УДК 343.63:343.9 DOI: 10.17223/23088451/17/6

Н.Б. Гулиева, Р.Г. Драпезо

ЗАВУАЛИРОВАННЫЙ СПОСОБ РАСПРОСТРАНЕНИЯ СВЕДЕНИЙ КЛЕВЕТНИЧЕСКОГО И ОСКОРБИТЕЛЬНОГО ХАРАКТЕРА: ПРОБЛЕМЫ ПРОЦЕССУАЛЬНОГО ДОКАЗЫВАНИЯ

Исследуются проблемные вопросы квалификации завуалированного способа распространения сведений клеветнического и оскорбительного характера, обусловленные сложностями процессуального доказывания. Сделан вывод о необходимости разработки соответствующих форм оперативно-розыскного реагирования применительно к случаям завуалированного совершения преступлений исследуемой категории посредством информационно-телекоммуникационных сетей.

Ключевые слова: *клевета, оскорбление, завуалированный способ, darknet*

В настоящее время высокую распространенность приобретают случаи совершения преступления посредством применения электронных или информационно-телекоммуникационных сетей, включая сеть Интернет. Преступления в сфере незаконного оборота наркотиков, деяния террористической и экстремисткой направленности, преступления в сфере незаконного оборота порнографических материалов и ряд других все чаще совершаются с использованием информационно-телекоммуникационных технологий (далее – сети Интернет). Этим обусловлено введение законодателем квалифицирующего признака, указывающего на применение такого способа совершения преступления. Примером тому служат деяния, уголовная ответственность за которые предусмотрена ст. 110.1, 110.2, 205.2, 228.1, 242 УК РФ и другими статьями.

Распространение дискредитирующей информации в социальных сетях, СМИ набирает обороты. В свете современных цифровых и технологических возможностей подобные действия вполне доступны, в том числе, для обычных граждан – непрофессиональных пользователей электронных и информационно-телекоммуникационных сетей. К сожалению, деяния, дискредитирующие честь, достоинство, репутацию человека, характеризуются повышенной степенью латентности (табл. 1), что в большей мере обусловлено неприменением уголовно-правовых способов защиты нарушенного права. Из табл. 1 видно, что тенденция динамики рассмотренных уголовных дел по распространению сведений клеветнического и оскорбительного характера по Российской Федерации полностью коррелирует с динамикой по Кемеровской области.

Таблица 1

Количество рассмотренных судами общей юрисдикции по первой инстанции дел, связанных с размещением контента клеветнического содержания в сети Интернет за период с 2015 по 2019 г. [1]

Страна/регион	Распределение по годам				
	2015	2016	2017	2018	2019
Российская Федерация	106	76	91	71	34
Кемеровская область	6	4	5	4	1

К 2019 г. отмечается падение в 3–4 раза по сравнению с 2015 г. рассмотренных уголовных дел по изучаемой категории преступлений.

Полагаем, что пассивное с юридической точки зрения поведение правообладателя послужило причиной декриминализации оскорбления. Однако основания декриминализации преступления не могут быть обусловлены его латентностью, а должны зависеть от степени общественной опасности деяния и возможности его предупреждения иными правовыми способами воздействия на нарушителя. К сожалению, неприменение уголовно-правовых способов защиты нарушенных прав вызвано, в том числе, и сложностями процессуального характера. Уголовно-правовая защита чести, достоинства и репутации граждан осуществляется в порядке производства по делам частного обвинения. В таком производстве потерпевший является частным обвинителем, что обязывает его самого осуществлять процессуальное доказывание. Законодательная конструкция деяний, посягающих на нематериальные блага, в частности отсутствие последствий, порождает сложности в доказывании причинения нематериального вреда. Для квалификации преступления с формальным составом последствия не имеют уголовно-правового значения, однако сам факт вменения в вину содеянного требует представления соответствующих процессуальных доводов, уличающих виновного в дискредитации чести, достоинства и репутации человека.

