Modern Technologies Law, 2023, 4(8) https://www.mtlj.usc.ac.ir

Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/mtlj.2023.382577.1160

Legal Challenges of Biometric Identity Systems in Law Enforcement of Recognition Policy (Voice): A Case Study of Siip in Europe

Sima Hatami[1], Fatollah Rahimi[2*], Ehsan Agha Mohammad Aghaei[3], Esmaeil Shahsavandi[4]

[1] PhD Candidate in Public International Law, Azad University, North Tehran Branch, Tehran, Iran

[2] Assistant Professor of Law, Azad University, North Tehran Branch, Tehran, Iran

[3] Assistant Professor, of Law, Islamic Azad University, North Tehran Branch, Tehran, Iran

[4] Assistant Professor of Law, Azad University, North Tehran Branch, Tehran, Iran

Article Info

Original Article

Received:
21-1-2023
Accepted:
17-04-2023

Keywords:
Voice Identification
Biometric
Identity
Recognition policy

Abstract

Today, voice Identification technology is developing as one of the modern techniques, which has a unique application in identifying the identity of people in the form of recorded voice. This method can be used in courts and tribunals, not only to convict people but also as a definite proof to prove the innocence of accused persons. In this approach, "identity recognition" is tested through face painting and the sound vibration diagram method of human voices. The uniqueness of the human voice is a great help for law enforcement in identifying criminals, especially in the field of emerging new crimes with technology. Ultra-modern, such as cyber terrorism, which threatens to bomb aeroplanes, government buildings, etc., or over the phone with the intention of extortion in the kidnapping. Biometric identity systems are currently a prominent feature of contemporary law enforcement in Europe, as the focus on time-consuming biometric data collection, such as fingerprinting and facial recognition, raises concerns about the impact of these technologies on surveillance. For judicial officers from the perspective of fundamental human rights. In particular, this paper examines the recent European project, the Integrated System for Voice Speaker Identification (SIIP), as a new Europe-wide initiative to create the first international voice biometric database, now the third largest biometric database in the world as used by Interpol.

***Corresponding author**
e-mail: rahimif_law@yahoo.com

How to Cite:
Hatami, S., Rahimi, F., Agha Mohammad Aghaei, E, & Shahsavandi, E. (2023). Legal Challenges of Biometric Identity Systems in Law Enforcement of Recognition Policy (Voice): A Case Study of Siip in Europe. *Modern Technologies Law*, *4*(8), 101-118.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

حقوق فناوری‌های نوین، ۱٤۰۲، ٤(۸) https://www.mtlj.usc.ac.ir

حقوق فناوری های نوین

http://doi.org/10.22133/mtlj.2023.382577.1160

چالش‌های حقوقی سیستم‌های هویت بیومتریک در اجرای قانون و سیاست تشخیص (صدا)، مطالعهٔ موردی: پروژهٔ سیپ در اروپا

سیما حاتمی[۱]، فتح‌الله رحیمی[۲*]، احسان آقامحمدآقایی[۳]، اسماعیل شاهسوندی[۴]

[۱] پژوهشگر دکتری حقوق بین‌الملل عمومی دانشگاه آزاد اسلامی واحد تهران شمال،تهران، ایران

