Научная статья
УДК 343.3/.7
DOI: 10.37973/VESTNIKKUI-2024-56-13

ДИПФЕЙК (DEEPFAKE) И УГОЛОВНЫЙ ЗАКОН

Марина Александровна Ефремова[1], Евгений Александрович Русскевич[2],
[1] Российский государственный университет правосудия
(Казанский филиал), Казань, Россия,
[2] Московский государственный юридический университет
имени О.Е. Кутафина (МГЮА), Москва, Россия,
[1] crimlaw16@gmail.com, [2] russkevich@mail.ru

Аннотация

Введение: в условиях цифровизации практика распространения недостоверных сведений приобрела совершенно новое содержание – дипфейк не просто создает конкуренцию объективному освещению событий, а претендует на то, чтобы подменить саму реальность. Авторы отмечают беспрецедентность данной проблемы не только для отдельного человека либо государства, но и для человечества в целом, поскольку дипфейк несет в себе экзистенциальную угрозу самой социальной коммуникации.

Материалы и методы: исследование проведено на основе общепринятой методологии (комбинации общих и частных методов познания). Работа осуществлялась на основе действующего российского законодательства, законодательства отдельных зарубежных стран, материалов правоприменительной практики, научной литературы и иных публикаций по теме в сети Интернет.

Результаты исследования: в работе аргументируется вывод о необходимости дополнения отечественной модели дифференциации уголовной ответственности новым квалифицирующим признаком – «совершение преступления с использованием технологии дипфейк».

Обсуждение и заключение: проблема использования технологии глубокого синтеза (дипфейка) в целях причинения вреда охраняемым законом интересам требует комплексного подхода и не имеет сугубо правового решения. С учетом особенностей технологии нет оснований говорить и о том, что имеются социально-правовые предпосылки к криминализации любых действий с дипфейками. Реальное противодействие предполагает выработку четких критериев вредоносного дипфейка на теоретическом уровне, технологических решений оперативного выявления и удаления такого контента, выстраивание государственно-частного партнерства в этой области, подготовку соответствующих кадров с необходимыми компетенциями и др.

Ключевые слова: дипфейк; фейк; фейковизация; преступный обман; преступления в сети «Интернет»

Для цитирования: Ефремова М.А., Русскевич Е.А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 2 (56). С. 97 – 105. DOI: 10.37973/VESTNIKKUI-2024-56-13. DOI: 10.37973/VESTNIKKUI-2024-56-13

Scientific article
UDC 343.3/.7
DOI: 10.37973/VESTNIKKUI-2024-56-13

DEEPFAKE AND CRIMINAL LAW

Marina Aleksandrovna Efremova[1], Evgeniy Aleksandrovich Russkevich[2],
[1] Russian State University of Justice (Kazan branch), Kazan, Russia,
[2] Kutafin Moscow State Law University (MSAL), Moscow, Russia,
[1] crimlaw16@gmail.com, [2] russkevich@mail.ru

Abstract

Introduction: in the context of digitalization, the dissemination of false information has acquired a completely new content – deepfake not only creates competition for objective coverage of events, processes or phenomena, but claims to replace reality itself. The authors note the unprecedented nature of this problem not just for an individual or state, but for humanity as a whole, since deepfake poses an existential threat to social communication itself.

Materials and Methods: the study was conducted on the basis of generally accepted methodology (a combination of general and specific methods of cognition). The work was carried out on the basis of current Russian legislation, the legislation of individual foreign countries, materials from law enforcement practice, scientific literature and publications on the topic on the Internet.

Results: the work argues for the conclusion that it is necessary to supplement the domestic model of differentiation of criminal liability with such a qualifying feature as committing a crime "using deepfake technology".

Discussion and Conclusions: the problem of using deep synthesis technology (deepfake) for the purpose of causing harm to legally protected interests requires an integrated approach and does not have a purely legal solution. Taking into account the peculiarities of the technology, there is no reason to say that there are social and legal prerequisites for the criminalization of any actions with deepfakes. Real counteraction involves developing clear criteria for malicious deepfake at a theoretical level, technological solutions for prompt identification and removal of such content, building public-private partnerships in this area, training appropriate personnel with the necessary competencies, and much more.

