Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. Т. 24, № 4. С. 91–104.
Pacific Rim: Economics, Politics, Law. 2022. Vol. 24, no. 4. P. 91–104.

ПРАВО

Научная статья
УДК 34.03:004.8(510)
https://doi.org/10.24866/1813-3274/2022-4/91-104

НАЦИОНАЛЬНОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ РЕАЛИСТИЧНЫХ АУДИОВИЗУАЛЬНЫХ ПОДДЕЛЬНЫХ МАТЕРИАЛОВ (DEEPFAKE): ОПЫТ КИТАЯ

Роман Игоревич Дремлюга[1], Владислав Викторович Моисейцев[2], Дмитрий Витальевич Парин[3], Лариса Ивановна Романова[4]
[1, 2, 3]Дальневосточный федеральный университет, г. Владивосток, Россия
[1]dreamluck@yandex.ru
[2]moiseitcev.vv@dvfu.ru
[3]parindv.students.dvfu@yandex.ru
[4]Сибирский федеральный университет, г. Красноярск, Россия,
larisa.i.romanova@mail.ru

Аннотация. Использование искусственного интеллекта в большинстве сфер общественной жизни стало повседневной реальностью. Современные технологии, имея ряд неоспоримых преимуществ, выражающихся в повышении экономической производительности, снижении издержек, эффективности государственного управления, оптимизации административно-распорядительных функций, тем не менее представляют собой опасность. Высокая распространённость технологий искусственного интеллекта среди широкой публики, простота их применения открывают возможности для использования достижений технологического прогресса не только во благо, но и в неправомерных и преступных целях. Свидетельством такого дуализма технологического прогресса в полной мере выступает методика генерации реалистичных аудиовизуальных поддельных образов и материалов посредством применения искусственного интеллекта (технология «смены лица», или дипфейк). Технологии, с помощью которых можно генерировать фальшивые аудиовизуальные материалы, на сегодняшний день достаточно «популярны» для использования в преступной среде. Применение технологий искусственного ин-

теллекта для генерации фальшивого контента неизбежно ставит вопрос о необходимости правового регулирования этой данной сферы. Одним из направлений в области регулирования создания и использования поддельных реалистичных аудиовизуальных образов и материалов является введение полного запрета и установление уголовной и административной ответственности за незаконные манипуляции с фальшивым цифровым контентом. В связи с этим особый интерес представляет опыт Китайской Народной Республики в сфере регулирования дипфейков. Законодателем Китая был избран иной путь для формирования национальной правовой базы использования технологий «смены лица». В статье рассматриваются принятые и предложенные для принятия правовые акты Китая, регламентирующие создание и распространение поддельных аудиовизуальных материалов. Анализ показывает, что китайский законодатель отказался от полного запрета дипфейков, однако определил ряд специальных правил для их использования. Одними из них выступают обязательная маркировка сгенерированных искусственным интеллектом материалов, а также наложение ряда дополнительных обязанностей на операторов и поставщиков информационных услуг. Принятые положения имеют одну цель – не допустить использование дипфейков в неправомерных целях, а именно для подрыва общественного порядка и государственного строя, а также в целях нарушения прав граждан (право на изображение, право на честь и достоинство, право на неприкосновенность частной жизни). Осознавая опасность использования технологии «смены лица», законодатель Китайской Народной Республики также установил ответственность за неправомерное создание и распространение поддельных аудиовизуальных образов и материалов: гражданско-правовую, уголовную. Авторы полагают, что подход законодателя Китая к регулированию дипфейков является наиболее оптимальным и отвечающим требованиям современности, а потому может стать примером построения национального правового регулирования этой сферы.

Ключевые слова: искусственный интеллект, поддельные реалистичные аудиовизуальные материалы, киберправо, право Китайской Народной Республики, право информационных технологий, развитие правового регулирования, неправомерное вмешательство в сферу прав и свобод человека и гражданина, компьютерные преступления.

Финансирование. Работа выполнена при финансовой поддержке ДВФУ (Программа стратегического академического лидерства «Приоритет-2030»: Центр цифрового развития) и при содействии Дальневосточного центра искусственного интеллекта ДВФУ (центр создан совместно с ПАО Сбербанк).

