


ЦИФРОВАЯ ИДЕНТИЧНОСТЬ: ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ

Марина Александровна Ефремова

*Казанский филиал Российского государственного университета правосудия им. В. М. Лебедева,
г. Казань, Российская Федерация
crimlaw16@gmail.com*

 <https://orcid.org/0000-0001-6037-6921>

Аннотация. В статье рассматривается проблема обеспечения надлежащей защиты цифровых данных физического лица. Взаимодействуя в сети с другими пользователями, каждый так или иначе оставляет некий цифровой след, формируя при этом образ цифровой личности. Для получения доступа ко всевозможным онлайн-сервисам необходимы учетные данные, финансовая информация, биометрические данные. Совокупность таких сведений позволяет идентифицировать человека в цифровой среде и составляет его цифровую идентичность. Подобного рода данные могут стать предметом кражи цифровой личности. Помимо получения данных о физических лицах, кража личных данных включает их использование или продажу, передачу другим лицам и дальнейшее использование в противоправной деятельности. Одним из новых методов, используемых для кражи личных данных и мошенничества, стали технологии искусственного интеллекта. Технология дипфейк может быть использована для кражи личных данных, как и цифровые данные о личности могут быть использованы для создания дипфейка. В статье делается вывод, что в большинстве случаев нормы действующего уголовного законодательства могут быть применены для квалификации описываемых деяний. Подчеркивается необходимость сосредоточения усилий для противодействия кражам личности и использованию дипфейк технологии на совокупности мер.

Ключевые слова: цифровая личность, цифровая идентичность, кража личности, компьютерная информация, неправомерный доступ к компьютерной информации, преступления в сфере компьютерной информации, уголовная ответственность


Для цитирования: Ефремова М. А. Цифровая идентичность: проблемы уголовно-правовой охраны // Правопорядок: история, теория, практика. 2025. № 3(46). С. 124–129. DOI: 10.47475/2311-696X-2025-46-3-124-129

Review article

DIGITAL IDENTITY: PROBLEMS OF CRIMINAL LAW PROTECTION

Marina A. Efremova

*Kazan Branch of the Russian State University of Justice named after V. M. Lebedev, Kazan, Russian Federation
crimlaw16@gmail.com*

 <https://orcid.org/0000-0001-6037-6921>

Abstract. The article discusses the problem of ensuring proper protection of an individual's digital data. Interacting online with other users, everyone leaves a digital footprint in one way or another, while forming an image of a digital personality. To gain access to various online services, you need credentials, financial information, and biometric data. The totality of such information makes it possible to identify a person in a digital environment and constitutes his digital identity. This kind of data can be the subject of digital identity theft. In addition to obtaining data about individuals, identity theft includes their use or sale, transfer to others, and further use in illegal activities. Artificial intelligence technologies have become one of the new methods used for identity theft and fraud. Deepfake technology can be used to steal personal data, just as digital identity data can be used to create a deepfake. The article concludes that in most cases the norms of the current criminal legislation can be applied to qualify the described acts. The need to focus efforts to counter identity theft and the use of deepfake technologies on a set of measures is emphasized.

Keywords: digital identity, digital identity, identity theft, computer information, unlawful access to computer information, crimes in the field of computer information, criminal liability

For citation: Efremova MA. Digital Identity: Problems of Criminal Law Protection. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2025;(3):124-129. (In Russ.) DOI: 10.47475/2311-696X-2025-46-3-124-129

Введение

В последние десятилетия интернет и информационно-телекоммуникационные технологии стали неотъемлемой частью жизни современного общества. Их влияние охватывает все сферы деятельности — от экономики и образования до государственного управления и социальной коммуникации. Информационные технологии позволяют создавать системы электронного правительства, обеспечивая прозрачность, доступность и оперативность государственных услуг. Это способствует укреплению доверия граждан к институтам власти и повышению качества публичного управления. Расширение сфер применения цифровых технологий приводит к массовому сбору, хранению и обработке конфиденциальной информации.

В 2024 году в России Интернетом пользовались свыше 130 млн человек¹. Современные реалии таковы, что многие люди проводят в социальных сетях и мессенджерах значительное количество времени. Заботясь о количестве лайков и просмотров, некоторые пользователи открыто делятся личной конфиденциальной информацией, не задумываясь о последствиях. Доступность информационно-телекоммуникационных технологий привела к существенному росту объемов конфиденциальной информации, находящейся под угрозой неправомерного доступа.