Keywords: deepfake; fake; fakery; criminal deception; crimes on the Internet

For citation: Efremova M.A., Russkevich E.A. Deepfake And Criminal Law. Bulletin of the Kazan Law Institute of MIA of Russia. 2024;15(2):97-105. (In Russ.). DOI: 10.37973/VESTNIKKUI-2024-56-13

Введение

Термин «дипфейк» впервые был использован на платформе социальных сетей Reddit в 2017 году [1]. Изначально дипфейк определялся как использование искусственного интеллекта для модификации карты лиц для создания новых реалистичных изображений. Однако с развитием самой технологии звук и изображение теперь могут создаваться одновременно или по отдельности. Сегодня технология дипфейк позволяет создавать аудио- или видеоматериалы с использованием голоса и (или) изображения другого человека. Использование данной технологии доступно любому владельцу смартфона, который с помощью нескольких приложений (FaceApp, ReFaceApp, FaceMagic и т.д.) после загрузки их на свое устройство может создать дипфейк за короткий промежуток времени. Технология дипфейк успешно применяется в киноиндустрии, где, например, один и тот же персонаж может быть молодым, а главный герой может говорить на разных языках. Положительное применение новой технологии не ограничивается кинематографом. Она может быть использована в сфере образования, здравоохранения и развлечений. Тот факт, что технология глубокой подделки все чаще используется обычными людьми, а не специалистами, открывает путь для ее неправомерного использования и заставляет нас рассматривать дипфейк через призму уголовного закона. Уже сегодня серьезно относясь к этому потенциалу, международные организации рассматривают дипфейк как одну из самых серьезных угроз будущего[1].

[1] Facing Reality? Law Enforcement and the Challenge of Deepfakes: An Observatory Report from the Europol Innovation Lab. LU: Publications Office. URL: https://data.europa.eu/doi/10.2813/08370 (дата обращения: 15.09.2023).

Технология глубокой подделки (или глубокого синтеза, как часто указывается в зарубежной литературе) довольно быстро получила популярность. На настоящий момент количество таких материалов в сети Интернет велико, по разным оценкам, составляет сотни тысяч, но, пожалуй, едва ли подлежит точному измерению. По данным DeepMedia, компании, работающей над инструментами для обнаружения дипфейков, в 2023 году в Интернете было опубликовано в три раза больше видео-дипфейков всех видов и в 8 раз больше голосовых дипфейков, чем в 2022 году[1]. Дополнительно следует обратить внимание на то, что технология непрерывно развивается и правдоподобность таких материалов все время повышается.

В результате в цифровом пространстве искушенный пользователь ставит под сомнение все – любую информацию независимо от ее содержания, контекста и способа презентации. Понятно, что при таком положении дел говорить о каком-либо доверии не приходится. На этом фоне наблюдается серьезнейшее сомнение и в том, чтобы вообще воспринимать Интернет как возможный источник достоверной информации.

Вполне очевидно, что в сложившихся условиях юридическая наука не может оставаться в стороне от осмысления технологии глубокого синтеза (дипфейка). В уголовно-правовом контексте требуется ответить на совокупность вполне традиционных вопросов: насколько применимы существующие правовые конструкции для реагирования на инциденты (известные и возможные) с дипфейками? Имеются ли социально-правовые предпосылки к полному запрету использования технологии, в том числе средствами механизма уголовной репрессии? Имеются ли основания для криминализации отдельных форм эксплуатации технологии?

Обзор литературы

Дипфейк исследуется на разных уровнях. С технологической точки зрения специалистами активно решается задача разработки инструментов, позволяющих оперативно выявлять такие материалы в сетевом пространстве с целью их удаления либо блокирования[2].

Вопросы глубокого синтеза изображений и видео прорабатываются в работах по социологии (В.Г. Иванов, Я.Р. Игнатовский [2]), политологии (Н.Р. Красовская, А.А. Гуляев [3]) и журналистике (И.А. Васильева, Н.В. Халина [4]).

В юридической науке обращается внимание на правовое регулирование использования дипфейков при посмертном использовании голоса или изображения человека (Т.С. Яценко [5]), исследуются риски глубокого синтеза для медиабезопасности (В.Д. Никишин [6]), анализируются имеющиеся возможности для противодействия созданию и распространению дипфейков (В.О. Калятин [7], А.В. Минбалеев [8]). Отдельно разрабатываются проблемы достоверности цифровых доказательств (Н.Н. Апостолова [9]) и развития онлайн-правосудия (В.А. Лаптев [10]).

В рамках самостоятельного направления исследуются вопросы правомерного использования технологии глубокого синтеза, например, в оперативно-розыскной деятельности (В.Б. Батоев [11]).

