УДК 343.41 Вестник СПбГУ. Право. 2025. Т. 16. Вып. 1

Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования

И. Н. Мосечкин

Вятский государственный университет,
Российская Федерация, 610000, Киров, ул. Московская, 36

Для цитирования: Мосечкин, И. Н. 2025. «Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования». *Вестник Санкт-Петербургского университета. Право* 1: 95–110. https://doi.org/10.21638/spbu14.2025.107

В статье исследуется целесообразность корректировки отечественного уголовного законодательства в части защиты лиц от фальсификации их биометрических персональных данных посредством использования систем искусственного интеллекта. Актуальность темы объясняется доступностью дипфейк-технологий, позволяющих быстро и реалистично создавать цифровые копии людей, а также распространенностью использования биометрических данных в повседневной жизни: при осуществлении покупок, подтверждении личности и проходе на охраняемые объекты. Появление новых компьютерных технологий обострило угрозу использования образа другого человека при совершении противоправных деяний. Первые случаи хищений с применением поддельных биометрических данных уже зафиксированы в Китае и Объединенных Арабских Эмиратах. Автор анализирует положения отечественного и зарубежного уголовного законодательства, что позволяет установить некоторые недостатки правового противодействия злонамеренной фальсификации внешности и голоса человека. Подчеркивается, что дипфейк-технологии — не единственный способ фальсификации, а их назначение не является строго криминальным, поэтому необходимо поставить вопрос о защите биометрических данных в целом. Аргументированно изложена позиция о недостаточности охранительного потенциала гражданского и административного права. Автор приводит доказательства того, что подделка внешности, голоса, папиллярных узоров пальцев и геномной информации несет большую общественную опасность, если осуществляется с целью скрыть другое преступление или облегчить его совершение. Обосновывается допустимость уголовно-правового запрета, имеющего сходства с положениями ст. 327 Уголовного кодекса РФ и нормами штата Массачусетс. В результате исследования сформулирована редакция соответствующей статьи, которая может быть использована как рекомендация при совершенствовании законодательства.

Ключевые слова: дипфейк, подделка, цифровая копия, фальсификация, биометрические данные, голос, лицо.

1. Введение

Появление систем искусственного интеллекта предоставило возможность выполнять различные задачи быстрее, качественнее и без прямого участия человека. Использование первых систем требовало особых знаний и навыков, однако впоследствии технический порог был существенно снижен, что позволило оперировать

© Санкт-Петербургский государственный университет, 2025

отдельными программами практически любому человеку с собственного смартфона. То, что ранее требовало месяцев подготовки, сейчас осуществляется нажатием пары кнопок.

Указанное привело не только к положительным изменениям в общественной жизни, отрицать которые невозможно, но и к негативным последствиям: нейросетевое программное обеспечение стало применяться при совершении мошенничеств, правонарушений экстремистской и террористической направленности, изготовлении порнографических материалов, а также распространении порочащей информации. Законодатель, в свою очередь, не всегда оперативно реагирует на данные преобразования, и это общемировая, а не исключительно отечественная тенденция.

В свете изложенного обратим внимание на повсеместное распространение технологий, позволяющих создавать (по существу, подделывать) изображения человека, неотличимые от оригинальных, а также синтезировать голос или иные звуки. Благодаря системам искусственного интеллекта процесс фальсификации существенно ускорился. В широкое употребление вошел термин «дипфейк» (*англ.* deepfake, от deep — «глубокий» и fake — «фальшивый»). Этот термин объединяет алгоритмы, обеспечивающие крайне реалистичную замену на изображении одного человека на другого, синхронизацию губ, а также синтез голоса. В содержание указанного выше понятия входит и результат применения технологий (т. е. изображение, видеозапись или звук). В настоящей работе в целях единообразия для наименования нейросетевого способа фальсификации в дальнейшем будет использоваться словесная конструкция «дипфейк-технологии».

Первый широко известный случай их применения связывается с публикацией в интернете изображений порнографического характера в 2017 г. Для их изготовления были заимствованы образы женщин, популярным благодаря ролям в художественных произведениях (Flynn, Clough, Cooke 2021, 584). С тех пор одна частная инициатива превратилась в неконтролируемый поток фальсифицированной продукции, производимой в совершенно различных целях. Например, ученые создали реалистичный видеоролик с участием Барака Обамы на основе других видеозаписей, а также синтезировали голос Джона Кеннеди (Delfino 2020, 889). Приложение ZaoApp, позволяющее убедительно заменять лица персонажей, в 2019 г. стало самым загружаемым в Китае всего лишь за три дня, что привело к появлению массы коротких видеороликов. Приводить примеры можно практически бесконечно. Соответствующие программы стали общедоступными и более совершенными, с каждым годом спектр их возможностей расширяется.

К сожалению, распространение дипфейк-технологий привело к угрозам массовой публикации фальсифицированной продукции, содержащей клеветническую информацию (например, демонстрация не соответствующих действительности получения взятки должностным лицом или участия в убийстве), а также рискам использования чужих внешности или голоса для совершения мошеннических или иных противоправных действий. По мнению зарубежных исследователей, фальсифицированная информация станет мощнейшим инструментом для дезинформации масс и оказания влияния на политические процессы, будет использоваться при проведении компьютеризированных специальных операций (Whyte 2020, 200).

Сами по себе дипфейк-технологии не являются абсолютным злом. Проблема использования чужой внешности (в законодательстве стран англосаксонской

правовой семьи подобное часто именуется кражей личности) существовала и до их возникновения. В то же время никогда прежде процесс замены лиц и синтезирования голоса не был таким простым, а цифровизация деятельности человека — повсеместной. С учетом технологических и общественных изменений, а также рисков расширения круга преступных деяний, осложненных использованием нейросетей, считаем необходимым изучение целесообразности применения мер уголовно-правового характера для защиты прав и свобод человека и гражданина от названных посягательств.

2. Основное исследование

Дипфейк-технологии представляют собой совокупность алгоритмов систем искусственного интеллекта, которые после проведенного глубокого обучения, как правило, заменяют одно изображение или звук другим. В итоговом результате тяжело заметить фальсификацию без применения специальных программ или наличия знаний в этой сфере. Обычно используются два распространенных способа (Mullen 2022, 213).

