Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2024. – Т. 10 (76). № 4. – С. 347–352.

УДК 343.721

К ВОПРОСУ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ДИСТАНЦИОННЫЕ ХИЩЕНИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ «ДИПФЕЙК»

Евтушенко И. И.

Крымский филиал Краснодарского университета МВД России

Рассматриваются вопросы уголовно-правового противодействия мошенничествам, совершаемым с помощью технологий искусственного интеллекта, цифровой обработки информации и ее последующей подмены, так называемые технологии DeepFake. Обращено внимание, что все чаще злоумышленники получают полную информацию о человеке, его персональных данных путем неправомерного доступа к ним. На основе зарубежного опыта противодействия DeepFake анализируются законодательные инициативы в России о введении новых составов преступлений или дополнении уже имеющихся составов преступлений новыми квалифицирующими признаками, связанными с незаконным оборотом персональных данных граждан. Автор предлагает ввести концептуальное понятие дистанционного хищения без деления его на формы, так как при дистанционном способе виктимации потерпевшего криминообразующим фактором является именно способ виктимации, а не способ изъятия имущества. Введение в УК РФ особенного вида – дистанционного хищения как раз должно учесть особенности получения информации о человеке в качестве квалифицирующего признака и ее подмены для введения потерпевшего в заблуждение.

Ключевые слова: дистанционное хищение, дистанционные мошенничества, дистанционная кража, дипфейк, персональные данные, компьютерная информация, преступления, совершаемые с помощью ИТТ.

Последнее время все большее распространение получают ситуации виктимации потерпевших через звонки и сообщения в социальных сетях и различных мессенджерах. И если еще несколько лет назад мошенники использовали методы массовой рассылки или случайного обзвона, то сейчас их общение с жертвой становится все более персонифицированным, тщательно подготовленным.

Преступники собирают, обрабатывают и затем используют большие массивы персональных данных о потерпевших, получаемые ими как из открытых источников – официальных аккаунтов организаций, предприятий, органов власти, так и неправомерно – из распространяемых «украденных» баз данных как частных организаций (служб доставки, такси, банков и т.п.), так и органов государственной власти (миграционного учета, ГАИ, Росреестра и т.д.), социальных учреждений (больниц, поликлиник, образовательных организаций). Поскольку у преступного мира высок спрос на любые персональные данные о людях, всегда будут находиться как технические уязвимости в защите баз данных, так и прямой подкуп уполномоченных сотрудников. Сами потерпевшие зачастую невольно помогают злоумышленникам собирать о себе информацию – в социальных сетях, в самих мессенджерах активно раскрывают информацию о себе, публикуют общедоступные истории, номера телефон, даты рождения, семейное положение. Таким образом, информация о каждом человеке может быть собрана без использования специальных познаний в компьютерных технологиях.

Но особое беспокойство у общества и профессиональных участников рынка информационных услуг вызывает все большее проникновение в нашу повседневную

жизнь технологий искусственного интеллекта, цифровой обработки информации и ее последующей подмены, так называемые технологии DeepFake, когда с помощью новейших программных средств искусственный интеллект подменяет один голос, лицо на другие, или даже фальсифицирует потоковое видео.

Технология DeepFake – это способ цифровой обработки информации с использованием технологий искусственного интеллекта в результате которого исходные файлы фото, видео или аудио подвергаются изменению, зачастую фальсифицируются без согласия и даже ведома как правообладателя, так и участников.

Как отмечают авторы исследования, проведенного в 2019 г. – 90-95% всех дипфейков создаются без согласия правообладателя и это были случаи фальсификации интимных изображения женщин [1]. И если еще 5-10 лет назад для использования данной технологии требовались глубокие познания в области компьютерных технологий и наличие специального профессионального программного обеспечения, то на сегодняшний день программистами создана масса готовых мини-программ, использующих технологию искусственного интеллекта для обработки небольших видео. Поэтому сегодня создание и распространение фальшивых изображений приняло массовый характер. Однако на практике возникают вопросы: как отличить оригинальные продукты от подделок? Как отличить дипфек, созданный правомерно правообладателем или с его согласия от неправомерного? Этот вопрос интересует и многих ученых [2, с. 215-240], как криминологов, так и криминалистов.