Материалы и методы

Исследование проведено на основе общепринятой методологии (комбинации общих и частных методов) и с использованием открытых источников информации. Объектом исследования выступали отношения, возникающие в связи с реализацией уголовной ответственности за преступления, совершаемые с использованием технологий глубокой подделки (дипфейк). Поставленная исследовательская задача предполагала уяснение природы и содержания самого явления – дипфейка – как процесса, приводящего к искажению индивидуального и (или) общественного сознания. По этой причине на начальном этапе исследования значительное место в методологии было уделено наблюдению, опросу специалистов и контент-анализу прессы. Накопление эмпирического материала сопровождалось его систематизацией и анализом. Формально-догматические методы исследования преимущественно были задействованы на втором этапе работы как при анализе материалов правоприменения, так и при оценке состояния действующего уголовного законодательства России. Исследование проведено с использованием сравнительно-правового метода, который позволил выявить подходы (модели) к установлению ответственности за дипфейк в зарубежных странах. На заключительном этапе благодаря синтезу полученной информации были сформулированы предложения по модернизации уголовного законодательства, разработаны рекомендации по совершенствованию правоприменения. Особо следует отметить, что значительное место в методологии проведенного исследования занимает метод научной экстраполяции. С учетом

[1] Deepfaking it: America's 2024 election collides with AI boom. URL: https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30 (дата обращения: 15.09.2023).

[2] Создан открытый алгоритм, защищающий изображения от дипфейков. URL: https://nauka.tass.ru/nauka/18686953?ysclid=lq3d4m827c148831024 (дата обращения: 15.09.2023); Российские ученые создали инструмент для выявления дипфейк-видео. URL: https://www.anti-malware.ru/news/2023-10-20-114534/42148 (дата обращения: 15.09.2023).

усиливающейся распространенности использования технологии глубокой подделки (дипфейк), ее все возрастающей доступности для пользователей сети Интернет авторы с использованием данного метода решали задачу выделения наиболее вероятных тенденций изменения состояния преступности в России.

Результаты исследования

Следует согласиться с мнением В.О. Калятина о бессмысленности дискуссии относительно того, приносит ли вред пользователям та или иная технология, поскольку это лишь инструмент, который может применяться в разных целях [7]. Верная и важная мысль. Дипфейк может быть эффективным средством презентации информации, безобидной шуткой, приятным розыгрышем или инновационным инструментом осуществления образовательного процесса. Представим себе ситуацию, что для урока географии учитель подготовил синтезированное видео, на котором учебный материал излагает Федор Конюхов или Николай Дроздов. Не следует забывать, что изначально технологии глубокого синтеза стали применяться в киноиндустрии для искусственного воспроизведения обстановки, замены актеров роботами-дублерами при выполнении опасных трюков и др. Благодаря этой технологии Брюс Ли «снялся» в рекламе виски «Джонни Уокер» [12]. В 2020 г. с согласия наследников изображение и голос актера Леонида Куравлева были использованы в образе известного персонажа Жоржа Милославского в рекламе Сбербанка[1].

В то же время известно, что технологии глубокого синтеза уже сейчас применяются для совершения мошенничества, вымогательства, изготовления порнографии, распространения заведомо ложной общественно значимой информации, дискредитации Вооруженных Сил Российской Федерации и т.д. Иными словами, свойством дипфейка – равно как и любой инновационной разработки – является амбивалентность с точки зрения возможных социальных последствий. Следовательно, ошибочно видеть общественную опасность в самой технологии. В этом отношении требуется осмыслить состояние действующего уголовного законодательства России на предмет его применимости к случаям использования технологии глубокого синтеза в преступных целях.

Здесь, пожалуй, наиболее актуальным является разрешение вопроса о возможности применения положений УК РФ об ответственности за изготовление и распространение порнографии к случаям использования изображения человека в таких материалах без его согласия. Полагаем, действующая редакция ст. 242 УК РФ в целом позволяет квалифицировать так называемый FaceSwap, то есть перенос лица одного человека в фото или видео вместо другого лица, как изготовление порнографических материалов. Конечно же, отмеченное является верным лишь при условии, если сами материалы будут носить явно выраженный сексуальный характер запечатленных процессов, касающихся интимной жизни и сферы сексуальных отношений, отличаться бесстыдством и пренебрежением к нормам общественной нравственности. То обстоятельство, что правонарушитель лишь подменяет изображение одного человека в изначально готовых порнографических файлах, не препятствует оценке содеянного как изготовления. Результат такой модификации направлен не просто на улучшение качества изображения материала, а на изменение его содержания. При этом нельзя, пожалуй, не согласиться с тем, что «замена» действующих лиц принципиально меняет материал с содержательной точки зрения, наполняет его новой информацией. Следовательно, такие действия обладают всеми признаками изготовления новых порнографических материалов, хотя бы и в результате глубокой переработки фотографий или видео, найденных преступником в сети Интернет.