Первый способ основывается на использовании генеративно-состязательных сетей. Одна из них создает продукт (изображение, звук) по задаваемым параметрам, а вторая оценивает его. Генеративно-состязательные сети корректируют продукт до тех пор, пока не исчезнут значительные различия между входным изображением или звуком и итоговым результатом.

Другой способ предполагает использование вариационных автокодировщиков — двух сетей, позволяющих распознавать определенные изображения и звуки, создавать новые, а затем сравнивать с необходимым результатом. Получившийся продукт поддается корректировке. Так, изображение может быть отредактировано для изменения поз или освещения. После обучения сетей выходные данные кодировщиков объединяются и получается итоговый продукт.

Для неспециалиста в области компьютерных технологий принципиально важно, что окончательный результат — реалистичные изображение, видеозапись или голос — внешне неотличимы от оригиналов. При этом открывается широкий простор для совершенствования противоправной деятельности, появления новых способов преступлений и ухода от ответственности. Полагаем, в данном контексте следует задаться вопросом: достаточно ли существующих норм для охраны прав и свобод человека от злонамеренного использования дипфейк-технологий?

Действующее уголовное законодательство обладает определенным потенциалом в борьбе с неправомерной фальсификацией изображений и звуков. Если имеется содержание, порочащее честь или достоинство другого лица, распространение подобного произведения может быть квалифицировано по ст. 128[1] Уголовного кодекса РФ от 13.06.1996 № 63-ФЗ[1] (УК) «Клевета». В случае направления в правоохранительные органы фальсифицированной информации о совершении преступления не исключается квалификация по ст. 306 УК «Заведомо ложный донос». В последнее время увеличилось количество видеороликов и изображений, направленных на создание негативного отношения к России в целом, Вооруженным

[1] Здесь и далее (если не указано иное) все ссылки на российские нормативно-правовые акты приводятся по СПС «КонсультантПлюс». Дата обращения 10 марта, 2025. http://www.consultant.ru.

Силам РФ, государственным органам и должностным лицам. Законодатель своевременно отреагировал на данные случаи организованной диффамации, включив в УК ст. 207^3 (один из квалифицирующих признаков которой предусматривает искусственное создание доказательств) и ст. 280^3. В зависимости от содержания фальсифицированных сведений возможно применение норм об ответственности за оборот порнографических материалов, материалов экстремистского или террористического характера, а также распространение заведомо ложной информации (например, ст. 207^1 и 207^2 УК).

Значительная доля противоправной деятельности связана с корыстными целями и корыстной мотивацией, поэтому нет ничего удивительного в том, что дипфейк-технологии становятся частью механизма хищений. Благодаря наличию образцов голоса и внешности, в изобилии имеющихся в интернете, преступники создают фальшивые изображения и записи для совершения мошенничества. Так, известность получило хищение денежных средств в сумме $ 35 млн из банка Объединенных Арабских Эмиратов. Организованная группа, используя системы искусственного интеллекта, синтезировала голос руководителя организации-клиента. От лица руководителя банка мошенники совершили звонок, в ходе которого сообщили о намерении перечислить денежные средства на указанный ими счет. Сотрудник банка не распознал фальсификацию голоса, поэтому согласился исполнить операцию. Денежные средства были похищены и распределены на множество других счетов (Rancourt-Raymond, Smaili 2023).

Кроме того, ущерб в сумме $ 25,6 млн был причинен международной организации, зарегистрированной в Гонконге. Работник финансового отдела организации получил приглашение для участия в видеоконференции, в которой задействовали фальсифицированный образ директора и топ-менеджеров. Для подготовки была осуществлена предварительная рассылка электронных сообщений. В ходе конференции работнику отдали команду срочно перевести денежные средства организации на пять местных банковских счетов. По итогам расследования было установлено, что виновные лица неоднократно задействовали фальсифицированные образы для обмана систем распознавания лиц[2].

Без сомнения, злонамеренные манипуляции с чужими голосом и внешностью при совершении мошенничества и иных хищений получат еще большее распространение. Более того, учитывая повсеместное внедрение в предпринимательстве дистанционных форм общения, полагаем возможным спрогнозировать противоправное использование образа руководителя организации при незаконном получении кредита, сведений, составляющих коммерческую, налоговую или банковскую тайну, и осуществлении ряда иных экономических преступлений.

Несмотря на наличие уголовных норм, применение которых возможно по отношению к высокотехнологичным преступлениям, все же считаем возможным согласиться с тем, что юридическая оценка злонамеренного взаимодействия с фальсифицированными внешностью и голосом весьма затруднительна. Часть составов преступлений попросту не учитывает психологические страдания потерпевшего, образ которого использовали в противоправных целях (Добробаба 2022, 115). Кроме того, в целом правовой ответ на случаи использования дипфейк-технологий

[2] «Украли 25 миллионов долларов, подделав лица на видео». *Комсомольская правда*. 2024. Дата обращения 10 марта, 2025. https://www.kp.ru/daily/27562/4887701/?ysclid=lsac8uk0ov844690571.

весьма фрагментарен. Применению подлежат нормы, предусматривающие ответственность за совершение традиционных преступлений: клеветы, мошенничества, заведомо ложного доноса и др. Их формулировка не позволяет охватить все возможные ситуации. Так, в 2023 г. голоса актеров озвучивания и дубляжа синтезировали и использовали без их согласия в различных сферах деятельности. Во-первых, осуществлялась продажа озвучивания за плату без согласия человека. Во-вторых, результаты синтеза распространились в интернете настолько, что их стали использовать бесконтрольно. Например, голосом известной актрисы была озвучена реклама материалов эротического и порнографического характера; голос другого человека использовали при подготовке видеороликов, содержащих информацию, осуждающую проведение специальной военной операции на Украине (Мардиева 2023, 241–242). Представить подобное еще десять лет назад было бы сложно.

