ЧАСТНОПРАВОВЫЕ (ЦИВИЛИСТИЧЕСКИЕ) НАУКИ
PRIVATE LAW SCIENCES

Вестник Челябинского государственного университета. Серия: Право. 2025. Т. 10, вып. 2. С. 5–12.
Bulletin of Chelyabinsk State University. Series: Law. 2025;10(2):5-12.

УДК 347.1

Научная статья DOI: 10.47475/2618-8236-2025-10-2-5-12

Цифровая идентификация гражданина: современные вызовы

Нина Александровна Новокшонова
Челябинский государственный университет, Челябинск, Россия
nina_novokshonov@mail.ru

Аннотация. В статье рассматриваются проблемы цифровой идентификации гражданина, соотношения данного института со смежными понятиями. Также обсуждаются проблемы использования дипфейка как части цифрового образа физического лица, пределы и критерии защиты цифрового образа как института нематериальных благ и исключительных прав. Сделан вывод, что выработка эффективных способов защиты своего цифрового образа так же необходима, как и традиционных средств индивидуализации физического лица.

Ключевые слова: неприкосновенность частной жизни, цифровой образ, физические лица, дипфейк, цифровая идентификация

Благодарности. Выполнено в соответствии с грантом ФПНИ ФГБОУ ВО «ЧелГУ».

Для цитирования: Новокшонова Н. А. Цифровая идентификация гражданина: современные вызовы // Вестник Челябинского государственного университета. Серия: Право. 2025. Т. 10, вып. 2. С. 5–12. DOI: 10.47475/2618-8236-2025-10-2-5-12

Original article

Digital identification of citizens: modern challenges

Nina A. Novokshonova
Chelyabinsk State University, Chelyabinsk, Russia
nina_novokshonov@mail.ru

Abstract. The article examines the problems of digital identification of a citizen and the relationship of this institution with related concepts. It also discusses the use of deepfake as part of a person's digital image, as well as the limits and criteria for protecting a person's digital image as an institution of intangible benefits and exclusive rights. The article concludes that developing effective methods for protecting a person's digital image is just as important as developing traditional methods for individualizing a person.

Keywords: privacy, digital image, individuals, deepfake, digital identification

Acknowledgments. Completed in accordance with the grant of the FPNI FGBOU VO "ChelSU".

For citation: Novokshonova NA. Digital identification of citizens: modern challenges. *Bulletin of Chelyabinsk State University. Series: Law.* 2025;10(2):5-12. (In Russ.). DOI: 10.47475/2618-8236-2025-10-2-5-12

Не грусти, — сказала Алиса. — Рано или поздно всё станет понятно, всё станет на свои места и выстроится в единую красивую схему, как кружева. Станет понятно, зачем всё было нужно, потому что всё будет правильно…

Льюис Кэрролл. Алиса в Стране Чудес. Алиса в Зазеркалье (сборник)

