

Дата поступления рукописи в редакцию: 02.04.2026 г.
Дата принятия рукописи в печать: 21.04.2026 г.

DOI: 10.24412/3033-7518-2026-1-27-30

ДОМНИНА Анастасия Валерьевна,
старший преподаватель
кафедры конституционного и муниципального права юридического факультета,
Нижегородский государственный университет им. Н.И. Лобачевского,
e-mail: anastasiy-domnina@yandex.ru

КОРОВКИНА Елизавета Алексеевна,
студентка юридического факультета,
Нижегородский государственный университет им. Н.И. Лобачевского,
e-mail: el_korovkina@mail.ru

ДИПФЕЙКИ КАК УГРОЗА КОНСТИТУЦИОННОМУ ПРАВУ НА ИНФОРМАЦИЮ

Аннотация. Научное исследование посвящено проблеме реализации права граждан на достоверную информацию в условиях стремительного развития технологий искусственного интеллекта, а именно – феномену дипфейков. Отмечается, что, не являясь субъектом правоотношений, искусственный интеллект выступает инструментом, трансформирующим информационную среду и создающим новые угрозы. Дипфейки, представляющие собой синтезированный контент, обладают высоким криминогенным потенциалом, так как их распространение вводит общественность в заблуждение и делает невозможной верификацию данных. В статье проводится анализ норм российского законодательства, направленных на регулирование данной сферы. В ходе научного исследования выявлен правовой пробел: действующие нормы не учитывают специфику дипфейков, что порождает сложности в доказывании умысла и квалификации деяний. Рассматривается судебная практика, которая демонстрирует защиту имущественных прав, но оставляет без внимания вопросы информационной безопасности. На основе анализа зарубежного опыта обосновывается необходимость заимствования превентивных механизмов регулирования. В качестве превентивной меры предлагается введение обязательной маркировки контента, созданного с помощью искусственного интеллекта, что позволит обеспечить прозрачность и безопасность информационного пространства и защитить конституционное право граждан на достоверную информацию.

Ключевые слова: искусственный интеллект, правовое регулирование, право на информацию, дипфейки, маркировка контента.

DOMNINA Anastasia Valeryevna,
senior lecturer
at the Department of Constitutional and Municipal Law of the Law Faculty
of the Lobachevsky State University of Nizhny Novgorod

KOROVKINA Elizaveta Alekseevna,
student of the Law Faculty
of the Lobachevsky State University of Nizhny Novgorod

DEEPFAKES AS A THREAT TO THE CONSTITUTIONAL RIGHT TO INFORMATION

Annotation. This scientific study examines the problem of realizing citizens' right to reliable information in the context of the rapid development of artificial intelligence technologies, specifically focusing on the phenomenon of deepfakes. It is noted that, while not being a subject of legal relations, artificial intelligence acts as a tool that transforms the information environment and creates new threats. Deepfakes, representing synthesized content, possess high criminogenic potential, as their dissemination misleads the public and makes data verification impossible. The article analyzes the provisions of Russian legislation aimed at regulating this area. The research identifies a legal gap: current norms don't account for the specific nature of deepfakes, which creates difficulties in proving intent and qualifying acts. The study examines judicial practice, which demonstrates the protection of property rights but leaves information security issues

unaddressed. Based on an analysis of foreign experience, the necessity of adopting preventive regulatory mechanisms is substantiated. As a preventive measure, the introduction of mandatory labeling for content created using artificial intelligence is proposed, which would ensure the transparency and security of the information space and protect citizens' constitutional right to reliable information.

Key words: artificial intelligence, legal regulation, right to information, deepfakes, content labeling.

В условиях стремительной цифровизации общества искусственный интеллект (далее также – ИИ) оказывает значительное влияние на все сферы общественной жизни человека, затрагивая и его информационные права. Однако искусственный интеллект не является субъектом общественных отношений, его правовой статус еще предстоит детально осмыслить законодателью в ближайшем будущем [6, с. 111]. Информационные права человека – комплекс прав и свобод, связанный с использованием, распространением и защитой информации. Искусственный интеллект выступает не только инструментом, оптимизирующим обработку информации, но и фактором, модифицирующим истинную природу информационных прав.

