Информационное общество и право

ТЕХНОЛОГИЯ ДИПФЕЙК: ВОПРОСЫ ОХРАНЫ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ ЛИЦА И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья рекомендована к публикации членом редакционного совета М. В. Якушевым 20.03.2024.

Жарова Анна Константиновна

Доктор юридических наук, доцент
Институт государства и права РАН, ведущий научный сотрудник
Москва, Российская Федерация
Anna_jarova@mail.ru

Аннотация

Мы все чаще слышим о таких правонарушениях, возникших в связи с использованием технологии дипфейк, как создание фейковых новостей, образа человека, не соответствующего действительности, например порнодипфейков. Анализ методов правового обеспечения неприкосновенности частной жизни лица и законной обработки персональных данных, при использовании технологии дипфейк, позволил прийти к следующим выводам - пользователь технологии дипфейк, создающий образ человека, становится оператором персональных данных. Судебная практика связывает субъективную сторону преступления с умыслом преступника на незаконное собирание и распространение данных о тайне частной жизни. Если человек не делал тайны из своей частной жизни, то создание дипфейка, не являющегося вредоносным, не подлежит уголовно-правовой ответственности. Для исключения гражданско-правовой ответственности пользователю технологии дипфейк, создающему новый позитивный образ жизнедеятельности человека, на основе общедоступных данных о частной жизни лица или общедоступных персональных данных, необходимо удостовериться в том, что эта информация является общедоступной по решению субъекта персональных данных, в рамках данного им согласия на обработку персональных данных или распространения информации о его частной жизни третьими лицами.

Ключевые слова

дипфейк; персональные данные; частная жизнь; уголовно-правовая ответственность; гражданско-правовая ответственность

Введение

Технологии будут развиваться вместе с человечеством, и во все времена человек находит возможности их применения как в законных, так и в противоправных целях – это две стороны информационной эволюции общества.

Еще в 2016 г. в Доктрине информационной безопасности Российской Федерации отмечались возрастающие масштабы компьютерной преступности, увеличивающееся число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. Было также отмечено, что методы, способы и средства совершения таких преступлений становятся все изощреннее [1].

Относительно недавно стала применяться технология «генеративный искусственный интеллект» (ГИИ). Благодаря своим алгоритмам генерации идей и концепций, текста и изображений, аудио – и видеоряда ГИИ позволил решить ряд различных социальных задач. Например, в области медицины, ГИИ помог ускорить процесс разработки лекарств и обнаружения

© Жарова А. К., 2024

Производство и хостинг журнала «Информационное общество» осуществляется Институтом развития информационного общества.

Данная статья распространяется на условиях международной лицензии Creative Commons «Атрибуция — Некоммерческое использование — На тех же условиях» Всемирная 4.0 (Creative Commons Attribution – NonCommercial - ShareAlike 4.0 International; CC BY-NC-SA 4.0). См. https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.ru

https://doi.org/10.52605/16059921_2024_05_114

новых связей в биологических системах, а также найти путь к преодолению проблемы лечения некоторых видов онкологии.

В 2020 г. российские и зарубежные ученые высказали предположение о том, что серьезную угрозу нарушения прав и свобод человека, возникающую в связи с использованием ГИИ несет технология дипфейк [2], [3], [4]. Технологий дипфейк предназначена для решения задач анализа неструктурированных данных, таких как язык, изображения или видео и создания новых аудио-видеоизображений. Используя эти возможности, со временем злоумышленники стали применять технологию дипфейк в целях совершения противоправных действий, например, для создания порнодипфейков. Технология дипфейк стала инструментом создания фейковых новостей, распространения дезинформации и пропаганды в том числе, кибербуллинга. В результате человек сталкивается с нарушением его прав и свобод, нравственными и физическими страданиями.

Число противоправных действий, осуществляемых с использованием технологии дипфейк, растет с каждым годом. Например, количество видеодипфейков не соответствующих действительности в 2023 г. увеличилось в три раза, по сравнению с 2022 г. аудиодипфейков в восемь [5]. Зачастую технологию дипфейк относят к вредоносному контенту, как показывает статистика, 96% из числа открыто представленных дипфейков в Сети, являются порнографическими [6].