Введение

Цифровая трансформация общества становится реальностью. Мы проводим большое количество времени в цифровом пространстве. Когда-то мультфильм «ВАЛЛ-И»[1] вызывал улыбку, сейчас это наша реальность. Данные процессы стимулируют как государственные органы, так и международные организации, кроме того они активно поддерживаются крупнейшими транснациональными корпорациями. В соответствии с Национальной стратегией развития искусственного интеллекта до 2023 года в 2018 году мировой рынок технологических решений, разработанных на основе искусственного интеллекта, составил 21,5 млрд долларов США, а к 2024 году он достигнет почти 140 млрд долларов США[2]. Мы всё активнее применяем технологические решения, разработанные на основе искусственного интеллекта. Это происходит в различных отраслях экономики, государственного и корпоративного управления, социальной и культурной сферах. Под искусственным интеллектом Национальная стратегия понимает комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. Мы можем по-разному относиться к этой технологии: радостно её приветствовать или наоборот опасаться. Но все мы каждый день используем эти технологии в нашей жизни, осмысленно или даже не замечая это. Государство активно реализует национальный проект «Экономика данных и цифровая трансформация государства»[3], целью которого является цифровая трансформация государственного и муниципального управления, экономики и социальной сферы за счёт обеспечения кибербезопасности, бесперебойного доступа к интернету, подготовки квалифицированных кадров для ИТ-отрасли, цифрового госуправления, развития отечественных цифровых платформ, программного обеспечения, перспективных разработок и искусственного интеллекта. Соответственно цифровая идентификация гражданина сегодня это не только про сферу развлечения, но про способ реализации и защиты его прав. Мы можем спорим о том, насколько безопасно размещать в сети Интернет свои данные, фотографии, оставлять комментарии, но это уже не только наша воля или желание, но и требование государства по формированию и ведению различных реестров и государственных информационных систем. Конечно, в связи с этим очень важным становится вопрос о том, насколько ведение таких реестров и возможность доступа к этим данным не только государственных структур, но и граждан и юридических лиц соответствует праву на охрану частной жизни гражданина. Насколько современный граждан осознает, что возможность доступа к его данным, фотографиям, информации о его интересах, членах семьи, состоянии здоровья и т.д. может быть доступна третьим лицам. Вопросы, что представляет собой цифровая идентификация человека, как она соотносится с такими понятиями, как «средства индивидуализации», «цифровой образ», «цифровой след», представляются сегодня достаточно актуальными. В рамках данного исследования вряд ли получится дать ответ на все вопросы, остановимся только на ряде аспектов.

Цифровая идентификация, цифровой образ и цифровой след: соотношение дефиниций

Как известно, каждый гражданин имеет средства индивидуализации. ГК РФ относит к ним имя (ст. 19 ГК РФ) и место жительство (ст. 20 ГК РФ), однако в литературе говорят и о других средствах индивидуализации, таких как пол, состояние здоровья, семейное положение и других. Вместе с тем в цифровой среде могут быть и другие средства индивидуализации физического лица: к ним можно отнести псевдоним, аватар, адрес электронной почты и другие. З. В. Талапина справедливо отмечает, что «человек нередко использует вымышленно созданный им цифровой образ для маскировки, позиционируя себя несуществующей виртуальной личностью [13]. Соответственно мы можем говорить о том, что в системе общих средств индивидуализации гражданина необходимо учитывать и его индивидуализацию в цифровой среде. Цифровая идентификация — это способ определения личности пользователя в цифровой среде, а цифровая аутентификация проверяет его подлинность личности, например при совершении сделок. Д. В. Санников считает, что «цифровой образ

[1] Полнометражный анимационный научно-фантастический фильм «ВАЛЛ-И» 2008 года, созданный Pixar Animation Studios, режиссёр Эндрю Стэнтон.

[2] О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») : указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_335184

[3] Национальный проект «Экономика данных и цифровая трансформация государства» URL: http://government.ru/rugovclassifier/923/events/