Исследователи отмечают два вектора развития права в сфере правового регулирования использовании технологии подмены личности, по которому пошли мировые державы. При этом следует различать два аспекта правого регулирования использования данной технологии: гражданско-правовой и уголовно-правовой.

В целом следует отметить, что развитие правового регулирования в сфере применения технологии искусственного интеллекта идет по пути разработки правовых рамок его использования. Соответственно, любое противоправное применение данной технологии должно быть запрещенным.

В сфере уголовно-правового регулирования, все больше юристов и руководителей федеральных органов власти обращают внимание на необходимость разработки эффективных механизмов противодействия противоправному использованию дипфейков и защиты прав добросовестных граждан, организаций, государства от преступных посягательств. Так, в частности, в России на государственном уровне в декабре 2023 г. по итогам прошедшей стратегической сессии, посвященной нацпроекту «Экономика данных» было принято решение о создании цифровой платформы для обнаружения дипфейков, созданных с помощью технологий искусственного интеллекта [3]. Однако эта платформа не сможет защитить обычных граждан от потокового поддельного аудио- или видео-звонка через мессенджеры, которые часто используют преступники в своих целях.

В США был предложен законопроект о введении уголовной ответственности за создание и использование технологии Дипфейк без согласия изображаемых лиц. В Китае же данную технологию посчитали полезной и обязали правообладателей наносить на изображение специальную маркировку, а ее отсутствие влечет существенные штрафы как для создателя дипфейка, так и цифровой платформы, его разместившей [4, с. 91-104].

В России в части установления уголовной ответственности за создание и использование дипфейков одновременно реализуются две стратегии противодействия преступности: и введение в УК РФ самостоятельного состава преступления, и дополнение уже существующих квалифицирующими признаками, усиливающими наказуемость деяний, совершенных с использованием дипфейков.

Первая стратегия подвергается критике из-за возможной конкуренции и дублирования норм, например, со ст. 146 УК РФ в части присвоения авторства или неправомерного использования произведения автора. Возникнут и другие примеры двойного вменения [5, с. 76-83]. Однако это не мешает Пленуму Верховного Суда РФ рекомендовать осуществлять двойное вменение по ст. 272 и 159.6 УК РФ в случаях компьютерного мошенничества. Именно поэтому в Государственной Думе РФ еще в декабре 2023 г. прошел первое чтение законопроект о введении новой статьи 272^1 в УК РФ, предусматривающий 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» [6]. Ко второму чтению рекомендовано учесть замечания, высказанные в официальных отзывах ВС РФ и Правительства РФ в части разграничения с административной ответственностью. Кроме того, у нас возникают вопросы и о конкуренции со ст. 272 УК РФ, где предметом уголовно-правовой охраны также могут быть персональные данные в цифровом виде, которые являются охраняемой законом компьютерной информацией.

Вторая стратегия была реализована в виде законопроекта об ужесточении ответственности для уже существующих составов преступлений путем дополнения их квалифицирующим признаком «с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, а равно с использованием биометрических персональных данных потерпевшего или иного лица», который был принят к рассмотрению Государственной Думой РФ 16.09.2024 г. [7, с. 76-83]. Однако на представленный законопроект были получены отрицательные заключения как ВС РФ, так и Правительства РФ. В частности, отмечено, что из пояснительной записки законопроекта не следует, чем использование технологии подмены личности при совершении мошеннического обмана повышает общественную опасность совершаемого преступления, и почему другие, более тяжкие преступления террористического характера или экстремисткой направленности не предлагается дополняться таким же квалифицирующим признаком.

