УДК 340.1:004
ББК 67.408.135

ВОПРОСЫ ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ ТЕХНОЛОГИИ DEEPFAKE

Е. В. Мицкая
Южно-Казахстанский университет им. М. Ауэзова (Шымкент, Казахстан)

С расширением применения информационных технологий и их потенциальными возможностями улучшения качества жизни во всех сферах жизнедеятельности человека становится понятным, насколько наряду с этим не ограничены их возможности причинения вреда человеку. Главным образом путем распространения недостоверной, заранее лживой информации и тем самым введения в заблуждение, обман граждан. В силу того, что в России и Казахстане законодательство нельзя признать полностью отвечающим потребностям противодействия deepfake-технологиям, необходимо обратиться к положительным примерам из зарубежных государств и на их основе предложить возможные меры противодействия deepfake-технологиям. Данное исследование посвящено поиску мер защиты человека от таких технологий. Предлагается введение на законодательном уровне обязанности разработчика программного обеспечения и поставщика данного продукта маркировать контент, созданный с использованием deepfake-технологий, включая звуковое, текстовое оповещение о том, что информация — фейк, в случае несоблюдения этого — привлечение к уголовной ответственности за распространение заведомо ложного контента. Кроме этого, необходимо создание эффективных механизмов, позволяющих удалять контент deepfake, который нарушает права человека, являясь незаконным или вредным; расширение уголовной ответственности за нарушение правил хранения, сбора биометрии человека, незаконное ее использование, передачу, получение; усиление межгосударственного взаимодействия по противодействию дипфейкам.

Ключевые слова: цифровизация, deepfake-технологии, правовое противодействие фейкам, криминализация, защита персональных данных

ISSUES OF LEGAL COUNTERACTION TO DEEPFAKE TECHNOLOGY

E. V. Mitskaya
M. Auezov South Kazakhstan University (Shymkent, Kazakhstan)

With the increasing use of information technologies and their potential to improve the quality of life in all areas of human activity, it becomes clear how unlimited their potential to cause harm is. This is mainly caused by the dissemination of unreliable and false information in advance, which misleads and deceives citizens. Due to the fact, that the legislation in Russia and Kazakhstan does not fully meet the needs of dealing with deepfake technologies, it is necessary to refer to positive examples from abroad and, based on them, to propose possible measures to deal with deepfake technologies. This study is dedicated to the search for measures to protect people from such technologies. It is proposed to introduce at the legislative level the obligation of the software developer and the supplier of this product to mark the content created with the use of deepfake technologies, including audio, textual notification that the information is fake, in case of non-compliance — bringing to criminal responsibility for the distribution of knowingly false content. In addition, it is necessary to create effective mechanisms for removing deepfake content that violates human rights, which is illegal or harmful; to extend criminal liability for violation of the rules of storage, collection of human biometrics, their illegal use, transfer, receipt; to strengthen interstate cooperation to deal with deepfakes.

Keywords: digitalisation, deepfake technologies, legal opposition to fakes, criminalisation, personal data protection

Doi: https://doi.org/10.14258/ralj(2025)1.8

Без информационных технологий сегодня уже невозможно представить дальнейшее развитие ни одной из сфер жизнедеятельности общества. Информационные технологии меняют нашу жизнь. Цифровизация не могла не затронуть и право. Информационные технологии составляют прочную основу правового регулирования. Государственные услуги переводятся в электронный формат, деятельность нотариусов осуществляется в рамках Единой нотариальной информационной системы. Суды также не остались в стороне от цифровизации. В настоящее время особое внимание обращается на расширение цифровизации при отправлении правосудия, благодаря которой возможно достичь единообразия в его отправлении. Действительно, праву априори присуща высокая степень формализации и логической строгости [1, с. 61], объяснимая регулятивными свойствами права [2, с. 203]. Соответственно цифровизация правосудия является не чем иным, как продолжением процесса формализации права, находящего проявление не только в единообразии формулировок норм права, но и в их применении. Информационные системы способны сопоставлять большие массивы данных, фактических обстоятельств [3, с. 49], обеспечивая достаточно высокую точность соответствия закону окончательного решения по делу.