Для цитирования: 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. Т. 24, № 4. С. 91–104. https://doi.org/10.24866/1813-3274/2022-4/91-104

LAW

Original article

NATIONAL LEGAL REGULATION OF THE USE AND DISSEMINATION OF REALISTIC AUDIOVISUAL FAKE MATERIALS (DEEPFAKES): CHINA'S EXPERIENCE

Roman Igorevich Dremlyuga[1], Vladislav Viktorovich Moiseitsev[2], Dmitry Vitalievich Parin[3], Larisa Ivanovna Romanova[4]

[1, 2, 3]Far Eastern Federal University, Vladivostok, Russia

[1]dreamluck@yandex.ru

[2]moiseitcev.vv@dvfu.ru

[3]parindv.students.dvfu@yandex.ru

[4]Siberian Federal University, Krasnoyarsk, Russia, larisa.i.romanova@mail.ru

Abstract. The use of artificial intelligence in most areas of public life has become an everyday reality. Modern technologies, having a number of indisputable advantages, expressed in increasing economic productivity, reducing costs, efficiency of public administration, optimization of administrative and administrative functions, nevertheless pose certain risks. The mass dissemination of artificial intelligence technologies among the general public and the simplification of their application open up the possibility of using the achievements of technological progress for illegal and criminal purposes. Such dualism of technological progress is fully proven by the method of generating realistic audiovisual fake images and materials by artificial intelligence (the technology of 'face change' or deepfakes), which has already gained great 'popularity' for its use in the criminal environment. The use of artificial intelligence technologies, no matter for what purposes, inevitably raises the question of the need for regulatory legal regulation of this new sphere. Deepfake technologies are no exception. One of the proposed directions, and the most widespread for regulating the creation and use of fake realistic audiovisual images and materials involves a complete ban and the establishment of criminal and administrative responsibility. In this regard, the experience of the People's Republic of China in the field of regulation of deepfakes is of particular interest. The legislator of China has chosen a different way to form a national legal framework for the use of 'face change' technologies. The article discusses the adopted and proposed for adoption legal acts of China

regulating the creation and distribution of fake audiovisual materials. The analysis shows that the Chinese legislator refused to completely ban deepfakes, but defined a number of special rules for their use. One of them is the mandatory labeling of materials generated by artificial intelligence, as well as the imposition of a number of additional responsibilities on operators and information service providers. The adopted provisions have one goal – to prevent the use of deepfakes for illegal purposes, namely to undermine public order and the state system, as well as to violate the rights of citizens (the right to image, the right to honor and dignity, the right to privacy). Realizing the danger of using the technology of 'face change', the legislator of the People's Republic of China also established responsibility for the illegal creation and distribution of fake audiovisual images and materials: civil and criminal. The authors believe that the approach of the Chinese legislator to the regulation of deepfakes is the most optimal one and meets the requirements of modernity, and therefore can become an example of building a national legal regulation of this sphere.

Keywords: artificial intelligence, deepfake, cyber law, China law, information technology law, development of legal regulation, unlawful interference in the sphere of human and civil rights and freedoms, computer crime.

Financial Support. The work was supported by FEFU (Strategic Academic Leadership Program "Priority 2030": Center for Digital Development) and with the assistance of the Far Eastern Center for Artificial Intelligence of FEFU (the center was created jointly with Sberbank).

For citation: Dremlyuga R. I., Moiseitsev V. V., Parin D. V. National legal regulation of the use and dissemination of realistic audiovisual fake materials (deepfake): China's experience // Pacific RIM: Economics, Politics, Law. 2022. Vol. 24, no. 4. P. 91–104. https://doi.org/10.24866/1813-3274/2022-4/91-104

Одним из популярнейших явлений в традиционной Сычуаньской опере в Китае является танец «бяньлянь» («смена лица») с мгновенной сменой танцором нескольких масок традиционных персонажей. Развитие цифровых технологий возродило этот вид традиционного искусства на новом уровне, позволяя обычным людям примерить на себя самые разнообразные внешние проявления личности. Класс технологий, которые предоставляют возможность делать это, получил свою известность под именем «deepfake». В литературе под дипфейками обычно понимают методику компьютерной генерации изображения, основанной на искусственном интеллекте и использующейся для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики [1, с. 381], а также сам продукт, итоговый результат, полученный в ходе процесса генерации искусственным интеллектом и представленный в виде аудио- или видеоизображения [2, с. 1].