Приведенная статистика позволяет сделать вывод о возрастании актуальности правового решения проблемы фальсификации контента в Сети, и важности противодействия таким информационным манипуляциям.

Увеличение законодательных инициатив в разных государствах в сфере охраны частной жизни лица, а также защиты биометрических персональных данных при применении технологии дипфейк, в том числе в области усиления ответственности за противоправные действия, совершаемые с использованием технологии дипфейк также подтверждает важность защиты прав и свобод человека от вмешательства в его личное пространство.

В связи с этим, целью статьи является анализ методов правового обеспечения неприкосновенности частной жизни лица и законной обработки персональных данных, при использовании технологии дипфейк.

1 Обработка персональных данных, с использованием технологии дипфейк

Активное использование технологии дипфейк для создания образа человека в противоправных целях требует от законодателей и ученых вырабатывать методы правового регулирования, применимые для решения задачи предотвращения незаконной обработки персональных данных [7], в том числе общедоступных данных.

В необходимость поиска правовых методов противодействия незаконному применению технологии дипфейк вносит и тот факт, что действующее законодательство в области охраны неприкосновенности частной жизни лица и защиты персональных данных разрабатывалось без учета регулирования отношений, возникающих с появлением новых технологий [7].

Докажем эту гипотезу на примере использования технологии дипфейк в целях создания образа о человеке.

Вначале рассмотрим проблему выполнения требований законодательства о персональных данных, в случае использования технологии дипфейк, а далее о неприкосновенности частной жизни лица, поскольку законодательство напрямую не связывает персональные данные с информацией о частной жизни лица, но, информация о частной жизни лица может содержать персональные данные, например, биометрические персональные данные, такие как изображение человека, его голос и др.

Лицо, использующее технологию дипфейк, становится оператором персональных данных, в соответствии с ФЗ «О персональных данных», поскольку это лицо «организует и (или) осуществляете обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными» (п. 2 ст.3 ФЗ «О персональных данных»).

В соответствии с требованиями ФЗ «О персональных данных» в большинстве случаев перед началом обработки персональных данных требуется получение согласия субъекта персональных данных. Кроме того, ФЗ «О персональных данных» определяя принципы обработки персональных данных, ориентируется на то, что цель обработки персональных данных должна «ограничиваться

достижением конкретных, заранее определенных и законных целей» (ч.2. ст. 5). В этой статье ФЗ «О персональных данных» также определяет недопустимость обработки персональных данных несовместимой с целями сбора персональных данных.

Однако, принципы, определенные в ст. 5 ФЗ «О персональных данных» выполнимы при таком взаимодействии оператора персональных данных с субъектом персональных данных, когда этот субъект известен. Но эти принципы невыполнимы при функционировании алгоритмов обработки неструктурированных данных и их анализа[9], например, в частном случае использования технологии дипфейк, когда происходит создание образа человека, на основании данных, размещенных в социальных сетях, субъект персональных данных заранее неизвестен пользователю этой технологии. В случае неструктурированных данных, связанных с человеком, например, размещенных в социальных сетях невозможно заранее – еще на стадии собирания данных, до осуществления их анализа, систематизировать данные по принадлежности к тому или иному объекту или субъекту. В связи с этим, невозможно, например в таком множестве неструктурированных данных, заранее определить данные, которые относятся к конкретному человеку с целью обращения к нему и получения информированного согласия на обработку его данных.

Однако после анализа данных, происходит их систематизация, результатом которого может быть визуализированная связь набора данных с объектом или субъектом. Например, результатом может быть идентификация человека в Сети, его нездоровой активности, преступных намерений. Иными словами, невозможно в случае работы с неструктурированными данными заранее знать о принадлежности данных к кому-либо, а это значит, что выполнить требование ФЗ «О персональных данных», в части получения информированного согласия субъекта персональных данных на их обработку невозможно.