В этой связи важно обратить внимание на влияние ИИ на право граждан на достоверную информацию. Интересен феномен создания «дипфейков» (deepfakes – «глубокие подделки»). Дипфейки – это преднамеренно искаженные аудио, видео или иные файлы с использованием технологии глубокого изучения (определение производное от словосочетания «deep learning» – глубокое изучение, «fake» – подделка), которые изображают что-то вымышленное или ложное, что позволяет злоумышленникам использовать новый и сложный инструмент социальной инженерии [5, с. 74]. По сути, природа дипфейка обладает общественной опасностью. Опасность представляет не сама технология, а использование результатов без указания на генерацию такого контента. Распространение цифровых подделок влечет серьезные юридические последствия, угрожая информационной безопасности личности, общества и государства.

Это, в свою очередь, порождает принципиально новую проблему – практически невозможное разоблачение такого рода медиапродукта. Вследствие этого формируется «благоприятная почва» для распространения ложной информации.

В последнее время технология дипфейк привлекла к себе внимание юридического сообщества [4, с. 64]. Правовое регулирование создания, распространения и использования такого контента прямо диктует формирование отдельного правового института. В Российской Федерации основными инструментами регулирования выступают нормы об административной ответственности за распространение заведомо ложной общественно значимой информации (статья 13.15 КоАП РФ) и уголовные статьи о клевете (статья 128.1 УК РФ), публичном распространении заведомо ложной информации об обстоятельствах,

представляющих угрозу жизни и безопасности граждан, и об использовании заведомо подложных документов (статьи 207.1, 207.2 и 327 УК РФ). Однако данные нормы не учитывают специфику общественной опасности таких материалов. В частности, возникают сложности с доказыванием умысла и определением момента, когда фейковый материал становится общественно опасным.

Особый интерес возникает к проблеме установления уголовной ответственности за совершение преступлений с использованием такой технологии. В данном вопросе нет однозначной позиции. С одной стороны, комиссия Правительства РФ по законопроектной деятельности не поддержала законопроект о введении уголовной ответственности за распространение дипфейков [8]. С другой стороны, Генеральная прокуратура Российской Федерации предусмотрела учет дипфейков в качестве средств, используемых при совершении преступлений (код 049 «с использованием технологии дипфейк» в справочнике № 25-ГП «предметы, устройства и другие средства, использованные при совершении преступлений», утвержденный Приказом Генпрокуратуры России от 09.12.2022 № 746 «О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре» [9]). Учет дипфейков в статистике Генпрокуратуры – важный шаг, но он не отменяет необходимости совершенствования законодательства в данной области.

Кроме того, в 2024 г. в целях обеспечения защиты персональных данных и охраны частной жизни лица в календарь рассмотрений Государственной Думы на 20 февраля 2024 г. был внесен Законопроект № 502113-8 «О внесении изменений в УК РФ», который прошел первое чтение [3, с. 119]. В дальнейшем предложенные изменения были внесены в УК РФ, но так и не решили проблему дипфейков.

В отличие от Российской Федерации, международное регулирование дипфейков уже находится в стадии активного формирования. Наблюдается становление нескольких моделей регулирования. В Китае, например, реализуется наиболее жесткий административно-уголовный подход, где с 2023 года действуют специальные положения об обязательной маркировке такого контента и предусматривающие ответственность за его использование в целях, подрывающих общественный порядок или права личности. Европейский Союз (далее – ЕС) выбрал путь комплексного регулирования, где ключевую роль играет Закон об искусственном интеллекте (AI Act). Это

одна из первых предпринятых попыток по закреплению на законодательном уровне норм функционирования системы искусственного интеллекта и введению ответственности за принятые ими решения [1, с. 97]. Он устанавливает жесткие требования прозрачности и обязательной маркировки сгенерированного контента, а также строгие санкции за их нарушения.