Исследование области использования аудиовизуальных образов, имитирующих изображение, речь реальных людей или вымышленных персонажей, за последние несколько лет приобретает всё большую популярность[1]. Распространение deepfake технологий порождает большое количество сложных проблем, решение которых может повлиять на развитие правового регулирования искусственного интеллекта в целом [3, с. 89]. Одним из пионеров всестороннего правового регулирования использования технологии имитации аудиовизуальных образов, без всякого сомнения, можно назвать Китайскую Народную Республику.

Развитие deepfake технологий и их распространённость привели к неправомерному использованию данного метода генерации изображений. В связи с этим новые смыслы обрела и традиционная китайская идиома «потеря лица». Помимо переносного значения, в цифровую эпоху у неё появился и прямой смысл: как говорят в Китае, «достаточно одной лишь фотографии, чтобы сыграть хорошую роль», а твоё лицо может достаться кому угодно. Такая «смена лица» с использованием искусственного интеллекта приводит к нарушению прав граждан, в числе которых право на изображение, право на честь и достоинство, право на неприкосновенность частной жизни [4, с. 57].

Актуальность проблемы правового регулирования отношений по поводу использования дипфейков значительно возрастает благодаря всё большему распространению технологии «распознавания лиц» (для идентификации пользователей при совершении покупок, посадке на транспорт, проходе на мероприятия и т. д.). По мере того, как лицо человека становится его «билетом» или «пропуском» к материальным благам, растёт и цена подделки изображения. Так, 20 ноября 2020 г. народный суд района Фуян г. Ханчжоу вынес решение по первому в КНР «делу о распознавании лица». В апреле 2019 г. доцент Чжэцзянского политехнического университета Го Бинь уплатил 1 360 юаней за два годовых абонемента в местный зоопарк, выбрав идентификацию по отпечаткам пальцев в качестве способа подтверждения личности при входе. При этом, помимо отпечатков пальцев, в базах данных зоопарка хранились и фотографии Го Биня, предоставленные им при оформлении абонемента. В июле того же года зоопарк в одностороннем порядке уведомил клиента о смене способа идентификации со сканирования отпечатков пальцев на распознавание лица. В противном случае зоопарк не гарантировал клиенту возможность посещения. Го Бинь посчитал, что его изображение относится к чувствительной категории персональных данных, отказался осуществлять вход в зоопарк при помощи идентификации лица и потребовал вернуть неиспользованный остаток стоимости абонемента. Суд первой инстанции поддержал истца, обязав зоопарк возвратить ему деньги, а в

[1] Согласно данным, приведённым в докладе, опубликованном компанией RealAI [5], количество статей по тематике технологии deepfake в период с 2017 г. по 2021 г. возросло в 4 раза – их число увеличилось с 1 012 до 4 559.

апелляции 9 апреля 2021 г. суд средней инстанции г. Ханчжоу также постановил удалить из базы данных зоопарка изображение лица и отпечатки пальцев Го Биня. Вместе с тем, это решение оставило и ряд вопросов, среди которых правовая защита граждан от взлома систем идентификации лица с помощью технологий deepfake [6].

Широкое применение deepfake технологий представляет угрозу не только в сфере прав и основных свобод человека и гражданина, но и в сфере государственного управления, общественной безопасности и общественного порядка. Отмечается, что широкое распространение и использование технологий «смены лиц» в ситуации отсутствия правового регулирования может привести к подрыву основ демократии, манипулированию выборами, подрыву доверия к органам государственной власти и правовым институтам, подрыву общественной безопасности и обострению социальных разногласий [7].

Аудиовизуальная поддельная информация, имитирующая объекты реальной действительности, опасна и ввиду своей масштабности и скорости распространения. Согласно результатам исследований Массачусетского технологического института, ложная информация распространяется в 6 раз быстрее, чем соответствующая действительности; охваты аудитории ложной информацией также в несколько раз превышают охваты информации правдивой [8].

