УДК 343.98

Кульпин Алексей Андреевич
Санкт-Петербургский юридический институт (филиал)
Университета прокуратуры Российской Федерации
Россия, Санкт-Петербург
Alex.kulp@yandex.ru
Kulpin Aleksey
St. Petersburg Law Institute (branch)
University of the Prosecutor's Office of the Russian Federation
Saint-Petersburg, Russia

ИСПОЛЬЗОВАНИЕ ВЫСОКИХ ТЕХНОЛОГИЙ ДЛЯ ПУБЛИЧНОГО РАСПРОСТРАНЕНИЯ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ, ПРЕДУСМОТРЕННОЙ СТ. 207.3 УК РФ

Аннотация: в статье представлены результаты исследования способов совершения публичного распространения заведомо ложной информации, предусмотренной ст. 207.3 УК РФ посредством современных технологий. Автор рассматривает такие аспекты, как создание фейковых новостных сайтов, использование социальных сетей и мессенджеров для распространения ложной информации, а также методы и средства, используемые преступниками для манипулирования общественным мнением. В целом, статья представляет собой важный вклад в изучение проблемы распространения заведомо ложной информации через Интернет и способов совершения этого преступления.

Ключевые слова: публичное распространение, заведомо ложная информация, фейк, способ совершения преступления, 207.3 УК РФ, специальная военная операция.

USE OF HIGH TECHNOLOGIES FOR THE PUBLIC DISTRIBUTION OF KNOWNLY FALSE INFORMATION PROVIDED BY ART. 207.3 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Annotation: the article presents the results of a study of ways to commit the public dissemination of knowingly false information under Art. 207.3 of the Criminal Code of the Russian Federation through modern technologies. The author considers such aspects as the creation of fake news sites, the use of social networks and instant messengers to spread false information, as well as the methods and means used by criminals to manipulate public opinion. In general, the article is an important contribution to the study of the problem of dissemination of deliberately false information via the Internet and the methods of committing this crime.

Key words: public distribution, deliberately false information, fake, the manner in which the crime was committed, 207.3 of the Criminal Code of the Russian Federation, special military operation.

В современной криминалистической литературе достаточно сложно найти работу, посвященную предварительному расследованию того или иного вида (разновидности) преступления, в которой не было бы упоминания о способах совершения преступления. Не является исключением и расследование публичного распространения заведомо ложной информации, предусмотренной ст. 207.3 УК РФ, посредством современных технологий.

Обобщенные сведения о способе преступления имеют высокое практическое значение, что неоднократно находило свое отражение в криминалистической литературе. По мнению В.Н. Кудрявцева, это связано с тем, что способ преступления отражает характер деяний преступника и является ключевым элементом при формировании информации о посягательстве, лице его совершившем, местонахождении следов преступления и других важных аспектах [3, с. 61]. Способ преступления определяется детерминированными

особенностями личности преступника, системой взаимосвязанных действий или воздержания от них, направленных на достижение преступной цели. Результаты анализа судебно-следственной практики подтверждают объективную сторону преступления, как характеристики действия (бездействия) виновного лица.

При этом необходимо отметить, что если выступление на публике или публикация в средствах массовой информации в процессе доказывания не вызывает сомнения в совершении рассматриваемого преступления конкретным лицом, то в доказывании публикации заведомо ложной информации с использованием сети «Интернет» все не так однозначно.

С.С. Шестало при анализе способов совершения распространения информации в сети «Интернет» делает уклон исключительно на возможность распространения посредством осуществления репостов [7, с. 65].

Полагаем, что данная позиция может быть оспорена. В современном цифровом мире информация может быть диссеминирована через многочисленные каналы сети «Интернет». Необходимо рассматривать все способы совершения данного преступления, среди которых:

1. Социально-информационные платформы.

Анализ судебно-следственной практики свидетельствует о том, что наиболее распространенным способом распространения дезинформации о специальной военной операции на территории Украины (207.3 УК РФ), с использованием IT технологий являются публикации постов в социальных сетях через аккаунты конкретных пользователей.

В настоящее время понятие «социальные сети», равно как и «аккаунт в социальных сетях» (далее - «аккаунты») так и не получили надлежащего правового регулирования. Таким образом, существующая тенденция недвусмысленно свидетельствует о недостаточной подготовленности государственного аппарата к процессу цифровой трансформации [6, с. 19].

Полагаем, что со столь категоричными выводами согласиться крайне сложно, однако при этом недопустимо оставить без внимания тот факт, что нормативная база следует за развитием технологий с существенным опозданием [4, с. 169]. К сожалению, социальные сети не стали исключением.

