО-ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ ДОКСИНГУ

Екатерина Андреевна Романовская

Пензенский государственный университет, Пенза, Россия
up406@mail.ru

Аннотация. *Актуальность и цели*. Цифровизация общественных отношений привела к масштабным накоплениям персональных данных в киберпространстве. Технологические особенности пользования интернетом облегчают возможности сбора и обработки персональных данных. Это актуализирует поиск эффективного механизма защиты права на неприкосновенность частной жизни при сборе личных данных в цифровой среде. Основная цель – определить правовые формы противодействия доксингу. Исходя из этого, задачи исследования заключались в изучении данного явления, выделении его признаков, возможностей введения ограничений. *Материалы и методы*. Эмпирическую базу исследования составили отечественные и зарубежные научные источники, а также материалы судебной практики, а именно иск Ассоциации младших офицеров полиции Гонконга, обратившейся к Комиссии по выборам о введении временного запрета на регистрацию данных в реестре и его общедоступность. *Результаты*. Указывается, что под доксингом понимается поиск и публикация персональной или конфиденциальной информации о человеке без его согласия. Показаны примеры как незаконных действий при доксинге, так и формально разрешенных. Сформулирован вывод о сложностях защиты частной жизни лица в условиях развития цифровых технологий. *Выводы*. Перевод значительного объема социальных отношений в цифровую форму обусловил простоту обработки персональных данных и создания цифрового профиля любого гражданина на основе информации, полученной из открытых источников. Основные научные дискуссии в области публичного права при этом происходят вокруг поиска баланса между такими правами, как свобода слова и право на неприкосновенность частной жизни. Ключевой подход, принятый за рубежом относительно доксинга, сводится к тому, что меры защиты могут применяться только при наличии негативного результата для самого субъекта.

Ключевые слова: права человека, свобода слова, право на неприкосновенность частной жизни, информация, доксинг, защита, персональные данные

Для цитирования: Романовская Е. А. Публично-правовые основы противодействия доксингу // Электронный научный журнал «Наука. Общество. Государство». 2023. Т. 11, № 2. С. 65–74. doi: 10.21685/2307-9525-2023-11-2-7. EDN: RPCHZR

PUBLIC LEGAL (STATE LEGAL) SCIENCES

Original article

PUBLIC LEGAL FRAMEWORKS FOR COUNTERING DOXXING

Ekaterina A. Romanovskaya

Penza State University, Penza, Russia

up406@mail.ru

Abstract. *Background*. The digitalization of public relations has led to large-scale accumulations of personal data in cyberspace. The technological features of using the Internet facilitate collecting and processing personal data. This actualizes the search for an effective mechanism for protecting the right to privacy when collecting personal data in the digital environment. The main goal is to determine the legal forms of countering doxxing. Based on this, the objectives of the study are to study this phenomenon, highlight its features, and the possibility of introducing restrictions. *Materials and methods*. The empirical base of the study is made up of Russian and foreign scientific sources, as well as materials of judicial practice, namely, the suit of the Association of Junior Police Officers of Hong Kong, it applied to the Election Commission to introduce a temporary ban on the registration of data in the register and its public availability. *Results.* The article states that doxxing is understood as the search and publication of personal or confidential information about a person without his or her consent. The examples of both illegal and formally permitted actions during doxxing are given. The conclusion is formulated about the difficulties of protecting the private life of a person in the context of the developing digital technologies. *Conclusions.* The digitization of a significant amount of social relations has led to the simplicity of processing personal data and creating a digital profile of any citizen based on information obtained from open sources. At the same time, the main scientific discussions in the field of public law take place around the search for a balance between such rights as freedom of speech and right to privacy. The key approach adopted abroad regarding doxxing is that protective measures can be applied only if there is a negative result for the person himself or herself.

