DOI: 10.18522/2070-1403-2021-85-2-2-11

ФИЛОСОФИЯ

(специальность: 09.00.08)

УДК 101

Д.С. Быльева, В.В. Лобатюк
Санкт-Петербургский политехнический
университет Петра Великого
г. Санкт-Петербург, Россия
redaction-el@mail.ru

ЛИЦО КАК ТЕХНОЛОГИЧЕСКИЙ ОБЪЕКТ

[*Daria S. Bylyeva, Viktoria V. Lobatyuk* Face as a technological object]

It is analyzed the phenomenon of the face as a technological object from the viewpoint of the philosophy of technology. Information and communication technologies do not simply change existing social practices, but "reontologize" the world, creating a new environment for existence. The human face begins to play an increasing role in the digital world, going far beyond self-presentation. The phenomenon of the popularity of social media has brought many photo and video images to digital reality. Having existed for a short time only as a reflection of physical reality, faces have be-come a "data bank" used for a variety of purposes. Face is both an object of digital identification (for access control, searching for an individual, analyzing a human flow), and property that can be used with malicious intent. The proliferation of altered faces, simulacrum faces that do not belong to anyone, digital copies of the dead bring digital reality to a new level of illusion.

Key words: face, technological object, deep fake, digital society, information and communication technologies, digital reality.

Взаимодействие, опосредованное информационно-коммуникативными технологиями, играет все более важную роль в жизни современного человека. Согласно концепции инфосферы итальянского философа Лучано Флориди, информационно-коммуникационные технологии "реонтологизируют" мир, создавая новую среду существования [6]. Данная среда меняет сущностные характеристики бытия. Ч. фон Ксайландер представляет его как воображаемое публичное пространство, скомпрометированное отсутствием конфиденциальности [15, с. 123]. В глобальном цифровом пространстве как в потустороннем мире люди, лишенные физической оболочки, оказываются трудно различимыми призраками. Презентуемая визуальная составляющая образа в сети может быть любая, виртуальная реальность располагает к игре с иден-

тичностью. Потребность доказывать экзистенциальную подлинность бытия личной самопрезентацией в социальных сетях заставила на время зеркало цифровой реальности отражать лица в их природной бесцельной бытийности. Однако цифровая реальность, вобрав в себя лицо как сложный и ценный технологический объект, обладающий очевидной уникальностью и неотчуждаемой принадлежностью конкретному субъекту, превратила его в визуальный идентификатор личности и одновременно отразила его множеством копий и симулякров. Став «анализируемыми данными» фото- и видео-определенность обращается в свою противоположность в бесконечной вариативности реальностей хаоса. Распознавания лиц безусловно более сложная задача для цифровых технологий, чем символьная последовательность, однако сегодня «искусственный интеллект» справляется с ней все с большей точностью, поэтому все большее количество контрольно-идентификационных функций может выполняться с помощью распознавания лиц.

Система распознавание лиц находит в современном мире все более разнообразное применение прежде всего в области контроля доступа/авторизации, поиска определенных индивидов, подсчета общего количества и по демографическим категориям людей в общественных местах. На практике распознавание лиц используется как на государственном уровне, так и частными фирмами: от поиска преступников до применения нормирование количества бумаги в общественных туалетах. Пин-коды как защита доступа уходят в прошлое, а на смену им приходит биометрия. Рассмотрим применение данной технологии в смартфонах [11]. Еще в пятой версии Android была предусмотрена возможность разблокировать телефон по лицу владельца, первыми это воплотили в компании Samsung в модели Galaxy S8. Но смартфон можно было вскрыть при помощи фотографии, поэтому пользователи предпочитали разблокировку через сканер отпечатка пальцев. Это связано с тем, что первоначально для данной технологии использовалось 2D распознавание лиц, основанное на не более чем сотне лицевых точек, по котором производилось сравнение.

В настоящее время 2D из-за слабых статистических показателей применяется лишь в многофакторной аутентификации, либо в социальных сетях (например, указание людей на фото в «Facebook»). Позднее за разработку данной технологии, но уже в 3D формате, взялись в Apple и создали систему Face

ID, которая полноценно реализована в смартфонах начиная с модели iPhone X. Используется нейросеть, обученная на миллиарде изображений людей разного пола, расы, возраста. Прическа, очки, контактные линзы или даже усы не оказывают существенного влияние на распознавание пользователя. Face ID постоянно обновляет и уточняет паттерн лица. Face ID стал результатом объединения самых передовых аппаратных и программных компонентов Apple. Камера TrueDepth захватывает данные лица, проецируя на него и анализируя более 30 000 невидимых точек. Таким образом, устройство составляет подробную структурную карту лица, а также его изображение в инфракрасном спектре.