Общественная опасность задействования поддельных внешности или голоса для вражеской пропаганды или изготовления порнографических материалов очевидна. Однако квалификация названных действий по какой-либо статье УК или спорна, или невозможна. Полагаем, наиболее соответствует обстоятельствам состав клеветы, о чем говорят и другие ученые (Перина 2023, 101). В то же время для квалификации по ст. 128[1] УК требуется распространение не только ложных, но и порочащих честь и достоинство, подрывающих репутацию лица сведений. Не во всех случаях использование голоса для озвучивания рекламы без разрешения обладателя нанесет ущерб чести, достоинству или репутации.

Кроме того, специфика способа и средств осуществления противоправных деяний не учитываются должным образом, не в полной мере дифференцируется ответственность при использовании систем искусственного интеллекта, а также фальсифицированных изображений и звуков. Изучение изменений в законодательстве говорит о том, что появление или чрезмерное распространение новых разновидностей отдельных преступлений уже приводило к необходимости пересмотра подходов к уголовно-правовому регулированию. В частности, неслучайно (хотя и весьма критикуемо) появление п. «г» ч. 3 ст. 158 УК. Введение квалифицирующего признака связывалось с наличием познаний в области цифровых технологий и повышенной общественной опасностью хищений электронных денежных средств. Со временем именно хищение с банковского счета стало типичным, но п. «г» ч. 3 ст. 158 УК пересмотру не подвергался. Совершение же других преступлений с помощью технологически фальсифицированных изображений и голоса пока не повлекло существенных законодательных изменений. В научной литературе справедливо замечалось: «Использование голоса и лица человека позволяет преступникам понизить уровень защищенности населения перед угрозой подмены их фото- и видеоизображений при незаконном получении кредитов, переоформлении недвижимости, дискредитации любого юридического и физического лица» (Архипцев, Сарычев 2022, 349).

Для противодействия злонамеренному использованию фальсифицированных изображений и звуков, а также для защиты прав и свобод граждан в теории уголовного права предлагается несколько подходов к изменению законодательства. Почти все они объединяются в три основные группы: криминализация отдельных явлений; добавление квалифицирующих или конститутивных признаков в уже существующие составы; расширение перечня обстоятельств, отягчающих наказание.

Встречается, например, рекомендация о включении в УК специальной нормы, предусматривающей ответственность за «создание и распространение дипфейков при отсутствии согласия обладателя внешности и голоса» (Першина 2021, 232). В некоторых странах действительно пошли по пути криминализации использования технологий синтеза, и ответственность устанавливается в зависимости от ряда существенно различающихся обстоятельств.

Так, в США принято несколько нормативных актов, предусматривающих уголовную ответственность за различного рода взаимодействие с дипфейк-технологиями. На федеральном уровне Сенат принял Закон о запрете вредоносных дипфейков[3] и Закон об ответственности за дипфейки[4], запрещающие создание и распространение фальсифицированных произведений в преступных или вредоносных целях. Кроме того, наказуемыми признаются создание и распространение фальсифицированных записей о личности, если они имеют унизительный и сексуальный характер или провоцируют насилие, вооруженный или дипломатический конфликт, а также создают помехи в проведении официального разбирательства. Неправомерны создание и распространение фальсифицированных записей о личности в целях совершения преступлений и вмешательства в избирательный процесс. Кроме уголовных мер, предусматриваются и иные (Liu, Zhang 2022).

На уровне штатов в США приняты поправки, позволяющие привлекать к уголовной ответственности за использование дипфейк-технологий. Так, в штате Вирджиния наказуем синтез для изготовления порнографии без согласия обладателя внешности или голоса[5]. Сенат штата Техас одобрил законопроект № 751, согласно которому противоправным является использование фальсифицированных произведений в избирательном процессе[6]. Наиболее широкая формулировка применяется в законопроекте, находящемся на рассмотрении в штате Массачусетс[7]: запрещается использовать дипфейк-технологии для облегчения совершения преступления или правонарушения (Mullen 2022, 226).

Региональному законодательству США давно известно такое традиционное преступление, как кража личности, которая вполне может осуществляться при помощи технологий синтеза (Okolie 2023, 6). Противоправное деяние заключается в использовании чужих персональных данных, выдаче себя за другое лицо или предъявлении документов другого лица, совершаемых, как правило, для извлечения материальной выгоды. Казуистичный характер регулирующих статей не всегда позволял охватить кражу личности с применением дипфейк-технологий, что обусловило необходимость принятия отдельных поправок.

В законодательстве Китайской Народной Республики (КНР) вместо понятия «дипфейк» используется словосочетание «технологии глубокого синтеза». Принятие поправок в нормативные акты позволило распространить действие уголовных

[3] Malicious Deep Fake Prohibition Act of 2018 S.3805 dated December 21, 2018. Дата обращения 10 марта, 2025. https://www.congress.gov/bill/115th-congress/senate-bill/3805/all-actions.

[4] Deep Fakes Accountability Act H. R.5586 dated September 20, 2023. Дата обращения 10 марта, 2025. https://www.congress.gov/bill/118th-congress/house-bill/5586/text.

[5] Code of Virginia dated February 1, 1950. Дата обращения 10 марта, 2025. https://www.lawserver.com/law/state/virginia/va-code/virginia_code_18-2-386-2.

[6] Texas Senate Bill 751. Дата обращения 10 марта, 2025. https://legiscan.com/TX/text/SB751/id/2686191.

[7] MA H72. Дата обращения 10 марта, 2025. https://www.billtrack50.com/billdetail/1603340.

положений на случаи фальсификации внешности и голоса людей. В частности, запрещается публикация обработанных с помощью технологии глубокого синтеза изображений, видеороликов и аудиозаписей без соответствующей маркировки или для создания не соответствующих действительности новостей (Geng 2023, 169).