Еще больше сложностей в процессуальном доказывании возникают в случаях распространения клеветнических или оскорбительных сведений в сети Интернет. Опасность информационно-телекоммуникационных технологий, включая сеть «Интернет», с наших позиций, состоит как минимум в следующем: 1) произведенный «сброс» информации получает доступ из любой точки планеты; 2) «сброс» информации может носить обезличенный характер; 3) клеветнические или оскорбительные сведения, размещенные в сети Интернет даже если имеют авторство, то, как правило, носят завуалированный характер. Обычному гражданину, не имеющему специальных познаний, сложно справиться с современными информационно-телекоммуникационными технологиями и, как следствие, доказать факт распространения дискредитирующих его сведений. Данное обстоятельство обусловлено существованием ограниченных в доступе контентов или применением таких способов распростра-

нения информации, которые затрудняют или делают невозможным установить личность распространителя, место отправной точки информации. Данные утверждения мы встречаем в немногочисленной литературе [2–5], где авторы говорят о высокой латентности распространения клеветы посредством сети Интернет, а также, ссылаясь на немногочисленную российскую судебную практику, о невозможности доказать причинно-следственную связь в цепи «размещение контента – авторство контента».

О.И. Максименко [3. С. 50] справедливо отмечает, что завуалированность подразумевает как минимум две технологии: 1) обеспечение в сети «Интернет» анонимизации субъекта преступления; 2) использование полисимвольных технологий с полной или частичной креолизацией текста. Первая технология обеспечивается ресурсами «темного сектора» сети Интернет или darknet. В сети darknet существует множество onion-ресурсов, в том числе и с анонимным (за определенное вознаграждение) распространением сведений оскорбительного или клеветнического характера как на самих onion-ресурсах сети darknet, так и с размещением контента в публичной сети Интернет (publicnet) [4. С. 62; 6. С. 35; 7. P. 415; 8. С. 7].

Проведенный нами анализ сети Интернет выявил множество способов размещения контента, содержащего клевету или сведения оскорбительного характера (рис. 1). Как видно, обнаруженные способы носят завуалированный характер. Классифицировать завуалированность размещения информации в сети Интернет, в соответствии с рис. 1, возможно как по способу, так и источнику размещения контента.

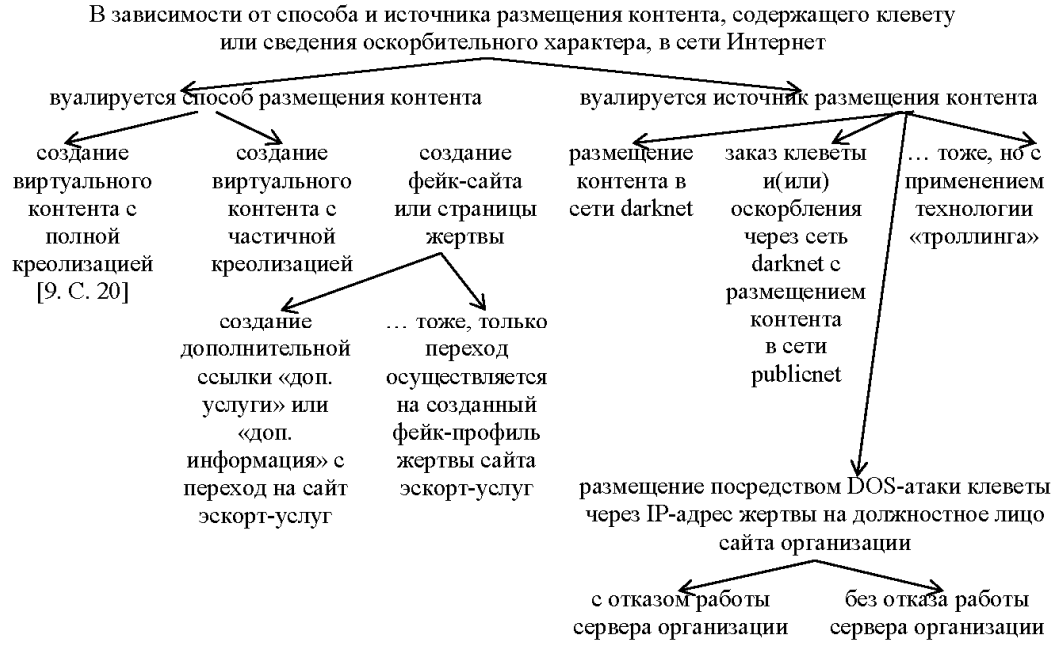

Рис. 1. Классификация распространения клеветы в зависимости от способа и источника размещения контента, содержащего клевету или сведения оскорбительного характера, в сети Интернет