2 Общедоступные персональные данные

Анализ законодательства о персональных данных, а также судебной практики позволяет сделать вывод, что и в случае обработки общедоступных персональных данных, например, размещенных в Сети, также требуется получение согласия субъекта персональных данных. Кроме того, оператору общедоступных персональных данных, в нашем случае – пользователю технологии дипфейк, необходимо иметь документальное подтверждение, того, что общедоступными свои персональные данные сделал сам человек [10]. Без письменного согласия субъекта персональных данных не представляется возможным утверждать, что они предоставлены именно им [11].

При отсутствии письменного согласия субъектов персональных данных, например, пользователей Сети, нельзя гарантировать, что персональные данные были сделаны общедоступными именно с их согласия или по их воле, а следовательно, данные в социальных сетях не являются общедоступными, даже в случае их размещения в общественном доступе, и их обработка не может осуществляться без согласия субъекта и в соответствии с п. 10 ч. 1 ст. 6 ФЗ «О персональных данных».

Этот вывод подтверждается судебной практикой. Так, рассмотрев кассационную жалобу акционерного общества «Национальное бюро кредитных историй» на решение Арбитражного суда города Москвы от 5 мая 2017 г. по делу N А40-5250/2017, постановление Девятого арбитражного апелляционного суда от 27 июля 2017 г. и постановление Арбитражного суда Московского округа от 9 ноября 2017 г. по тому же делу, Пленум Верховного Суда РФ приходит к выводу, что использование обществом "Национальное бюро кредитных историй" общедоступных данных пользователей социальной интернет-сети без подтверждения наличия от них согласия, была верно сочтена Роскомнадзором и судами противоречащей законодательству о персональных данных[12].

Размещение персональных данных в открытых источниках исходя из положений ФЗ «О персональных данных» не делает их автоматически общедоступными.

Таким образом, можно сделать вывод, что в случае создания дипфейка, содержащего изображение человека, на основе данных, размещенных, например, в Сети, пользователю технологии дипфейк как оператору персональных данных нужно удостовериться в том, что персональные данные, находящиеся в общем доступе, были размещены самим субъектом персональных данных. В таком случае пользователь технологии дипфейк не будет признан нарушителем требований ФЗ «О персональных данных».

3 Информация о частной жизни человека, обрабатываемая с использованием технологии дипфейк

Анализ научной литературы, позволил отметить встречающуюся позицию, что создание аудиовизуального изображения человека посредством технологии дипфейк, содержащего информацию о частной жизни лица, может являться нарушением права человека на ее неприкосновенность. Но, так ли это в самом деле?

3.1 Была ли частная жизнь тайной?

Несомненным правонарушением является нарушение режима конфиденциальности информации [19]. Но, можем ли мы, охраняя право человека на неприкосновенность частной жизни, говорить о том, что любая информация о частной жизни лица является тайной?

Министерство внутренних дел по Республике Адыгея под частной жизнью понимает «физическую и духовную сферу, которая контролируется самим индивидом, свободна от внешнего воздействия, то есть это семейная и бытовая сфера индивида, сфера его общения, отношение к религии, внеслужебные занятия, увлечения и иные сферы отношений, которым сам человек не желает придавать гласность, если этого не требует закон» [14]. Тем самым Министерство внутренних дел по Республике Адыгея связывает частную жизнь с информацией, которую человек не желает придавать гласности, т. е. он сохраняет ее в тайне от третьих лиц. Анализ данного определения, позволяет сделать предположение, что публичная информация о частной жизни лица, не попадает под охрану неприкосновенности частной жизни, поскольку эта информация уже оглашена.

Однако, Конституция РФ, определяет «право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» (ст.23). Мы видим, что Конституция РФ не ставит знак равенства между частной жизнью и личной и семейной тайной, в ст. 23 термины следуют друг за другом, как возможные самостоятельные состояния, связанные с человеком. При определенных условиях, такие категории тайны как личная и семейная тайна могут стать составной частью информации о частной жизни лица, но, верно, также и то, что частная жизнь может являться самостоятельным явлением, не содержащим никаких тайн, например, некоторые блогеры не делают никакой тайны из своей жизни, ведут запись всего, что с ними происходит[15], но от этого она не перестает быть частной жизнью.