Материалы и методы

Исследование базируется на следующих материалах: труды отечественных и зарубежных ученых по проблемам информационной безопасности личности в цифровую эпоху; нормативно-правовых актах, регулирующих сферу обращения личной конфиденциальной информации; опубликованных данных статистики, обзорах практики, отчетах различных ведомств и организаций, отражающих современное состояние правовой защищенности личной конфиденциальной информации.

В основу исследования положены общенаучные и частнонаучные методы познания, в том числе анализ, синтез, индукция, дедукция и др.

Результаты исследования

О каждом Интернет-пользователе сегодня можно говорить как о «цифровой личности». Это широкий и комплексный концепт, включающий не только учетные данные пользователя, но и цифровой след: как лицо

ведет себя в сети, что публикует, как взаимодействует с другими. Это своего рода «образ» личности в Интернете. В социальных сетях цифровая личность — это профиль, фотографии, посты, комментарии, лайки и репутация среди других пользователей.

Близким понятием следует признать «цифровую идентичность» (digital identity) — это совокупность данных и атрибутов, идентифицирующих человека в цифровой среде. Она включает в себя: учетные данные (логины, пароли) для доступа к различным онлайн-сервисам, социальным сетям, электронной почте; персональные данные (ФИО, дата рождения, адрес, телефон, данные документов); финансовую информацию (номера банковских карт, счетов, данные платежных систем); биометрические данные (фотографии, отпечатки пальцев, сканы сетчатки глаза). Иными словами, цифровая идентичность — это цифровой паспорт реальной личности в виртуальном мире.

Приведенные понятия взаимосвязаны, но не тождественны: цифровая идентичность — это часть цифровой личности, но цифровая личность — гораздо шире и включает в себя все, что связано с присутствием человека и поведением в цифровом пространстве.

Профили в социальных сетях часто служат средством конструирования идеализированной виртуальной картинки, представляющей собой, по сути, сублимированную проекцию личности. В рамках данной парадигмы пользователи социальных сетей склонны к репрезентации тех черт и характеристик, которые они субъективно оценивают как эталонные, что, в свою очередь, может приводить к диссонансу между цифровым и реальным личностным профилем. При этом следует подчеркнуть, что действующее законодательство не содержит императивных предписаний, возлагающих на пользователей юридическую обязанность по предоставлению аутентичной информации о себе, а равно не предусматривает мер ответственности за искажение личных цифровых данных самим пользователем. Ученые все больше говорят о цифровой идентичности как о праве. Более того, высказываются предложения о признании права на идентичность на международном [1] и национальном уровнях [3].

Вместе с тем, незаконное присвоение данных о цифровом образе человека, даже если он является идеализированным, может использоваться для проведения противоправных финансовых операций, создания «цифровых двойников» и других незаконных целей. Такие действия получили название «кража цифровой личности» или «кража цифровой идентичности» (digital identity theft). Термин «кража цифровой личности» появился в 1964 году и с тех пор ассоциируется

¹ Путин назвал число пользователей интернета в России // URL: https://www.rbc.ru/technology_and_media/11/12/2024/6759b4709a79472b45d8949e?ysclid=mb5d6k525700552871 (дата обращения 26.05.2025)

с неправомерным использованием личной цифровой информации.

Термин «кража личности» следует использовать с некой долей условности, так как он неточно отражает суть явления. Фактически речь идет не о краже самой личности, включающей характер, эмоции и переживания, а о хищении и использовании удостоверительных признаков, позволяющих преступнику выдавать себя за другое лицо. Таким образом, более точным было бы говорить о краже или присвоении цифровых идентификационных данных лица или личных цифровых данных.

Анализ существующих немногочисленных доктринальных определений кражи цифровых данных показывает, что акцент в них делается на получение материальной выгоды, в то время как неправомерный доступ к цифровому объекту рассматривается как сопутствующий элемент, а не как самостоятельная цель. Другими словами, основным мотивом признается корыстный, а сам факт несанкционированного доступа к цифровой личной информации играет роль средства реализации преступного намерения. Некоторые исследователи и вовсе рассматривают кражу личности как разновидность мошенничества [3]. Однако хотя кража личных цифровых данных в большинстве случаев и совершается с целью получения материальной выгоды, имущественный ущерб личности физической причиняется не всегда, хотя при этом всегда нарушаются его личные права. Как справедливо отмечает А. В. Майоров, личные цифровые данные, полученные незаконным путем, в дальнейшем используются для социальной инженерии, то есть для манипуляции людьми со стороны злоумышленников, получения иной информации для использования в преступных целях [4, с. 82–83].