Проблема технологии глубокой подделки или дипфейка находится в неразрывном единстве с такой категорией, как манипулирование общественным мнением или массовым сознанием. Действительно, прежде всего, специалисты отмечают очевидные риски, которые подобные технологии несут для установления и поддержания доверия между гражданским обществом и государством. В условиях когда дипфейк ставит под сомнение практически любой источник получения социально значимой информации, возникает состояние недоверия между личностью и государством. Предсказуемым следствием этого является недоверие, отторжение и даже противодействие.

В современной литературе процесс создания и распространения недостоверных сведений получил наименование фейковизация. По мнению ученых, фейковизация представляет собой процесс, приводящий к изменению современного дискурса (его насыщению недостоверной информацией), а также результат этого процесса. Фейковизация является одним из основных спутников манипулирования массовым сознанием, осуществляемого в рамках информационной войны. И наконец, фейковизация не может рассматриваться в отры-

[1] Сбер заплатил семье Куравлёва за «оживление» образа на экране. URL: https://octagon.media/novosti/sber_zaplatil_seme_kuravleva_za_ozhivlenie_obraza_na_ekrane.html?ysclid=lq3cweqr9r770825906 (дата обращения: 11.12.2023).

ве от своих конкретных проявлений – фейковых (недостоверных) информационных продуктов в медиасреде [13, с. 22].

Уже сейчас можно говорить о том, что дипфейк может выступать средством совершения любых преступлений, связанных с распространением недостоверной либо иной вредоносной информации. Использование технологии глубокого синтеза создает основания для квалификации, например, клеветы по такому квалифицирующему признаку как использование информационно-телекоммуникационных сетей, а применительно к публичному распространению дезинформации о Вооруженных Силах Российской Федерации – по признаку искусственного создания доказательств обвинения (п. «в» ч. 2 ст. 207^3 УК РФ). Немногочисленная правоприменительная практика придерживается именно такого подхода[1].

Дипфейк позволяет распространить вредоносную информацию с использованием изображения другого человека. В связи с этим важно отметить, что такие действия должны быть квалифицированы не только в соответствии со статьей уголовного закона об ответственности за соответствующие призывы, оправдание, дискредитацию и т.п. (ст. 205^2, 280, 280^3 УК РФ), но и по ст. 128^1 УК РФ. В этих ситуациях дипфейк всегда посягает на честь и достоинство личности. Конечно же, исключением является ситуация, когда используется изображение несуществующего в действительности персонажа (кинематографического или мультипликационного героя).

Дипфейк может иметь ярко выраженный недостоверный и одновременно оскорбительный характер, когда целью преступника является именно умаление достоинства личности. В этом случае корректировка изображений либо видеозаписей может иметь очевидно абсурдный характер. В предусмотренных уголовным законом случаях лицо может подлежать ответственности за такие действия (например, по ст. 297 УК РФ)[2].

В зарубежной литературе проблема дипфейка прежде всего была поставлена применительно к посягательствам на отношения, связанные с реализацией избирательного процесса [14, с. 366]. В 2020 г. президент США Дональд Трамп подписал первый в истории страны закон, направленный на противодействие фейковизации (The National Defense Authorization Act for Fiscal Year 2020). Исполнение данного закона предполагало подготовку исследований в области оказания неправомерного влияния на внутриполитические процессы страны путем распространения недостоверных сведений, в т.ч. дипфейков. Кроме того, были организованы соревнования (Deepfakes Prize Competition) с целью разработки наиболее эффективных способов противодействия дипфейкам. Вознаграждение победителей соревнований было определено в размере 5 млн. долларов США.

В отдельных штатах США были предприняты меры, направленные на дополнение уголовного законодательства специальными нормами об ответственности за создание либо распространение дипфейков. Так, например, в 2019 г. в штате Техас были введены специальные положения об ответственности за создание и распространение дипфейков в целях опорочить кандидата на выборную должность либо иным образом повлиять на результаты выборов (наказывается лишение свободы на срок до одного года со штрафом до 4 тыс. долларов США) [14, с. 373]. В штате Вирджиния были приняты специальные изменения в целях регламентации ответственности за создание и распространение дипфейк-порнографии [14, с. 370-371].

