УДК 340

Шубенкова Ксения Владимировка
кандидат юридических наук, доцент кафедры юриспруденции,
Волжский филиал Волгоградского государственного университета
shubenkova34@yandex.ru
Ksenia V. Shubenkova
PhD in Law, Associate Professor of the Department of Jurisprudence,
Volga Branch, Volgograd State University
shubenkova34@yandex.ru

ПРАВОВЫЕ ПРОБЛЕМЫ ОХРАНЫ ЦИФРОВОГО ОБРАЗА ЛИЧНОСТИ В РФ

LEGAL ISSUES OF PROTECTION OF THE DIGITAL IMAGE OF THE PERSON IN THE RUSSIAN FEDERATION

Аннотация. *Развитие цифровых технологий, в том числе, связанных с моделированием цифрового облика конкретного человека, сформировал правовую необходимость закрепления в законодательстве ряда прав, связанных непосредственно с цифровой идентичностью граждан, при этом большинство ученых продолжают отмечать наличие существенных нормативных недостатков в данной сфере.* ***Целью работы*** *является проведение научного обзора существующих правовых подходов к цифровому образу личности и обоснование необходимости продолжения работ по правовому обеспечению цифровых прав гражданина, связанных с данной категорией.* ***С помощью методов*** *научного познания, прежде всего, метода системного анализа, установлено, что сложность выделенной проблемы предполагает использование как правотворческого, так и правореализационного «виденья» основных направлений и форм предотвращения нарушений порядка использования цифровой идентификации личности в ущерб его прав.* ***Результаты:*** *рассматриваемые подходы и правовые механизмы защиты цифровых прав личности, позволят обосновать необходимость организационных мероприятий по совершенствованию норм права и правоприменительной практики в стране и предложить ряд мер по их устранению.* ***Выводы:*** *необходимо 1) усилить защиту персональной информации пользователей социальных сетей от третьих лиц; 2) создать на основе уже существующих систем (к примеру: яндекс.картинки) специальный портал для проверки и оценки размещаемой в открытом доступе фейковой информации; 3) увеличить круг субъектов, подлежащих юридической ответственности (административной или уголовной) за нарушение права на цифровой образ личности и др.*

Ключевые слова: *deepfake, цифровые права личности, электронная безопасность, ответственность за нарушения прав личности.*

Annotation. *The development of digital technologies, including those related*

to the modeling of the digital appearance of a particular person, has formed the legal need to consolidate in legislation a number of rights directly related to the digital identity of citizens, while most scientists continue to note the presence of significant regulatory shortcomings in this area. ***The purpose of the work*** *is to conduct a scientific review of existing legal approaches to the digital image of the individual and substantiate the need to continue work on the legal provision of digital rights of a citizen related to this category.* ***Using the methods*** *of scientific cognition, first of all, the method of system analysis, it is established that the complexity of the highlighted problem involves the use of both law-making and law-realization "vision" of the main directions and forms of preventing violations of the procedure for using digital identification of a person to the detriment of his rights.* ***Results:*** *the considered approaches and legal mechanisms for the protection of digital rights of the individual will justify the need for organizational measures to improve the norms of law and law enforcement practice in the country and propose a number of measures to eliminate them.* ***Conclusions****: it is necessary to 1) strengthen the protection of personal information of users of social networks from third parties; 2) create a special portal based on existing systems (for example: yandex.pictures) for checking and evaluating fake information posted in the public domain; 3) increase the number of subjects subject to legal liability (administrative or criminal) for violation of the right to a digital image of a person, etc.*

Key words: *deepfake, digital rights of the individual, electronic security, liability for violations of individual rights.*

Введение.

В рамках развития цифрового статуса электронной информации и близких к ней категорий 18 марта 2019 г. Государственная Дума Российской Федерации приняла Федеральный закон № 34-ФЗ "О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации", позволивший нормативно определить правовую природу цифровых прав, в том числе, связанных с правами личности. Согласно трактовке данных изменений, цифровые права нормативно были отнесены к объектам неимущественных гражданских правоотношений. Это позволяет данные объекты цифрового права включить в качестве элементов гражданского оборота и урегулировать в рамках информационной системы непосредственную принадлежность отмеченных объектов лицу, обладающему правом непосредственного распоряжения ими [2].