Keywords: human rights, freedom of speech, right to privacy, information, doxxing, protection, personal data

For citation: Romanovskaya E.A. Public legal frameworks for countering doxxing. *Elektronnyy nauchnyy zhurnal "Nauka. Obshchestvo. Gosudarstvo" = Electronic scientific journal "Science. Society. State*". 2023;11(2):65–74. (In Russ.). doi: 10.21685/2307-9525-2023-11-2-7

Развитие цифровых технологий в большей мере затронуло право на неприкосновенность частной жизни. Эпоха социальных сетей и электронных коммуникаций привела к тому, что каждый внешний шаг может отслеживаться и анализироваться. Этому способствует использование различных гаджетов, которым человек доверяет те или иные сведения, касающиеся его личной жизни. Систематизация сведений, обработка по заранее определенному алгоритму позволяют манипулировать гражданином (что используют различные кибермошенники), осуществлять различные преступные действия. К тому же персональные данные стали основой цифровой экономики [1]. Если в XX в. углеводороды считались «кровью» экономического развития, то сейчас, в эпоху декарбонизации, персональные данные являются основой роста материальной базы современного государства. Этот аспект учитывается в большинстве стран мира, что обусловливает определенное стимулирование граждан к переносу личной информации в цифровое пространство.

Росту объема персональных данных способствует появление мессенджеров и социальных сетей. Даже простой вход в киберпространство с любого цифрового устройства оставляет

определенный след (как минимум, некоторые метаданные: IP-адрес, браузер, геолокация и др.). Анализ таких оставленных «отпечатков» происходит с помощью искусственного интеллекта, позволяющего достаточно быстро обрабатывать большие данные. Понятно, что при таких возможностях актуализируются вопросы обеспечения безопасности. Система противодействия любым противоправным поступкам в виртуальном мире строится во многом вокруг установления правового режима персональных данных. В Российской Федерации в этой сфере сформирована целостная правовая система, в центре которой следующие правовые акты:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

4. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"».

Несмотря на создание системы защиты персональных данных, есть такие формы их раскрытия, которые при видимом уроне правам конкретного человека формально не являются каким-то нарушением. Одной из серьезных проблем в мире считается такое явление, как доксинг.

Доксинг в англоязычном сегменте имеет различное написание – doxing или doxxing. Происходит от слова documents, его сокращенного варианта docs. Под доксингом понимается поиск и публикация персональной или конфиденциальной информации о человеке без его согласия. Не всегда это связано с кражей персональных данных, поскольку таковые могут находиться в открытом доступе, но на разных цифровых платформах. Создаются специальные программы, систематизирующие все сведения о том или ином гражданине, опубликованные в киберпространстве. Доксировать означает собирать и распространять указанную информацию, субъект же таких действии – это доксер.

Приведем пример. Гражданин А. ведет страницы в социальных сетях, в которых могут указываться не только его личные персональные данные (фамилия, имя, отчество, место работы, место получения образования, дата рождения, семейное положение и др.), но и коммуникации – отношение к тем или иным торговым точкам (в частности, могут публиковаться товарные предпочтения), перемещения с видеоотчетами, фотографии друзей и родственников. Помимо этого есть страницы официальных сайтов места работы, где также размещается персональная информация. По ряду ведомств опубликование сведений происходит в обязательном порядке. Так, ст. 29 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» посвящена информационной открытости образовательной организации. В ее развитие Постановлением Правительства РФ от 20 октября 2021 г. № 1802 утверждены Правила размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации. Согласно указанным документам в постоянном открытом доступе находятся фамилии, имена, отчества (при наличии) и должности руководителей структурных подразделений. Обширная информация размещается в отношении каждого педагогического работника – от занимаемой должности, его квалификационных характеристик, преподаваемых предметов до сведений о повышении квалификации и профессиональной переподготовке. Рособрнадзором разработано специальное Руководство по соблюдению образовательными организациями требований законодательства Российской Федерации в сфере образования в части

информационной открытости образовательных организаций. Несоблюдение требований влечет за собой установленную законом ответственность (от дисциплинарной до административной).

Статья 79 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» содержит аналогичные требования, но применительно к медицинским организациям. Боле детально перечень доступной информации определен в Приказе Минздрава России от 30 декабря 2014 г. № 956н.

Аналогичные примеры можно приводить и по иным профессиональным сферам. Многие реестры находятся в открытом доступе, что дает возможность оперативно узнать информацию о статусе того или иного специалиста. Это позволяет минимизировать мошеннические действия, но создает сложности для самих граждан, для которых границы частной жизни последовательно сужаются.

