DOI 10.34755/IROK.2026.30.77.049

Вердиян Г.В.
к.ю.н., профессор
ВГУЮ «РПА Минюста России»
г. Москва, Россия
Травова А.А.
магистрант кафедры «Юридическое сопровождение бизнеса»
ВГУЮ «РПА Минюста России»
г. Москва, Россия

Deepfake и дипфейки: уголовно-правовые риски генеративного ИИ в России

Аннотация. В статье рассматриваются понятие и виды дипфейков, анализируются действующие нормы УК РФ, применяемые к преступлениям с использованием генеративного ИИ, а также законопроекты 2024–2026 гг. Выявляются основные проблемы правоприменения: сложность доказывания, идентификация автора, трансграничный характер и отсутствие специального состава. Целью данного исследования является анализ различных составов преступлений, под которые и попадают преступления, совершенные с использованием генеративного ИИ, а также связанную с этим судебную практику и законопроекты. Методологическую основу исследования составляют всеобщий диалектический метод, общенаучные (описание, сравнение, обобщение, моделирование и др.) и частнонаучные методы.

Ключевые слова: дипфейк, генеративный контент, уголовное право, мошенничество, клевета, частная жизнь, законопроекты.

Verdiyan G.V.
Candidate of Legal Sciences, Professor
All-Russian State University of Justice “RPA of the Ministry of Justice of Russia”
Moscow, Russia
Travorova A.A.
Master’s student at the Department of “Legal Support of Business”
All-Russian State University of Justice “RPA of the Ministry of Justice of Russia”
Moscow, Russia

Deepfake and deepfakes: criminal law risks of generative ai in Russia

Annotation. The article examines the concept and types of deepfakes, analyzes the current norms of the Criminal Code of the Russian Federation applicable to crimes committed using generative AI, as well as legislative bills of 2024–2026. The main law enforcement problems are identified: the complexity of proof, identification of the author, cross-border nature, and the absence of a special offence. The aim of this study is to analyze various elements of crimes that cover offences committed using generative AI, as well as related judicial practice and legislative initiatives. The methodological basis of the research comprises the general dialectical method, general scientific methods (description, comparison, generalization, modeling, etc.), and specific scientific methods.

Keywords: deepfake, generative content, criminal law, fraud, defamation, privacy, legislative bills.

По информации Центра аналитики социальной инженерии и искусственного интеллекта в кибермошенничестве (ЦАСИ), с начала 2026 года количество дипфейков,

которые всё активнее используют злоумышленники, увеличилось вдвое по сравнению с аналогичным периодом 2025 года [1].

Термин дипфейк в современном правовом и научном дискурсе означает - цифровой продукт в виде текста, графики, звука или их сочетания, сгенерированный полностью или частично при помощи нейросетевых технологий, используемый для целей введения в заблуждение или преодоления пользователем систем контроля и управления доступом [2].

В основе дипфейка (название происходит от слов «deep learning», т. е. «глубокое изучение» и «fake», т. е. «подделка») – нейросеть, которая детально изучает лицо человека, а затем подставляет к исходному файлу лицо «реципиента», т. е. с максимальной реалистичностью «оживляет» изображение человека и заставляет его говорить и делать то, чего он не делал и не говорил [3].

То есть, обобщая все вышесказанное, дипфейк – это различный синтезированный с помощью алгоритмов глубокого изучения контент, (видео, аудио-изображения), основанный с помощью генеративных состязательных моделей (далее – GAN) и вариационных автокодировщиков (далее – VAE), который выглядит и звучит крайне реалистично и может быть даже неотличим от действительности.

Чтобы понимать механизмы создания таких подделок и их уязвимости, представляется необходимым кратко описать ключевые технологии, которые используются для создания дипфейков.

1. GAN – это два нейросетевых модуля (генератор и дискриминатор), которые соревнуются друг с другом: генератор создаёт подделку, дискриминатор пытается её распознать. В результате такого состязания качество синтезированного контента постоянно повышается.
2. VAE и автокодировщики – используются для выделения и реконструкции ключевых параметров лица, мимики, голоса, позволяя сжимать и восстанавливать характерные признаки с высокой точностью.
3. Общий процесс – это алгоритм, который выделяет характерные черты (очертания лица, интонации, микродвижения), а затем накладывает их на другой источник, создавая синтезированное изображение или звук.

Существует множество разновидностей дипфейков, но более целесообразным видится разобрать самые основные категории, первой из которых является категория «визуальные подделки». Они используют такие техники как: замену лица, оживление мимики, синтез полностью нового лица и локальное редактирование лица.

