

ОБЗОРЫ НАУЧНЫХ ФОРУМОВ И ИЗДАНИЙ

УДК 340.1:004
ББК 67с51

ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ФЕЙКОВИЗАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

В. В. Сорокин

Алтайский государственный университет (Барнаул, Россия)

В обзоре излагаются основные идеи, высказанные участниками Всероссийской научно-практической конференции под названием «Фейковизация Интернета, масс-медиа и рекламы: правовое противодействие», проходившей в ноябре 2024 г. Организаторы крупного научного форума с вузами Минска и Гродно (Беларусь), Херсона, Калининграда, Владивостока, Москвы, Санкт-Петербурга, Ростова-на-Дону, Саратова, Казани, Белгорода, Уфы, Воронежа, Оренбурга, Омска, а также вузов Северного Кавказа, Кубани, Крыма, Донецкой Народной Республики выражают уверенность в том, что тем самым обеспечивают технологический суверенитет России и дружественных ей стран, подготавливают нормы и процедуры для информационной безопасности личности, общества и государства. Факт проведения такой всероссийской конференции может являться примером чувства гражданской ответственности научного сообщества.

Ключевые слова: фейк, информационная безопасность, киберпространство, суверенитет, мошенничество, дискредитация, историческая память, цифровизация, экстремизм, идентификация информационного контента, международный терроризм

LEGAL COUNTERACTION TO THE FAKE INFORMATION SPACE

V. V. Sorokin

Altai State University, Barnaul

The review outlines the main ideas expressed by the participants of the All-Russian scientific and practical conference entitled «Fake Internet, mass media and advertising: legal counteraction», held in November 2024. The organizers of a major scientific forum with universities in Minsk and Grodno (Belarus), Kherson, Kaliningrad, Vladivostok, Moscow, St. Petersburg, Rostov-on-Don, Saratov, Kazan, Belgorod, Ufa, Voronezh, Orenburg, Omsk, as well as universities in the North Caucasus, Kuban, Crimea, Donetsk People's Republic express confidence that thereby they ensure the technological sovereignty of Russia and its friendly countries, prepare norms and procedures for information security of the individual, society and states. The fact of holding such an All-Russian conference may be an example of the sense of civic responsibility of the scientific community.

Keywords: fake, information security, cyberspace, sovereignty, fraud, discredit, historical memory, digitalization, extremism, identification of information content, international terrorism

Doi: [https://doi.org/10.14258/ralj\(2025\)1.18](https://doi.org/10.14258/ralj(2025)1.18)

22 ноября 2022 г. Юридический институт Алтайского государственного университета провел Всероссийскую научно-практическую конференцию под названием «**Фейковизация Интернета, масс-медиа и рекламы: правовое противодействие**».

Конференция была названа Всероссийской, однако в ее работе приняли участие семь зарубежных ученых: шесть из вузов Минска и Гродно (Республика Беларусь) и профессор из Китая — Чжао Чжэн.

Как заметил при открытии конференции директор юридического института АлтГУ, доктор юридических наук, профессор, заведующий кафедрой конституционного и международного права **Е. С. Аничкин**, «наш институт очень вовремя организовал всероссийский форум для противодействия фейковизации информационного пространства». Он напомнил, что ЮИ АлтГУ инициировал цикл больших научных конференций в 2024 г. (в феврале провели Всероссийскую научно-практическую конференцию «**Правовые вопросы воссоединения новых регионов с Российской Федерацией**» с участием ученых ДНР, ЛНР и Крыма, в мае — Международную научно-практическую конференцию «**Фронтиры правового развития в XXI веке**» с участием ученых Индонезии, Белоруссии, Киргизии, Узбекистана, Казахстана, Таджикистана). «Цифровая трансформация вывела 2023 год на рекордное количество преступлений в сфере цифровых технологий, — сообщил директор института. — По официальной статистике МВД России в 2023 г. в стране было зафиксировано более 677 тыс. IT-преступлений. В 2022 г. настоящие показатели были на треть меньше, или равнялись 522 тыс. подобных преступлений. В 2023 г. удельный вес преступлений в сфере цифровых технологий вырос до 34,8% по сравнению с 2022 г., когда удельный вес подобных преступлений составлял 26,5%. Более половины зарегистрированных преступлений, совершенных с помощью информационных технологий, относятся к категориям тяжких и особо тяжких. За 2023 г. по сравнению с предыдущим годом больше всего в абсолютном выражении выросло количество преступлений, совершенных с использованием сети Интернет. Показатели выросли с 381,1 тыс. до 526,7 тыс. Примечательно, что на втором и третьем местах оказалось мошенничество, совершенное с применением средств мобильной связи и пластиковых карт».