Приведенные примеры показывают, что, не имея каких-то специальных программ и технических навыков, можно о каждом гражданине собрать значительный объем личных данных. Именно в этом направлении развивается доксинг. Его первые проявления наблюдались в конце 90-х гг. прошлого столетия, когда на различных интернет-площадках стали распространяться персональные данные лиц, чьи взгляды оценивались как неонацизм. Перечень личных сведений включал имена, адреса электронной почты, адреса места жительства, номера телефонов.

Первым системным раскрытием информации стало появление в 1997 г. специального веб-сайта под названием «Нюрнбергские файлы», на котором приводились данные (включая, адреса, телефоны и личные фото) около 200 человек, осуществлявших операции по искусственному прерыванию беременности (их называли «абортивистами»). На сайте недвусмысленно предлагалось преследовать и убивать перечисленных граждан. Медицинская организация из штата Орегон «Planned Parenthood» обратилась с иском о запрете на распространение информации и блокировании сайта. После продолжительной судебной тяжбы в 2002 г. иск был удовлетворен Апелляционным судом 9-го округа США. Сайт вел активист Нил Хорсли[1].

Массовое распространение доксинг получил после 2010 г., когда он стал использоваться в различных противоправных целях. Некоторые хакерские группы стали выкладывать персональные данные различных представителей социальных групп (от правоохранительных органов до общественных организаций). Впервые о доксинге как о новом приеме противодействия (цифровом оружии) стали говорить после распространения личных данных о полицейских, применявших «чрезмерное» насилие в отношении представителей движения «Захвати Уолл-стрит». Создание специальной базы позволяло узнать место жительства, электронный адрес, телефон сотрудников правоохранительных органов. С того момента технологии продвинулись: в различных странах можно найти интерактивные карты политических оппонентов, позволяющие их быстро идентифицировать.

Доксинг стал одной из основных форм еще одного особого проявления цифровой трансформации – цифрового вигилантизма (в англоязычной сфере используется различная терминология – Internet vigilantism, netilantism, cyber-vigilantism). Его классическим определением считается «взятие закона в свои руки во имя справедливости» [2]. В этом случае наиболее инициативные граждане активно «реагируют на угрозы или действия, нарушающие формальные границы установленного социально-политического порядка» [3]. В российском сегменте признаками цифрового вигилантизма принято считать:

– реализацию акций через социальные онлайн-платформы (социальные сети, мессенджеры, чаты, имидж-борды и т.д.);

– отсутствие формализации и строгой иерархии, что характерно для любого сетевого сообщества;

[1] Cohen David S., Connon K. Strikethrough (Fatality). The origins of online stalking of abortion providers. URL: https://slate.com/news-and-politics/2015/05/neal-horsley-of-nuremberg-files-died-true-threats-case-reconsidered-by-supreme-court-in-elonis.html (дата обращения: 15.06.2023).

– элемент гражданского общества, хотя и не имеющий однозначной позитивной оценки;

– претензии на формирование определенных ценностей с требованием их соблюдения (даже если это не предусмотрено официальными нормативными актами);

– применение кары – от публичного осуждения до преследования (в крайних случаях с элементами самосуда и преступных действий).

При этом вигилантизм может быть институциональным, вплоть до прямой поддержки со стороны органов публичной власти, а также спонтанным – реакцией общества на внезапно возникшую острую проблему. В указанной системе координат доксинг занимает основное место, поскольку позволяет выявить оппонента и подвергнуть его преследованию.

Доксинг также практикуется в журналистских расследованиях.

Данное явление может приобретать противоправные формы. В этом случае происходит взлом личных аккаунтов, электронной почты, установка на мобильные устройства программ слежения [4]. Этими приемами пользуются так называемые хактивисты [5]. Зачастую взламываются различные государственные информационные ресурсы, из которых черпаются сведения о наличии в собственности объектов недвижимости, транспортных средств, о наложенных штрафах, участии в деятельности юридических лиц и т.д. Все это систематизируется и придается огласке со скриншотами, официальными выписками, раскадровкой видеозаписей с камер наблюдения и иными элементами цифровой фиксации.