При этом законодатель в своих актах обращает внимание на то, что цифровые права должны быть четко определены в законах, которые будут разрабатываться с непосредственным участием федеральных министерств. Так, к примеру, был принят Федеральный закон от 31 июля 2020 г. № 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации", определивший, меры защиты прав лица на цифровые финансовые активы.

Научный обзор правового статуса цифровых прав личности.

Как не однократно отмечается специалистами, до сих пор остается спорным вопрос о существе права на цифровой образ личности. С каждым годом растет число случаев использования фото- и видеоизображений, аудиозаписей людей без их согласия на это. Копирование и использование таких данных легло в основу методики синтеза изображений, основанной на искусственном интеллекте и получившей название deepfake[8]. Появление этой технологии, позволяющей сфальсифицировать медиаматериалы с использованием копии изображения и голоса человека, вызвало рост числа фейков, особенно, в новостной журналистике. К примеру, в мае 2021 г. в интернете был опубликован видеоролик о том, как глава регионального штаба оппозиционного движения якобы дает интервью по видео-конференц-связи местным журналистам и парламентариям. Как позже выяснилось, представитель оппозиции не давал данного интервью, а с журналистами и парламентариями общались пранкеры (лица, инсценирующие розыгрыши, часто с хулиганскими целями)[8].

Использование данной технологии привело к возможности создания произведений с участием любых артистов, которые на самом деле не только не принимали участия в работе, но и не были информированы о таком проекте. Так, блогер Race Archibold в 2021 г. презентовал версию кинофильма "Гарри Поттер" не с оригинальным актерским составом, а с участием голливудских киноартистов, которые не снимались в этой ленте и не давали согласия на использование их образов.

Отмеченное позволяет сделать вывод о том, что технология deepfake несложна в формальном применении (цифровой образ личности можно изготовить, используя программное приложение, доступное всем пользователям), что и подтверждается, в большинстве случаев, в рамках анализа периодически возникающих, в т.н., "желтых изданиях", неожиданных фейковых сенсаций или при попытках решения политических задач не добросовестным путем. Иногда за такими актами формирования цифрового образа стоят представители преступной среды [3].

Совершенно справедливы опасения М.А. Желудкова, с точки зрения которого, "подобные технологии в условиях удаленного доступа могут быть использованы для оформления подложных товарно-денежных операций, изменения доказательств по реальным уголовным делам. Если сегодня такие программы пока еще недостаточно совершенны, то пройдет небольшой промежуток времени, и технология дипфейков с открытым кодом создаст серьезные трудности в идентификации аудио- и видеоинформации в интернет-пространстве" [4].

Появление доступной технологии deepfake несет в себе опасности разного рода: помимо авторитета журналисткой деятельности под угрозой оказываются также общественная и национальная безопасность, международные (дипломатические) отношения, подвергаются нападкам принципы демократического устройства государства, усугубляются социальные противоречия и др.

Т.А. Нестик и Е.А. Михеев, рассматривая деструктивную информацию

(дезинформацию) и ее воздействие на сознание масс, выделяют автоматизированный фишинг и компьютерную пропаганду [7]. В первом случае, вредоносные программы применяются для разработки дипфейка в целях совершения правонарушения или преступления, во втором - технологии deepfake активно используются для манипулирования общественным сознанием посредством распространения слухов и сплетен.

Чтобы предупредить распространение лжеинформации (фейков), кражу персональных данных, унижение достоинства личности и иные правонарушения с использованием искусственного интеллекта, в том числе, с применением технологии deepfake, необходимо признать право на цифровой образ личности каждого гражданина и задействовать эффективные меры его защиты.

Согласно точки зрения Чернышенко И.Г., широкое распространение технологии deepfake объясняется, прежде всего, тем, что фото- и видеоматериалы с изображениями многих граждан - пользователей интернета находятся в открытом доступе, в частности, в личных аккаунтах в социальных сетях. Таким гражданам целесообразно позаботиться о конфиденциальности своих данных, установив настройки приватности, используя функционал закрытых профилей. Если же обеспечить защиту сведений этими способами невозможно, надо обращаться к разработчикам интернет-платформ с требованием о прекращении обработки персональных данных в части аудио-, фото- и видеоматериалов в открытом доступе [8].