Представляется, что кражу личных цифровых данных можно рассматривать в двух аспектах: узком и широком. В узком смысле (или кража личных цифровых данных «в чистом виде») — это незаконное получение данных об одном или нескольких физических лицах. В широком смысле, помимо получения данных о физических лицах, кража личных данных включает их использование или продажу, передачу другим лицам и дальнейшее использование в противоправной деятельности.

В специальной литературе отмечается, что ввиду терминологической неопределенности следует рассматривать отдельно каждую разновидность кражи личных данных (например, неправомерное использование существующих банковских счетов, неправомерное использование существующих кредитных карт и открытие новых счетов) вместо анализа кражи личных данных в целом [5, с. 180].

Следует выделить следующие виды кражи личных цифровых данных:

1. Кража личных данных для создания цифрового двойника — использование личной информации другого человека, чтобы представлять или идентифицировать себя как этого человека.

2. Кража личных данных ребенка — кража и использование личных цифровых данных ребенка другим лицом в противоправных целях. Полученные данные могут быть использованы для создания поддельных аккаунтов, а также шантажа и мошенничества. Интерес со стороны преступников к цифровым данным детей обусловлен тем, что дети зачастую не обладают достаточными знаниями для защиты своей цифровой информации, а также не всегда осознают последствия раскрытия своих данных третьим лицам.

3. Кража личных данных пожилых людей — кража, целью которой являются пенсионеры, так как большинство из них не знакомы с технологиями и по этой причине легко уязвимы. Данные похищаются с целью последующего оформления кредитов на имя пенсионера, получения доступа к государственным выплатам и сбережениям.

4. Кража платежных или финансовых данных предполагает последующее получение учетных данных кредитной или дебетовой карты, а также их незаконное использование, например, снятие средств со счета другого лица без согласия этого лица. Одной из наиболее распространенных является кража личных данных, связанная с использованием кредитных карт. Возросшее число мобильных и онлайн-транзакций привело к тому, что в последние годы участились случаи мошенничества и кражи личных данных, когда платежная карта физически не используется. Потерпевший обычно узнает о мошенничестве, когда получает сообщение от банка о том, что была совершена транзакция.

Следует отметить, что приведенная классификация не исчерпывает все возможные виды кражи цифровых личных данных, а отражает наиболее распространенные из них.

Чаще всего лицо, чьи личные цифровые данные попали в руки преступников, не знает о случившемся до тех пор, пока они не будут использованы в противоправной деятельности. Это не удивительно, так как в настоящее время существует множество схем и способов неправомерного завладения цифровыми личными данными, включая покупку их в Darknet, фишинговые атаки, рассылку вредоносного программного обеспечения и плечевой серфинг. Личные данные могут быть получены как физически, так и в электронном формате. Физические кражи часто происходят с компьютеров, устройств хранения данных, мобильных телефонов, а также из рюкзаков, сумок и бумажников.

Рассматривая кражу цифровых личных данных через призму уголовного права, следует отметить, что в большинстве случаев подобным деяниям можно дать надлежащую правовую оценку. Так, если преступник получил доступ к охраняемой законом компьютерной информации, то содеянное может быть квалифицировано по ст. 272 УК РФ. Если виновный для получения личных цифровых данных использовал вредоносное программное обеспечение, то деяние должно квалифицироваться по ст. 273 УК РФ и по совокупности с другими статьями УК РФ [6, с. 84]. В зависимости от ха-

рактера сведений и способа получения доступа к ним, деяние может быть квалифицировано по совокупности со ст. 137, 138, 183 УК РФ. Если с использованием данных об украденной цифровой личности совершаются финансовые операции, то подобного рода действия могут быть квалифицированы по ст. 159.6 УК РФ как хищение путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, или просто как мошенничество по ст. 159 УК РФ.

Нельзя не отметить что, УК РФ был дополнен новой статьей 272¹, 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. Объектом преступного посягательства выступает компьютерная информация, содержащая персональные данные, полученная путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем. С ростом числа пользователей возросло и число утечек информации, которое в последние годы остается стабильно высоким. По данным экспертов, в 2024 году произошло 778 случаев утечки информации ограниченного доступа. Аналитики подчеркивают, что объемы утекших данных оцениваются только в количестве записей и касаются только персональных данных и платежной информации¹. Положения ст. 272.1 УК РФ направлены на противодействие утечек массивов компьютерной информации, содержащей персональные данные, а не единичных случаев краж цифровой личности.

