

Кошелева Екатерина Анатольевна
Смоленский государственный университет
г. Смоленск, Россия
Научный руководитель:
Фролов Михаил Григорьевич
Смоленский государственный университет
г. Смоленск, Россия

УДК 343.232

КЛЕВЕТА В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ДОКАЗЫВАНИЯ

В современном мире невозможно представить жизнь без информационных технологий. Ускоренная цифровизация предоставляет большие преимущества человеку. Однако это также влечет возникновение проблем при квалификации преступлений, совершенных в информационно-телекоммуникационной сети Интернет. В статье рассмотрены основные проблемы, возникающие при квалификации и доказывании преступлений, предусмотренных частью 2 статьи 128.1 Уголовного кодекса РФ. Особое внимание уделено ключевым понятиям и характеристикам. Выявлены возможные пути решения проблем.

Ключевые слова: преступление, клевета, информационно-телекоммуникационная сеть, доказывание, квалификация.

Отличительной чертой современности является ускоренное развитие информационных технологий и глобальная цифровизация всех областей жизни общества. Новые технологии, в том числе информационно-телекоммуникационная сеть Интернет (далее – Интернет), оказали огромное влияние на социальное взаимодействие людей. С одной стороны, Интернет стал неотъемлемой частью жизни человека независимо от возраста и статуса, а также предоставил новые возможности для реализации права на свободу слова, поиска, получения, передачи информации любым законным способом. С другой стороны, появление данных технологий привело к возникновению новых вызовов для правопорядка. Одним из них является проблема квалификации и доказывания клеветы в цифровой сфере. В связи с тем, что Всемирная сеть обладает такими свойствами как общедоступность,

мгновенность передачи данных, сложность идентификации субъекта, устойчивость и многократное тиражирование информации, клевета приобретает качественно иной характер, что существенно затрудняет защиту чести, достоинства и деловой репутации граждан и организаций.

Ответственность за клевету предусмотрена статьей 128.1 Уголовного кодекса Российской Федерации [10]. Объективная сторона данного преступления состоит в распространении сведений, не соответствующих действительности и порочащих честь, достоинство и (или) деловую репутацию другого лица. Обязательным признаком является осведомлённость лица, совершившего данное деяние, о недостоверности распространяемых сведений.

Судебная практика показывает, что клеветнические сведения должны касаться только фактических обстоятельств, а не являться оценочными суждениями. [5, с. 73]. Описываемое обстоятельство учитывается и в практике Европейского суда по правам человека. Например, в судебном решении по делу *Lingens vs Austria* указано, что «необходимо тщательно проводить различие между фактами и оценочными суждениями. Наличие фактов может быть доказано, тогда как справедливость оценочных суждений недоказуема [2, с. 244].

Законодатель регламентировал более строгую ответственность за клевету с использованием средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть "Интернет". Под информационно-телекоммуникационной сетью законодатель понимает технологическую систему, которая предназначена для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [11]. Особое внимание следует обратить на то, что в определении законодатель делает упор на двух ключевых характеристиках: технической составляющей (сеть представляет собой систему, то есть совокупность технических устройств и линий связи) и способе доступа (передача осуществляется по линиям связи, а доступ к ней возможен только посредством

использования средств вычислительной техники (компьютер, телефон и т.д.)). Таким образом, с юридической точки зрения, Интернет — это не отдельный феномен, а разновидность (часть) информационно-телекоммуникационной сети. В законе это отражается через термин "сеть «Интернет»".

Согласно официальному толкованию, под сетью Интернет следует понимать информационно-телекоммуникационную сеть, объединяющую информационные системы, доступ к которым осуществляется по доменным именам и (или) по сетевым адресам [11].

В юридической литературе отмечается, что интернет как объект правового регулирования обладает специфическими признаками: он не имеет территориальных границ, является публичным (доступен неопределенному кругу лиц) и децентрализован [3].

Следует уделить особое внимание понятию клеветы в Интернете. Указанная дефиниция в связи с недавним появлением в практике не получила должного теоретического толкования. По мнению А.М. Васильева, С.М. Скаян «клевета в сети «Интернет» — это такое же распространение ложных сведений, но с использованием информационно-телекоммуникационных сетей и технологий». [1, с. 55]. Таким образом, особенностью данного состава преступления является способ совершения преступления.

Однако при квалификации указанного преступного деяния необходимо уметь отграничивать клевету от оскорбления и распространения «фейковой» информации. Под оскорблением принято понимать унижение чести и достоинства другого лица, выраженное в некорректной и (или) противоречащей принятым в обществе нормам нравственности и морали форме [4, с. 63]. Понятие «фейковая информация» возникла от английского слова «fake», которое имеет смысловое значение «подделка». Исходя из этого, под распространением фейковой информации принято понимать распространение намерено сфабрикованных, заведомо недостоверных и (или) вводящих в заблуждение сведений. Отличительной чертой рассматриваемой информации

является то, что она выдается за реальные новости, факты или экспертное мнение. Основной целью создания фейковой информации является манипулирование мнением общественности, получение какой-либо выгоды или дискредитация кого-либо [12].

