

ПЕРЕВОДНЫЕ СТАТЬИ / TRANSLATED ARTICLES

УДК 343.63:004(73)

DOI: <http://dx.doi.org/10.21202/1993-047X.14.2020.1.105-141>

Р. А. ДЕЛФИНО¹

¹Школа права Лойолы, г. Лос-Анджелес, США

ПОРНОГРАФИЧЕСКИЕ ДИПФЕЙКИ: СЛЕДУЮЩИЙ ТРАГИЧЕСКИЙ АКТ ФЕНОМЕНА «ПОРНО ИЗ МЕСТИ» И НЕОБХОДИМОСТЬ ПРИНЯТИЯ УГОЛОВНОГО ЗАКОНА НА ФЕДЕРАЛЬНОМ УРОВНЕ*

Ребекка А. Делфино, внештатный преподаватель права, Школа права Лойолы
Адрес: Loyola Law School, 919 Albany Street, Los Angeles, California 90015–1211

Цель: изучение проблемы порнографических дипфейков – сфальсифицированных фотографий и видеороликов с наложением изображений лиц людей, не участвовавших в их съемке, и внесение предложений по ее решению.

Методы: наблюдение, изучение документов, сравнение, анализ, синтез.

Результаты: предлагается на уровне федерального уголовного законодательства Соединенных Штатов Америки решение общенациональной проблемы порнографических дипфейков, поскольку ни один федеральный закон или закон штата в настоящее время не предусматривает ответственности за их создание или распространение.

Научная новизна: впервые рассматривается правовой аспект порнографических дипфейков как феномена современной цифровизации и использования новых методов создания вредоносной для человека виртуальной реальности.

Практическая значимость: предлагается новый федеральный уголовный закон, регулирующий создание и распространение порнографических дипфейков. В этом законе сочетаются компоненты законов ENOUGH и MDFPA и добавлены другие необходимые компоненты с целью поставить заслон порнографическим дипфейкам и защитить их жертвы. Приводятся текст и анализ предлагаемого закона. Результаты исследования могут быть востребованы для учета в последующих научных работах, при совершенствовании законодательства и в правоприменительной деятельности не только Соединенных Штатов Америки, но также Российской Федерации и других стран.

Ключевые слова: порнографический дипфейк; цифровизация; виртуальная реальность; порнографические материалы; аудиозапись; видеозапись; правонарушение; киберпреступность

Благодарность: автор благодарит Кэтрин Бросэмл, Дженнифер Роджес и Кэтлин Саймерс за помощь в исследовании, Школу права Лойолы за щедрую стипендиальную поддержку и, как всегда, семью за терпение, снисходительность и содействие и посвящает эту статью своим родителям, Кену и Розмари Делфино, которые научили ее не только отделять правду от вымысла, но и изучать разницу между ними.

* Впервые статья опубликована на английском языке в журнале Fordham Law Review. По вопросам коммерческого использования обратитесь по адресу: tmelnick@law.fordham.edu.

Цитирование оригинала статьи на английском: Rebecca A. Delfino, Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act, 88 Fordham L. Rev. 887 (2019).

URL публикации: <https://ir.lawnet.fordham.edu/flr/vol88/iss3/2>

Как цитировать русскоязычную версию статьи: Делфино Р. А. Порнографические дипфейки: следующий трагический акт феномена «порно из мести» и необходимость принятия уголовного закона на федеральном уровне // *Актуальные проблемы экономики и права*. 2020. Т. 14, № 1. С. 105–141. DOI: <http://dx.doi.org/10.21202/1993-047X.14.2020.1.105-141>

R. A. DELFINO¹

¹Loyola Law School, Los Angeles, USA

PORNOGRAPHIC DEEPPAKES: THE CASE FOR FEDERAL CRIMINALIZATION OF REVENGE PORN'S NEXT TRAGIC ACT*

Rebecca A. Delfino, Clinical Professor of Law at Loyola Law School, Los Angeles.
Address: Loyola Law School, 919 Albany Street, Los Angeles, California 90015–1211

Objective: to study the problem of pornographic deepfakes – doctored images and videos featuring faces of persons who were not engaged in the acts, and to propose solutions for the problem.

Methods: observation, document study, comparison, analysis, synthesis.

Results: it is proposed to solve the problem of pornographic deepfakes at the level of the U.S. federal criminal legislation, as currently there is no federal or state law criminalizing their creation or distribution.

Scientific novelty: for the first time, the legal aspect of pornographic deepfakes is considered as a phenomenon of today's digitalization and using of new techniques for creating virtual reality harmful for humans.

Practical significance: a new federal criminal statute is proposed to regulate creation or distribution of pornographic deepfakes. The proposed law combines components of the ENOUGH Act and MDFPA with other necessary elements to combat pornographic deepfakes and protect their victims. The proposed statute text is set forth and analyzed. The research results can be used in further scientific works, to improve legislation and law-enforcement practice not only in the United States but also the Russian Federation and other countries.

Keywords: Pornographic deepfake; Digitalization; Virtual reality; Pornographic materials; Audio recording; Video recording; Offense; Cybercrime

Acknowledgements: I am grateful and indebted to Katherine Brosamle, Jennifer Roges, and Kathleen Simers for their research assistance, Loyola Law School for its generous support of faculty scholarship and, as always, my family for their patience, indulgence, and encouragement. This Article is dedicated to my parents, Ken and Rosemary Delfino, who not only taught me to discern fact from fiction at a young age but also inspired me to care about the difference.

For citation of Russian version: Delfino R. A. Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act, *Actual Problems of Economics and Law*, 2020, Vol. 14, No. 1, pp. 105–141. DOI: <http://dx.doi.org/10.21202/1993-047X.14.2020.1.105-141>

* This Note is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.

For original publication: Rebecca A. Delfino, Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act, 88 Fordham L. Rev. 887 (2019).

Publication URL: <https://ir.lawnet.fordham.edu/flr/vol88/iss3/2>

Это может произойти с вами.

Как и миллионы людей во всем мире, вы загружали свои цифровые фотографии в Интернет через социальные медиаплатформы. Ваши фотографии не имеют отношения к сексу – они изображают вашу повседневную жизнь, как вы проводите время с друзьями или делаете селфи в отпуске. Но затем кто-то решает, что вы ему не нравитесь. Используя приложение, доступное на любом смартфоне, этот ваш противник вырезает ваше лицо из невинных фотографий и приставляет его к телу человека, участвующего в откровенно сексуальных сценах. Без вашего ведома и согласия вы становитесь «звездой» реалистичного порнографического дипфейка.

Эта гипотетическая ситуация отражает новое явление в сфере криминальной сексуальной эксплуатации – это следующий шаг после незаконного публичного распространения личных сексуально откровенных фото- или видеоматериалов, известных как порно из мести. Можете ли вы что-то сделать, если вас вставили в фейковое порнографическое фото или видеоизображение против вашей воли? Законно ли создавать, публиковать и распространять фальсифицированную порнографию в Интернете?

Ответ на эти вопросы в лучшем случае будет сложным и неопределенным. В худшем случае ответ – «нет». Хотя самым эффективным сдерживающим фактором подобных деяний является их криминализация, в настоящее время нет ни одного федерального закона или закона на уровне штата, который бы устанавливал ответственность за создание или распространение порнографических дипфейков. А поскольку дипфейки существуют в киберпространстве, они не относятся к юрисдикции отдельных штатов. В данной статье впервые рассматривается правовой аспект порнографических дипфейков и предлагается законодательное решение относительно различных видов ущерба, который они причиняют. Таким образом, в статье предлагается решение, основанное на федеральном уголовном законодательстве и затрагивающее проблему на общенациональном уровне, так как жертвой дипфейка может стать каждый – даже вы.

Введение

Личина! Видно, ты полна коварства
И бес тобой воспользоваться рад!

Уильям Шекспир.
Двенадцатая ночь, акт 2, сцена 2¹

Ежедневно в реальном и виртуальном мире на нас обрушивается шквал правдивой и ложной информации, новостей, изображений, видео. Мы не всегда можем отделить истину от вымысла, и право не поспевает за темпом возникновения проблем. В последние годы в темных углах Интернета появилось нечто новое: обработанные фото- и видеоизображения, в которых лицо одного человека убедительно приставлено к телу другого, участвующего в откровенно сексуальных сценах. Создатели², комментаторы³ и исследователи⁴ называют такие изображения дипфей-

ками⁵. Хотя эти изображения фиктивные, созданные с помощью новых технологий искусственного интеллекта (далее – ИИ), они предлагаются как реальные изображения реальных людей, обычно женщин. Технология их создания развивалась так быстро, что сейчас стало широко доступно соответствующее при-

⁵ Название происходит от псевдонима пользователя платформы Reddit, который впервые выложил в Интернет обработанные видео с откровенно сексуальными сценами [2]. Термин объединяет две концепции: deep – «глубокий», от deep learning – «глубокое обучение»: аспект искусственного интеллекта, основанный на тех же принципах, что и обучение человека; и fake, от fake news – «фейковые новости», т. е. ложное или сенсационное сообщение, созданное, чтобы привлечь внимание, ввести в заблуждение или испортить репутацию. См. [8, 9]. Хотя происхождение слова известно, его написание остается противоречивым: можно встретить слитное (deepfake), дефисное (deep-fake) и раздельное (deep fake) написания. Правоведы и политики чаще пишут раздельно. См. Malicious Deep Fake Prohibition Act of 2018, S. 3805, 115th Cong. (2018); [6, 7]. Напротив, в блоге словаря Merriam-Webster и как минимум одном онлайн-словаре технического направления используется слитное написание: deepfake. См. Words We're Watching: 'Deepfake', Merriam-Webster (July 31, 2019). URL: <https://www.merriam-webster.com/words-at-play/deepfake-slang-definition-examples> [<https://perma.cc/W8FG-75QU>]; см. также [9]. В данной статье мы используем слитное написание, так как это слово образовано слиянием двух слов, что часто встречается при описании современных технологий (например, Pinterest, sexting, webinar).

¹ Twelfth Night act 2, sc. 2: пер. А. Кронеберга.

² См. [1] (описывается, как осенью 2017 г. анонимный пользователь Reddit разместил в Интернете несколько порнографических видео под псевдонимом «Дипфейки» (Deepfakes), на одном из которых лицо актрисы Дейзи Ридли было прикреплено к телу порноактрисы); см. также [2].

³ См., например, [3–5].

⁴ См. [6]. См. в целом [7].

ложение для смартфона [1]. Это приложение снизило технический порог, необходимый для их создания, поэтому фейковые порнографические изображения публичных фигур и рядовых граждан будут, вероятно, все более распространены. Сегодня любой, кто имеет цифровое фото, может против своей воли стать «порнозвездой», а в законе нет никаких средств помешать этому.

Неспособность закона защитить потенциальных жертв становится все более очевидной по мере усовершенствования и упрощения соответствующей технологии. Рассмотрим пример. Отелло и Дездемона находятся в долговременных отношениях. Отелло увлекается цифровой фотографией и снимает Дездемону на свой смартфон везде, где они бывают: гуляя по улочкам Венеции, осматривая морской порт на Кипре, устраивая пикник в саду своего замка. Дездемона не возражает против этих снимков, но никогда не разрешает Отелло фотографировать себя обнаженной или с сексуальным подтекстом. Они расстаются после того, как Отелло начинает подозревать, что Дездемона имела любовную связь с его другом Кассио. В отместку Отелло загружает снимки Дездемоны в приложение на своем смартфоне и накладывает ее лицо на тело некоей актрисы, занятой в порнографических сценах. Затем он размещает эти фейковые видео и контактную информацию Дездемоны на различных площадках социальных медиа.

Когда Дездемона обращается в правоохранительные органы, требуя, чтобы порнографические фейковые видео удалили, а Отелло арестовали, она узнает, что его поведение не нарушает никакого закона. Когда она спрашивает, можно ли осудить его по новому закону штата о порнографии из мести или по другому закону о киберпреступлении, ей не могут ответить с уверенностью и начинают сомневаться, является ли она вообще жертвой преступления, ведь она не была владельцем этих фото, а Отелло использовал в видео только ее лицо. К сожалению, эта история отражает новый зарождающийся феномен в киберпреступлениях с сексуальной эксплуатацией – это следующий трагический акт в неправомерном публичном распространении частных, сексуально откровенных фото- и видеоматериалов, которое известно как порно из мести.

В разд. I данной статьи дается определение и объясняется феномен дипфейков, а также их место в контексте Интернета. В этом разделе рассматриваются потенциальные опасности и риски, которые дипфейки

несут нашему обществу и демократическим институтам из-за их связи с фейковыми новостями и фальшивыми изображениями публичных и официальных лиц, а затем дипфейки рассматриваются в контексте порнографии, снятой без согласия участников, и близкого к ней явления «порно из мести».

В разд. II исследуется весь комплекс правовых и иных проблем, связанных с дипфейками. Например, как определить, кто на самом деле стал жертвой дипфейка, ведь видео изображает как минимум двух участников – того, чье тело было использовано, и того, чье лицо было добавлено. Является ли жертвой преступления первый, второй или оба? В этом разделе также обсуждаются трудности, связанные с выявлением личности и местонахождения преступников и привлечением их к ответственности, а также с удалением дипфейков из Интернета, учитывая принятый в 1996 г. Акт о соблюдении приличий в СМИ (Communications Decency Act, CDA)⁶, который освобождает дистрибьюторов контента от ответственности за контент, принадлежащий третьим сторонам.

В разд. III изучаются существующие меры правового воздействия. Хотя обвинители могут инициировать иски о преследовании в Сети, криминальных угроз, незаконном доступе к цифровой информации, детской порнографии, существующее уголовное федеральное законодательство не предусматривает наказания конкретно за дипфейки. В этом разделе также рассматриваются федеральные законы, находящиеся на стадии обсуждения, включая Акт 2018 г. о запрете дипфейков, созданных со злым умыслом (Malicious Deep Fake Prohibition Act)⁷, и Акт 2017 г. о борьбе с преследованиями, осуществляемыми с помощью изображений пользователя в Сети, полученных без его согласия (Ending Nonconsensual Online User Graphic Harassment Act)⁸. В разд. III обсуждаются уголовные законы четырех штатов: Калифорнии, Техаса, Флориды и Нью-Йорка, которые показывают, что даже эти штаты с самым многочисленным населением, самым большим количеством как зарегистрированных киберпреступлений, так и законов против порно из мести, не успевают реагировать на ущерб, причиняемый технологией дипфейка.

⁶ Pub. L. No. 104–104, tit. V, 110 Stat. 56 (кодифицирован с поправками в отдельных разделах 15, 18, и 47 U.S.C.).

⁷ S. 3805.

⁸ S. 2162, 115th Cong. (2017).

В разд. IV исследуются недостатки и ограничения как действующих, так и предложенных уголовных законов и показано, что они неспособны полностью исключить ущерб от дипфейковой порнографии. В этом разделе рассматриваются также аспекты, связанные с действием Первой поправки и цензуры.

Наконец, в разд. V рассматриваются пути решения проблемы порнографических дипфейков через принятие федерального уголовного закона. Предлагается правовое решение, совмещающее существующие элементы обсуждаемых федеральных законов, в которых предусматривается ответственность за порно из мести и дипфейки, и новые элементы, включая запретительные нормы и возмещение ущерба жертвам. Наконец, в этом разделе обсуждаются неюридические решения, которые должны создаваться и применяться параллельно. Такие решения включают разработку технологических средств верификации контента и повышение цифровой грамотности населения, так чтобы каждый потребитель контента в Сети знал: интернет-контент может быть истинным и фейковым; необходимо помнить об этом, прежде чем принимать решения или предпринимать какие-либо действия.

I. ФЕНОМЕН ДИПФЕЙКА

В Интернете появилась опасная новая технология, размывающая границы между фактом и вымыслом. Она позволяет пользователям создавать дипфейки – обработанные фото- и видеозображения, правдоподобно объединяющие лицо одного человека и тело другого [2]. Эта технология, основанная на искусственном интеллекте, имеет законные и полезные сферы применения⁹, однако она может также применяться со злым умыслом¹⁰, а именно при производстве порнографии без согласия задействованных лиц

⁹ См. [6, рукопись, pp. 14–16] (обсуждаются возможные «просоциальные» применения дипфейков в образовании, искусстве и самовыражении). См. также [10] («Эту технологию используют также для создания безобидных видео для розыгрышей и пародий, например, вставляют культовую для Reddit фигуру актера Николаса Кейджа в фильмы, где он не снимался»).

¹⁰ Chesney и Citron определили области, в которых возможно использование дипфейков, вредоносное для частных лиц (например, саботаж, шантаж, эксплуатация) или для общества (включая вред для демократических институтов, гражданского дискурса, общественной безопасности, национальной безопасности). См. [6, рукопись, pp. 16–29].

[11, 12]. На большинстве подобных изображений лица знаменитостей женского пола накладываются на тела других людей, участвующих в сексуальных актах¹¹. Миллионы людей, выкладывавших свои фотографии в Интернет, могут без своего ведома стать участниками таких порнографических изображений, которые легко создать с помощью приложения¹².

A. Развитие технологии дипфейка

Дипфейки впервые появились в Интернете в конце 2017 г., когда анонимный пользователь платформы Reddit¹³ выложил реалистичные порнографические видео со знаменитостями [10]. Вскоре после этого другой анонимный пользователь платформы создал и выпустил бесплатное приложение FakeApp, позволяющее легко создавать дипфейки [15]. До создания приложения FakeApp производство обработанных видео было дорогостоящим и трудоемким процессом, доступным только на киностудиях Голливуда¹⁴. Создатель FakeApp «сделал технологию дипфейка доступной людям без технического образования и опыта программирования» [1].

FakeApp загружает цифровые изображения в «алгоритм машинного обучения, который научился прикреплять одно лицо поверх другого» [2]; этот алгоритм известен также как «глубокое обучение искусственного интеллекта» (AI deep learning) [11, p. 1]. В этой технологии искусственный интеллект анализирует и изменяет изображение лица одного человека, а затем прикрепляет его к телу другого человека на

¹¹ См. [2] (в качестве некоторых жертв дипфейков называются Эмма Уотсон, Галь Гадот, Тейлор Свифт и Дэйзи Ридли); [13] (обсуждаются дипфейки, нацеленные против знаменитостей).

¹² См. в целом [11] (обсуждается вероятное использование дипфейков в случаях домашнего насилия и киберпреследования).

¹³ Reddit входит в десятку самых популярных веб-сайтов в США и в первую двадцатку в мире, позиционируя себя как «первая страница Интернета». См. [14]. Сайт представляет собой собрание форумов, известных также как subreddits, в которых группы пользователей обмениваются новостями и контентом или комментируют сообщения на самые разные темы. Там же. Заголовок сабреддита начинается на «r/», что отражает структуру URL-адреса на Reddit. Например, форум r/Shakespeare обсуждает жизнь и творчество Шекспира, а форум r/birdswitharms публикует изображения птиц с руками. Там же.

¹⁴ См. [16]. См. также [15] (показано, что приложение FakeApp «делает технологию дипфейка доступной рядовому пользователю»); [13].

видео [11]. Создание такого видео требует всего пяти несложных шагов¹⁵.

Кроме того, FakeApp может извлекать изображения из Google, Instagram и Facebook и использовать их для создания порнографии, отсюда преобладание дипфейков со знаменитостями¹⁶.

В. Распространение дипфейков в других областях

Хотя наиболее известно использование описанной технологии для создания реалистичных порнографических видео, ее можно также использовать для создания фейковых новостей и фейковых изображений с участием политиков и официальных лиц¹⁷. Так могут появиться видео политиков, берущих взятки, солдат, совершающих военные преступления, кандидатов в президенты, совершающих уголовные преступления, официальных лиц, объявляющих о террористической атаке¹⁸. Все эти ситуации способны причинить вред нашей демократии, особенно учитывая, что технологии продолжают быстро развиваться¹⁹. Например, ученые из Университета Вашингтона создали реалистичное видео с участием президента Барака Обамы с синхронизацией движения губ, «совместив аудиоряд с одной из его видеозаписей»²⁰. Это стало возможным, поскольку «в Сети было достаточно видеозаписей Обамы в форме интервью, речей, выступлений и т. п.» [19]. Кроме того, звукоинженеры использовали технологию искусственного интеллекта для «синтезирования 116 777 образцов голоса, каждый

длинной 0,4 секунды, взятых из 831 речи и радиобращения [президента Джона Кеннеди]» [20] и записали его голосом речь, которую он произнес бы 22 ноября 1963 г., если бы не был убит в тот день. Также кинорежиссер Джордан Пил создал с помощью технологии искусственного интеллекта речь Барака Обамы с предупреждением против фейковых видео [21]. По мере развития технологии дипфейка различать обработанные и настоящие видео- и фотоизображения станет все труднее.

Рост количества дипфейков в последнее время показывает несовершенство законодательства и поднимает сложные вопросы о необходимости решения проблем, связанных с дипфейками [6, рукопись, pp. 30–58]. Хотя такие сайты, как Reddit, Pornhub и Twitter, запретили размещение порнографических дипфейков на своих площадках [15], данная ИИ-технология будет, вероятно, все больше распространяться [6, рукопись, pp. 2–4, 8–14]. Имея такие приложения, как FakeApp или Snapchat, который позволяет изменять черты лица, все больше граждан смогут неконтролируемо создавать реалистичные фейковые видео [22; 6, рукопись, p. 814]. Чтобы защищать жертв дипфейка и предотвращать его негативные последствия, законы должны изменяться вместе с технологиями.