Следующая категория – это аудиоподделки. Клонирование голоса, синтез речи по тексту, редактирование аудио – все это основные способы создания данного вида дипфейков.

Также, можно выделить последнюю категорию (комбинированное использование), которая включает в себя точное совмещение движений губ в видео с синтезированной аудиодорожкой.

Для целей уголовно-правового анализа наиболее значима классификация по тем противоправным действиям, в которых дипфейки задействуются чаще всего.

1. Мошенничество. По состоянию на ноябрь 2025 года, согласно исследованию сервиса «RWB исследования» объединённой компании Wildberries и Russ, каждый десятый житель России лично сталкивался с попытками мошенничества на основе дипфейков [4]. Чаще всего мошенники действуют следующим способом: они подделывают голос или видео знакомого или родственника, с целю получить конфиденциальные данные или заставить совершить денежный перевод.

Так, по данным в России, за пять месяцев этого года мошенники обманули таким способом четыре тысячи человек. Ущерб оценивается в 21 миллиард рублей, а средний «чек» составил 16 миллионов.

В Китае же в 2024 году сотрудник гонконгской компании перевел 225 миллионов долларов США со счета компании мошеннику. Мошенник сделал с ним видеосвязь от

имени финансового директора и попросил его осуществить перевод. Во время видеосвязи сотрудник видел не только «финансового директора», но и других «коллег».

2. Клевета и посягательство на честь, достоинство, деловую репутацию. Лицо жертвы вставляют в компрометирующие видео или фото (порнографические или скандальные) и распространяют с целью опорочить. Это особо опасный вид дипфейков, носящий не только вымогательский характер, но и гендерно окрашенный: в подавляющем большинстве случаев жертвами становятся именно женщины.

Использование дипфейков для помещения лиц женщин в порнографические материалы, что считается формой цифрового насилия, при которой реальные фотографии жертв используются для создания поддельных интимных изображений без их согласия. По данным ООН, такие материалы составляют около 98% всех дипфейков, и в 99% случаев их целями становятся женщины и девочки [5].

Так, в России, наиболее распространенным сценарием является, когда бывшие партнеры, чтобы оказать давление на женщину, угрожают выложить или публикуют созданные с помощью ИИ порнографические фото или видео. В 2023–2024 годах в сети фиксировались десятки таких случаев, когда злоумышленники использовали боты для замены лиц в Telegram.

В Китае недавний прецедент: Центральный суд Ханчжоу рассмотрел дело о защите общественных интересов, связанное с использованием технологии «изменения лица» для создания поддельных видео с подтверждением в реальном времени. Фигуранты Чжан и Ван получали номера телефонов, фото аватаров и идентификационные данные из зарубежных соцсетей, затем с помощью ИИ создавали поддельные видео и осуществляли несанкционированный вход на торговые платформы, похищая адреса доставки и информацию о корзинах покупок [6].

3. Политическая дезинформация и манипуляция общественным мнением. Данный метод подразумевает создание фальшивых видео с выступлениями политиков и их ложными заявлениями или объявлениями об отставке, чтобы повлиять на выборы или общественное мнение.

В июне 2023 года Россия стала жертвой подобной операции. Хакеры взломали трансляции в нескольких регионах РФ (в особенности приграничных с Украиной) и пустили в эфир поддельное экстренное обращение президента Владимира Путина. «Путин» объявил, что украинские войска при поддержке НАТО вторглись в Брянскую, Белгородскую и Курскую области. Поддельный лидер декларировал введение военного положения, всеобщую мобилизацию и призывал население к эвакуации вглубь страны [7].

В КНР в 2025 году гражданин Го Моухэн сфабриковал и распространил в интернете слух о том, что «клиент был забит камнями до смерти в отеле в Уланчабе». Расследование отдела интернет-безопасности показало, что Го безуспешно пытался договориться с отелем о компенсации и, не добившись своего, разместил ложное сообщение на короткой видеоплатформе, введя в заблуждение большое количество пользователей и нарушив общественный порядок [8].

Все вышеперечисленные типы злоупотреблений дипфейками затрагивают различные составы уголовных преступлений, что и будет рассмотрено далее.

На сегодняшний день одним из наиболее распространённых способом использования дипфейков в преступных целях является мошенничество (ст. 159 УК РФ). В этом случае синтезированное видео или аудиообращение выступает не самостоятельным составом преступления, а способом хищения чужого имущества или приобретения права на него путём обмана или злоупотребления доверием.