Важным представляется вопрос о совершении сделки передачи в пользование цифрового образа личности. Позиция законодателя следующая: правомочия владельца цифрового образа своей личности включают передачу этого объекта, залог, обременение и другие способы, реализующиеся только с применением информационных систем без обращения к третьему лицу.

Представим, что недобросовестное лицо использует цифровой образ для совершения преступного деяния. Очевидно, что обладатель указанного права может лишь воспользоваться механизмом защиты нарушенного права после того, как ему стало известно о нарушении. Данный вопрос следует решить, закрепив порядок пользования цифровым образом личности с участием третьей стороны, которая предварительно будет проверять конкретные сделки на применение технологии deepfake [8].

Если же обратиться к зарубежному опыту в рассматриваемой сфере, то, к примеру, в США существуют три федеральные комиссии, в компетенцию которых входит проверка добросовестного и разумного использования технологии deepfake: Федеральная торговая комиссия, Федеральная комиссия по связи и Федеральная избирательная комиссия [1]. Федеральная торговая комиссия призвана обеспечить прозрачность обязательств, связанных с коммерческим взаимодействием хозяйствующих субъектов (например, сдерживая использование любой фейковой информации в рекламе); Федеральная комиссия по связи рассматривает вопросы спонсорства и финансирования политической рекламы, ее полномочия позволяют требовать указания правдивого источника представленной информации. Таким образом,

федеральные комиссии США в определенных случаях де-факто считаются третьими сторонами при заключении сделок, в которых фигурируют технологии искусственного интеллекта (в сфере рекламы, осуществления обязательств и т.д.).

Данный опыт заслуживает внимания и в России, урегулировать правила участия третьих лиц (территориальных органов исполнительной власти) в процессе проверки совершаемой сделки, связанной с использованием права на цифровой образ личности, в частности, предусмотреть в законодательстве случаи, когда такая проверка будет обязательной (например, при опубликовании видео-, фото-, аудиозаписей с использованием технологии deepfake на интернет-портале для неограниченного круга лиц при наличии у ответственных лиц оснований полагать, что такая сделка может причинить юридически значимый вред и др.). Один из недостатков зарубежного опыта в данной сфере - ограниченная юрисдикция федеральных комиссий по взаимодействию с интернет-платформами. В связи с этим, предлагается предусмотреть возможность установления порядка взаимодействия интернет-платформ с территориальными органами исполнительной власти по проверке и контролю ранее указанных сделок непосредственно в Российской Федерации.

Чернышенко И.Г. также определяет и техническое решение данных проблем, доступное модераторам интернет-пространства [8]. В качестве примера может послужить портал FactCheck.org, определяющий фейковую информацию и ее источники. Создание единого портала проверки фейковой информации с широким функционалом, позволило бы оперативно блокировать пользователей, размещающих фейковый контент, а также, сами аккаунты таких пользователей, что способствовало бы устранению ряда проблем ещё на стадии первичной модерации.

П.Г. Кошкин обращает внимание на реализацию программ повышения цифровой грамотности, способствующих развитию критического мышления и медиаграмотности граждан, обучающих принципам проверки информации [5]. Правовое просвещение поможет снизить неоправданно высокий уровень доверия пользователей сети к публикуемым фактам. Следует создать такие условия, при которых люди освободятся от необходимости получения информации посредством использования цифровых технологий, научатся подозрительно относиться к любым данным, изготовленным посредством использования искусственного интеллекта.