гражданина — это нематериальное благо, полученное в результате реализации права на неприкосновенность частной жизни, включающее цифровой след и цифровую тень, состоящие из идентификационной, тайной и коммуникационной информации» [12]. При этом он выстраивает терминологический ряд следующем образом: персональный образ — информационный образ — цифровой образ. Следует согласиться с тем, что цифровой образ является частью образа физического лица в целом, который должен быть с ним тесно связан и защищён всеми средствами гражданского права. Однако следует признать, что этот образ может состоять из образа, который требует его жёсткой идентификации с физическим лицом (госуслуги, единая биометрическая система, сетевой город и т. д.), и идентификации, которая допускает создание фантазийного цифрового образа, привязанного к личности субъекта любым способом: через телефон, электронную почту. Таких цифровых образов гражданин может иметь несколько. В этом случае уже сложнее обеспечить защиту прав граждан в случае их нарушения, так как сложно доказать привязку аккаунта к конкретному субъекту. Однако следует признать право на создание фантазийного цифрового образа как часть права на неприкосновенность частной жизни гражданина. Так, В. О. Пучков понимает под цифровым образом «проекцию личности в цифровой среде, в том числе за счёт аккаунтов в социальных сетях, профилях в мессенджерах, каналов на видеохостингах и т. д» [10]. В своей работе он обращает внимание на признак цифровой частной жизни — её управляемость субъектом персональных данных. Следует с ним согласиться, что цифровой образ, созданный и контролируемый конкретным физическим лицом, не всегда отражает объективную социальную реальность. Результатом использования цифрового образа является создание цифрового следа. А. М. Кондаков и А. А. Костылева считают, что цифровой след состоит из трёх слоёв. «Первый слой составляют те данные, которые мы размещаем о себе и можем контролировать, управлять ими. Второй слой состоит из информации о нашем поведении в сети. Это не столько выбор, который мы сознательно делаем, сколько метаданные, которые дают контекст для этих выборов… Третий слой состоит из интерпретаций первого и второго. Наши данные анализируются различными алгоритмами и сравниваются с данными других пользователей для выявления значимых статистических корреляций» [6]. Соответственно, цифровой след — это те данные, которые можно получить при анализе цифрового образа гражданина. Возникает вопрос о том, насколько можно использовать данные цифрового следа. Этот вопрос рассматривался в суде в рамках спора между «ВКонтакте» и сервисом Double Data, который собирал из открытых профилей Ф. И. О пользователей, информацию об их датах рождения и другие данные. После 6 лет спора было заключено мировое соглашение, по которому действия ответчика по извлечению и последующему использованию информационных элементов из базы данных пользователей социальной сети «ВКонтакте» были признаны нарушением исключительных прав Истца как изготовителя базы данных пользователей социальной сети «ВКонтакте». Ответчик не вправе извлекать и использовать информационные элементы из базы данных пользователей социальной сети «ВКонтакте», в том числе с использованием программных продуктов Ответчика переносить информационные элементы из базы данных. Размер компенсации за нарушение исключительных прав составил 1 рубль[1]. Несмотря на то, что спор касался цифрового образа пользователей социальной сети, истец выбрал тактику защиты через нарушение исключительных прав на базу данных. Вопрос о том, можно ли анализировать информацию и использовать информацию цифрового образа, и его соотношения с исключительным правом остался не решён. Если рассматривать с точки зрения интеллектуального права, любое использование исключительного права правообладателя базы данных возможно только с его согласия.

Дипфейк и цифровой образ физического лица

Термин «дипфейк» (deep-fake) происходит от двух английских слов: deep learning — «глубокое обучение» и fake — «фальшивый». В рекомендательном глоссарии терминов и определений государств — членов ОДКБ (организация Договора о коллективной безопасности) в сфере обеспечения национальной и международной безопасности под дипфейком понимается созданное с помощью технологий искусственного интеллекта реалистичное изображение, аудио- или видеоинформация, не соответствующие действительности. Оно может быть как полностью вымышленным, так и включающим реальные материалы или их фрагменты, в том числе позволяющие идентифицировать личность конкретного человека, группу лиц, организацию и показать их действия или участие в событиях, никогда не имевших место в действительности[2]. В большинстве случаев в основе

[1] Постановление Суда по интеллектуальным правам от 23 сентября 2022 года Дело № А40-18827/2017. URL: https://kad.arbitr.ru/Document/Pdf/1f33e071-4a16-4bf9-ab17-4df80f6c1556/f65ad222-5073-44eb-b13e-f1010bc22855/A40-18827-2017_20220923_Reshenija_i_postanovlenija.pdf?isAddStamp=True

[2] Рекомендательный глоссарий терминов и определений государств — членов ОДКБ в сфере обеспечения национальной и международной безопасности. Принят 19.12.2023 Постановлением 16–6.3 Парламентской Ассамблеи Организации Договора о коллективной безопасности // Офиц. сайт Парламентской Ассамблеи Организации Договора о коллективной безопасности. URL: https://paodkb.org/