Следует отметить, что в настоящее время положения уголовного законодательства о защите личной тайны, охраняемой компьютерной информации и положения федерального закона о защите персональных данных не согласованы между собой. Е.В. Хохолова в своем диссертационном исследовании отмечает, что данные понятия пересекаются, но не совпадают, различаясь режимом правовой охраны. Так, «персональные данные могут находиться в режиме конфиденциальности (ограниченного доступа) или доступной информации (общедоступной)». При чем, их общедоступность должна исключать уголовную ответственность за их собирание или распространение. И соответственно, предлагает «ввести в научный оборот опреде-

ление неприкосновенности персональных данных» [8, с. 13-14] как самостоятельного права человека. Полагаем, что предложение Е.В. Хохоловой о дополнении УК РФ новым составом преступлений в виде ст. 137^1 УК РФ «Нарушение неприкосновенности персональных данных» в главе «Преступления против конституционных прав и свобод граждан» более обоснованы, чем рассмотренный уже в Государственной Думе законопроект о введении новой ст. 272^1 УК РФ в главу «Преступления против компьютерной информации», поскольку определяющим для квалификации являются особенности предмета посягательства – персональные данные о человеке, не находящиеся в открытом доступе, а объектом – его право на личную неприкосновенность, а не способ их изъятия или форма записи этих сведений – в цифровом виде.

При криминализации деяний в УК РФ определяющими могут быть разные признаки состава преступления. И тут важно в первую очередь определиться с объектом посягательства: что защищает государство? Личную тайну о человеке? Собственность? Компьютерную информацию о человеке или его собственности? Полагаем, что внесение изменений в УК РФ последних лет нарушило систему и принципы криминализации деяний, о чем не раз говорили авторитетные ученые. В настоящий момент мы имеем различные составы преступлений, пересекающиеся между собой, но имеющие различные объекты посягательства. И поскольку эти объекты разные, то необходимой квалифицировать такие деяния по совокупности, например, ст. 159^6 и 272 УК РФ, или 137 и 272 УК РФ. Но при дистанционных хищениях мы будем квалифицировать не только дважды за одно, но и трижды: по ст.ст. 272^1, 143^1 и 159 (альтернативно ст. 158) УК РФ. Такое положение нельзя признать допустимым.

Как отмечает МВД России, «почти две трети преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (70,2%) совершается путем кражи или мошенничества: 475,3 тыс.». А за 8 месяцев 2024 г. доля преступлений, совершенных с использованием ИТТ возросла с 32,9% в январе-августе 2023 г. до 39,2% [9]. Учитывая степень распространенности дистанционных хищений, а их число по статистике за 2023 год возросло на 28%, необходимо в целом усилить уголовную ответственность за такие хищения. Дистанционный способ изъятия ценностей гражданина учтен законодателем как квалифицирующий признак в п. «г» ч.3 ст. 158, ст. 159^1 и ст. 159^6 УК РФ и, соответственно, влекущий более строгое наказание. И при этом Верховный Суд РФ полагает возможным дополнительное вменение статей 272 или 273 УК РФ. Т.е., особенности способа изъятия имущества фактически дважды учитываются при квалификации и влекут еще более строгое наказание по совокупности преступлений, что является прямым нарушением международного принципа справедливости – «не дважды за одно».

Потерпевшему, государству, да и правоприменителю, по сути, нет разницы, по какой статье уголовного закона будут квалифицированы действия мошенников: как кража или как собственно мошенничество. Поэтому считаем целесообразным вместо введения новых квалифицирующих признаков в составы преступлений против собственности, ввести концептуальное понятие дистанционного хищения без деления его на формы (кража, мошенничество, вымогательство), так как при дистанционном способе виктимации потерпевшего криминообразующим фактором является

именно способ виктимации, а не способ изъятия имущества. Дистанционный способ изъятия имущества не повышает степень общественной опасности самого преступления, а значительно затрудняет раскрываемость этих преступлений (так, по итогам 2023 года по главе 28 УК РФ раскрываемость оказалась чуть выше 6%, а по дистанционным мошенничествам – 10%!!!). Вместе с тем введение в УК РФ особенного вида – дистанционного хищения как раз должно учесть особенности получения персональных данных о человеке в качестве квалифицирующего признака и подмены информации для введения потерпевшего в заблуждение.