[۲] استادیار گروه حقوق دانشگاه آزاد اسلامی واحد تهران شمال، تهران، ایران

[۳] استادیار گروه حقوق دانشگاه آزاد اسلامی واحد تهران شمال، تهران، ایران

[۴] استادیار گروه حقوق دانشگاه آزاد اسلامی واحد تهران شمال، تهران، ایران

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۱۱/۱

تاریخ پذیرش:
۱۴۰۲/۰۱/۲۸

واژگان کلیدی:
شناسایی صدا
بیومتریک
هویت
سیاست تشخیص

چکیده

امروزه صداشناسی، که در تشـخیص هویـت اشـخاص کاربردی بی‌همتا دارد، به‌منزلهٔ یکـی از روش‌هاش مـدرن درحـال پیشـرفت است. از این روش، به‌منزلهٔ ادلهٔ ابزاری مستند و مستدل در محاکم، نفیاً یا اثباتاً استفاده می‌شود. در رویکرد «تشخیص هویـت» با صـورت‌نگـاری و ترسـیم نمـودار ارتعاشـات صـوتی اصوات انسانی آزمـایش می‌شوند. منحصربه‌فردبودن صدای انسان در زمینهٔ تشخیص مجرمان جرایم نوظهور ازطریق فنّاوری‌های فوق نوین، مانند تروریسم سایبر، تهدید به بمب‌گـذاری در هواپیماهـا و ابنیهٔ دولتـی با تلفن به قصـد اخـاذی و آدم‌ربایی کمـک بزرگـی است. درحال حاضر، سیستم‌های هویت بیومتریک یکی از طرق اجرای قانون در اروپاست. توجه به جمع‌آوری داده‌های بیومتریک در مقایسه با روش‌های وقت‌گیر، مانند انگشت‌نگاری و تشخیص چهره، نگرانی‌هایی را دربارهٔ تأثیر این قبیل فنّاوری‌ها در حوزهٔ تجسس و تفحص برای ضابطان قضایی از منظر حقوق اساسی بشر به وجود آورده است. پژوهش حاضر، چالش‌های حقوقی پروژهٔ اخیر اروپا با عنوان «سیستم یکپارچهٔ شناسایی سخن‌گوی صوتی (سیپ)» را، که به‌منزلهٔ ابتکاری نوین برای راه‌اندازی اولین پایگاه دادهٔ بین‌المللی بیومتریک صوتی به‌کار می‌رود، بررسی می‌کند.

***نویسندهٔ مسئول**

رایانامه: rahimif_law@yahoo.com

نحوهٔ استناددهی:

حاتمی، سیما، رحیمی، فتح‌الله، آقا محمد آقایی، احسان، شاهسوندی، اسماعیل (۱۴۰۲). چالش‌های حقوقی سیستم‌های هویت بیومتریک در اجرای قانون و سیاست تشخیص (صدا)، مطالعهٔ موردی: پروژهٔ سیپ در اروپا. *حقوق فناوری‌های نوین*، ۴ (۸)، ۱۰۱-۱۱۸.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir

شاپای الکترونیکی: ۳۸۳٦-۲۷۸۳

مقدمه

فنّاوری نوین بیومتریک[1] به‌سرعت به یکی از ویژگی‌های اصلی حاکمیت[2] معاصر تبدیل می‌شود. سیر روند تکاملی در سیستم‌های تشخیص هویت، مانند معرفی اشخاص با استفاده از نام و نام‌خانوادگی، کد شناسایی شهروندی، ثبت کد مالیاتی، ادغام داده‌های بیومتریک در اسناد هویتی، مانند گذرنامه‌ها را با استفاده از اثر انگشت و دی‌ان‌ای در تحقیقات پلیسی درپی دارد. این نوع سیستم اطلاعات برای طیف وسیعی از عوامل دولتی و غیردولتی قابلیت خوانش دارد (Scott, 1998; Van der Ploeg, 1999) و با اشکال جدیدتری از فنّاوری‌های بیومتریک تکمیل می‌شود که با استفاده از نمایش‌های دیجیتالی و بخش‌های منحصربه‌فرد بدن انسان همچون چهره «در مکان و زمان واقعی»،[3] هویت‌های واحدی را دسته‌بندی و ایجاد می‌کند (Edri, 2020). بااین‌حال، سیستم‌های تشخیص صدا کمتر شناخته‌شده‌اند. پروژهٔ یکپارچهٔ شناسایی صدا (سیپ)[4] در اروپا، نمونهٔ بارز این نوع توسعه است. اکنون این پایگاه داده ـ که در سال ۲۰۱۴ با هدف راه‌اندازی اولین پایگاه بین‌المللی با قابلیت کارکرد بیومتریک صوتی راه‌اندازی شد ـ سومین پایگاه دادهٔ بیومتریک بزرگ در اینترپل پس از اثر انگشت‌نگاری و چهره‌نگاری است (Kofman, 2018).