Завуалированность также может проявляться в размещении конкретной информации в параллели с дискредитирующими высказываниями или изображениями внешне никому адресованных или адресованных вымышленным лицам, например книжным персонажам. В качестве примера можно привести следующий случай распространения информации в завуалированной форме. В электронном журнале была опубликована статья о плачевном состоянии дорог в городе «А» в связи с деятельностью главы города. Контент при этом был организован журналистом с использованием полисимвольных технологий с полной креолизацией текста.

Другими словами, между вербальными (текстовыми) и иконическими (символьными) компонентами контента присутствовала смысловая связь, предполагающая, что вербальный текст в существенной степени зависит от анимационного ряда (например, баннерная реклама в сети Интернет). При этом сама анимация (сменяющиеся символы, изображения и т.п.) и изображение выступают в качестве обязательного элемента контента [9. С. 20].

Виртуальный текст содержал элементы словесного описания проблемы, другой виртуальный элемент – всплывающие баннеры, изготовленные с применением средств gif-анимации. При этом баннеры содержали высказывания из русской классической литературы, например «в России две беды: дураки и дороги…». Глава города «А», усмотрев в этом скрытое (завуалированное) оскорбление, обратился с заявлением в правоохранительные органы. Проведенная по делу судебно-лингвистическая экспертиза установила связь между содержимым контента и всплывающими баннерами, содержащими выражения из русской классической литературы. В частности, эксперт констатировал связь между вербальными и иконическими компонентами контента, т.е. семантическое единство лингвистического ряда: «текст контента – всплывающий баннер».

Возможно, состояние дорог в городе действительно плачевное, поэтому говорить об уголовном преследовании за распространение сведений клеветнического характера в приведенном примере нельзя. Не усматриваются и признаки состава оскорбления представителя власти, ибо нет той неприличной формы выражения оскорбительных фраз, что необходимо установить для вменения в вину данного состава преступления. Поэтому в описанной ситуации можно прибегнуть к гражданско-правовым способам защиты нарушенного права. Однако приведенный пример демонстрирует возможность совершения преступлений в завуалированной форме, если бы информация содержала нецензурную лексику.

Сложной в доказывании завуалированного способа совершения преступления представляется проблема констатации связи между распространенными сведениями и личностью правообладателя (потерпевшего). Особенность скрытого распространения сведений заключается в том, что внешне наблюдается лишь параллельное размещение информации, поэтому какой-либо связи между их содержанием и человеком, в адрес которого такие сведения направлены, не прослеживается. Учитывая, что информация может распространяться с разных контентов (интернет-источников), то установить связь между ними при анонимности распространителя практически невозможно.

К сожалению, такие случаи приобретают все большую распространенность, что обусловлено, в том числе, и злоупотреблением недобросовестными пользователями Сети своим правом. «Злоупотребление правом может оказаться при определенных обстоятельствах опаснее правонарушения, подобно тому, как завуалированную клевету труднее доказывать в сравнении с клеветой открытой и незавуалированной. И данное обстоятельство является одной из причин наличия разночтений в юридической квалификации» [10. С. 89].

Очевидно, что в целях обеспечения правильной квалификации необходимо назначение и проведение соответствующих лингвистических исследований с грамотной формулировкой вопросов. Учитывая, что информация преимущественно распространяется лицами, являющимися профессиональными пользователями компьютерной сети, доступ к контентам для рядовых пользователей может быть затруднителен, что препятствует формированию доказательственной базы по делу. С такими сложностями преимущественно сталкиваются обычные граждане, выступающие, как ранее нами было отмечено, в производстве по указанной категории дел частными обвинителями. По делам публичного обвинения, возбуждаемых в случаях распространения сведений в отношении обладателей особо статуса (представитель власти, военнослужащий, судья и т.д.), такие функции возложены на государственного обвинителя, что упрощает положение потерпевшего в виду того, что доказательственная база формируется государственными органами, профессионально осуществляющими функции уголовного преследования. Однако даже при таких обстоятельствах проблемы технологического характера, завуалированность контента препятствуют в выявлении виновных лиц.