Одним из новых методов, используемых для кражи личных данных и мошенничества, стали технологии искусственного интеллекта. В последнее время возможности искусственного интеллекта все чаще стали использоваться для создания дипфейков. Дипфейки (deepfakes) — это технология, которая позволяет создавать реалистичные, но при этом фальшивые видео- и аудиозаписи. Сам термин deepfake образован сочетанием двух слов: глубокое обучение и подделка, и основан он на глубоких нейронных сетях, которые позволяют создавать правдоподобный контент, который на самом деле является подделкой. Широкое

распространение данной технологии актуализирует фундаментальные вопросы о подлинности цифровой информации и надежности средств массовой информации в эпоху, когда все больше доминируют цифровые коммуникационные платформы. Распространение технологии глубокой подделки обостряет опасения общества по поводу размывания правды и манипулирования реальностью [7, с. 90]. Технология дипфейк может быть использована для кражи личных данных, как и цифровые данные о личности могут быть использованы для создания дипфейка.

Сегодня в открытом доступе есть программы, которые имитируют лицо и мимику по фото и видео из соцсетей. Они способны заставить цифровую копию гражданина отвечать на вопросы. Так же доступен софт, который синтезирует голос, используя за основу аудио, отправленное в виде голосового сообщения в мессенджерах.

Последствия кражи личных данных с помощью дипфейков не ограничиваются мошенничеством и предполагают более широкие социальные риски. Например, они могут использоваться для выдачи себя за политических лидеров или других общественных деятелей, распространения ложной информации или разжигания социальных конфликтов.

Наибольшее распространение технология дипфейк получила при совершении мошенничества. Первый случай использования поддельного голоса, созданного с помощью искусственного интеллекта, при совершении мошенничества произошел в 2019 г., когда генеральный директор британской энергетической компании полагал, что разговаривает по телефону со своим начальником, генеральным директором немецкой компании и выполнил приказ немедленно перевести 220 000 евро². Сегодня звонок «от руководителя» — одна из наиболее распространенных схем использования дипфейк технологий при мошенничестве.

Уязвимости в системе цифровой идентификации, а именно в системе биометрической аутентификации, позволяют злоумышленникам использовать дипфейки для того, чтобы выдавать себя за отдельных лиц и получать несанкционированный доступ к конфиденциальным данным или услугам. Поддельная видео- или аудиозапись голоса человека может быть использована для обхода систем аутентификации на основе голоса, позволяя мошенникам выдавать себя за жертву и осуществлять мошеннические транзакции. Более того, дипфейки могут использоваться для создания поддельных удостоверений личности, паспортов или других документов. В недавних исследованиях, посвященных рассматриваемой проблеме, высказывается гипотеза о том, что подделка именно биометрических данных является наиболее опасной. А для противодействия этому явлению предлагается криминализовать фальсификацию биометрических данных с целью скрыть

¹ Россия: утечки информации ограниченного доступа, 2023–2024 // URL: <https://www.infowatch.ru/company/presscenter/news/kolichestvo-slitykh-personalnykh-dannykh-v-dve-tysyachidvadtsat-chetvertom-godu-vyroslo-na-tret> (дата обращения 26.05.2025)

² URL: <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/> (дата обращения 26.05.2025)

другое преступление или облегчить его совершение, то есть речь идет об ответственности за подготовительную преступную деятельность к совершению иных преступлений с использованием поддельного образа другого лица [8]. Другие ученые предлагают дополнить ч. 1 ст. 63 УК РФ новым отягчающим наказанием обстоятельством «совершение преступления с использованием искусственного интеллекта или технологий, созданных на его основе» [9].

Говоря о необходимости и перспективах совершенствования действующего уголовного законодательства, следует отметить, что отдельные государства уже предусмотрели уголовную ответственность за кражу личных данных, хотя большинство стран все еще рассматривают кражу личных данных как способ незаконного доступа к данным, мошенничества, подделки документов, нарушения авторских прав или как действие, предшествующее совершению другого преступления. Так, например, законодательства США, Великобритании, Франции содержат отдельные нормы, предусматривающие ответственность за кражу личных данных. Многие страны ЕС (Австрия, Болгария, Бельгия, Венгрия, Греция, Германия, Ирландия, Италия, Нидерланды, Польша, Румыния, Испания) пока еще не признают кражу личных данных самостоятельным преступлением [10].