Предложения по установлению в отечественном уголовном законодательстве запретов во многом обусловлены опасениями причинения какого-либо вреда при распространении фальсифицированных изображений и звуков. Однако дипфейк-технологии — всего лишь один из инструментов, позволяющих производить указанный продукт. До появления искусственного интеллекта и компьютерных программ неоднократно производились подделки фотографий или документов. Дипфейк-технологии ускорили процесс и вывели его на новый уровень, однако достаточной степени реалистичности можно добиться и без них. Если выйти за пределы обсуждения цифровой среды, то следует упомянуть существование реалистичных силиконовых масок, высокое качество исполнения которых затрудняет или делает почти невозможным осознание того, что под искусственным лицом спрятан другой человек (Еремченко 2017, 196). Несомненно, в будущем появятся другие способы и другие материалы. С учетом развития технологий представляется возможным спрогнозировать создание программ, не заменяющих лица, тела и звуки, а формирующих их с нуля по задаваемым пользователями параметрам. Исходный результат рано или поздно совпадет с внешностью или голосом какого-либо человека. Таким образом, сегодня фальсификация внешности и голоса способна причинить вред общественным отношениям независимо от того, каким образом была осуществлена, поэтому запрет создания и распространения именно дипфейков видится нам нецелесообразным.

Ученые-правоведы аргументируют важность закрепления в качестве конструктивных или квалифицирующих таких признаков, как использование информационно-телекоммуникационных сетей, в том числе сети Интернет и искусственного интеллекта (Ибатуллина 2023, 68); использование робота или систем искусственного интеллекта (Камалова 2020, 385); использование технологий искусственного интеллекта или информационно-телекоммуникационных сетей (Савельев 2020, 484). Полагаем, в литературе встречаются и другие похожие утверждения, общий посыл которых сводится к добавлению признаков, учитывающих новые технологии.

Применение систем искусственного интеллекта при совершении преступлений действительно может повышать степень общественной опасности, хотя и не во всех случаях. Соглашаясь с изложенной позицией в общих чертах, отметим, что тема настоящего исследования согласуется с ней лишь частично. Фальсификация внешности и голоса человека осуществляется как с помощью искусственного интеллекта, так и без таковой. Было бы нелогичным и неполным запретить такое явление только для тех случаев, когда оно совершается определенным способом.

Еще одно концептуальное изменение законодательства заключается в расширении закрепленного в ст. 63 УК перечня обстоятельств, отягчающих наказание. В частности, предлагается включить в него признаки «совершение преступления, сопряженного с использованием цифровых технологий» или «совершение преступления с использованием искусственного интеллекта или технологий, созданных на его основе» (Грешнова, Ситник 2022, 188; Архипцев, Сарычев, Мотузов 2022, 179).

Представляется, что подобный подход не будет обеспечивать полноценной дифференциации ответственности, которой можно добиться путем, например, формулирования квалифицированных составов преступления и установления санкции за их совершение. Вновь заметим, что основанные на использовании искусственного интеллекта технологии — лишь один из инструментов создания фальсифицированных изображений и звуков. Силиконовые маски и подделка фотографий вручную останутся за пределами действия предлагаемых поправок.

Принципиально иное разрешение назревших проблем встречается в трудах отдельных зарубежных ученых. Отмечается, что чрезмерное правовое регулирование дипфейк-технологий способно принести больше вреда, чем пользы. В частности, по мнению М. Фини, причиненный фальсифицированными записями ущерб мотивирует законодателей на принятие новых поправок, однако всесторонний запрет препятствует свободе слова и прессы. Именно поэтому нормы должны носить узкий характер, препятствующий случаям целенаправленного причинения какого-либо ущерба (Feeney 2021). Другие авторы также говорят о регулировании лишь критически важных моментов, указывая на приоритет рыночных и технических механизмов противодействия фальсификациям (Meskys et al. 2020, 30–31).

Последние позиции во многом представляются нам наиболее верными по ряду причин. Появление дипфейк-технологий — достаточно закономерное следствие научно-технического прогресса. Компьютерные устройства и телекоммуникации тоже существуют не столь давно по историческим меркам, их активно используют в противоправной деятельности, но запрет их применения действует лишь в той степени, в какой осуществляется причинение вреда общественным отношениям. Создание фальсифицированных (или синтезированных) изображений, видео- и аудиозаписей часто осуществляется в целях, не противоречащих законодательству и его принципам. Например, изготавливается и демонстрируется пародийный или сатирический контент. В ряде стране уже обыденным стало наличие цифровых ведущих программы новостей и прогноза погоды, внешность и голос которых синтезированы на основе реальных обладателей (с их согласия, разумеется). Известные отечественные пранкеры в дистанционных беседах использовали фальсифицированные внешность и голоса для розыгрышей, в результате которых становилась известной информация, во многом способствующая обеспечению безопасности РФ. Дипфейк-технологии применяются для достижения общественно полезных целей: осуществляются перевод и трансляция речей политиков на различные языки; производится замена погибших киноактеров (Грешнова, Ситник 2022, 185). С большой вероятностью технологии синтеза займут прочное место в массовой культуре в ближайшие годы, а положительные стороны их применения отрицать невозможно.

Действующее уголовное законодательство не признает неправомерным воспроизведение внешнего вида человека или его голоса, если не имеется других юридически значимых обстоятельств. В то же время при отсутствии согласия на использование этих индивидуальных признаков при создании какого-либо продукта восстановление прав и возмещение причиненного вреда возможны иными правовыми средствами. В научной литературе отмечается, что результат, полученный с применением дипфейк-технологий, следует оценивать как производный (Добробаба 2022, 116). Поэтому в первую очередь необходимо отметить имущественную

ответственность, реализуемую посредством предъявления иска. Так, решением Арбитражного суда города Москвы с ООО «Бизнес-аналитика» в пользу ООО «Рефейс Технолоджис» была взыскана компенсация в размере 500 тыс. руб. за незаконное использование аудиовизуального произведения. В произведении использовалась внешность актера Киану Ривза, синтезированная посредством применения дипфейк-технологий. В решении суд отметил: «Доводы ответчика о том, что созданный видеоролик не является объектом авторского права по причине использования технологии deep-fake отклоняются судом, поскольку технология deep-fake — это дополнительный инструмент обработки (технического монтажа) видеоматериалов, а не способ их создания»[8].

Вместе с тем нельзя исключать привлечение к административной ответственности. При наличии соответствующих обстоятельств могут быть применены нормы, предусмотренные, например, следующими статьями Кодекса РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ (КоАП): ст. 13.11 «Нарушение законодательства РФ в области персональных данных», ст. 13.11.3 «Нарушение требований в области размещения биометрических персональных данных», ст. 14.3 «Нарушение законодательства о рекламе» и др. Следовательно, в случаях злонамеренного использования дипфейк-технологий и при отсутствии угрозы общественным отношениям, охраняемым уголовным законом, достаточно эффективными могут оказаться гражданско-правовые и административно-правовые инструменты. Существуют также неправовые средства, включающие дополнительную проверку информации, использование компьютерных программ для анализа какого-либо произведения и маркировку.