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 (далее — фейк).

Фейк-технологии, по нашему мнению, — это новый тип угроз. Они используют искусственный интеллект для создания правдоподобных, реалистичных изображений, видео-, аудиоматериалов 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, и естественной склонности людей верить в то, что они видят, слышат, так как видео- и аудиозаписи, тексты будут правдоподобными. Западные государства столкнулись с использованием таких видео в целях шантажа, вымогательства. Фото обычных людей, включая детей, и общедоступных изображений стали основой для сфабрикованных порновидео [4, с. 38], размещенных на соответствующих сайтах и форумах с целью нанести данным лицам психологический вред, крушение их репутации, не исключая вымогательство денег за удаление такого контента [5, с. 299]. Дипфейки также могут использоваться для того, чтобы заманить людей инвестировать или раздавать свои с трудом заработанные деньги. Причем программные системы, если они имеют заданный определенный алгоритм, могут самостоятельно использовать повторно уже сгенерированные персональные данные какого-либо человека, взяв их также из «машинной» памяти в просторах интернета. В данной ситуации Ф. Морено обращает внимание: а будут ли тогда персональные данные считаться персональными [5, с. 307]? Да и доказать то, что они были сгенерированы нейронной сетью, достаточно трудно [6].

И не задаваться вопросом правового противодействия фейкам становится опасным. Из всей ложной или фейковой информации следует выделять особо ее новый вид — в мире стала возможной «кража лица» с помощью deepfake-технологий, использующих наложение лица, голоса одного человека на другого, с чем до этого правоприменительная практика противодействия мошенничеству не сталкивалась [7]. Это значит, что информационные технологии открывают для преступников возможности использования как подлинной биометрии человека, так и поддельной для совершения преступлений. Deepfake-технологии были опробованы и в Казахстане, когда мошенники уже трижды сгенерировали при помощи нейросети реальное выступление Президента РК с Посланием народу 2022 г. и сделали на его основе фейковое выступление: то Президент обещает выплаты по госпрограмме и возврат денег всем гражданам, пострадавшим от мошенников, то агитирует вкладывать деньги в платформу Илона Маска [8].

Если по некоторым оценкам к 2026 г. до 90% онлайн-контента может быть создано искусственным путем, то использование дипфейков, вероятно, станет распространенным источником киберпреступности [9, с. 5], способом совершения различных преступлений [10, с. 99]. И тогда для тех государств, где законодательно отсутствует криминализация заведомо ложной информации, и дипфейков в том числе, за них невозможно будет привлечь к уголовной ответственности. Поэтому неудивительно, что некоторые государства криминализовали распространение недостоверной информации.

Так, в Уголовном кодексе Литвы распространение любой дезинформации запрещено (ст. 19 (2)) [11]. Фейковые новости являются преступлением в Сингапуре, наказание предусмотрено в виде тю-

ремного заключения сроком до 10 лет и наложения штрафа в размере до 1 млн сингапурских долларов, что равняется 735 тыс. долл. США.

С октября 2023 г. в Уголовный кодекс Республики Польша внесена поправка, предусматривающая наказание за дезинформацию — не менее 8 лет лишения свободы за распространение ложной или вводящей в заблуждение информации, которая направлена «на серьезное нарушение политической системы или экономики Республики» [12]. Так же как и Мальта ввела уголовную ответственность за фейковые новости, предусматривающую тюремное заключение сроком от 1 до 3 месяцев или от 3 до 6 месяцев, если преступление приводит к беспорядкам [13].