Противоправное использование сгенерированных искусственным интеллектом аудиовизуальных образов, потенциальные масштабные угрозы общественной безопасности и порядка, скорость их распространения диктуют необходимость правового регулирования рассматриваемой сферы общественных отношений. Цифровая эпоха задаёт вопросы, на которые национальным законодателям необходимо оперативно искать ответы.

Злонамеренное вторжение в сферу нематериальных благ, принадлежащих каждому гражданину от рождения, привело к тому, что при подготовке проекта Гражданского кодекса КНР в отчёте конституционного и юридического комитета ВСНП «О ситуации с внесением поправок в проект раздела «Личные неимущественные права» Гражданского кодекса», датированном 20 апреля 2019 г., было указано, что использование средств информационных технологий для подделки изображения и голоса других лиц не только нарушает личные неимущественные права физических лиц, но более того, может иметь сугубо отрицательные социальные последствия. Такие деяния представляют угрозу государственной безопасности и публичным интересам. Законодателю рекомендовали сформировать «нормативный ответ» на вызванную технологией deepfake проблему «смены лица».

Столь необходимый ответ на современные реалии цифровой эпохи, выражающиеся в широком использовании deepfake технологий, был дан в ряде положений Гражданского кодекса КНР, принятого 28 мая 2020 г. на Третьей сессии 13-го Всекитайского собрания народных представителей и вступившего в силу с 1 января

2021 г. Особое внимание в четвертой части Гражданского кодекса КНР уделяется вопросам защиты изображения и голоса физических лиц, в том числе от посягательств с использованием информационных технологий. Так, статьёй 1019 Гражданского кодекса КНР устанавливается, что никакие организации и физические лица не должны посягать на право других лиц на изображение посредством его подделывания с помощью использования средств информационных технологий; статьёй 1023 положения о защите авторских прав были распространены и на голос физических лиц [9, с. 351].

По мнению профессора Ван Лимина, одного из авторов проекта Гражданского кодекса КНР, кодекс расширил сферу охраны права на изображение. Во-первых, от определения изображения как совокупности особенностей лица законодатель перешёл к его определению через узнаваемость, тем самым включив в сферу правовой охраны также силуэты (например, заснятые при скрытой съёмке) либо совокупность движений, которые позволяют идентифицировать конкретного человека. Во-вторых, в сравнении с ранее действовавшими «Основами гражданского законодательства КНР», из Гражданского кодекса КНР исключено положение о корыстной цели использования как условие нарушения права на изображение [10, с. 48]. В пункте 139 указаний Верховного народного суда КНР «О некоторых вопросах применения «Основ гражданского законодательства КНР» говорилось, что действиями, нарушающими право гражданина на изображение, должно признаваться использование его изображения при изготовлении рекламы, товарных знаков, элементов оформления витрин и т. д., совершённое с корыстной целью и без согласия гражданина. Теперь нарушение права на изображение констатируется и в случае использования чужого изображения в целях «очернения, выставления в дурном свете или подделки с помощью средств информационных технологий» [11, с. 3].

Однако сегодня невозможно признать, что действующие положения Гражданского кодекса КНР предоставляют полную правовую защиту изображения и голоса гражданина от посягательств с использованием искусственного интеллекта. Так, например, положения статьи 1027 Гражданского кодекса КНР, регламентирующие вопрос гражданско-правовой ответственности за описание, носящие оскорбительный или клеветнический характер или нарушающие право на репутацию, не распространяются на ситуации, связанные с использованием deepfake технологий [12, с. 98].

Помимо вышеприведённых положений Гражданского кодекса КНР, отношения, связанные с распространением поддельных аудиовизуальных образов, регламентированы Правилами администрирования сервисов аудио- и видеоинформации [13], совместно изданными Управлением киберпространства Китая, Министерством культуры и туризма и Государственным управлением радио и телевидения. Данные Правила являются одним из первых нормативных правовых актов в Китае, регулирующих вопросы, возникающие при создании и использовании

поддельных аудиовизуальных материалов. Правилами не запрещается ни создание, ни использование (за исключением использования в целях распространения ложной информации и новостей) аудиовизуальных материалов, сгенерированных с помощью deepfake технологий. При этом на акторов сферы аудио- и видеоинформационных услуг возлагаются дополнительные обязанности по маркировке такой компьютерной информации. Нарушение правил маркировки является основанием для применения, в основном, мер административно-правового характера, при этом предусмотрена и уголовная ответственность [14, с. 376]. Необходимость такой маркировки объясняется публичным интересом в этом. Указанное ограничение было введено с целью предотвращения угроз национальной безопасности, нарушений социальной стабильности и общественного порядка, нарушений прав и интересов других лиц.