Т. е. фактически Конституция РФ определяет право человека на неприкосновенность любой информации, которая так или иначе относится к его частной жизни, в том числе это касается и общедоступной частной жизни.

Конституционный Суд РФ право на неприкосновенность частной жизни определил как «предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера» [16].

Из определения Конституционного Суда РФ можно сделать вывод, что неприкосновенность частной жизни связана не с тайной, а с возможностью контролировать информацию о своей частной жизни. Например, человек готов размещать такую информацию на странице сайта в конкретной социальной сети, но запрещает ее распространение в другой социальной сети.

В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер [16]. Мы согласны с позицией Сухих Д. Н., которая в своей статье приходит к выводу, что «частная жизнь» является более общим понятием по отношению к понятиям «личная и семейная тайна» [17].

В таком случае можем ли мы прийти к выводу, что не будет являться правонарушением создание нового аудиовизуального образа другого человека, с применением технологии дипфейк, на основе открытых данных о частной жизни этого лица, которые он сам разместил о себе?

3.2 Общедоступная информация о частной жизни лица

Рассмотрим этот вопрос с позиций Гражданского кодекса Российской Федерации (ГК РФ) и Уголовного кодекса Российской Федерации (УК РФ).

Статья 152.2 ГК РФ устанавливает требования к получению согласия субъекта персональных данных в случаях, когда осуществляются действия по сбору, хранению, использованию или

распространению информации о его личной жизни, включая данные о происхождении, месте пребывания или жительства, личной и семейной жизни.

В данном случае речь идет о любой информации о частной жизни человека. Если информация о частной жизни гражданина получена с нарушением закона и используется при создании произведений науки, литературы и искусства, «содержится в документах, видеозаписях или на иных материальных носителях», то гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении дальнейшего ее распространения путем изъятия и уничтожения материальных носителей, содержащих соответствующую информацию, без какой бы то ни было компенсации (п. 4 ст. 152.2 ГК РФ).

Таким образом в случае, если дипфейк содержит информацию, полученную способом, который нарушает право гражданина контролировать информацию о себе, то он в рамках гражданского законодательства имеет основания обратиться в суд. Например, подобное нарушение права гражданина возможно в случае, если пользователь технологии дипфейк создал новый образ гражданина на основе размещенной этим гражданином в социальной сети информации, и распространил его в других социальных сетях. Поскольку в этом случае, во-первых, нарушается право гражданина контролировать информацию о своей частной жизни, а во-вторых, созданный новый образ является информацией не соответствующей действительности, хотя создан на основе реальных отдельных изображений человека. Данные правонарушения возникают, даже если образ не является вредоносным. В случае, если образ порочит честь, достоинство и деловую репутацию, то гражданин может защитить себя и требовать по суду опровержения этой информации (ст. 152 ГК РФ).

В соответствии со ст. 137 УК РФ, нарушением неприкосновенности частной жизни является «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации».

Под объективной стороной преступления, предусмотренного ст. 137 УК РФ понимают действия, нарушающие режим конфиденциальности частной жизни лица, влекущие нарушение конституционных принципов о тайне частной жизни лица. Иными словами, преступлением будет признаваться незаконные действия, при которых нарушается личная и семейная тайна. В тоже время не будет являться преступлением собирание информации о частной жизни лица, которую он оставил в Сети, поскольку в этом случае никакой тайны не существует.

Пленум Верховного Суда Российской Федерации выделил еще один критерий, который судам необходимо устанавливать для решения вопроса о наличии в действиях лица состава преступления, предусмотренного ч. 1 или ч.2 ст.137 УК РФ – это наличие умысла преступника, «что сведения о частной жизни гражданина хранятся им в тайне».