В ОАЭ за распространение ложной, вредоносной или вводящей в заблуждение информации предусмотрен штраф в размере около 27,4 тыс. долл. США и заключение под стражу на срок от 1 года [14]. В Республике Корея в случае распространения ложной информации или клеветы нарушителю грозит до 5 лет лишения свободы или штраф до 7 тыс. долл. США [15].

В УК РФ были введены новые составы: ст. 207.1 («Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан»), ст. 207.2 («Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия», ст. 207.3 УК РФ предусматривает наказание за распространение заведомо ложной информации о действиях Вооруженных сил РФ, а ст. 280.3 УК РФ — за публичные действия, направленные на дискредитацию использования Вооруженных сил РФ [16]. К объектам защиты по ст. 280.3 УК РФ добавили также государственные органы, которые исполняют свои полномочия за пределами России в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности.

В Казахстане действует ст. 274 УК РК о распространении заведомо ложной информации, под которой понимается информация, создающая опасность нарушения общественного порядка или причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства [17].

В США в пяти штатах приняты законы, касающиеся deepfake. В 2019 г. Техас принял закон SB751, Калифорния приняла закон № 730, оба они запрещают использование дипфейков для оказания влияния на предстоящие выборы. В том же году Калифорния также приняла AB602, Джорджия — SB337, а Вирджиния — SB1736, которые запрещают создание и распространение поддельной порнографии без согласия сторон. В 2020 г. в Нью-Йорке был принят закон S6829A, который предусматривает средства правовой защиты в случае незаконной публикации откровенных подделок [18].

С 1 января 2020 г. дипфейки стали преступлением в Китае. Уголовный закон предусматривает, что лицам, которые фабрикуют ложную информацию и распространяют ее через информационные сети или другие медиа-платформы с намерением нарушить общественный порядок или нанести ущерб репутации других лиц, может грозить наказание в виде тюремного заключения сроком до трех лет или штрафа [19]. Таким образом, создание дипфейков без согласия пользователей будет 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 на непосредственно разработчиков. Закон 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 [20]. Интернет-платформы согласно закону обязаны самостоятельно осуществлять проверку своего контента, и так как 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 ответствен-

ность за дипфейки разработчиков такого программного продукта и их поставщиков [21, с. 608–610], а не пользователей дипфейков.

Противники криминализации как фейков, так и дипфейка считают, что тем самым ограничивается свобода на получение информации, свобода на свободу мнений, закрепляемых Европейской конвенцией о правах человека [22]. Действительно, право на свободу получения информации во многих государствах стало конституционным [23, с. 112; 24, с. 64]. Под конституционным правом личности на информацию следует понимать закрепленную в Конституции возможность человека и гражданина свободно искать, собирать, выбирать, получать, создавать, передавать и распространять информацию любыми не запрещенными законом способами.

В России, Казахстане свобода получения и распространения информации гарантируется конституционным запретом цензуры. В Законе Республики Казахстан «О масс-медиа» под цензурой понимается «предварительное согласование сообщений и материалов средствами массовой информации с государственными органами, должностными лицами и иными организациями по их требованию или по иным основаниям с целью ограничения или наложения запрета на распространение сообщений и материалов либо их отдельных частей» [25]. Аналогичное определение цензуры имеется и в российском законе «О средствах массовой информации» [26].

Такой подход вполне оправдан, ибо цензура запрещена официально. Вместе с тем кроме официальной цензуры, имевшей место в условиях тоталитарного общества, существует неофициальная цензура, когда отдельные руководители государственных органов берут на себя полномочия по ограничению или запрету распространения той или иной информации, не закрытой для доступа. Однако в любой форме цензура запрещается, а при обнаружении органов, организаций, учреждений или должностей, в задачи или функции которых входит осуществление цензуры средств массовой информации, их финансирование немедленно прекращается и они немедленно ликвидируются в установленном законом порядке.