В российском праве квалификация по ст. 159 УК РФ зависит от размера причинённого ущерба. Часть 2 (мошенничество с причинением значительного ущерба гражданину), часть 3 (крупный размер – свыше 250 тыс. рублей), часть 4 (особо крупный размер – свыше 1 млн рублей) предусматривают, соответственно, более строгое наказание. В случаях с дипфейками, как правило, речь идёт о крупных и особо крупных суммах.

Ключевой правовой вопрос при квалификации таких деяний: необходимо ли доказывать, что потерпевший был введён в заблуждение именно дипфейком, а не иными обстоятельствами (например, общей доверчивостью или невнимательностью). На практике для признания состава мошенничества достаточно установить причинно-следственную связь между использованием поддельного контента и передачей имущества. Однако сторона защиты часто ссылается на то, что потерпевший мог бы распознать подделку при должной осмотрительности, что осложняет доказывание умысла.

Также, одним из способов использования дипфейков в действиях преступного характера является клевета (ст. 128.1 УК РФ). То есть, дипфейк используется для создания и распространения заведомо ложных сведений, порочащих честь, достоинство и деловую репутацию. Обязательный признак данного состава преступления – это прямой умысел, то есть лицо должно в полной мере осознавать, что распространяемые сведения являются ложными. Так, например, впервые в России был вынесен судебный приговор по делу о порнодипфейках. Гражданина Липчанина, чьё имя скрыто в картотеке суда, признали виновным в изготовлении и распространении порнографических материалов в интернете (п. «б» ч. 3 ст. 242 УК РФ, до шести лет лишения свободы) и распространении там же сведений, порочащих честь и достоинство (ч. 2 ст. 128.1 УК РФ, до двух лет лишения свободы).

Данная статья состоит из нескольких частей, каждая последующая предусматривает более строгую ответственность при наличии отягчающих признаков. Базовый состав влечёт штраф до 500 тыс. руб. либо обязательные работы до 160 часов. Квалифицированные составы (публичная клевета, в отношении нескольких лиц, с использованием служебного положения или о наличии опасного заболевания) караются штрафом до 2 млн руб. и лишением свободы до 4 лет. Наиболее строгое наказание – до 5 лет лишения свободы – предусмотрено за клевету, соединённую с обвинением лица в совершении тяжкого, особо тяжкого преступления либо преступления против половой неприкосновенности.

Ключевой момент для квалификации содеянного как клеветы, заключается в том, что необходимо доказать наличие умысла на распространение сведений, порочащих честь и достоинство личности, а также то, что совершен он с использованием технологии дипфейка. Именно здесь возникает истинная проблема, так как он выглядит как подлинное аудио или видео, поэтому может восприниматься как реальный факт. Следовательно, в суде нужно не только установить факт создания дипфейка, но и доказать, что нарушитель в полной мере осознавал искусственность распространяемого контента.

Также дипфейки используются для собирания и распространения сведений о частной жизни лица без его согласия, что попадает под действия 137 статьи УК РФ. Всего статья состоит из трех частей, квалифицированный состав (с использованием служебного положения) влечёт наказание до 4 лет лишения свободы, а распространение информации о несовершеннолетнем потерпевшем с причинением тяжких последствий – до 5 лет.

Ключевой момент для квалификации преступления по этой статье является согласие. Ответственность по ст. 137 УК РФ наступает, только если человек не давал разрешения на использование и распространение изображения, а само это изображение на момент создания или публикации составляло его личную тайну. Если же снимок уже был в открытом доступе (например, человек сам его опубликовал), или его распространение оправдано публичными интересами, или есть другое законное основание, то состава преступления нет.

Если в основе такого дипфейка лежит фото человека из частной, закрытой от посторонних сферы жизни, и человек не давал согласия на его использование, то действия того, кто создал подделку подпадают под ст. 137 УК РФ. То есть, дипфейк здесь рассматривается не как самостоятельный состав, а лишь как способ незаконного использования уже существующего, защищаемого изображения.

Практика применения перечисленных статей выявила ряд пробелов, которые законодатель попытался устранить несколькими законопроектами, внесёнными в 2024–2026 годах. Рассмотрим их последовательно.

1. Законопроект №718538-8 (сентябрь 2024 г.).

Был внесен 16 сентября 2024 года и предлагал дополнить в статьи 128.1 («Клевета»), 158 («Кража»), 159 («Мошенничество»), 159.6 («Мошенничество в сфере компьютерной информации»), 163 («Вымогательство») и 165 («Причинение имущественного ущерба путём обмана или злоупотребления доверием») УК РФ новый квалифицирующий признак – «совершение преступления с использованием изображения или голоса человека, а также его биометрических данных» [9].