Ректор Алтайского государственного университета, доктор экономических наук, профессор **С. Н. Бочаров** сказал, что сейчас вузы России ищут пути опережающего развития, а «конференция Юридического института — это и есть опережающее развитие». Слова ректора вызвали бурные аплодисменты поддержки.

Заместитель Председателя Правительства Алтайского края **Ю. Г. Абдуллаев** подчеркнул важность научных рекомендаций для противодействия фейкам в таком приграничном, поликонфессиональном и многонациональном регионе, каким является Алтайский край. Им были отмечены коллективные монографии, которыми Юридический институт Алтайского государственного университета обеспечивает осязаемые результаты организуемых форумов, в том числе связь юридической науки с практикой управления и правоприменения.

Министр цифрового развития и связи Алтайского края **Е. А. Зрюмов** пришел на конференцию вместе с начальниками отделов министерства: начальником отдела информационной безопасности Министерства цифрового развития и связи Алтайского края **М. Ю. Бобиним**, начальником отдела правовой, кадровой и организационно-контрольной работы Министерства цифрового развития и связи Алтайского края **Н. В. Митькиной**, начальником сектора правовой и кадровой работы Министерства цифрового развития и связи Алтайского края **Д. В. Старцевой**. В выступлении министра была проведена убедительная связь между противодействием фейкам и безопасностью цифрового развития экономики.

Затем начальник управления юстиции Алтайского края **О. В. Грохотова** и ректор Алтайского государственного университета **С. Н. Бочаров** подписали *Соглашение о сотрудничестве между Управлением юстиции Алтайского края и Алтайским государственным университетом*.

Начальник управления печати и массовых коммуникаций Алтайского края **В. А. Киричук** в своем выступлении сказал: «Практика противодействия фейковизации у нас есть. Нам нужна теория».

Заместитель руководителя следственного управления Следственного комитета РФ по Алтайскому краю, полковник юстиции **А. А. Россоха** сделал обстоятельный доклад с анализом расследования уголовных дел, связанных с распространением фейков. Он уделил внимание важности разъяснений Верховного Суда РФ в части причинения вреда и угрозы причинения такового по данной категории уголовных дел. Для выявления такого рода преступлений в приоритетном порядке необходимо произ-

водство осмотра места происшествия, осмотра предметов (компьютера, мобильного телефона, иного технического устройства), которые могут рассматриваться как средства совершения преступления, а также назначение и производство судебных экспертиз, в том числе лингвистических, в отношении сведений, которые могут быть обнаружены.

Г. А. Василевич, заведующий кафедрой конституционного права, доктор юридических наук, профессор Белорусского государственного университета (Беларусь, г. Минск), отметил необходимость межгосударственного взаимодействия с целью разработки и принятия международного механизма сотрудничества в сфере противодействия «фейковой информации», что позволит создать унифицированный комплексный механизм, включающий международные стандарты правового и технологического характера. Это, в свою очередь, будет способствовать преодолению фрагментарности односторонних мер, принимаемых на уровне отдельных государств, и минимизации попыток превращения «медийных» технологий в орудие информационного противостояния.

Т. В. Ефимцева, зав. кафедрой предпринимательского и природоресурсного права Оренбургского института Московского государственного юридического университета им. О. Е. Кутафина, доктор юридических наук (Россия, г. Оренбург), сообщила, что по данным аналитического центра StormWall по итогам 2023 г. Россия находится на 12-м месте в рейтинге наиболее атакуемых хакерами стран мира. В целом к концу года на фоне увеличения количества DDoS-атак в мире на 43% на Российскую Федерацию было совершено на 29% больше аналогичных нападений.

Декан Гродненского государственного университета (Республика Беларусь) **С. Е. Чебуранова** отметила, что правовое противодействие фейкам представляет собой актуальную межгосударственную проблему, а в рамках Союзного государства она получает адекватную правовую оценку в рамках данной конференции.

