УДК 343.34
DOI: 10.18384/2310-6794-2023-2-106-117

ПРОТИВОПРАВНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ СОВЕРШЕНИИ МАССОВЫХ БЕСПОРЯДКОВ

Маджумаев М. М.
Российский университет дружбы народов имени Патриса Лумумбы
117198, г. Москва, ул. Миклухо-Маклая, д. 6, Российская Федерация

Аннотация
Цель. Обоснование необходимости посреднической ответственности провайдеров интернет-услуг в условиях глобальных тенденций развития информационно-коммуникационных технологий (ИКТ) и цифрового населения мира на основе анализа их влияния на организацию, координацию, подстрекательство и совершение массовых беспорядков.
Процедура и методы. В работе использованы общенаучные методы исследования – диалектический, логический, системный, а также частнонаучные методы – формально-юридический, статистический, толкования и др.
Результаты. Обозначены тенденции использования ИКТ в массовых беспорядках и сформулирован вывод о целесообразности привлечения к посреднической уголовной ответственности провайдеров интернет-услуг, имеющих организационные и технические возможности в любой момент влиять на информационные общественные отношения своих пользователей.
Теоретическая и/или практическая значимость. Представлены положения, призванные усовершенствовать вопросы уголовной ответственности за преступления, совершаемые с использованием высоких технологий, в т. ч. переосмыслить уголовную политику.

Ключевые слова: информационные и коммуникационные технологии, массовые беспорядки, организация массовых беспорядков, подстрекательство к массовым беспорядкам, посредническая ответственность, провайдеры интернет-услуг, скопление толпы

THE UNLAWFUL UTILIZATION OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN RIOTING

M. Madzhumayev
RUDN University
ul. Miklukho-Maklaya 6, Moscow 117198, Russian Federation

Abstract
Aim. Justification of the need for intermediary responsibility of Internet service providers in the context of global trends in information and communication technology (ICT) and digital population of the world based on the analysis of their impact on the organization, coordination, incitement and commission of riots.
Methodology. The work used general scientific methods of research - dialectical, logical, systematic, as well as private scientific methods - formal-legal, statistical, interpretative, etc.
Results. The trends in the use of ICTs in riots were outlined, leading to the conclusion that it is reasonable to hold internet service providers criminally liable for the intermediary if they have the organizational and technical capacity to intervene in the informational social relations of their users at any time.
Research implications. Measures to address the criminal liability issues of offenses perpetrated utilizing high technology are presented, along with the reconceptualization of the criminal policy.

Keywords: information and communication technologies, riots, organization of riots, incitement to riot, intermediary liability, internet service providers, mob assembly

Введение

Доступность, надёжность, безопасность информационно-телекоммуникационных сетей и систем являются критически важными факторами повышения уровня жизни, занятости, улучшения деятельности организаций бизнеса и гражданского общества, а также реализации экономического потенциала страны. Информация в формате цифровых данных, информационные объекты, связанные с цифровыми данными, являются объектами цифровых правоотношений[1].

Под информационными и коммуникационными технологиями (ИКТ) в настоящей статье будет подразумеваться предметы (устройства) материального мира, сети, системы, процессы и способы, отличающиеся качественно-передовым технологическим уровнем, предназначенные для создания, поиска, приёма, доступа, обработки, управления, хранения и передачи любых сведений (сообщений, данных), представленных в виде электрических сигналов, вне зависимости от того, какими средствами они хранятся, обрабатываются и передаются. К таковым также могут быть отнесены, электронные вычислительные машины и другие компьютерные устройства. Последние в целом определяются в качестве компьютерных устройств в п. 2 Постановления Пленума Верховного Суда Российской Федерации № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"»[2].

К числу компьютерных устройств принято относить все виды электронных устройств, пригодных к выполнению операций по приёму, обработке, хранению и передаче закодированной в форме электрических сигналов информации, изготовленные или модифицированные промышленным либо кустарным способами. В частности, это персональные компьютеры, в т. ч. портативные ноутбуки и планшетные устройства, мобильные телефоны, смартфоны и другие виды электроники, включая объекты физического происхождения, оборудованные интегрированными вычислительными устройствами, инструментами и технологиями по сбору и передаче информации, взаимодействию пользователей между собой или взаимодействию с внешней средой без участия самого пользователя.

Непосредственно в ходе совершения общественно опасных деяний информационно-коммуникационные технологии могут быть использованы и фактически применяются в качестве «высокотехнологичных» средств совершения преступления как один из элементов объективной стороны состава преступления.

Эксплуатация информационно-коммуникационных технологий при совершении преступлений сопряжена с вовлечением, помимо непосредственного исполнителя преступления, ещё и других лиц, обеспечивающих техническое сопровождение в фоновом режиме. Обозначая их, в статье будем использовать такие понятия, как: *провайдеры интернет-услуг* (и их разновидности: *провайдеры доступа*, *хостинг-провайдеры*, *провайдеры услуг кэширования*, *магистральные провайдеры и провайдеры «последней мили»*), *оператор связи, оператор информационной системы*, а также *владелец сайта в сети Интернет*. Здесь речь идёт о субъектах рассматриваемых правоотношений (технического сопровождения), в отношении которых осуществляется исследование на предмет возможного признания их субъектом преступления, т. е. привлечения к посредственной уголовной ответственности за деяния их пользовате-

[1] Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. М.: Проспект, 2020. 640 с.