Запрет на цензуру, во-первых, закреплен нормами Конституции и текущего законодательства, т. е. имеет правовую форму и, следовательно, обеспечивается принудительной силой государства; во-вторых, охватывает запрет предварительного согласования публикуемых и распространяемых иным способом сообщений и материалов средствами массовой информации с любыми государственными органами, должностными лицами или организациями, в т. ч. негосударственными. В-третьих, указанный запрет касается только согласования материалов по требованию соответствующих государственных органов, должностных лиц либо организаций или по иным основаниям, но не распространяется на добровольное согласование с ними, которое осуществляется по инициативе самих СМИ. В-четвертых, цензура преследует конкретную цель — ограничение или наложение запрета на распространение сообщений и материалов либо их отдельных частей. Поэтому если требование предварительного согласования материалов и сообщений имеет иную цель — например, не допустить искажения позиции, взглядов, мнений того или иного лица, органа, организации, — цензуры нет, а следовательно, требование такого согласования не запрещено.

Запрет цензуры не означает полной вседозволенности в получении, распространении любой информации. Как справедливо пишет Л. Ахметова, «пройдя период анархической свободы, начинаешь понимать и ценить свободу слова как ответственность. А ее отсутствие и порождает разговоры о введении цензуры» [27]. И в этом плане нельзя не согласиться с ее резонным замечанием о том, что «у настоящего журналиста всегда была некая внутренняя самоцензура, понимаемая как этический самоконтроль». И если понятия «свобода слова» и «цензура» несовместимы, то «свобода слова» и «ответственность» — братья-близнецы [27].

Свобода СМИ как один из составных элементов свободы информации означает прежде всего независимость прессы, радио, телевидения в выборе информационных материалов, художественных форм их выражения и подачи, право самостоятельно подбирать редакционный коллектив, направлять в разные регионы и за рубеж собственных корреспондентов, строить свои отношения с международными информационными агентствами. В отдельных странах допускается государственное лицензирование радиовещательных, телевизионных или кинематографических предприятий, т. е. выдача государством в лице уполномоченных органов разрешений на деятельность указанных СМИ. Однако эти меры не означают создания государственной монополии на средства массовой информации, т. е. устранения с информационного рынка негосударственных СМИ. Так, Европейский суд по правам че-

ловека определил нарушение ст. 10 Европейской конвенции о защите прав человека, когда Австрия законодательно установила государственную монополию на вещание. Главный вопрос для суда состоял в том, необходима ли такая монополия для достижения какой-либо из допустимых схем лицензирования. Суд сделал вывод, что она не является необходимой для обеспечения объективной беспристрастности, сбалансированности и разнообразия вещания [28, с. 245].

Свобода СМИ выражает и их плюрализм, т. е. допущение на информационный рынок не только государственных, но и частных средств массовой информации. В юридической литературе отмечалось, что, по сути, свобода массовой информации является прежде всего свободой частных средств массовой информации в их воздействии на общественное мнение и на государственную власть. Существование государственных СМИ допустимо лишь постольку, поскольку в условиях существования аналогичных частных СМИ государственные СМИ не смогут оказать существенное влияние на формирование общественного мнения. Такова, например, позиция по этому вопросу Федерального конституционного суда ФРГ [29, с. 296].

Следует сказать, что, конечно, когда речь идет о свободе на получение, распространение информации, доступ к информации, то под информацией в первую очередь понимается правдивая, достоверная информация. Государства, закрепляющие уголовную ответственность за распространение недостоверной информации, ставят, по мнению некоторых ученых, свободу получения информации в зависимость от государства.

Надо сказать, как тогда запрет дипфейков будет согласовываться с уголовной ответственностью за отказ в предоставлении гражданину информации (ст. 140 УК РФ, ст. 154 УК РК [16; 17]). Дело в том, что нельзя забывать, что понятие «свобода информации» не является абсолютным и безбрежным. Оно может быть ограничено определенными рамками, обеспечивающими защиту интересов общества и государства, а также частной жизни граждан от незаконного и необоснованного вторжения. Существуют ограничения на получение и распространение информации, относящейся к государственным секретам, к коммерческой или служебной тайне, а также составляющей личную либо семейную тайну гражданина.