В. Ю. Голубовский, доктор юридических наук, профессор ВНИИ МВД России (Россия, г. Москва), проанализировал статистические данные. По данным Национального агентства финансовых исследований в 2023 г. 91% россиян сталкивались с попытками мошенничества, что на 9% больше, чем годом ранее (82%). По данным Центрального банка Российской Федерации за 2022 г. мошенники похитили у россиян 14 млрд руб. Утрата профилактических возможностей произошла в связи с часто неоправданной либерализацией судебной практики, когда судами назначается даже за тяжкие преступления наказание ниже низшего предела на основании ст. 64 УК РФ [1].

В. В. Сорокин, доктор юридических наук, профессор кафедры теории и истории государства и права Алтайского государственного университета (Россия, г. Барнаул), в своем докладе отметил, что в юридическом смысле фейковизация есть распространение заведомо ложной информации под видом достоверных сведений с целью обмана и манипулирования людьми. По его мнению, было бы некорректно называть фейком любую распространяемую ложь, выдаваемую за правду. Иначе нам придется считать фейками измененные имплантами женские губы, детскую фантазию и взаимные обещания новобранцев. В юридическом аспекте фейк представляет собой заведомо ложную информацию, распространяемую в правовом пространстве, — это обстоятельство дает государству основание наказывать за фейки. Для распространения фейка не имеет значения публичность пространства. Фейки предполагают извлечение политических нематериальных и экономических материальных выгод для преступников. Заказчики и распространители фейков преследуют задачи незаконного обогащения, манипуляций сознанием и поведением, дискредитации охраняемых правом объектов. Цель фейковизации одина для всех разновидностей фейков — это причинение вреда. Фейковизация — родная сестра цифровизации, темный двойник цифровизации. Чем тотальнее, всеохватнее цифровизация общества, тем больше цифрового обмана, т. е. фейков. Фейковизация стала средством информационной войны в мире. Докладчик охарактеризовал некоторые разновидности фейков. Слух — актуальная и интересная фальшивая история. Фейковые новости — преднамеренная дезинформация. Дипфейк — фальшивое видео с помощью замены лица одного человека на другого с помощью специальных программ. Фальшивый аккаунт в интернете, который используется для обмана или манипулирования. Фотофейк — разновидность фотомонтажа.

А. А. Богустов, кандидат юридических наук, доцент Гродненского государственного университета им. Янки Купалы (Беларусь, г. Гродно), заметил, что среди нерешенных проблем правового регулирования сферы национальной безопасности на сегодняшний день назрела необходимость принятия новых международных документов в области обеспечения информационной безопасности с учетом

практики России и Беларуси в данной сфере. Предпосылками данных изменений служит неуклонный рост международной информационно-телекоммуникационной преступности, которая, в свою очередь, угрожает безопасности всех государств мира. Однако этому шагу препятствует рост конфронтации между развитыми мировыми державами, в том числе в информационной среде. Это вредит всем членам мирового сообщества. Однако по-прежнему транснациональные корыстные интересы преобладают над интересами мировой информационной безопасности.

С. А. Васильев, зав. кафедрой конституционного и административного права Севастопольского государственного университета, кандидат юридических наук, доцент (Россия, Крым, г. Севастополь), выступил с докладом на тему «СМИ и государство против фейков: правовые аспекты консолидации российского общества». Он привел примеры ответственного, законопослушного и патриотического поведения средств массовой информации. «В сфере борьбы с фейками государству необходимо координировать деятельность правоохранительных органов с деятельностью институтов гражданского общества», — подчеркнул он.

