ГРАЖДАНСКО-ПРАВОВОЙ СТАТУС ДИПФЕЙКОВ: СОГЛАСИЕ НА ОБРАБОТКУ ГОЛОСА И ИЗОБРАЖЕНИЯ

О.С. Афонина, *старший преподаватель*
В.В. Рокова, *студент*
А.С. Соболева, *студент*
Калужский государственный университет им. К.Э. Циолковского
(Россия, г. Калуга)

DOI:10.24412/2500-1000-2026-5-2-142-145

Аннотация. *Статья посвящена анализу тенденций, связанных с распространением дипфейк-технологий. Авторы детально изучают судебную практику, посвящённую данному вопросу, а также исследуют научные работы и существующие подходы к регулированию подобных явлений в других странах. На основе исследуемых данных устанавливается отсутствие юридического определения термина «дипфейк», вследствие чего возникает сложность в контроле контента и установления ответственности за его создание. Делается вывод о необходимости распространения этой проблемы на государственном уровне, а также внесения соответствующих изменений в российское законодательство с целью сдерживания возрастающей популярности дипфейков.*

Ключевые слова: *дипфейк; ИИ-технологии; ложный контент; гражданско-правовой статус; авторское право; мониторинг.*

С развитием цифровизации и бурного прогресса в сфере искусственного интеллекта, создание и распространение дипфейков – синтезированного мультимедийного контента – представляет собой предмет многочисленных дискуссий и серьёзных опасений. Особую значимость приобретает их изучение, так как данная технология не является уникальной, а имеет общедоступный характер. Если раньше для создания реалистичных подделок требовались специализированное оборудование и глубокие технические познания, то сегодня любой желающий может воспользоваться простыми в освоении приложениями и программами. Кроме того, качество создаваемых подделок достиг такого уровня совершенства, что зачастую человеку трудно распознать фальсификацию без специальных навыков.

Основная проблема заключается в том, что дипфейки всё чаще применяются с целью причинения вреда, а не просто для развлечения. Они становятся инструментом для распространения ложной информации, манипулирования общественным мнением, а также для вымогательства и мошенничества. Особенно тревожным является отставание законодательства многих стран, включая Россию, от темпов развития этих технологий, а также нехватка эффективных мер противодействия дипфейкам.

Данная технология превращается из развлекательного инструмента в опасное средство, способное нанести не физический, а скорее психологический и финансовый ущерб. Проблема усугубляется зачастую пренебрежительным отношением к ней и недостаточным информированием населения, что приводит к низкому уровню осведомлённости. Пока общество не осознаёт всю серьёзность потенциальных угроз, злоумышленники активно используют человеческую доверчивость и цифровую безграмотность, вводя в заблуждение всё больше людей.

Первый зафиксированный дипфейк был опубликован в 2017 году анонимным пользователем платформы Reddit, который загрузил порнографические видеоролики с лицами известных актрис (Тейлор Свифт, Скарлетт Йоханссон и др.) [2]. Тенденция распространения порнографических дипфейков идет на спад с конца 2018 года, когда, в связи с выборами в США, публикуются дипфейки с Б. Обамой и Д. Трампом. С тех пор прослеживается тенденция политизации использования технологии и связанного с ней манипулирования и мошенничества в различных сферах [3]. На сегодняшний день дипфейки представлены

разнообразными формами, каждая из которых обладает уникальными чертами и способами применения.

Первые заметные случаи использования дипфейков в России, связанные преимущественно с политической сферой, стали появляться в начале 2020-х годов. Один из наиболее резонансных инцидентов произошёл в 2023 году, когда в эфире некоторых телеканалов и радиостанций распространилось фейковое «экстренное обращение» президента Владимира Путина о введении военного положения в приграничных регионах и всеобщей мобилизации [11].

В 2023–2024 годах фиксировались и другие политические дипфейки. Например, распространялись видео с участием бывшего губернатора Курской области Алексея Смирнова и губернатора Приморского края Олега Кожемяко, которым приписывались заявления, которых они никогда не делали. Также встречались дипфейки с «предсмертными заявлениями» глав регионов - например, фейковый ролик о «самоубийстве» губернатора Самарской области Вячеслава Федорищева, после которого чиновнику пришлось публично опровергать собственную «гибель» [5]. Представленные случаи демонстрируют, что дипфейк-технологии носят общественно вредный характер, поскольку с их помощью люди распространяют информацию, порочащую честь и достоинство личности, а также популяризируют её в обществе. Вследствие чего пострадавшие вынуждены опровергать ложные сведения, однако эти меры не всегда способны восстановить утраченную репутацию. Кроме того, следует также учитывать, что дипфейки, являясь относительно новой формой контента, представляют угрозу обществу ввиду низкой информированности населения о них. Многие не осознают, что дипфейки содержат сгенерированные изображения реальных людей, чьи лица и голос были использованы без их разрешения. Это не только посягает на личные неимущественные права граждан, но и способствует нарастанию конфликтных настроений в обществе, провоцируя беспорядки и подрывая общественную безопасность.