Фрагмент нейронного ядра микропроцессоров A11, A12 Bionic, A12X Bionic и A13 Bionic, защищенный модулем Secure Enclave, преобразует карту глубины и инфракрасное изображение в математическое представление, которое сравнивается с зарегистрированными данными лица. Технология Face ID проверяет соответствие с использованием данных о структуре лица, которые невозможно считать с напечатанной или цифровой двухмерной фотографии. А сложные нейронные сети защищают от мошенничества с использованием масок или других приемов. Хотя существует один зафиксированный случай, когда Face ID обманули маской. Это было сделано экспертами вьетнамской компании Bkav, специализирующейся на исследованиях в области кибербезопасности, в качестве подтверждения они опубликовали видеоролик, который во всех подробностях демонстрирующий процесс разблокировки. Но создание масок, с высокой точностью копирующих человеческое лицо, это процесс не только крайне долгий, но и дорогостоящий, видимо с этим связано отсутствие информации о массовом повторение опыта Bkav.

Подобные по механизму действия Face ID технологии используются и в других сферах. Не менее популярна замена пин-кода на идентификацию по лицу в банковской сфере. На презентации нового логотипа и экосистемы в 2020 г. Сбербанк представил гаджеты и платформы, на которых будет основана технологическая составляющая банка. Среди новинок оказался банкомат, для которого не нужны карточки. Банкоматы смогут идентифицировать клиента по лицу, а также будут понимать голосовые команды. Идентификация по лицу без карты применялась в банкоматах Сбербанка с 2017 г., но имела определенные ограничения, которые будут упразднены при переходе к новым аппаратам (можно было произвести только платеж или перевод). А возможность «Оплаты

одним взглядом» была запущена в Москве в сети кофеен в июле 2020 г. После активации режима «Оплата одним взглядом» в приложение или отделение Сбербанка достаточно сообщить на кассе о желании оплатить заказ лицом.

Системы идентификации по лицу используются и в аэропортах. Так международный аэропорт Гонконга применяет новые биометрические технологии для более быстрого и беспрепятственного взаимодействия с пассажирами в аэропорту. Пассажиру с единым удостоверением личности достаточно однажды предъявить проездной документ, после этого его лицо становится «паспортом». Биометрическая система идентификации пассажиров, получившая название SmartGate, была развернута в Австралии. SmartGate – это автоматическая система, дающая пассажирам, прибывающим в международные аэропорты Австралии, возможность самостоятельного прохождения паспортного контроля без участия сотрудников аэропорта, она использует данные биометрического паспорта и технологии распознавания лиц для выполнения таможенных и иммиграционных проверок, которые обычно проводятся офицерами пограничной службы. К концу 2023 г. биометрическая идентификация по лицу при прохождении предполетных процедур должна появиться и в 6% российских аэропортов, т.е. по меньшей мере в 12. Все более широкое применение распознавания лиц приводит к расширению баз данных лиц и увеличению количества следящих камер. Помимо удобства в использование биоидентификация создает ряд потенциальных угроз, среди которых и утечки баз данных, и тотальный цифровой контроль, и утрата цифровой личности.

В цифровой среде сохранить за собой собственность на лицо оказывается все более сложно. Как любая информация, попавшая в сеть, фотографии могут быть скопированы и сохранены любым пользователем. Что, конечно, еще не похищение лица с точки зрения цифрового мира. Присвоить здесь скорее означает не просто иметь, а использовать в собственных целях. И именно это стало возможно с появлением технологии машинного обучения «face swap» (для «deep fake»), позволяющих заменять лица на видео [10]. Надо сказать, что сегодня фото и видео все еще являются достаточно сильными доказательствами истинности чего-либо. И если доверие фотографиям все больше подрывается фильтрами, программами для обработки фотографий и многочленными шуточными и арт-фоторабоотами в сети, то видео до последнего времени являлось бесспорным доказательством. Действительно,