Как мы отмечали ранее, дистанционные хищения независимо от способа изъятия имущества, объединяют несколько существенных особенностей: изъятие денежных средств совершается в условиях неочевидности, когда преступник и потерпевший не видят друг друга и, как правило, незнакомы; преступник находится, как правило, в другом субъекте РФ и даже за пределами РФ; такие преступления носят организованный, тщательно подготовленный характер, позволяющий вовлечь неопределенно большой круг потерпевших, в том числе путем неправомерного завладения базами персональных данных граждан, используя современное программное обеспечение, новейшие технические разработки и устройства; предметом таких преступлений выступают только денежные средства, которые обезличены, могут быть переданы преступнику как в безналичной, так и наличной форме; потерпевший в момент изъятия денежных средств с его счета вообще не осознает факта хищения [10, с. 65-67].

Все вышеуказанные признаки позволяют выделить дистанционные хищения в особую криминологически значимую группу, в которую должны входить и кражи, и мошенничества, и вымогательства, совершенные с применением информационно-телекоммуникационных технологий. Соответственно, и меры противодействия таким хищениям должны быть общими, учитывающими не столько способ изъятия денежных средств, сколько способ виктимации потерпевших.

Что касается введения новых составов преступлений – статей 143^1 и 272^1 в УК РФ, то этот вопрос требует еще более детального изучения на предмет исключения двойного или тройного вменения совместно с преступлениями против собственности.

Список литературы:

1. Simonite T. Most Deepfakes are Porn, and They’re Multiplying Fast // URL:: https://www.wired.com/story/most-deepfakes-porn-multiplying-fast/ (дата обращения: 20.09.2024)
2. Виноградов В.А., Кузнецова Д.В. Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. – Том 17. – № 2. С. 215–240.
3. Арялина М. Минцифры планирует создать систему для выявления дипфейков // URL:: https://www.vedomosti.ru/technology/articles/2024/03/21/1026954-mintsifri-planiruet-sozdat-sistemu-dlya-viyavleniya-dipfeikov?utm_campaign=vedomosti_public&utm_content=1026954-mintsifri-planiruet-sozdat-sistemu-dlya-viyavleniya-dipfeikov&utm_medium=social&utm_source=telegram_ved (дата обращения: 20.09.2024)
4. Дремлюга Р.И., Моисейцев В.В., Парин Д.В., Романова Л.И. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (deepfake): опыт Китая //Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. – Т. 24. – № 4. С. 91–104.
5. Ситник В.Н./ Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк// Уральский журнал правовых исследований. – 2022. – № 3. С. 76–83.
6. Законопроект № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации (в части установления ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные)» // URL: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 20.09.2024)

7. Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности)» // URL: https://sozd.duma.gov.ru/bill/718538-8#bh_histras (дата обращения: 20.09.2024)
8. Хохлова Е.В. Незаконные действия с персональными данными: уголовно-правовое исследование специальность 5.1.4 «Уголовно-правовые науки»: автореф. дис. … канд. юрид. наук. / Хохлова Елена Васильевна. – Саратов, 2024. – 26 с. – Текст: непосредственный.
9. Состояние преступности в РФ за январь-декабрь 2023 г.// URL: https://мвд.рф/ (дата обращения: 20.09.2024)
10. Евтушенко, И. И. Дистанционные хищения: понятие и признаки / И. И. Евтушенко, А. А. Венедиктов // Гуманитарные, социально-экономические и общественные науки. – 2020. – № 12-2. – С. 65-67.

Evtushenko I.I. On the issue of criminal liability for remote theft committed using deepfake technology // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2024. – T. 10 (76). № 4. – P. 347–352.