Доксинг может происходить вполне легально. При этом подходе систематизируется вся информация в отношении конкретного лица, размещенная в сети Интернет в открытом доступе. Значительный объем сведений может быть получен из социальных сетей с учетом того, что немногие пользователи закрывают свои личные страницы [6]. Возможна систематизация публикаций, размещенных в информационных агентствах, средствах массовой информации. Достаточно большой объем информации может быть получен из деклараций о доходах (или расходах) государственных служащих, что является одновременно элементом гражданского контроля [7]. В интернет-пространстве могут создаваться специализированные досье на конкретных лиц, в которых любой желающий может представить свою часть (как правило, при минимальной проверке со стороны администратора). Интернет максимально демократизировал указанный процесс: практически любой гражданин, имеющий доступ в онлайн-пространство, необходимое время и минимум навыков работы с программой-поисковиком, может систематизировать значительный объем чужой персональной информации. Причем объектом сбора могут быть данные как в отношении известных общественных деятелей, привлекающих внимание, так и обывателей, ведущих совсем непубличную жизнь.

Если в отношении противоправной модели поведения законодательство устанавливает меры противодействия доксингу, то при формальном соблюдении требований законодательства ввести какие-то ограничительные меры достаточно сложно. В то же время можно приводить отрицательные примеры, когда ошибочная идентификация приводит к быстрому доксингу в отношении гражданина при ложном обвинении в совершении антиобщественного поступка. В качестве яркого примера негативных последствий доксинга приводят историю Сунила Трипати, 22-летнего студента Университета Брауна (Род-Айленд, США), которого после Бостонского теракта в 2013 г. добровольные помощники в поиске виновных в теракте ошибочно опознали как основного подозреваемого. Сетевые волонтеры занялись опознанием возможных преступников, в числе которых оказался молодой человек, ранее заявленный как пропавший без вести. В специально созданном сетевом сообществе Сунил Трипати неоднократно упоминался как основной подозреваемый, причем уже после того, как произошло выявление истинных виновников теракта. Это вызвало негативное внимание к его семье, а также чрезмерное вмешательство в их частную жизнь. 25 апреля 2013 г. было найдено тело Сунила – несостоявшийся подозреваемый покончил жизнь самоубийством[1].

[1] Koh E. Body found Tuesday confirmed to be Tripathi's // The Brown Daily Herald. 2013. 25 April. URL: https://www.browndailyherald.com/article/2013/04/body-found-tuesday-confirmed-to-be-tripathi-s (дата обращения: 15.06.2023).

Приведенный пример показателен: подобные киберохоты всегда основаны на использовании большого числа персональных данных. Каждый из участников вносит свой вклад, раскрывая те или иные данные объекта преследования.

Проведенные исследования показывают, что чаще всего раскрываются:

– адрес места жительства (в 90 % случаев);

– личный номер телефона (61 %);

– электронная почта (53 %);

– информация на членов семьи (51 %) [8].

В подавляющем большинстве случаев систематизированная информация придается огласке, что в сопровождении с какими-то обвинениями наносит серьезный вред. Зачастую доксинг осуществляется не в отношении реальных преступников, а в отношении политических оппонентов или лиц, занимающих какую-то общественную позицию, которая имеет своих противников. При этом раскрытие личных данных в подавляющем большинстве случаев происходит с призывом о нарушении частной жизни лица: звонить, писать письма на электронную почту, пикетировать около места жительства.

Доксинг применяется при позитивном поведении, когда требуется помощь правоохранительным органам в поиске правонарушителя. Цифровые технологии внесли свои коррективы и в этот процесс. Ранее о розыске преступника сообщалось в виде печатного объявления, которое придавалось максимальной огласке (в том числе через средства массовой информации). Сейчас наиболее эффективный поиск происходит с помощью привлечения сетевых помощников (через мессенджеры, социальные платформы), которые могут сегментировать участки киберпространства и заняться обработкой необходимой информации. Сбор персональных данных может дать свой результат – обличение и поимка преступника. С другой стороны, увлеченность таким поиском для некоторых граждан может стать основой для «безудержной бдительности».

Д. М. Дуглас представляет собственную классификацию доксинга:

– деанонимизация;

– таргетинг;

– делегитимизация.