Анализируя иные меры защиты права на цифровой образ личности, В.А. Першина настаивает на законодательном урегулировании дефиниции deepfake и предлагает следующую формулировку: дипфейк - это аудиовизуальная запись, созданная или измененная таким образом, что она ошибочно представляется разумному наблюдателю аутентичной записью реальной речи, поведения, внешности или образа индивидуума [6]. Также, автор рассматривает еще один вариант толкования данного явления: аудио-, фото- и видеоматериалы, содержащие в себе образ конкретного человека (лицо, голос, мимику, артикуляцию и др.), используемый без согласия на то обладателя права на этот образ, либо без согласия его представителей. Под

представителями здесь следует понимать близких родственников лица, имеющих право распоряжаться цифровым образом личности в случаях, определенных гражданским законодательством (например, при вступлении в права наследования, при опекунстве, попечительстве, патронаже и т.д.). Согласие на пользование цифровым образом личности должно быть обязательным условием сделки. Также, у лица, передающего в пользование данный образ, должна быть юридическая гарантия прекращения такого использования после достижения оговоренной цели применения (например, сразу же после завершения съемок фильма).

В.А. Першина выступает за привлечение к ответственности интернет-провайдера в случае нарушения права на цифровой образ личности, если провайдеру стало известно о распространении дипфейка, но он допускает дальнейшее опубликование такого материала. Юридической ответственности должны подлежать также сотрудники отдела модерации интернет-платформы, допустившие публикацию дипфейка.

Обязательно должен быть установлен порядок опровержения от имени физического или юридического лица, которые использовали цифровой образ личности в целях распространения недействительной информации или унижении чести и достоинства обладателя права на такой цифровой образ. Опровержение должно даваться на том же ресурсе, где был размещен дипфейк, при этом ресурс должен до и после момента опровержения находиться в открытом доступе для третьих лиц. Гарантированным правом требовать опровержения дипфейка должны обладать как сам человек, чей образ был использован, так и его представители.

Юридические механизмы противодействия нарушениям статуса цифровых прав личности.

Рассматривая институт ответственности за противоправное применение технологии deepfake, следует обратить внимание на разграничение административной и уголовной ответственности. Уголовная ответственность должна быть напрямую связана с совершением преступления путем применения технологии deepfake с прямым умыслом, с целью дискредитации чести и достоинства физических лиц, подрыва конституционного порядка и общественного строя (общественной и национальной безопасности), т.е., с причинением вреда [8].

Административная ответственность может быть предусмотрена за незаконное использование чужого образа личности, если данное использование не было направлено на подрыв общественного (социального) доверия к физическому лицу (т.е. ущерб ему не нанесен). Например, если лицо незаконно использовало цифровой образ личности для создания пародии на данного гражданина, но в данном материале отсутствовала любая информация, которая могла бы ввести в заблуждение иных лиц по поводу представленной личности, то применим институт административной ответственности.

Совершение преступления (мошенничества, вымогательства, лжесвидетельства и др.), сопряженное с неправомерным использованием права на цифровой образ личности, должно включать совокупность преступлений;

т.е., основное преступное деяние (например, вымогательство) и вытекающее из него неправомерное использование права на цифровой образ личности посредством применения технологий искусственного интеллекта с причинением вреда личности, обществу или государству.

Основаниями для применения мер государственного принуждения в случае неправомерного использования технологии deepfake выступают:

- неправомерное использование чужого образа личности (в отсутствие согласия владельца цифрового права);
- присвоение имени или образа личности с определенным интересом;
- публичное распространение любых медиаматериалов с использованием чужого образа (исключая случаи, когда лицо не могло осознавать, что созданный им материал будет в публичном доступе);
- наличие заведомо ложных сведений о личности, причиняющие вред (в случае применения уголовной ответственности) [2].

Выводы.

Случаи использования технологии deepfake для недобросовестных целей продолжают увеличиваться. Для снижения угроз в данной сфере, целесообразно применить комплекс мер [8]:

- усилить защиту персональной информации пользователей социальных сетей от третьих лиц с помощью настроек конфиденциальности данных;
- урегулировать в специальном федеральном законе все разновидности цифровых прав относительно нематериальных благ личности: понятие дипфейка, право на цифровой образ личности, содержание правомочий владельца такого права, специфические меры защиты и охраны данного права;
- создать специальный портал для проверки и оценки размещаемой в открытом доступе фейковой информации;
- организовать оперативные допубликационные проверки информации на наличие дипфейков силами модераторов интернет-платформ;
- включить в перечень способов защиты права на цифровой образ личности обращение в суд за получением опровержения от ответственных представителей интернет-платформы, распространивших дипфейк, при условии открытого доступа к ресурсу для третьих лиц;
- законодательно урегулировать составы административного правонарушения и преступления в части неправомерного использования цифрового чужого образа личности.