Действительно, технология глубокого синтеза может быть использована в процессе политической борьбы в целях дискредитации отдельных лиц, формирования неверного представления у общественности относительно конкретных событий или процессов. В соответствии с отечественным уголовным законодательством такие действия могут быть квалифицированы как воспрепятствование свободному осуществлению гражданином своих избирательных прав или права на участие в референдуме, соединенное с обманом (п. «а» ч. 2 ст. 141 УК РФ).

Однако здесь необходимо сделать одну весьма важную оговорку. Проблема дипфейка всегда будет самым тесным образом соприкасаться с правом на свободу слова и самовыражения. Нельзя не учитывать, что технология может быть использована для подачи материала в жанре сатиры либо комедии при остром обсуждении общественно значимых проблем и критике конкретных лиц, наделенных властными полномочиями. В этом отношении перспективным представляется разработать механизм об обязательной маркировке материалов, созданных с использованием технологии глубокого синтеза. Соответственно, нанесение пометки «дипфейк» автором и (или) распространителем подобного материала, должно исключать возможную ответственность в случаях, когда лицо действует в общественном интересе.

[1] Апелляционное постановление Юрьев-Польского районного суда Владимирской области от 22.08.2023 по делу № 10-4/2023. СПС «КонсультантПлюс» (дата обращения: 20.12.2023).

[2] Приговор Сыктывдинского районного суда Республики Коми от 30.05.2022 по делу № 1-85/2022. СПС «КонсультантПлюс» (дата обращения: 20.12.2023).

Заблуждением является представление о том, что проблема дипфейка затрагивает или может быть поставлена исключительно к посягательствам, связанным с распространением недостоверной и (или) вредоносной информации. К сожалению, это далеко не так. Технологии глубокой подделки уже в самом ближайшем будущем могут весьма существенно изменить практику по делам о мошенничестве. Дипфейк как форма высокотехнологичного и изощренного обмана в скором времени может создать серьезнейшие затруднения на уровне использования сервисов дистанционного банковского обслуживания. Такие случаи уже имели место на практике. Так, в 2019 г. преступник, использовав аудио-дипфейк, представился руководителем головной компании. Служащий, доверившись голосу по телефону, решил, что разговаривает со старшим руководителем. Последний распорядился осуществить транзакцию поставщику. В результате этого компании был причинен ущерб в размере более двухсот тысяч долларов США[1].

Похожий инцидент в декабре 2023 г. произошел с концертным директором Александра Буйнова. В течение двух дней он полагал, что общается с артистом посредством переписки в Telegram, в т.ч. путем получения коротких видео от него. Оказалось, что все было сфальсифицировано – с помощью дипфейка злоумышленник пытался похитить 10.000 долларов США[2]. Таким образом, преимущества технологии дипфейк позволяют использовать доверие потерпевшего, который не сомневается, что общение происходит с его реальным знакомым, коллегой и т.д.

Очень многое указывает на то, что в ближайшем будущем технология глубокого синтеза (дипфейк) ознаменует принципиально новый этап в практике дистанционного мошенничества, и если не сменит, то во всяком случае существенно потеснит «звонарей». Понятно, что это будет представлять новый вызов для правоохранительной системы, который потребует раскрытия криминалистической характеристики дипфейк-мошенничества, разработки новых алгоритмов проведения отдельных следственных действий, проработки вопросов применения института специальных знаний при расследовании таких преступлений и др.

Кроме изготовления порнографических материалов, в том числе для последующего вымогательства, данная технология может быть использована при компрометации государственных служащих или иных лиц в целях прекращения их профессиональной деятельности, а равно по мотиву мести за такую деятельность либо из карьеризма, личной неприязни и т.п. В последнем случае материалы могут быть связаны с изображением конкретного человека, якобы совершающего аморальный поступок или правонарушение, либо действия, подрывающие деловую репутацию организации, в которой он осуществляет свою трудовую деятельность. Уже в настоящее время суды рассматривают обращения граждан, оспаривающих решения об увольнении по таким основаниям, ссылаясь на то, что соответствующие материалы были искусно сфальсифицированы путем редактирования фотографий и видеозаписей, изменения их содержания, в т.ч. с включением нецензурных выражений[3].

Потерпевших можно шантажировать новыми изображениями, полученными с помощью глубокой подделки, и их репутация в социальной и деловой сфере может серьезно пострадать. В 2021 году в США женщина использовала несколько изображений девочек из школьной команды чирлидеров, чтобы создать поддельные изображения их обнаженными, употребляющими алкоголь и курящими электронные сигареты. Сообщения были разосланы самим потерпевшим и тренеру команды[4].