для качественного изменения видео-контента были необходимы профессиональные программы, специальное образование и большой опыт. Сегодня нейросети прекрасно справляются с разнообразными способами обработки видео. Для замены лиц были разработаны несколько альтернативных вариантов обучения нейросетей. Первым был студент Стэнфордского университета Ян Гудфеллоу в 2014 г. Для массового потребителя первым в 2019 г. появилось китайское приложение Zao, позволяющее изменять лица в определённых фильмах (то есть с помощью предварительно обученной на данной базе сети), в 2020 г. Doublicat от компании Neocortext, Inc предлагает для замены лица популярные GIF-анимации. На GitHub есть два варианта программное обеспечение DeepFaceLab и faceswap, позволяющие обучить нейронную сеть менять лица на любом видео. Хотя далеко не любой пользователь сможет овладеть данной технологией, тем не менее благодаря этим программам в сети существует масса измененных видео.

Таким образом, становится возможным поместить лицо на любое видео. Какие могут быть цели использования чужих лиц? Для массовых пользователей это юмор: от безобидных шуток до жестоких розыгрышей. Порноролики с измененными лицами были одним из первых применений технологии в 2017 г. (на Reddit от пользователя с ником Deepfake), и до сих пор это применение технологии крайне популярно. Понятно, что еще не потерянная вера в подлинность видео-подтверждений, может использоваться для дискредитации, черного пиара, пропаганды. Хотя разрабатываются программы для распознавания подлинности видео-контента, они недостаточно эффективны и мало доступны [5]. Так что единственной реальной защитой остается способность к критическому мышления и недоверчивость, что, по мнению К. Ваккари, Э. Чедвик, в целом усиливает неопределенность и цинизм [14].

В кинематографе цифровые копии звезд экрана стали появляться гораздо раньше, прежде всего чтобы обезопасить прибыльные проекты от потери актеров. В 2013 г. в рекламе шоколада появилась Одри Хепберн, умершая за 20 лет до этого. В мировом кино одним из самым известным примеров игры умерших актеров является фильм «Звездные войны: Скайуокер. Восход», где Леи Органа продолжала играть ушедшая Кэрри Фишер. Также вместо того чтобы переснимать «Форсажа 7» после смерти главного героя, было решено воспользоваться имеющимся материалом для воссоздания внешности Пола

Уокера. Эти вынужденные эксперименты подтолкнули режиссеров к тому, чтобы заняться «воскрешением» нарочно – в боевике «В поисках Джека» «снялась» цифровая копия актера Джеймса Дина, погибшего в 1955 г. Музей Сальвадора Дали во Флориде с помощью нейросетей создал цифровую копию художника, к которому можно обратиться, послушать истории и сделать совместное селфи. Для этого потребовалось 6000 фотографий Дали, 1000 часов машинного обучения и 145 видео с актером. Самым простым применением технологии является цифровой ведущий новостей.

Но в 2020 г. появились первые эксперименты, имеющие целью непосредственно «воскрешение» мертвых в цифровой реальности, а не использование известного образа. Возникло несколько стартапов, нацеленных на широкое распространение возможности сохранения своей цифровой копии даже без необходимости съемки со всех сторон в специальной студии. В январе 2021 г. компания Microsoft запатентовала способ цифровой реинкарнации любого человека, включающую трехмерную цифровую модель, персонализированный синтезатор голоса, а также психологию личности на основе фотографий, видео, голоса, постов в социальных сетях, писем и сообщений в мессенджерах. Таким образом, становится возможным сохранение цифрового образа человека после его физической смерти. Реальностью становятся цифровые призраки или даже цифровые зомби, как их из-за их активного поведения называет Дебра Бассет [4]. Цифровая копия лица может остаться живой памятью для последующих поколений.