Как верно отмечает Е.С. Гринь, в юридической науке «аккаунты» также не имеют точного определения [2, с. 128]. Однако следует отметить, что отклоненный проект поправок для Федерального закона «Об информации, информационных технологиях и о защите информации» определяет «аккаунт», как страницу в сети «Интернет» конкретного пользователя [11]. Таким образом, распространение ложной информации путем размещения постов в «аккаунтах» осуществляется с личных страниц конкретных людей в сети «Интернет».

Так, например, гражданин Н., постоянно проживая за пределами территории РФ, с использованием сети «Интернет» разместил на персональном аккаунте в социальной сети дезинформацию о намеренном обстреле российскими военнослужащими родильного дома в Мариуполе и убийстве мирного населения в городе Буча [8].

2. Видеохостинговые сервисы.

С начала XXI века, как верно отмечает И.В. Пащенко, наблюдается интенсивное распространение радикальных идей и привлечение сторонников с использованием ведущих социальных медиа-платформ, включая «Facebook», «ВКонтакте» и «YouTube» [5, с. 14]. Полагаем, что детерминантами данного явления стали такие факторы, как сосредоточение большого числа пользователей на указанных платформах, возможность эффективного продвижения тематических сообществ без крупных финансовых инвестиций, а также демонстрируемая администрацией этих ресурсов относительная терпимость к публикуемому и продвигаемому контенту.

В свою очередь, преступники используют данные ресурсы для публикации и распространения своих видеоматериалов, включая пропагандистские и

обучающие видеоролики. Абсолютно прав О.Ю. Антонов, подчеркивая, что они активно используют алгоритмы рекомендаций Интернет-платформ для привлечения внимания к своим материалам, а также создают видео с провокационными заголовками и описаниями, что позволяет привлекать больше просмотров и увеличивать вероятность попадания в рекомендации пользователей [1, с. 26].

Так, гражданин Я, зная, что опубликованные в украинских средствах массовой информации фото- и видеоматериалы о совершении российскими военнослужащими актов насилия в отношении мирного населения города Буча являются ложными (фейком), диссеминировал эту информацию во время прямой трансляции на платформе YouTube [9].

С учетом изложенного совершение анализируемого нами преступления посредством применения видео-площадок является серьезной проблемой, требующей комплексного подхода к решению. Усиление контроля со стороны платформ, сотрудничество с правоохранительными органами и проведение образовательных программ являются ключевыми стратегиями противодействия данному явлению.

3. Телефонная коммуникация.

В современном обществе телефонные коммуникации стали одним из ключевых средств взаимодействия между индивидами. Тем не менее, существует опасность использования данного канала для трансляции ложных материалов и пропаганды радикальных идеологий. Такое явление представляет собой значительную угрозу общественной безопасности и социальной стабильности, поскольку может способствовать процессу радикализации населения и, в итоге, привести к возникновению террористических действий.

Современные технологии и глобализация упрощают доступ к информации и облегчают коммуникацию между людьми, однако это также создает условия для распространения экстремистских идеологий через телефонные переговоры.

В связи с этим, необходимо осознавать потенциальные риски, связанные с использованием телефонных коммуникаций в качестве инструмента для трансляции радикальных взглядов и материалов.

Такое явление может привести к усилению социальных напряжений, углублению межэтнических и межрелигиозных разногласий, а также к формированию экстремистских групп и организаций, стремящихся к насильственному изменению общественного порядка. В этой связи актуальность проблемы публичного распространения заведомо ложной информации через телефонные переговоры требует всестороннего анализа и разработки эффективных мер по ее преодолению.

Для борьбы с данным явлением необходимо применять комплексный подход, включающий в себя многоуровневые стратегии и меры, направленные на предотвращение и противодействие распространению радикальных идеологий через телефонные коммуникации. Важным аспектом является разработка и внедрение инновационных технологий для мониторинга и анализа телефонных переговоров, а также сотрудничество между государственными структурами.

Так, например гражданин В., в отношении которого проводились ОРМ, с момента начала СВО на территории Украины выражал критическую позицию относительно действий российских Вооруженных Сил в рамках телефонных переговоров с коллегами (в марте 2022 года он трижды обсуждал ситуацию на Украине с друзьями и коллегами посредством телефонной связи, высказывая осуждение в отношении действий российских вооруженных сил) [10].

4. Автоматизированные системы (фермы ботов)

В современном информационном пространстве наблюдается активное распространение экстремистских материалов с использованием автоматизированных систем, таких как фермы ботов. Данный процесс характеризуется применением искусственного интеллекта и алгоритмических

методов для создания и управления виртуальными агентами, способными маскироваться под реальных пользователей и осуществлять массовую рассылку радикальных идеологий.