Не исключена возможность использования дипфейка при совершении должностных преступлений. Здесь наиболее наглядным примером может выступать использование технологии при служебном подлоге (например, для фальсификации приложений к официальному документу). Технология глубокого синтеза может быть также использована при совершении такого преступления как фальсификация доказательств и результатов оперативно-разыскной деятельности. В таких случаях современная редакция ст. 303 УК РФ позволяет надлежащим образом квалифицировать содеянное.

В зарубежной литературе обращено внимание на то, что в скором времени распространение дипфейков может создать реальную угрозу для

[1] Stupp C. Fraudsters Used Ai to Mimic CEO's Voice in Unusual Cybercrime Case // The Wall Street Journal. 30.08.2019. URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (дата обращения: 17.11.2023).

[2] Мошенник под видом Буйнова пытался выманить деньги у директора артиста. URL: https://lenta.ru/news/2023/12/18/buynov-moshennik/ (дата обращения: 20.12.2023).

[3] Определение Восьмого кассационного суда общей юрисдикции от 11.07.2023 № 88-14506/2023 по делу № 2-4240/2022. СПС «КонсультантПлюс» (дата обращения: 20.12.2023).

[4] URL: https://www.bbc.com/news/technology-56404038#:~:text=A%20mother%20allegedly%20used%20xplicit,smoking%22%20%2D%20to%20the%20coach (дата обращения: 20.12.2023).

поддержания международного мира и безопасности человечества. В подтверждение этого авторы, как правило, ссылаются на получивший широкую известность дипфейк, в котором президент Дональд Трамп обращается к нации с сообщением о ядерной атаке в отношении Северной Кореи [15, с. 102]. Отечественное уголовное законодательство позволяет реагировать и на такие деяния. Так, использование дипфейка может выступать способом публичных призывов к развязыванию агрессивной войны (ст. 354 УК РФ) и реабилитации нацизма (ст. 354[1] УК РФ).

Использование технологии глубокого синтеза уже частично нашло свое отражение в отечественном правовом поле. Так, в соответствии с приказом Генпрокуратуры России от 09.12.2022 № 746 «О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре», в разделе «Предметы, устройства и другие средства, использованные при совершении преступлений» выделен отдельный показатель – «с использованием технологии дипфейк» (п. 049)[1]. Полагаем, такое решение об организации статистического учета за преступностью является верным и своевременным. Для принятия конкретных шагов в области изменения законодательства следует, прежде всего, иметь представление о фактической распространенности явления.

В доктрине уголовного права была обоснована необходимость самостоятельной криминализации создания и распространения реалистичных поддельных аудиовизуальных материалов. Р.И. Дремлюга предлагает установить ответственность за дипфейк в ст. 274[3] УК РФ [16, с. 277]. Не вдаваясь глубоко в содержание инициативы, следует высказать сомнение в правильности самого размещения нормы в главе 28 УК РФ. Крайне спорным также является выделение автором в качестве квалифицирующего признака – использование информационно-телекоммуникационных сетей. Вряд ли дипфейк вообще можно представить вне сетевого пространства. Полагаем, в настоящий момент можно говорить о наличии социально-правовых предпосылок к дополнению отечественной модели дифференциации уголовной ответственности новым квалифицирующим признаком – *совершение преступления с использованием технологии дипфейк.*

Обсуждение и заключение

Проведенное исследование убеждает в том, что технология глубокой подделки преимущественно используется как средство при совершении других преступлений. Подобная «инструментальная роль» технологии в механизме преступного посягательства ставит под сомнение мысль о необходимости принятия каких-либо специальных мер по самостоятельной криминализации дипфейка.

Визуализация оказывает очень серьезное воздействие на потенциального адресата ложной информации. Полагаем, совершение обманного преступления с использованием заранее изготовленного дипфейка свидетельствует о значительном увеличении общественной опасности деяния. До настоящего времени данное обстоятельство не учтено в российском законодательстве в полной мере.

Проблема неправомерного использования технологии дипфейк не имеет сугубо правового решения. Реальное противодействие предполагает выработку технологических решений оперативного выявления и удаления ложного контента, выстраивание государственно-частного партнерства в этой области, подготовку соответствующих кадров с необходимыми компетенциями. Значительную роль в преодолении синтезированного вредоносного контента могут сыграть технологии искусственного интеллекта.