Профессор Хэйлунцзянского государственного университета (Китай) **Чжао Чжэн** рассказала, что с 1 января 2020 г. дипфейки стали преступлением в КНР. Уголовный закон предусматривает, что лицам, которые фабрикуют ложную информацию и распространяют ее через информационные сети или другие медиаплатформы с намерением нарушить общественный порядок или нанести ущерб репутации других лиц, может грозить наказание в виде тюремного заключения сроком до 3 лет или штрафа [2]. Тем самым создание дипфейков без согласия пользователей стало уголовно наказуемым, а от создателей различных интернет-платформ китайский законодатель требует четкой идентификации контента, созданного с помощью искусственного интеллекта. В Китае введена обязательная маркировка любого видео- или аудиоконтента, а также контента, созданного с использованием искусственного интеллекта и нейросетей, т. е. дипфейка. Обязанность маркировать указанный контент возлагается на поставщиков приложений и непосредственно на разработчиков. Закон КНР обязывает операторов платформ самостоятельно идентифицировать и помечать или удалять немаркированный контент, а также содержать платформу для подачи жалоб на неправомерный контент — любой контент, который наносит ущерб имиджу государства, создает угрозу национальной безопасности, подрывает экономику [3]. Интернет-платформы согласно закону КНР обязаны самостоятельно осуществлять проверку своего контента, и поскольку производство и распространение фейковых новостей запрещены, то они должны подлежать незамедлительному удалению после идентификации. Общий контроль за исполнением закона возложен на Управление киберпространства Китая. Более того, пользователь не обладает полной свободой пользования интернет-контентом, без регистрации с указанием персональных паспортных данных и номера мобильного телефона это сделать невозможно. Для использования дипфейка по отношению к конкретному лицу китайское законодательство обязывает получить сначала согласие данного лица. Таким образом, Китай пока единственное государство, которое устанавливает в первую очередь ответственность за дипфейки для разработчиков недостоверного программного продукта и на их поставщиков [4, с. 608], а не на пользователей дипфейков.

Д. В. Бугаков, судья Алтайского краевого суда, отметил, что конференцию можно расценивать как свидетельство повышенного уровня общественной опасности проблемы распространения «фейковой информации», актуальности разработки и принятия эффективного правового механизма противодействия данной угрозе. Он уделит внимание вопросу отграничения уголовных преступлений, связанных с распространением фейков, от соответствующих административных правонарушений.

Е. С. Крюкова, кандидат юридических наук, доцент кафедры криминалистики Московского государственного университета им. М. В. Ломоносова (Россия, г. Москва), затронула проблему суверенитета в киберпространстве, проблема разделена на два направления. В России и Китае действует подход, согласно которому на цифровое пространство распространяется национальный суверенитет. Экспансионистский подход США и Великобритании, напротив, сосредоточен на недопустимости распространения на него суверенитета. Неопределенность вносит тот факт, что киберпространство — это совершенно новая область, и вопрос суверенитета в киберпространстве не полностью эквивалентен сухопутному и морскому суверенитету. И, несмотря на формальное признание суверенитета в киберпространстве, его практическая реализация осложнена разобщенностью на мировом уровне и отсутствием необходимого правоприменительного опыта ввиду специфики киберпространства.

И. Ю. Панькина, кандидат юридических наук, доцент Института управления и территориально-го развития Балтийского федерального университета им. И. Канта (Россия, г. Калининград), посвятила свое выступление медиаграмотности в формировании неприятия террористической и экстремистской идеологии.

Ю. В. Холоденко, кандидат юридических наук, доцент кафедры гражданского права Алтайского государственного университета (Россия, г. Барнаул), коснулся вопросов защиты чести и достоинства граждан при распространении фейковых сообщений.

С. Р. Чеджемов, доктор педагогических наук, профессор кафедры теории и истории государства и права Северо-Осетинского государственного университета (Россия, г. Владикавказ), охарактеризовал фейки в сфере здравоохранения. Он отметил, что дискредитировать фейками пытаются не только армию, но и систему здравоохранения и другие структуры и сферы государства.

Е. Ю. Вакаева, прокурор отдела по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях и противодействии экстремизму и терроризму Прокуратуры Алтайского края, проанализировала Федеральный закон от 18 марта 2019 г. № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», который установил ответственность за размещение в информационно-телекоммуникационных сетях и средствах массовой информации заведомо недостоверной общественно значимой информации под видом достоверных сообщений. Административная ответственность за распространение фейковой (недостоверной) информации предусматривается пунктами 9, 10, 10.1 и 10.2 статьи 13.15 КоАП РФ. При этом разграничение составов указанных административных правонарушений осуществляется по вышеобозначенным пунктам ст. 13.15 КоАП РФ в зависимости от характера наступивших общественно-опасных последствий и категорий субъектов, совершивших данные действия. Так, пункты 9, 10 ст. 13.15 КоАП РФ предусматривают административную ответственность для граждан, должностных лиц и юридических лиц, в то время как пункты 10.1 и 10.2 ст. 13.15 КоАП РФ предусматривают административную ответственность только для юридических лиц. Сотрудниками правоохранительных органов выработана система способов предотвращения совершения любого компьютерного преступления. Но пока недостаточно профилактических мер, направленных на защиту компьютерных систем и их сетей, а также программного обеспечения.