Таким образом, распространение уничижительных или клеветнических сведений посредством информационно-телекоммуникационных технологий, включая сеть Интернет, в завуалированной форме отличается сложностями процессуального доказывания в совершении преступления. Наличие процессуальных препятствий не умаляет общественной опасности таких деяний, что требует разработки и последующего применения соответствующих форм процессуального и оперативно-розыскного реагирования. К сожалению, в настоящее время возможность привлечения к уголовной ответственности за совершение преступлений, причиняющих вред нематериальным благам, в большей мере зависят от процессуальных вопросов. Игнорирование случаев распространения уничижительных и клеветнических сведений в завуалированной форме приводит к их распространенности и безнаказанности виновных. Поэтому своевременная реакция государства в целях предупреждения подобного рода поступков крайне важна.

В этой связи нами разработаны некоторые оперативно-розыскные приемы обнаружения и фиксации следов распространения клеветнических и оскорбительных сведений в завуалированной форме в сети Интернет. Такие приемы могут содействовать формированию доказательственной базы по делу. Нами показано, что в зависимости от способа и источника размещения контента в сети Интернет, формируется специфическая следовая картина (табл. 2). В табл. 2 мы сопоставили механизм образования следовой картины и возможные приемы обнаружения и фиксации следов. В табл. 3 представлены оперативно-розыскные приемы борьбы с распространением сведений клеветнического и оскорбительного характера в сети Интернет.

Таблица 2

Механизм образования и характеристика некоторых цифровых следов в зависимости от способа и источника размещения контента, содержащего клевету или сведения оскорбительного характера, в сети Интернет

Способ и источник размещения контента	Характер следовой картины	Возможные приемы обнаружения и фиксации следов
Создание виртуального контента с полной или частичной креолизацией	Файлы, цифровые следы, остающиеся в результате применения программных технологий креолизации и т.п.	«Уборка мусора» (осмотр мусорных корзин на наличие распечаток деловой переписки и т.п., в том числе и в электронной форме); осмотр cookie; скриншот монитора цифрового устройства и др.
Создание фейк-сайта или страницы жертвы	Файлы, цифровые следы; IP-адрес и MAC-адрес цифрового устройства	Скриншот монитора цифрового устройства; осмотр cookie, буфера обмена и кэш-памяти; фиксация метаданных и EXIF-тегов (дистанционно и (или) локально); признаки администрирования сайта

Способ и источник размещения контента	Характер следовой картины	Возможные приемы обнаружения и фиксации следов
Размещение контента в сети darknet	Фото, видеофайлы	Скриншот монитора цифрового устройства; фиксация метаданных и EXIF-тегов (дистанционно и (или) локально); осмотр cookie, буфера обмена и кэш-памяти (локально)
Заказ клеветы и (или) оскорбления через сеть darknet с размещением контента в сети publicnet	Контенты, содержащие сведения дискредитирующего характера	Скриншот монитора цифрового устройства; фиксация метаданных и EXIF-тегов (дистанционно и (или) локально); методы «компьютерной разведки (например, «контролируемый» фишинг* со стороны оперативных служб)»
Размещение посредством DOS-атаки, дискредитирующих сведений	Следы присутствия ботнетов; IP-адрес и MAC-адрес цифрового устройства, посредством которого осуществляется DOS-атака	Скриншот монитора цифрового устройства; фиксация (посредством скриншотов) IP и mac-адреса; методы «компьютерной разведки (например, «контролируемый» фишинг со стороны оперативных служб [11. С. 81]; методы компрометации

* Вид мошенничества с использованием компьютерной информации в целях несанкционированного получения доступа к конфиденциальным сведениям пользователя (например, паролям от личного кабинета онлайн-банка).