В первом случае происходит раскрытие личности (ее идентификация), либо действующей анонимно, либо скрывающейся под псевдонимом. В отношении некоторых лиц ведется настоящая охота. Например, до сих пор не ясно, кто скрывается под именем Бэнкси. Бэнкси – это известный художник, представитель стрит-арта, политический активист, чьи работы оцениваются в миллионы долларов.

Во втором – идентификация лица осуществляется с указанием на его местонахождение. Д. М. Дуглас в качестве примера приводит «Нюрнбергские файлы», когда каждый пользователь мог узнать место жительства врача, согласного осуществлять операцию по искусственному прерыванию беременности.

При делегитимации личная информация раскрывается с конкретной целью – подорвать доверие к субъекту, его репутации. Зачастую это происходит при компрометации, когда гражданина изображают нарушителем установленных (или предполагаемых) социальных норм. Принятие или активное продвижение норм самим субъектом значения не имеет. Происходит разоблачение субъекта как лицемера (при публичной поддержке социальной нормы и нарушении ее в частном порядке). В качестве примера Д. М. Дуглас приводит публикации расставшимися партнерами интимных фото, получивших самостоятельное значение, – порно-месть [9]. Следует отметить, что классификация, предложенная Д. М. Дугласом, хотя и признается многими исследователями как сочетающая в себе противоречивые элементы, широко применяется, считается одной из основных [10].

В настоящее время доксинг активно используется как форма воздействия на политического оппонента, на органы публичной власти. Так, в 2019 г. в Гонконге были выложены персональные данные сотрудников полицейской службы, участвующих в разгоне демонстраций. Большинство сведений было получено из реестра избирателей, находившегося в открытом доступе.

Ассоциация младших офицеров полиции Гонконга обратилась в суд с иском к Комиссии по выборам (аналог российской Центральной избирательной комиссии [11]) о введении временного запрета на регистрацию данных в реестре и его общедоступность. Суд согласился с доводами истцов, постановил ввести временный запрет для Комиссии «публиковать или делать доступными для всеобщего ознакомления любой опубликованный список избирателей для выборов, или предоставлять членам публичные выписки из любого списка, чтобы представители общественности могли связать имена избирателей с их соответствующими основными адресами проживания». Судебный запрет касался также возможности выдачи выписок представителям общественности, но не распространялся на выписки для зарегистрированных кандидатов. В решении подчеркивалось, что доксинг может оказывать воздействие и на политические процессы – иметь «сдерживающий эффект» для некоторых лиц, что повлечет отказ в регистрации и участии в выборах[1].

В ходе научных дискуссий доксинг всегда рассматривается в разрезе конфликта свободы слова, свободы поиска информации и права на неприкосновенность частной жизни. Статья 29 Конституции РФ каждому гарантирует свободу мысли и слова. Показательно, что именно в этой статье (в ч. 4) закрепляется право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Одновременно ст. 23 Конституции РФ предусматривает право каждого на неприкосновенность частной жизни. При этом ст. 24 Конституции РФ устанавливает запрет: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются». Иными словами, при конкуренции заявленных конституционных норм необходим поиск баланса, где проблема доксинга выступает некоторым катализатором (хотя до недавнего времени поиск баланса при появляющейся конкуренции был актуален при анализе принципа гласности судебного разбирательства [12, 13]). П. Б. Блохин справедливо отмечает, что приоритет одного права почти автоматически влечет за собой ограничение другого, что обусловливает необходимость анализа ст. 55 Конституции РФ (в части допустимости ограничений конституционных прав) [14].

С. А. Авакьян подчеркивает, что цифровизация так развернула рамки свободы получения информации, что теперь актуальна иная постановка – защита от полученной информации: происходит ее неуправляемое распространение [15]. О. А. Снежко дополняет: в Конституции отсутствует указание на поиск и распространение достоверной информации [16]. Это создает дополнительные риски и сложности при введении запретов на фейк-индустрию. Производство и тиражирование фейк-новостей получили грандиозные масштабы, когда для того, чтобы отличить вымысел от реальности, требуются значительные усилия [17].