Е. Н. Абрамова, кандидат юридических наук, доцент кафедры гражданского и корпоративного права Санкт-Петербургского государственного экономического университета (Россия, г. Санкт-Петербург), поделилась соображениями о гражданско-правовой квалификации цифрового образа человека. Фото обычных людей, включая детей, и общедоступных изображений стали основой для сфабрикованных видео, размещенных на сомнительных сайтах и форумах с целью нанести данным лицам психологический вред, крушение их репутации, не исключая вымогательство денег за удаление такого контента [5; с. 299].

Е. Б. Серова, зав. кафедрой уголовного процесса и криминалистики Санкт-Петербургского института (филиала) Университета прокуратуры РФ, кандидат юридических наук, доцент (Россия, г. Санкт-Петербург), посвятила свое выступление вопросам доказывания по делам о преступлениях, предусмотренных ст. 207.3 УК РФ. С целью грамотного и профессионального формирования доказательственной базы по такого рода преступлениям при осмотре места происшествия необходимо устанавливать не только наличие программы (позволяющей, например, создавать фейковые сведения, включая монтаж deep fake), но и фиксировать, с какого компьютера осуществлялось распространение информации, имелись ли технические возможности компьютера поддерживать эти программы, объемы жестких дисков, их количество, видеокарты, их уровень и другие параметры.

Ю. Ю. Малышева, кандидат юридических наук, доцент, зав. кафедрой уголовного права и криминологии Казанского института РПА Минюста РФ (Россия, г. Казань), убедительно доказала в своем докладе, что мошенничество является разновидностью фейковизации в информационном пространстве.

О. А. Попова, старший помощник прокурора Индустриального района г. Барнаула (Россия), под информационным суверенитетом государства предложила понимать независимость, полноту и верховенство государственной власти в информационной сфере. В условиях внедрения цифровых технологий информация приобретает статус важнейшего стратегического ресурса в государстве. До-

кладчик подчеркнула: «Ни одна машина не может заменить практического работника в деле распознавания фейков».

В. Ф. Борисова, кандидат юридических наук, доцент кафедры гражданского процесса Саратовской государственной юридической академии (Россия, г. Саратов) отметила, что, с одной стороны, цифровизация делает жизнь комфортнее, с другой стороны — таит в себе определенные угрозы, одной из которых является обман граждан с использованием fake-технологий. Фейк-технологии — это новый тип угроз. Они используют искусственный интеллект для создания правдоподобных, реалистичных видео, изображений, аудио и текстов о событиях, которых никогда не было. Угроза исходит не от технологии, используемой для их создания, а от создаваемого ею продукта, который будут видеть люди. Расчет преступников делается на естественную склонность людей верить в то, что они видят, слышат, так как видео- и аудиозаписи, тексты изготавливаются «правдоподобными». В мире стала возможной «кража лица» с помощью deepfake-технологий, использующих наложение лица [1; с. 8], голоса одного человека на другого, с чем до этого правоприменительная практика противодействия мошенничеству не сталкивалась.

Е. В. Семенкова, кандидат юридических наук, доцент кафедры уголовного процесса Московского университета МВД России (Россия, г. Москва) сосредоточила внимание на проблемах использования в доказывании по уголовным делам о фейках. Ограничения на свободу получения информации, созданной посредством дипфейк-технологий, нельзя признать ограничением свободы на получение информации в силу вредоносности данной информации, подчеркнула она.

Т. Л. Тенилова, кандидат юридических наук, доцент кафедры теории и истории государства и права Волжского государственного университета водного транспорта (Россия, г. Нижний Новгород), отметила: «Представляется невозможным остановить распространение фейковых новостей без вмешательства государства. Ни один частный субъект не в состоянии остановить распространение такого рода информации».

