УДК 34:004

Геворгян Марианна Севадаевна,
студент,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»
г. Екатеринбург, Российская Федерация

Сибиряков Павел Олегович,
студент,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»
г. Екатеринбург, Российская Федерация

Жевняк Оксана Викторовна,
кандидат юридических наук, доцент,
кафедра правового регулирования экономической деятельности,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»
г. Екатеринбург, Российская Федерация

ПРАВОВОЙ РЕЖИМ DEEPFAKE

Аннотация:
Рассмотрено использование дипфейков в современном мире, в том числе при оплате с помощью биометрических данных. Исследованы этические и правовые аспекты использования изображений умерших людей в дипфейках, применение аудиофейков и возможность введения «права на голос», влияние дипфейков в социальных сетях. Сделан вывод о необходимости разработки мер по борьбе с распространением дипфейков.

Ключевые слова:
DeepFake, дипфейк, нейросети, авторское право, изображение умерших, биометрические данные, аудиодипфейки, голосовая аутентификация, ложные новости, правовой режим DeepFake, этика DeepFake, дезинформация, DeepFake в социальных сетях, защита от DeepFake.

Современный мир развивается очень быстро. Информационные технологии становятся всё лучше, и одним из ключевых направлений совершенствования этой сферы является разработка и улучшение нейросетей. Они, подобно человеку, уже могут создавать изображения, понимать смысл текста и речи, писать программы и анализировать данные. Одной из возможностей нейросетей является замена одного фрагмента изображения, аудио или видео другим так, что на первый взгляд невозможно определить подделка это или нет. Такая технология называется дипфейк (DeepFake). Дипфейк – это соединение двух слов «глубокий» (в контексте ИИ чаще понимается как глубокое обучение) и «подделка» [1].

В России и других странах право авторства на дипфейки, как и на другие виды контента, защищается законодательством об авторском праве. Это означает, что автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат (ст. 1228 ГК РФ [2]), а правообладателем может быть как гражданин, так и юридическое лицо. Таким образом, можно заключить, что объект авторского права не будет создан, пока к работе искусственного интеллекта не будет причастен человек.

Рассмотрим вопрос использования изображения умерших людей в материалах, созданных с помощью дипфейк. В случае, когда с помощью этой технологии создаются фотографии, всё довольно просто. Данную проблему регулирует ст. 152.1 ГК РФ [3]. В ней сказано, что после смерти человека его изображение может использоваться только с разрешения близких людей, за исключением некоторых ситуаций.

Однако стоит отметить, что в результате генерации видео с умершим мы получим не просто изображение человека, а целиком его образ. В существующем законодательстве нет правовых актов, регламентирующих использование таких видеоматериалов. В судебной практике так же не было прецедентов применения образа умершего человека. Поэтому в данном случае стоит обратиться к ст. 6 ГК РФ [3] и рассматривать использование образа человека по аналогии с использованием изображения.

Большой угрозой дипфейки являются для персональных данных и денежных средств, защищенных биометрическими системами. Мошенники с помощью нейросетей генерируют сканы документов, видеоролики с лицом жертвы, которые используют для аутентификации по биометрии в различных системах, а также при

онлайн-общении с сотрудниками банков. Считается возможным даже копирование изображения сетчатки глаза. Поэтому многие компании задумались о защите данных своих клиентов.

В 2023 г. VisionLabs разработали технологию, которая позволяет определить, присутствует ли замена лица на фото или видео, перенос выражения лица и мимики. Кроме того, в этом направлении работают такие разработчики, как Intel, Zemana, Sensity и конечно же Сбер [4].

Но помимо лица, отпечатка пальцев и сетчатки глаз, одним из наиболее распространенных способов аутентификации с помощью биометрии является авторизация с помощью голоса. Мошеннику достаточно пары секунд телефонного разговора для того, чтобы создать его копию и использовать для своих целей. Аудиодипфейки можно назвать одними из самых опасных, ведь человеческий голос не является объектом собственности и, соответственно, право на него пока не защищается ни в одной стране мира. Кроме того, что аудиофейки используются при идентификации личности с помощью биометрии, голоса политиков и знаменитостей активно используются для создания как развлекательного контента, так и более серьезного, который может вводить в заблуждение их аудиторию.

Вред от распространения аудиодипфейков может быть значительным. Они могут использоваться для создания ложных новостей, политической пропаганды, фальшивых аудиодоказательств в суде или для порочных целей в общественном дискурсе. Это может привести к распространению недостоверной информации, спровоцировать конфликты, повлиять на решения, принимаемые на основе поддельных данных, и подорвать доверие к СМИ и другим источникам информации.

Одним из путей решения этой проблемы стало обучение программ распознаванию аудиодипфейков. Ученые пришли к выводу, что в этом вопросе с искусственным интеллектом могут справиться только ему подобные, ведь даже самый чуткий слух не сможет распознать хорошо подделанный голос. Поэтому разрабатываются различные программы, способные распознать поддельные голосовые записи. Так, сингапурская DSO National Laboratories разработала программу, которая оценивает неестественные эффекты в аудиозаписях – резкие паузы и внезапные изменения темпа речи. Resemble AI после разработки системы синтезирования голосовых фейков создали платформу по их распознаванию. Американская компания Pindrop также разработали действенный метод по определению аудиодипфейков [5].