Однако при наличии весомой угрозы общественным отношениям применение уголовно-правовых мер видится целесообразным, а охранительный потенциал иных отраслей права — недостаточным. Как верно отмечается в литературе, правоохранительные органы обладают максимальными ресурсами для расследования и ведения дел по нарушению прав. Имущественная ответственность не гарантирует удаления синтезированных произведений из интернета, а удовлетворение иска не гарантирует получения возмещения вреда (Delfino 2019, 902). Соответственно, социальная справедливость может быть восстановлена посредством применения уголовного наказания к лицу, совершившему преступление. Как отмечалось выше, криминализация не должна быть связана с искоренением дипфейк-технологий. Ее предназначение видится в предупреждении причинения вреда и привлечении к ответственности, если такой вред все же был причинен.

Говоря о противоправном использовании персональных данных (к которым относится и внешность), В. В. Вабищевич приводит следующие предпосылки к установлению уголовной ответственности:

— стремительное развитие информационно-коммуникационных технологий, рост числа пользователей информационных систем;

— бессистемное и неполное правовое регулирование сферы оборота персональных данных;

[8] Решение Арбитражного суда города Москвы от 30.11.2023 г. по делу № А40-200471/23-27-1448. Дата обращения 10 марта, 2025. https://kad.arbitr.ru/Document/Pdf/4d7f0305-69af-44fe-8841-a59e84aa7deb/8dedc372-21f6-4751-ab3c-8a320fe435ce/A40-200471-2023_20231130_Reshenija_i_postanovlenija.pdf?isAddStamp=True.

— масштабность незаконного использования персональных данных;

— наличие уголовной ответственности и практики привлечения к ней за сам факт хищения персональных данных в развитых зарубежных странах (Вабищевич 2020, 62–63).

Многие из вышеперечисленных предпосылок вполне справедливы по отношению к злонамеренному использованию внешности и голоса человека. Стремительное развитие информационно-коммуникационных технологий привело к появлению дипфейк-технологий, которые сделали возможным массовое, быстрое и качественное синтезирование произведений, но регулирование данной сферы остается фрагментарным. Поправки в законодательство вносятся достаточно часто: в 2024 г. в УК введена ст. 272[1], направленная на повышение эффективности системы защиты персональных данных, в том числе биометрических. Масштабность незаконного использования чужих внешности или голоса является общемировой тенденцией: практически любой человек, имеющий профиль в социальных сетях, подвергается потенциальному риску быть «подделанным» (Flynn, Clough, Cooke 2021, 590). Наконец, первые законодательные изменения, учитывающие использование технологии синтеза и преступные цели, приняты в США и КНР. Их эффективность трудно оценить, так как не наработана практика применения, но потенциал у них значительный.

Таким образом, предпосылки для установления уголовной ответственности за злонамеренное использование дипфейк-технологий в целом имеются. В то же время, как ранее указывалось в статье, эти технологии являются одним из инструментов взаимодействия с изображениями и звуками, но не единственным и наверняка не последним. Факт использования при совершении преступления чужих внешности и голоса позволяет виновному лицу избежать ответственности, повысить убедительность смыслового содержания и вероятность успеха манипуляции, что не только увеличивает степень общественной опасности, но и меняет ее характер. Актуальность рассматриваемой проблематики настолько остра, что отдельные исследователи справедливо говорят о целесообразности криминализации подготовительной деятельности для эффективного противостояния данному явлению (Михайлов, Кокодей 2023, 454). Мы же, в свою очередь, дополним: криминализация должна затрагивать не столько использование дипфейк-технологий, сколько использование образа другого человека и иных индивидуальных признаков.

Согласно Федеральному закону от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и/или аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты РФ и признании утратившими силу отдельных положений законодательных актов РФ», к биометрическим персональным данным относятся изображение лица человека и запись его голоса. Данные, полученные в результате преобразования биометрических персональных данных, произведенного с использованием информационных технологий и технических средств, именуются вектором единой биометрической системы.

С каждым годом биометрические данные все больше используются в общественной жизни. Сканирование отпечатков пальцев и сетчатки глаз, например, осуществляется системами контроля и управления доступом различных охраняемых объектов. Благодаря образцам голоса производится распознавание клиентов

банков по телефонным звонкам. Лицо человека участвует в сервисах оплаты супермаркетов и метрополитенов.

В литературе вполне справедливо утверждается, что к биометрическим данным относятся результаты анализов ДНК и геномная информация в целом (Чукреев 2022, 115). Они еще не получили широкого распространения в общественной жизни, однако в дальнейшем не следует исключать подобного развития событий. В частности, не столь отдаленным представляется появление вещей индивидуального пользования, предназначенных только для обладателя определенной геномной информации.

Законодатель предпринял определенные правовые меры защиты персональных (в том числе биометрических) данных. Установлена административная ответственность за нарушение порядка их обработки, уточнения, блокирования или уничтожения (ст. 13.11 и 13.11.3 КоАП). При определенных обстоятельствах возможно применение уголовно-правовых мер. Так, распространена практика применения нормы, закрепленной в ст. 272 УК, по отношению к случаям продажи баз данных клиентов сотрудниками операторов связи или иных организаций. Прямое указание на использование персональных данных в контексте образования (создания, реорганизации) юридического лица содержится в ст. 173^2 УК. В то время как уголовным законодательством охватываются неправомерные доступ, уничтожение, блокирование, модификация, копирование, а также (крайне ограниченно) использование биометрических данных, синтез (или фальсификация) остается за пределами действия норм. Новая ст. 272^1 УК не устранила этот пробел. По существу, данное явление имеет много общего с подделкой, применимой по отношению к документам, средствам идентификации, пробирным клеймам и другим предметам. Неслучайно отечественные авторы даже предлагают включить в предмет преступления, предусмотренного ст. 327 УК, физические объекты, содержащие биометрические данные человека (Чукин, Муфаздалов 2020, 41–42).