Но, в анализируемой нами ситуации, когда информация о частной жизни лица оставлена человеком в Сети, она не может быть отнесена к тайне, поскольку сам человек обладающий возможностью контроля над информацией о себе, разместил ее для общего доступа. Соответственно он сам принял решение об отсутствии режима конфиденциальности, правда нельзя сбрасывать со счетов, требование о том, что необходимо удостовериться, что подтверждение этим действиям человека должно быть зафиксировано в его согласии.

Верховный Суд РФ считает, что в этом случае такие действия не содержат состава преступления, предусмотренного ст. 137 УК РФ. «С учетом положений указанных норм уголовного закона в их взаимосвязи с положениями п. 1 ст. 152.2 ГК РФ не может повлечь уголовную ответственность собирание или распространение таких сведений в случаях, если сведения о частной жизни гражданина ранее стали общедоступными либо были преданы огласке самим гражданином или по его воле»[12].

Таким образом, с точки зрения правового регулирования отношений, связанных с использованием технологии дипфейк, если дипфейк был создан с использованием общедоступных данных о частной жизни лица, которые человек сам разместил о себе, а также если полученный контент не является вредоносным, то такие действие не будут признаваться уголовно-наказуемыми деяниями.

Однако несмотря на то, что Уголовный закон не связывает применение дипфейков с объективной стороной преступления, Генпрокуратура России с 2022 г. фиксирует и анализирует статистические данные о преступлениях, совершенных в том числе, с использованием технологии дипфейк [20].

Кроме того, в 2024 г. в целях обеспечения защиты персональных данных и охраны частной жизни лица в календарь рассмотрений Государственной Думы на 20 февраля 2024 г. был внесен

Законопроект № 502113-8 «О внесении изменений в УК РФ», который прошел первое чтение. Он дополняет УК РФ статьей 272.1, «предусматривающей уголовную ответственность за использование и(или) передачу (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем, а также за создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для незаконного хранения и (или) распространения персональных данных».

В то же время в законопроекте № 502113–8 отдельно урегулировано, что уголовное законодательство не будет рассматривать случаи, когда персональные данные используются правомерно в личных или семейных целях.

Таким образом, в законопроекте «конкретизирован объект преступного посягательства (компьютерная информация), который содержит персональные данные, полученные незаконным путем. Это позволяет разграничивать новый состав УК РФ от правонарушений, ответственность за которые предусмотрена КоАП в статье 13.11 «Нарушение законодательства РФ в области персональных данных», а также иных составов преступлений» [21].

Заключение

Подводя итог, можно отметить, что на данный момент судебная практика связывает субъективную сторону преступления с умыслом преступника на незаконное собирание и распространение данных о тайне частной жизни. Если человек не делал тайны из своей частной жизни, например, вел ее публичную трансляцию как в примере с блогером, то создание дипфейка, не являющегося вредоносным, не подлежит уголовно-правовой ответственности.

В тоже время для исключения гражданско-правовой ответственности пользователю технологии дипфейк, создающему новый позитивный образ жизнедеятельности человека, на основе общедоступных данных о частной жизни лица или общедоступных персональных данных, необходимо удостовериться в том, что эта информация является общедоступной по решению субъекта персональных данных, в рамках данного им согласия на обработку персональных данных или распространения информации о его частной жизни третьими лицами.