Имеются и другие общие ограничения, которые предъявляются ко всем субъектам, действующим на политическом пространстве. Они исходят из конституционной нормы о недопустимости пропаганды и оправдания экстремизма или терроризма, пропаганды наркотических средств, психотропных веществ, их аналогов и прекурсоров, взрывчатых веществ и взрывных устройств, пропаганды или агитации насильственного изменения конституционного строя, нарушения целостности республики, подрыва безопасности государства, войны, социального, расового, национального, религиозного, сословного и родового превосходства, а также культа жестокости и насилия (ч. 4 ст. 2 Закона РК «О масс-медиа»).

Закон РК «О масс-медиа» запрещает использование средства массовой информации в этих же целях, а также для пропаганды порнографии. Это дополнение основано на конституционных положениях о недопустимости посягательства на общественную нравственность (п. 5 ст. 12) и защите нравственности населения (п. 1 ст. 39), т. е. такие законодательные ограничения введены в силу того, что абсолютная свобода слова может нанести вред мирному существованию граждан и демократии.

Конечно же, установленные законодательством ограничения ни в коем случае не должны использоваться как предлог для отказа в предоставлении информации по необоснованным мотивам, введения цензуры в мирное время. Ограничения на свободу получения информации, созданной посредством дипфейк-технологий, нельзя признать ограничением свободы на получение информации в силу вредоносности данной информации. В данной связи «криминализация — это форма общественного признания противоправности нарушений права на жизнь и свободу» [30, с. 21]. Социальная реальность находится в процессе постоянных изменений, и закон должен соответствовать этому. Если возникают новые процессы, потенциально способные причинить вред людям, закон должен останавливать такие процессы.

Некоторые мировые технологические компании вносят свой вклад в предотвращение и борьбу с использованием глубоких подделок. Например, Intel запустила первый детектор глубоких подделок в режиме реального времени, который анализирует видео, чтобы определить подлинность и то, создан он человеком или искусственным интеллектом. Другие компании, такие как Microsoft, Optic, Sentinel, Reality Defender и Attestiv, работают над аналогичными инструментами и платформами

для обнаружения мультимедиа. Однако саморегулирование частного сектора оказалось неэффективным во многих областях, особенно на платформах социальных сетей, где этот тип контента распространяется в соответствии с различными и непоследовательными правилами и стандартами. Поэтому Китай, ОАЭ предприняли попытку законодательно обязать интернет-платформы самостоятельно проверять контент на предмет выявления дипфейков и маркировать такой контент, чтобы интернет-пользователь заранее знал, что просматриваемая им информация — фейк.

Для решения этих проблем и обеспечения ответственного и этичного использования технологии deepfake платформы и приложения, которые обеспечивают такие функции, должны быть осведомлены о потенциальных обязательствах и принимать дополнительные меры, а также проводить соответствующую оценку и/или регистрацию, если это применимо, в соответствии с действующими правилами. Вот некоторые возможные решения.

Принятие четких и прозрачных политики и условий предоставления услуг, которые информируют пользователей о рисках и последствиях использования функций deepfake, и получения их явного и осознанного согласия перед обработкой их персональных данных или контента. В настоящее время подавляющая часть интернет-пользователей является не защищенной от воздействия деструктивной фейковой информации, а значит, является ведомой таким подложным контентом и подвержена различным провокациям. Несовершеннолетние пользователи тем более становятся уязвимыми для фейковой информации. В данной связи введение обязательной маркировки информации, что она создана с использованием дипфейк-технологий, заслуживает внимания. Кроме нанесения на контент определенного значка — фейк, нелишним было бы также обеспечение звукового, текстового оповещения о том, что информация — фейк [31].