С. Дипфейки в контексте порнографии, созданной без согласия участников

Хотя первоначально дипфейки были направлены против знаменитостей, обычный человек также может обнаружить свое изображение в фейковом видео [11, p. 3]. Теперь, когда социальные медиа широко распространены и многие люди выкладывают свои фотографии в Сеть, пользователи FakeApp могут использовать изображения любого человека из Instagram или Facebook²¹. Так, пользователи Reddit открыто обсуждали создание дипфейков, изображающих друзей, преподавателей или бывших партнеров [23].

Поскольку технология дипфейка позволяет создавать реалистичные порнографические видео без согласия изображенных людей и поскольку эти видео могут широко распространяться в Интернете, они относятся к области киберпреступлений, ис-

¹⁵ Процесс сводится к следующим шагам: «1. Загрузите приложение FakeApp или подобное. 2. Убедитесь, что ваша видеокарта достаточно мощная... 3. Укажите видео, которое будете использовать. 4. Соберите несколько сотен фотографий... которые будут накладываться на видео. 5. Загрузите фотографии в FakeApp и запустите программу» [11, p. 5].

¹⁶ [11, pp. 6, 17].

¹⁷ См. [2] («В дипфейках хуже всего то, что эта жалкая порнография – только пролог к тому, что нас ждет дальше»); [13] (утверждается, что технология дипфейков «в будущем может быть использована для дискредитации правительств и народов, вызывая международные конфликты»); см. также [6, рукопись, pp. 16–29). Поиск в Сети может дать множество качественных фотографий, что достаточно для создания дипфейка.

¹⁸ См. [6, рукопись, pp. 16–29]. См. также [18].

¹⁹ См. [10] (отмечается, что технология «глубокого обучения», на которой основано создание дипфейков, стремительно развивается).

²⁰ Там же.

²¹ [13] (показано, что жертвами дипфейков могут стать рядовые граждане, если их качественные фотографии доступны в Сети).

пользующих сексуальную эксплуатацию. К этой же категории относятся такие преступления, как порно из мести и порнография, созданная без согласия участников [24]. Порно из мести – это преступление, состоящее в «предоставлении частного, сексуально откровенного изображения лицу, для которого оно не предназначалось» без согласия участников [25, 26]. Здесь речь идет о настоящих, а не обработанных фото- и видеоизображениях²². Обычно партнеры делятся подобными изображениями по взаимному согласию, а позже один из них распространяет их, желая отомстить другому [26, р. 346].

Однако материалы порно из мести могут также быть краденными или полученными посторонними людьми путем взлома или кражи сотового телефона или компьютера²³. Хакеры могут размещать эти материалы в Сети вместе с идентифицирующей информацией жертвы или без таковой²⁴. Более широкое понятие – «порнография, созданная без согласия участников» – включает сексуально откровенные фото- и видеоизображения, записанные без согласия участника, например, скрытой камерой [26, р. 346].

Порнографические дипфейки и порно из мести имеют ряд тревожных общих черт. Во-первых, и то и другое преимущественно затрагивает женщин²⁵. Один журналист описывал дипфейки как «способ для мужчин иметь неограниченную воображаемую власть над женскими телами» [28]. Во-вторых, оба явления предполагают распространение сексуально откровенных материалов без согласия. Жертвы порно из мести не соглашались на публичное распространение изображений, так же как жертвы дипфейков не соглашались на манипулирование их изображениями. Таким образом, и то и другое нарушает ожидания человека, что его сексуальная активность будет основана исключительно на добровольном согласии [11, р. 4].

Оба эти явления могут иметь долгосрочные эффекты на жертв²⁶ и вызывать схожие эмоциональные и психологические негативные последствия²⁷. Примечательно, что порно из мести не только наносит вред репутации и эмоциональному благополучию человека, но и несет в себе риски значительного законодательного, профессионального и даже физического ущерба²⁸. Проблемы с физической безопасностью включают насилие, преследование и другие преступные деяния²⁹.

Однако между этими явлениями существуют и значительные различия, которые не позволяют жертвам дипфейка заглядывать нанесенный им вред. Во-первых, дипфейки могут представлять собой продукт художественного самовыражения, созданный без злого умысла, тогда как порно из мести всегда представляет собой преступление. Действительно, больше всего внимания привлекают дипфейки, изображающие общественных деятелей и знаменитостей в безобидных и юмористических сочетаниях, – например, лицо Стива Бушеми наложено на тело Дженнифер Лоуренс в видеозаписи, где актриса обсуждает свое любимое реалити-шоу «Настоящие домохозяйки»³⁰. В таких случаях, когда видео явно фейковое, зритель понимает шутку – так, даже порнографические дипфейки изначально создавались как развлечение и художественное самовыражение, а не преступное деяние³¹.

Порно из мести, напротив, изображает частных лиц в интимных актах, которые должны были остаться частным делом, а не служить для массового распространения и развлечения. Аргументация правоведов

²⁶ См. Cyber Exploitation FAQs, выше примечание 23 (цитируя исследование Cyber Civil Rights Initiative's 2014 End Revenge Porn, в котором было показано, что подавляющее большинство пострадавших от порно из мести – женщины); см. также Revenge Porn Statistics, Cyber C.R. Initiative. URL: <https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf> [<https://perma.cc/29NH-7848>] (дата обращения: 12.11.2019).

²⁷ [6, рукопись, pp. 16–20; 26, р. 347].

²⁸ См. цитируемые источники выше, примечание 27.

²⁹ См. цитируемые источники выше, примечание 27.

³⁰ См. Birbfakes, Jennifer Lawrence-Buscemi on Her Favorite Housewives [Deepfake], YouTube (Jan. 14, 2019). URL: <https://www.youtube.com/watch?v=r1jng79a5xc> [<https://perma.cc/VDT2-L54N>].

³¹ См. [29]. См. также [15] («В настоящее время законодательство США не может защитить жертв порнографических дипфейков, в основном потому, что суды до сих пор расценивали такие материалы как пародию или сатиру, которые надежно защищены Первой поправкой»).

²² См. в целом [27] (описывается проблема порно из мести).

²³ Cyber Exploitation – Law Enforcement FAQs, Off.Att’yGen. URL: <https://oag.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-law-enforcement-faqs.pdf> [<https://perma.cc/FBX2-55YZ>] (дата обращения: 12.11.2019) [далее – Cyber Exploitation FAQs].

²⁴ Там же.

²⁵ [26, pp. 347–348] («Наше общество до сих пор плохо справляется с защитой женщин и девушек, становящихся жертвами преступлений»).

за введение гражданской и уголовной ответственности за порно из мести строится вокруг нарушения права жертвы на неприкосновенность частной сексуальной жизни [26, pp. 350–356].

В случае порнографических дипфейков не возникает такого нарушения неприкосновенности частной сексуальной жизни. Ведь они не изображают какого-либо реально существующего человека³², а значит, ничья неприкосновенность частной сексуальной жизни не нарушается. Тем не менее зритель может не понимать, что видео является фейковым, и предполагать, что оно изображает реального человека, т. е. того, чье лицо было использовано.

Кроме того, дипфейки отличаются от других форм порнографии, созданной без согласия участников, и от порно из мести тем, что они могут затронуть практически бесконечное количество жертв. Сюда включаются как те, кто согласился на сексуально откровенные фото- и видеоизображения, которые затем были распространены без их согласия (т. е. жертвы обычного порно из мести), так и любой, кто имеет цифровые изображения [29].

II. МОРАЛЬНЫЕ И ЮРИДИЧЕСКИЕ ПРОБЛЕМЫ ДИПФЕЙКОВ

Быстрое распространение фейковых порнографических видео и стремительное развитие технологий, позволивших появиться феномену дипфейка, поднимают сложные юридические и моральные проблемы. В данном разделе обсуждается трудность в определении преступников и жертв дипфейков, а также проблема удаления дипфейков с интернет-площадок в свете Акта о соблюдении приличий в СМИ 1996 г. (CDA). Эти проблемы ведут к необходимости принятия адекватного уголовного законодательства.

³² В данной статье рассматриваются только те дипфейки, представляющие собой предмет предлагаемого автором закона, описанного в разд. V, в которых изображение лица одного человека правдоподобно накладывается на тело другого человека, участвующего в сексуальном акте. Другие разновидности дипфейка, например обработка речи или изображения узнаваемой персоны с целью симулировать какое-либо действие или речь, остаются за пределами данного исследования.

A. Проблема определения жертв дипфейков

Развитие новых технологий поднимает проблему определения жертв дипфейков, так как они изображают двух людей: того, кто участвовал в сексуальном акте, и того, чье лицо было наложено [6, рукопись, pp. 9, 16–17]. Несмотря на это, в большинстве статей и комментариев жертвой называют того, чье лицо было использовано (см., например, [6, рукопись, pp. 16–20]). Однако если видео было использовано без согласия участника акта, то не является ли этот человек также жертвой преступления? Кроме того, как в законе может быть определен причиненный вред, если дипфейк не изображает настоящих эпизодов из жизни жертвы? За что должна наступить ответственность, если не был показан ни один реальный человек? Человек, чье лицо было использовано, вероятно, не давал согласия на участие в порнографии, но это не так однозначно относительно того, чье тело было использовано. Актер, чье тело появляется на видео, мог согласиться на оригинальное порнографическое видео, но, скорее всего, не на то, чтобы чье-то лицо было приставлено к его телу. Это также жертва преступления. Таким образом, оба человека, изображенных в дипфейке, должны считаться жертвами.

B. Проблемы с установлением преступников и возмещением вреда

Дипфейки поднимают также сложные проблемы определения правонарушителя и удаления видео после публикации в Интернете. После того как видео опубликовано в Интернете, его сложно удалить, и, как правило, репутационный и эмоциональный ущерб уже нанесен³³. В идеале виновным по закону должен считаться тот, кто создал и опубликовал фейковое видео. Однако определить это лицо бывает сложно по двум причинам. Во-первых, многие площадки, например Reddit, Twitter и Pornhub, предусматривают анонимное использование; неудивительно, что дипфейки процветают именно на этих площадках³⁴. Во-вторых, создатели

³³ [30] («Почти невозможно удалить видео после того, как оно попало в Сеть... Если вы ищете волшебную палочку, которая удалит видео навсегда, то ее, видимо, не существует») (цитируется Eric Goldman, профессор права Школы права Университета Санта-Клары).

³⁴ См. [10] (отмечается, что дипфейки были впервые выложены на Reddit пользователем, который до сих пор остается анонимным); [16] (отмечается, что создатель FakeApp остался анонимным).

дипфейков могут использовать такие программы, как Tor, скрывающие IP-адрес, связанный с дипфейком³⁵.

Поскольку определить создателя видео затруднительно, жертва может попробовать подать в суд на интернет-платформу, разместившую видео. Тогда в действие вступает § 230 Акта CDA³⁶, который отменяет гражданскую и уголовную ответственность по законам штата за размещение контента третьей стороны. Согласно § 230, «провайдер или пользователь интерактивных компьютерных сервисов не рассматривается как лицо, публикующее или сообщающее какую-либо информацию, предоставленную другим производителем контента»³⁷. Это положение снимает с провайдеров контента ответственность за размещение контента третьей стороны на своих площадках³⁸. В теории этот иммунитет призван сохранить свободу выражения в Интернете, снимая ответственность за действия третьей стороны³⁹. Согласно § 230, веб-сайты могут размещать видео, обзоры, разрешенную рекламу и профили в социальных сетях, созданные сотнями миллионов пользователей, не неся ответственности за их содержание⁴⁰. Хотя § 230 прославляют как один из важнейших инструментов, защищающих свободу слова в Интернете⁴¹, он также позволяет интернет-платформам безнаказанно размещать порно из мести, а теперь и дипфейки [35].

Иммунитет по § 230 не позволяет жертвам дипфейков судиться с интернет-платформами за размещение дипфейков [36, pp. 423–424]. Жертвы дипфейков и пор-

но из мести не могут преодолеть иммунитет по Акту CDA, так как «суды предоставляют высокую степень защиты веб-сайтам в рамках § 230» [36, p. 423]. Широкая интерпретация судами Акта CDA основана на желании поддержать намерение Конгресса «поощрять свободную и открытую коммуникацию в Интернете, даже если эта коммуникация включает потенциально вредоносные высказывания или поведение» [36].

Действительно, в деле *Barnes v. Yahoo!, Inc.*⁴² Окружной суд постановил, что § 230 не позволяет привлечь компанию Yahoo! к ответственности «за ненадлежащее оказание услуг» за отказ удалить сексуально откровенные фотографии истца, размещенные ее бывшим партнером. Дело *Barnes* «продемонстрировало эффективность § 230... защищающего веб-сайты от исков за порно из мести» [36, p. 424]. Иск против дипфейка, несомненно, закончится с тем же результатом. С помощью § 230 веб-сайты защищены от ответственности за размещение дипфейков пользователями. Таким образом, жертвы дипфейков не пользуются защитой закона, поскольку они не могут ни определить правонарушителя из-за анонимности, ни подать в суд на интернет-платформу из-за § 230. Даже если правонарушитель определен, успешный иск против создателей дипфейков не затронет провайдеров контента.

Несмотря на защиту по Акту CDA, многие интернет-платформы сами запретили размещение дипфейков и удалили размещенные видео⁴³. Платформа Reddit обнародовала новые правила, касающиеся порнографии, сделанной без согласия участников. Согласно этим правилам, запрещено распространение фото- и видеоматериалов, изображающих любого человека обнаженным или занятым в любом акте сексуального поведения, если эти материалы были созданы или размещены без его разрешения, «включая фейковые изображения такого рода»⁴⁴.

³⁵ См. [31] (объясняется, как программа Tor позволяет пользоваться Интернетом анонимно).

³⁶ 47 U.S.C. § 230 (2012). В соответствующем разделе § 230 указано, что никакой провайдер или пользователь интерактивных компьютерных сервисов не несет ответственности за какие-либо действия, предпринятые добровольно, по ограничению доступа к материалам, которые провайдер или пользователь считает неприличными, непристойными, чрезмерно агрессивными, раздражающими или недопустимыми по иным причинам, независимо от того, защищены ли такие материалы Конституцией. Там же, § 230(c)(2).

³⁷ Там же, § 230(c)(1).

³⁸ См. там же; см. также [32].

³⁹ Section 230 of the Communications Decency Act, Electronic Frontier Found. URL: <https://www.eff.org/issues/cda230> [<https://perma.cc/N9CT-XXPY>] (дата обращения: 12.11.2019); см. также [33].

⁴⁰ Section 230 of the Communications Decency Act, выше примечание 39.

⁴¹ [34] (отмечается, что CDA часто называют «законом, который больше всего влияет на свободу слова в Сети»).

⁴² 570 F.3d 1096, 1105 (9th Cir. 2009).

⁴³ [37] (названы платформы, запретившие размещение дипфейков: Twitter, Pornhub, Gfycat (платформа для размещения GIF-файлов), Discord (платформа, размещающая чаты об играх)).

⁴⁴ Account and Community Restrictions: Do Not Post Involuntary Pornography, Reddit. URL: <https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/do-not-post-involuntary-pornography> [<https://perma.cc/23EF-SYBD>] (дата обращения: 12.11.2019); см. также Account and Community Restrictions: Do Not Post Sexual or Suggestive Content Involving Minors, Reddit. URL: <https://www.reddithelp.com/en/>

Аналогичным образом платформа Pornhub объявила, что считает дипфейки порнографией без согласия, нарушающей условия пользования платформой [38, 39]. Платформа Twitter также пообещала закрывать все аккаунты, распространяющие или производящие порнографию без согласия⁴⁵. Недавно платформа Tumblr заявила о своей новой политике, предусматривающей запрет на «нежелательную сексуализацию и сексуальное преследование»⁴⁶.

Проблемы с определением жертвы и правонарушителя, с ответственностью платформы еще больше запутываются из-за неясностей в применении действующего законодательства к дипфейкам. Этому мешают все те же проблемы с изменением изображения и анонимностью, так как остается неясным, кто именно должен нести ответственность за дипфейки. Некоторые меры направлены на создателей контента, другие – на социальные сети, неспособные отследить распространяемый на них контент, третьи – и на то и на другое. Примечательно, что такие платформы, как Pornhub, в целом не смогли удалить существующий контент такого рода и препятствовать размещению нового; уже одно это демонстрирует острую необходимость законодательных решений, затрагивающих как создателей, так и провайдеров такого контента [42].

categories/rules-reporting/account-and-community-restrictions/donot-post-sexual-or-suggestive [https://perma.cc/3F54-P7KX] (дата обращения: 12.11.2019).

⁴⁵ Non-Consensual Nudity Policy, Twitter (Mar. 2019). URL: https://help.twitter.com/en/rules-and-policies/intimate-media [https://perma.cc/F36B-G4UB]; [40].

⁴⁶ Tumblr Bans Non-Consensual Creepshots and Deepfake Porn, BBC News (Aug. 27, 2018). URL: https://www.bbc.com/news/technology-45323287 [https://perma.cc/TXK4-5BP2]; см. также Community Guidelines, Tumblr (Dec. 17, 2018). URL: https://www.tumblr.com/policy/en/community [https://perma.cc/P3E5-ULPQ]. Хотя публичный отказ от распространения порнографических дипфейков является хорошим знаком, они остаются доступными на таких платформах, как Reddit и Pornhub. На платформах Reddit, Pornhub, Twitter и Tumblr пользователи должны выявлять и сообщать о дипфейках [17]. Дипфейки продолжают появляться на этих платформах, потому что «невозможно проверить каждый элемент контента». Там же. Кроме того, после удаления контента правонарушители переходят на другие площадки, например, Erome и Sendvid [38]. Что еще хуже, компания Naughty America, занимающаяся развлечениями для взрослых, начала монетизацию дипфейков, разрешив пользователям получать комиссию за клипы, созданные методом дипфейка [41]. Andreas Hronopoulos, глава Naughty America, назвал «кастомизацию и персонализацию» будущим порноиндустрии. Там же.

С. Необходимость принятия уголовных мер

Каждая жертва дипфейка сталкивается с различными видами несовершенства законодательства. Например, человек, чье лицо было использовано в видео, может стремиться получить компенсацию за показ интимных частей тела, которые не принадлежат ему. Напротив, тот, чье тело было использовано, возможно, будет доказывать, что его тело слишком узнаваемо, и подавать в суд на этом основании. При этом, даже если оба будут признаны жертвами, они должны будут доказывать причинение ущерба по отдельности, что также проблематично, потому что видео не представляет собой изображения интимных деталей жизни конкретного человека [43].

Даже если ущерб доказан, определены жертвы и правонарушители, проблемой может стать получение возмещения. Гражданская ответственность подразумевает единственный правовой способ возмещения ущерба и принуждения правонарушителя к соблюдению общественных норм поведения. Ряд исследователей попытались определить и оценить возможный круг исков и реакцию рынка по этой проблеме⁴⁷.

Однако гражданская ответственность имеет свои ограничения и часто неэффективна. Например, многие создатели дипфейков могут оказаться неподсудны, а значит, наступление гражданской ответственности не остановит их противоправного поведения. Кроме того, жертвы дипфейков, особенно те, чьи тела (но не лица) были использованы в изображениях, могут не хотеть обнародовать свою личность, а гражданские иски могут быть поданы только под настоящим именем. Во-вторых, высокая стоимость расследования и ведения дел по дипфейкам ограничит круг истцов только теми, кто имеет на это достаточно ресурсов. И даже если эти дела против создателей дипфейков будут выиграны, нет гарантии, что дипфейки будут удалены из Интернета, учитывая иммунитет для провайдеров контента третьей стороны, предоставляемый Актом CDA⁴⁸.

⁴⁷ Решения, предлагаемые гражданским законодательством и регулирующие меры в этой области, требуют специального рассмотрения и не входят в сферу данной статьи. Возможность наступления гражданской ответственности за дипфейки и возмещения их жертвам обсуждалась в работах других исследователей. См., например, [6, рукопись, pp. 31–41].

⁴⁸ См. выше примечания 36–40 и соответствующий текст.