Исходя из вышеизложенного, можно сделать следующие закономерные выводы. Во-первых, не за все неприятные или недостоверные сведения, распространенные в Интернете, лицо можно привлечь к уголовной ответственности по части 2 статьи 128.1 Уголовного кодекса Российской Федерации. Во-вторых, в уголовном законе содержатся иные статьи, предусматривающие ответственность за указанные деяния.

Особые проблемы при квалификации рассматриваемого состава преступления возникают при разграничении статьи 128.1 и статьи 319 Уголовного кодекса. Статьей 319 предусмотрена уголовная ответственность за публичное оскорбление представителя власти в процессе исполнения им служебных обязанностей. В доктрине уголовного права и в соответствии с примечанием к ст. 318 УК РФ, представитель власти характеризуется наличием особого публично-правового статуса. К данной категории относятся должностные лица, реализующие функции законодательной, исполнительной или судебной ветвей власти, а также сотрудники правоохранительных и контролирующих органов. Объединяющим признаком для них является наличие распорядительных полномочий, реализуемых в отношении лиц, не связанных с ними отношениями служебной зависимости, а также способность издавать акты (принимать решения), имеющие общеобязательную юридическую силу [10].

При отграничении рассматриваемых составов преступлений решающее значение имеет характер распространяемых сведений [9]. Цель распространения в данных составах также различна. Так, при оскорблении представителя власти целью виновного лица является унижение, а при клевете – подрыв репутации, деловой репутации.

Особые затруднения возникают при доказывании состава преступления, предусмотренного частью 2 статьи 128.1 Уголовного кодекса Российской Федерации. Одной из ключевых проблем является высокая уязвимость цифровых доказательств. Имеется в виду наличие возможности корректировать сведения, распространенные в сети Интернет, а также отсутствие особых затруднений при их удалении или уничтожении. Сквозное шифрование (end-to-end encryption) в современных мессенджерах технически не позволяет получить доступ к данным без устройства пользователя, что делает невозможным получение информации от провайдера. Это обусловлено тем, что при таком шифровании провайдер не является обладателем информации. Он лишь транспортирует криптограмму. Следовательно, получение информации от лица, контролирующего сервер (оператора), о содержании зашифрованных сообщений технически невозможно. Способом получения доступа к таким данным является работа с самим устройством.

Как указывалось ранее, одной из ключевых характеристик сети Интернет является децентрализованность. В результате этого возникает сложность с установлением принадлежности сообщений конкретному лицу. Аккаунты в социальных сетях и мессенджерах могут содержать только псевдонимы, привязываются к SIM-картам, которые могут быть перевыпущены, похищены или оформлены на третье лицо, а также допускают синхронизацию между несколькими устройствами, что затрудняет определение конкретного отправителя.

Еще одной характеристикой преступлений, совершенных в сети Интернет, является трансграничность. Это подразумевает возможность нахождения преступника или серверов в любой точке мира на момент распространения информации, которые находятся в других юрисдикциях. Это влечет возникновение ряда сложностей с получением доказательств от иностранных провайдеров; исполнением международных запросов о правовой помощи, возникновением коллизий национальных законодательств.

Помимо этого, многие цифровые платформы позволяют отправителю или получателю редактировать или удалять сообщения, посты после отправки или размещения, а скриншоты не отражают этих изменений, если не проведен анализ серверных журналов. Это влечет за собой возникновение следующей проблемы: исключение возможности оперативного ознакомления с переписками в социальных сетях и мессенджерах без судебного решения. Статья 23 Конституции РФ гарантирует право на тайну переписки, ограничение которого допускается только на основании судебного решения. Однако на практике возникает коллизия: если сообщения уже находятся на изъятом мобильном устройстве, требуется ли отдельное судебное решение для их осмотра? Конституционный Суд Российской Федерации в ряде определений указывал, что осмотр уже изъятого телефона не требует дополнительного судебного разрешения, если само изъятие произведено законно. Вместе с тем, исследователи отмечают отсутствие четкого алгоритма действий следователя и необходимость дополнения УПК РФ специальной нормой об осмотре мобильных устройств [6].