Основными целями использования ферм ботов для распространения деструктивных материалов являются манипуляция общественным мнением, подрыв социальной стабильности и создание условий для реализации антиобщественных действий. В рамках данной проблематики актуальным становится изучение механизмов идентификации и противодействия таким автоматизированным системам.

Фермы ботов обладают высокой степенью анонимности и масштабируемости, что затрудняет их обнаружение и блокировку со стороны правоохранительных органов и специализированных служб. В связи с этим, разработка новых методов и подходов к выявлению и нейтрализации подобных угроз является приоритетным направлением научных исследований в области информационной безопасности.

Так, в составе организованной группы гражданин Х. приобрел мобильные аппараты и SIM-карты, настроил соответствующее программное обеспечение, обеспечивающее возможность дистанционного контроля над устройствами и проведение масштабной рассылки информационных сообщений, и разместил в одном из торговых центров г. Москвы, тем самым создав «ферму ботов».

Позднее, лица, чья идентичность не была установлена, дистанционно контролировали приобретенные и настроенные гражданином Х. аппараты, с помощью которых осуществлялась масштабная рассылка абонентам российских мобильных операторов текстовых сообщений, включающих в себя преднамеренно недостоверные данные. В сообщениях, в частности, распространялись сведения о совершении российскими военными преступлений против мирного населения Украины, а также о дополнении численности

вооруженных сил резервистами, призывниками, иностранными воинами и учащимися [12].

В качестве возможных решений для борьбы с распространением экстремистских материалов посредством ферм ботов предлагается использование машинного обучения и анализа больших данных для выявления аномальных паттернов поведения, характерных для автоматизированных агентов, а также разработка адаптивных систем контроля и фильтрации контента на основе семантического анализа и нейронных сетей.

Таким образом, распространение дезинформации об участниках специальной военной операции на территории Украины (ст. 207.3 УК РФ), посредством современных технологий является сложной и многоаспектной проблемой, требующей комплексного подхода и совместных усилий государства и общества. Только скоординированные действия в области законодательства, технологий и образования позволят эффективно противодействовать данному явлению и обеспечить безопасность и стабильность в современном мире.

Список литературы:

1. Антонов О.Ю. Экстремистская преступная деятельность в сети Интернет: правовой и криминалистический анализ, пути противодействия // Актуальные вопросы борьбы с преступлениями. 2017. № 1. С.26-31.

2. Гринь Е.С. Наследование аккаунтов в социальных сетях: российский и зарубежный опыт // Актуальные проблемы российского права. - 2022. - Т. - № 2 (135) февраль. - С. 128–134.

3. Кудрявцев В.Н. Способ совершения преступления и его уголовно-правовое значение //Советское государство и право. 1957. № 8. С. 60–69.

4. Кульпин А. А. Конструктор актов прокурорского реагирования, как необходимый элемент цифровой трансформации органов прокуратуры РФ/ А. А. Кульпин // Альманах молодого исследователя. - 2023. - № 14. - С. 169–173.

5. Пащенко И.В. Идеология террористических сообществ в сети Интернет: технологии распространения и специфика противодействия // Caucasian Science Bridge. 2018.1(2). С. 12–24.

6. Цифровая трансформация государственного управления: мифы и реальность: докл. / Высш. шк. экономики. - Москва: Изд. дом Высш. шк. экономики, 2019. - 44 с.

7. Шестало С. С. Новый раунд борьбы с экстремизмом: уголовная ответственность за распространение запрещенных материалов в информационно-телекоммуникационной сети Интернет // Юрист. 2019. № 9. С. 64–69.

8. Архив Басманного районного суда г. Москвы. Уголовное дело № 01–0001/2023 (2023 г.).

9. Архив Мещанского районного суда г. Москвы. Уголовное дело № 01–1300/2022 (2022 г.).

10. Архив Перовского районного суда г. Москвы. Уголовное дело № 01–0042/2023 (2023 г.).

11. Законопроект № 883844–6 [Электронный ресурс] // URL: https://sozd.duma.gov.ru/bill/883844-6 (дата обращения 20.07.2023 г.)

12. Головинский районный суд города Москвы 16 мая 2023 года вынес приговор в отношении Хиральдо Сарай Альберто Энрике обвиняемого в совершении преступления, предусмотренного п. «б,г» ч.2ст. 207.3 УК РФ [Электронный ресурс] // URL: https://mos-gorsud.ru/rs/golovinskij/news/golovinskij-rajonnyj-sud-goroda-moskvy-16-maya-2023-goda-vynes-prigovor-v-otnoshenii-hiraldo-saraj-alberto-enrike-obvinyaemogo-v-sovershenii-prestupleniya-predusmotrennogo-p-b-g-ch2st-2073-uk-rf (дата обращения 14.06.2023 г.)