Принятие мер по уголовному законодательству не сталкивается с такими проблемами, как по гражданскому. Уголовное преследование за дипфейки будет иметь более выраженный сдерживающий эффект на правонарушителей. В работах Bobby Chesney и Danielle Citron отмечается, что, «имея статус неподсудности, человек может не бояться гражданских исков, но от тюрьмы это его не защитит» [6, рукопись, р. 42]. Кроме того, правоохранительные органы обладают гораздо большими ресурсами, чем большинство истцов, даже знаменитостей, которые они могут использовать для расследования и ведения дел по дипфейкам. Эти аргументы были подробно рассмотрены в работах, доказывающих необходимость криминализации порно из мести⁴⁹. Кроме того, за последние сто лет введение уголовной ответственности за вторжение в частную жизнь получило значительную поддержку в правовой литературе⁵⁰ и в законодательстве – от уголовных наказаний за раскрытие частной финансовой⁵¹ и медицинской информации⁵² и кражи личной информации⁵³ до Акта о предотвращении вуайеризма посредством видео (Video Voyeurism Prevention Act) 2004 г.⁵⁴, которым запрещается намеренное изготовление и трансляция изображения другого человека раздетым. Наконец, уголовное наказание за порнографические дипфейки подаст более жесткий сигнал по сравнению с гражданскими мерами о том, что общество считает такое поведение неприемлемым⁵⁵. В частности, тем

самым передается мысль, что это поведение выходит за рамки нормы и что оно наносит ущерб не только конкретному гражданину, но и обществу в целом [26, pp. 361–363]. Учитывая, что жертвами таких дипфейков становятся преимущественно женщины и девушки, меры общественной защиты в форме уголовного закона вполне оправданы.

III. ДЕЙСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО

Уже более двух столетий законодатели признают необходимость для закона и правовых институтов идти в ногу с развитием технологий⁵⁶. Реальность, однако, не соответствует этим стремлениям⁵⁷. Стараюсь не отставать от быстрого развития технологий, право все же отстает⁵⁸. Закон о дипфейках не является исключением [49]. Здесь мы сосредоточимся на федеральных законах и законах уровня штата, преимущественно уголовных, которые в настоящее время предусматривают наказания за подобное поведение, включая создание и распространение порнографии без согласия участников и порно из мести. Такие законы могут дать аналогии и рамки для анализа ситуации с дипфейками.

кон создает в обществе комплекс значений и общего понимания между государством и обществом», а также: «... поскольку закон создает и определяет общественные нормы, постольку он имеет важное культурное значение» [46, р. 407].

⁵⁶ Letter from Thomas Jefferson to Samuel Kercheval (July 12, 1816), in 10 The Writings of Thomas Jefferson 37, 42–43 (New York, G. P. Putnam's Sons 1899). В 1816 г. Томас Джефферсон писал: «Законы и институты должны идти рука об руку с прогрессом человеческой мысли. По мере того, как мысль становится более развитой, более просвещенной, делаются новые открытия, раскрываются новые истины, а нормы поведения и мнения изменяются вместе с меняющимися обстоятельствами, институты должны также меняться, не отставая от времени». Там же, р. 43.

⁵⁷ Профессор Jr. Henry H. Perritt выдвинул две идеи, определяющие взаимоотношения между законом и технологиями: во-первых, что технологические изменения являются главным источником тех проблем человечества, на которые должен отвечать закон, и, во-вторых, что «закон отстает от технологий» потому, что рыночные силы и традиции общего права требуют, «чтобы правовая система не предопределяла траекторию применения технологий и разработки новых продуктов» [47].

⁵⁸ Там же. Существует понятие «отставание права», означающее, что право всегда отстает от других областей и что развитие науки и технологии является «силой, определяющей текущую повестку, на которую право может только реагировать» [48, pp. 768–769].

⁴⁹ См. [26, pp. 361–365] (обсуждается необходимость наступления правовой ответственности за порно из мести, поскольку гражданские меры возмещения неэффективны); см. также [44, pp. 36–37] (высказывается требование криминализации порно из мести на федеральном уровне).

⁵⁰ Почти 130 лет назад Samuel D. Warren и Louis D. Brandeis впервые показали, что уголовный закон должен предусматривать ответственность как за тяжкое преступление за публикацию «любоей информации, касающейся частной жизни другого человека, при наличии письменной просьбы... не публиковать такой информации» при условии, что эта информация не относится к квалификации данного человека для занятия какой-либо государственной должности или профессии и не представляет государственного интереса» [26, р. 346, п. 11] (цитируя [45, р. 219, п. 8]).

⁵¹ См. 5 U.S.C. § 552(b)(4) (2012).

⁵² См. 42 U.S.C. § 1320d-6 (2012).

⁵³ См. в целом 18 U.S.C. § 1028 (2012).

⁵⁴ 18 U.S.C. § 1801.

⁵⁵ Citron писал о криминализации домашнего насилия: «За-

А. Федеральное законодательство

Нет ни одного федерального закона, предусматривающего уголовную ответственность конкретно за дипфейки и порно из мести. Таким образом, федеральное законодательство и прокуратура в настоящее время не могут справиться с распространением в Интернете порнографии, созданной без согласия участников.

1. Действующее уголовное федеральное законодательство

Не имея специализированного закона для наказания тех, кто создает и распространяет дипфейки, обвинители пользуются другими федеральными уголовными законами в области киберпреступности⁵⁹. Среди них различные положения ст. 18 Свода законов США, в которых устанавливается уголовная ответственность за требование выкупа, вымогательство, угрозы похищения людей; домогательство в Сети; преследование в Сети [50, pp. 12–14]. Могут использоваться такие положения, как угрозы с помощью средств коммуникации; незаконный доступ к компьютеру; преследование как домашнее насилие⁶⁰. Далее мы разберем каждое из этих положений.

Согласно ст. 18 U.S.C. § 875(c), виновный приговаривается к штрафу, тюремному заключению сроком до двух лет или и тому и другому, если он: «(1) намеренно участвует в акте коммуникации, содержащем реальную угрозу причинения ущерба обмену между штатами и международному обмену, и (2) намеренно придает акту коммуникации характер угрозы или знает, что получатель угрозы интерпретирует ее как угрозу»⁶¹. Учитывая, что выкладывание дипфейка в Сеть считается «актом коммуникации»⁶² согласно разд. 875 и при условии, что присутствуют остальные составляющие разд. 875(c), обвинитель может предъявить создателю дипфейка нарушение разд. 875(c).

⁵⁹ Cyber Exploitation FAQs, выше примечание 23.

⁶⁰ См. в целом 18 U.S.C. § 875, 1030, 2261A (2012).

⁶¹ Cyber Exploitation FAQs, выше примечание 23 (парафразируя ст. 18 U.S.C. § 875(c)).

⁶² Например, в деле *United States v. Jeffries* Окружной суд постановил, что музыкальный видеоклип представлял собой угрожающий акт коммуникации согласно § 875(c), потому что «закон предусматривает любую угрозу, независимо от того, была ли она передана устно (лично, по телефону) или письменно (письмом, электронным письмом, факсом), с помощью видео или песни, старомодными или самыми современными способами». 692 F.3d 473, 482 (6th Cir. 2012).

Кроме того, иск может быть предъявлен по ст. 18 U.S.C. § 1030 за незаконный доступ к компьютеру, т. е. взлом компьютера (хакинг)⁶³. Это положение может быть использовано, если порнографические материалы были получены через незаконный доступ к компьютеру или электронной почте жертвы [50, p. 16]. Наказание также может включать штрафы, тюремное заключение или и то и другое⁶⁴, а также может возрасти в зависимости от того, как виновный получил доступ. Например, если информация получена путем кражи логинов и паролей, то может применяться более строгое наказание за кражу личной информации с обязательным лишением свободы на два года⁶⁵.

В-третьих, при ведении дел, подобных дипфейкам и порно из мести, федеральные обвинители применяли статью о преследовании в Сети, 18 U.S.C. § 2261A⁶⁶. Это положение применяется, когда речь идет о действиях, которые «заставили испытывать обоснованный страх смерти или тяжких телесных повреждений по отношению... (i) к самому себе; (ii) близкому члену семьи или (iii) супругу или близкому партнеру»⁶⁷. Виновный должен иметь намерение «убить, причинить телесные повреждения, преследовать, запугать, следить за [жертвой]» с теми же намерениями; наказание включает штраф, тюремное заключение или и то и другое⁶⁸. Таким образом, если распространение материалов из мести сочетается с преследованием в Сети или сравнимо по уровню с таковым, то возможно наступление уголовной ответственности⁶⁹. В деле *United States v. Matusiewicz*⁷⁰ обвинение опровергло мнение о чрезмерной широте

⁶³ См. 18 U.S.C. § 1030; [50, p. 16].

⁶⁴ См. Cyber Exploitation FAQs, выше примечание 23.

⁶⁵ См. в целом *United States v. Barrington*, 648 F.3d 1178 (11th Cir. 2011).

⁶⁶ 18 U.S.C. § 2261A(1)(A), 2261A(2)(A) (2012); см. [51, p. 12].

⁶⁷ 18 U.S.C. § 2261A(1)(A).

⁶⁸ Там же; см. Cyber Exploitation FAQs, выше примечание 23.

⁶⁹ Согласно опросу EndRevengePorn.org, 49 % респондентов подвергались домогательствам или преследованию в Сети со стороны пользователей, видевших размещенное в Сети порно из мести с их участием. *Revenge Porn Statistics*, выше примечание 26 (показаны результаты опроса, проводившегося на EndRevengePorn.org с августа 2012 г. по декабрь 2013 г., с важным примечанием, что выборка состояла преимущественно из женщин).

⁷⁰ 84 F. Supp. 3d 363 (D. Del. 2015).

ст. 18 U.S.C. § 2261A(2), тем самым дав возможность применять ее к случаям преследования в Сети с применением порнографии⁷¹.

Наконец, если материал порно из мести содержит изображения несовершеннолетних, то обвинение может быть выдвинуто по ст. 18 U.S.C. § 2251 за производство детской порнографии и ст. 18 U.S.C. § 2422(b) за соблазнение или соращение несовершеннолетнего⁷². Опубликованное в 2016 г. исследование показало, что как минимум 3 % жертв порно из мести были в возрасте между пятнадцатью и семнадцатью годами [52], а в исследовании BBC News было показано, что возраст жертв порно из мести в мире начинается от одиннадцати лет [53]. Если жертва несовершеннолетняя, то вышеуказанные статьи могут быть использованы при обвинении за создание и распространение таких материалов.

2. Ранее предложенные федеральные уголовные законы

Правоведы⁷³ и заинтересованные группы⁷⁴ выступают за принятие федерального закона, прямо запрещающего порнографию без согласия⁷⁵. Ими предложены проекты законов, устанавливающих ответственность за порно из мести и дипфейки.

а. Закон 2017 г. «О прекращении домогательств в Сети с использованием изображений пользователя, сделанных без его согласия»: The ENOUGH Act

В 2016 г. член Конгресса Jackie Speier (D-CA) представила акт о защите частной жизни (Intimate Privacy Protection Act, IPPA)⁷⁶, который вводил уголовную ответственность за распространение порнографии без согласия участников⁷⁷. Представляя проект за-

кона, Speier указала, что его необходимо принять потому, что большинство жертв порно из мести не имеет достаточно средств на гражданские иски; таким образом, введение уголовной ответственности на федеральном уровне должно исправить ситуацию⁷⁸. Срок рассмотрения проекта истек к концу 114-го заседания Конгресса.

Затем законопроект был изменен⁷⁹ и в конце 2017 г. подан одновременно в Сенат и в палату представителей под названием «О прекращении домогательств в Сети с использованием изображений пользователя, сделанных без его согласия» (Ending

ми, или любого другого средства обмена между штатами или государствами, для распространения визуального изображения человека, участвующего в сексуально откровенных действиях, которое позволяет визуально идентифицировать личность по самому изображению или информации, размещенной совместно с изображением, или обнаженные гениталии или, в случае женщины в постпубертатном возрасте, сосок, при условии отсутствия согласия этого человека на такое распространение, влечет ответственность в виде штрафа, установленного данной статьей, или лишения свободы сроком до пяти лет, или и того и другого». Там же § 1802(a). Предусматривалось исключение из этого положения в случае использования таких изображений для целей охраны правопорядка, судебных процедур и в других случаях добросовестного использования в интересах общества, а также если изображение было сделано добровольно в публичном месте или в предусмотренной законом коммерческой ситуации. Законопроект также особо выделял провайдеров телекоммуникационных и интернет-услуг, освобождая их от ответственности согласно § 230, кроме случаев, когда провайдер «привлекает или распространяет контент, о котором ему известно, что он нарушает требования данного раздела». Там же § 1802(b)(4).

⁷⁸ Press Release, Congresswoman Jackie Speier, Congresswoman Speier, Fellow Members of Congress Take on Nonconsensual Pornography, AKA Revenge Porn (July 14, 2016). URL: <https://speier.house.gov/media-center/press-releases/congresswoman-speier-fellow-members-congress-take-nonconsensual> [<https://perma.cc/ZE25-WQST>]; см. также [56] (обсуждается попытка Speier ввести такой закон еще в 2014 г.).

⁷⁹ Критики законопроекта IPPA указывали, что он может повредить добросовестной журналистике и ограничить возможности журналистов публиковать фото- и видеоматериалы в интересах общества [57]. Законопроект ENOUGH Act снял это возражение, предусматривая, что лицо, публикующее материалы, может нести ответственность только в случае, если «нет оснований считать, что распространяемое изображение затрагивает общественные интересы». Там же. В комментарии для интернет-площадки Bustle сенатор Kamala Harris пояснил, что законопроект «устанавливает узкие рамки уголовной ответственности». Там же. В законопроекте также предусматривались оговорки, призванные защитить права в рамках Первой поправки. Там же.

⁷¹ Там же. Рр. 366–368.

⁷² 18 U.S.C. § 2251, 2422(b).

⁷³ См. [51, р. 3]. См. также [54].

⁷⁴ Cyber C.R. Initiative. URL: <https://www.cybercivilrights.org/> [<https://perma.cc/Z5SF-9F6D>] (дата обращения: 12.11.2019); см. также [55].

⁷⁵ Advocacy, Cyber C.R. Initiative. URL: <https://www.cybercivilrights.org/advocacy/> [<https://perma.cc/TG74-AML3>] (дата обращения: 12.11.2019).

⁷⁶ Intimate Privacy Protection Act of 2016, H.R. 5896, 114th Cong. (2016).

⁷⁷ В проекте закона предусматривалось (H.R. 5896): «Намеренное использование почты, любого интерактивного компьютерного сервиса, или средства электронной коммуникации, или системы электронной коммуникации для обмена между штата-

Nonconsensual Online User Graphic Harassment Act of 2017, ENOUGH)⁸⁰. Закон должен был явиться поправкой к ст. 18 Свода законов США, так чтобы становилось незаконным намеренно использовать любые средства коммуникации между штатами или государствами для распространения интимных изображений человека:

«(1) зная или игнорируя –

(A) отсутствие согласия этого человека на такое распространение;

(B) обоснованные ожидания этого человека, что такое изображение останется неопубликованным;

(C) ущерб, который такое распространение причинит этому человеку; а также (2) не имея объективно обоснованного убеждения, что такое распространение затрагивает общественные интересы»⁸¹.

Закон ENOUGH определяет интимное изображение как любое изображение:

«(A) позволяющее визуально идентифицировать личность человека по самому изображению или информации, размещенной совместно с изображением;

(B) на котором:

(i) индивидуум участвует в сексуально откровенных действиях или

(ii) видны обнаженные гениталии или, в случае женщины в постпубертатном возрасте, сосок;

(C) на котором содержание, описанное в подпараграфе (B), не является симуляцией»⁸².

Наказание предусматривалось в виде штрафа, тюремного заключения до пяти лет или обеих мер вместе⁸³. Законопроект ENOUGH предусматривал исключения для целей охраны правопорядка, судебных процедур и «провайдеров информационного контента», как определено в ст. 47 U.S.C. § 230(f), «кроме случаев, когда провайдер коммуникационных услуг намеренно поощряет или распространяет контент, о котором ему известно, что он нарушает требования данного раздела»⁸⁴. Хотя законопроект ENOUGH имел сторонников как среди республиканцев, так и среди демократов, он не вышел за пределы комис-

сии и не был рассмотрен до конца 115-го заседания Конгресса⁸⁵.

b. Акт 2018 г. о запрете дипфейков, созданных со злым умыслом

В конце декабря 2018 г. сенатор Ben Sasse (R-NE) представил законопроект, предусматривающий уголовную ответственность за злоумышленное создание и распространение дипфейков, – Акт 2018 г. о запрете дипфейков, созданных со злым умыслом (the Malicious Deep Fake Prohibition Act of 2018, MDFPA)⁸⁶. Этот Акт запрещает использование любых средств коммуникации между штатами с целью:

«(1) создания дипфейка для его распространения, заведомо зная, что такое распространение повлечет за собой криминальные или правонарушающие действия согласно федеральному, местному, племенному законодательству, законодательству штата; или

(2) распространения аудиовидеозаписи при условии:

(A) фактического знания о том, что данная аудиовидеозапись является дипфейком и

(B) знания о том, что распространение данной аудиовидеозаписи повлечет за собой криминальные или правонарушающие действия согласно федеральному, местному, племенному законодательству, законодательству штата»⁸⁷.

Законопроект MDFPA определяет дипфейк как «аудиовидеозапись, созданную или измененную таким образом, что она воспринимается как аутентичная запись реальной речи или действий индивидуума»⁸⁸. Он должен был применяться к индивидуальным создателям дипфейков, размещающим их с незаконными целями (например, мошенничество) на таких платформах, как Facebook, однако платформы можно было бы привлечь к ответственности, только если они знали, что распространяют дипфейк. Предусматривалось наказание в виде штрафа или лишения свободы

⁸⁵ См. US S2162, Bill Track 50. URL: <https://www.billtrack50.com/BillDetail/897787> [<https://perma.cc/FX4S-GPK5>] (дата обращения: 12.11.2019).

⁸⁶ S. 3805, 115th Cong. (2018).

⁸⁷ Там же.

⁸⁸ Там же. Согласно MDFPA, «термин “аудиовидеозапись” (A) предполагает любую аудио- или видеoinформацию в электронной форме и (B) включает любые фотографии, кинофильмы, видеозаписи, электронные изображения или звукозаписи». Там же.

⁸⁰ S. 2162, 115th Cong. (2017); H.R. 4472, 115th Cong. (2017). В данной статье мы цитируем преимущественно версию.

⁸¹ S. 2162.

⁸² Там же.

⁸³ Там же.

⁸⁴ Там же.

сроком до двух лет, или, если дипфейк мог вызвать акт насилия или подорвать деятельность правительства или ход выборов, до десяти лет⁸⁹. Сенатор Sasse внес законопроект MDFPA за день до закрытия сессии в декабре 2018 г.; проект был отправлен в Юридический комитет Сената, срок его представления истек в конце 2018 г.⁹⁰ Он не получил поддержки⁹¹.

В. Законодательство штатов

В настоящее время ни один штат не предусматривает уголовной ответственности за дипфейк. Как и на федеральном уровне, жертвы порнографических дипфейков, желающие подать иски по законодательству штатов, вынуждены обращаться к законам о сопутствующих преступлениях, например, о порно из мести. В отсутствие федеральных законов о порнографии без согласия жертвы довольствуются «разрозненными уголовными законами штатов, часто неадекватными ситуации» [51, р. 3]. Разброс в этих законах велик – от ответственности за порно из мести как за тяжкое преступление до расценивания его как мисдиминора⁹² и даже до полного отсутствия наказания⁹³. В данном разделе рассмотрены штаты Калифорния, Техас, Флорида и Нью-Йорк – штаты с наибольшим количеством исков по киберпреступлениям⁹⁴ и с самой большой численностью населения⁹⁵.

⁸⁹ Там же.

⁹⁰ См. US S3805, Bill Track 50. URL: <https://www.billtrack50.com/BillDetail/1000397> [<https://perma.cc/2HEQ-4WYU>] (дата обращения: 12.11.2019).

⁹¹ Там же.

⁹² Мисдиминор (англ. *misdemeanour*) – в уголовном праве США и Великобритании категория наименее опасных преступлений, граничащих с административными правонарушениями. – Прим. ред.

⁹³ См. [58, pp. 956–957] (обобщены различные подходы законодательств штатов к установлению уголовной ответственности за порно из мести). Согласно исследованию Cyber Civil Rights Initiative, в настоящее время 41 штат имеет такие законы. Cyber C.R. Initiative, выше примечание 74.

⁹⁴ См. в целом Fed. Bureau of Investigation, 2017 Internet Crime Report (2017). URL: https://pdf.ic3.gov/2017_IC3Report.pdf [<https://perma.cc/Y2S8-8RRE>].

⁹⁵ US States – Ranked by Population 2019, World Population Review. URL: <http://worldpopulationreview.com/states/> [<https://perma.cc/FSA7-NGAR>] (дата обращения: 12.11.2019).

1. Калифорния

а. Порно из мести

В 2013 г. законодательство штата Калифорния ответило на волну порно из мести изменением существовавшего ранее уголовного закона о нарушении общественного порядка⁹⁶. Изменения вступили в действие 1 октября 2013 г. и коснулись ст. 647 Уголовного кодекса штата Калифорния. Устанавливалось, что за порнографию без согласия предъявляется обвинение в нарушении общественного порядка:

«...лицу, которое намеренно распространяет изображение интимных частей тела другого опознаваемого лица, или изображение человека, участвующего в половом акте, содомии, оральном совокуплении, сексуальном проникновении, или изображение мастурбации изображенного человека, если участвующие лица считали или соглашались, что указанные изображения должны остаться частными при обстоятельствах, в которых лицо, распространяющее такие изображения, знает или должно знать, что их распространение вызовет серьезный эмоциональный стресс у изображенного на них лица»⁹⁷.