The issues of criminal law counteraction to fraud committed with the help of artificial intelligence technologies, digital information processing and its subsequent substitution, the so-called DeepFake technologies, are considered. Attention is drawn to the fact that more and more often intruders receive complete information about a person and his personal data through unauthorized access to them. Based on the foreign experience of countering DeepFake, legislative initiatives in Russia on the introduction of new elements of crimes or the addition of existing elements of crimes with new qualifying signs related to the illegal trafficking of personal data of citizens are analyzed. The author proposes to introduce the conceptual concept of remote theft without dividing it into forms, since with the remote method of victimization of the victim, the criminalizing factor is precisely the method of victimization, and not the method of seizure of property. The introduction of a special type of remote theft into the Criminal Code of the Russian Federation should take into account the peculiarities of obtaining information about a person as a qualifying feature and its substitution for misleading the victim

Keywords: remote theft, remote fraud, remote theft, deepfake, personal data, computer information, crimes committed with the help of ITT.

Spisok literatury:

1. Simonite T. Most Deepfakes are Porn, and They’re Multiplying Fast // URL:: https://www.wired.com/story/most-deepfakes-porn-multiplying-fast/ (data obrashheniya: 20.09.2024)
2. Vinogradov V.A., Kuzneczova D.V. Zarubezhny`j opy`t pravovogo regulirovaniya texnologii «dipfejk» // Pravo. Zhurnal Vy`sshej shkoly` e`konomiki. 2024. – Tom 17. – № 2. S. 215–240.
3. Aryalina M. Mincifry` planiruet sozdat` sistemu dlya vy`yavleniya dipfejkov // URL:: https://www.vedomosti.ru/technology/articles/2024/03/21/1026954-mintsifri-planiruet-sozdat-sistemu-dlya-viyavleniya-dipfeikov?utm_campaign=vedomosti_public&utm_content=1026954-mintsifri-planiruet-sozdat-sistemu-dlya-viyavleniya-dipfeikov&utm_medium=social&utm_source=telegram_ved (data obrashheniya: 20.09.2024)
4. Dremlyuga R.I., Moisejcev V.V., Parin D.V., Romanova L.I. Nacional`noe pravovoe regulirovanie ispol`zovaniya i rasprostraneniya realistichny`x audiovizual`ny`x poddel`ny`x materialov (deepfake): opy`t Kitaya //Aziatsko-Tixookeanskij region: e`konomika, politika, pravo. 2022. – T. 24. – № 4. S. 91–104.
5. Sitnik V.N. Perspektivy` ustanovleniya ugolovnoj otvetstvennosti za prestupleniya, sovershenny`e s ispol`zovaniem texnologii dipfejk// Ural`skij zhurnal pravovy`x issledovanij. – 2022. – № 3. S. 76–83.
6. Zakonoproekt № 502113-8 «O vnesenii izmenenij v Ugolovny`j kodeks Rossijskoj Federacii (v chasti ustanovleniya otvetstvennosti za nezakonny`e ispol`zovanie i peredachu, sbor i xranenie komp`yuternoj informacii, soderzhashhej personal`ny`e danny`e)». – URL: https://sozd.duma.gov.ru/bill/502113-8 (data obrashheniya: 20.09.2024)
7. Zakonoproekt № 718538-8 «O vnesenii izmenenij v Ugolovny`j kodeks Rossijskoj Federacii (v chasti ustanovleniya ugolovnoj otvetstvennosti za sovershenie prestuplenij s ispol`zovaniem texnologij podmeny` lichnosti)» // URL: https://sozd.duma.gov.ru/bill/718538-8#bh_histras (data obrashheniya: 20.09.2024)
8. Xoxlova E.V. Nezakonny`e dejstviya s personal`ny`mi danny`mi: ugolovno-pravovoe issledovanie special`nost` 5.1.4 «Ugolovno-pravovy`e nauki»: avtoref. dis. … kand. yurid. nauk / Xoxlova Elena Vasil`evna. – Saratov, 2024. – 26 s. – Tekst: neposredstvenny`j.
9. Sostoyanie prestupnosti v RF za yanvar`-dekabr` 2023 g. – URL: https://mvd.rf/ (data obrashheniya: 20.09.2024)
10. Evtushenko, I. I. Distancionny`e xishheniya: ponyatie i priznaki / I. I. Evtushenko, A. A. Venediktov // Gumanitarny`e, social`no-e`konomicheskie i obshhestvenny`e nauki. – 2020. – № 12-2. – S. 65-67.

.