Борьба законодателя с дипфейками не должна быть связана с прямым запретом на их применение. Ограничения призваны лишь защитить общество от последствий неправомерного использования технологии deepfake и обеспечить точность и правдивость публикуемой информации. При этом само обществу вынуждено реагировать на данные угрозы, в частности после начала специальной военной операции на Украине по «демилитаризации и денацификации страны» в цифровом пространстве возникло огромное количество фейковой информации, использующей, в том числе, технологии deepfake, для борьбы с которой в общем вещании стали доступны передачи по

разоблачению данных подделок, примером такой передачи выступил проект 1 Канала "Антифейк".

Литература:

1. Chesney B., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. 2019. Vol. 107. P. 1804-1808.

2. Shubenkova K., Egorov G.G. Legal and technical forms of developing digital law-enforcement in modern Russia: problems and prospects //Lecture Notes in Networks and Systems (см. в книгах). 2020. Т. 111. С. 705-711.

3. Егоров Г.Г. Нормативно-правовые особенности реализации цифровых технологий в российском правосудии // Экология, экономика, право: взгляд в будущее : сборник статей по материалам научно-практической конференции, проходившей в рамках Недели науки (апрель, 2018 г.) / отв. ред. Ю. И. Миронов, Г. Г. Егоров ; ВФ ВолГУ. - Волгоград : Изд-во ВолГУ, 2018. - С. 145-153. - Библиогр.: с. 153 (2 назв.).

4. Желудков М.А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex russica (Русский закон). 2021. № 4. С. 66-67.

5. Кошкин П.Г. Американская журналистика и постправда. М., 2019. С. 43.

6. Першина В.А. Технология deepfake: необходимость внесения изменений в Уголовный кодекс РФ // Современные наука и образование: достижения и перспективы развития: Материалы национальной научно-практической конференции: В 2 ч. Керчь, 2021. С. 231-232.

7. Нестик Т.А., Михеев Е.А. Информационные войны с использованием систем искусственного интеллекта: анализ психологических механизмов воздействия // Организационная психология и психология труда. 2019. № 4. С. 155.

8. Чернышенко И.Г. Правовая охрана цифрового образа личности // Законодательство, № 4, апрель 2022 г., с. 55-58.

REFERENCES

1. Chesney B., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. 2019 Vol. 107. R. 1804-1808.

2. Shubenkova K., Egorov G.G. Legal and technical forms of developing digital law-enforcement in modern Russia: problems and prospects //Lecture Notes in Networks and Systems (see in books). 2020. V. 111. S. 705-711.

3. Egorov G.G. Regulatory and legal features of the implementation of digital technologies in Russian justice // Ecology, economics, law: a look into the future: a collection of articles based on the materials of the scientific and practical conference held as part of the Science Week (April, 2018) / ed. ed. Yu. I. Mironov, G. G. Egorov; VF VolGU. - Volgograd: VolGU Publishing House, 2018. - S. 145-153. - Bibliography: p. 153 (2 titles).

4. Zheludkov M.A. Justification of the need to adapt the activities of law enforcement agencies to the conditions of digital transformation of the criminal

environment // Lex russica (Russian law). 2021. No. 4. S. 66-67.

5. Koshkin P.G. American journalism and post-truth. M., 2019. S. 43.

6. Pershina V.A. Deepfake technology: the need to amend the Criminal Code of the Russian Federation // Modern science and education: achievements and development prospects: Proceedings of the national scientific and practical conference: At 2 hours. Kerch, 2021. P. 231-232.

7. Nestik T.A., Mikheev E.A. Information wars with the use of artificial intelligence systems: analysis of psychological mechanisms of influence // Organizational psychology and labor psychology. 2019. No. 4. P. 155.

8. Chernyshenko I.G. Legal protection of the digital image of a person // Legislation, No. 4, April 2022, p. 55-58.