Соответственно, лицо, намеренно распространяющее порнографические материалы опознаваемой жертвы без его разрешения, виновно в нарушении общественного порядка, если знает или должно было знать, что это деяние вызовет серьезный эмоциональный стресс у изображенного на них лица и жертва испытывает этот стресс⁹⁸. Осужденный по данной статье виновен в нарушении общественного порядка, что составляет мисдиминор⁹⁹. Максимальное наказание составляет шесть месяцев заключения в тюрьме штата, или штраф до тысячи долларов, или и то и другое¹⁰⁰. Наказание ужесточается за повторные нарушения или если жертвой является несовершеннолетний¹⁰¹.

б. Преследование в Сети

Калифорния стала первым штатом, где было введено наказание за киберпреследование [59, р. 358]. Это было сделано не с помощью особого закона, а с помощью внесения изменений в существовавшие законы о преследовании, чтобы учесть случаи с применением

⁹⁶ Cal. Penal Code § 647(j)(4)(A) (West 2019).

⁹⁷ Там же.

⁹⁸ Там же.

⁹⁹ Там же, § 647.

¹⁰⁰ Там же, § 19.

¹⁰¹ Там же, § 647(1)(1)–(2).

Сети¹⁰². Согласно Уголовному кодексу Калифорнии, ст. 646.9, незаконно «намеренно, злоумышленно и последовательно преследовать <...> или намеренно, злоумышленно домогаться <...> другого человека» и «правдоподобно угрожать <...> с целью заставить человека опасаться за свою безопасность или за безопасность своих близких»¹⁰³. Таким образом, для признания виновным следует доказать не только факт преследования или домогательства, но и намеренность и правдоподобность угрозы¹⁰⁴. Закон учитывал угрозы, сделанные «с использованием средств электронной коммуникации», включая мобильный телефон и компьютер¹⁰⁵. В Калифорнии преследование может рассматриваться и как тяжкое преступление, и как мисдиминор в зависимости от обстоятельств дела¹⁰⁶.

В 2009 г. в Калифорнии была принята ст. 653.2 Уголовного кодекса с целью ликвидировать пробел ст. 646.9, связанный с электронными средствами коммуникации, и «дать возможность привлекать к ответственности тех, кто преследует жертву с помощью электронных средств» [60, р. 741]. Эта узконаправленная статья дополняет законодательство против преследования и устанавливает следующее:

«Намеренные действия с целью вызвать у другого лица опасения за свою безопасность или безопасность члена семьи с применением средств электронной коммуникации и без согласия данного лица, или с целью вызвать у данного лица опасения перед неизбежным причинением нежелательного физического контакта, ущерба, домогательства посредством третьей стороны, с помощью электронного распространения, публикации, рассылки, создания гиперссылок, предоставления для скачивания персональной идентифицирующей информации, включая, но не только цифровые изображения другого лица или электронные сообщения о другом лице, имеющие характер домогательства, которые могут спровоцировать или вызвать вышеуказанные незаконные действия, относятся к категории “мисдиминор” и наказываются лишением свободы на срок до одного года, штрафом в размере не более одной тысячи долларов или штрафом и лишением свободы совместно»¹⁰⁷.

Наличие фразы «цифровые изображения другого лица» может дать возможность в будущем применить данную статью к случаям порно из мести или дипфейков.

с. Другие уголовные законы в данной сфере

Хотя Уголовный кодекс штата Калифорния включает разделы о присвоении личности¹⁰⁸, персонация [выдача себя за другое лицо], будь то цифровая или иная, сама по себе не является уголовным преступлением в этом штате¹⁰⁹. Так, ст. 528.5 Уголовного кодекса Калифорнии устанавливает ответственность за «намеренную, достоверную и совершенную без согласия выдачу себя за иное реальное лицо через интернет-сайт или с помощью другого электронного средства с целью... совершения мошеннических действий в отношении другого лица»¹¹⁰. Такое деяние относится к категории «мисдиминор» и наказывается лишением свободы в окружной тюрьме на срок до одного года, штрафом в размере не более одной тысячи долларов или штрафом и лишением свободы совместно¹¹¹. Статья 529 Уголовного кодекса Калифорнии дает более расширенное толкование персонации: «...ложно выдавать себя за другого человека»¹¹². Однако ст. 529 также применяется, только если «под видом другого человека» обвиняемый совершил одно или несколько из перечисленных мошеннических действий¹¹³. Наконец, в раздел персонации Уголовного кодекса Калифорнии входит положение о «краже

¹⁰⁸ Там же, § 528.

¹⁰⁹ В дополнение к перечисленным в статье преступлениям офис Генерального прокурора представил список других киберпреступлений. См. Cyber Exploitation FAQs, выше примечание 23.

¹¹⁰ Penal, § 528.5(a) (курсив автора).

¹¹¹ Там же § 528.5(d).

¹¹² Там же § 529.

¹¹³ Там же § 529(a). Незаконные действия включают те, в ходе которых лицо, виновное в персонации: (1) «становится гарантом или поручителем...», (2) подписывает или заверяет «любой письменный документ с целью представить, предъявить или использовать его как подлинный» или (3) подвергает представляемое лицо ответственности или наказанию или получает преимущество под видом этого лица. Там же. Выдача себя за другое лицо может рассматриваться и как тяжкое преступление, и как мисдиминор, в зависимости от обстоятельств дела. Wobbler, Black's Law Dictionary (11th ed., 2019). Предусматривается наказание в виде лишения свободы в окружной тюрьме на срок до одного года, штрафа в размере не более одной тысячи долларов или и того и другого совместно. Penal § 529(b).

¹⁰² Penal, § 646.9.

¹⁰³ Там же, § 646.9(a).

¹⁰⁴ Там же.

¹⁰⁵ Там же, § 646.9(g)–(h).

¹⁰⁶ Там же, § 646.9(a)–(c) (предусматривается, что нарушение судебного запрета или повторные правонарушения должны рассматриваться как тяжкое преступление).

¹⁰⁷ Penal, § 653.2(a).

личности»¹¹⁴. Согласно ст. 530.5, кража личности состоит в намеренном присвоении «идентифицирующей информации» другого лица и использовании этой информации «с любыми незаконными целями»¹¹⁵.

d. Предлагаемые законы против дипфейков

В попытке решить проблему дипфейков законодательная власть Калифорнии за последний год успела предложить несколько новых уголовных и гражданских законопроектов против этого явления.

Первое из этих предложений, Assembly Bill 602, было поддержано Гильдией киноактеров (Screen Actors Guild)¹¹⁶. В представленном проекте закона устанавливалась ответственность как за мисдиминор для лица, создающего ложные записи с целью их распространения, заведомо зная, что такая запись введет зрителя в заблуждение¹¹⁷. В ходе последующей доработки законопроекта Assembly Bill 602 уголовные наказания были удалены из него и заменены гражданской ответственностью за ущерб, возникший из-за намеренного создания и опубликования сексуально откровенных материалов без согласия участников¹¹⁸. В таком виде законопроект Assembly Bill 602 предусматривает гражданское возмещение экономических и штрафных убытков, судебных издержек, а также судебные запреты¹¹⁹. Согласно Assembly Bill 602, от ответственности освобождается лицо, публикующее

материалы в ходе сообщения о незаконной деятельности; в ходе судебной процедуры; в ходе исполнения служебных обязанностей сотрудника правоохранительных органов; в связи с законными общественными интересами; в ходе деятельности, представляющей политическую или общественную ценность; с целью комментирования или критики¹²⁰. Также поясняется, что сам факт изображения общественного деятеля недостаточен для признания сексуально откровенного материала имеющим общественную ценность¹²¹.

Другой законопроект, Assembly Bill 1280, определяет дипфейк как запись, которая была создана или изменена таким образом, что может быть ошибочно принята за настоящую запись реальной речи или действий лица, изображенного на ней¹²². В случае принятия данный законопроект создаст новый вид преступлений, состоящий в создании или распространении без согласия участников дипфейка, который изображает человека, участвующего в сексуальных действиях¹²³.

К концу законодательной сессии 2019 г. Assembly Bill 1280 оставался на рассмотрении комиссий, а Assembly Bill 602 был уже одобрен и законодательными органами и направлен губернатору для рассмотрения¹²⁴. Оба законопроекта вызвали критику

¹¹⁴ Там же, § 530.5.

¹¹⁵ Там же, § 530.5(a). Кража личности может рассматриваться и как тяжкое преступление, и как мисдиминор в зависимости от обстоятельств дела. Там же § 529(b).

¹¹⁶ См. Press Release, SAG-AFTRA, Action Alert: Support California Bill to End Deepfake Porn (Apr. 29, 2019). URL: <https://www.sagaftra.org/action-alert-support-california-bill-end-deepfake-porn> [<https://perma.cc/WQM9-22XF>]; California Legislation Takes First Steps Against Deepfakes, SAG-AFTRA (May 3, 2019). URL: <https://www.sagaftra.org/california-legislation-takes-first-steps-against-deepfakes> [<https://perma.cc/Y5QB-GU4J>].

¹¹⁷ См. Assemb. 602, 2019–2020 Leg., Reg. Sess. (Cal. 2019) (в представленном виде); Legislature Grapples with Three Bills to Address "Deepfake" Videos, Cal. News Publishers Ass'n (Mar. 29, 2019). URL: <https://cnpa.com/legislature-grapples-with-three-bills-to-address-deepfake-videos/> [<https://perma.cc/88AS-ULXH>].

¹¹⁸ Cal. Assemb. 602; см. также From a Field of Three, One Deepfake Bill Is Left, Cal. News Publishers Ass'n. URL: <https://cnpa.com/from-a-field-of-three-one-deepfake-bill-is-left/> [<https://perma.cc/4SUV-XYKF>] (дата обращения: 12.11.2019). Похожее предложение, Senate Bill 564, было подано в законодательную комиссию. См. S. 564, 2019–2020 Leg., Reg. Sess. (Cal. 2019).

¹¹⁹ Cal. Assemb. 602.

¹²⁰ Там же.

¹²¹ Там же.

¹²² Assemb. 1280, 2019–2020 Leg., Reg. Sess. (Cal. 2019).

¹²³ Там же. Assembly Bill 1280 также устанавливает уголовную ответственность за создание и распространение без согласия изображенного лица дипфейка с намерением принудить или обманом заставить избирателя голосовать за или против кандидата или предложение, если выборы состоятся в течение 60 дней. Там же. В другом предложенном законопроекте, Assembly Bill 730, устанавливается запрет лицу, комитету или иной организации в течение 60 дней до выборов с участием кандидата на выборную должность распространять *со злым умыслом* ложные аудио- и видеоматериалы, изображающие кандидата, с намерением навредить репутации кандидата или обманом заставить избирателей голосовать за или против него. Assemb. 730, 2019–2020 Leg., Reg. Sess. (Cal. 2019) (курсив автора) (дайджест законодательного совета).

¹²⁴ AB-602 Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action, Cal. Legis. Info. URL: http://leginfo.ca.gov/faces/billHistoryClient.xhtml?bill_id=201920200AB602 [<https://perma.cc/5FA6-Z4HH>] (дата обращения: 12.11.2019); AB-1280 Crimes: Deceptive Recordings, Cal. Legis. Info. URL: http://leginfo.ca.gov/faces/billHistoryClient.xhtml?bill_id=201920200AB1280 [<https://perma.cc/B4M6-NXNW>] (дата обращения: 12.11.2019).

по поводу соответствия Первой поправке со стороны общественных групп, включая такие группы, как Калифорнийское отделение Американского союза гражданских свобод (American Civil Liberties Union, the ACLU of California), Ассоциация новостных компаний Калифорнии (the California News Publishers Association), Ассоциация телерадиовещательных компаний Калифорнии (the California Broadcasters Association) [61, 62].

2. Техас

а. Порно из мести

В 2015 г. в штате Техас был принят (вступил в действие 1 сентября 2015 г.) закон против порно из мести под названием «Закон о защите личных отношений» (Relationship Privacy Act of 2015)¹²⁵. Статья 21.16 Уголовного кодекса штата Техас предусматривает уголовную ответственность за «незаконное раскрытие или распространение интимных визуальных материалов»¹²⁶. Ответственность наступает, если: (1) указанное раскрытие или распространение было сделано намеренно и без согласия жертвы, (2) жертва «имела основания ожидать, что визуальный материал останется в частном использовании», (3) раскрытие причинило вред жертве и (4) раскрытие позволило идентифицировать жертву «любым способом»¹²⁷. Распространение интимных визуальных материалов относится к категории «мисдиминор класса А» и карается штрафом в 4 000 долларов, лишением свободы до одного года или и тем и другим вместе¹²⁸.

б. Преследование в Сети

В штате Техас имеется один закон против преследования в целом, и он не дает прямых отсылок к киберпреследованию¹²⁹. Данный закон устанавливает ответственность за намеренное участие в действиях, направленных против другого лица (или членов его семьи) с целью домогательства или угроз (или создания страха) физического насилия или смерти, или заставляющих жертву обоснованно чувствовать до-

могательства, раздражение, тревогу, преследование, мучения, смущение, обиду и подобные страдания¹³⁰.

Преследование относится к категории тяжких преступлений третьей степени и наказывается лишением свободы от двух до десяти лет и штрафом до 10 000 долларов¹³¹. При повторных нарушениях категория меняется на вторую степень и наказывается лишением свободы от двух до двадцати лет и штрафом до 10 000 долларов¹³².

Хотя ст. 42.072 не выделяет киберпреследование или домогательства с применением электронных средств, апелляционный суд Техаса интерпретировал это положение как включающее средства электронной коммуникации¹³³. Кроме того, в положении о домогательствах вышеупомянутой ст. 42.07 устанавливается уголовная ответственность за «неоднократные электронные сообщения, посылаемые таким образом, чтобы вызвать обоснованные чувства домогательства, раздражения, тревоги, преследования, мучений, смущения, обиды у другого человека»¹³⁴. Этот случай классифицируется как мисдиминор класса В и наказывается лишением свободы на срок до 180 дней, штрафом до 2 000 долларов или и тем и другим совместно¹³⁵. В случае повторных нарушений, участия несовершеннолетних или нарушения судебного запрета это деяние будет относиться к категории «мисдиминор класса А» и караться штрафом в 4 000 долларов, лишением свободы до одного года или и тем и другим вместе¹³⁶.

с. Другие уголовные законы в данной сфере

Законодательство штата Техас ответило на появление домогательств в Интернете принятием в 2009 г. уголовного закона, направленного конкретно против персонации в Сети¹³⁷. Статья 33.07 устанавливает уголовную ответственность за два вида персонации¹³⁸. Первая категория, относящаяся к тяжким преступлениям третьей степени¹³⁹, состоит в использовании

¹²⁵ 2015 Tex. Gen. Laws 8723-26.

¹²⁶ Tex. Penal Code Ann. § 21.16 (West 2019).

¹²⁷ Там же, § 21.16(b).

¹²⁸ Там же, § 12.21, 21.16.

¹²⁹ Там же, § 42.072.

¹³⁰ Там же, § 42.072(a).

¹³¹ Там же, § 12.34, 42.072(b).

¹³² Там же, § 12.33, 42.072(b).

¹³³ Manuel v. State, 357 S.W.3d 66, 83 (Tex. App. 2011).

¹³⁴ Penal, § 42.07(a)(7).

¹³⁵ Там же, § 12.22, 42.07(c).

¹³⁶ Там же, § 12.21, 42.07(c).

¹³⁷ Там же, § 33.07.

¹³⁸ Там же.

¹³⁹ Там же, § 12.34, 33.07(c) (предусматривает от двух до десяти лет лишения свободы и штраф до 10 000 долларов).

«без согласия и с целью причинить вред, совершить мошеннические действия, запугивать или угрожать» имени или личности иного лица путем создания веб-страницы или сообщения в социальных сетях или на других веб-сайтах, кроме электронной почты и форумов¹⁴⁰. Вторая категория, мисдиминор класса А¹⁴¹, состоит в отправлении электронного письма, мгновенного, текстового или иного сообщения, содержащего «имя, электронный адрес, номер телефона или иную идентифицирующую информацию, принадлежащую другому лицу» без согласия этого лица и с намерением вызвать у получателя этого сообщения обоснованную уверенность, что оно было отправлено обладателем указанной информации или с его согласия, и с намерением «причинить вред или совершить мошеннические действия по отношению к любому лицу»¹⁴². Термин «идентифицирующая информация» определяется в ст. 32.51 как «информация, которая сама по себе или в сочетании с иной информацией идентифицирует человека»¹⁴³. В ст. 32.51 также устанавливается уголовная ответственность за мошенническое использование или владение идентифицирующей информацией¹⁴⁴.

3. Флорида

а. Порно из мести

В 2015 г. законодательство штата Флорида занялось проблемой порно из мести и ввело закон, устанавливающий уголовную ответственность за «сексуальные домогательства в Сети»¹⁴⁵. Это деяние определяется в законе как «публикация... сексуально откровенного изображения человека, которое содержит или передает личную идентифицирующую информацию изображенного лица [на веб-сайте] без согласия изображенного лица... без какой-либо законной цели,

с намерением вызвать существенный эмоциональный стресс у изображенного лица»¹⁴⁶. Нарушение относится к категории «мисдиминор первой степени» и наказывается лишением свободы на срок до одного года или штрафом до 1 000 долларов^{147, 148}. Повторные нарушения относятся к категории тяжких преступлений третьей степени и наказываются лишением свободы на срок до пяти лет или штрафом до 5 000 долларов¹⁹⁴.

б. Преследование в Сети

Во Флориде положение о преследовании в Сети появилось 1 июля 2004 г.¹⁴⁹ Это деяние определяется в законе как «участие в передаче или способствовании передаче через электронную почту или средства электронной коммуникации слов или изображений, направленных на вызывание существенного эмоционального стресса у другого лица и не выполняющих никакой законной функции»¹⁵⁰. Закон штата Флорида против преследования уникален также тем, что выделяет две категории преследования – обычное и с отягчающими обстоятельствами¹⁵¹. Обычное преследование состоит в «намеренном, злоумышленном и неоднократном» преследовании в Сети и классифицируется как мисдиминор первой степени¹⁵². Оно наказывается лишением свободы на срок до одного года или штрафом до 1 000 долларов¹⁵³. То же деяние плюс одно из следующих обстоятельств: (1) представляет достоверную угрозу, (2) нарушает судебный запрет или иное судебное решение или (3) направлено против несовершеннолетнего в возрасте до 16 лет – являются преследованием с отягчающими обстоятельствами; это тяжкое преступление третьей степени¹⁵⁴. Преследование с отягчающими обстоятельствами наказывается лишением свободы на срок до пяти лет или штрафом до 5 000 долларов¹⁵⁵.

¹⁴⁰ Там же, § 33.07(a).

¹⁴¹ Там же, § 12.21, 33.07(c) (предусматривает до одного года лишения свободы, или штраф в 4 000 долларов, или и то и другое).

¹⁴² Там же, § 33.07(b).

¹⁴³ Там же, § 32.51(a)(1) (включая имя, дату рождения, «уникальные биометрические данные», «уникальную электронную идентифицирующую информацию», «телекоммуникационную идентифицирующую информацию», «номер социального страхования или иные государственные идентифицирующие номера»).

¹⁴⁴ См. в целом там же, § 32.51.

¹⁴⁵ Fla. Stat. § 784.049 (2019).

¹⁴⁶ Там же, § 784.049(2)(c).

¹⁴⁷ Там же, § 784.049(3)(a); см. также там же, § 775.082(4)(a), 775.083(1)(d).

¹⁴⁸ Там же, § 784.049(3)(b); см. также там же, § 775.082(3)(e), 775.083(1)(c).

¹⁴⁹ Там же, § 784.048.

¹⁵⁰ Там же, § 784.048(d).

¹⁵¹ Там же, § 784.048(2)–(5).

¹⁵² Там же, § 784.048(2).

¹⁵³ Там же, § 775.082(4)(a), 775.083(1)(d), 784.048(2).

¹⁵⁴ Там же, § 784.048(3)–(5).

¹⁵⁵ Там же, § 775.082(3)(e), 775.083(1)(c), 784.048(3)–(5).

4. Нью-Йорк

а. Порно из мести

Нью-Йорк остается одним из двенадцати штатов, в которых нет уголовного наказания за порно из мести¹⁵⁶. Законопроект Senate Bill 642 стал третьей попыткой законодательства штата ввести уголовное наказание за порнографию без согласия¹⁵⁷. Закон был одобрен Сенатом 19 марта 2018 г., а затем передан в Ассамблею, где не получил поддержки, и срок его рассмотрения истек¹⁵⁸.

б. Преследование в Сети

Закон штата Нью-Йорк против преследования в Сети выделяет четыре категории этого правонарушения: преследование четвертой степени¹⁵⁹, третьей¹⁶⁰, второй¹⁶¹, первой степени¹⁶². Положение о преследовании четвертой степени не содержит упоминания о киберпреследовании или домогательствах в Сети¹⁶³. Далее ответственность нарастает в зависимости от таких факторов, как повторность нарушения, возраст жертвы, использование оружия¹⁶⁴.