Важно отметить, что реалистичная подделка, на взгляд китайского законодателя, является опасной сама по себе [15, с. 207]. Этим объясняется распространение действия на сферу «цифровых фальшивок» ряда статей Уголовного кодекса КНР, прямо не регламентирующих данные вопросы. Так, например, статья 253-1 Уголовного кодекса КНР в полной мере должна распространяться на действия, направленные на незаконное получение биометрической информации лиц с целью дальнейшего её использования для создания поддельных аудио- или видеоматериалов [16, с. 42]. В случаях намеренного создания и распространения материала клеветнического характера, сгенерированного искусственным интеллектом, предполагается, что уголовная ответственность должна наступать в соответствии с положениями статьи 246 Уголовного кодекса КНР либо статьи 221 Уголовного кодекса КНР в случае порочения деловой репутации. Однако, если возможность квалификации действий по статье 221 Уголовного кодекса не вызывает больших споров, то возможность применения положений статья 246 единодушия не встречает. Традиционными способами распространения порочащих фактов являются письменный или устный, что ставит вопрос о том, можно ли рассматривать использование поддельного цифрового контента «надлежащим» способом совершения преступления [12]. При этом стоит обратить внимание на то, что перечень способов совершения преступления, предусмотренного статьёй 246 Уголовного кодекса КНР, является открытым. Единственным необходимым условием выступает достаточная серьёзность избранного способа совершения преступления. Представляется, что использование искусственного интеллекта является достаточно «серьёзным способом» для квалификации действий в качестве уголовно наказуемого деяния. Применение deepfake технологий предполагает посягательство одновременно на несколько объектов охраняемых законов: права и свободы лица в качестве основного объекта и компьютерная информация в качестве дополнительного объекта. Повышенную общественную опасность использования технологий «смены лица» обусловливает

высокая степень распространения материала в сети Интернет, а как следствие – и сложность опровержения клеветнического и фальсифицированного материала.

Принятые на сегодняшний день иные нормативные правовые акты КНР не устанавливают иных специальных правил регулирования использования deepfake технологий, отличных от приведённых в Правилах администрирования сервисов аудио- и видеоинформации. Общий запрет, отражённый в Правилах на использование информационных технологий в деятельности, запрещённой законом и иными нормативными правовыми актами, получил свою конкретизацию применительно к дипфейкам в Положении «Об управлении сетевым информационным контентом» [17], вступившем в силу 1 марта 2020 г. Статья 23 Положения устанавливает императивное требование, что пользователи услуг сетевого информационного контента, производители сетевого информационного контента и платформы сетевого информационного контента не должны использовать технологии искусственного интеллекта, в том числе deepfake технологии, для участия в деятельности, запрещённой законами и иными правилами. Запрет на распространение ложной информации и новостей, в том числе сгенерированных и созданных с помощью искусственного интеллекта, также отражён в статье 13 Положения «О регулировании алгоритмов рекомендаций информационных сервисов в интернете» [18]. Подобные запреты можно обнаружить также в муниципальных правовых актах. Так, например, статьёй 67 Положения муниципалитета Шанхая «О содействии развитию индустрии искусственного интеллекта» профильным организациям, осуществляющим разработку, применение и исследование искусственного интеллекта, запрещено применять технологию deepfake в деятельности, запрещённой законом.