метода дипфейка лежат генеративно-состязательные нейросети. Идея генеративно-состязательных сетей была выдвинута в 2014 году Яном Гудфеллоу и его соавторами [1]. За это время технология дипфейков значительно изменилась и стала более совершенной. По данным статистики 71 % дипфейков распространены в сфере развлечения, 25 % — в индустрии моды, и 4 % — в сфере спорта, бизнеса и политики. При этом потребители, которые осведомлены о дипфейках и клонировании голоса, выражают большую озабоченность: около 60 % говорят, что они либо «очень», либо «чрезвычайно» обеспокоены. Наибольшие опасения потребителей вызывает область, где используется конфиденциальная личная информация (банковская сфера). При этом 25 % потребителей считают, что у дипфейков нет положительных качеств, а 60 % смогли определить аспекты, которые им нравятся в этой технологии. В целом стоит отметить улучшение отношения потребителей к технологии дипфейка[1]. Именно поэтому исследование правовой природы дипфейков и его соотношение с правом на неприкосновенность частной жизни представляется своевременным. Следует согласиться с Е. А. Останиной, которая пишет, что «неприкосновенность частной жизни включает в себя право гражданина самому решать, какие события и обстоятельства его частной жизни могут быть разглашены, в том числе и в художественном произведении» [8]. Соответственно, использование дипфейка реального гражданина или дипфейка фантазийной личности, но из образа которой достоверно можно узнать реального гражданина, даже в художественных целях, должно охраняться тайной частной жизни.

Проблемы правового регулирования дипфейка являются предметом исследования как с точки зрения уголовного права (М. М. Долгиева [3], К. Ю. Яковлева [14]), так и гражданского права (В. О. Калятин [5], И. Н. Самойлов, Д. Ю. Камышанский [11], К. М. Глинкова [2], В. А. Виноградов, Д. В. Кузнецова [1]).

Несмотря на то, что технология искусственного интеллекта создания дипфейков достаточно молодая, она уже широко распространена. Соответственно, необходимо комплексно рассмотреть некоторые проблемы применения этой технологии гражданами и предпринимателями. Прежде всего, исследуем, как технология дипфейка активно внедряется в индустрию развлечений. Как справедливо отмечает В. О. Калятин, дипфейки вошли в нашу жизнь не только как новый вид нарушений, но и как важный инструмент, расширяющий творческие возможности человека [5]. Эта технология активно применяется в рекламе. Например, в социальной рекламе о борьбе с малярией футболист Дэвид Бекхэм обращается к зрителям на девяти языках, благодаря искусственной интеллекту генерации голоса. В марте 2022 года американский актёр Брюс Уиллис завершил свою карьеру, но при этом передал права на использование своего «цифрового двойника» компании Deepcake для использования как в рекламных видео, так и в фильмах или сериалах. В частности, его образ использовался оператором сотовой связи «Мегафон» в своей рекламе. С помощью искусственного интеллекта были восстановлены утраченные части картины Рембрандта «Ночной дозор», которые были отрезаны в 1715 году, чтобы поместить картину в зал ратуши (на основании сохранившейся копии голландского художника Геррита Ланденса). Современный российский кинематограф также активно использует эту технологию. Так, в фильме «Диверсант: Идеальный штурм» с помощью данной технологии воссоздан герой Владислава Галкина — майор Калтыгин, или дипфейк Юрия Никулина в фильме «Манюня: Приключения в Москве». Однако не все представители культуры выступают за применение данной технологии. Так, Борис Галкин в интервью сказал: «Когда уже увидел, ахнул. Напрасные хлопоты. Кроме смущения и отторжения ничего не вызвало»[2]. Соответственно, киноиндустрия широко использует технологию дипфейка для создания развлекательного контента, видя в этом новые возможности, но представители актёрской профессии видят угрозу обесценивания человеческого труда. Криминологи выстраивают концепции борьбы с «нежелательным контентом». При этом следует признать, что, видя дипфейк реального человека, даже если у нас есть возможность понять это, мы отождествляем дипфейк с самим человеком. Соответственно, дипфейк можно признать частью цифрового образа человека. А использование дипфейка частью цифровой идентификации гражданина. Следует признать справедливость требования ряда стран проводить маркировку такого видео и осуществлять контроль за таким контентом. Примером может служить законодательство Китая [4] и Франции[3].