Кроме того, штат Нью-Йорк имеет отдельное законодательство, направленное против криминальных домогательств¹⁶⁵. Так, лицо, намеренно «участвующее в действиях или неоднократно совершающее действия, которые вызывают серьезную тревогу или раздражение другого лица и не выполняют никакой законной функции», обвиняется в домогательствах второй степени¹⁶⁶. Однако такое нарушение наказывается всего лишь лишением свободы на срок до 15 су-

ток и штрафом до 250 долларов¹⁶⁷. Домогательство второй степени с отягчающими обстоятельствами подразумевает использование электронных средств коммуникации с целью угрозы физического насилия, нанесения вреда имуществу или членам семьи¹⁶⁸. Такое правонарушение относится к категории «мисдиминор класса А» и наказывается лишением свободы на срок до одного года или штрафом до 1 000 долларов¹⁶⁹.

с. Другие уголовные законы в данной сфере

Как и в Калифорнии, ст. 190.25 Уголовного кодекса штата Нью-Йорк устанавливает ответственность за персонацию в Сети только в сочетании с какой-либо из обозначенных в этом законе целей¹⁷⁰. Так, ст. 190.25 предусматривает, что криминальная персонация второй степени с использованием веб-сайта или другого средства электронной коммуникации состоит в выдаче себя за другое лицо с «намерением получить выгоду, или причинить ущерб, или совершить мошеннические действия в отношении другого лица»¹⁷¹. Криминальная персонация второй степени относится к категории «мисдиминор класса А» и наказывается лишением свободы на срок до одного года или штрафом до 1 000 долларов¹⁷².

д. Предлагаемые новые гражданские права

Законопроект Assembly Bill 8155 был внесен на рассмотрение Ассамблеи штата 31 мая 2017 г.¹⁷³ В нем делалась попытка решить проблему дипфейков путем создания новых гражданских прав и средств возмещения ущерба:

«...установить право на частную жизнь и право на публичность для живущих и умерших индивидуумов; установить, что личность индивидуума является его личной собственностью и может свободно передаваться и наследоваться; установить процедуру регистрации таких прав умерших людей через департамент штата; установить, что использование цифровых копий для целей торговли в сфере искусства является нарушением»¹⁷⁴.

¹⁵⁶ [63, p. 119] («Тридцать восемь штатов и округ Колумбия приняли законы против порнографии без согласия»).

¹⁵⁷ S. 642, 2017–2018 Leg., Reg. Sess. (N.Y. 2017).

¹⁵⁸ Senate Bill 642, N.Y. St. Senate. URL: <https://www.nysenate.gov/legislation/bills/2017/s642> [<https://perma.cc/TZ2F-9ZMU>] (дата обращения: 12.11.2019). После провала законопроекта, направленного против порно из мести, его сторонники обвиняли компанию Google и другие подобные технологические компании в лоббировании. См. [64, 65].

¹⁵⁹ N.Y. Penal Law § 120.45 (McKinney 2019) (мисдиминор класса B).

¹⁶⁰ Там же, § 120.50 (мисдиминор класса A).

¹⁶¹ Там же, § 120.55 (тяжкое преступление класса E).

¹⁶² Там же, § 120.60 (тяжкое преступление класса D).

¹⁶³ Там же, § 120.45 (включая только телефонную связь и использование GPS для установления местонахождения человека).

¹⁶⁴ Там же, § 120.50, 120.55, 120.60.

¹⁶⁵ См. в целом там же, § 240.25–240.32.

¹⁶⁶ Там же, § 240.26(3).

¹⁶⁷ Там же, § 70.15(4), 80.05(4), 240.26.

¹⁶⁸ Там же, § 240.30(1).

¹⁶⁹ Там же, § 70.15(1), 80.05(1), 240.30.

¹⁷⁰ См. там же, § 190.25.

¹⁷¹ Там же, § 190.25(4).

¹⁷² Там же, § 70.15(1), 80.05(1), 190.25.

¹⁷³ Assemb. 8155, 2017–2018 Leg., Reg. Sess. (N.Y. 2017).

¹⁷⁴ Assembly Bill A8155B, N.Y. St. Senate. URL: <https://www.nysenate.gov/legislation/bills/2017/a8155> [<https://perma.cc/Y9PF-8PZR>] (дата обращения: 12.11.2019) (обзор законопроекта).

Законопроект прошел рассмотрение Ассамблеи и был направлен в Сенат штата Нью-Йорк 18 июня 2018 г.¹⁷⁵ Широта формулировок представленной версии законопроекта вызвала серьезную критику со стороны развлекательных компаний, включая Disney и NBCUniversal), и Американской кинематографической ассоциации (Motion Picture Association of America)¹⁷⁶.

IV. ОГРАНИЧЕНИЯ СУЩЕСТВУЮЩИХ УГОЛОВНЫХ ЗАКОНОВ

Хотя против дипфейков могут быть использованы существующие (и предложенные) законы, все они имеют ограничения. В настоящем разделе исследуются недостатки существующих и предлагаемых законов в контексте дипфейков, включая ограничения, связанные с Первой поправкой.

А. Недостатки существующих и предлагаемых законов

1. Недостатки действующих уголовных федеральных законов и законов на уровне штатов против киберпреступности, преследования, криминальных угроз и домогательств

Сразу после появления феномена порно из мести его жертвы, их адвокаты и правоведы отметили, что существующие уголовные законы, как федеральные, так и на уровне штатов, недостаточны для того, чтобы наказать создателей и распространителей и возместить ущерб жертвам¹⁷⁷. Та же недостаточность существует и относительно порнографических дипфейков, то же верно и для существующего уголовного законодательства штатов, даже тех, где введена уголовная ответственность за порно из мести. Краткий обзор

норм, касающихся преследования, криминальных угроз и домогательств, показывает, что существующее законодательство не решает проблем, связанных с порнографией без согласия, будь то порно из мести или порнографические дипфейки.

Федеральный закон о преследовании¹⁷⁸ и соответствующие законы многих штатов, таких как Калифорния¹⁷⁹ и Техас¹⁸⁰, включают специфическое требование относительно страха. Для осуждения обвиняемого необходимо, чтобы он намеренно или по небрежности (в зависимости от юрисдикции) угрожал жертве или действовал таким образом, чтобы жертва испытывала страх физического насилия или смерти относительно себя или члена своей семьи¹⁸¹. Аналогичным образом другие законы также содержат требование доказать «эмоциональный стресс» жертвы¹⁸². Законы против «криминальной угрозы» также могут быть бессильны против дипфейков, так как требуют доказательства наличия угрозы похищения или причинения физического вреда жертве¹⁸³. Хотя дипфейки могут нанести вред жертве, они не всегда представляют собой угрозу нанесения вреда. Хотя многие жертвы порнографии без согласия страдают от эмоционального стресса¹⁸⁴ и опасаются за свою безопасность, особенно если личная информация также была опубликована¹⁸⁵, эти

¹⁷⁸ 18 U.S.C. § 2261A (2012).

¹⁷⁹ Cal. Penal Code § 646.9 (West 2019).

¹⁸⁰ Tex. Penal Code Ann. § 42.072 (West 2019).

¹⁸¹ Cp. 18 U.S.C. § 2261A(1)(A) (относится к действиям, которые «вызывают у жертвы обоснованный страх смерти или серьезного физического ущерба по отношению к (i) самому человеку, (ii) члену семьи или (iii) супругу (супруге) или близкому партнеру такого человека»), with Tex. Penal Code Ann. § 42.072 (West 2019) (устанавливается ответственность за угрозы «(A) физического ущерба или смерти другого человека; (B) физического ущерба или смерти члена семьи или домохозяйства или человека, с которым имеются близкие отношения; или (C) преступления, которое будет совершено против имущества другого человека»).

¹⁸² См., например, Fla. Stat. § 784.048(1)(d) (2019).

¹⁸³ См. 18 U.S.C. § 875(c).

¹⁸⁴ [26, p. 351] (сообщается, что «80 % жертв порно из мести испытывают значительный эмоциональный стресс и беспокойство»).

¹⁸⁵ Там же, pp. 350–351 («Порнография без согласия повышает риск преследования в реальности и физического нападения. Из 1 244 опрошенных более 50 % жертв сообщили, что их фото в обнаженном виде были опубликованы с указанием их полного имени и профиля в социальных сетях; более 20 % жертв сообщили, что вместе с фотографией были опубликованы их электронные адреса и номера телефонов»).

¹⁷⁵ Там же.

¹⁷⁶ Katyanna Quach, *New York State Is Trying to Ban ‘Deepfakes’ and Hollywood Isn’t Happy*, Register (June 12, 2018, 10:22 PM). URL: https://www.theregister.co.uk/2018/06/12/new_york_state_is_trying_to_ban_deepfakes_and_hollywood_isnt_happy/ [<https://perma.cc/33HL-8X2P>]; см. также Memorandum from the Motion Picture Ass’n of Am., Inc. (June 8, 2018). URL: https://www.rightofpublicityroadmap.com/sites/default/files/pdfs/mpaa_opposition_to_a8155b.pdf [<https://perma.cc/L6DV-TF4H>]; Letter from Lisa Pitney, Vice President, Walt Disney Co., to Senator Martin Golden (June 8, 2018). URL: https://www.rightofpublicityroadmap.com/sites/default/files/pdfs/disney_opposition_letters_a8155b.pdf [<https://perma.cc/TBL6-V5U5>].

¹⁷⁷ См., например, [26, p. 365; 51, p. 12].

субъективные аспекты сложно, если вообще возможно, доказать в суде.

Кроме того, указанные требования упрощают вред, причиняемый порнографией без согласия. Само требование, чтобы сторона обвинения доказывала эти субъективные аспекты, сигнализирует о том, что публичной демонстрации сексуально откровенного поведения жертвы без ее согласия недостаточно самой по себе для судебного иска¹⁸⁶. Более того, многие законы о преследованиях и домогательствах, например, законы Техаса¹⁸⁷ и Флориды¹⁸⁸, требуют систематического поведения или неоднократных случаев¹⁸⁹. Таким образом, публикация одного материала, даже если он стал вирусным, не будет считаться преступлением по этим законам [44, pp. 24–25].

Законы о персоналии также не отвечают многим сценариям в случае порнографии без согласия. Прежде всего, они применимы только тогда, когда изображение распространялось якобы от лица жертвы¹⁹⁰. Очевидно, что это далеко не всегда так, особенно в отношении дипфейков, изображающих известных людей в порнографических сценах, как те, которые первыми появились на платформе Reddit [15]. Кроме того, в ситуациях, когда элемент персоналии все же присутствует, онлайн- или цифровая персоналия не считается преступлением сама по себе, как было показано выше¹⁹¹; уголовная ответственность предусмотрена только за использование персоналии для совершения противоправного деяния, такого как мошенничество в отношении третьей стороны или наложение ответственности на лицо, за которое себя выдают¹⁹². Эти законы не могут защитить жертв пор-

нографии без согласия, так как размещение порно из мести или дипфейков редко сочетается с дополнительной криминальной целью.

Законы о краже личности могли бы стать многообещающим вариантом, учитывая, как часто порнография без согласия сопровождается личной идентифицирующей информацией [26, p. 351]. Ярким примером является дело Кевина Болларта в Калифорнии. Болларт создал и запустил сайт для размещения порно из мести *ugotposted.com* и сопутствующий сайт *changemyreputation.com*, через который жертве предлагалось заплатить от 250 до 350 долларов за удаление изображения с первого сайта¹⁹³. Болларт был осужден за кражу личности и вымогательство¹⁹⁴. Веб-сайт был закрыт, Болларт получил 18 лет тюрьмы, однако очевидно, что он «был осужден не за преступление, непосредственно связанное с порно из мести, а за требование оплаты за удаление изображений» [51, pp. 20–21]. Соответственно, хотя законы о краже личности могут быть использованы в некоторых случаях порнографии без согласия, они не устанавливают уголовной ответственности за соответствующее поведение, в первую очередь *размещение* порнографии без согласия в Сети.

Аналогичным образом законы о киберпреступлениях, например о несанкционированном доступе или взломе¹⁹⁵, применимы в некоторых ситуациях, когда порнографические материалы, использованные при создании дипфейка, были получены через незаконный доступ к компьютеру или электронной почте жертвы [50, p. 16]. И снова, хотя обвинение по этим законам может привести к желаемому результату, они не нацелены на истинный ущерб, причиняемый распространением порно из мести или порнографических дипфейков, а диапазон их применимости очень узок.

Перечисленные федеральные законы и законы штатов дают некоторые возможности для подачи исков о дипфейках, но они неприменимы к дипфейкам как таковым. И независимо от степени предосудительности деяния, судьи не обязаны распространять действие этих законов на деяния, для которых они не предназначены. Примером является недавнее решение Высшего апелляционного суда штата Массачусетс о том, что фотографирование тела человека под одеж-

¹⁸⁶ См. там же, pp. 350–354 (описывается ущерб, причиняемый жертвам с помощью порно из мести).

¹⁸⁷ Tex. Penal Code Ann. § 42.072 (West 2019).

¹⁸⁸ Fla. Stat. § 784.048(1)(d) (2019).

¹⁸⁹ См. [26, pp. 350–354] (описывается ущерб, причиняемый с помощью порно из мести).

¹⁹⁰ См. [66, p. 194] (обсуждаются схожие моменты преступлений с персоналией и порно из мести); см. также [67, p. 464] («Если злоумышленник просто размещает изображение в Сети, не выдавая жертву за другого человека и не размещая личной информации жертвы, то он не будет обвинен в персоналии или незаконном распространении личной информации через электронные средства коммуникации»).

¹⁹¹ Cal. Penal Code § 528.5(a) (West 2019); N.Y. Penal Law § 190.25 (McKinney 2019); Tex. Penal Code Ann. § 33.07 (West 2019).

¹⁹² См. цитируемые выше источники, примечание 190.

¹⁹³ *People v. Bollaert*, 203 Cal. Rptr. 3d 814, 819 (Ct. App. 2016).

¹⁹⁴ Там же.

¹⁹⁵ 18 U.S.C. § 1030 (2012).

дой является законным, если фотографируемый не обнажен или частично обнажен¹⁹⁶. Нежелание судей расширительно толковать законы – еще один довод в пользу необходимости принятия особых законов против дипфейков.

2. Недостатки действующих и предложенных законов против порно из мести

Вышеперечисленные недостатки привели к тому, что большинство штатов приняли законы, специально нацеленные против порно из мести¹⁹⁷. Эти законы, часто несовершенные даже в контексте порно из мести, не могут исправить ситуацию с дипфейками.

а. Законы штатов

По мере появления законов против порно из мести в разных штатах эти законы стали подвергаться критическому рассмотрению. Выделяются три особенно распространенных и очевидных аспекта критики. Во-первых, многие законы против порно из мести, включая законы Калифорнии, Техаса и Флориды, содержат требование относительно намерения¹⁹⁸. Доказать наличие виновной воли сложно¹⁹⁹. Кроме того, происходит «несоответствие»²⁰⁰: правонарушение состоит в «публикации фотографий обнаженного человека без его согласия и с нарушением его ожидания, что изображение не будет опубликовано»; при этом мотивация такого опубликования не имеет значения [26, р. 387]. Второе возражение касается наличия требования доказать ущерб; законы многих штатов, включая Калифорнию, требуют доказать, что жертве был причинен реальный вред или эмоциональный

стресс²⁰¹. Это тоже сложно доказать в суде, к тому же это «заставляет жертву еще больше раскрывать свою частную жизнь на публике» [71, р. 358]. Наконец, многие законы предусматривают очень незначительное наказание за порно из мести²⁰².

б. Закон 2017 г. «О прекращении домогательств в Сети с использованием изображений пользователя, сделанных без его согласия» (The ENOUGH Act)

Помимо вышеперечисленных аспектов, законы против порно из мести – как действующие законы штатов, так и предложенный федеральный закон ENOUGH Act – не будут действовать против дипфейков по четырем основным причинам.

Во-первых, закон ENOUGH Act, как и законы, введенные штатами, включая Калифорнию, Техас и Флориду²⁰³, требуют наличия жертвы, которая (1) либо участвует в сексуально откровенных действиях, либо чьи интимные части тела были показаны, и (2) в определенной степени может быть идентифицирована на визуальном изображении²⁰⁴. В случае дипфейков выполнить эти требования проблематично, поскольку жертву нелегко идентифицировать и поскольку изображение обязательно включает две жертвы, а не одну. Человек, чье лицо было использовано, может быть легче идентифицирован, тогда как для человека, чье тело было использовано, это сделать сложнее. Оба эти индивидуума являются жертвами, но законы о порно из мести неспособны полностью защитить ни одного из них [63, р. 122].

Второй аспект – согласие. Согласно закону ENOUGH Act и законам штатов против порно из мести, публикация или распространение должны быть сде-

¹⁹⁶ См. *Commonwealth v. Robertson*, 5 N.E.3d 522, 528 (Mass. 2014) (суд установил законность скрытого фотографирования под одеждой, если человек не обнажен или частично обнажен); см. также [68].

¹⁹⁷ 46 States + DC + One Territory Now Have Revenge Porn Laws, Cyber C.R. Initiative. URL: <https://www.cybercivilrights.org/revenge-porn-laws/> [<https://perma.cc/V276-JCYC>] (дата обращения: 12.11.2019).

¹⁹⁸ См., например, Cal. Penal Code § 647(j)(4) (West 2019); Fla. Stat. § 784.049 (2019); Tex. Penal Code Ann. § 21.16 (West 2019).

¹⁹⁹ [69, р. 387] («Обвинение должно “доказать при отсутствии обоснованного сомнения, что обвиняемый разместил фотографии с намерением причинить страдания жертве”, а не “чтобы получить деньги”, “просто для смеха”, “чтобы позлить”, или по любой другой причине, которую он может назвать» (цитируется [70])).

²⁰⁰ Там же.

²⁰¹ См., например, Cal. Penal Code § 647(j)(4) (West 2019).

²⁰² Законы штатов Калифорния, Флорида и Техас квалифицируют первый случай такого правонарушения без отягчающих обстоятельств как мисдиминор, предусматривая в качестве наказания от шести месяцев до одного года лишения свободы и штраф от одной до четырех тысяч долларов. См. Cal. Penal Code § 647(j)(4), (l) (West 2019); Fla. Stat. § 775.082(4)(a), 775.083(1)(d), 784.049(3)(a) (2019); Tex. Penal Code Ann. § 12.21, 21.16 (West 2019).

²⁰³ См., например, Cal. Penal Code § 647(j)(4) (West 2019); Fla. Stat. § 784.049 (2019); Tex. Penal Code Ann. § 21.16 (West 2019).

²⁰⁴ См. S. 2162, 115th Cong. (2017). Закон ENOUGH Act также имеет сходство с некоторыми законами штатов против порно из мести. А именно он не включает требование доказать ущерб, но включает требование доказать намерение. Там же.

ланы без согласия жертвы²⁰⁵. По типичному сценарию порно из мести жертва часто изначально соглашается на создание фото- или видеоизображения в контексте конкретных взаимоотношений. Проблема возникает, когда это изображение показывается в ином контексте, на что жертва согласия не давала [26, pp. 345–348]. Понятие согласия становится еще более размытым в случае дипфейков. Чье согласие требуется? Того, чье лицо было использовано, чье тело было использовано или обоих? О чем должно быть согласие: на создание или на распространение дипфейка? На использование самих изображений или сходства? На использование видео или фотографий, с помощью которых был создан дипфейк? Человек, чье тело было использовано в дипфейке, мог дать согласие на создание и распространение оригинальной записи; однако он, скорее всего, не соглашался на наложение лица другого человека. Аналогично жертва, чье лицо было использовано в дипфейке, вероятно, соглашалась на использование своих фотографий или видео в одном контексте, даже в социальных сетях, но не в дипфейке.

В-третьих, закон ENOUGH Act и законы штатов Техас и Калифорния требуют, чтобы жертва имела обоснованные ожидания, что изображение останется частным²⁰⁶. И снова этот элемент относительно очевиден в контексте порно из мести, когда один из партнеров публикует интимное изображение другого, сделанное в предположении, что оно не будет опубликовано. В контексте дипфейка этот элемент отсутствует и не может быть доказан; ни одна из жертв не имела ожиданий относительно приватности своего изображения.

В-четвертых, закон ENOUGH Act исключает симулированные действия из определения «интимного визуального изображения»²⁰⁷. Это положение прямо противоречит включенному в этот закон определению «сексуально откровенного поведения» в формулировке ст. 18 U.S.C. § 2256, которая включает симулированное поведение²⁰⁸. Это положение исключает

уголовную ответственность за дипфейки, которые по определению являются симуляцией.

Таким образом, поскольку идентификация жертв, первоначальное согласие и ожидание приватности являются явными или скрытыми элементами существующих законов, устанавливающих уголовную ответственность за порно из мести, и поскольку эти элементы либо не существуют (приватность или согласие), либо сложно доказуемы (идентификация всех жертв) в случае дипфейков, действующие и предложенные законы против порно из мести не могут быть использованы против дипфейков. Необходимо новое законодательство, нацеленное против дипфейков.