Литература

1. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" //СЗ РФ. 2016. № 50. Ст. 7074.
2. Deepfakes’ ranked as most serious AI crime threat // https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat
3. Добробаба, М. Б. Дипфейки как угроза правам человека / М. Б. Добробаба // Lex Russica (Русский закон). – 2022. – Т. 75, № 11(192). – С. 112–119. – DOI 10.17803/1729-5920.2022.192.11.112-119. – EDN XMHEAJ.
4. Ефремов, А. А. Оценка воздействия правового регулирования на развитие информационных технологий: зарубежный опыт и российские подходы к методике / А. А. Ефремов // Информационное право. – 2018. – № 4. – С. 29-32. – EDN SYCQHU.
5. Количество дипфейков в Сети увеличилось в разы в 2023 году — СМИ // https://d-russia.ru/kolichestvo-dipfejkov-v-seti-uvelichilos-v-razy-v-2023-godu-smi.html
6. Исследование показало, что 96% дипфейков в интернете — это порно с известными женщинами или бывшими подругами. URL: https://habr.com/ru/news/471208/
7. Амелин, Р. В. Презумпция достоверности информации в государственных информационных системах / Р. В. Амелин // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. – 2017. – Т. 17, № 4. – С. 458–464. – DOI 10.18500/1994-2540-2017-17-4-458-464. – EDN PYUEFC.
8. Жарова, А. К. Обеспечение права на доступ к Интернету и забвение в цифровом пространстве Российской Федерации / А. К. Жарова, В. М. Елин // Мониторинг правоприменения. – 2021. – № 2(39). – С. 48–53. – DOI 10.21681/2226-0692-2021-2-48-53. – EDN NEDFXI.

9. Zharova, A. K. The use of Big Data: A Russian perspective of personal data security / A. K. Zharova, V. M. Elin // Computer Law & Security Report. – 2017. – Vol. 33, No. 4. – P. 482-501. – DOI 10.1016/j.clsr.2017.03.025. – EDN XNHUQM.
10. Постановление Арбитражного суда Московского округа от 09.11.2017 N Ф05-16382/2017 по делу N А40-5250/2017 // СПС «КонсультантПлюс»
11. Определение Верховного Суда РФ от 29 января 2018 г. N 305-КГ17-21291 // СПС «КонсультантПлюс»
12. Постановление Пленума Верховного Суда РФ от 25.12.2018 N 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // Бюллетень Верховного Суда РФ, N 2, февраль, 2019.
13. Жарова, А. К. (2023). Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы. Journal of Digital Technologies and Law, 1(4), 973–993. https://doi.org/10.21202/jdtl.2023.42
14. Право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23, 24 Конституции России) https://01.мвд.рф/document/201354#:~:text=Под%20частной%20жизнью%20понимается%20физическая,одним%20из%20элементов%20частной%20жизни
15. Круглосуточные тиктокеры: сколько зарабатывают на продолжительных стримах // https://adpass.ru/kruglosutochnye-tiktokery-skolko-zarabatyvayut-na-prodolzhitelnyh-strimah/
16. Определение Конституционного Суда РФ от 09.06.2005 N 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом "б" части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации» // СПС «КонсультантПлюс».
17. Сухих, Д. Н. Правовые проблемы регулирования и применения личной и семейной тайны в Российской Федерации / Д. Н. Сухих // Ленинградский юридический журнал. – 2012. – № 4(30). – С. 250–256. – EDN PYQSRT.
18. Постановление Пленума Верховного Суда РФ от 25.12.2018 N 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // Бюллетень Верховного Суда РФ, N 2, февраль, 2019.
19. Abdelkarim, Y. A. (2023). Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism. Journal of Digital Technologies and Law, 1(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43
20. Приказ Генпрокуратуры России от 9 декабря 2022 г. № 746 «О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре» (вместе с «Положением о государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре», «Инструкцией о порядке предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в государственную автоматизированную систему правовой статистики», «Правилами заполнения учетных документов, используемых для предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в государственную автоматизированную систему правовой статистики») // Законность. № 2. 2023 (Приказ).
21. О внесении изменений в Уголовный кодекс Российской Федерации (в части установления ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержа-щей персональные данные).URL: https://sozd.duma.gov.ru/bill/502113-8

DEEPFAKE TECHNOLOGY: ISSUES OF PROTECTING THE PRIVACY OF A PERSON AND PROTECTING PERSONAL DATA

Zharova, Anna Konstantinovna

Doctor of law, associate professor
Institute of State and Law of the Russian Academy of Sciences, senior researcher
Moscow, Russian Federation
Anna_jarova@mail.ru