Позиция Верховного суда: в законопроекте отсутствует мотивированное обоснование, подкреплённое убедительными данными о недостаточности действующего правового регулирования, а также специальными исследованиями, подтверждающими необходимость введения новых норм, ужесточающих уголовную ответственность [10].

Позиция Правительства: Правительство также отметило, что пояснительная записка к законопроекту не содержит статистических и иных данных, свидетельствующих об общественной опасности криминализируемых деяний

Также является важным отметить тот факт, что в 2023 году Правительство РФ отклонила вынесенное предложение о создании отдельной статьи за дипфейки, и указало, что незаконное распространение персональных данных с использованием ИИ уже подпадает под ст. 137 УК РФ.

2. Введение ст. 272.1 УК РФ (ноябрь 2024 г.)

30 ноября 2024 года в УК РФ введена ст. 272.1 («Незаконные использование и (или) передача (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации»). Пункт 2 этой статьи предусматривает ответственность за действия в отношении компьютерной информации, содержащей биометрические персональные данные. На сегодняшний день – это единственное специальное положение в российском законодательстве, прямо касающееся биометрии.

3. Законопроект №1133088-8 (январь 2026 г.)

Авторы законопроекта предлагали включить в ст. 272.1 УК РФ «автоматизированную обработку» биометрических данных как самостоятельный состав преступления – чтобы наказывать уже за сам факт машинной обработки чужих персональных данных, даже без их последующего использования [11]. Инициатива была призвана устранить пробел, связанный с созданием дипфейков. Однако в феврале 2026 года законопроект вернули инициаторам по процедурным основаниям, и он не был принят.

4. Законопроект №1288702-8 (июль 2026 г.)

Авторы инициативы предлагают дополнить ст. 63 УК РФ (общие начала назначения наказания) новым отягчающим обстоятельством – совершение преступления с использованием сгенерированных ИИ аудиовизуальных материалов [12].

Позиция Правительства РФ: в официальных отзывах от 22 июля 2024 г. и 22 августа 2025 г. были высказаны замечания, которые, по словам вице-премьера Дмитрия Григоренко, остаются актуальными. Позиция Правительства не изменилась.

Исходя из всего вышесказанного, мы можем выделить множество проблем, которые возникают при попытке доказать, что правонарушение было совершено именно при помощи дипфейка.

В самом начале правоприменитель сталкивается со сложностью доказывания. Например, для выявления дипфейка требуется дорогостоящая видеотехническая экспертиза, стоимость которой может составлять 90 000 рублей и выше [13]. Далее возникают процессуальные проблемы. В УК РФ вообще не закреплены такие термины, как «электронные доказательства», «электронный документ», «электронный носитель информации» [14]. Из-за этого возникает путаница: например, суды по-разному оценивают, относится ли мобильный телефон к электронным носителям, или можно ли признать

скриншотом переписки вещественным доказательством. Также необходимо доказывать, что лицо знало о ложности распространяемых сведений или о том, что использует именно дипфейк, а не подлинную запись.

Для правильного назначения меры наказания необходимо правильно идентифицировать личность нарушителя, был ли это один человек или правонарушение было совершено группой лиц. Использование VPN, анонимайзеров и зарубежных платформ позволяет злоумышленникам действовать анонимно, а сама технология не оставляет прямых следов авторства, что порождает вопрос о субъекте ответственности. Кто им является: разработчик ИИ, хостинг-платформа или конечный пользователь. Ситуация усугубляется трансграничным характером таких преступлений: дипфейк может быть создан в одной стране, размещён на сервере в другой, а вред причинён в третьей, при этом эффективные механизмы международного сотрудничества, в связи с сложившейся политической ситуацией в мире, на данный момент в РФ значительно затруднены, а различия в национальных подходах к регулированию ИИ делают сложным взаимную правовую помощь. Кроме того, в УК РФ отсутствует специальный состав за создание или использование дипфейков, и квалификация осуществляется по общим статьям, что не всегда позволяет учесть специфику деяния; как справедливо отмечает доктор юридических наук И.С. Алихаджиева, «уголовно-правовая реакция законодателя на новые способы совершения преступлений с помощью технологии дипфейк будет запоздалой» [15], а законодательные инициативы пока не находят поддержки Правительства РФ.