[2] Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» // Верховный Суд Российской Федерации: [сайт]. URL: https://vsrf.ru/documents/own/31913/ (дата обращения: 06.02.2023).

лей. В соответствующих частях статьи представлены их определения.

Распространение ИКТ, особенно мобильной телефонии, произошло стремительнее, чем коммуникационных технологий предыдущих поколений (рис. 1). Наблюдается быстрый переход к мобильным сетям и устройствам в качестве основного средства телекоммуникаций, включая доступ в интернет.

В настоящее время более 95% территории Земли охватывают мобильные сети, а мобильные широкополосные сети, которые обеспечивают гораздо лучшее подключение к интернету, покрывают около 94%[1]. По состоянию на конец 2022 г. интернетом пользовались более половины мирового населения (66%), при этом доля молодёжи (от 15 до 24 лет) увеличилась и составила более 75% (рис. 2). Мировая прогрессивная тенденция в области распространения ИКТ и роста числа пользователей интернета позволяет говорить о цифровом населении Земли и (или) отдельных стран.

В реалиях современного мира использование ИКТ имеет как положительные, так и отрицательные аспекты. Обратной стороной является нарастающая тенденция совершения преступлений с использованием таких технологий. Так, в настоящее время они взяты на вооружение террористическими, организованными преступными и экстремистскими формированиями в целях оказания влияния на государственную политику и (или) принимаемые властью решения.

Информационно-коммуникационные технологии как высокотехнологичное средство совершения массовых беспорядков

Как свидетельствуют события последнего десятилетия в разных странах, с помощью таких технологий можно воздействовать на сознание широких масс людей и впоследствии провоцировать эскалацию беспорядков. Показательными в этом смысле являются события «арабской весны», «цветные революции» (например, в странах бывшего Восточного блока), беспорядки в Миннеаполисе с последующим распространением на другие города США и т. д. Отдельно можно выделить и тактику, используемую несистемной оппозицией в ряде стран, когда в интернете размещаются призывы к «мирным» собраниям, заведомо спланированным с целью обострения ситуации, да к тому же не санкционированным официально.

Существуют мнения относительно исключительной роли интернета в коллективных действиях: интернет порождает экстремизм; интернет позволяет людям подключаться к «мега-подпольной» площадке участников; интернет охватывает широкий диапазон пользователей в «киберкаскаде»; интернет расширяет географическое разнообразие участников беспорядков; интернет повышает скорость и спонтанность; интернет делает рассредоточение толпы невыполнимым [9; 12; 13].

Такие учёные, как Д. Кристенсен и Ф. Гарфиас, выделяют прямое и косвенное влияние мобильных телефонов на различные виды общественной активности. Потенциальная координация лиц, обмен информацией о месте, времени и форме протестных акций через мобильные телефоны демонстрируют прямой эффект. Косвенный эффект выражается в расширении круга пользователей мобильных телефонов [9, p. 91–92]. В таком случае, когда возникают необходимые триггеры, широкая общественность становится о них осведомленной, и потенциальная мобилизация значительного числа людей – более вероятной.

Влияние ИКТ на массовые беспорядки рассматривается профессором К. Фуксом в двух плоскостях:

1) *в оптимистической форме*: социальные сети поспособствуют преодолению беспорядков; следует контролировать социальные сети и мобильные телефоны; необходимо ограничить доступ к мессен-

[1] Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU), Development Sector. 2022. Official text [Электронный ресурс]. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (дата обращения: 14.02.2023).

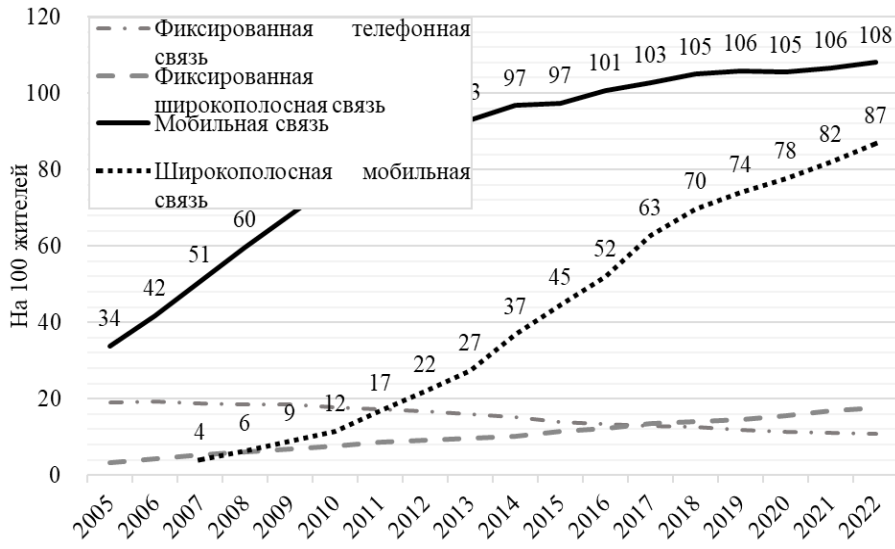

Рис. 1 / Fig. 1. Глобальные тенденции в области ИКТ в 2005–2022 гг. (на 100 жителей) / Global trends in ICTs in 2005–2022 (per 100 inhabitants)