3. Недостатки Акта 2018 г. о запрете дипфейков, созданных со злым умыслом (MDFPA)

При несомненной необходимости уголовной ответственности за порнографические дипфейки Акт 2018 г. о запрете дипфейков, созданных со злым умыслом (MDFPA), нельзя считать адекватным решением. Прежде всего, закон MDFPA во многих отношениях имеет слишком расширительные формулировки. Во-первых, чрезмерно широко определение дипфейка согласно MDFPA, включающее любые «аудио- и видеозаписи, созданные или измененные таким образом, что запись ошибочно воспринимается как аутентичная запись реальной речи или действий индивидуума»²⁰⁹. Такое определение, не содержащее каких-либо ограничений или модификаторов, очевидно, включает широкий спектр материалов, в том числе законный, неоскорбительный контент, например, компьютерные спецэффекты в фильмах. Чтобы конкретизировать это широкое определение, в законе MDFPA приводится настолько же широкое исключение, соответствующее Первой поправке²¹⁰. В таком виде закон MDFPA приведет к тому, что практически любой дипфейк можно будет представить в суде как пародию или сатиру. Кроме того, он налагает чрезмерно обширную ответственность на распространителей, что может привести к превентивному удалению большого количества кон-

²⁰⁵ См. цитируемые выше источники, примечание 202.

²⁰⁶ S. 2162; См. выше разд. III.B.

²⁰⁷ S. 2162.

²⁰⁸ 18 U.S.C. § 2256 (2012) («Сексуально откровенное поведение» означает «одно из реальных или симулированных действий (i), половой акт, включая генитально-генитальный, орально-генитальный, анально-генитальный, орально-анальный, между людьми одного или разных полов... или (v) раз-
вратное демонстрирование гениталий или лобковой зоны»).

²⁰⁹ S. 3805, 115th Cong. (2018).

²¹⁰ Там же. («Никто не может быть осужден по данному закону за какую-либо деятельность, защищенную Первой поправкой к Конституции Соединенных Штатов»).

тента, включая вполне законный, в отсутствие четкого критерия законности и незаконности контента²¹¹.

Кроме того, MDFPA устанавливает уголовную ответственность только за дипфейки, созданные с намерением «спровоцировать криминальное или противоправное поведение» после их распространения²¹². Другими словами, согласно MDFPA, деяние только тогда уголовно наказуемо, когда дипфейк распространяется с намерением совершить какое-либо другое уголовное или гражданское правонарушение. Ставя условием уголовной ответственности за дипфейки доказательство нарушения другого закона создателем или распространителем дипфейка, закон MDFPA проявляет одновременно излишнюю узость²¹³ и излишнюю широту²¹⁴ формулировок, добавляя сложности в работу обвинителя. В то же время, как было показано выше, этот закон не обеспечивает адекватной защиты жертв порнографии без согласия. Таким образом, закон MDFPA не устанавливает уголовной ответственности за порнографические дипфейки, если они не сопровождаются каким-либо другим уголовным или гражданским правонарушением. Однако создание или распростра-

нение порнографического дипфейка и само по себе заслуживает уголовного наказания, без требования наличия намерения нарушить какой-либо иной закон.

Далее, закон MDFPA совершенно не ставит задачи защитить жертв порнографического дипфейка. Он нацелен на политические дипфейки [74]. Фальсификации на выборах, фейковые новости и другие возможные способы нанести ущерб демократическим институтам, несомненно, заслуживают внимания; однако эти ситуации привлекают много внимания и ресурсов. Напротив, жертвы порнографии без согласия, включая дипфейки, не пользуются таким вниманием и приоритетом [46, pp. 402–404]. Хотя порнографические дипфейки, изображающие знаменитостей, сначала привлекли внимание к этой новой технологии, ее потенциальными жертвами являются не только такие люди, как Скарлетт Йоханссон [75]. С самого начала сложилось так, что закон, правоохранительные органы и даже общество в целом не смогли должным образом обратить внимание на жертв порнографии без согласия и защитить их [46, pp. 402–404]. Поэтому, подобно тому, как развитие порно из мести привело к появлению целого ряда законов против него, бороться против порнографических дипфейков придется также с помощью особого уголовного закона.

В. Аспекты, связанные с Первой поправкой

Сразу после того, как в конце 2017 г. появились первые ставшие вирусными в Интернете порнографические дипфейки, изображающие знаменитостей, праведы и журналисты заговорили о том, что это затронет защиту в рамках Первой поправки, которой пользуется сетевой контент²¹⁵. Положения Первой поправки о свободе слова защищают как вербальные средства выражения, так и действия; государство не может «ограничивать свободу самовыражения по причине его смысла, идей, темы или содержания»²¹⁶. Даже если сообщение носит оскорбительный или неприятный характер, оно пользуется защитой как свободное самовыражение²¹⁷.

²¹¹ См. [72] («Профессор права в Университете штата Мэриленд и соавтор основополагающей статьи о дипфейках Danielle Citron говорит, что данный законопроект налагает чрезмерно большую ответственность на дистрибьюторов. По ее мнению, это может заставить платформы немедленно удалить все, что кто-то назовет дипфейком, включая, возможно, и настоящие изображения»).

²¹² S. 3805.

²¹³ Согласно MDFPA, создатель или дистрибьютор порнографического дипфейка избежит уголовной ответственности по предложенному федеральному закону, если независимо от причиненного им ущерба его поведение не нарушает другого закона. Там же. Учитывая неэффективность существующих гражданских мер и уголовного законодательства в отношении дипфейков и иных подобных форм порнографии без согласия, а также необходимость доказывания причиненного ущерба, вероятность успешного обвинения за порнографические дипфейки по закону MDFPA очень низка.

²¹⁴ Согласно MDFPA, сравнительно безобидные дипфейки могут повлечь за собой уголовную ответственность для их создателей и распространителей, если их поведение нарушает другой закон. См. [73] («Рассмотрим пример того, как могут действовать широкие формулировки законопроекта сенатора Sasse. Представьте, что Салли создает дипфейк, наложив свое лицо на видео с политическим выступлением президента Трампа. По мнению Салли, видео очень смешное, и она решает поделиться им с друзьями. Она устраивает вечеринку с живой музыкой, на которой раздает копии своего смешного видео. Однако группа играет так громко, что нарушает закон штата и частную жизнь соседей»).

²¹⁵ [30] («Вероятно, удаление контента означало бы нарушение Первой поправки». «По словам профессора права Эрика Голдмана, весь контент изначально защищен Первой поправкой»).

²¹⁶ *United States v. Alvarez*, 567 U.S. 709, 716 (2012) (цитируя *Ashcroft v. ACLU*, 535 U.S. 564, 573 (2002)).

²¹⁷ *Virginia v. Black*, 538 U.S. 343, 358 (2003) («Основная цель защиты свободы слова – обеспечивать “свободный обмен

Подобным образом попытки установить уголовную ответственность за порно из мести в разных штатах и на федеральном уровне были встречены с сомнениями по поводу соблюдения Первой поправки [26, pp. 374–377]. Поэтому, чтобы пройти проверку на конституционность, законы против порно из мести были сформулированы узко, чтобы формулировки не затрагивали правдивые, хотя и спорные, сообщения, защищенные положениями о свободе слова [26, pp. 374–377].

Те же сложности возникают и в случае дипфейков [6, р. рукопись, pp. 31–33]. Действительно, Верховный суд США однозначно постановил, что ложные сообщения защищены Первой поправкой²¹⁸. Кроме того, учитывая цифровой характер дипфейков, появляются дополнительные сложности, связанные с пародией и сатирой. Эти опасения правомерны, и законодательство против дипфейков должно учитывать риск, связанный с ограничениями на основе содержания. Однако есть способы и соблюсти требования Первой поправки, и защитить жертв порнографии без согласия, включая дипфейки²¹⁹.

Одно из решений заключается в том, чтобы включить оговорку относительно наличия явно выраженных общественных интересов в закон против порнографических дипфейков [26, р. 388]. Несколько штатов включили в свои законы против порно из мести оговорку «учитывая отсутствие уголовной ответственности за обнародование материалов, затрагивающих общественные интересы» [26]. Права в рамках Первой поправки будут защищены, если освободить от уголовной ответственности за распространение

дипфейков или порно из мести, которые относятся к сфере значимых общественных интересов [26].

Другой вариант – разработать законы таким образом, чтобы они четко определяли дипфейки как материалы, не подпадающие под требования свободы слова, а именно в данном случае по причине непристойности [26, pp. 384–385]. Верховный суд твердо дал понять, что непристойные материалы не пользуются защитой Первой поправки²²⁰. Критерий непристойности контента следующий:

«(а) если “среднестатистический гражданин, применяя существующие в современном обществе стандарты”, считает, что материал, взятый в совокупности, возбуждает сексуальный интерес; (б) если материалы изображают или описывают, явно оскорбительным образом, сексуальное поведение, как оно определяется соответствующим законом штата и (в) если материал, взятый в совокупности, не имеет серьезного литературного, художественного, политического или научного значения»²²¹.

В деле *Miller v. California*²²² суд даже привел примеры непристойности, подлежащей регулированию по закону, например, «явно оскорбительное изображение или описание полового акта, нормального или извращенного, реального или симулированного» или «явно оскорбительное изображение или описание мастурбации, выделительных функций или распутная демонстрация гениталий»²²³. Таким образом, закон против порнографических дипфейков может пройти проверку на соответствие Первой поправке, если регулируемый контент будет определен в терминах непристойности.

V. ПРЕДЛАГАЕМЫЕ РЕШЕНИЯ

В этом разделе приводятся возможные решения проблемы порнографических дипфейков, как правовые, так и внеправовые. Ущерб от дипфейков, как и от порно из мести, состоит в сексуальной объективации без согласия. Они нарушают «ожидания, что все аспекты сексуальной деятельности будут основаны на согласии» [11, р. 4]. Поэтому жертвы порнографических дипфейков, как и жертвы порно из мести, нуждаются в конкретных решениях, в результате которых созда-

идеями” – даже такими, которые подавляющему большинству людей могут показаться неприемлемыми и неудобными» (цитируя *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., особое мнение)); *Texas v. Johnson*, 491 U.S. 397, 414 (1989) («Основополагающий принцип Первой поправки состоит в том, что государство не может запретить выражать какую-либо идею только потому, что общество находит эту идею оскорбительной или неприемлемой»).

²¹⁸ См. *Alvarez*, 567 U.S., pp. 721–722.

²¹⁹ Уголовное законодательство часто используется для защиты неприкосновенности частной жизни, включая уголовные законы против несанкционированного раскрытия частной финансовой или медицинской информации или законы против нарушения границ владения или вуайеризма. См. 18 U.S.C. § 1028, 1801 (2012); 42 U.S.C. § 1320d-6 (2012). Если уголовные законы, защищающие неприкосновенность финансовых, медицинских и других форм частной жизни, совместимы с требованиями Первой поправки, то уголовные законы, направленные против дипфейков, также должны быть совместимы с ней.

²²⁰ *Miller v. California*, 413 U.S. 15, 23 (1973).

²²¹ Там же, р. 24 (цитата опущена) (цитируя *Kois v. Wisconsin*, 408 U.S. 229, 230 (1972)).

²²² 413 U.S. 15 (1973).

²²³ Там же, р. 25.

тели контента понесут ответственность, распространители будут контролироваться, а незаконный контент будет удален из Интернета. Сложилась необходимость принятия федерального уголовного закона, предусматривающего такие решения для защиты жертв.

А. Ответственность по федеральному закону, а не по законам штатов

Федеральный закон, криминализирующий дипфейки, создал бы мощную и эффективную преграду для их создания и распространения²²⁴. Медленные и неровные попытки криминализации порно из мести на уровне штатов, предпринимавшиеся в последнее десятилетие²²⁵, показывают, что такое же медленное движение против дипфейков не будет успевать за техническими разработками, которые становятся все сложнее, но вместе с тем доступнее [76, 77]. Криминализация дипфейков на федеральном уровне необходима по нескольким причинам. Во-первых, Интернет действует вне границ юрисдикций и включает коммуникацию между штатами и государствами; распространяемые в Интернете дипфейки не являются правонарушением в границах штата или региона. Создатель дипфейка может проживать в одном штате, жертва в другом, а дипфейк распространяться везде. Таким образом, порнографические дипфейки, как и другие преступления в Сети, по своей сути находятся вне границ юрисдикций какого-либо штата²²⁶.

Во-вторых, поскольку создание порнографических дипфейков является преступлением вне границ юрисдикций, то и ответственность за него должна быть одинаковой для всей страны, универсальной и последовательной – наказание и возмещение ущерба не должны зависеть от того, в каком штате живет правонарушитель или жертва. Принятие федерального уголовного закона обеспечит защиту жертв в тех штатах, которые

отказываются принимать свои законы или делают это слишком медленно. Кроме того, жертва может испытывать трудности, обратившись за помощью в правоохранительные органы своего штата, если, к примеру, правонарушитель проживает в другой юрисдикции, особенно в той, где данная деятельность не подлежит уголовной ответственности. В таких случаях федеральный уголовный закон говорит о том, что данная деятельность незаконна и должна быть пресечена.

В-третьих, федеральный закон необходим потому, что законы штатов ограничены § 230 Закона CDA, который запрещает иски штатов против операторов веб-сайтов, размещающих порнографию без согласия; однако иммунитет по § 230 не распространяется на федеральное уголовное законодательство²²⁷. В-четвертых, криминализация порнографических дипфейков на федеральном уровне позволит использовать значительные ресурсы федерального правительства, включая обвинительные действия Департамента юстиции и следовательские навыки ФБР.

Наконец, уголовная ответственность за дипфейки на федеральном уровне показывает серьезность ситуации и привлекает внимание к причиняемому вреду, демонстрируя, что проблема важна на общенациональном уровне. Как показали недавние меры интернет-провайдеров по удалению детской порнографии и контролю над другими видами опасного или оскорбительного контента, криминализация дипфейков по федеральному закону может привести к поиску средств и созданию интерактивных сервисов для решения вопроса на добровольной основе [80].

В. Предлагаемый федеральный уголовный закон: Закон об уголовной ответственности за порнографические дипфейки

Проблема порнографических дипфейков нарастает и требует законодательных решений. В данном разделе предлагается новый федеральный уголовный закон, регулирующий создание и распространение порнографических дипфейков. В этом законе сочетаются компоненты законов ENOUGH и MDFPA и добавлены другие необходимые компоненты с целью поставить заслон порнографическим дипфейкам и защитить их жертв. Ниже приводится текст предлагаемого закона, а затем его анализ.

²²⁴ Как отмечали Mary Anne Franks и Danielle Keats Citron, выступая в защиту криминализации порно из мести, «всплеск порнографии без согласия, несомненно, связан с тем, что у правонарушителей мало стимулов воздерживаться от такого поведения» [26, р. 361].

²²⁵ См. [44, pp. 36–37] (требование криминализации порно из мести на федеральном уровне).

²²⁶ См. [78] (отмечается, что большинство преступлений в Сети связано со средствами коммуникации между штатами или государствами); [79, р. 385] (обсуждается неадекватность законодательств штатов для контроля спама, потому что действие Интернета происходит вне границ юрисдикций).

²²⁷ См. 47 U.S.C. § 230(e) (2012).

1. Предлагаемый текст закона

НАЗВАНИЕ. – Закон об уголовной ответственности за порнографические дипфейки.

(а) ПРЕДПОСЫЛКИ. – Законодательный орган считает, что:

(1) технологии, необходимые для создания дипфейков, являются общедоступными и не требуют технического образования, что приводит к быстрому распространению дипфейков;

(2) порнографические дипфейки, как и порнография из мести, являются формой порнографии без согласия;

(3) жертвы порнографии без согласия могут испытывать серьезный эмоциональный и психологический ущерб и опасаться за свою физическую безопасность; а также

(4) порнография без согласия непропорционально виктимизирует лиц женского пола.

(b) ЦЕЛЬ. – Целью данного закона является:

(1) криминализация создания и распространения порнографических дипфейков без согласия;

(2) защита жертв и обеспечение адекватного возмещения ущерба;

(3) установление ответственности для создателей и провайдеров.

(c) ОПРЕДЕЛЕНИЯ.

(1) АУДИОВИЗУАЛЬНАЯ ЗАПИСЬ. – Понятие «аудиовизуальная запись» означает:

(A) любой аудио- или видеоматериал в электронном формате; а также

(B) любые фотография, движущееся изображение, фильм, видеозапись, электронное изображение, звукозапись.

(2) ДИПФЕЙК. – Понятие «дипфейк» означает аудиовизуальную запись, созданную или измененную таким образом, что она ошибочно представляется разумному наблюдателю аутентичной записью реальной речи, поведения, внешности или образа индивидуума.

(3) ИНДИВИДУУМ. – Понятие «индивидуум» относится к человеку, чье лицо изображено в дипфейке, или к человеку, чье тело изображено в дипфейке, а понятие «индивидуумы» относится ко всем изображенным в дипфейке.

(4) ПОРНОГРАФИЧЕСКИЙ ДИПФЕЙК. – Понятие «порнографический дипфейк» означает любой дипфейк (как определено в параграфе (2)):

(A) в котором:

(i) какой-либо из индивидуумов участвует или изображен участвующим в сексуально откровенных действиях или

(ii) видны обнаженные гениталии или, в случае женщины в постпубертатном возрасте, соски любого из индивидуумов;

(B) в первоначальной или измененной форме, например, с наложенным фильтром или текстом.

(5) СЕКСУАЛЬНО ОТКРОВЕННОЕ ПОВЕДЕНИЕ. – Термин «сексуально откровенное поведение» имеет значение, изложенное в разд. 2256(2)(A).

(6) ИНТЕРАКТИВНЫЙ КОМПЬЮТЕРНЫЙ СЕРВИС. – Термин «интерактивный компьютерный сервис» имеет значение, изложенное в разд. 230 Закона CDA (47 U.S.C. § 230).

(7) ПРОВАЙДЕР ИНФОРМАЦИОННОГО КОНТЕНТА. – Термин «провайдер информационного контента» имеет значение, изложенное в разд. 230 Закона CDA (47 U.S.C. § 230).

(d) ПРАВОНАРУШЕНИЕ. – За исключением случаев, описанных в подразделе (g), является незаконным сознательно использовать любое средство коммуникации между штатами или государствами для распространения или создания порнографического дипфейка:

(1) зная или игнорируя по небрежности:

(A) отсутствие согласия индивидуума или индивидуумов на использование их внешности или образа для создания или распространения порнографического дипфейка, а также

(B) ущерб, который такое распространение может причинить данному индивидууму или индивидуумам;

(2) не имея объективно обоснованных причин полагать, что такое распространение затрагивает общественные интересы.

(e) НАКАЗАНИЕ. – Лицо, нарушающее положения подраздела (d), подвергается наказанию в виде:

(1) штрафа в соответствии с данным законом, лишения свободы сроком до 5 лет или обоим этим наказаниям;

(2) штрафа в соответствии с данным законом, лишения свободы сроком до 10 лет или обоим этим наказаниям в случае второго или последующих нарушений или

(3) штрафа в соответствии с данным законом, лишения свободы сроком до 10 лет или обоим этим наказаниям в случае нарушения, когда любой

индивидуум, изображенный в дипфейке, является несовершеннолетним.

(f) ВОЗМЕЩЕНИЕ УЩЕРБА. – Возмещение ущерба производится на усмотрение суда и должно отвечать целям, описанным в подразделе (b). Возможные меры возмещения ущерба включают, но не ограничиваются следующими:

(1) постановление суда об уничтожении аудиовизуальной записи;

(2) постановление суда об обязательстве интерактивного компьютерного сервиса или провайдера информационного контента удалить аудиовизуальную запись;

(3) постановление суда о временном или постоянном запрете для предотвращения дальнейшего распространения дипфейка;

(4) возмещение оплаты судебных издержек в разумных пределах;

(5) возмещение ущерба или реституции жертвам, а также

(6) любые другие меры возмещения, которые суд сочтет необходимыми.

(g) ИСКЛЮЧЕНИЯ. –

(1) ДЕЙСТВИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И ДРУГИЕ ЗАКОННЫЕ ПРОЦЕДУРЫ. – Данный закон:

(A) не запрещает какой-либо законной правоохранительной, коррекционной или разведывательной деятельности;

(B) не применяется в случае личного добровольного сообщения о незаконной деятельности, а также

(C) не применяется в случае производства или хранения документации, связанной с судебными процедурами.

(2) ПОСТАВЩИКИ УСЛУГ. – Данный закон не применяется к поставщику информационных услуг в отношении контента, предоставленного другим поставщиком информационных услуг, за исключением случаев, когда поставщик информационных услуг намеренно привлекает либо распространяет сознательно или по небрежности контент, нарушающий положения данного закона.

(h) УГРОЗЫ И ВЫМОГАТЕЛЬСТВО. – Лицо, которое намеренно угрожает совершить преступление, описанное в подразделе (d), независимо от того, является ли данная угроза вымогательством, подлежит наказанию в соответствии с подразделом (e).

(i) ОБЛАСТЬ ДЕЙСТВИЯ И ЭКСТРАТЕРРИТОРИАЛЬНОСТЬ. – Обвинение по данному закону может быть выдвинуто по месту проживания ответчика или любого из изображенных индивидуумов, или по месту распространения порнографического дипфейка. Данный закон обеспечивает экстратерриториальную федеральную юрисдикцию указанного правонарушения, если ответчик или изображенный индивидуум является гражданином США или постоянно проживает в США.