Российская правовая система на данный момент не содержит юридического определения понятия «дипфейк». Научное сообщество, в свою очередь, предлагает множество различных интерпретаций этого термина. Например, Лужинская Е.Л. считает, что «Дипфейки – это синтетически произведённый медиаконтент, в котором оригинальный человек (тот, кто изначально находится на изображении) замещается другим человеком» [7]. Игнатенков Г.К. пишет, что «дипфейки – это преднамеренно искаженные аудио, видео или иные файлы с использованием технологии глубокого обучения (определение производное от словосочетания «deep learning» – глубокое обучение, «fake» – подделка), которые изображают что-то вымышленное или ложное, что позволяет злоумышленникам использовать новый и сложный инструмент социальной инженерии» [6].

Анализ предложенных определений позволяет выделить ключевые характеристики дипфейка. Первое – это создание контента при помощи специальных программных средств. Второе – использование личных данных реального человека (внешности, голоса, манеры поведения), чаще всего без его согласия. Третье – намерение выдать ложную информацию за достоверную.

Для определения гражданско-правового статуса дипфейков требуется установить, какие именно нематериальные права граждан они нарушают.

В первую очередь, речь идет о праве на изображение. Согласно статье 152.1 Гражданского кодекса РФ (далее – ГК РФ), использование изображения гражданина допускается только с его согласия, за исключением прямо установленных законом случаев [1]. Дипфейк прямо нарушает это право, так как изображение гражданина в большинстве случаев используется без его согласия. Во-вторых, если дипфейк представляет человека в невыгодном свете, создавая искаженное представление о нем, то это может негативно сказаться на его репутации. Таким образом, нарушается право на честь, достоинство и деловую репутацию, гарантированное статьей 152 ГК РФ [1]. Следовательно, дипфейк выступает инструментом, посягающим на основополагающие права личности и создающим прямую угрозу репутации.

Кроме того, дипфейки могут нарушать авторское право, о чем свидетельствует дело, связанное с незаконным использованием изображения актера Киану Ривза. Московский

арбитражный суд официально признал дипфейк объектом авторского права и взыскал компенсацию в размере 500 000 рублей с компании, распространявшей дипфейк-видео с изображением Киану без соответствующего разрешения [9].

Также дипфейки могут использоваться для фальсификации доказательств при судебных разбирательствах. Например, дело, рассмотренное Куйбышевским районным судом Санкт-Петербурга в 2023 году (дело №2-1347/2023) [10], где сторона ответчика представила аудиозапись телефонного разговора, достоверность которой была оспорена истцом со ссылкой на признаки дипфейка. В ходе разбирательства эксперты не смогли определить подлинность данного доказательства, из-за отсутствия четких методик анализа цифровых материалов, созданных нейросетью. Эти примеры также демонстрируют область применения дипфейков и случаи распространения данного явления.

Ключевое различие дипфейков от других видов фейкового контента заключается в том, что ответственность за распространение последних в основном связана с введением в заблуждение и нанесением ущерба общественным интересам, тогда как ответственность за дипфейки обусловлена, прежде всего, неправомерным использованием персонального образа. Даже имитация внешности или голоса конкретного человека в развлекательных целях, созданная без его согласия и позволяющая его идентифицировать, представляет собой вмешательство в сферу его нематериальных благ и потому является противоправной.

Основная проблема дипфейков заключается в широкой доступности ИИ-сервисов для их создания. Любой человек может использовать чужое изображение для генерации контента, который зачастую трудно отследить. Это порождает вопрос об ответственности за создание и распространение подобных материалов.