Источник: Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU), Development Sector. 2022. Official text [Электронный ресурс]. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (дата обращения: 14.02.2023).

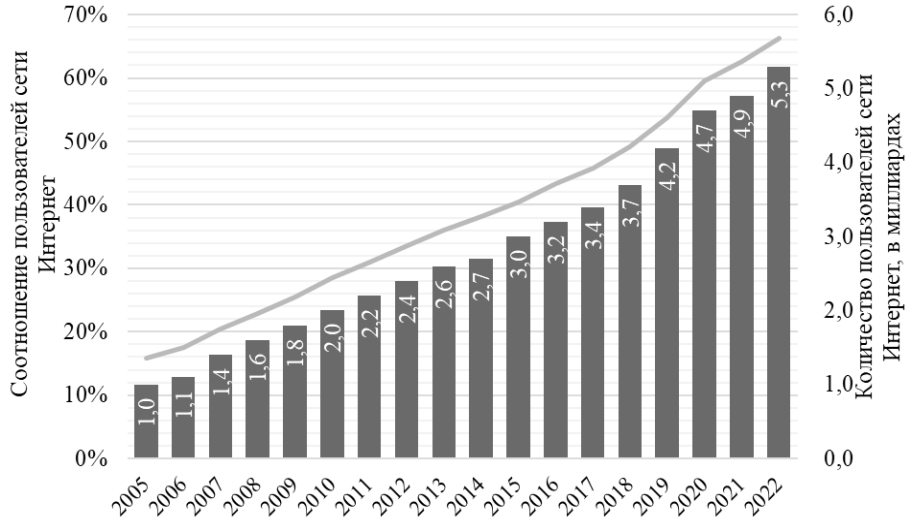

Рис. 2 / Fig. 2. Пользователи интернете в 2005–2022 гг., % / Individuals using the Internet in 2005–2022, %

Источник: Measuring digital development Facts and Figures 2022. United Nations International Telecommunication Union (ITU), Development Sector. 2022. Official text [Электронный ресурс]. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (дата обращения: 14.02.2023).

джеру *Blackberry*[1]; нужно усилить систему видеонаблюдения;

2) *в пессимистической форме*: социальные сети способствуют появлению, развитию, стимулированию, усилению, организации и разжиганию насилия.

Попытка объяснить причины беспорядков не сложными социальными противоречиями, а лишь технодетерминистической инструментальной идеологией является всего лишь «фетишизмом вещей» [12, p. 383–391].

Рассматривая вопрос об использовании ИКТ во время массовых беспорядков, можно выделить следующие варианты их применения:

– информационное взаимодействие, коммуникация, призывы;

– мобилизация людей;

– организация беспорядков;

– распределение ролей;

– координация в противостоянии с правоохранительными органами;

– координация в достижении конечной цели.

При проявлении гражданского недовольства в связи с определёнными социальными проблемами ИКТ способствуют обмену информацией, общению и призывам к определённым (не всегда законным) действиям.

Катализаторами общественного волнения могут быть самые разные факторы: неправомерные либо правомерные действия полиции; безработица; неудовлетворительные жилищные условия; ненадлежащее качество образования; неудовлетворительные рекреационные условия и программы; неэффективная политическая структура и механизмы обжалования; дискриминационное отношение; несправедливое отправление правосудия; неадекватные федеральные программы; неприемлемые муниципальные услуги; несоответствующие программы социального обеспечения [10, p. 8–20].

Зачастую СМИ не транслируют всей сути публичной активности. Допускается блокирование отдельных веб-сайтов и коммуникационных потоков. ИКТ же обеспечивают преодоление подобных медиаструктур, предоставляя информацию без «фильтров» и цензуры.

Процесс массовой «мобилизации» может длиться от нескольких часов, дней, недель до нескольких месяцев и задействовать значительное количество граждан. К фактору мобилизации лиц относятся механизмы, способствующие вовлечению отдельных людей в коллективные противоправные действия [14, p. 797–798]. Помимо последних вовлекаются различные формирования, как общественные движения, так и неформальные структуры в виде ассоциаций активистов. В этом контексте важны наличие причин для общественного недовольства и желание исправить ситуацию, устранение таких причин демонстрациями, чтобы власти прислушались к требованиям населения. В условиях массовой мобилизации происходит воздействие на общественное мнение путём привлечения внимания и вовлечения населения [16, p. 7–12]. Отличительная черта такого феномена заключается в его деструктивном характере.