Рассматривая современную обстановку в России, где, с одной стороны, органы публичной власти уделяют внимание данной проблеме, а с другой – законодатели проявляют осторожность и предусмотрительность в установлении уголовной ответственности, своевременным и разумным решением могло бы стать заимствование ключевого принципа из Закона об искусственном интеллекте ЕС – обязательный маркировки контента, созданного или существенно измененного с помощью ИИ. Этот подход, уже реализованный в качестве общеевропейского стандарта, представляет собой превентивную и регуляторную модель, которая не предполагает уголовное преследование за факт создания технологии, но устанавливает правила ограничения распространения такого контента. Для России внедрение подобного требования стало бы логичным решением проблемы; такой подход гармонично вписался бы в текущее правовое регулирование, так как он не требует существенного изменения правовых норм, но при этом фокусируется на профилактике создания и распространения дипфейков. К тому же, внедряя нормы о маркировке, Россия может одновременно стимулировать развитие отечественных технологий по распознаванию сгенерированного общественно опасного контента. В далеком будущем возможна и разработка профильного законодательства о системах «глубоких подделок» и распределении ответственности за их создание и распространение.

Интересна судебная практика по данному вопросу. Судебное дело № А40-200471/2023, рассмотренное Арбитражным судом г. Москвы с последующим подтверждением в апелляционной и кассационной инстанциях – наглядный пример того, как российская правовая система всё-таки столкнулась с необходимостью квалификации материалов, созданных с помощью технологии deepfake. Истец – компания, создавшая рекламный ролик, где с помощью нейросети лицо известного актера было наложено на тело другого человека. Ответчик использовал это видео без разрешения, утверждая, что продукт нейросети не является объектом авторского права, так как творческий вклад человека минимален или вообще отсутствует.

Суды трех инстанций единогласно отвергли данную позицию. Они постановили, что технологии Deep-fake – это дополнительный инструмент обработки (технического монтажа) видеоматериалов, а не способ их создания [10]. Конечно, готовый ролик был защищен авторским правом, а его

использование без согласия признано нарушением такого права. Однако суд рассматривал спор исключительно в рамках защиты имущественных прав. При этом спорный вопрос о законности использования остался без внимания. Исходя из этого, дипфейк – искусственный медиапродукт, который свободно может использоваться для распространения заведомо ложной информации, введения людей в заблуждение и манипулирования общественным мнением. В этом контексте такая технология создает реальную угрозу реализации конституционному праву на информацию.

С учётом вышеизложенного криминогенный потенциал такого рода контента крайне сложно переоценить, особенно с учётом степени осведомлённости среднестатистического пользователя и в условиях дефицита правовой регламентации технологий и результатов синтеза в отечественной правовой системе [2, с. 36].

Таким образом, развитие информационно-коммуникационных технологий неминуемо приводит к ситуациям, угрожающим обеспечению прав человека. Ни технические, ни законодательные, ни этические препятствия не способны полностью устранить эту проблему [7, с. 128]. В частности, технологии «глубоких подделок» (deepfakes) создают вызовы для реализации права граждан на достоверную информацию, которые проявляются в сложности верификации достоверного контента и потери доверия к информации в цифровой среде. Анализ судебной практики наглядно демонстрирует отставание правового регулирования от стремительно развивающихся общественных отношений. Это проявляется, например, в отсутствии законодательного определения «дипфейк» и процессуальных аспектов экспертизы по выявлению такого рода контента. В этой связи маркировка сгенерированного контента – наиболее эффективный механизм для обеспечения прозрачности информационного потока. Очевидно, что искусственный интеллект – это не только катализатор цифровизации общества и государства, но и препятствие для реализации конституционных прав человека и гражданина. Однако масштаб проблемы достаточно шире: автоматизированные системы, основанные на ИИ, все чаще ограничивают доступ граждан к информации, но данная тема заслуживает внимания в рамках отдельного научного исследования.

Список литературы:

[1] Белов И.И. Закон Европейского союза об искусственном интеллекте: вызовы и возможности для управления документацией // Вестник ВНИИ-ДАД. 2024. № 6. С. 96-106.

[2] Бодров Н.В., Лебедева А.К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. № 11. С. 26-39.

[3] Жарова А.К. Технология дипфейк: вопросы охраны неприкосновенности частной жизни лица и

защиты персональных данных // Информационное общество. 2024. № 5. С. 114-122.

[4] Жарова А.К. Технология дипфейк: социально-правовые риски нарушения частной жизни лица и правовые решения // Правопорядок: история, теория, практика. 2025. № 2. С. 63-68.