А. В. Червяковский, кандидат юридических наук, доцент кафедры теории и истории права и государства Омской академии МВД России (Россия, г. Омск), в частности, сказал: «Попытки организовать борьбу с недостоверной информацией на международном уровне в настоящее время пока не приносят желательного результата. Основная причина заключается в том, что мировое сообщество не может прийти к единому подходу относительно пределов контроля за созданием, распространением и хранением информации, размещаемой в сети. Имеется опыт принятия отдельных правовых актов на региональном и межгосударственном уровне. Безусловно, имеются определенные пределы информационной открытости, невозможно существование государства без наличия в его распоряжении информации, содержащей сведения, которые не могут быть доступны всем гражданам, даже если у них возникает потребность в получении такой информации. Но важно понимать, что чем больше в государстве имеется «секретов», тем больше поводов для появления недостоверной, а иногда заведомо ложной (фейковой) информации, в которую могут поверить люди».

О. И. Захарова, адвокат коллегии адвокатов Воронежской области (Россия, г. Воронеж), говорила о роли административного права в противодействии фейкам. Сегодня в России отсутствует защита персональных данных, что непосредственно влияет на изобретение и рождение новых схем мошенничества, фейков, дипфейков в современных условиях цифровых реалий. Следы преступлений зачастую могут быть в виде записей в файлах статистики коммуникационного оборудования, серверов операторов связи, лог-файлов журналов активности пользователей операционной системы и т. д. Указанная информация имеет ограниченный срок хранения, связанный с двумя группами условий: а) техническими, когда такая информация уничтожается автоматически спустя определенный промежуток времени, что связано с ограниченным объемом памяти носителя, настройками операционной системы, техническим сбоем и т. д.; б) нормативными, к которым можно отнести требования законодательства или локальных нормативных актов, регламентирующих сроки хранения информации. Так, в соответствии с п. 1 ст. 64 Федерального закона «О связи» операторы связи хранят на территории Российской Федерации информацию о фактах оказания услуг связи в течение 3 лет, а информацию самих сообщений — до 6 месяцев. Таким образом, в соответствии с нормативными правовыми актами Российской Федерации срок хранения фейковой цифровой информации, как правило, ограничен по времени. Соответственно проведение следственных

действий, направленных на изъятие такой информации, по истечении сроков хранения последней может не дать никакого результата.

Н. Н. Мазурова, аспирант кафедры международного права Российского государственного педагогического университета им. Герцена (Россия, г. Москва), связала в своем выступлении фейковые новости с международным терроризмом. Важным аспектом противодействия киберпреступности является повышение осведомленности и обучения.

Всего в организованной Юридическим институтом конференции приняли участие более 70 ученых-юристов от вузов Китая, Минска и Гродно (Беларусь), Херсона, Калининграда, Владивостока, Москвы, Санкт-Петербурга, Ростова-на-Дону, Саратова, Казани, Белгорода, Уфы, Воронежа, Оренбурга, Омска, а также вузов Северного Кавказа, Кубани, Крыма, Донецкой Народной Республики. Были доклады федеральных судей, прокуроров, следователей следственных управлений Следственного комитета РФ. География участников охватила регионы буквально от Калининграда до Владивостока. В тематике докладов были представлены почти все отрасли права.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Костюк М. Ф., Кунц Е. В. Криминологические аспекты дистанционного мошенничества // Проблемы права. 2022. № 3. С. 70.
2. Dixit A., Kaur N. & Kingra S. Review of audio deepfake detection techniques: issues and prospects // Expert Systems. 2023. Vol. 40, no. 8. <https://doi.org/10.1111/exsy.13322>
3. Moreno F. R. Generative AI and deepfakes: a human rights approach totackling harmful content // International review of law, computers & technology. 2024. Vol. 38, no. 3. P. 299. <https://doi.org/10.1080/13600869.2024.2324540>
4. Hine E., Floridi L. New deepfake regulations in China are a tool for social stability, but at what cost? // Nature Machine Intelligence. 2022. Vol. 4. P. 608–610.
5. AI-Deep Synthesis Regulations and Legal Challenges: Recent Face Swap Fraud Cases in China // <https://www.herbertsmithfreehills.com/notes/data/2023-08/ai-deep-synthesis-regulations-and-legal-hallenges-recent-face-swap-fraud-cases-in-China>