Отмечается, что ИКТ сокращают затраты на обнародование необходимой информации об общественных движениях в короткий промежуток времени, тем самым способствуя росту числа активных участников [8, p. 78–83]. Использование ИКТ позволяет моделировать децентрализованные, неиерархические организационные формы толпы. Безусловно, подобные свойства ИКТ способствуют организации массовых беспорядков [11, p. 90].

Тактические планы по определению формы реализации коллективных действий и распределению ролей участников мобилизованной толпы могут быть обозначены организаторами с помощью ИКТ. Распределение между участниками толпы функциональных ролей осуществляется на этапе приготовления к совершению и (или) осуществле-

[1] Бесплатный сервис сообщений, доступный на телефонах BlackBerry, известный как BBM, широко использовался для коммуникации, обмена информацией и планирования беспорядков 2011 г. в Лондоне, Бирмингеме, Манчестере, Сэлфорде, Ливерпуле и Ноттингеме.

нию актов массовых беспорядков в рамках преступного умысла. Причём это может сопровождаться условной дисциплинированностью, активной деятельностью организаторов, (при необходимости) продуманной системой обеспечения орудиями и средствами совершения преступления.

Как правило, любая социальная активность граждан, будь то санкционированная или несанкционированная, сопровождается представителями органов правопорядка в целях обеспечения общественного порядка и общественной безопасности. В ходе несогласованных демонстраций высока вероятность столкновений участников коллективных действий с сотрудниками правоохранительных органов. Интересы организаторов подобных акций могут диктовать несколько вариантов развития событий:

1) организаторы акции не заинтересованы в жёстком противостоянии с силами правопорядка, а потому призывают участников несанкционированной акции прекратить её, как только этого потребовала полиция;

2) организаторы априори заинтересованы в эскалации противостояния и своими провоцирующими действиями (призывами, приказами и т. д.) способствуют скорейшим и жёстким столкновениям с силами правопорядка;

3) организаторы акции решают не подчиняться законным требованиям властей и начинают «на месте» координировать действия участников акции, которые будут направлены на противодействие силам правопорядка.

Во всех вышеперечисленных случаях оповещения могут передаваться через средства ИКТ: о приближении национальной гвардии, полиции (отрядов по ликвидации беспорядков); о координации действий внутри «малых групп»; о руководстве к дальнейшим массовым насильственным акциям.

Участникам мобилизованной толпы должен быть известен конкретный план действий по реализации противоправной социальной активности, поскольку неопределённость действий других участников может снизить эффективность акции в целом.

Посредническая ответственность провайдеров интернет-услуг

Рассматривая влияние ИКТ на массовые беспорядки, необходимо определить круг виновных лиц, которых можно привлечь к уголовной ответственности. Мы видим, что ИКТ и соответствующие девайсы выступают в качестве средств и орудий совершения преступления. Достаточно обратиться к изучению объективной стороны преступления, предусмотренного ст. 212 УК РФ, чтобы увидеть «многомерность» самостоятельных деяний, влекущих уголовную ответственность. Как минимум призывы, организация и склонение к массовым беспорядкам невозможны в современных условиях без применения ИКТ.

Однако крайне важной проблемой на сегодня, является вопрос об уголовной ответственности провайдеров интернет-услуг. Причиной тому служит то обстоятельство, что при распространении информации в сети задействованы, наряду с самим автором, и другие субъекты, в частности правообладатель сетевого информационного ресурса, владелец сервера и т. д. [4, с. 103]. Провайдеры интернет-услуг могут быть провайдерами доступа, хостинг-провайдерами, провайдерами услуг кэширования, магистральными провайдерами, и провайдерами «последней мили». Определяя юридическую ответственность, следует дифференцировать провайдеров интернет-услуг на основе выполняемых ими функций [5, с. 20], которые описываются ниже.

В функции провайдеров доступа входит предоставление доступа к контенту третьих лиц путём перемещения, маршрутизации данных без их постоянного хранения [2, с. 63]. Например, посредством такого провайдера пользователь, подключаясь к интернету или информационной системе из своего местоположения, соединяется с базовой сетью интернета [2, с. 63].

Хостинг-провайдеры осуществляют хранение, обеспечивают доступность контента третьих лиц как на собственной, так и на арендованной технической базе (сервере). Вследствие этого контент на посто-

янной основе находится в интернет. Чаще всего пользователям предоставляется прямой доступ для загрузки контента в сеть, минуя механизм ручного контроля со стороны хостинг-провайдера [2, с. 63].

Механизм автоматического временного хранения и передачи данных в целях оптимизации технологического процесса передачи информации осуществляется провайдером услуг кэширования. Будучи технологическим процессом, кэширование с целью сокращения интенсивности потока, ускорения загрузки веб-сайтов и улучшения передачи информации обеспечивает промежуточное хранение в памяти кэша сервера [7, с. 42].