[1] Отчёт Pindrop об отношении потребителей к дипфейка и клонированию голоса 2023 год, Deepfake and Voice Clone Consumer Sentiment Report 2023, Voicebot Research. URL: file:///C:/Users/пользователь/Downloads/2023 %20Отчет%20об%20отношении%20потребителей%20к%20дипфейкам%20и%20клонированию%20голоса%202023 %20Deepfake%20and%20Voice%20Clone%20Consumer%20Sentiment%20Report%202023.pdf

[2] Смущение и отторжение: отец Владислава Галкина прокомментировал «воскрешение» сына. URL: https://rg.ru/2023/05/09/smushchenie-i-ottorzhenie-otec-vladislava-galkina-prokommentiroval-voskreshenie-syna.html

[3] French Avia law declared unconstitutional: what does this teach us at EU level? // EDRi. 2020. 24 June. URL: https://edri.org/our-work/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/

Соотношение дипфейка как части цифрового образа физического лица и авторских прав на произведение

В литературе высказано мнение, что видеоролик, созданный с использованием технологии дипфейка должен рассматриваться как аудиовизуальное произведение, т. е. как объект авторского права. За основу наших рассуждений можно взять спор между обществом «Бизнес-аналитика» и обществом «Рефейс Технолоджис». Ответчик использовал в сети Интернет аудиовизуальное произведение (рекламный ролик), исключительное право на которое принадлежит истцу. По мнению «Бизнес-аналитики», на такое видео не распространяется авторское право, поскольку его создали с помощью нейросети. Моушен-дизайнер наложил на исходный материал лицо известного актёра Киану Ривза. По мнению двух инстанций, технология дипфейк — не способ создания видеоматериалов, а дополнительный инструмент обработки контента. Частичное преобразование произведения с помощью нейросетей не свидетельствует о том, что авторы не вносили творческий вклад. Поэтому суд взыскал компенсацию с ответчика 500 000 рублей за незаконное использование чужого творческого труда[1]. В соответствии со статьёй 1263 ГК РФ аудиовизуальным произведением является произведение, состоящее из зафиксированной серии связанных между собой изображений (с сопровождением или без сопровождения звуком) и предназначенное для зрительного и слухового (в случае сопровождения звуком) восприятия с помощью соответствующих технических устройств. Аудиовизуальные произведения — это кино-, теле- и видеофильмы и другие подобные произведения, независимо от способа их первоначальной или последующей фиксации. Каждый автор произведения, вошедшего составной частью в аудиовизуальное произведение, как существовавшего ранее (автор произведения, положенного в основу сценария, и другие), так и созданного в процессе работы над ним (оператор-постановщик, художник-постановщик и другие), сохраняет исключительное право на своё произведение, но при этом они не могут отозвать части своего произведения или запретить использование этого произведения. Поэтому видеоролики, созданные группой авторов (сценаристом, видеооператором, моушн-дизайнером, актёром) является аудиовизуальным произведением. В свою очередь технология дипфейка — это всего лишь дополнительный инструмент обработки (технического монтажа) видеоматериалов, используемый моушн-дизайнером. Соответственно, сам объект (пример, воссоздание персонажа), созданный таким образом, навряд ли можно считать объектом авторского права, скорее это объект смежных прав. Это обусловлено тем, что к объектам смежных прав не применим критерий оригинальности. Также, как и с исполнением артиста, который давно известен как объект смежных прав, полной идентификацией произведения как объекта авторского права с исполнением не происходит. Так А. Л. Маковская обращает внимание на то, что признание авторства произведения обусловлено творческим характером, права исполнителя обусловлены призванием авторства исполнителя [9]. Смежные права традиционно носят технический организационный характер и зависят от соблюдения авторских прав, поэтому и носят название «смежные» (ст. 1303 ГК РФ). К. М. Глинкова предлагает считать дипфейки производными произведениями, так как авторы представляют креативное, нестандартное, ранее не виданное и никем не воображаемое произведение [2]. Но этот аргумент спорный, так как именно близость к образу стремится достигнуть создатель. При этом при создании и использовании такого объекта нельзя не учитывать, что образ, который использовался при создание дипфейка затрагивает сферу нематериальных благ физического лица. А то, что «говорит» такой дипфейк, в каких роликах используется и какие идеи продвигает — это уже сфера частной жизни гражданина. Соответственно, сам дипфейк как объект смежных прав может считаться частью цифровой идентификации физического лица. Недопустимо использовать такой дипфейк для продвижения тех идей, которые сам граждан не разделял. Соответственно, в случае смерти физического лица создание дипфейка возможно с согласия наследников, но только в рамках идей, взглядов умершего, а не наследников, при условии, что гражданин не оставил завещательное распоряжение о запрете создание дипфейка после его смерти.