Возникает вопрос о том, можно ли использовать публично доступные изображения и видео людей для создания дипфейк-материалов. В этом случае такие ресурсы относятся к категории общедоступной информации и регулируются Федеральным законом «Об информации, информационных технологиях и о защите информации» [6]. В соответствии с этим законом дипфейки, созданные на основе общедоступных персональных данных, не являются противоправными. Однако их распространение без согласия субъекта персональных данных будет незаконным [7].

Распространение дипфейков в социальных сетях и СМИ стало серьезной проблемой в современном информационном пространстве. Их регулирование представляет собой сложную задачу для законодателей, так как необходимо соблюдать баланс между свободой слова и защитой от манипуляций. Для контроля за распространением дипфейков правительства разрабатывают и внедряют различные стратегии. В основном это сотрудничество с социальными сетями для разработки технологических решений, способных обнаруживать и удалять подобный контент. На законодательном уровне дипфейки запрещены лишь в нескольких странах, в число которых Россия, к сожалению, пока не входит; не предусмотрены и специальные составы соответствующих правонарушений, что, однако, не исключает применения ответственности по существующим статьям российского законодательства. В КНР, например, распространение дипфейков признано уголовным преступлением. В ряде других стран также обсуждается вопрос о том, чтобы ограничить их использование и публикацию [8].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. DeepFake в условиях современности: что, почему и возможно ли защититься [Электронный ресурс]// Сайт проекта «Хабр». Блог компании FirstVDS. Автор статьи: @DeathDay 2022. 23 декабря. URL : https://habr.com/ru/companies/first/articles/707246/ (дата обращения: 14.04.2024).
2. Гражданский кодекс Российской Федерации. Часть четвертая: Федеральный закон от 18.12.2006 г. № 230-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL : https://www.consultant.ru/document/cons_doc_LAW_64629/ (дата обращения: 14.04.2024).
3. Гражданский кодекс Российской Федерации. Часть первая: Федеральный закон от 30.11.1994 г. № 51-ФЗ (с изм. и доп.) [Электронный ресурс]// СПС «КонсультантПлюс». URL : https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 14.04.2024).
4. Кинякина Е., Заруцкая Н. Биометрические проверки начнут защищать от дипфейков [Электронный ресурс]// Сетевое издание Ведомости (Vedomosti). 2023. 1 июня. URL : https://www.vedomosti.ru/technology/articles/2023/06/01/978035-biometricheskie-proverki-nachnut-zaschischat-ot-dipfeikov (дата обращения: 14.04.2024).
5. Янина Ноэль. Дипфейки: как трансформируется авторское право на контент [Электронный ресурс]// Сетевое издание «РБК.Тренды». 2021. 18 мая. URL : https://trends.rbc.ru/trends/industry/5fc688fe9a79473e6ff9b82a (дата обращения: 14.04.2024).

6. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп.) [Электронный ресурс]// СПС «КонсультантПлюс». URL : https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 14.04.2024).
7. Рожкова М. А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? [Электронный ресурс] // Закон.ру. 2021. 13 января. URL : https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye_i_personalnye_dannye_razreshennye_subektom_dlya_raspros (дата обращения: 14.04.2024).
8. Дремлюга Р. И., Моисейцев В. В., Парин Д. В., Романова, Л. И. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (deepfake): опыт Китая [Электронный ресурс] // Азиатско-Тихоокеанский регион: экономика, политика, право. 2023. № 24(4). С. 91-104. URL: https://doi.org/10.24866/1813-3274/2022-4/91-104 (дата обращения: 14.04.2024).

Gevorgyan Marianna Sevadaevna,
student,
Institute of Economics and Management,
Ural Federal University named after the first President of Russia B.N. Yeltsin,
Yekaterinburg, Russian Federation

Sibiryakov Pavel Olegovich,
student,
Institute of Economics and Management,
Ural Federal University named after the first President of Russia B.N. Yeltsin,
Yekaterinburg, Russian Federation

Zhevnyak Oksana Viktorovna,
Candidate of Legal Sciences, Associate Professor,
Associate Professor of the Department of Legal Regulation of Economic Activities,
Institute of Economics and Management,
Ural Federal University named after the first President of Russia B.N. Yeltsin,
Yekaterinburg, Russian Federation

LEGAL REGIME OF DEEPFAKE

Abstract:
The use of deepfakes in the modern world, including when paying with biometric data, is considered. The ethical and legal aspects of the use of images of deceased people in deepfakes, the use of audio fakes and the possibility of introducing the “right on vote,” and the influence of deepfakes on social networks have been studied. It is concluded that it is necessary to develop measures to combat the spread of deepfakes.

Keywords:
DeepFake, deepfake, neural networks, copyright, images of the dead, biometric data, audio deepfakes, voice authentication, fake news, legal regime of DeepFake, ethics of DeepFake, disinformation, DeepFake on social networks, protection from DeepFake.