СПИСОК ИСТОЧНИКОВ

1. Kugler, Matthew B. and Pace, Carly, Deepfake Privacy: Attitudes and Regulation (February 8, 2021). 116 Nw. U. L. Rev. 611 (2021)., Northwestern Public Law Research Paper. № 21-04.
2. Иванов В.Г., Игнатовский Я.Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2020. Т. 7. № 4. С. 379 – 386.
3. Красовская Н.Р., Гуляев А.А. Технологии манипуляции сознанием при использовании дипфейков как инструмента информационной войны в политической сфере // Власть. 2020. № 4. С. 93 – 98.
4. Васильева И.А., Халина Н.В. Дипфейк как технология призрачных коммуникаций // PR и реклама в изменяющемся мире: региональный аспект. 2021. № 25. С. 111 – 116.
5. Яценко Т.С. Проблемы гражданско-правового регулирования посмертного использования нематериальных благ // Журнал российского права. 2023. № 7. С. 35 – 46.

[1] Законность. 2023. № 2 (приказ).

6. Никишин В.Д. Репутационная безопасность и медиабезопасность компаний и проектов в контексте целей устойчивого развития и ESG-принципов // Актуальные проблемы российского права. 2022. № 9. С. 73 – 82.
7. Калятин В.О. Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон. 2022. № 7. С. 87 – 103.
8. Минбалеев А.В. Проблемы гражданско-правовой защиты личных неимущественных прав в процессе цифрового профилирования граждан // Гражданское право. 2022. № 2. С. 9 – 11.
9. Апостолова Н.Н. Достоверность доказательств и технологии дипфейка // Российский судья. 2023. № 11. С. 7 – 11.
10. Лаптев В.А. Deepfake и иные продукты искусственного интеллекта на пути развития онлайн-правосудия // Актуальные проблемы российского права. 2021. № 11. С. 180 – 186.
11. Батоев В.Б. Об использовании технологии «Deepfake» в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1 (61). С. 70 – 76.
12. Gilden A. Endorsing After Death // William and Mary Law Review. 2022. Vol. 63. Iss. 5. URL: https://wmlawreview.org/sites/default/files/wmlr_63-5_Gilden-pgs1531-1598.pdf (дата обращения: 11.12.2023).
13. Галяшина Е.И. Никишин В.Д., Богатырев К.М., Пфейфер Е.Г. Фейковизация как средство информационной войны в интернет-медиа: научно-практическое пособие. Москва: Блок-Принт, 2024. 144 с.
14. Lussier N. Nonconsensual deepfakes: detecting and regulating this rising threat to privacy // Idaho Law Review. 2022. Vol. 58. URL: https://digitalcommons.law.uidaho.edu/cgi/viewcontent.cgi?article=1252&context=idaho-law-review (дата обращения: 11.12.2023).
15. Harris D. Deepfakes: false pornography is here and the law cannot protect you // Duke Law & Technology Review. 2019. Vol.17. № 1. URL: https://dltr.law.duke.edu/2019/01/05/deepfakes-false-pornography-is-here-and-the-law-cannot-protect-you/ (дата обращения: 17.12.2023).
16. Дремлюга Р.И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография. Москва: Юрлитинформ, 2022. 328 с.