Публичные интересы, персональные данные и право на частную жизнь

Как известно, целью использования изображения гражданина и пределом вмешательства в его частную жизнь является публичный интерес (ст. 152.1 и ст. 152.2 ГК РФ). В соответствии в разъяснениями Верховного Суда «публичный интерес» имеет место, когда такой гражданин является публичной фигурой (занимает государственную или муниципальную должность, играет существенную роль в общественной жизни в сфере политики, экономики, искусства, спорта или любой иной области), а обнародование и использование изображения осуществляется в связи с политической или общественной дискуссией,

[1] Решение Арбитражного суда г. Москва Дело № А40-200471/23-27-1448 30 ноября 2023 г. URL: 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

или интерес к данному лицу является общественно значимым[1]. Однако для использования изображения в противоправных целях, для извлечения прибыли или для удовлетворения обывательского интереса к его частной жизни не может служить оправданием его статус как публичного лица. Соответственно, воссоздание цифрового облика гражданина может осуществляться им самим или только с его согласия. Вместе с тем использование облика исторических деятелей возможно без согласия, если имеет место публичный интерес, но при отсутствии возмездного характера отношений, пример — использование технологии дипфейка в музее[2]. На практике возникает вопрос о том, являются ли врачи или преподаватели публичными фигурами? Речь идёт о том, возможно ли создание профиля врача или преподавателя на сайте для оценки его работы. Как известно, существует множество различных рейтинговых сайтов, где благодарные или не очень благодарные клиенты и пациенты могут под профилем изложить своё мнение о профессиональных и личностных качествах врача, учителя или юриста. Если создание такого профиля инициировано самим гражданином, то модерация может касаться самого отзыва, создание же цифрового образа не вызывает сомнения. В ситуации, когда только после появления негативных отзывов гражданин узнаёт о таком рейтинговом сайте, может ставится вопрос о том, насколько законно использовали персональные данные гражданина и насколько законен сам факт создания такого цифрового образа гражданина. Е. А. Останина пишет, что «наиболее актуальной проблемой для российской практики является соотношение права на свободу слова с запретом использовать персональные данные без согласия лица, которого эти данные касаются. Практически каждый рейтинговый сайт, предлагая оценивать специалистов, указывает фамилию, имя и отчество специалиста, место работы, иногда телефон. Оптимален вариант, когда любые персональные данные будут включаться в содержание рейтинговых сайтов только с согласия управомоченного» [7]. Ещё один риск — это нарушение ст. 11 Федерального закона «О персональных данных»[3], так как сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных законом. Соответственно, использование биометрических данных реальных людей возможно только с их согласия, если цели не носят правоохранительный характер.

Выводы

Цифровой образ гражданина — фантазийный, или связанный с личностью физического лица способом аутентификации, — является частью образа физического лица. Защита права на цифровой образ может осуществляться, как нематериального блага, так и исключительного права, исходя из характера правонарушения. Цифровая идентификация физического лица как самого себя, так и других субъектов правоотношений в цифровом пространстве — это вопрос финансовой и информационной безопасности, а также добросовестного осуществления своих гражданских прав. Выработка эффективных способов защиты своего цифрового образа так же необходима, как и традиционных средств индивидуализации физического лица.

[1] О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации : постановление Пленума Верховного Суда РФ от 23.06.2015 № 25 // Российская газета. 2015. 30 июня.

