



Научная статья

УДК 343.364

EDN: <https://elibrary.ru/JMSAKO>

ИПОН: 2007-0083-1/26-788

MOSURED: 77/27-005-2026-01-988

Юридическая ответственность за распространение фейков: границы допустимого регулирования в демократическом обществе

Александр Владимирович Токолов

Московский университет МВД России имени В.Я. Кикотя, Москва, Россия,

altok45@mail.ru

Аннотация. Посвящена необходимости установления юридической ответственности за распространение фейковой информации, так как современные технологии, основанные на технологиях искусственного интеллекта, способны создавать крайне реалистичные видеозаписи, аудиофайлы, рукописные документы, что ставит под сомнение достоверность представленных доказательств, подвергает угрозе взлома банковских систем, компрометации частных лиц или компаний, манипуляции общественным мнением и создания фейковых новостей, а также используется в целях шантажа и вымогательства. С ростом популярности фейков возросли и риски их использования в мошенничестве, клевете и других уголовных правонарушениях.

Ключевые слова: информационное право, информационная безопасность, искусственный интеллект, фейки, цифровизация, цифровая трансформация, социально-опасная деятельность, проникновение криминала в сферу информационных технологий

Для цитирования: Токолов А. В. Юридическая ответственность за распространение фейков: границы допустимого регулирования в демократическом обществе // Криминологический журнал. 2026. № 1. С. 208–211. EDN: JMSAKO.

Original article

Legal responsibility for spreading fakes: the limits of acceptable regulation in a democratic society

Alexander V. Tokolov

Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia,

altok45@mail.ru

Abstract. Is devoted to the need to establish legal liability for the dissemination of fake information, as modern technologies based on artificial intelligence are capable of creating extremely realistic video recordings, audio files, and handwritten documents, which casts doubt on the authenticity of the presented evidence, poses a threat to the hacking of banking systems, the compromise of individuals or companies, the manipulation of public opinion, and the creation of fake news, as well as being used for the purposes of blackmail and extortion. With the growing popularity of fakes, the risks of their use in fraud, libel, and other criminal offenses have also increased

Keywords: information law, information security, artificial intelligence, fake news, digitalization, digital transformation, socially dangerous activities, the penetration of crime into the field of information technology

For citation: Tokolov A. V. Legal responsibility for spreading fakes: the limits of acceptable regulation in a democratic society. Criminological Journal. 2026;(1):208–211. (In Russ.). EDN: JMSAKO.

© Токолов А. В., 2026



Развитие цифровых коммуникаций радикально изменило способы распространения информации. Сегодня для обмена данными используются основные технологии, связанные с применением телекоммуникационной сети Интернет, мобильной и спутниковой связи, а также технологии, осуществляющие передачу данных по беспроводным сетям с помощью света (Li-Fi). К ним, в первую очередь, относятся социальные сети, различные сайты знакомств, публичные каналы в мессенджерах и др. В связи с этим данные интернет-платформы и приложения, предназначенные для построения виртуального общения и обмена информацией между субъектами информационных правоотношений, представляют из себя информационную систему, т. е. совокупность цифровых платформ и программно-технических средств, а также технологических инструментов. Внедрение этих цифровых решений имеют две принципиальные противоположные стороны: позитивную — кратно увеличивает возможности субъектов правоотношений для реализации свободы слова и свободного обсуждения актуальных вопросов; негативную — значительный рост рисков массового распространения недостоверных сведений, деструктивной информации и создание проблем в сфере информационной безопасности, тая в себе различные уязвимости и опасности.

Фейки — заведомо ложные или искаженные сообщения, подаваемые как достоверные факты. Их распространение несет следующие угрозы:

- дезориентация граждан в ключевых социальных и политических вопросах; подрыв доверия к государственным институтам и СМИ;
- провоцирование социальной напряженности и противоправных действий.

В связи с этим перед демократическим государством возникает важнейший правовой вызов: как защитить общественный порядок и права граждан, не нарушая при этом конституционных свобод — свободы слова, право искать, получать, передавать, производить и распространять информацию любым законным способом и права на выражение мнений?

Цель исследования — проанализировать правовые механизмы противодействия фейкам, определить допустимые границы государственного регулирования в цифровой среде и оценить их соответствие демократическим принципам.

Под фейками в юридическом [1] поле обычно понимают:

- заведомо ложные сообщения, распространяемые с умыслом (например, дезинформация о действиях госорганов);
- искаженные факты, поданные как достоверные (например, монтаж видео с целью дискредитации лица);
- непроверенную информацию, распространяе-

мую без злого умысла, но с последствиями для общественной безопасности.