Е. С. Аничкин отмечает, что цифровые отношения обладают определенными особенностями, которые по многим параметрам не могут регулироваться стандартными правовыми формами и средствами [18]. Действительно, информация, один раз попавшая в онлайн-мир, практически не подлежит удалению (по крайней мере, удаление сопряжено с большими сложностями). Каждый гражданин вынужден (поскольку основные социальные отношения привязаны к цифровой форме) передавать информацию в киберпространство. Ее накопление при последующей систематизации и обработке позволяет создавать цифровой профиль гражданина. При этом к большинству данных имеется открытый доступ. В таких условиях выстроить эффективную защиту права на неприкосновенность частной жизни юридическим путем очень сложно.

Зарубежный опыт в большинстве случаев исходит из того, что компенсационный механизм включается только тогда, когда присутствует негативный результат для субъекта [19]. Каждый гражданин может доксировать, собирая информацию из открытых источников, но при этом не использовать ее в противоправных целях. Это означает, что при конкуренции свободы слова и права на неприкосновенность частной жизни приоритет будет отдаваться именно свободе слова. Введение штрафных санкций будет подчиняться базовым правилам

[1] Court of Appeal. Civil Appeal № 489 of 2019 (ON APPEAL FROM HCAL 3042/2019).

допустимости ограничений указанной свободы [20, 21]. Точно также будет поддерживаться подход, связанный с криминализацией кибербуллинга – преследования в сети. Если сбор персональной информации изначально нацелен на нанесение вреда субъекту, то он может быть ограничен, а к лицу, собирающему информацию, могут применяться различные меры ответственности.

Таким образом, доксинг представляет собой серьезную форму вмешательства в частную жизнь лица. Однако современное законодательство не выработало четких подходов к механизмам защиты от данного противоправного явления. Научная интерпретация доксинга в большинстве случаев исходит из его криминологических характеристик, когда субъекту уже причиняется какой-то вред. Однако проблема находится намного глубже, поскольку затрагивает реликтовое содержание конституционного права на неприкосновенность частной жизни, где меры защиты не ограничиваются только уголовным правом.

Список литературы

1. Экономическое право : учебник / Н. С. Бондарь, Р. В. Амелин, Д. И. Артемова [и др.] ; под науч. ред. Н. С. Бондаря. М. : Проспект, 2021. 352 с. doi: 10.31085/9785392336791-2021-352. EDN: IYMONQ

2. Trottier D. Digital Vigilantism as Weaponisation of Visibility // Philosophy & Technology. 2017. Vol. 30. P. 55–72. URL: https://link.springer.com/article/10.1007/s13347-016-0216-4. doi: 10.1007/s13347-016-0216-4

3. Волкова А. В., Лукьянова Г. В., Кулакова Т. А. Гендерное измерение цифрового вигилантизма в России // Вестник Российского университета дружбы народов. Сер.: Политология. 2022. Т. 24, № 1. С. 120–135. doi: 10.22363/2313-1438-2022-24-1-120-135. EDN: GUFVNE

4. Мусеибов У. А., Куприянов Е. И. Способы совершения клеветы в социальных сетях // Российский следователь. 2022. № 8. С. 17–20. doi: 10.18572/1812-3783-2022-8-17-20. EDN: RWOIZA

5. Омелин В. Н., Горовой В. В. Анализ судебной практики по блокировке интернет-групп в мессенджерах и страниц в социальных сетях // Уголовно-исполнительная система: право, экономика, управление. 2019. № 1. С. 8–11. doi: 10.18572/2072-4438-2019-1-8-11. EDN: VPYIRC

6. Харитонова А. Р. Сохранность и анонимность персональных данных в социальных сетях // Право и Бизнес. 2019. № 4. С. 48–55. EDN: JXDJBG

7. Романовский Г. Б. Контроль над расходами чиновников // Гражданин и право. 2013. № 4. С. 3–10. EDN: PZRDJP

8. Cheung A. Doxing and the challenge to legal regulation: when personal data become a weapon // The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies In Digital Crime, Technology and Social Harms). Bingley : Emerald Publishing Limited, 2021. P. 577–594.