А можно ли «подделать» лицо? Как уже отмечалось, сегодня изменение фотографий не представляет никаких проблем даже для непрофессионалов: помимо фильтров, входящих в стандартный набор функций смартфона, существует множество приложений, позволяющих идеализировать внешность, нанести макияж и т.п. [9]. Таким образом, использование несколько измененной внешности для цифровой презентации становится нормой [8]. Однако знание о фильтрах делает людей недоверчивыми, все знают, что фильтры используются, и сомневаются, что их сетевые собеседники на самом деле так прекрасны, как кажутся. Х. Лавренче и К. Камбре отмечают, что от нарочитых "игровых" фильтров происходит переход к тонким "натуральным" формам редактирования [7]. Хотя существуют и те, кто слишком активно пользуется разнообразными формами редактирования, создавая образы, существо-

вание которых возможно только в рамках цифрового мира. Признание условности внешности собеседников еще больше усиливает тенденцию названную О. И. Северской коммуникативным симулякром, когда собеседник воспринимается виртуальным персонажем, отражением себя [2]. Непреднамеренное использование "игровых" фильтров внешности в ходе таких серьезных онлайн мероприятий как богослужение или судебное заседание также служит усилению впечатление иллюзорности происходящего.

Вскоре сервисы стали предлагать и более кардинальные изменения внешности, например, меняя пол и возраст. Нейросети стали обучаться изменять лица и делать их принципиально отличными от оригинальной загруженной фотографии. Абсолютно новые лица сегодня создаются чаще всего с помощью обученной генеративная нейросети StyleGAN от Nvidia. Для ее работы необходимо не меньше 11 ГБ ОЗУ и несколько видеокарт. Однако рядовой пользователь может воспользоваться результатами на специальных сайтах. Например, на сайте https://thispersondoesnotexist.com/ при каждом открытии создается новое лицо. Другой сервис Anonymizer (от Generated Media) создает фотографии, похожие на загружаемые, но отличающиеся от них, и не повторяющие другие используемые для изменений фото. Никому не принадлежащее лицо может быть востребовано теми, кто, например, хочет создать где-то в сетевом пространстве профиль, не демонстрируя свое настоящее лицо.

Однако современный цифровой мир населен не только людьми, но и разнообразными нечеловеческими сущностями. Искусственный интеллект все чаще предстает перед нами в антропоморфном облике, например, как виртуальный собеседник или игровой персонаж. Он также нуждается в облике, и все чаще максимально реалистичном. Заимствование лиц, принадлежащих кому-то, может стать предметов судебного разбирательства. Так, в конце 2020 г. студентка обвинила Riot Games в незаконном использовании ее внешности для создания Seraphine, героини League of Legends [13]. Поэтому создание симулякров становится актуальной задачей для создателей виртуальных существ.

Таким образом, лицо в цифровом обществе является: 1) визуальным кодом, используемым для идентификации личности; 2) уникальной собственностью, которая может быть похищена и использована с коммерческими, компрометирующими, дискредитирующими или сексуальными целями; 3) частью уникального цифрового облика личности, существование которого мо-

жет быть продлено далеко за пределы земного; 4) объектом изменения или подделки, лицо может быть изменено для презентации в сети или вовсе быть "фейковым", не принадлежащим никому. Лицо, как неповторимость, данная от природы, в цифровом пространстве утрачивает уникальность и принадлежность, подвергается изменению, отчуждению, обособлению, снижая восприятие подлинности цифрового мира.

Л И Т Е Р А Т У Р А

1. *Евсеева Л.И., Матвеевская А.С., Тараканова Т.С.* Политическая коммуникация в условиях цифровизации // Коммуникативные стратегии информационного общества: Труды XI междунар. науч.-теор. конф. СПб: Политех-пресс, 2019.
2. *Северская О.И.* Есть контакт? О коммуникативных девиациях цифровой эпохи // Коммуникативные исследования. 2016. № 10 (4).
3. *Шипунова О.Д., Поздеева Е.Г., Евсеева Л.И.* Мультиагентный подход в анализе образовательной среды // Социология. 2020. (6).
4. *Bassett D.* Who Wants to Live Forever? Living, Dying and Grieving in Our Digital Society // Social Sciences. 2015. № 4 (4).
5. *Ciftci U.A., Demir I., Yin L.* How Do the Hearts of Deep Fakes Beat? Deep Fake Source Detection via Interpreting Residuals with Biological Signals // 2020 IEEE International Joint Conference on Biometrics (IJCB)IEEE, 2020.
6. *Floridi L.* The fourth revolution: How the infosphere is reshaping human reality. Oxford: OUP Oxford, 2014.
7. *Lavrence C., Cambre C*. Do I Look Like My Selfie?: Filters and the Digital-Forensic Gaze // Social Media + Society. 2020. No 4 (6).
8. *Leone M*. The semiotics of the face in digital dating: A research direction // Digital Age in Semiotics & Communication. 2019. No 2.
9. *Leyvand T., Cohen-Or D., Dror G., Lischinski D*. Digital face beautification // ACM SIGGRAPH 2006 Sketches on - SIGGRAPH ’06. New York, New York, USA: ACM Press, 2006.
10. *Naruniec J., Helminger L., Schroers C., Weber R.M*. High-Resolution Neural Face Swapping for Visual Effects // Computer Graphics Forum. 2020. No 4 (39).