2. Анализ Закона об уголовной ответственности за порнографические дипфейки

Предлагаемый закон призван сбалансировать защиту жертв, наказание для правонарушителей и защиту свободы самовыражения. Подразделы от (a) до (c) описывают контекст, цель и рамки данного закона.

В отличие от MDFPA предлагаемый закон более узконаправлен против *порнографических* дипфейков, а в отличие от Закона ENOUGH он в явном виде включает *симулированные* изображения²²⁸. Цель закона и необходимость его принятия раскрываются в контексте порнографии без согласия и непропорционально высокого ущерба для женщин²²⁹.

Далее, определения проясняют область применения и назначение данного закона. С целью дополнить определение дипфейков, данное в Законе MDFPA, но при этом избежать чрезмерно широкого определения в предлагаемом законе к понятию «дипфейк» добавлено уточнение «порнографический»²³⁰. Область применения закона ограничена дипфейками, изображающими «сексуально откровенные действия»²³¹. Это

²²⁸ См. выше разд. IV.A.2.b (отмечается, что порнографические дипфейки не соответствуют рамкам Закона ENOUGH); См. также выше разд. IV.A.3 (обсуждаются чрезмерно расширительные формулировки Закона MDFPA).

²²⁹ См. выше разд. I.C (обсуждается проблема дипфейков в контексте порнографии без согласия и ущерба, причиняемого жертвам).

²³⁰ См. выше разд. IV.A.3 (обсуждаются чрезмерно расширительные формулировки Закона MDFPA).

²³¹ Статья 18 U.S.C. § 2256(2)(A) (2012), инкорпорирующая в предлагаемый закон, определяет «сексуально откровенное поведение» как «одно из реальных или симулированных действий (i), половой акт, включая генитально-генитальный, орально-генитальный, анально-генитальный, орально-анальный, между людьми одного или разных полов; (ii) скотоложество; (iii) мастурбация; (iv) акты садизма или мазохизма или (v) развратное демонстрирование гениталий или лобковой зоны».

ограничение необходимо, чтобы закон мог защитить жертв порнографии без согласия, но при этом не применялся против безобидных дипфейков. Кроме того, в законе особо оговаривается включение *обеих* жертв в определение *пострадавших*. Это обеспечивает защиту обоих лиц, чьи изображения манипулировали и распоряжались без их согласия²³².

Подраздел (d) начинается с требования федеральной юрисдикции²³³ и описывает правонарушение – создание и распространение порнографического дипфейка без ведома или игнорируя отсутствие согласия любой из жертв на использование его (ее) изображения в дипфейке, а также возможный ущерб, причиненный жертве. Намеренные угрозы о совершении данного правонарушения также включены в подраздел (h). Соответственно, предлагаемый закон должен применяться к тем, кто создает или распространяет порнографические дипфейки и расширяет понятие виновной воли на тех, кто действует сознательно или по небрежности²³⁴. Требование намерения не включено не случайно. С одной стороны, как было показано в контексте порно из мести, требование доказать, что нарушитель опубликовал изображение с конкретным намерением причинить ущерб жертве, лишает жертву защиты и делает преступление недоказуемым [58, pp. 979–980]. С другой стороны, такие организации, как ACLU и Electronic Frontier Foundation, традиционно возражали против законов, которые не включают положение о «намеренном причинении ущерба», руководствуясь идеей, что отсутствие требования доказать намерение может нарушать Первую поправку²³⁵. Предлагаемый закон является разумным компромиссом, поскольку включает понятие небрежности как альтернативу виновной воли. Сложная проблема с согласием, присутствующая во многих

законах против порно из мести²³⁶, также частично решена, поскольку в предлагаемом законе требуется знание об отсутствии согласия жертвы на использование изображения в дипфейке или игнорирование такого отсутствия. Аналогично нет и требования причинения реального ущерба; понятие ущерба включено в требование виновной воли в подразделе (d)(1)(B)²³⁷.

Кроме того, данный закон не предусматривает наказания для тех, кто имел «объективно обоснованные причины считать, что распространение данных материалов имеет общественное значение»²³⁸. Это положение повторяет Закон ENOUGH и направлено на то, чтобы обеспечить отсутствие уголовного наказания за законную деятельность в рамках Первой поправки²³⁹. Кроме того, это положение формулируется более узко, чем положение о Первой поправке в Законе MDFPA²⁴⁰.

В подразделе (g) оговариваются две категории исключений – правоохранительные органы и интернет-провайдеры. Последняя категория соответствует иммунитету в рамках § 230²⁴¹, но не безусловно. В данном законе предлагается ответственность «поставщика услуг за намеренное привлечение контента, сознательное или по небрежности распространение контента, нарушающего положения данного раздела»²⁴². Хотя интернет-платформы сложно привлечь к ответственности, данный закон может стимулировать провайдеров самих контролировать и ограничивать распространяемый контент²⁴³.

Заключительные части предлагаемого закона устанавливают: меры наказания (подраздел (e)) и возмещение ущерба (подраздел (f)). Основные меры

²³² См. выше разд. II.A (дается определение жертв); см. также выше разд. IV.A (выделяются сложности, связанные с требованием «возможности идентифицировать жертву», присутствующим во многих законах штатов о порно из мести и в Законе ENOUGH).

²³³ См. выше разд. V.B.1; см. также [81, pp. 235–234].

²³⁴ См. выше разд. IV.A.2.a (обсуждаются сложности, связанные с возможностью обвинителя убедительно доказать наличие виновной воли по требованиям многих законов штатов о порно из мести).

²³⁵ См. [58, p. 979]; см. также [82].

²³⁶ См. выше разд. IV.A.2.b.

²³⁷ См. выше разд. IV.A.2.a (обсуждаются проблемы, возникающие в связи с требованием доказать реальный вред согласно многим законам штатов против порно из мести); см. также выше разд. V.B.1.

²³⁸ См. выше разд. V.B.1 (цитируется раздел (d)(2) предлагаемого закона).

²³⁹ См. выше разд. IV.B (описываются проблемы применения Первой поправки к регулированию на основе контента).

²⁴⁰ См. S. 3805, 115th Cong. (2018) («Никто не может быть осужден по данному закону за какую-либо деятельность, защищенную Первой поправкой к Конституции»).

²⁴¹ См. выше разд. II.B (описываются проблемы применения CDA при попытках регулирования дипфейков).

²⁴² См. выше разд. V.B.1 (цитируется раздел (g)(2) предлагаемого закона).

²⁴³ Многие платформы уже приняли собственные меры, ограничивающие порнографию без согласия. См. [80].

наказания совпадают с таковыми в Законе ENOUGH; пятилетний срок лишения свободы, подчеркивающий тяжесть данного преступления, присутствует и в других законах против порнографии без согласия²⁴⁴. Предложенный закон устанавливает также усиленные меры наказания за повторные правонарушения и за преступления с участием несовершеннолетних.

Помимо наказания виновным, закон предусматривает также меры возмещения для жертв. Учитывая тяжелые и часто долгосрочные последствия для жертв порнографии без согласия, необходимо, чтобы закон помогал жертвам. В данном случае предусматривается возможность судам назначать возмещение по своему усмотрению с целью защиты и компенсации жертвам; суд может потребовать уничтожить оригиналы дипфейков и удалить их с платформ для защиты жертв от последующего ущерба²⁴⁵. Кроме того, могут быть приняты судебные запреты. Могут быть также рекомендованы возмещение судебных издержек и реституция жертвам²⁴⁶.

С. Дополнения к Закону об уголовной ответственности за порнографические дипфейки: внеюрисдикционные решения

В дополнение к принятию федерального уголовного закона необходимо разработать меры противодействия и поддержки, направленные на борьбу с порнографическими дипфейками, включая обучение сотрудников правоохранительных и судебных органов, широкой публики; поддержку организаций и общественных групп; технологические решения. В данном разделе мы остановимся на этих аспектах.

1. Информирование, обучение и воспитание

Чтобы уголовный закон, подобный предложенному, работал в полную силу, т. е. предотвращал и наказывал за противоправные действия, необходимо, чтобы потенциальные правонарушители и представители правоохранительных и судебных органов больше знали о сущности порнографических дипфейков и ущербе от них. Важно понимать,

что потенциальными жертвами являются не только знаменитости и общественные деятели, но и любой человек, которого когда-либо снимали на цифровую фото- или видеокамеру. Прежде всего, необходимо информировать общество о вреде порнографических дипфейков с помощью сообщений на интернет-сервисах и в традиционных СМИ. Информацию об этом преступлении следует включить в школьные программы как часть сексуального воспитания, а в колледжах и на рабочих местах – как часть обучения против сексуальных домогательств и дискриминации.

Сотрудники правоохранительных и судебных органов должны пройти обучение. Представители правоохранительных органов часто недооценивают проявления домашнего насилия и других форм сексуального насилия и домогательств против женщин как дома, так и на рабочем месте, считая эти преступления частным делом или чем-то незначительным, повседневным²⁴⁷. Такое отношение правоохранительных органов сохраняется и в случае домогательств в Сети, включая порно из мести²⁴⁸. Представители правоохранительных и судебных органов должны научиться воспринимать эти преступления серьезно; они должны быть натренированы правильно распознавать их, хорошо знать законы, а также регулярно повышать свою квалификацию вместе с развитием технологий, компьютерных программ и приложений. Кроме того, офицеры полиции и судьи должны владеть технологическим инструментарием для распознавания порнографических дипфейков.

Кроме повышения эффективности правоохранительной деятельности, образовательная деятельность в указанном направлении может привести к сокращению количества порнографических дипфейков, как произошло в случае домашнего насилия²⁴⁹. Чтобы достичь такого эффекта, представители правоохрани-

²⁴⁴ См. [26, pp. 365–367] (обсуждаются меры наказания).

²⁴⁵ См. выше разд. V.B.1 (цитируется раздел (e) предлагаемого закона).

²⁴⁶ См. выше разд. V.B.1 (цитируется раздел (f) предлагаемого закона).

²⁴⁷ Citron описывает случаи, когда полиция отказывала в помощи жертвам порно из мести или домогательств в Сети [83, pp. 20–21, 41, 84–85]. Например, когда жертва домогательств в Сети обратилась в полицию, ее опасения не восприняли всерьез; полицейские сказали: «Мальчишки есть мальчишки» и посоветовали улучшить свою репутацию в Сети [83, p. 41].

²⁴⁸ См. в целом там же.

²⁴⁹ См. [46, p. 409] (описывается развитие законодательства, в результате которого домашнее насилие превратилось из частного дела семьи в уголовно наказуемое деяние, что привело к сокращению случаев домашнего насилия).

тельных и судебных органов, общественности должны понимать роль технологий в проблеме дипфейков, а также ее последствия. Заложенные в законе меры тогда дадут результат, когда в обществе возникнет понимание проблемы и стремление работать над ее решением.

2. Группы поддержки

В настоящее время не существует общественных групп поддержки, нацеленных конкретно на помощь жертвам порнографических дипфейков. Пока не появятся такие группы, жертвы порнографических дипфейков будут вынуждены искать помощи, руководства и поддержки в группах, нацеленных на жертв порно из мести, и следует способствовать тому, чтобы эти группы оказывали помощь жертвам порнографических дипфейков, поскольку ущерб, причиняемый ими, сходен.

Став в 2000-е гг. жертвой порно из мести, Holly Jacobs [55] начала кампанию под названием «Остановим порно из мести» с призывом законодательно ввести уголовную ответственность за это деяние. Позже это движение стало помогать жертвам советами и информацией [55]. В итоге оно слилось с движением «Инициатива за гражданские права в Сети» (Cyber Civil Rights Initiative, CCRI), которое выступает «за технологические, социальные и правовые инновации, направленные против преследования в Сети» в соответствии с положением о некоммерческих организациях 501(c)(3)²⁵⁰. Этот ресурс предоставляет жертвам порнографии без согласия различные виды помощи – от кризисной горячей линии до дешевых или бесплатных услуг и мер поддержки²⁵¹. CCRI предоставляет информацию о том, как сообщить о размещении порнографических постов и потребовать их удаления²⁵². Они также призывают изменить законодательство и предлагают варианты федеральных законов и законов штатов против порно из мести²⁵³.

Другие общенациональные кампании, например, «Без моего согласия», нацелены на нарушения част-

ной жизни в Сети и домогательства в целом, особенно на порнографию без согласия²⁵⁴. Это мощный ресурс для жертв, предоставляющий разнообразную помощь, включая горячие линии, программы защиты жертв, услуги юристов, данные, блоги, а также постоянные обзоры законодательства каждого штата и федерального законодательства²⁵⁵.

Кроме того, помощь жертвам оказывается на уровне отдельных штатов. Например, генеральный прокурор штата Калифорния запустил кампанию «Киберэксплуатация», предоставляющую онлайн-ресурсы жертвам и правоохранительным органам²⁵⁶. По его словам, «размещение интимных изображений в Сети без согласия подрывает неприкосновенность частной жизни, основные гражданские права и общественную безопасность»²⁵⁷. Офис генерального прокурора публикует результаты исследований, согласно которым киберэксплуатация, так же как сексуальные домогательства, насилие и домашнее насилие, причиняет непропорционально больший вред женщинам²⁵⁸. Поэтому была предпринята инициатива «Остановить киберэксплуатацию» (#EndCyberExploitation), имеющая четыре сферы приложения: (1) рабочая группа генерального прокурора по данному вопросу; (2) судебные процессы [;] (3) изменение законодательства и (4) обучение сотрудников правоохранительных органов²⁵⁹. Пример штата Калифорния следует взять на вооружение другим штатам и федеральному правительству.

3. Технологические решения

Наряду с ответственностью за создание и распространение порнографических дипфейков на уровне федерального закона одновременно могут быть приняты иные меры, способствующие возмещению ущерба жертв с помощью существующих технологий.

²⁵⁴ Without My Consent. URL: <http://www.withoutmyconsent.org/> [<https://perma.cc/6TCB-978S>] (дата обращения: 12.11.2019).

²⁵⁵ Там же.

²⁵⁶ Cyber Exploitation, Off.Att’yGen. URL: <https://oag.ca.gov/cyberexploitation> [<https://perma.cc/8B9E-GLJG>] (дата обращения: 12.11.2019).

²⁵⁷ Там же.

²⁵⁸ Там же.

²⁵⁹ Там же.

²⁵⁰ About Us, Cyber C.R. Initiative. URL: <https://www.cybercivilrights.org/welcome/> [<https://perma.cc/MpW3-8RE2>] (дата обращения: 12.11.2019).

²⁵¹ Там же.

²⁵² Там же.

²⁵³ Там же.

а. Требования об удалении контента

Жертва дипфейка может даже не знать о его создании или распространении. Как только это становится известно, можно направить запрос на удаление материала еще до того, как правонарушитель будет определен и осужден. Закон о цифровых авторских правах в новом тысячелетии (The Digital Millennium Copyright Act, DMCA)²⁶⁰ позволяет удалить контент по запросу владельца авторских прав²⁶¹. Это широко распространенная стандартная процедура, хорошо известная владельцам веб-сайтов и провайдером²⁶². Такие запросы жертва может делать, если является владельцем контента и считает, что он «размещен в Сети без ее согласия», даже если контент не защищен авторским правом²⁶³. Однако закон DMCA не дает решения относительно дипфейков в форме видео, если жертва не является владельцем записи. Технически такие видеозаписи могут нарушать права как тех, кто участвовал в оригинальных съемках, так и тех, чьи лица были наложены [84]. Это особенно верно для случаев, когда были использованы лица знаменитостей [84]. Существуют две различные точки зрения на запрос об удалении цифрового материала в случае персонификации. Во-первых, владельцем контента может быть человек, создавший первоначальное видео. Тогда подать запрос может только жертва, чье тело использовано в дипфейке. Второй вариант, представленный на веб-сайте DMCA, – запрос об удалении может подать любой, кто изображен на видео, а значит, любая из жертв дипфейка²⁶⁴.

Запрос на удаление в рамках Закона DMCA, очевидно, не всегда может защитить жертву дипфейка; однако есть и другие меры, которые можно предпринять для удаления видео с веб-сайтов [11, р. 7]. На таких площадках, как Facebook, Instagram, Twitter, Reddit и Tumblr, есть собственные службы для выявления

и удаления порнографии без согласия по запросам²⁶⁵. В отличие от DMCA в этом случае жертва может сообщить о порнографическом дипфейке, даже если не является владельцем копирайта, и контент будет удален с платформы. На веб-сайте CCRJ есть раздел с подробными инструкциями о том, как сообщить о порнографическом дипфейке и потребовать его удаления с каждой из этих платформ²⁶⁶. Кроме того, жертва может удалить из своих списков или заблокировать пользователей; однако это не поможет удалить контент [11, р. 7].

б. Независимые наблюдатели

Развитие технологии дипфейков может привести к появлению рынка того, что называется «неизменяемым идентификационным следом» [85]. Это платная услуга (подобная мониторингу финансового состояния) по отслеживанию цифровых данных, перемещений и изображений [85]. Она позволит следить за физическими перемещениями и коммуникациями человека с помощью его электронных данных, связи, навигации, присутствия в Интернете, включая социальные сети [85]. Теоретически возможно будет определять фейковую информацию и удалять ее от имени клиента²⁶⁷.

²⁶⁵ См. Online Removal Guide, Cyber C.R. Initiative. URL: <https://www.cybercivilrights.org/online-removal/> [<https://perma.cc/9VYP-4TC5>] (дата обращения: 12.11.2019) (дается пошаговая инструкция по подаче запроса на удаление в различных социальных медиаплатформах, включая Facebook, Instagram, Twitter, Reddit, Tumblr, Yahoo!, Google и Microsoft).

²⁶⁶ Там же.

²⁶⁷ [85]. Однако идея такого рода сервиса, даже созданного с благими намерениями, имеет много недостатков. При обладании множеством личных данных о клиенте может оказаться невозможно оценить их все. Кроме того, человеческие и/или машинные ошибки при определении реального и фейкового будут серьезной проблемой. Наконец, и это, возможно, самое главное, возникают проблемы частной жизни. Считается, что, независимо от того, какие блага может принести такая услуга, она повлечет за собой «риск разрушения частной жизни – другими словами, уничтожение частной жизни в результате общественного договора, несмотря на все возможные правовые меры ее защиты». Там же. Компания, которая будет иметь не только доступ, но и возможности обработки бесконечного объема данных об отдельном человеке, будет обладать неограниченной властью над ним и представлять собой бесценный инструмент для рынка и исследований. Там же.

²⁶⁰ Pub.L. No. 105–304, 112 Stat. 2860 (1998) (кодифицировано с изменениями в различных разделах Свода законов США).

²⁶¹ What Is a DMCA Takedown?, DMCA. URL: <http://www.dmca.com/solutions/view.aspx?ID=aa18445c-9d91-44b3-9718-49da3eb208a2&ref=sol5a32> [<https://perma.cc/4BL8-WP5E>] (дата обращения: 09.04.2019).

²⁶² Там же.

²⁶³ Там же.

²⁶⁴ [84]. См. также What Is a DMCA Takedown?, выше примечание 260.

Стремительно развиваются не только технологии создания дипфейков, но и технологии, позволяющие определить их. В настоящее время подлинность цифрового и сетевого контента определяется с помощью алгоритмов машинного обучения, водяных знаков, цифровых ключей, отпечатков пальцев. Очевидно, что технологии распознавания также будут развиваться. Первая из них, алгоритмы машинного обучения, уже используется [11, р. 7]. Например, компания Gfycat применяет алгоритм, позволяющий определить фейковое видео путем сравнения его с оригинальным контентом [11]. Однако пока этот алгоритм не может проверять видео на частных серверах или личных аккаунтах в социальных сетях, поэтому для проверки дипфейк должен быть размещен в Интернете [11].

Технологическая «гонка вооружений» приблизилась к тому, чтобы различать ложную информацию, фото- и видеоизображение [6]. Идеальным ответом «на угрозу дипфейка стало бы одновременное развитие и распространение программного обеспечения, способного быстро и надежно распознавать дипфейки», а также «не отстающего от инноваций в технологии дипфейка» [6]. В настоящее время, однако, программное обеспечение для мониторинга и реагирования на данную проблему отстает от техно-

логий, позволяющих создавать дипфейки [6]. Поэтому принятие федерального уголовного закона против дипфейков является насущной необходимостью.

Заключение

Порнографические дипфейки стали феноменом в области киберпреступности с использованием сексуальной эксплуатации, который появился в последние несколько лет и в Интернете, и в повседневной жизни миллионов людей. Хотя первоначально жертвами этого явления были только женщины-знаменитости, быстрое развитие и широкое распространение технологий искусственного интеллекта ставит под угрозу каждого, кто имеет цифровые изображения. Подобно феномену «порно из мести», порнографические дипфейки стали представлять собой проблему прежде, чем законодатели могли на нее ответить. Поскольку ни один федеральный закон или закон штата в настоящее время не предусматривает ответственности за создание или распространение порнографических дипфейков, а также поскольку эти действия не ограничены какой-либо одной юрисдикцией, необходимо принимать меры на общенациональном уровне путем принятия федерального уголовного закона против дипфейков, так как их жертвой может стать каждый.