Внедрение технических стандартов и методов для маркировки контента deepfake как такового и отслеживания его происхождения и подлинности. На сегодняшний день есть ряд программных продуктов, которые способны определить фейковые новости: Botometer, Detecting Fake News, Fake Bananas, Hoaxy, Politifact, Snopes [32, с. 624]. Однако защита человека со стороны государства именно от получения фейковой информации должна быть, и пока что, по нашему мнению, лучше, чем установлено в китайском законодательстве, нет: введение обязанности разработчика программного обеспечения и поставщика данного продукта маркировать контент и уголовной ответственности за распространение заведомо ложного контента. Разработчики искусственного интеллекта должны обеспечить четкие определения, прозрачный и подотчетный надзор и надежные гарантии как для пользователей, так и для поставщиков.

Создание эффективных механизмов, позволяющих пользователям сообщать, отмечать или удалять контент deepfake, который нарушает их права или интересы, является незаконным или вредным. В России контроль за публикацией фейковых новостей в медиа осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). При этом предусматривается уведомление прокуратуры РФ обо всех случаях возбуждения дел в течение суток. В Казахстане в ноябре 2024 г. появился департамент МВД, который создан специально для противодействия киберпреступности. В США, например, в 2023 г. Агентство национальной безопасности совместно с ФБР и Агентством кибербезопасности и защиты инфраструктуры (CISA) выпустили информационный листок кибербезопасности (Cybersecurity Information Sheet (CSI) — «Контекстуализация угроз дипфейков для организаций») [33].

Сотрудничество с властями и другими заинтересованными сторонами в целях предотвращения, выявления и пресечения преступлений, связанных с глубокими подделками, а также предоставления доказательств или помощи, когда это необходимо. Сотрудничество между государственным и частным секторами будет иметь решающее значение для выработки эффективных ответных мер, поскольку сообщество киберпреступников всегда на шаг впереди, когда речь заходит о технологиях.

Расширение уголовной ответственности за нарушение правил хранения, сбора биометрии человека, незаконное ее использование, передачу, получение. Дипфейк-технологии, когда мошенники способны оживить фотографию: фотография способна моргать, открывать рот, кивать и др. [34] — заставляет задуматься о безопасности биометрии человека, о защищенности биометрических данных людей, а также введении уголовной ответственности за нарушение хранения биометрических данных, незаконное их использование, передачу, получение. Согласно законодательному акту Европейского союза (General Data Protection Regulation) одной из мер противодействия незаконному ис-

пользованию биометрии человека является блокировка интернет-ресурса либо приложения, включая запрет на деятельность дочерних компаний, расположенных в ЕС. Штрафы за несоблюдение правил защиты данных, содержащихся в GDPR, могут быть внушительными для бизнеса, достигая до 20 млн евро либо 4% от годового оборота компании [35], что нужно принять как эталон для установления неменьших штрафов в национальном законодательстве. В РФ и РК продолжает формироваться правовая база регулирования персональных данных. Анализ действующего законодательства РФ, РК показывает параллельное стремление этих стран в поиске тех правовых механизмов, которые оптимально защищали бы персональные данные. Как в РФ, так и в РК информационная безопасность отнесена к разновидности национальной безопасности. Однако при этом правовое регулирование отношений, связанных с персональными данными, пока не достигло совершенства. Для российского и казахстанского законодательства остается открытым вопрос о четкой правовой регламентации обеспечения защиты биометрических данных [36, с. 82]. Социальная реальность находится в процессе постоянных изменений, и закон должен соответствовать этому. Если возникают новые процессы, потенциально способные причинить вред людям, закон должен участвовать и останавливать такие процессы.