Abstract

Deepfake technology is designed to solve the problems of analyzing unstructured data, such as language, images or video, and creating new text or audio-video images. The analysis of the methods of legal protection of the privacy of a person and the legitimate processing of personal data, using deepfake technology, conducted in the article, allowed us to come to some conclusions/ The user of deepfake technology, creating an image of a person, becomes an operator of personal data; at the moment, judicial practice connects the subjective side of the crime with the criminal's intent to illegally collect and distribute data about the secret of private life. If a person did not make a secret of his private life, then the creation of a non-malicious deepfake is not subject to criminal liability. To exclude civil liability, a user of deepfake technology who creates a new positive way of life based on publicly available data about a person's private life or publicly available personal data must make sure that this information is publicly available by the decision of the personal data subject, within the framework of his consent to the processing of personal data or the dissemination of information about his privacy by third parties.

Keywords

deepfake; personal data; private life, criminal liability, civil liability

References

1. Ukaz Prezidenta RF ot 05.12.2016 N 646 "Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii" // SZ RF. 2016. № 50. St. 7074.
2. Deepfakes' ranked as most serious AI crime threat/ URL: https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat
3. Dobrobaba, M. B. Dipfejki kak ugroza pravam cheloveka / M. B. Dobrobaba // Lex Russica (Russkij zakon). – 2022. – T. 75, № 11(192). – S. 112-119. – DOI 10.17803/1729-5920.2022.192.11.112-119. – EDN XMHEAJ.
4. Efremov, A. A. Ocenka vozdejstviya pravovogo regulirovaniya na razvitie informacionnyh tekhnologij: zarubezhnyj opyt i rossijskie podhody k metodike / A. A. Efremov // Informacionnoe pravo. – 2018. – № 4. – S. 29-32. – EDN SYCQHU.
5. Kolichestvo dipfejkov v Seti uvelichilos' v razy v 2023 godu — SMI/ URL: https://d-russia.ru/kolichestvo-dipfejkov-v-seti-uvelichilos-v-razy-v-2023-godu-smi.html
6. Issledovanie pokazalo, chto 96% dipfejkov v internete — eto porno s izvestnymi zhenshchinami ili byvshimi podrugami https://habr.com/ru/news/471208/
7. Amelin, R. V. Prezumpciya dostovernosti informacii v gosudarstvennyh informacionnyh sistemah / R. V. Amelin // Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya: Ekonomika. Upravlenie. Pravo. – 2017. – T. 17, № 4. – S. 458-464. – DOI 10.18500/1994-2540-2017-17-4-458-464. – EDN PYUEFC.
8. Zharova, A. K. Obespechenie prava na dostup k Internetu i zabvenie v cifrovom prostranstve Rossijskoj Federacii / A. K. Zharova, V. M. Elin // Monitoring pravoprimeneniya. – 2021. – № 2(39). – S. 48-53. – DOI 10.21681/2226-0692-2021-2-48-53. – EDN NEDFXI.
9. Zharova, A. K. The use of Big Data: A Russian perspective of personal data security / A. K. Zharova, V. M. Elin // Computer Law & Security Report. – 2017. – Vol. 33, No. 4. – P. 482-501. – DOI 10.1016/j.clsr.2017.03.025. – EDN XNHUQM.
10. Postanovlenie Arbitrazhnogo suda Moskovskogo okruga ot 09.11.2017 N F05-16382/2017 po delu N A40-5250/2017 // SPS «Konsul'tantPlyus».
11. Opredelenie Verhovnogo Suda RF ot 29 yanvarya 2018 g. N 305-KG17-21291 // SPS «Konsul'tantPlyus»