Правотворческий процесс в сфере регулирования технологии «смены лица» не остановился на общих запретах и обязанности маркировать продукцию, сгенерированную искусственным интеллектом. Государственное информационное управление Интернета Китайской Народной Республики обнародовало Положение «Об управлении DeepSynthesis технологиями на информационных сервисах в интернете» [19]. Декларированная цель указанного положения заключается в содействии рациональному и эффективному использованию искусственного интеллекта в рассматриваемом аспекте. Предложенное положение можно назвать прорывным в сфере правового регулирования технологии «смены лица», поскольку это один из первых нормативных правовых актов, комплексно регулирующих использование технологии deepfake. Отдельные положения, затрагивающие сферу использования искусственного интеллекта с целью создания поддельных аудиовизуальных образов, объединяются в одно Положение, которое фактически выступает в данном случае консолидирующим актом.

Положение регулирует гораздо более широкую сферу, которая выходит за пределы регулирования технологии «смены лица». Оно направлено на установление административных правил предоставления информационных услуг в Интерне-

те, в том числе и при помощи технологии «глубокого синтеза». Положение в статье 2 раскрывает содержание технологии «глубокого синтеза» и включает в данный термин как методы генерации искусственным интеллектом голосового контента, видео, изображения (дипфейки), так и методы генерации текстов и их стилей, преобразования речи в текст, улучшения и восстановления изображения, создания и редактирования виртуальных сцен.

Вопрос использования искусственного интеллекта в целях создания и распространения поддельных аудиовизуальных образов разрешается, как и во всех вышеприведённых нормативных правовых актах. Запрещается лишь использование искусственного интеллекта в деятельности, противоречащей законам и нормативным актам (угроза национальной безопасности, нарушение социальной стабильности, нарушение общественного порядка и посягательство на законные права и интересы других). При этом вводится полный запрет на распространение некоторых видов информации. В частности, не допускается распространение информации, которая направлена на подстрекательство к подрыву государственной власти, которая угрожает национальной безопасности и социальной стабильности, которая носит непристойный характер или содержит порнографию. Отдельно устанавливается запрет на распространение поддельных аудиовизуальных материалов, посягающих на права и репутацию других лиц (право на изображение, право на неприкосновенность частной жизни и др.).

Маркировка конечного продукта, сгенерированного искусственным интеллектом, выступает необходимым элементом механизма правомерного использования технологий «глубокого синтеза». Отсутствие идентификации полученной информации в качестве поддельной влечёт за собой прекращение её передачи, осуществить которое обязаны поставщики информационных услуг. Помимо маркировки на поставщиков информационных услуг налагается ряд дополнительных обязанностей по проверке подлинности идентификационной информации пользователей услуг DeepinSynthesis, усиления управления технологиями искусственного интеллекта, совершенствования механизма распространения слухов для борьбы с незаконной и нежелательной информацией. Неисполнение обязанностей влечёт за собой наложение штрафа от 10 000 до 100 000 юаней, а в отдельных случаях и наступление уголовной ответственности.

Подход в сфере правового регулирования Китайской Народной Республики в сфере использования технологий «дипфейка» нельзя назвать бесспорным. Вместе с тем, он достаточно логичен, прагматичен и целесообразен. Любая техническая инновация в условиях современного мира вызывает жаркие споры о необходимости разработки абсолютного новой нормативной базы, направленной на регулирование отдельных аспектов использования инноваций. В правовом дискурсе существует также тезис о полном запрете применения плодов технологического прогресса с

целью воспрепятствования возможным нарушениям прав и свобод граждан или подрыва основ государственного строя. Технология «смены лица» и споры, связанные с ней, являются ярким тому подтверждением.

Законодатель Китайской Народной Республики попытался соблюсти баланс между вышеупомянутыми крайностями, избрав путь «золотой середины». Ограничивая использование рядом административных регламентов технологии «смены лица» в неправомерных целях, законодатель Китая не ввёл абсолютного запрета на создание, использование и распространение дипфейков, которые помимо угроз несут в себе и полезный арсенал[1]. Является ли такая позиция эффективной, покажет только время.

Список источников

1. Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Сер.: Государственное и муниципальное управление. 2020. Т. 7, № 4. С. 379–386.

2. Sloot B., van der, Wagensveld Y. Deepfakes: regulatory challenges for the synthetic society // Computer law and Security review. 2022. Vol. 46. P. 1–15.

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

4. Li Jing. On the legal nature of artificial intelligence virtual idol // Zhejiang Social Science. 2020. No. 9. P. 57–63.