Таблица 3

Сравнение возможных оперативно-розыскных приемов по делам о клевете и оскорблении специальных субъектов

Оперативно-розыскной прием	Характеристика приемов	Особенность применения приемов
Компрометация	Доведение до лица (например, лица оперативной разработки либо неопределенного круга лиц) сведений об известной оперативным службам информации (разной степени достоверности) о приготовлении к преступлению [12. С. 164]	Компрометация конкретного или предполагаемого оперативными подразделениями места или сектора в сети Интернет. Это дает возможность последним предвидеть действия предполагаемых лиц, пресечь их деятельность на стадии зарождения преступного замысла
ОРМ «Получение компьютерной информации»	Многоходовая операция, предпринимаемая оперативными службами для оперативного внедрения в сеть darknet при наличии разработанной легенды внедрения	Разработка легенды, оперативной комбинации; в некоторых ситуациях – создание «сайтов-прикрытия». Так, в уголовном деле (№ дела в суде 1-96/2015 [1]) оперативные службы посредством ОРМ «Получение компьютерной информации» смогли установить связь пользователя с контентом, где последний размещал дискредитирующие сведения (в одной из социальных сетей)

Примечание. ОРМ – оперативно-розыскное мероприятие.

Таким образом, распространение сведений клеветнического и оскорбительного характера, совершаемое в условиях анонимности через сеть Интернет, могут получить дальнейшее уголовно-процессуальное развитие.

ЛИТЕРАТУРА

1. *Официальный* интернет-портал «Судебные и нормативные акты РФ». URL: https://sudact.ru/ (дата обращения: 29.10.2020).
2. *Королева М.М.* Клевета и оскорбление в сети Интернет // Законность. 2010. № 7. С. 50–53.
3. *Максименко О.И.* Семиотические особенности медиатекста Интернета // Вестник Российского университета дружбы народов. Серия: теория языка, семиотика, семантика. 2011. № 1. С. 50–58.
4. *Соловьев В.С.* Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Всероссийский криминологический журнал. 2016. Т. 10, № 1. С. 60–72.
5. *Кочанова Т.* Клевета: анализ судов по теме с важными примерами // Жилищное право. 2019. № 3. С. 105–112.
6. *Драпезо Р.Г., Зникин В.К.* Darknet как источник сыскной информации // Оперативник (сыщик). 2017. Т. 52, № 3. С. 35–38.
7. *Ladegaard I.* We Know Where You Are, What You Are Doing and We Will Catch You: Testing Deterrence Theory in Digital Drug Markets // British Journal of Criminology. 2018. Vol. 58, is. 2. P. 414–433. doi: https://doi.org/10.1093/bjc/azx021.
8. *Суходолов А.П., Бычкова А.М.* Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 5–16.
9. *Беляков И.М.* Особенности баннерной Интернет-рекламы как поликодового текста: лингвистический аспект : автореф. дис. ... канд. филол. наук. М., 2009. 24 с.
10. *Бармина О.Н.* Злоупотребление правом / отв. ред. В.А. Кодолов. Киров : Радуга-ПРЕСС, 2015. 133 с.
11. *Павлюков В.В.* Правовые и практические аспекты получения компьютерной информации о киберпреступниках // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами : сб. науч. ст. / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул : Изд-во Алт. ун-та, 2017. Вып. XIV. 118 с.
12. *Кокурин Г.А.* Использование метода компрометации в оперативно-розыскной деятельности // Российский юридический журнал. 2016. № 5. С. 164–169.

Статья принята к публикации 24.05.2021.