REFERENCES

1. Kugler, Matthew B. and Pace, Carly, Deepfake Privacy: Attitudes and Regulation (February 8, 2021). 116 Nw. U. L. Rev. 611 (2021)., Northwestern Public Law Research Paper. № 21-04.
2. Ivanov V.G., Ignatovskij Ya.R. Deepfakes: perspektivy` primeneniya v politike i ugrozy` dlya lichnosti i nacional`noj bezopasnosti // Vestnik Rossijskogo universiteta druzhby` narodov. Seriya: Gosudarstvennoe i municipal`noe upravlenie. 2020. T. 7. № 4. S. 379 – 386.
3. Krasovskaya N.R., Gulyaev A.A. Texnologii manipulyacii soznaniem pri ispol`zovanii dipfejkov kak instrumenta informacionnoj vojny` v politicheskoj sfere // Vlast`. 2020. № 4. S. 93 – 98.
4. Vasil`eva I.A., Xalina N.V. Dipfejk kak texnologiya prizrachny`x kommunikacij // PR i reklama v izmenyayushhemsya mire: regional`ny`j aspekt. 2021. № 25. S. 111 – 116.
5. Yacenko T.S. Problemy` grazhdansko-pravovogo regulirovaniya posmertnogo ispol`zovaniya nematerial`ny`x blag // Zhurnal rossijskogo prava. 2023. № 7. S. 35 – 46.
6. Nikishin V.D. Reputacionnaya bezopasnost` i mediabezopasnost` kompanij i proektov v kontekste celej ustojchivogo razvitiya i ESG-principov // Aktual`ny`e problemy` rossijskogo prava. 2022. № 9. S. 73 – 82.
7. Kalyatin V.O. Dipfejk kak pravovaya problema: novy`e ugrozy` ili novy`e vozmozhnosti? // Zakon. 2022. № 7. S. 87 – 103.
8. Minbaleev A.V. Problemy` grazhdansko-pravovoj zashhity` lichny`x neimushhestvenny`x prav v processe cifrovogo profilirovaniya grazhdan // Grazhdanskoe pravo. 2022. № 2. S. 9 – 11.
9. Apostolova N.N. Dostovernost' dokazatel'stv i tekhnologii dipfejka // Rossijskij sud'ya. 2023. № 11. S. 7 – 11.
10. Laptev V.A. Deepfake i inye produkty iskusstvennogo intellekta na puti razvitiya onlajn-pravosudiya // Aktual'nye problemy rossijskogo prava. 2021. № 11. S. 180 – 186.
11. Batoev V.B. Ob ispol'zovanii tekhnologii «Deepfake» v operativno-rozysknoj deyatel'nosti // YUridicheskaya nauka i praktika: Vestnik Nizhegorodskoj akademii MVD Rossii. 2023. № 1 (61). S. 70 – 76.
12. Gilden A. Endorsing After Death // William and Mary Law Review. 2022. Vol. 63. Iss. 5. URL: https://wmlawreview.org/sites/default/files/wmlr_63-5_Gilden-pgs1531-1598.pdf (data obrashcheniya: 11.12.2023).
13. Galyashina E.I. Nikishin V.D., Bogatyrev K.M., Pfejfer E.G. Fejkovizaciya kak sredstvo informacionnoj vojny v internet-media : nauchno-prakticheskoe posobie. Moskva: Blok-Print, 2024. 144 s.

14. Lussier N. Nonconsensual deepfakes: detecting and regulating this rising threat to privacy // Idaho Law Review. 2022. Vol. 58. URL: https://digitalcommons.law.uidaho.edu/cgi/viewcontent.cgi?article=1252&context=idaho-law-review (data obrashcheniya: 11.12.2023).
15. Harris D. Deepfakes: false pornography is here and the law cannot protect you // Duke Law & Technology Review. 2019. Vol.17. № 1. URL: https://dltr.law.duke.edu/2019/01/05/deepfakes-false-pornography-is-here-and-the-law-cannot-protect-you/ (data obrashcheniya: 17.12.2023).
16. Dremlyuga R.I. Ugolovno-pravovaya ohrana cifrovoj ekonomiki i informacionnogo obshchestva ot kiberprestupnyh posyagatel'stv: doktrina, zakon, pravoprimenenie: monografiya. Moskva: YUrlitinform, 2022. 328 s.

Информация об авторах:
Ефремова Марина Александровна, доктор юридических наук, доцент, заведующая кафедрой уголовно-правовых дисциплин Казанского филиала Российского государственного университета правосудия, crimlaw16@gmail.com
Русскевич Евгений Александрович, доктор юридических наук, доцент, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), russkevich@mail.ru, ORCID: 0000-0003-4587-8258
Авторы прочитали и одобрили окончательный вариант рукописи.

Information about the authors:
Efremova Marina A., Doctor of Law (Doctor habilitatus), Associate Professor, Head of the Department of Criminal Law Disciplines Kazan Branch of the Russian State University of Justice, crimlaw16@gmail.com, ORCID: 0000-0001-6037-6921
Russkevich Evgeny A., Doctor of Law (Doctor habilitatus), Professor of the Department of Criminal Law of the Kutafin Moscow State Law University (MSAL), russkevich@mail.ru, ORCID: 0000-0003-4587-8258
The authors have read and approved the final version of the manuscript.

Заявленный вклад авторов:
Ефремова Марина Александровна – постановка проблемы, определение объекта и методов исследования, разработка обзора литературы, уточнение выводов и рекомендаций;
Русскевич Евгений Александрович – анализ доктринально-прикладных данных, подготовка введения и результатов исследования, формирование заключения.

Статья получена: 23.02.2024.
Статья принята к публикации: 25.06.2024.
Статья опубликована онлайн: 28.06.2024.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.