Что же касается противодействию использованию дипфейк технологий при совершении преступлений, то здесь вновь хочется отметить законодательство США. На федеральном уровне борьба с дипфейками велась в рамках механизма, регулируемого Законом о разрешении на национальную оборону (NDAA), в котором вводятся ограничения на его использование. Федеральный законодатель рассматривает дипфейки

как проблему, связанную с национальной безопасностью. В 2019 году в Калифорнии и Техасе были приняты первые два закона, касающиеся борьбы с фейками во время избирательного процесса. Немецким законодателем в 2017 году был принят специальный закон, направленный на борьбу с дезинформацией и введение мер, ограничивающих незаконный контент, путем отчетности и установления ответственности платформ социальных сетей за незаконный контент.

Заключение

Подводя итог изложенному выше, следует отметить, что кража личных цифровых данных преимущественно осуществляется с целью последующего неправомерного использования этих данных для совершения других преступлений. Сама по себе кража личных цифровых данных «в чистом виде», равно как и дальнейшие противоправные действия с этими данными, сегодня вполне могут быть квалифицированы по уже имеющимся статьям Особенной части УК РФ. Противодействие же использованию поддельных биометрических данных человека исключительно посредством установления уголовно-правового запрета видится утопичным. Перспективными направлениями могут стать разработка соответствующих технологических решений, способных распознавать подделку, а также подготовка соответствующих специалистов. Учитывая глобальный характер Интернета и цифровых платформ, кража цифровых данных личности может выйти за рамки национальных границ, поэтому совместные усилия между странами по обмену передовым опытом и участию в совместных исследованиях и разработках могут сыграть важную роль.

Список источников

1. Sullivan C., Digital identity — a legal perspective // SCHIRN Mag. 2015. <https://www.schirn.de/schirnmag/digitale-identitaet-und-die-rechtlichen-aspekte/> (дата обращения 26.05.2025)
2. Напсо М. Д., Напсо М. Б. Тренды цифровой трансформации общества: актуальные проблемы реализации прав индивида в сфере информации // Журнал российского права. 2021. № 10. С. 85–97.
3. Pontell H. Pleased to Meet You. . . Won't You Guess My Name: Identity Fraud, cyber-crime, and white-collar Delinquency // *Adelaide Law Review*. 2002. Vol. 23, no. 2. P. 305–328.
4. Майоров А. В. Виктимологическое обеспечение информационной безопасности личности // *Правопорядок: история, теория, практика*. 2024. № 3(42). С. 80–88.
5. Xiaochen Hu, Jae-Seung Lee & Nicholas P. Lovrich Do Commonly Recommended Preventive Actions Deter Identity Theft Victimization? Findings from NCVS Identity Theft Surveys // *Journal of Crime and Justice*. 2023. Vol. 46, no. 2. P. 172–193.
6. Русскевич Е. А. О совокупности преступлений в сфере компьютерной информации с другими преступлениями // *Уголовное право*. 2025. № 4. С. 76–84.
7. Mansoor S. I. U. Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft // *Central University of Kashmir Law Review*. 2024. No. 4. P. 65–92.
8. Мосечкин И. Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // *Вестник Санкт-Петербургского университета. Серия право*. 2025. № 1. С. 95–110.
9. Архипцев И. Н., Сарычев А. В., Мотузов А. В. К вопросу о правовом обеспечении предупреждения преступлений, совершаемых с использованием искусственного интеллекта и технологий, созданных на его основе в Российской Федерации // *Правовая парадигма*. 2022. Т. 21, № 2. С. 175–181.
10. Merdović B., Jovanović B. Understanding Identity Theft and Fraud // *Kultura polisa*. 2024. Vol. 21, no. 2. P. 17–43. DOI: 10.51738/Kpolisa2024.21.2r.17mj

СВЕДЕНИЯ ОБ АВТОРЕ

Ефремова Марина Александровна

Доктор юридических наук, профессор, заведующий кафедрой уголовно-правовых дисциплин, Казанский филиал Российского государственного университета правосудия им. В. М. Лебедева
Россия, 420088, г. Казань, 2-я Азинская ул., 7А
E-mail: crimlaw16@gmail.com
ORCID: 0000-0001-6037-6921

INFORMATION ABOUT THE AUTHOR

Marina A. Efremova

Doctor of Legal Sciences, Professor,
Head of the Department of Criminal Law Disciplines of the Kazan Branch of the Russian State University of Justice named after V. M. Lebedev
7A 2nd Azinskaya str., Kazan, 420088, Russia
E-mail: crimlaw16@gmail.com
ORCID: 0000-0001-6037-6921

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 25.06.2025.

Дата рецензирования статьи / Revised: 14.07.2025.

Дата принятия статьи к публикации / Accepted: 15.08.2025.