9. Douglas D. M. Doxing: a conceptual analysis // Ethics and Information Technology. 2016. № 18. P. 199–210.

10. Anderson B., Wood Mark A. Doxxing: a scoping review and typology // The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies In Digital Crime, Technology and Social Harms). Bingley : Emerald Publishing Limited, 2021. P. 205–226.

11. Артемова О. Е., Романовская О. В. Конституционно-правовой статус Центральной избирательной комиссии Российской Федерации : монография. М. : Проспект, 2017. 176 с. EDN: ZTFWWT

12. Михайлов В. К. Обеспечение открытости и гласности суда как гарантия независимости правосудия // Журнал российского права. 2022. Т. 26, № 2. С. 138–151. doi: 10.12737/jrl.2022.022. EDN: FCDFXE

13. Михайлов В. К. Кодексы этики профессиональных сообществ: гарантия независимости или инструмент давления? // Журнал российского права. 2021. Т. 25, № 2. С. 160–170. doi: 10.12737/jrl.2021.026. EDN: SDVKTB

14. Блохин П. Д. Структура основных прав и их правомерное ограничение: российская конституционная модель // Закон. 2022. № 12. С. 14–33. doi: 10.37239/0869-4400-2022-19-12-14-33. EDN: HPWBLF

15. Авакьян С. А. Задачи конституционного права в аспекте защиты (от) информации // Конституционное и муниципальное право. 2022. № 8. С. 3–11. doi: 10.18572/1812-3767-2022-8-3-11. EDN: OTJIGG

16. Снежко О. А. Обеспечение права на достоверную информацию в цифровом пространстве // Конституционное и муниципальное право. 2021. № 6. С. 38–43. doi: 10.18572/1812-3767-2021-6-38-43. EDN: CXSQHL

17. Плешанова О. П. Фейки в сторону // Закон. 2019. № 4. С. 114–119. EDN: YNIHHS

18. Аничкин Е. С. Модернизация конституционно-правового статуса личности в условиях формирования цифрового пространства // Конституционное и муниципальное право. 2019. № 12. С. 19–22. EDN: PTNGOI

19. Douglas H., Harris B. A., Dragiewicz M. Technology-facilitated domestic and family violence: Women's experiences // The British Journal of Criminology. 2019. Vol. 59, № 3. P. 551–570.

20. Bancroft A., Scott Reid P. Challenging the techno-politics of anonymity: The case of cryptomarket users // Information, Communication & Society. 2017. Vol. 20, № 4. P. 497–512.

21. MacAllister J. M. The doxing dilemma: Seeking a remedy for the malicious publication of personal information // Fordham Law Review. 2017. Vol. 85, № 5. Art. 21. P. 2451–2483. URL: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5370&context=flr

References

1. Bondar N.S., Amelin R.V., Artemova D.I. et al. *Ekonomicheskoe pravo: uchebnik = Economic Law*: Textbook. Moscow: Prospekt, 2021:352. (In Russ.). doi: 10.31085/9785392336791-2021-352

2. Trottier D. Digital Vigilantism as Weaponisation of Visibility. *Philosophy & Technology*. 2017;30:55–72. (In Russ.). doi: 10.1007/s13347-016-0216-4

3. Volkova A.V., Lukyanova G.V., Kulakova T.A. Gender Dimension of Digital Vigilantism in Russia. *Vestnik Rossiyskogo universiteta druzhby narodov. Ser.: Politologiya = Bulletin of Peoples' Friendship University of Russia. Series: Political Science*. 2022;24(1):120–135. (In Russ.). doi: 10.22363/2313-1438-2022-24-1-120-135

4. Museibov U.A., Kupriyanov E.I. Ways of Committing Slander in Social Media. *Rossiyskiy sledovatel = Russian investigator*. 2022;(8):17–20. (In Russ.). doi: 10.18572/1812-3783-2022-8-17-20

5. Omelin V.N., Gorovoy V.V. Analysis of Judicial Practice on Blocking Internet Groups in Instant Messengers and Pages in Social Media. *Ugolovno-ispolnitelnaya sistema: pravo, ekonomika, upravlenie = Penitentiary System: Law, Economy, Management*. 2019;(1):8–11. (In Russ.). doi: 10.18572/2072-4438-2019-1-8-11

6. Kharitonova A.R. Safety and Anonymity of Personal Data in Social Media. *Pravo i Biznes = Law and Business*. 2019;(4):48–55. (In Russ.)