Предоставление услуг передачи данных и связи обычно обеспечивается транспортной телекоммуникационной инфраструктурой. Магистральные провайдеры прокладывают опорные линии передачи данных, а именно соединяют стратегические части интернета с магистральными линиями [3, с. 44].

Коммуникационная линия напрямую от магистральных сетей до пользователя/потребителя прокладывается провайдерами «последней мили» [6, с. 48].

Субъекты рассматриваемых правоотношений также предусматриваются законодательством Российской Федерации об информации и связи.

Федеральный закон № 126-ФЗ «О связи»[1] определяет субъекта, оказывающего услуги связи, в частности операции по приёму, обработке, хранению, передаче, доставке электросвязи или почтовых отправлений, основываясь на понятии оператора связи. В соответствии с п. 12 ч. 1 ст. 2 ФЗ «О связи» таковым признаётся юридическое лицо или индивидуальный предприниматель, оказывающий указанные услуги на основании соответствующей лицензии.

В соответствии с Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2] субъектом правоотношений, возникающих при реализации права на поиск, получение, передачу, производство и распространение информации, помимо обладателя информации устанавливаются:

– оператор информационной системы;
– владелец сайта в сети Интернет;
– провайдер хостинга.

Под оператором информационной системы согласно п. 12 ч. 1 ст. 2 ФЗ «Об информации» подразумевается физическое или юридическое лицо, занимающееся эксплуатацией информационной системы наряду с обработкой информации в её базах данных. В п. 17 ч. 1 ст. 2 содержится определение владельца сайта в сети Интернет в качестве лица, независимо и по собственному усмотрению определяющего порядок использования сайта в сети Интернет, включая процедуру размещения информации на таком сайте. В той же норме в п. 18 провайдером хостинга обозначается лицо, обеспечивающее услуги по выделению вычислительных мощностей для размещения информации на информационной системе, постоянно подключённой к интернету.

Основной закон России гарантирует право на свободу мысли и слова, а также право каждого на поиск, получение, передачу, производство и распространение информации любым законным способом (ч.ч. 1, 4 ст. 29 Конституции РФ). А также запрещает принуждать кого-либо высказывать свои мнения и убеждения или отрицать их (ч. 3 ст. 29 Конституции РФ).

Безусловно, каждый имеет право на самовыражение с соблюдением установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования. При возникновении коллизии между правом

[1] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Официальный интернет-портал правовой информации: [сайт]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102082548&rdk= (дата обращения: 06.02.2023).

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Официальный интернет-портал правовой информации: [сайт]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264&rdk= (дата обращения: 06.02.2023).

на свободу самовыражения, ассоциаций (ст. 31 Конституции РФ) и обеспечением общественного порядка, общественной безопасности важно установить баланс. Свобода слова и ассоциаций – это фундаментальные права граждан в демократическом и правовом обществе. Столь же важна и безопасность мирного населения, подвергающегося непосредственной опасности, которой угрожает потенциальная эскалация действий по осуществлению упомянутых прав.

Следовательно, закономерен запрет распространения информации, направленной на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность (ч. 6 ст. 10 ФЗ «Об информации»).

В процессе квалификации деяний по подстрекательству, склонению, вербовке или иному вовлечению лица в совершение актов массовых беспорядков в интернете следует учитывать и вышеупомянутое информационное законодательство. При распространении в соцсетях информации с целью привлечения лиц к участию в массовых беспорядках владелец сайта и (или) страницы в интернете, и (или) информационной системы, и (или) программного обеспечения для электронных средств обработки данных обязан руководствоваться действующим законодательством страны, а именно: он не должен допускать использование ресурса для совершения преступлений, а также распространения сведений, пропагандирующих культ насилия и жестокости (п. 1 ч. 1 ст. 10.6 ФЗ «Об информации»). Более того, в его обязанности входит мониторинг социальной сети на предмет выявления (п.п. е, з, п. 5 ч. 1 ст. 10.6 ФЗ «Об информации»):

– информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

– информации, содержащей призывы к массовым беспорядкам;

– информации, содержащей призывы к участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка;

– недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создаёт угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращению функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи.

Обнаружив такую информацию, владелец сайта обязан немедленно принять меры по ограничению доступа к ней (ч. 4 ст. 10.6 ФЗ «Об информации»). Подобная практика чревата возможными злоупотреблениями со стороны владельца социальной сети при реализации лицом права на свободу слова. Хотя российское законодательство предусматривает право пользователя обратиться к владельцу социальной сети, а затем в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, – Роскомнадзор – с заявлением об отмене мер, принятых по ограничению доступа к конкретной информации, тем не менее требуется наличие эффективной процедуры рассмотрения таких обращений.