11. *Nasution M.I.P., Nurbaiti N., Nurlaila N., Rahma T.I.F., Kamilah K*. Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic // 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)IEEE, 2020.
12. *Rubtsova A. V., Krylova E.A., Smolskaia N.B., Odinokaya M.A*. Polycultural Linguistic Personality Formation In A Digital Educational Environment Of A University // Dialogue of Cultures - Culture of Dialogue: from Conflicting to Understanding. European Proceedings Of Social And Behavioural Sciences. London: European Publisher, 2020.
13. *Stephanie* The Problem With Seraphine [Электронный ресурс]. URL: https://step-nie.medium.com/the-problem-with-seraphine-58dc16c07e79 (дата обращения: 25.02.2021).
14. *Vaccari C., Chadwick A.* Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News // Social Media + Society. 2020. No 1 (6).
15. *Xylander C. von* A(l)gora: the Mindscape // Technology and Language. 2020. No 1 (1). P. 115–125. https://doi.org/10.48417/technolang.

R E F E R E N C E S

1. *Evseeva L.I., Matveevskaya A.S., Tarakanova T.S*. Political communication in the context of digitalization // Communication strategies of the information society: Proceedings of the XI Intern. scientific-theoretical conference. SPb: Polytech-press, 2019.
2. *Severskaya O.I*. Have a contact? About communicative deviations of the digital age // Communication research. 2016. No. 10 (4).
3. *Shipunova O.D., Pozdeeva E.G., Evseeva L.I*. Multiagent approach in the analysis of the educational environment // Sociology. 2020. (6).
4. *Bassett D*. Who Wants to Live Forever? Living, Dying and Grieving in Our Digital Society // Social Sciences. 2015. No. 4 (4).
5. *Ciftci U.A., Demir I., Yin L*. How Do the Hearts of Deep Fakes Beat? Deep Fake Source Detection via Interpreting Residuals with Biological Signals // 2020 IEEE International Joint Conference on Biometrics (IJCB) IEEE, 2020.

6. *Floridi L.* The fourth revolution: How the infosphere is reshaping human reality. Oxford: OUP Oxford, 2014.
7. *Lavrence C., Cambre C*. Do I Look Like My Selfie?: Filters and the Digital-Forensic Gaze // Social Media + Society. 2020.No 4 (6).
8. *Leone M.* The semiotics of the face in digital dating: A research direction // Digital Age in Semiotics & Communication. 2019.No 2.
9. *Leyvand T., Cohen-Or D., Dror G., Lischinski D*. Digital face beautification // ACM SIGGRAPH 2006 Sketches on SIGGRAPH '06. New York, New York, USA: ACM Press, 2006.
10. *Naruniec J., Helminger L., Schroers C., Weber R. M*. High-Resolution Neural Face Swapping for Visual Effects // Computer Graphics Forum. 2020.No 4 (39).
11. *Nasution M.I.P., Nurbaiti N., Nurlaila N., Rahma T.I.F., Kamilah K*. Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic // 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE) IEEE, 2020.
12. *Rubtsova A. V., Krylova E.A., Smolskaia N.B., Odinokaya M.A*. Polycultural Linguistic Personality Formation In A Digital Educational Environment Of A University // Dialogue of Cultures - Culture of Dialogue: from Conflicting to Understanding. European Proceedings Of Social And Behavioral Sciences. London: European Publisher, 2020.
13. *Stephanie* The Problem With Seraphine [Electronic resource]. URL: https://step-nie.medium.com/the-problem-with-seraphine-58dc16c07e79 (date accessed: 25.02.2021).
14. *Vaccari C., Chadwick A*. Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News // Social Media + Society. 2020.No 1 (6).
15. *Xylander C. von* A (l) gora: the Mindscape // Technology and Language. 2020.No 1 (1). P. 115-125. https://doi.org/10.48417/technolang.

1 марта 2021 г.