[2] Примером является музей Военно-морской славы в Кронштадте. URL: https://mvms.ru/about

[3] О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ (ред. от 28.02.2025) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

Список источников

1. Виноградов В. А., Кузнецова Д. В. Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. № 2. URL: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-pravovogo-regulirovaniya-tehnologii-dipfeyk (дата обращения: 04.07.2025).

2. Глинкова К. М. Нарушение авторских прав посредством создания дипфейков в сети // Интернет ИС. Авторское право и смежные права. 2023. № 6. С. 25–45.

3. Долгиева М. М. Квалификация дипфейк-мошенничества и киберпохищения человека // Актуальные проблемы российского права. 2024. № 11. С. 106–113.

4. Дремлюга Р. И., Моисейцев В. В., Парин Д. В., Романова Л. И. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (deepfake): опыт Китая // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. № 4. URL: https://cyberleninka.ru/article/n/natsionalnoe-pravovoe-regulirovanie-ispolzovaniya-i-rasprostraneniya-realistichnyh-audiovizualnyh-poddelnyh-materialov-deepfake (дата обращения: 04.07.2025).

5. Калятин В. О. Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон. 2022. № 7. С. 87–103.

6. Кондаков А. М., Костылева А. А. Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы // Вестник РУДН. Серия: Информатизация образования. 2019. № 3. URL: https://cyberleninka.ru/article/n/tsifrovaya-identichnost-tsifrovaya-samoidentifikatsiya-tsifrovoy-profil-postanovka-problemy (дата обращения: 04.07.2025).

7. Останина Е. А. Нарушают ли рейтинги и публикуемые на сайте оценки право на репутацию и неприкосновенность частной жизни? // В сборнике: Право цифровой экономики — 2020 (16). Ежегодник-антология. Сер. «Анализ современного права / IP & Digital Law» ; руковод. и науч. ред. М. А. Рожкова. М., 2020. С. 245–270.

8. Останина Е. А. Некоторые вопросы защиты права на имя, псевдоним и неприкосновенность частной жизни // Вестник Челябинского государственного университета. Серия: Право. 2019. Т. 4, вып. 3. С. 48–50.

9. Право интеллектуальной собственности. Авторское право : учебник. Т. 2 / под ред. Л. А. Новоселовой. М. : Статут, 2017. 234 с.

10. Пучков В. О. Основные проблемы цифрового образа субъекта гражданского права в цивилистической доктрине и судебной практике // Арбитражные споры. 2020. № 3. С. 143–158.

11. Самойлов И. Н., Камышанский Д. Ю. Потенциальные и реальные угрозы технологии deepfake (дипфейк) // ИС. Авторское право и смежные права. 2024. № 4. С. 17–22.

12. Санников Д. В. Цифровой образ гражданина: анализ понятийно-категориального аппарата // Проблемы экономики и юридической практики. 2023. № 5. URL: https://cyberleninka.ru/article/n/tsifrovoy-obraz-graz (дата обращения: 04.07.2025)

13. Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5–17.

14. Яковлева К. Ю. Информационная технология «дипфейк»: понятие и доказательственное значение в уголовном процессе // Законность. 2024. № 11. С. 65–66.

References

1. Vinogradov VA, Kuznetsova DV. Foreign Experience of Legal Regulation of Deepfake Technology. *Pravo. Zhurnal Vysshey shkoly ekonomiki = Pravo. Journal of the Higher School of Economics*. 2024;(2). Available from: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-pravovogo-regulirovaniya-tehnologii-dipfeyk (accessed: 04.07.2025). (In Russ.).

2. Glinkova KM. Violation of Copyrights through the Creation of Deepfakes on the Internet. *Internet IS. Avtorskoye pravo i smezhnyye prava = Internet IP. Copyright and Related Rights*. 2023;(6):25-45. (In Russ.).

3. Dolgieva MM. Qualification of Deepfake Fraud and Cyber-Kidnapping of a Person. Aktual'nyye problemy rossiyskogo prava = Actual Problems of Russian Law. 2024;(11):106-113. (In Russ.).