Немаловажной является и политика конкретных каналов информационных систем и программ, обеспечивающих возможность передачи и приёма сообщений путём сквозного шифрования (*end-to-end encryption*). Криптографические алгоритмы в таких средствах ИКТ составлены по принципу шифрования таким образом, что отправляемые и получаемые сообщения предназначены только для двух сторон, исключается получение информации третьими лицами, в т. ч. государствен-

ными структурами [15, p. 138]. Наряду с *Telegram* к таким системам и программам можно отнести *SafeSMS, None of your business (NOYB), FlyByNight, Pretty Good Privacy (PGP), Off-the-record (OTR), Signal.* Естественно, организаторы беспорядков будут эксплуатировать такие технологии.

Назревают 2 вопроса: о возможности блокировки конкретных лиц, пользующихся ИКТ в незаконных целях, представителями этих сетей, и о допустимости мониторинга переписки граждан посредством таких технологий со стороны государства. В отношении первого вопроса известны примеры по блокированию учётных записей 45-го Президента США Д. Трампа, а также других учётных записей, ретранслирующих его сообщения. Тем не менее существуют многочисленные аккаунты, которые подстрекают, призывают, вербуют и вовлекают людей в насильственные действия, оставаясь при этом незамеченными или незаблокированными. Касаемо второго вопроса представляется, что контроль и мониторинг за перепискаами допустимы в случаях угрозы безопасности личности, общества и государства.

Анализ положений российского информационного законодательства позволяет констатировать следующий порядок действий при обнаружении в информационно-телекоммуникационных сетях, в т. ч. в интернете, информации, призывающей к массовым беспорядкам, экстремистской деятельности или участию в массовых (публичных) мероприятиях с нарушением установленного порядка (ст. 15.3 ФЗ «Об информации», ст. 46 ФЗ «О связи»):

1) генеральный прокурор РФ или его заместители направляют в Роскомнадзор требование об ограничении доступа к таким информационным ресурсам;

2) Роскомнадзор уведомляет редакцию сетевого издания о необходимости удаления указанной информации; последняя обязана удалить такую информацию;

3) в случае непринятия редакцией мер по незамедлительному удалению соответствующей информации Роскомнадзор направляет оператору связи требование об ограничении доступа к сетевому изданию. Оператор связи обязан безотлагательно ограничить доступ к такому сетевому изданию;

4) в остальных случаях при поступлении запроса, указанного в п. 1, Роскомнадзор идентифицирует хостинг-провайдера, направляет ему запрос об ограничении доступа к такой информации;

5) хостинг-провайдер информирует владельца информационного ресурса о необходимости немедленного удаления информации; у последнего имеется 24 ч на выполнение данного требования;

6) при отказе или бездействии последнего хостинг-провайдер самостоятельно ограничивает доступ к такой информации;

7) в соответствии с ФЗ «О связи» оператор связи, предоставляющий доступ к интернету, в установленных случаях обязан ограничить и возобновить доступ к информации и обеспечить установку технических средств контроля. Он также обязан предоставлять в Роскомнадзор данные о фактическом месте установки указанных технических средств (п. 5 ч. 1 ст. 46 ФЗ «О связи»).

По фактам выявления нарушений, способных нанести ущерб правам, законным интересам, жизни или здоровью граждан, а также безопасности государства и правопорядку, коими являются призывы, организация и подстрекательство к массовым беспорядкам, наряду с такими мерами, как предупреждение о приостановлении или лишении лицензии, лица, нарушившие законодательство РФ о связи, подлежат уголовной, административной и гражданско-правовой ответственности (ч. 1 ст. 68 ФЗ «О связи»).

Квалифицируя деяния в виде подстрекательства, склонения, вербовки или иного вовлечения лица в совершение актов массовых беспорядков в интернете, следует однозначно выяснить выполняемую каждым конкретным лицом (провайдерами интернет-услуг) функцию при совершении общественно опасного деяния. Наличие вины и, соответственно, наступление уголовной ответственности за эти

деяния зависит от когнитивных элементов в психике лица, т. е. интеллектуальных (способность понимать противоправность своего поведения, предвидеть последствия), и направленности психических и физических усилий на принятие решения, т. е. волевых (желание наступления этих последствий) элементов вины.

В этом плане можно согласиться со взглядами исследователей С. А. Перчаткина, М. Е. Черемисинова и др. [5] и М. А. Цирина [6], полагающих, что провайдеры интернет-услуг, оказывающие технологическую поддержку в коммуникации субъектов, т. е. предоставляющие только техническую поддержку/подключение доступа к сети, не подлежат уголовной ответственности. По их мнению, уголовная ответственность провайдеров интернет-услуг наступает в случае наличия у них организационно-технической возможности в любое время воздействовать на информационные общественные отношения своих пользователей. Соответственно, провайдеры доступа, провайдеры услуг кэширования, магистральные провайдеры, провайдеры «последней мили» не должны привлекаться к ответственности, т. к. их деятельность заключается лишь в технологической поддержке подключения пользователей к сети [5, с. 20; 6, с. 49].