Кроме того, как разновидность фейков существует такая категория, как дипфейк (от англ. deepfake). Эти технологии, основанные на технологиях искусственного интеллекта, способны создавать крайне реалистичные видеозаписи, аудиофайлы, рукописные документы, что ставит под сомнение достоверность представленных доказательств, подвергает угрозе взлома банковских систем, компрометации частных лиц или компаний, манипуляции общественным мнением и создания фейковых новостей, а также используется в целях шантажа и вымогательства. С ростом популярности дипфейков возросли и риски их использования в мошенничестве, клевете и других уголовных правонарушениях.

Идея создания дипфейков зародилась благодаря разработке генеративно-сопоставительной сети (Generative adversarial network, сокращенно GAN), т. е. технологии «глубокого обучения» двух одновременно обучающихся генеративной и дискриминативной моделей, создающих и анализирующих фотографии, молодым исследователем Яном Гудфеллоу в 2014 г. [5]. Технология GAN используется во многих прогрессивных разработках в различных сферах деятельности человека. Например, StarGAN можно использовать для улучшения качества фотографий или создания различных выражений лица на них, CycleGAN (где уже двойной набор моделей: две генеративные и две дискриминативные) — создает, раскрашивает, придает определенный стиль полученным изображениям, GigaGAN — преобразует текст в изображение, 3DGAN — позволяет на основе 2D объекта изготовить объемную 3D модель [6], а в медицине с успехом может применяться «метод создания реалистичных биомедицинских изображений с помощью GAN для увеличения ограниченного набора данных» [2], что позволяет улучшить качество и информативность медицинских снимков.

Но, эти технологии не всегда используются во благо. Особенно опасной ее делает скорость улучшения этой технологии и масштабы ее распространения, а также ее массовая доступность. Например, появился новый вид мошенничества с использованием технологии дипфейк для создания видеосообщений в телеграмм, так называемых «кружочков» [3], которые записываются в режиме онлайн, т. е. сразу в момент отправления. Но современные технологии позволяют сделать любое видео, в том числе заранее созданный дипфейк, в таком же формате (кружочка). «Свободный доступ к крупномасштабным публичным базам данных вместе с быстрым прогрессом методов глубокого обучения, в частности генеративно-сопоставительных сетей, привели к созданию очень реалистичного фейкового контента с соответствующими последствиями для общества в эту



эпоху фейковых новостей». Зачастую такие технологии применяются в политических гонках с целью дискредитации оппонентов на выборах, но, в то же время, есть случаи использования технологии дипфейк не во вред другим оппонентам. Например, индийский политик Маной Тивари в 2020 г. использовал эту технологию с целью охвата большего количества избирателей, создав дипфейк своего же выступления на разных языках и местных диалектах [4].

В российском законодательстве ответственность за фейки закреплена в нескольких нормах:

- ст. 207.1 УК РФ — публичное распространение заведомо ложной информации об обстоятельствах, угрожающих жизни и безопасности граждан;
- ст. 207.2 УК РФ — распространение ложной общественно значимой информации, повлекшее тяжкие последствия;
- ст. 13.15 КоАП РФ — злоупотребление свободой массовой информации (в том числе распространение фейков в СМИ и соцсетях).

Баланс свобод и ограничений: принципы демократического регулирования.

Демократическое общество исходит из приоритета свободы слова, однако допускает ее ограничение в целях:

- защиты прав и репутации других лиц;
- обеспечения государственной безопасности;
- предотвращения беспорядков или преступлений.

Применительно к фейкам это означает, что правовое регулирование должно быть:

- четко сформулированным (нормативные правовые акты не должны допускать произвольного толкования);
- необходимым (ограничения оправданы только при наличии реальной угрозы);
- соразмерным (указывать на то, что наказание соответствует тяжести совершенного деяния).

Необходимо определить проблемы правоприменения, а также выяснить, где проходят границы правового регулирования фейковой информации?

На практике регулирование фейков сталкивается с рядом вызовов: Во первых, существует сложность доказывания умысла. Как отличить злонамеренный фейк от ошибки или интерпретации? Например, репост новости из сомнительного источника может быть следствием невнимательности, а не умысла. Во вторых, присутствуют риски цензуры. Широкие формулировки законов (например, «угроза общественной безопасности») могут использоваться для подавления критики власти. Кроме того, возросла скорость распространения информации. Правовые механизмы реагируют медленнее, чем вирусные фейки, что снижает их превентивный эффект. Также хочется отметить фактор трансграничности интернета. Фейки часто ге-

нерируются за рубежом, что затрудняет определение юрисдикции.

Оптимальные механизмы борьбы с фейками.

Для гармонизации правового регулирования можно предложить следующее.