7. Romanovskiy G.B. Control over the Costs of Public Officials. *Grazhdanin i parvo = Citizen and Law*. 2013;(4):3–10. (In Russ.)

8. Cheung A. Doxing and the challenge to legal regulation: when personal data become a weap-on. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology and Social Harms)*. Bingley: Emerald Publishing Limited, 2021:577–594.

9. Douglas D.M. Doxing: a conceptual analysis. *Ethics and Information Technology*. 2016;(18):199–210.

10. Anderson V., Wood Mark A. Doxxing: a scoping review and typology. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology and Social Harms)*. Bingley: Emerald Publishing Limited, 2021:205–226.

11. Artemova O.E., Romanovskaya O.V. *Konstitutsionno-pravovoy status Tsentralnoy izbiratelnoy komissii Rossiyskoy Federatsii: monografiya = Constitutional and Legal Status of the Central Election Commission of the Russian Federation: Monograph*. Moscow: Prospekt, 2017:176. (In Russ.)

12. Mikhaylov V.K. Ensuring Openness and Publicity of the Court as a Guarantee of the Independence of Justice. *Zhurnal rossiyskogo prava = Journal of Russian Law*. 2022;26(2):138–151. (In Russ.). doi: 10.12737/jrl.2022.022

13. Mikhaylov V.K. Codes of Ethics of Professional Communities: Guarantee of Independence or Instrument of Pressure? *Zhurnal rossiyskogo prava = Journal of Russian Law*. 2021;25(2):160–170. (In Russ.). doi: 10.12737/jrl.2021.026

14. Blokhin P.D. Structure of Fundamental Rights and Their Lawful Restriction: Russian Constitutional Model. *Zakon = Law*. 2022;(12):14–33. (In Russ.). doi: 10.37239/0869-4400-2022-19-12-14-33

15. Avakyan S.A. Tasks of Constitutional Law in the Aspect of Protecting (from) Information. *Konstitutsionnoe i munitsipalnoe parvo = Constitutional and Municipal Law*. 2022;(8):3–11. (In Russ.). doi: 10.18572/1812-3767-2022-8-3-11

16. Snezhko O.A. Ensuring Right to Reliable Information in Digital Space. *Konstitutsionnoe i munitsipalnoe parvo = Constitutional and Municipal Law*. 2021;(6):38–43. (In Russ.). doi: 10.18572/1812-3767-2021-6-38-43

17. Pleshanova O.P. Fake aside. *Zakon = Law*. 2019;(4):114–119. (In Russ.)

18. Anichkin E.S. Modernization of Constitutional and Legal Status of the Individual in the Conditions of Digital Space Formation. *Konstitutsionnoe i munitsipalnoe parvo = Constitutional and Municipal Law*. 2019;(12):19–22. (In Russ.)

19. Douglas H., Harris B.A., Dragiewicz M. Technology-facilitated domestic and family violence: Women's experiences. *The British Journal of Criminology*. 2019;59(3):551–570.

20. Bancroft A., Scott Reid P. Challenging the techno-politics of anonymity: The case of cryptomarket users. *Information, Communication & Society*. 2017;20(4):497–512.

21. MacAllister J.M. The doxing dilemma: Seeking a remedy for the malicious publication of personal information. *Fordham Law Review*. 2017;85(5):2451–2483. (In Russ.). Available at: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5370&context=flr

Информация об авторе / Information about the author

Е. А. Романовская – преподаватель кафедры уголовного права, Пензенский государственный университет, 440026, г. Пенза, ул. Красная, 40.

E.A. Romanovskaya – Lecturer of the Sub-department of Criminal Law, Penza State University, 40 Krasnaya street, Penza, 440026.

Автор заявляет об отсутствии конфликта интересов /
The author declares no conflict of interests

Поступила в редакцию / Received 20.06.2023

Поступила после рецензирования и доработки / Revised 28.06.2023

Принята к публикации / Accepted 07.07.2023