Между тем близость фальсификации документов и фальсификации биометрических данных представляется очевидной. И то и другое используется при получении услуг, подтверждении личности и прохождении контроля для допуска на охраняемые объекты. В обоих случаях речь идет не об использовании оригинала, а об использовании его реалистичной копии, поэтому слово «подделка» равным образом применимо к обоим явлениям. Документы и биометрические данные обладают уникальными чертами, позволяющими их отличать. Наконец, их использование существенно облегчает совершение отдельных преступлений, позволяет избежать обнаружения и привлечения виновного лица к ответственности.

Мы, безусловно, согласны с исследователями, утверждающими, что противоправное обращение персональных данных представляет особую опасность при маскировке под другого человека. Чужой образ может быть использован при совершении хищений, клеветы, преступлений террористической направленности и многих других, преимущественно имеющих цифровой элемент (Чукреев 2022, 115).

В то же время подделка именно биометрических данных обладает большей общественной опасностью по сравнению с подделкой иных персональных данных. Так, фальсификация принадлежности к определенной социальной группе, профессии, фальсификация номера телефона или электронной почты практически не способны привести к подмене личности и каким-либо тяжким последствиям,

а использование настоящих, неподдельных данных — способно. Биометрические данные считаются достаточно надежным инструментом, с которым связываются проведение оплаты, заключение договоров и пропуск на охраняемые объекты, поскольку они индивидуальны и, например, в отличие от фамилии и места регистрации, обычно не могут с легкостью изменяться. Однако, как видим, их фальсификация реальна и трудноразличима. Создание поддельных биометрических данных также свидетельствует о наличии заранее обдуманного, а не внезапно возникшего умысла, что часто связывается с негативной оценкой личности при назначении наказания.

Отталкиваясь от высокой общественной опасности создания биометрических данных другого человека, увеличения их значимости в общественной жизни с каждым годом и появления доступного и эффективного инструмента фальсификации, считаем необходимым закрепить в уголовном законодательстве специальный состав, охватывающий данное явление. Применение дипфейк-технологий нельзя назвать единственным способом фальсификации, в связи с чем при конструировании новой статьи следует отказаться от сосредоточения на них. Поскольку биометрические данные индивидуальны и всегда принадлежат отдельному лицу, то в роли родового объекта преступления будут выступать общественные отношения, охраняющие личность. В гл. 19 УК сосредоточены статьи, описывающие преступления, посягающие на наиболее значимые права и свободы, за исключением права на жизнь, здоровье, свободу и половую неприкосновенность. Если следовать логике законодателя, статью, предусматривающую ответственность за посягательство на биометрические данные, следует разместить именно в этой главе.

Так как фальсификация биометрических данных, в том числе посредством дипфейк-технологий, не представляется опасной сама по себе, следует указать конкретизирующие и ограничивающие признаки. К таковым, безусловно, относится цель скрыть другое преступление или облегчить его совершение, как это сделано в штате Массачусетс или в ч. 4 ст. 327 УК, действующей по отношению к поддельным документам, наградам, штампам, печатям и бланкам. Таким образом будет криминализована подготовительная деятельность к совершению иных противоправных деяний, а уголовная ответственность — дифференцирована с учетом использования образа другого гражданина.

3. Выводы

В рамках исследования проблем уголовно-правового противодействия злонамеренному использованию дипфейк-технологий и посягательствам с применением чужих биометрических данных считаем возможным сформулировать несколько важных выводов, которые могут быть учтены при развитии и совершенствовании отечественного законодательства.

Развитие компьютерных систем в целом и искусственного интеллекта в частности привело к появлению технических решений, позволяющих создавать цифровую копию чужих внешности и голоса, практически неотличимых от оригинальных. Результат используется в развлекательной деятельности, при замещении людей в телевизионных программах и других областях. Криминальная сфера не стала исключением. Совершение посягательств с применением дипфейк-технологий

вынудило законодателей США и КНР принять специальные запрещающие поправки. Подходы при этом варьируются: ответственность устанавливается за распространение фальсифицированных новостей, вмешательство в выборы или создание порнографических материалов. В штате Массачусетс запрещается использовать дипфейк-технологии для облегчения совершения преступления или правонарушения.

В то же время скопировать образ другого человека позволяют не только нейросети: в качестве аналогии можно назвать ретуширование фотографий (известное в прошлые века) и создание реалистичных силиконовых масок (появившихся относительно недавно). Иначе говоря, по нашему мнению, нецелесообразно запрещать лишь один способ злонамеренной деятельности, даже если он является массовым и эффективным.

Гораздо более важным представляется факт использования чужого образа (и его элементов) при совершении общественно опасных деяний, что обусловлено повышением значимости биометрических данных в общественной жизни с каждым годом. Оправданным видится установление уголовной ответственности за фальсификацию внешности, голоса, папиллярных узоров пальцев и других разновидностей биометрических данных для дальнейшего совершения преступления в новой ст. 136[1] УК. В диспозиции целесообразно описать следующие признаки: подделка, изготовление или оборот поддельных биометрических персональных данных с целью скрыть другое преступление или облегчить его совершение.

Сформулированные рекомендации по дополнению уголовного законодательства новой нормой могут быть дополнены или отвергнуты в рамках соответствующих исследований. Мы видим массу вариантов для корректировки, включающих, например, ограничение круга преступлений, включение общественно опасных последствий в качестве обязательного признака или уточнение предмета преступления. Однако необходимость повышенной защиты биометрических данных представляется нам неоспоримой. Выражаем надежду на фокусировку научного внимания на рассматриваемой проблеме и появление новых исследований, касающихся совершенствования уголовного закона.

Библиография

Архипцев, И. Н., А. В. Сарычев, А. В. Мотузов. 2022. «К вопросу о правовом обеспечении предупреждения преступлений, совершаемых с использованием искусственного интеллекта и технологий, созданных на его основе в Российской Федерации». *Legal Concept* 2 (21): 175–181.

Архипцев, И. Н., А. В. Сарычев. 2022. «Искусственный интеллект и уголовное право». *Правовая культура в современном обществе*: сб. науч. ст., 346–351. Могилёв: Могилёв. ин-т МВД РБ.