Список литературы / References

1. Cole S. We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now, *VICE: Motherboard*, Jan. 24, 2018, available at: https://motherboard.vice.com/en_us/article/bjye8a/reddit-fake-porn-app-daisy-ridley [<https://perma.cc/EN85-JSM7>].
2. Dold K. Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy, *Rolling Stone*, Apr. 17, 2018, available at: <https://www.rollingstone.com/culture/features/face-swapping-porn-how-creepy-trend-could-threaten-democracy-w518929> [<https://perma.cc/7J2Q-J2QD>].
3. Schwartz O. You Thought Fake News Was Bad?: Deep Fakes Are Where Truth Goes to Die, *Guardian*, Nov. 12, 2018, available at: <https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth> [<https://perma.cc/2KBB-FDWH>].
4. All Things Considered: Technologies to Create Fake Audio and Video Are Quickly Evolving, *NPR*, Apr. 2, 2018, available at: <https://www.npr.org/2018/04/02/598916380/technologies-to-create-fake-audio-and-video-are-quickly-evolving> [<https://perma.cc/V5TM-AUVJ>].
5. BuzzFeed (@BuzzFeed), *Twitter*, Apr. 17, 2018, available at: <https://twitter.com/BuzzFeed/status/98625799179922272> [<https://perma.cc/6A5J-RBEG>].
6. Bobby Chesney, Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, *Calif. L. Rev.*, 2019, available at: <http://dx.doi.org/10.2139/ssrn.3213954> [<https://perma.cc/FQG5-RG3Y>].
7. Blitz M. J. Lies, Line Drawing and (Deep) Fake News, *Okla. L. Rev.*, 2018, Vol. 71, p. 59.
8. Vincent J. Why We Need a Better Definition of 'Deepfake', *Verge*, May 22, 2018, available at: <https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news> [<https://perma.cc/Z2VE-56UV>].
9. Rouse M. Deepfake (Deep Fake AI), *Whatis.com*, available at: <https://whatis.techtarget.com/definition/deepfake> [<https://perma.cc/8UEZ-4NNP>] (дата обращения: 12.11.2019).
10. Rise of the Deepfakes, *Week*, June 9, 2018, available at: <http://theweek.com/articles/777592/rise-deepfakes> [<https://perma.cc/2P9A-DRWF>].

11. Adam Dodge, Johnstone E. Using Fake Video Technology to Perpetuate Intimate Partner Abuse, *Without my consent*, available at: <https://withoutmyconsent.org/perch/resources/2018-04-25deepfakedomesticviolenceadvisory.pdf> [<https://perma.cc/Q6DS-8G7S>] (дата обращения: 12.11.2019).
12. Roettgers J. 'DeepFakes' Will Create Hollywood's Next Sex Tape Scare, *Variety*, Feb. 2, 2018, available at: <http://variety.com/2018/digital/news/hollywood-sex-tapes-deepfakes-ai-1202685655/> [<https://perma.cc/Q4Q7-SCM5>].
13. Lee D. Deepfakes Porn Has Serious Consequences, *BBC News*, Feb. 3, 2018, available at: <https://www.bbc.com/news/technology-42912529> [<https://perma.cc/R4TY-LJQK>].
14. Jake Widman, Nicol W. What Is Reddit?: A Beginner's Guide to the Front Page of the Internet, *Digital Trends*, May 22, 2019, available at: <https://www.digitaltrends.com/social-media/what-is-reddit/> [<https://perma.cc/6ATF-U9FE>].
15. Hawkins D. Reddit Bans 'Deepfakes,' Pornography Using the Faces of Celebrities Such as Taylor Swift and Gal Gadot, *Wash. Post.*, Feb. 8, 2018, available at: <https://www.washingtonpost.com/news/morning-mix/wp/2018/02/08/reddit-bans-deepfakes-pornography-using-the-faces-of-celebrities-like-taylor-swift-and-gal-gadot/> [<https://perma.cc/2TPE-AYBG>].
16. Roose K. Here Come the Fake Videos, Too, *N. Y. Times*, Mar. 4, 2018, available at: <https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html> [<https://perma.cc/6QA8-78NL>].
17. Rense S. What Are 'Deepfakes,' and Why Are Pornhub and Reddit Banning Them?, *Esquire*, Feb. 12, 2018, available at: <https://www.esquire.com/lifestyle/sex/a17043863/what-are-deepfakes-celebrity-porn/> [<https://perma.cc/3QQS-XUCF>].
18. Donovan J. Deepfake Videos Are Getting Scary Good, *How Stuff Works*, Sept. 5, 2018, available at: <https://electronics.howstuffworks.com/future-tech/deepfake-videos-scary-good.htm> [<https://perma.cc/D6FA-HJA9>].
19. Suwajanakorn S. et al. Synthesizing Obama: Learning Lip Sync from Audio, *ACM Transactions on Graphics*, July 2017, p. 95:1.
20. Steinbuch Y. Listen to JFK Speak from Beyond the Grave, *N. Y. Post.*, Mar. 16, 2018, available at: <https://nypost.com/2018/03/16/jfks-voice-delivers-speech-he-never-gave-day-of-assassination/> [<https://perma.cc/TJQ9-6AFQ>].
21. Gstalter M. 'Obama' Voiced by Jordan Peele in PSA Video Warning About Fake Videos, *Hill*, Apr. 17, 2018, available at: <http://thehill.com/blogs/in-the-know/in-the-know/383525-obama-voiced-by-jordan-peelee-in-psa-video-warning-about-fake> [<https://perma.cc/9F4R-466W>].
22. McCarter R. Idiots on the Internet Are Getting Really Good at Splicing Nic Cage's Face onto Every Movie, *AV Club*, Sept. 4, 2018, available at: <https://news.avclub.com/idiots-on-the-internet-are-getting-really-good-at-splic-1828799192> [<https://perma.cc/5VAP-WQTK>].
23. Cole S. People Are Using AI to Create Fake Porn of Their Friends and Classmates, *Vice: Motherboard*, Jan. 26, 2018, available at: https://motherboard.vice.com/en_us/article/ev5eba/ai-fake-porn-of-friends-deepfakes [<https://perma.cc/8EPJ-GNNA>].
24. Roberts J. J. Fake Porn Videos Are Terrorizing Women. Do We Need a Law to Stop Them?, *Fortune*, Jan. 15, 2019, available at: <http://fortune.com/2019/01/15/deepfakes-law/> [<https://perma.cc/TNA3-G7TM>].
25. Franks M. A. Drafting an effective "Revenge porn" law, *A Guide for Legislators*, 2016, available at: <https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf> [<https://perma.cc/W3KB-Q7YQ>].
26. Danielle Keats Citron, Franks M. A. Criminalizing Revenge Porn, *Wake Forest L. Rev.*, 2014, Vol. 49, pp. 345.
27. Gilden A. Sex, Death, and Intellectual Property, *Harv. J. L. & Tech.*, 2018, Vol. 32, p. 67.
28. Cole S. Deepfakes Were Created as a Way to Own Women's Bodies – We Can't Forget That, *Vice: Broadly*, June 18, 2018, available at: https://broadly.vice.com/en_us/article/nekqmd/deepfake-porn-origins-sexism-reddit-v25n2 [<https://perma.cc/7FJ4-99T8>].
29. Buxton M. The Deep Dark World of Fake Porn, *Refinery*, available at: <https://www.refinery29.com/en-gb/2018/02/190383/deepfakes-ai-assisted-fake-porn> [<https://perma.cc/6NPX-KKQX>] (дата обращения: 07.02.2018).
30. Farokhmanesh M. Is It Legal to Swap Someone's Face into Porn Without Consent?, *Verge*, Jan. 30, 2018, available at: <https://www.theverge.com/2018/1/30/16945494/deepfakes-porn-face-swap-legal> [<https://perma.cc/5HP9-FQM6>].
31. Greenberg A. It's About to Get Even Easier to Hide on the Dark Web, *Wired*, Jan. 20, 2017, available at: <https://www.wired.com/2017/01/get-even-easier-hide-dark-web/> [<https://perma.cc/HKB6-C924>].
32. Spiccia P. The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given, *Val. U. L. Rev.*, 2013, Vol. 48, p. 369.
33. Bridy A. Remediating Social Media: A Layer-Conscious Approach, *B.U. J. SCI. & Tech. L.*, 2018, Vol. 24, p. 193.
34. Klonick K. The New Governors: The People, Rules, and Processes Governing Online Speech, *Harv. L. Rev.*, 2018, Vol. 131, p. 1598.
35. Cole S. Targets of Fake Porn Are at the Mercy of Big Platforms, *Vice: Motherboard*, Feb. 5, 2018.
36. Patton R. B. Taking the Sting Out of Revenge Porn: Using Criminal Statutes to Safeguard Sexual Autonomy in the Digital Age, *Geo. J. Gender & L.*, 2015, Vol. 16, p. 407.
37. Gil N. "Deepfake" Porn: The New Way Women Are Being Exploited Online, *Refinery29*, June 21, 2018, available at: <https://www.refinery29.com/en-gb/2018/06/202456/deepfake-pornography> [<https://perma.cc/J75W-MJJK>].
38. McKay T. Pornhub Says Digitally Generated 'Deepfakes' Are Non-Consensual and It Will Remove Them, *Gizmodo*, Feb. 6, 2018, available at: <https://gizmodo.com/pornhub-says-digitally-generated-deepfakes-are-non-cons-1822786071> [<https://perma.cc/6EJH-E7HU>].

39. Terms & Conditions, *Pornhub*, available at: <https://www.pornhub.com/information#terms> [<https://perma.cc/UB7Q-9D78>] (дата обращения: 18.05.2018).
40. Vincent J. Twitter Is Removing Face-Swapped AI Porn from Its Platform, Too, *Verge*, Feb. 7, 2018, available at: <https://www.theverge.com/2018/2/7/16984360/twitter-ban-fake-porn-ai-face-swap> [<https://perma.cc/NE6B-HSXL>].
41. Roettgers J. Naughty America Wants to Monetize Deepfake Porn, *Variety*, Aug. 20, 2018, available at: <https://variety.com/2018/digital/news/deepfake-porn-custom-clips-naughty-america-1202910584/> [<https://perma.cc/4PLT-BK7V>].
42. Clark B. Pornhub Promised to Ban ‘Deepfakes’ Videos. And It Failed Miserably, *TNW*, Apr. 18, 2018, available at: <https://thenextweb.com/insider/2018/04/19/pornhub-promised-to-ban-deepfakes-videos-and-it-failed-miserably/> [<https://perma.cc/GYC8-48AF>].
43. Ellis E. G. People Can Put Your Face on Porn – and the Law Can’t Help You, *Wired*, Jan. 26, 2018, available at: <https://www.wired.com/story/face-swap-porn-legal-limbo/> [<https://perma.cc/5VSH-CYRA>].
44. Linkous T. It’s Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn, *Rich. J. L. & Tech.*, 2014, Vol. 20, p. 14.
45. Samuel D. Warren, Brandeis L. D. The Right to Privacy, *Harv. L. Rev.*, 1890, Vol. 4, p. 193.
46. Citron D. K. Law’s Expressive Value in Combating Cyber Gender Harassment, *Mich. L. Rev.*, 2009, Vol. 108, p. 373.
47. Perritt H. H. *Law and the Information Superhighway*, New York, 1996.
48. Jasanoff S. Making Order: Law and Science in Action, *The Handbook of Science and Technology Studies*, 2008, p. 761.
49. Chris Meserole, Polyakova A. The West Is Ill-Prepared for the Wave of “Deep Fakes” That Artificial Intelligence Could Unleash, *Brookings*, May 25, 2018, available at: <https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash/> [<https://perma.cc/NNL4-9F8D>].
50. Groban M. S. Intimate Partner Cyberstalking – Terrorizing Intimate Partners with 21st Century Technology, *U. S. Attorneys’ Bull.*, May 2016, p. 12.
51. Brady K. M. Revenge in Modern Times: The Necessity of a Federal Law Criminalizing Revenge Porn, *Hastings Women’s L. J.*, 2017, Vol. 28, p. 3.
52. Amanda Lenhart et al. Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of “Revenge Porn”, *Data & Soc’y Res. Inst.*, Dec. 13, 2016, available at: https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf [<https://perma.cc/Q6KG-F5P6>].
53. Sherlock P. Revenge Pornography Victims as Young as 11, Investigation Finds, *BBC News*, Apr. 27, 2016, available at: <https://www.bbc.com/news/uk-england-36054273> [<https://perma.cc/S339-LKSR>].
54. Fay M. The Naked Truth: Insufficient Coverage for Revenge Porn Victims at State Law and the Proposed Federal Legislations to Adequately Redress Them, *B. C. L. Rev.*, 2018, Vol. 59, p. 1839.
55. Jacobs H. This Is What It Is Like to Be the Victim of Revenge Porn, and Why We Need to Criminalise It, *Independent*, Feb. 13, 2015, available at: <https://www.independent.co.uk/voices/comment/this-is-what-it-is-like-to-be-the-victim-of-revenge-porn-and-why-we-need-to-criminalise-it-10045067.html> [<https://perma.cc/Y9WV-PW66>].
56. Nelson S. Federal ‘Revenge Porn’ Bill Will Seek to Shriveled Booming Internet Fad, *U. S. News & World Rep.*, Mar. 26, 2014, available at: <https://www.usnews.com/news/articles/2014/03/26/federal-revenge-porn-bill-will-look-to-shriveled-booming-internet-fad> [<https://perma.cc/86UZ-LCNQ>].
57. Lahitou J. What Is the ENOUGH Act?: Lawmakers Are Pushing to Criminalize Revenge Porn with a New Bill, *Bustle*, Nov. 28, 2017, available at: <https://www.bustle.com/p/what-is-the-enough-act-lawmakers-are-pushing-to-criminalize-revenge-porn-with-a-new-bill-6337236> [<https://perma.cc/3ZXU-HXQD>].
58. Roffer J. Nonconsensual Pornography: An Old Crime Updates Its Software, *Fordham Intell. Prop. Media & Ent. L. J.*, 2017, Vol. 27, p. 935.
59. Carter T. B. Local, State, and Federal Responses to Stalking: Are Anti-Stalking Laws Effective?, *Wm. & Mary J. Women & L.*, 2016, Vol. 22, p. 333.
60. Wegman A. N. Cyberbullying and California’s Response, *U. S. F. L. Rev.*, 2013, Vol. 47, p. 737.
61. Christopher B. Can California Crack Down on Deepfakes Without Violating the First Amendment?, *Kqed News*, July 3, 2019, available at: <https://www.kqed.org/news/11758994/can-california-crack-down-on-deepfakes-without-violating-the-first-amendment> [<https://perma.cc/MA3Q-JJ7V>].
62. Sheeler A. California Is Moving to Ban Deepfakes. What Are They, Anyway?, *Sacramento Bee*, July 1, 2019, available at: <https://www.sacbee.com/news/politics-government/capitol-alert/article232162032.html> [<https://perma.cc/Y375-9QTK>].
63. Harris D. Student Article, Deepfakes: False Pornography Is Here and the Law Cannot Protect You, *Duke L. & Tech. Rev.*, 2019, Vol. 17, p. 99.
64. Kirstan Conley, Fonrouge G. Google Kills Revenge Porn Bill, *N. Y. Post*, June 21, 2018, available at: <https://nypost.com/2018/06/21/new-yorks-revenge-porn-bill-dies-after-11th-hour-campaign-by-google/> [<https://perma.cc/8YSF-Z8V3>].

65. Hetherington J. What Happened to New York's Revenge Porn Bill?, *Newsweek*, June 21, 2018, available at: <https://www.newsweek.com/what-happened-new-yorks-revenge-porn-bill-google-989666> [<https://perma.cc/7ZHY-C8JD>].
66. Greene A. The Ill of Misogyny on the Internet: Why Revenge Porn Needs Federal Criminalization, *Colo. Tech. L. J.*, 2017, Vol. 16, p. 175.
67. Desai S. Smile for the Camera: The Revenge Pornography Dilemma, California's Approach, and Its Constitutionality, *Hastings Const. L. Q.*, 2015, Vol. 42, p. 443.
68. Assefa H. Massachusetts Court Says 'Upskirt' Photos Are Legal, *CNN*, Mar. 6, 2014, available at: <https://www.cnn.com/2014/03/05/us/massachusetts-upskirt-photography/index.html> [<https://perma.cc/943Q-R2EA>].
69. Bustamante D. Florida Joins the Fight Against Revenge Porn: Analysis of Florida's New Anti-Revenge Porn Law, *Fiu L. Rev.*, 2017, Vol. 12, p. 357.
70. Fox H. Why Revenge Porn Laws May Not Protect Women, *Takepart*, Dec. 2, 2014, available at: <http://www.takepart.com/article/2014/12/02/revenge-porn-protections/> [<https://perma.cc/V6ZZ-Z8V4>].
71. Nisttahuz C. Fifty States of Gray: A Comparative Analysis of "Revenge-Porn" Legislation Throughout the United States and Texas's Relationship Privacy Act, *Tex. Tech L. Rev.*, 2018, Vol. 50, p. 333.
72. Waddell K. Lawmakers Plunge into "Deepfake" War, *Axios*, Jan. 31, 2019, available at: <https://www.axios.com/deepfake-laws-fb5de200-1bfe-4aaf-9c93-19c0ba16d744.html> [<https://perma.cc/KRH5-ZRWE>].
73. Kerr O. S. Should Congress Pass a "Deep Fakes" Law?, *Volokh Conspiracy*, Jan. 31, 2019, available at: <https://reason.com/volokh/2019/01/31/should-congress-pass-a-deep-fakes-law> [<https://perma.cc/6M8U-G7MA>].
74. Sasse B. This New Technology Could Send American Politics into a Tailspin, *Wash. Post.*, Oct. 19, 2018, available at: https://www.washingtonpost.com/opinions/the-real-scary-news-about-deepfakes/2018/10/19/6238c3ce-d176-11e8-83d6-291fced2ab1_story.html [<https://perma.cc/SL33-27K8>].
75. Hollister S. Scarlett Johansson Slams Deepfakes, Says She Can't Stop the Internet from Pasting Her Face on Porn, *Verge*, Dec. 31, 2018, available at: <https://www.theverge.com/2018/12/31/18163351/scarlett-johansson-slams-deepfakes-internet-lost-cause> [<https://perma.cc/SMK2-3H3P>].
76. Bloomberg. How Faking Videos Became Easy – and Why That's so Scary, *Fortune*, Sept. 11, 2018, available at: <http://fortune.com/2018/09/11/deep-fakes-obama-video/> [<https://perma.cc/64MB-JGG9>].
77. Donie O'Sullivan et al. When Seeing Is No Longer Believing: Inside the Pentagon's Race Against Deepfake Videos, *CNN Bus.*, available at: <https://www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/> [<https://perma.cc/6ASD-WK3Y>] (дата обращения: 12.11.2019).
78. Robert L. Ullmann, Ferrera D. L. Crime on the Internet, *Bos. B. J.*, Nov./Dec. 1998, p. 4.
79. Hawley A. E. Taking Spam out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail, *UMKC L. Rev.*, 1997, Vol. 66, p. 381.
80. Petroff A. Google, Microsoft Move to Block Child Porn, *CNN Bus.*, Nov. 18, 2013, available at: <https://money.cnn.com/2013/11/18/technology/google-microsoft-child-porn/index.html> [<https://perma.cc/6V7F-JFQM>].
81. Burrell A. Hell Hath No Fury Like a Woman Porned: Revenge Porn and the Need for a Federal Nonconsensual Pornography Statute, *Fla. L. Rev.*, 2014, Vol. 66, p. 2325.
82. Danny O'Brien, DiaKayyali. Facing the Challenge of Online Harassment, *Electronic Frontier Found.*, Jan. 8, 2015, available at: <https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment> [<https://perma.cc/9994-VK52>].
83. Citron D. K. *Hate Crimes in Cyberspace*, 2014.
84. Cole S. Personalized Fake Porn Videos Now for Sale on Reddit, *Vice: Motherboard*, Feb. 6, 2018, available at: https://motherboard.vice.com/en_us/article/7x799b/selling-ai-generated-fake-porn-is-probably-a-good-way-to-get-sued [<https://perma.cc/P5X7-VASJ>].
85. Robert Chesney, Citron D. Deep Fakes: A Looming Crisis for National Security, Democracy, and Privacy?, *Lawfareblog*, Feb. 21, 2018, available at: <https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy> [<https://perma.cc/SBJ2-7B3x>].
86. Rebecca A. Delfino, Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act, *Fordham L. Rev.*, 2019, 88, p. 887.

Дата поступления / Received 15.01.2020

Дата принятия в печать / Accepted 03.03.2020

Дата онлайн-размещения / Available online 25.03.2020

© Делфино Р. А., 2020. Впервые опубликовано на русском языке
в журнале «Актуальные проблемы экономики и права» (<http://apel.ieml.ru>) 25.03.2020

© Delfino R. A., 2020