4. Dremlyuga RI, Moiseyev VV, Parin DV, Romanova LI. National Legal Regulation of the Use and Distribution of Realistic Audio-Visual Fake Materials (Deepfake): China's Experience. *Aziatsko-Tikhookeanskiy region: ekonomika, politika, pravo = Asia-Pacific Region: Economics, Politics, Law*. 2022;(4). Available from: https://cyberleninka.ru/article/n/natsionalnoe-pravovoe-regulirovanie-ispolzovaniya-i-rasprostraneniya-realistichnyh-audiovizualnyh-poddelnyh-materialov-deepfake (accessed: 04.07.2025). (In Russ.).

5. Kalyatin VO. Deepfake as a Legal Problem: New Threats or New Opportunities? *Zakon = Law*. 2022;(7):87-103. (In Russ.).

6. Kondakov AM, Kostyleva AA. Digital Identity, Digital Self-Identification, Digital Profile: Statement of the Problem. *Vestnik RUDN. Seriya: Informatizatsiya obrazovaniya = Bulletin of RUDN*. Series: Informatization of Education. 2019;(3). Available from: https://cyberleninka.ru/article/n/tsifrovaya-identichnost-tsifrovaya-samoidentifikatsiya-tsifrovoy-profil-postanovka-problemy (accessed: 04.07.2025). (In Russ.).

7. Ostanina EA. Do ratings and assessments published on the website violate the right to reputation and privacy? In the collection: Pravo tsifrovoy ekonomiki — 2020 (16). Yezhegodnik-antologiya. Ser. «Analiz sovremennogo prava / IP & Digital Law» = Digital Economy Law — 2020 (16). Yearbook-Anthology. Ser. "Analysis of Modern Law / IP & Digital Law". Head and Scientific Editor MA. Rozhkova. Moscow; 2020. Pp. 245-270. (In Russ.).

8. Ostanina EA. Some Issues of Protecting the Right to a Name, a Pseudonym, and Privacy. *Vestnik Chelyabinskogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of the Chelyabinsk State University. Series: Law*. 2019;4(3):48-50. (In Russ.).

9. Pravo intellektual'noy sobstvennosti. Avtorskoye pravo = Intellectual Property Law. Copyright Law. Textbook. Vol. 2. Ed. by LA. Novoselova. Moscow: Statut; 2017. 234 p. (In Russ.).

10. Puchkov BO. The Main Problems of the Digital Image of a Subject of Civil Law in Civil Law Doctrine and Judicial Practice. *Arbitrazhnyye spory = Arbitration Disputes*. 2020;(3):143-158. (In Russ.).

11. Samoilov IN, Kamyshansky DY. Potential and real threats of deepfake technology. *IS. Avtorskoye pravo i smezhnyye prava = IS. Copyright and related rights*. 2024;(4):17-22. (In Russ.).

12. Sannikov DV. The digital image of a citizen: an analysis of the conceptual and categorical apparatus. *Problemy ekonomiki i yuridicheskoy praktiki = Problems of economics and legal practice*. 2023;(5). Available from: https://cyberleninka.ru/article/n/tsifrovoy-obraz-graz (accessed: 04.07.2025). (In Russ.).

13. Talapina ZV. Law and Digitalization: New Challenges and Prospects. Zhurnal rossiyskogo prava = Journal of Russian Law. 2018;(2):5-17. (In Russ.).

14. Yakovleva KYu. Information Technology "Deepfake": Concept and Evidential Significance in Criminal Procedure. Zakonnost' = Legality. 2024;(11):65-66. (In Russ.).

Информация об авторе

Н. А. Новокшонова — кандидат юридических наук, доцент, доцент кафедры гражданского права и процесса Института права.

Information about the author

N. A. Novokshonova — Candidate of Legal Sciences, Associate Professor, Associate Professor of the Department of Civil Law and Procedure of the Institute of Law.

Статья поступила в редакцию 05.07.2025. Одобрена после рецензирования 25.07.2025. Принята в печать 25.07.2025.

The article was submitted 05.07.2025; approved after reviewing 25.07.2025; accepted for publication 25.07.2025.

Автор заявляет об отсутствии конфликта интересов.

The author declares no conflict interest.