1. Необходимо определить четкие критерии ложной информации. Законодательство должно разграничивать: умышленную дезинформацию, непроверенные данные и оценочные суждения.

2. Направить усилия на повышение медиаграмотности. В первую очередь это профилактика эффективнее репрессий: образовательные программы помогут гражданам распознавать фейки.

3. Осуществлять независимый надзор. Это создание органов (например, при Роскомнадзоре), которые будут оценивать обоснованность блокировок контента.

4. Важно уделять внимание международному сотрудничеству. Выработать и согласовать стандарты борьбы с трансграничной дезинформацией (например, в рамках ООН или ОБСЕ).

Борьба с фейками является необходимой задачей государства, но ее решение не должно подрывать демократические принципы. Юридическая ответственность за распространение ложной информации допустима лишь при трех условиях:

- доказанный умысел распространителя;
- реальная угроза общественным интересам; 2) соразмерность наказания совершенному деянию.

Оптимальная модель регулирования включает три элемента.

- Четкие правовые рамки: ясные критерии определения фейков, конкретный перечень правонарушений и прозрачные процедуры доказывания.
- Саморегулирование платформ: а) премодерация (процесс проверки пользовательского контента модератором перед его публикацией) и постмодерация (способствует текущим обсуждениям от членов онлайн-сообщества) контента; б) алгоритмы выявления ложной информации; в) механизмы оперативного опровержения.
- Медиаобразование: а) обучение методам проверки информации; б) повышение осведомленности о рисках дезинформации; в) развитие критического мышления.

Такой подход позволяет одновременно защитить общество от дезинформации, сохранить свободу слова и не допустить превращения антифейкового законодательства в инструмент цензуры. Ключевой принцип здесь — поддержание баланса между защитой общественных интересов и соблюдением конституционных прав граждан в цифровой среде.



Список источников

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 25 декабря 2025 г.).
2. Новоселов И. Э., Смирнов А. А. Генерация биомедицинских изображений для аугментации данных с помощью генеративно-состязательных сетей // МНИЖ. 2024. № 5 (143)
3. Фролова М. Под видео друга: мошенники стали подделывать «кружочки» в Telegram // URL: <https://iz.ru/>
4. Иванов В. Г. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности / В. Г. Иванов, Я. Р. Игнатовский // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2020. № 4. С. 379–386.
5. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с англ. А. А. Слинкина. 2-е изд., испр. М. : ДМК Пресс, 2018.
6. Choi Y., Choi M., Kim M., Ha J. W., Kim S., & Choo J. Stargan: Unified generative adversarial networks for multi-domain image-to-image translation. In Proceedings of the IEEE conference on computer vision and pattern recognition. 2018. P. 8789–8797.
2. Novoselov I. E., Smirnov A. A. Generation of biomedical images for data augmentation using generative-adversarial networks // MNIZH. 2024. No. 5 (143)
3. Frolova M. Under the video of a friend: scammers began to fake «circles» in Telegram // URL: <https://iz.ru/>
4. Ivanov V. G. Deepfakes: prospects for application in politics and threats to personality and national security / V. G. Ivanov, Ya. R. Ignatovsky // Bulletin of the Peoples' Friendship University of Russia. Series: State and Municipal Administration. 2020. No. 4. P. 379–386.
5. Goodfellow Ya., Bendjio I., Courville A. Deep learning / translated from English by A. A. Slinkin. 2nd ed., ispr. M. : DMK Press, 2018.
6. Choi Y., Choi M., Kim M., Ha J. W., Kim S., & Choo J. Stargan: Unified generative adversarial networks for multi-domain image-to-image translation. In Proceedings of the IEEE conference on computer vision and pattern recognition. 2018. P. 8789–8797.

References

1. Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended on December 25, 2025).

Библиографический список

1. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 25 декабря 2025 г.).

Bibliographic list

1. Code of Administrative Offences of the Russian Federation No. 195-FZ dated December 30, 2001 (as amended on December 25, 2025).

Информация об авторе

А. В. Токолов — доцент кафедры противодействия преступлений в сфере информационно-телекоммуникационных технологий Московского университета МВД России имени В.Я.Кикотя, кандидат юридических наук, доцент.

Information about the author

A. V. Tokolov — Associate Professor of the Department of Crime Prevention in the Field of Information and Telecommunication Technologies of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Candidate of Legal Sciences, Associate Professor.

Статья поступила в редакцию 27.01.2026; одобрена после рецензирования 03.02.2026; принята к публикации 10.02.2026.

The article was submitted 27.01.2026; approved after reviewing 03.02.2026; accepted for publication 10.02.2026.