5. Shen Changxiang. Depth synthesis of the Top ten trend report. URL: https://book.yunzhan365.com/owjnh/zfjo/mobile/index.html.

6. The first face recognition case has been completed: it remains unclear how to avoid «face loss» and «face theft». URL: http://www.jjckb.cn.

7. Chesney B., Citron D. Deep Fakes: a looming challenge for privacy, democracy, and national security // California Law Review. 2019. Vol. 107, iss. 1753. P. 1753–1820.

8. Vosoughi S., Roy D., Aral S. The spread of true and false news online // Science. 2018. Vol. 359, iss. 6380. P. 1146–1151.

9. Гражданский кодекс Китайской Народной Республики / отв. ред. П. В. Трощинский. М.: Синосфера, 2020. 448 с.

10. Qi Xiaodan. Ten issues that should be paid attention to in the understanding and application of personality rights in the Civil Code // Law Applicable. 2020. Vol. 17. P. 48–59.

[1] Польза дипфейков подтверждается на сегодняшний день в сфере кинематографа, образования, средств массовой информации, искусства. Так, именно при помощи технологий «глубокого синтеза» была восстановлена повреждённая ещё в начале XVIII в. картина Рембрандта «Ночной дозор» или стало возможным осуществление сурдоперевода новостей без участия человека.

11. Wang Liming. The Legislative highlights, characteristics and application of the Personality Rights Compilation of the Civil Code // Law Applicable. 2020. Vol. 17. P. 3–21.

12. Mao Ning, Yang Hui. The regulatory dilemma of deep forgery technology and its legal response // Changbai Journal. 2021. Vol. 5 (221). P. 94–101.

13. The notice on the issuance of the «Regulations on the management of online audio and video information services». URL: http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/42311/44109/xgzc44115/Document/1691062/1691062.htm.

14. Дремлюга Р. И., Коробеев А. И. Борьба с распространением реалистичных аудиовизуальных поддельных материалов за рубежом (deepfake): уголовно-правовые и криминологические аспекты // Всероссийский криминологический журнал. 2021. Т. 15, №. 3. С. 372–379.

15. Дремлюга Р. И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: монография. М., 2022. 328 с.

16. Zhou Zhi-yi. The Criminal regulation path of deepfake cybercrime // Journal of Hubei Industrial Polytechnic. 2022. Vol. 35, no 3. P. 41–48.

17. The regulations on the ecological governance of network information content shall come into force. URL: http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.

18. The internet information service algorithm recommendation management regulations. URL: http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm.

19. The regulations on the management of in-depth synthesis of internet information services (draft for solicitation of comments). URL: http://www.gov.cn/xinwen/2022-01/28/content_5671053.htm.

References

1. Ivanov V. G., Ignatovsky Ya. R. Deepfakes: perspektivy primeneniya v politike i ugrozy dlya lichnosti i natsional'noi bezopasnosti [Deepfakes: prospects for application in politics and threats to the individual and national security]. *Vestnik Rossiiskogo universiteta druzhby narodov. Ser.: Gosudarstvennoe i munitsipal'noe upravlenie*, 2020, vol. 7, no. 4, pp. 379–386. (In Russ.).

2. Sloot B., van der, Wagensveld Y. Deepfakes: regulatory challenges for the synthetic society. *Computer law and Security review,* 2022, vol. 46, pp. 1–15.

3. Kalyatin V. O. Dipfeik kak pravovaya problema: novye ugrozy ili novye vozmozhnosti? [Deepfake as a legal problem: new threats or new opportunities?]. *Zakon*, 2022, no. 7, pp. 87–103. (In Russ.).

4. Li Jing. On the legal nature of artificial intelligence virtual idol. *Zhejiang Social Science,* 2020, no. 9, pp. 57–63.

5. Shen Changxiang. Depth synthesis of the Top ten trend report. URL: https://book.yunzhan365.com/owjnh/zfjo/mobile/index.html.

6. The first face recognition case has been completed: it remains unclear how to avoid «face loss» and «face theft». URL: http://www.jjckb.cn.