[5] Игнатенков Г.К. Технология дипфейк как угроза информационной безопасности // Наука. Исследования. Практика: Сборник избранных статей по материалам Международной научной конференции. 2022. С. 74-77.

[6] Ковалева Н.Н., Жирнова Н.А. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта // Журнал российского права. 2024. Т. 28, № 7. С. 109-121.

[7] Михайлов М.А., Кокодей Т.А. Цифровые инновации и права человека: дилеммы международной правоохранительной практики // Правоприменение. 2022. Т. 6, № 3. С. 120-133.

[8] В правительстве не поддержали законопроект об уголовной ответственности за дипфейки // Информационное агентство ТАСС. URL: <https://tass.ru/obschestvo/17922853> (дата обращения: 01.02.2026).

[9] Приказ Генпрокуратуры России от 09.12.2022 N 746 «О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре» (вместе с «Положением о государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре», «Инструкцией о порядке предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в государственную автоматизированную систему правовой статистики», «Правилами заполнения учетных документов, используемых для предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в государственную автоматизированную систему правовой статистики»). // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_433986/ (дата обращения: 01.02.2026).

[10] Постановление Девятого арбитражного апелляционного суда от 08.04.2024 № 09АП-642/2024 по делу № А40-200471/2023 // СПС «КонсультантПлюс». URL: <https://clcl.ru/kNUic> (дата обращения: 02.02.2026).

References:

[1] Belov I.I. The European Union Law on Artificial

Intelligence: Challenges and Opportunities for Document Management // VNIIDAD Bulletin. 2024. No. 6. pp. 96-106.

[2] Bodrov N.V., Lebedeva A.K. The Concept of Deepfake in Russian Law, Classification of Deepfakes and Issues of Their Legal Regulation // Legal Research. 2023. No. 11. pp. 26-39.

[3] Zharova A.K. Deepfake Technology: Issues of Protecting the Inviolability of an Individual's Privacy and Protecting Personal Data // Information Society. 2024. No. 5. pp. 114-122.

[4] Zharova A.K. Deepfake Technology: Social and Legal Risks of Violating an Individual's Privacy and Legal Solutions // Law and Order: History, Theory, Practice. 2025. No. 2. Pp. 63-68.

[5] Ignatenkov G.K. Deepfake Technology as a Threat to Information Security // Science. Research. Practice: Collection of Selected Articles Based on the Proceedings of the International Scientific Conference. 2022. Pp. 74-77.

[6] Kovaleva N.N., Zhimova N.A. Problems of Ensuring the Confidentiality of Personal Data When Using Artificial Intelligence Systems // Journal of Russian Law. 2024. Vol. 28, No. 7. Pp. 109-121.

[7] Mikhailov M.A., Kokodey T.A. Digital Innovations and Human Rights: Dilemmas of International Law Enforcement Practice // Law Enforcement. 2022. Vol. 6, No. 3. Pp. 120-133.

[8] The government did not support the bill on criminal liability for deepfakes // TASS Information Agency. URL: <https://tass.ru/obschestvo/17922853> (date accessed: 01.02.2026).

[9] Order of the Prosecutor General's Office of Russia dated 09.12.2022 N 746 «On the state unified statistical accounting of data on the state of crime, as well as on reports of crimes, investigative work, inquiry, prosecutorial supervision» (together with the «Regulation on the state unified statistical accounting of data on the state of crime, as well as on reports of crimes, investigative work, inquiry, prosecutorial supervision», «Instructions on the procedure for providing primary statistical data on the state of crime, on reports of crimes, investigative work and inquiry to the state automated system of legal statistics», «Rules for filling out accounting documents used to provide primary statistical data on the state of crime, on reports of crimes, investigative work and inquiry to the state automated system of legal statistics»). // SPS «ConsultantPlus». URL: https://www.consultant.ru/document/cons_doc_LAW_433986/ (accessed: 01.02.2026).

[10] Resolution of the Ninth Arbitration Court of Appeal dated 08.04.2024 No. 09AP-642/2024 in case No. A40-200471/2023 // SPS «ConsultantPlus». URL: <https://clcl.ru/kNUic> (accessed: 02.02.2026).