Просвещение и повышение осведомленности пользователей и общественности о природе и влиянии технологии deepfake, а также о том, как идентифицировать и проверять контент deepfake. Повышение осведомленности общественности об этих формах мошенничества и социальной инженерии имеет основополагающее значение для защиты общества от преступной эксплуатации и технологического ущерба в долгосрочной перспективе. Очевидно, что перед нами стоит задача, как регулировать технологию, которая используется для производства дипфейков, балансируя между правом на неприкосновенность частной жизни и свободой выражения мнений. Однако насколько заранее недостоверное мнение является значимым для общества, — это большой вопрос. Коррекция поведения в социуме должна базироваться на поведении, которое не нарушает установленные правила, а дипфейковая информация способна нести только деструктивный потенциал. Так зачем тогда давать свободу на выражение деструктивных мыслей?

Представляется невозможным остановить распространение фейковых новостей без вмешательства государства. Ни один частный субъект не в состоянии остановить распространение такого рода информации. Необходима правовая база для обеспечения соблюдения определенных правил поведения. Если нет нарушения правовых норм, то существуют ограниченные меры по блокированию или удалению таких новостей. Технологические платформы могут действовать, принимая определенные правила, запрещающие распространение фейковых новостей, но все же возможно создавать или публиковать информацию в других местах интернета. Одной из основных проблем реализации противодействия фейкам государством в одиночку является выявление источника ложной информации или киберпреступности. Во многих случаях источник ложной информации или киберпреступления сложно отследить, поскольку преступник может находиться в другой стране или использовать прокси-сервер, чтобы скрыть свою личность. Это затрудняет работу правоохранительных органов по выявлению преступника и привлечению его к ответственности. Следовательно, необходимо понимание проблемы на международном уровне и закрепления обязанности для государств оказания помощи в рамках международного сотрудничества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Хорунжий С. Н. Правовой баланс как самостоятельная юридическая ценность: механизмы его обеспечения и регулирования : моногр. Воронеж : Издательский дом ВГУ, 2019. 526 с.

2. Черданцев А. Ф. Теория государства и права. М. : Юрайт, 1999. 432 с.

3. Кулюшин Е. Н. О применении технологий искусственного интеллекта в административном судопроизводстве // Российское право: образование, практика, наука. 2024. № 2. С. 48–54.

4. Schick N. Chapter One. Essay. In Deepfakes: The Coming Infocalypse. New York: Grand Central Pub, 2021. P. 37–42.

5. 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. 297–326.

6. What Is Deep Learning? IBM. URL: https://www.ibm.com/topics/deep-learning#:~: text=the%20next%20step, What%20is%20deep%20learning%3F, from%20large%20amounts%20of%20data (дата обращения 04.11.2024).

7. Dixit A., Kaur N. & Kingra S. Review of audio deepfake detection techniques: issues and prospects // Expert Systems. 2023. vol. 40, no. 8. URL: https://doi.org/10.1111/exsy. 13322 (дата обращения 04.11.2024).

8. Мошенники создали дипфейк с участием Токаева для обмана казахстанцев. URL: https://kz.kursiv.media/2024–05–23/lsbs-dipfaiktok (дата обращения 04.11.2024).

9. Busch E. & Ware J. The Weaponization of Deepfakes: Digital Deception on the Far-Right. Hague: International Centre for Counter-Terrorism, 2023. 20 p.

10. Ефремова М. А., Русскевич Е. А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 2 (56). С. 97–105.

11. Lietuvos Respublikos baudžiamasis kodeksas. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS. 111555/asr (дата обращения 04.11.2024).

12. Art. 132. Dezinformacja wywiadowcza. Kodekskarny. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/art-132 (дата обращения 04.11.2024).

13. Farrugia, L. (2018). Can the spreading of false news as a criminal offence hinder freedom of expression? (Bachelor's dissertation).

14. Федеральный Указ-закон № 34 от 2021 года о борьбе с ложной информацией и киберпреступлениями. URL: https://uaelegislation.gov.ae/en/legislations/1526 (дата обращения 02.11.2024).

15. Уголовный кодекс Республики Корея. URL: https://vseokoree.com/vse-o-koree/zakony-i-normativnye-pravovye-akty/ugolovnyj-kodeks-respubliki-koreya (дата обращения 02.11.2024).

16. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020). URL: http:// www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 04.11.2024)

17. Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V. URL: https://online.zakon.kz/ (дата обращения 04.11.2024).

18. Quirk C. The High Stakes of Deepfakes: The Growing Necessity of Federal Legislation to Regulate This Rapidly Evolving Technology. Princeton University, 2023. URL: https://legaljournal.princeton.edu/the-high-stakesof-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/ (дата обращения 06.11.2024).

19. AI–Deep Synthesis Regulations and Legal Challenges: Recent Face Swap Fraud Cases in China. URL: https://www.herbertsmithfreehills.com/notes/data/2023–08/ai-deep-synthesis-regulations-and-legal-challenges-recent-face-swap-fraud-cases-in-china (дата обращения 04.11.2024).

20. Zou M. China's Deepfake Regulations: navigating security, misinformation and innovation. URL: https://www.oxfordmartin.ox.ac.uk/events/chinas-deepfake-regulations (дата обращения 06.11.2024).

21. 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.

22. Alkiviadou N. Prison for Fake News: A Proposal to Criminalize Fake News in Cyprus, VerfBlog, 2024/7/12. URL: https://verfassungsblog. de/prison-for-fake-news/. DOI: 10.59704/77977eadcc5ea19f (дата обращения 04.11.2024).

23. Мицкая Е. В. Обеспечение прав и свобод человека и гражданина в условиях интеграционных процессов // Евразийская интеграция: экономика, право, политика. 2010. № 7. С. 110–115.

24. Мицкая Е. В. Методологические и историко-правовые основы построения конституционных прав и свобод граждан // Современное право. 2007. № 5. С. 63–66.

25. О масс-медиа: Закон Республики Казахстан от 19.06.2024 № 93-VIII. URL: https://online.zakon.kz/Document/?doc_id=38665430&pos=153 (дата обращения 04.11.2024).

26. О средствах массовой информации: Закон РФ от 27.12.91 № 2124–1 (ред. от 11.03.2024). URL: https://www.consultant.ru (дата обращения 04.11.2024).

27. Ахметова Л. Близнецы и антиподы // Казахстанская правда. 2003. 12 ноября.

28. Дженис М., Кэй Р., Брэдли Э. Европейское право в области прав человека (практика и комментарии). М. : Права человека, 1997. 640 с.

29. Государственное право Германии. В 2 т. Т. 2. М. : Бек, 1994. 320 с.

30. Harel A. The duty to criminalize // Law and Philosophy. 2015. Vol. 34, no. 1. P. 1–22.

31. H. R. 5586 — DEEP FAKES Accountability Act. 118th Congress (2023–2024). URL: https://www.congress.gov/bill/118th-congress/house-bill/5586/text (дата обращения 06.11.2024).

32. Гуськова С. В., Шестерина А. М. Технологии распространения фейковых новостей в массмедиа и способы их верификации: лингвистический аспект // Неофилология. 2023. Т. 9, № 3. С. 618–629.

33. Contextualizing Deepfake Threats to Organizations. URL: https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI–DEEPFAKE-THREATS. PDF (дата обращения 08.11.2024).

34. Мошенники в Китае. URL: https://pulse.mail.ru/article/v-kitae-pojmali-moshennikovkotorye-s-pomoschyu-dipfejkov-obmanuli-gossistemu-raspoznavaniya-lic-na-76-millionov-dollarov-6543561398487495-7–506895075424152725/ (дата обращения 08.11.2024).

35. Защита персональных данных граждан РК vs Европейского союза. URL: https://profit.kz/articles/14832/Zaschita-personalnih-dannih-grazhdan-RK-vs-Evropejskogo-souza/ (дата обращения 08.11.2024).

36. Мицкая Е. В. Правовое обеспечение защиты персональных данных (на примере Российской Федерации и Республики Казахстан) // Теория государства и права. 2016. № 2. С. 78–83.