Кроме того, требуется ряд системных изменений в российском законодательстве:

1. нормативное закрепление термина «дипфейк» и его определение с учётом технологических возможностей и рисков;
2. внесение дополнений в Уголовный кодекс и Кодекс об административных правонарушениях, связанных с применением дипфейк-контента в качестве предмета противоправного посягательства, элемента способа совершения правонарушения либо обстоятельства, отягчающего ответственность (дипфейк представляет собой более изощрённый высокотехнологичный продукт, обладающий высоким уровнем общественной опасности и трудно распознаваемый на современном уровне развития криминалистической техники);
3. внесение дополнений в Гражданский кодекс, в частности в части защиты чести, достоинства и деловой репутации, а также охраны изображения гражданина (ст. 152 и 152.1 ГК РФ);
4. разработка профильного законодательства о системах искусственного интеллекта, робототехники, виртуальной реальности и больших данных, которое бы комплексно регулировало общественные отношения в этой сфере.

Анализ действующего российского уголовного законодательства и законопроектной деятельности показывает, что, несмотря на наличие отдельных норм, позволяющих привлекать к ответственности за использование дипфейков, системного подхода к регулированию этой сферы пока не сложилось. А предложенные в статье меры – направлены на создание сбалансированного механизма. Главное – найти золотую середину между безопасностью и свободой. Технологии уже стали частью реальности, и право должно эволюционировать вместе с ними.

Список источников

1. Количество дипфейков в России выросло вдвое с начала года // РБК URL: https://www.rbc.ru/rbcfreenews/6a2827219a79471b9a70392f (дата обращения: 25.07.2026).
2. Бодров Н.Ф., Лебедева А.К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования.- 2023.- №11.- С. 26-41.

3. Киселёв А.С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Московский юридический журнал.- 2021.- №3.- С. 54-64

4. Каждый десятый россиянин сталкивался с попытками дипфейк-мошенничества // ТАСС URL: https://tass.ru/obschestvo/25841977 (дата обращения: 25.07.2026).

5. When justice fails: Why women can’t get protection from AI deepfake abuse // UN News URL: https://news.un.org/en/story/2026/03/1167174 (дата обращения: 25.07.2026).

6. The Hangzhou Central Court heard a public interest litigation case involving the protection of personal information related to “AI face-changing” // Baijiahao (Baidu) URL: https://baijiahao.baidu.com/s?id=1842400719968497801&wfr=spider&for=pc (дата обращения: 25.07.2026). (на китайском)

7. Дипфейки в политике: Восточная Европа, Китай, Индия // Azbuka Media URL: https://azbukamedia.com/dipfejki-v-politike-2/#i (дата обращения: 25.07.2026).

8. Shao Lei. The Ministry of Public Security announced eight typical cases of online rumors related to police situation and public policy//Ministry of Public Security of the People's Republic of China : [официальный сайт]. – URL: https://www.mps.gov.cn/n2254098/n4904352/c10208563/content.html (дата обращения: 25.07.2026). (на китайском)

9. Проект федерального закона № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности)» // Система обеспечения законодательной деятельности URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 25.07.2026).

10. Официальный отзыв на проект федерального закона № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» : письмо Верховного Суда Российской Федерации от 20 июня 2024 г. № 4-ВС-2774/24. – Текст : электронный // СПС «Гарант». – URL: https://base.garant.ru/76869957/ (дата обращения: 25.07.2026).

11. Уголовный кодекс предлагают дополнить нормами об использовании дипфейков // РАПСИ URL: https://rapsinews.ru/legislation_news/20240916/310242023.html (дата обращения: 25.07.2026).

12. Проект федерального закона № 1288702-8 «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации» // Система обеспечения законодательной деятельности URL: https://sozd.duma.gov.ru/bill/1288702-8 (дата обращения: 25.07.2026).

13. Экспертиза видеозаписей на предмет выявления дипфейков: методология, инструменты и практическая реализация // Федерация судебных экспертов URL: https://bneks.ru/ekspertiza-ideozapisej-na-predmet-vyyavleniya-dipfejkov-metodologiya-instrumenty-i-prakticheskaya-realizatsiya/ (дата обращения: 25.07.2026).

14. Андреева Ю.И. Электронные доказательства в уголовном процессе // Закон и право.- 2025.- №8.- С. 147-152.

15. Алихаждиева И.С. Перспективы установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности (законопроект № 718538-8) // Известия Юго-Западного государственного университета. Серия: История и право.- 2025.- Т.15, №2.- С. 154-171.