Также следует уделить особенное внимание проблеме оценки допустимости и достоверности доказательств. Так Верховный суд в Постановлении Пленума от 23 апреля 2019 г. № 10 "О применении части четвертой Гражданского кодекса Российской Федерации" определил критерии допустимости скриншотов как доказательств. Согласно указанным положениям, они должны содержать URL-адрес страницы, дату и время создания, а также быть заверены лицом, участвующим в деле. Однако практика показывает, что суды нередко руководствуются устаревшими подходами, предъявляя дополнительные требования, что значительно затрудняет доказывание по данной категории дел [8].

Подводя итог, можно сказать следующее. На данный момент времени квалификация составов, предусмотренных частью 2 статьи 128.1 Уголовного кодекса Российской Федерации, имеет определенные проблемы. В первую

очередь это связано с дифференциацией понятий и разграничением смежных составов преступлений. Особое же затруднение вызывает доказывание по данной категории дел. Это обусловливается природой информационно-коммуникационной сети Интернет.

В связи с тем, что Интернет предоставляет огромные возможности человеку для получения, распространения, изменения и удаления данных, доказать наличие состава преступления в сведениях затруднительно. Это влечет не только большие временные затраты, но и финансовые расходы, поскольку для получения доказательств, соответствующих требованиям закона, необходимо привлечение технических специалистов, обращение к провайдерам, получение соответствующих разрешений суда.

Таким образом, для решения рассмотренных проблем необходимо ужесточить законодательство в области регулирования изменения сведений в сети Интернет. Например, целесообразно будет внести изменения в Кодекс Российской Федерации об административных правонарушениях, установив ответственность за неисполнение требований частей 4.1 и 4.3 статьи 10.1 Федерального закона № 149-ФЗ в виде административного штрафа.

Также следует оптимизировать процедуру получения данных от провайдеров. Для данной цели необходимо создать и использовать защищенные каналы связи и унифицированные, прикладной программный интерфейс для направления запросов и получения ответов между правоохранительными органами и провайдерами. Разработка такого интерфейса значительно ускорит и упростит получение информации. Также это позволит минимизировать риск подделки запросов на получение данных. Развитие международного взаимодействия по данным вопросам значительно упростит получение доказательств по цифровым преступлениям.

Список литературы

1. Васильев А.М., Скаян С.М. Профессиональные навыки лиц, совершающих преступления // Юридическая наука. 2019. № 7. (С. 54 -56).

2. Гомьен Д., Харрис Д., Зваак Л. Европейская конвенция о правах человека и Европейская социальная хартия: право и практика. М., 1998. 367 с.
3. Минбалеев А.В. Основы правового регулирования сети Интернет / А. В. Минбалеев. - Текст: непосредственный // Право и кибербезопасность. - 2014. - № 1 (4). (С. 20 -26).
4. Найда К.В., Васильев А.М. Клевета в сети «Интернет» // АВБсП. 2023. № 2. (С. 62-64).
5. Наумов А.В., Кибальник А.Г. Уголовное право. Особенная часть: учебник для вузов / ответственные редакторы А. В. Наумов, А.Г. Кибальник. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 564 с. — (Высшее образование).
6. Недиков В.Б. Проблемы получения информации доказательственного значения по преступлениям, совершённым посредством использования социальных сетей и мессенджеров // Журнал юридических исследований. 2024. № 4. С. 122-128.
7. Подройкина И.А., Серегина Е.В., Улезько С.И. Уголовное право. Особенная часть. Семестр I: учебник для вузов / ответственные редакторы И. А. Подройкина, Е. В. Серегина, С. И. Улезько. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 556 с. — (Высшее образование).
8. Постановление Пленума Верховного Суда РФ от 23.04.2019 N 10 "О применении части четвертой Гражданского кодекса Российской Федерации" // "Российская газета", N 96, 06.05.2019.
9. Романенко П.А. Отграничение состава оскорбления представителя власти со смежными составами преступлений и административных правонарушений // Вестник магистратуры. 2020. № 2-3 (101). (С. 63-65).
10. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 29.12.2025) // "Собрание законодательства РФ", 17.06.1996, N 25, ст. 2954.
11. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 24.06.2025) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2026) // "Российская газета", N 165, 29.07.2006.
12. Хохолков М. Клевета, фейки и оскорбления: о различиях негативной информации // МедиаПраво.ком. 2021 год. (С. 3-5).

Kosheleva E.A.

Smolensk State University, Smolensk, Russia

Defamation in the information and telecommunications network Internet: problems of qualification and proof

In the modern world, it is impossible to imagine life without information technology. Accelerated digitalization provides great benefits to people. However, this also leads to problems in the qualification of crimes committed on the Internet.

The article discusses the main problems that arise in the qualification and proof of crimes provided for in part 2 of Article 128.1 of the Criminal Code of the Russian Federation. Special attention is paid to key concepts and characteristics. Possible ways to solve the problems have been identified.

Keywords: Slander, information and telecommunication network Internet, problems of proof, qualification.