Для решения данной проблемы необходим комплексный подход, затрагивающий правовые, технологические и международные аспекты. Во-первых, требуется законодательно урегулировать использование дипфейков, опираясь на удачные примеры правового регулирования других государств. Показательным примером служит первый проект Кодекса практики Еврокомиссии по маркировке и идентификации ИИ-контента, который уже включает обязательные включающие машиночитаемые метки, раскрытие факта ИИ-генерации перед пользователем и формализацию обязанностей платформ [8]. США тоже усилили контроль за ИИ-контентом: подписанный Дональдом Трампом Take It Down Act [4] закрепил за платформами обязанность оперативно удалять несанкционированные интимные изображения и их ИИ-подделки. В российское законодательство необходимо закрепить понятие дипфейка, а также, ссылаясь на вышеупомянутые примеры, ввести специальные маркировки на ИИ-контент. Во-вторых, необходимо создать специальный комитет, который будет специализироваться на дипфейках и отслеживать использование ИИ-технологий в противоправных целях. Следует разработать эффективную программу мониторинга данного контента, чтобы в последующем можно было бы ввести ответственность за создание и распространение этих материалов. В-третьих, нельзя забывать о международном сотрудничестве, так как данная проблема затрагивает все страны, а не только Российскую Федерацию. Необходимо разрабатывать совместные положения, регулирующие ИИ-контент в целом, а также распространение дипфейков, так как это нарушает общественный порядок.

Таким образом, хотя феномен дипфейков существует давно, наибольшее распространение он получил относительно недавно с развитием искусственного интеллекта. Поскольку это довольно новая тема, то законодательство всех стран, в том числе и России, не ориентировано на регулирование данной проблемы. Несмотря на это, многие учёные начинают излагать свои мысли по этому поводу, показывая, что люди нуждаются в государственной защите от такого контента, ведь он нарушает права человека. Реализация предложенных мер должна запустить процесс изучения и регулирования дипфейков на государственном и международном уровнях, что в перспективе приведёт к снижению распространения такого контента.

Библиографический список

1. Гражданский кодекс Российской Федерации (ГК РФ) 30 ноября 1994 года N 51-ФЗ // СПС Консультант Плюс. – [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_5142/.
2. Albahar M., Almalki J. Deepfakes: Threats and countermeasures systematic review // Journal of Theoretical and Applied Information Technology. – 2019. – Т. 97. – № 22. – С. 3242-3250. – [Электронный ресурс]. – Режим доступа: https://www.academia.edu/94949998/Deepfakes_Threats_and_Countermeasures_Systematic_Review.
3. Appel M., Prietzel F. The detection of political deepfakes // Journal of Computer-Mediated Communication. – 2022. – Т. 27. – №4. – [Электронный ресурс]. – Режим доступа: https://colab.ws/articles/10.1093%2Fjcmc%2Fzmac008.
4. Congress.Cov. – [Электронный ресурс]. – Режим доступа: https://www.congress.gov/bill/118th-congress/senate-bill/3696.
5. Дзен. – [Электронный ресурс]. – Режим доступа: https://dzen.ru/a/aUW90ej8yzbxqmaR.
6. Игнатенков, Г.К. Технология дипфейк как угроза информационной безопасности / Г.К. Игнатенков // Наука. Исследования. Практика: Сборник избранных статей по материалам Международной научной конференции, Санкт-Петербург, 25 июня 2022 года. – Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2022. – С. 74-77. – EDN ILYZTN.
7. Лужинская Е.Л. Особенности исследования изображений внешнего облика человека, измененного при помощи программных средств / Е.Л. Лужинская, В.А. Чванкин // Вопросы криминологии, криминалистики и судебной экспертизы. – 2022. – № 2(52). – С. 116-121. – EDN PLZXXD.
8. Официальный сайт Европейского союза. – [Электронный ресурс]. – Режим доступа: https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content.
9. Постановление от 7 апреля 2024 г. по делу № А40-200471/2023. – [Электронный ресурс]. – Режим доступа: https://sudact.ru/arbitral/doc/FPdEj2cpgSdC/.
10. Решение Куйбышевского районного суда г. Санкт-Петербурга от 17 апреля 2023 года по делу № 2-1347/2023. – [Электронный ресурс]. – Режим доступа: https://судебныерешения.рф/73588166.
11. ТАСС Медиа. – [Электронный ресурс]. – Режим доступа: https://tass.ru/obschestvo/17933053.

CIVIL STATUS OF DIPFAKES: CONSENT TO PROCESSING VOICE AND IMAGE

O.S. Afonina, *Lecturer*
V.V. Rokova, *Student*
A.S. Soboleva, *Student*
Kaluga State University named after K.E. Tsiolkovsky
(Russia, Kaluga)

Abstract. *The article is devoted to the analysis of trends related to the spread of deepfake technologies. The authors study in detail the judicial practice devoted to this issue, as well as research scientific works and existing approaches to regulating such phenomena in other countries. Based on the data studied, it is established that there is no legal definition of the term "deepfake", which results in the complexity of controlling the content and establishing responsibility for its creation. It is concluded that it is necessary to spread this problem at the state level, as well as to make appropriate changes to Russian legislation in order to curb the growing popularity of deepfakes.*

Keywords: *deepfake; AI technologies; false content; civil status; copyright; monitoring.*