7. Chesney B., Citron D. Deep Fakes: a looming challenge for privacy, democracy, and national security. *California Law Review,* 2019, vol. 107, iss. 1753, pp. 1753–1820.

8. Vosoughi S., Roy D., Aral S. The spread of true and false news online. Science, 2018, vol. 359, iss. 6380, p. 1146–1151.

9. Troshchinsky P. V. (ed.). Civil Code of the People's Republic of China. Moscow: Sinosphera Publ., 2020. 448 p. (In. Russ.).

10. Qi Xiaodan. Ten issues that should be paid attention to in the understanding and application of personality rights in the Civil Code. *Law Applicable,* 2020, vol. 17, pp. 48–59. (In Russ.).

11. Wang Liming. The Legislative highlights, characteristics and application of the Personality Rights Compilation of the Civil Code. *Law Applicable,* 2020, vol. 17, pp. 3–21.

12. Mao Ning, Yang Hui. The regulatory dilemma of deep forgery technology and its legal response. *Changbai Journal,* 2021, vol. 5 (221), pp. 94–101.

13. The notice on the issuance of the «Regulations on the management of online audio and video information services». URL: http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/42311/44109/xgzc44115/Document/1691062/1691062.htm.

14. Dremlyuga R. I., Korobeev A. I. Bor'ba s rasprostraneniem realistichnykh audiovizual'nykh poddel'nykh materialov za rubezhom (deepfake): ugolovno-pravovye i kriminologicheskie aspekty [Combating the spread of realistic audiovisual fake materials abroad (deepfake): criminal law and criminological aspects]. *Vserossiiskii kriminologicheskii zhurnal*, 2021, vol. 15, no. 3, pp. 372–379. (In Russ.).

15. Dremlyuga R. I. Ugolovno-pravovaya okhrana tsifrovoi ekonomiki i informatsionnogo obshchestva ot kiberprestupnykh posyagatel'stv [Criminal law protection of the digital economy and information society from cybercriminal attacks: monograph]. Moscow, 2022. 328 p.

16. Zhou Zhi-yi. The Criminal regulation path of deepfake cybercrime. *Journal of Hubei Industrial Polytechnic,* 2022, vol. 35, no 3, pp. 41–48. (In Russ.).

17. The regulations on the ecological governance of network information content shall come into force. URL: http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.

18. The internet information service algorithm recommendation management regulations. URL: http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm.

19. The regulations on the management of in-depth synthesis of internet information services (draft for solicitation of comments). URL: http://www.gov.cn/xinwen/2022-01/28/content_5671053.htm.

Информация об авторах

Р. И. Дремлюга – кандидат юридических наук, профессор Института математики и компьютерных технологий, директор Дальневосточного центра изучения правовых и этических аспектов искусственного интеллекта и цифровых технологий, Дальневосточный федеральный университет, г. Владивосток, Россия.

В. В. Моисейцев – специалист Службы проректора по международным отношениям ДВФУ, Дальневосточный федеральный университет, г. Владивосток, Россия.

Д. В. Парин – магистрант Юридической школы, Дальневосточный федеральный университет, г. Владивосток, Россия.

Л. И. Романова – доктор юридических наук, профессор, заслуженный работник высшей школы, профессор кафедры деликтологии и криминологии Сибирского федерального университета, г. Красноярск, Россия.

Information about authors

R. I. Dremliuga – Candidate of Law, Professor of the Institute of Mathematics and Computer Technologies, Director of Far Eastern Center for the Study of Legal and Ethical Aspects of AI and digital technologies, Far Eastern Federal University, Vladivostok, Russia.

V. V. Moiseytsev – Specialist of the Service of the Vice-Rector for International Relations, Far Eastern Federal University, Vladivostok, Russia.

D. V. Parin – master's student of School of Law, Far Eastern Federal University, Vladivostok, Russia.

L. I. Romanova – Doctor of Law, Professor, Honored Worker of Higher Education, Professor of the Department of Delictology and Criminology, Siberian Federal University, Krasnoyarsk, Russia.

Статья поступила в редакцию 03.10.2022; одобрена после рецензирования 03.11.2022; принята к публикации 10.11.2022.

The article was submitted 03.10.2022; approved after reviewing 03.11.2022; accepted for publication 10.11.2022.