В отношении хостинг-провайдера существует особый подход ответственности в зависимости от конкретных выполняемых функций. Если хостинг-провайдер предлагает только дисковое пространство для физического размещения информации, постоянно находящейся в сети, то он не должен нести ответственность. Если же компетентные органы уведомили о незаконном содержании загруженной информации, а также в случаях, когда имеется техническая возможность ограничить доступ к такой информации, провайдер хостинга должен нести ответственность, если не ограничивает доступ к такой информации [5, с. 20].

Заключение

С учётом изложенного можно утверждать, что ответственность провайдеров интернет-услуг за непринятие мер по ограничению доступа у пользователей интернета к информации, содержащей призывы, подстрекательство, вербовку или иное вовлечение лиц в совершение актов массовых беспорядков, возникает только в том случае, если они осознают общественную опасность неограничения доступа к такой информации, предвидят опасные последствия в виде массовых беспорядков, явившихся прямым последствием такого неограничения, и при этом сознательно направляют свои умственные и физические усилия на это.

При недоказанности вины лицо не подлежит уголовной ответственности, поскольку Уголовный кодекс запрещает объективное вменение (ст. 5 УК РФ). Установление вины провайдера основывается на оценке фактических обстоятельств конкретного дела, наличия или отсутствия в действиях лица психического отношения к бездействию (неограничению доступа к указанной информации), которое впоследствии привело к массовым беспорядкам.

Хотя в теории науки уголовного права встречаются утверждения, что объективное вменение фактически существует в правоприменительной практике, а это противоречит принципу виновности [1, с. 17]. В частности, объективное вменение рассматривается как необходимый инструмент в противодействии преступности при дополнении УК чёткими критериями его применения [1, с. 18].

В заключении отметим, что обзор литературы свидетельствует о том, что атрибуты информационного общества, будучи вспомогательными и периферийными, не являются непосредственным детерминантом массовых беспорядков. Отклоняясь от техно-детерминистской модели, автор склоняется ко взглядам профессора К. Фукса, который рассматривает исключительно социальные отношения как триггерные факторы конфликтной атмосферы.

Статья поступила в редакцию 27.02.2023.

ЛИТЕРАТУРА

1. Бавсун М. В. Целесообразность объективного вменения // Научный вестник Омской академии МВД России. 2005. № 2. С. 15–18.
2. Жарова А. К. О необходимости правовой классификации операторов сети Интернет // Бизнес-информатика. 2011. № 3. С. 60–65.
3. Ожиганова Е. М. Применение системы мотивации временных сотрудников на примере АО «ЭР-Телеком холдинг» // Бизнес-образование в экономике знаний. 2016. № 1. С. 43–48.
4. Рассолов И. М. Правовые проблемы обеспечения информационной безопасности: юридическая ответственность операторов связи // Вестник Московского университета МВД России. 2013. № 12. С. 103–108.
5. Социальные интернет-сети: правовые аспекты / С. А. Перчаткина, М. Е. Черемисинова, А. М. Цирин, М. А. Цирина, Ф. В. Цомартова // Журнал российского права. 2012. № 5. С. 14–24.
6. Цирина М. А. Распространение пронаркотической информации в Интернете: меры противодействия // Журнал российского права. 2012. № 4. С. 44–50.
7. Чубукова С. Г. Проблемы правового статуса информационного посредника // Вестник Академии права и управления. 2017. № 2. С. 39–44.
8. An Exploratory Examination of Agent-based Modeling for the Study of Social Movements / A. B. Frank, M. N. Posard, T. C. Helmus, K. Marcinek, J. Grana, O. Kahn, R. Zutshi. RAND Corporation, 2022. 120 p.
9. Christensen D., Garfias F. Can You Hear Me Now?: How Communication Technology Affects Protest and Repression // Quarterly Journal of Political Science. 2018. Vol. 13. Iss. 1. P. 89–117.
10. Cobb J., Guariglia M. The Essential Kerner Commission Report. Liveright Publ., 2021. 320 p.
11. Duncan F. Collective Action and Digital information Communication Technologies: The Search for Explanatory Models of Social Movement Organizations' Propensity to Use DICTS in Developed Democracies: Thesis Doctor of Philosophy (PhD) in Communication. Pennsylvania, 2015. 208 p.
12. Fuchs C. Social media, riots, and revolutions // Capital & Class. 2012. Vol. 36. Iss. 3. P. 383–391.
13. Gaudette T., Scrivens R., Venkatesh V. The role of the internet in facilitating violent extremism: insights from former right-wing extremists // Terrorism and Political Violence. 2022. Vol. 34. Iss. 7. P. 1339–1356.
14. Ley S. High-risk participation: Demanding peace and justice amid criminal violence // Journal of peace research. 2022. Vol. 59. Iss. 6. P. 794–809.
15. Schillinger F., Schindelhauer C. End-to-End Encryption Schemes for Online Social Networks // Security, Privacy, and Anonymity in Computation, Communication, and Storage: 12th International Conference, SpaCCS Atlanta, USA, July 14–17, 2019 Proceedings. Springer Nature Switzerland AG, 2019. P. 133–146.
16. Shultziner D., Goldberg S. The stages of mass mobilization: separate phenomena and distinct causal mechanisms // Journal for the theory of social behaviour. 2019. Vol. 49. Iss. 1. P. 2–23.