A Veiled Way of Disseminating Defamatory and Offensive Information: Problems of Procedural Proof
Ugolovnaya yustitsiya – Russian Journal of Criminal Law, 2021, no. 17, pp. 30–34. DOI: 10.17223/23088451/17/6
Natavan B. kyzy Gulieva, Kemerovo State University (Kemerovo, Russian Federation). E-mail: natavan-1212@mail.ru
Roman G. Drapezo, Kemerovo State University (Kemerovo, Russian Federation). E-mail: uri_nit@kemsu.ru
Keywords: libel, insult, veiled way, darknet

The classification of the studied phenomena is of great importance, because it gives such phenomena a certain structuredness, which makes it possible to characterize their features in more detail. The classification of crimes helps to differentiate them and allows their correct qualification. Classification of crimes that harm honor, dignity, and reputation is of a certain difficulty due to the legislator's specific approach to the law protection of these intangible benefits. Such benefits are mostly protected by special rules designed, primarily, to protect other objects. Within the framework of this study, it is proposed to distinguish between the acts in the broad and narrow sense of the word. The authors suggest distinguishing the types of crimes that cause harm to honor, dignity, and reputation in terms of the objective and subjective side and on the grounds related to the victim.

References

1. Sudact.ru. (n.d) *Sudebnye i normativnye akty RF* [Judicial and Regulatory Acts of the Russian Federation]. Official website. [Online] Available from: https://sudact.ru/ (Accessed: 29th October 2020).
2. Koroleva, M.M. (2010) Kleveta i oskorblenie v seti Internet [Libel and insult on the Internet]. *Zakonnost'*. 7. pp. 50–53.
3. Maksimenko, O.I. (2011) Semiotic characteristics of the Internet media-texts. *Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: teoriya yazyka, semiotika, semantika – RUDN Journal of Language Studies, Semiotics and Semantics*. 1. pp. 50–58. (In Russian).
4. Soloviev, V.S. (2016) Prestupnost' v sotsial'nykh setyakh Interneta (kriminologicheskoe issledovanie po materialam sudebnoy praktiki) [Crime in social networks of the Internet (criminological research based on the materials of judicial practice)]. *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 10(1). pp. 60–72.
5. Kochanova, T. (2019) Kleveta: analiz sudov po teme s vazhnymi primerami [Slander: analysis of court cases with important examples]. *Zhilishchnoe pravo*. 3. pp. 105–112.
6. Drapezo, R.G. & Znikin, V.K. (2017) Darknet as a source of detective information. *Operativnik (syshchik) – Field Investigator (Sleuth)*. 52(3). pp. 35–38. (In Russian).
7. Ladegaard, I. (2018) We Know Where You Are, What You Are Doing and We Will Catch You: Testing Deterrence Theory in Digital Drug Markets. *British Journal of Criminology*. 58(2). pp. 414–433. DOI: 10.1093/bjc/azx021
8. Sukhodolov, A.P. & Bychkova, A.M. (2019) Digital Technologies and Drug-Related Crime: Problems of Counteracting the Use of "Telegram" Messenger for Trafficking Drugs. *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 13(1). pp. 5–16. (In Russian). DOI: 10.17150/2500-4255.2019.13(1).5-17
9. Belyakov, I.M. (2009) *Osobennosti bannernoy Internet-reklamy kak polikodovogo teksta: lingvisticheskiy aspect* [Internet banner advertising as a polycode text: a linguistic aspect]. Abstract of Law Cand. Diss. Moscow.
10. Barmina, O.N. (2015) *Zloupotreblenie pravom* [Abuse of Right]. Kirov: Raduga-PRESS.
11. Pavlyukov, V.V. (2017) Pravovye i prakticheskie aspekty polucheniya komp'yuternoy informatsii o kiberprestupnikakh [Legal and practical aspects of obtaining computer information about cybercriminals]. In: Davydov, S.I. & Polyakov, V.V. (eds) *Ugolovno-protsessual'nye i kriminalisticheskie chteniya na Altae: problemy protivodeystvie kiberprestupnosti ugolovno-protsessual'nymi, kriminalisticheskimi i operativno-rozysknymi sredstvami* [Criminal procedural and forensic readings in Altai: problems of countering cybercrime by criminal procedural, forensic and operational-search means]. Barnaul: Altai State University.
12. Kokurin, G.A. (2016) On the use of a "compromise" method in operative research activities. *Rossiyskiy yuridicheskiy zhurnal – Russian Juridical Journal*. 5. pp. 164–169. (In Russian).

Received: 24 May 2021.