12. Postanovlenie Plenuma Verhovnogo Suda RF ot 25.12.2018 N 46 "O nekotoryh voprosah sudebnoj praktiki po delam o prestupleniyah protiv konstitucionnyh prav i svobod cheloveka i grazhdanina (stat'i 137, 138, 138.1, 139, 144.1, 145, 145.1 Ugolovnogo kodeksa Rossijskoj Federacii)" // Byulleten' Verhovnogo Suda RF, N 2, fevral', 2019.
13. Zharova, A. K. (2023). Dostizhenie algoritmicheskoj prozrachnosti i upravlenie riskami informacionnoj bezopasnosti pri prinyatii reshenij bez vmeshatel'stva cheloveka: pravovye podhody. Journal of Digital Technologies and Law, 1(4), 973–993. https://doi.org/10.21202/jdtl.2023.42
14. Pravo na neprikosnovennost' chastnoj zhizni, lichnuyu i semejnuyu tajnu, zashchitu svoej chesti i dobrogo imeni (st. 23, 24 Konstitucii Rossii). URL: https://01.mvd.rf/document/201354#:~:text=Pod%20chastnoj%20zhizn'yu%20ponimaetsya%20fizicheskaya,odnim%20iz%20elementov%20chastnoj%20zhizni
15. Kruglosutochnye tiktokery: skol'ko zarabatyvayut na prodolzhitel'nyh strimah // https://adpass.ru/kruglosutochnye-tiktokery-skolko-zarabatyvayut-na-prodolzhitelnyh-strimah/
16. Opredelenie Konstitucionnogo Suda RF ot 09.06.2005 N 248-O "Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdan Zaharkina Valeriya Alekseevicha i Zaharkinoj Iriny Nikolaevny na narushenie ih konstitucionnyh prav punktom "b" chasti tret'ej stat'i 125 i chast'yu tret'ej stat'i 127 Ugolovno-ispolnitel'nogo kodeksa Rossijskoj Federacii" // SPS «Konsul'tantPlyus».
17. Suhih, D. N. Pravovye problemy regulirovaniya i primeneniya lichnoj i semejnoj tajny v Rossijskoj Federacii / D. N. Suhih // Leningradskij yuridicheskij zhurnal. – 2012. – № 4(30). – S. 250-256. – EDN PYQSRT.
18. Postanovlenie Plenuma Verhovnogo Suda RF ot 25.12.2018 N 46 "O nekotoryh voprosah sudebnoj praktiki po delam o prestupleniyah protiv konstitucionnyh prav i svobod cheloveka i grazhdanina (stat'i 137, 138, 138.1, 139, 144.1, 145, 145.1 Ugolovnogo kodeksa Rossijskoj Federacii)" // Byulleten' Verhovnogo Suda RF, N 2, fevral', 2019.
19. Abdelkarim, Y. A. (2023). Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism. Journal of Digital Technologies and Law, 1(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43
20. Prikaz Genprokuratury Rossii ot 9 dekabrya 2022 g. № 746 "O gosudarstvennom edinom statisticheskom uchete dannyh o sostoyanii prestupnosti, a takzhe o soobshcheniyah o prestupleniyah, sledstvennoj rabote, doznanii, prokurorskom nadzore" (vmeste s "Polozheniem o gosudarstvennom edinom statisticheskom uchete dannyh o sostoyanii prestupnosti, a takzhe o soobshcheniyah o prestupleniyah, sledstvennoj rabote, doznanii, prokurorskom nadzore", "Instrukciej o poryadke predostavleniya pervichnyh statisticheskih dannyh o sostoyanii prestupnosti, o soobshcheniyah o prestupleniyah, sledstvennoj rabote i doznanii v gosudarstvennuyu avtomatizirovannuyu sistemu pravovoj statistiki", "Pravilami zapolneniya uchetnyh dokumentov, ispol'zuemyh dlya predostavleniya pervichnyh statisticheskih dannyh o sostoyanii prestupnosti, o soobshcheniyah o prestupleniyah, sledstvennoj rabote i doznanii v gosudarstvennuyu avtomatizirovannuyu sistemu pravovoj statistiki") // Zakonnost'. № 2. 2023 (Prikaz).
21. O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii (v chasti ustanovleniya otvetstvennosti za nezakonnye ispol'zovanie i peredachu, sbor i hranenie komp'yuternoj informacii, soderzha-shchej personal'nye dannye) //https://sozd.duma.gov.ru/bill/502113-8