REFERENCES

1. Bavsun M. V. [The expediency of objective imputation]. In: *Nauchnyy vestnik Omskoy akademii MVD Rossii* [Scientific Bulletin of Omsk Academy of the Ministry of Internal Affairs of Russia], 2005, no. 2, pp. 15–18.
2. Zharova A. K. [On the need for a legal classification of Internet operators]. In: *Biznes-informatika* [Business Informatics], 2011, no. 3, pp. 60–65.
3. Ozhiganova E. M. [Application of the motivation system for temporary employees on the example of ER-Telecom Holding JSC]. In: *Biznes-obrazovaniye v sfere znaniy* [Business education in the knowledge economy], 2016, no. 1, pp. 43–48.
4. Rassolov I. M. [Legal problems of ensuring information security: legal responsibility of telecom operators]. In: *Vestnik Moskovskogo universiteta MVD Rossii* [Bulletin of Moscow University of the Ministry of Internal Affairs of Russia], 2013, no. 12, pp. 103–108.
5. Perchatkina S. A., Cheremisinova M. E., Tsirin A. M., Tsirina M. A., Tsomartova F. V. [Social Internet networks: legal aspects]. In: *Zhurnal rossiyskogo prava* [Journal of Russian Law], 2012, no. 5, pp. 14–24.
6. Tsirina M. A. [Distribution of pro-drug information on the Internet: countermeasures]. In: *Zhurnal rossiyskogo prava* [Journal of Russian law], 2012, no. 4, pp. 44–50.
7. Chubukova S. G. [Problems of the legal status of an information intermediary]. In: *Vestnik akademii prav i upravleniya* [Bulletin of the Academy of Law and Management], 2017, no. 2, pp. 39–44.
8. Frank A. B., Posard M. N., Helmus T. C., Marcinek K., Grana J., Kahn O., Zutshi R. An Exploratory Examination of Agent-based Modeling for the Study of Social Movements. RAND Corporation, 2022. 120 p.

9. Christensen D., Garfias F. Can You Hear Me Now?: How Communication Technology Affects Protest and Repression. In: Q*uarterly Journal of Political Science*, 2018, vol. 13, iss. 1, pp. 89–117.
10. Cobb J., Guariglia M. The Essential Kerner Commission Report. Liveright Publ., 2021. 320 p.
11. Duncan F. Collective Action and Digital information Communication Technologies: The Search for Explanatory Models of Social Movement Organizations' Propensity to Use DICTS in Developed Democracies: Thesis Doctor of Philosophy (PhD) in Communication. Pennsylvania, 2015. 208 p.
12. Fuchs C. Social media, riots, and revolutions. In: *Capital & Class,* 2012, vol. 36, iss. 3, pp. 383–391.
13. Gaudette T., Scrivens R., Venkatesh V. The role of the internet in facilitating violent extremism: insights from former right-wing extremists. In: *Terrorism and Political Violence,* 2022, vol. 34, iss. 7, pp. 1339–1356.
14. Ley S. High-risk participation: Demanding peace and justice amid criminal violence. In: *Journal of Peace Research,* 2022, vol. 59, iss. 6, pp. 794–809.
15. Schillinger F., Schindelhauer C. End-to-End Encryption Schemes for Online Social Networks. In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 12th International Conference, SpaCCS Atlanta, USA, July 14–17, 2019 Proceedings*. Springer Nature Switzerland AG, 2019, pp. 133–146.
16. Shultziner D., Goldberg S. The stages of mass mobilization: separate phenomena and distinct causal mechanisms. In: *Journal for the Theory of Social Behavior*, 2019, vol. 49, iss. 1, pp. 2–23.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Маджумаев Мурад Мамедович – кандидат юридических наук, ассистент кафедры уголовного права, уголовного процесса и криминалистики, Юридического института Российского университета дружбы народов им. Патриса Лумумбы (РУДН);
e-mail: murad.mad@outlook.com

INFORMATION ABOUT THE AUTHOR

Murad M. Madzhumayev – Cand. Sci. (Law), Assistant, Department of Criminal Law, Criminal Procedure and Criminalistics, Law Institute, RUDN University;
e-mail: murad.mad@outlook.com

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Маджумаев М. М. Противоправное использование информационно-коммуникационных технологий при совершении массовых беспорядков // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2023. № 2. С. 106–117.
DOI: 10.18384/2310-6794-2023-2-106-117

FOR CITATION

Madzhumayev M. M. The Unlawful Utilization of Information and Communication Technologies in Rioting. In: *Bulletin of Moscow Region State University. Series: Jurisprudence*, 2023, no. 2, pp. 106–117.
DOI: 10.18384/2310-6794-2023-2-106-117