Вабищевич, В. В. 2020. «Социально-правовые и исторические предпосылки криминализации вмешательства в персональные данные». *Журнал Белорусского государственного университета. Право* 1: 61–71.

Грешнова, Н. А., В. Н. Ситник. 2022. «Обеспечение общественного интереса в условиях цифровизации: проблемы уголовного законодательства в России (на примере технологии дипфейк (deepfake))». *Вестник Саратовской государственной юридической академии* 5 (148): 182–189.

Добробаба, М. Б. 2022. «Дипфейки как угроза правам человека». *Lex Russica* 11 (192): 112–119.

Еремченко, В. И. 2017. «Современные проблемы свободного оборота средств совершения и сокрытия преступлений». *Общество и право* 2 (60): 195–197.

Ибатуллина, Д. М. 2023. «Искусственный интеллект в уголовно-правовой доктрине». *Вестник Казанского юридического института МВД России* (14) 2: 65–69.
Камалова, Г. Г. 2020. «Некоторые вопросы уголовно-правовой ответственности в сфере применения систем искусственного интеллекта и робототехники». *Вестник Удмуртского университета. Сер.: Экономика и право* 3 (30): 382–388.
Мардиева, Э. Р. 2023. «О проблемах использования персональных данных». *Скиф. Вопросы студенческой науки* 11 (87): 239–243.
Михайлов, М. А., Т. А. Кокодей. 2023. «Риски злонамеренного использования искусственного интеллекта и возможности их минимизации». *Всероссийский криминологический журнал* 17 (5): 452–461.
Перина, А. С. 2023. «Квалификация цифровых преступлений против личности: проблемные вопросы». *Вестник Югорского государственного университета* 2 (69): 87–102.
Першина, В. А. 2021. «Технология deepfake: необходимость внесения изменений в Уголовный кодекс РФ». *Современные наука и образование: достижения и перспективы развития:* мат-лы Нац. науч.-практ. конф., 230–233. Керчь: Керч. гос. мор. техн. ун-т.
Савельев, И. В. 2020. «Преступление, осложненное искусственным интеллектом: перспективы ближайших уголовно-правовых преобразований». *Вопросы российской юстиции* 7: 475–488.
Чукин, Д. С., С. И. Муфаздалов. 2020. «Объекты с биометрическими данными как предмет преступления, предусмотренного ст. 327 Уголовного кодекса РФ». *Право в Вооруженных силах — Военно-правовое обозрение* 4: 37–42.
Чукреев, В. А. 2022. «Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны». *Вестник Университета им. О. Е. Кутафина (МГЮА)* 3 (91): 107–116.
Delfino, R. A. 2019. "Pornographic deepfakes: The case for federal criminalization of revenge porn's next tragic act". *Fordham Law Review* 88 (3): 887–938.
Feeney, M. 2021. *Deepfake laws risk creating more problems than they solve*. Accessed February 9, 2024. https://rtp.fedsoc.org/wp-content/uploads/Paper-Deepfake-Laws-Risk-Creating-More-Problems-Than-They-Solve.pdf.
Flynn, A., J. Clough, T. Cooke. 2021. "Disrupting and preventing deepfake abuse: Exploring criminal law responses to AI-facilitated abuse". *The Palgrave Handbook of Gendered Violence and Technology*, 583–603. Cham: Palgrave Macmillan.
Geng, Y. 2023. "Regulatory regimes in the United States, the European Union, and China". *Georgetown Law Technology Review* 7 (1): 157–178.
Liu, M., X. Zhang. 2022. "Deepfake technology and current legal status of it". *2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022)*, 1308–1314. Zhengzhou: Atlantis Press.
Meskys, E., A. Liaudanskas, J. Kalpokiene, P. Jurcys. 2020. "Regulating deep fakes: Legal and ethical considerations". *Journal of Intellectual Property Law & Practice* 15 (1): 24–31.
Mullen, M. 2022. "A new reality: Deepfake technology and the world around us". *Mitchell Hamline Law Review* 48 (1): 210–234.
Okolie, C. 2023. "Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns". *Journal of International Women's Studies* 25 (2): 1–16.
Rancourt-Raymond, A., N. Smaili. 2023. "The unethical use of deepfakes". *Journal of Financial Crime* 30 (4): 1066–1077.
Whyte, C. 2020. "Deepfake news: AI-enabled disinformation as a multi-level public policy challenge". *Journal of Cyber Policy* 5 (2): 199–217.

Статья поступила в редакцию 27 марта 2024 г.;
рекомендована к печати 30 октября 2024 г.

Контактная информация:

Мосечкин Илья Николаевич — канд. юрид. наук, доц.; https://orcid.org/0000-0002-9724-9552, weretowelie@gmail.com

Deepfake technologies and biometric data: Directions of criminal legal regulation

I. N. Mosechkin

Vyatka State University,
36, ul. Moskovskaya, Kirov, 610000, Russian Federation

For citation: Mosechkin, I. N. 2025. "Deepfake technologies and biometric data: Directions of criminal legal regulation". *Vestnik of Saint Petersburg University. Law* 1: 95–110.
https://doi.org/10.21638/spbu14.2025.107 (In Russian)

The article is devoted to the study of the need to adjust Russian criminal legislation in terms of protecting individuals from falsification of their biometric personal data through the use of artificial intelligence systems. The relevance of the topic is explained by the availability of deepfake technologies, which allow you to quickly and realistically create digital copies of people, as well as the prevalence of the use of biometric data in everyday life: when making purchases, confirming identity and entering protected areas. The article explains that the emergence of new computer technologies has exacerbated the threat of using the image of another person when committing illegal acts. The first cases of theft using fake biometric data have already been recorded in China and the United Arab Emirates. The author analyzed the provisions of domestic and foreign criminal legislation, which made it possible to establish some shortcomings of legal counteraction to malicious falsification of a person's appearance and voice. The work emphasizes that deepfake technologies are not the only method, and their purpose is not strictly criminal in nature, and therefore it is necessary to raise the issue of protecting biometric data in general. The position on the insufficiency of the protective potential of civil and administrative law is stated in a reasoned manner. The author provides evidence that falsification of appearance, voice, finger papillary patterns and genomic information poses a great social danger if carried out with the aim of hiding another crime or facilitating its commission. The admissibility of a criminal law prohibition that is similar to the provisions of Art. 327 of the Criminal Code of the Russian Federation and the rules of the State of Massachusetts. As a result of the study, an edition of the corresponding article was formulated, which can be used as a recommendation when improving legislation.

Keywords: deepfake, forgery, digital copies, falsification, biometric data, voice, face.

References

Arkhiptsev, I. N., A. V. Sarychev, A. V. Motuzov. 2022. "On the legal support for the prevention of crimes committed using artificial intelligence and technologies created on its basis in the Russian Federation". *Legal Concept* 2 (21): 175–181. (In Russian)

Arkhiptsev, I. N., A. V. Sarychev. 2022. "Artificial intelligence and criminal law". *Pravovaia kul'tura v sovremennom obshchestve: sbornik nauchnykh statei*, 346–351. Mogilev, Mogilevskii institut Ministerstva vnutrennikh del Respubliki Belarus Publ. (In Russian)

Chukin, D. S., S. I. Mufazdalov. 2020. "Objects with biometric data as the subject of a crime under Article 327 of the Criminal Code of the Russian Federation". *Pravo v Vooruzhennykh silakh — Voenno-pravovoe obozrenie* 4: 37–42. (In Russian)

Chukreev, V. A. 2022. "Personal biometric data as subjects of criminal law protection". *Vestnik Universiteta imeni O. E. Kutafina (MGIuA)* 3 (91): 107–116. (In Russian)

Delfino, R. A. 2019. "Pornographic deepfakes: The case for federal criminalization of revenge porn's next tragic act". *Fordham Law Review* 88 (3): 887–938.

Dobrobaba, M. B. 2022. "Deepfakes as a threat to human rights". *Lex Russica* 11 (192): 112–119. (In Russian)

Eremchenko, V. I. 2017. "Modern problems of free trafficking of the means of committing and concealing crimes". *Obshchestvo i pravo* 2 (60): 195–197. (In Russian)

Feeney, M. 2021. *Deepfake laws risk creating more problems than they solve*. Accessed February 9, 2024. https://rtp.fedsoc.org/wp-content/uploads/Paper-Deepfake-Laws-Risk-Creating-More-Problems-Than-They-Solve.pdf.

Flynn, A., J. Clough, T. Cooke. 2021. "Disrupting and preventing deepfake abuse: Exploring criminal law responses to AI-facilitated abuse". *The Palgrave Handbook of Gendered Violence and Technology*, 583–603. Cham, Palgrave Macmillan.

Geng, Y. 2023. "Regulatory regimes in the United States, the European Union, and China". *Georgetown Law Technology Review* 7 (1): 157–178.

Greshnova, N. A., V. N. Sitnik. 2022. "Ensuring public interest in the context of digitalization: Problems of criminal law in Russia (On the example of deepfake technology)". *Vestnik Saratovskoi gosudarstvennoi iuridicheskoi akademii* 5 (148): 182–189. (In Russian)

Ibatullina, D. M. 2023. "Artificial intelligence in the criminal law doctrine". *Vestnik Kazanskogo iuridicheskogo instituta MVD Rossii* (14) 2: 65–69. (In Russian)

Kamalova, G. G. 2020. "Some questions of criminal legal responsibility in the field of application of artificial intelligence systems and robotics". *Vestnik Udmurtskogo universiteta. Seriia: Ekonomika i pravo* 3 (30): 382–388. (In Russian)

Liu, M., X. Zhang. 2022. "Deepfake technology and current legal status of it". *2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022)*, 1308–1314. Zhengzhou, Atlantis Press.

Mardieva, E. R. 2023. "About the problems of using personal data". *Skif. Voprosy studencheskoi nauki* 11 (87): 239–243. (In Russian)

Meskys, E., A. Liaudanskas, J. Kalpokiene, P. Jurcys. 2020. "Regulating deep fakes: Legal and ethical considerations". *Journal of Intellectual Property Law & Practice* 15 (1): 24–31.

Mikhailov, M. A., T. A. Kokodey. 2023. "Risks of the malicious use of artificial intelligence and the possibility of minimizing them". *Vserossiiskii kriminologicheskii zhurnal* 17 (5): 452–461. (In Russian)

Mullen, M. 2022. "A new reality: Deepfake technology and the world around us". *Mitchell Hamline Law Review* 48 (1): 210–234.

Okolie, C. 2023. "Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns". *Journal of International Women's Studies* 25 (2): 1–16.

Perina, A. S. 2023. "Qualification of digital crimes against person: Problematic issues". *Vestnik Iugorskogo gosudarstvennogo universiteta* 2 (69): 87–102. (In Russian)

Pershina, V. A. 2021. "Deepfake technology: The need to amend the Criminal Code of the Russian Federation". *Sovremennye nauka i obrazovanie: dostizheniia i perspektivy razvitiia: materialy Natsional'noi nauchno-prakticheskoi konferentsii*, 230–233. Kerch, Kerchenskii gosudarstvennyi morskoi tekhnologicheskii universitet Publ. (In Russian)

Rancourt-Raymond, A., N. Smaili. 2023. "The unethical use of deepfakes". *Journal of Financial Crime* 30 (4): 1066–1077.

Savelyev, I. V. 2020. "Crime complicated by artificial intelligence: Prospects for criminal law reforms". *Voprosy rossiiskoi iustitsii* 7: 475–488. (In Russian)

Vabischevich, V. V. 2020. "Socio-legal and historical background of the criminalization of illegal interference with personal data". *Zhurnal Belorusskogo gosudarstvennogo universiteta. Pravo* 1: 61–71. (In Russian)

Whyte, C. 2020. "Deepfake news: AI-enabled disinformation as a multi-level public policy challenge". *Journal of Cyber Policy* 5 (2): 199–217.

Received: March 27, 2024
Accepted: October 30, 2024

Author's information:

Ilya N. Mosechkin — PhD in Law, Associate Professor; https://orcid.org/0000-0002-9724-9552, weretowelie@gmail.com