احراز هویت بیومتریک فرایندی امنیتی است که مشخصات فرد را با مجموعه‌ای از داده‌های بیومتریک ذخیره‌شده قیاس و تطبیق داده و درصورت تأیید، اجازهٔ دسترسی به سامانه‌های هدف را می‌دهد. ظهور سیستم‌های هویت بیومتریک همواره محل مناقشه بوده است. تحقیقات بسیاری درخصوص ارزیابی عملکرد سیستم‌های تشخیص چهره، به‌ویژه در اقلیت‌های جنسیتی، زنان سیاه‌پوست، سالمندان، افراد کم‌توان و کارگران مهاجر انجام شده است (Buolamwini & Gebru, 2018) که بیم تبعیض و چالش‌های حقوق بشری را سبب می‌شود (Kak, 2020). استفاده از این فنّاوری، پیامدهای متفاوتی به همراه داشته است که بررسی هویت جوامع خاصی را شامل می‌شود، جوامعی که پیش‌تر تحت نظارت پلیس به‌طرزی افراط‌گونه قرار داشتند (Watch. B. B, 2018). دراین‌میان، آزادی‌های مدنی، همچون حق حریم خصوصی، حق آزادی تشکل و اجتماع و حق عدم تبعیض مطرح می‌شود. چارچوب‌های نظارتی برای کنترل فنّاوری‌های مذکور در اروپا، مقررات حفاظت از داده‌های عمومی اروپا[5] و دستورالعمل قانونی درخصوص پایگاه‌های داده را شامل می‌شوند و برای جمع‌آوری داده‌های بیومتریک[6] شهروندان اروپایی ازطریق سیستم‌های هویت عمل می‌کنند. دراین‌میان، به‌ویژه در ایالات متحده و بریتانیا، چندین کمپین با پردازش اطلاعات موصوف مخالفت کرده‌اند (Kindt, 2020) و خواستار توقف کامل و ممنوعیت استفاده از فنّاوری مذکور در مکان‌های عمومی شده‌اند (Kind, 2019).

چالش‌های موجود ناظر به نقشی هستند که این قبیل فنّاوری‌ها، در شکل‌دهی فرصت‌ها برای افراد و گروه‌های مختلف جامعه ایفا می‌کنند. پردازش بسیاری از داده‌های بیومتریک به‌منزلهٔ بازتعریف مفهوم «شناسایی فنّاوری در جامعه» است. سیستم‌های الگوریتمی ترتیبات «اخلاقی ـ سیاسی»[7] هستند و باید در تغییر وضعیت و شرایط خاصِ رؤیت و دسترس‌پذیربودن بررسی شوند (Amoor, 2020). فنّاوری‌های بیومتریک سیستم‌های تأیید تشخیص را با فعال‌کردن اتصالات گوناگون قابل جست‌وجو ـ ازجمله ویدیوهای یوتیوب[8]، مکالمه‌های تلفنی یا پایگاه‌های دادهٔ پلیسی ـ فراهم می‌آورند. در سطح جهانی، استفاده از فنّاوری‌های بیومتریک سیاست شناسایی خاصی را درپی دارد که پیامدهای آن، موقعیت افراد در جامعه را رقم می‌زند. بنابراین، بررسی رژیم حقوقی خاص با رویکرد نظارت پسینی در اروپا مدنظر قرار دارد؛ گرچه برخی نظام‌های حقوقی ممکن است «نظارت پیشینی»، از اخذ مجوز گرفته تا رعایت مواد قانونی و ضوابط قاعده‌محور، را تجویز کنند.

---

1. Biometric Technologies
2. Contemporary Governance
3. ‘in the Wild’ and in ‘Real-Time’.
4. Speaker Identification Integrated Project (SIPP)
5. European General Data Protection Regulation
6. Biometric Identity Systems
7. Politics of Recognition
8. Youtube Video

در این پژوهش، شرایط تشخیص در سیستم‌های هویت بیومتریک با تمرکز بر ویژگی‌های فنی جدید سیستم شناسایی صدا[1] بررسی می‌شود. تمرکز پژوهش حاضر، بر تحقیق و توسعهٔ فنّاوری «سیپ» است تا این مسئله را به بوتهٔ نقد گذارد و متعاقب آن، به این پرسش پاسخ دهد که نقش صدا در تشخیص هویت افراد با چه نوع چالش‌های حقوقی مواجه است؟

دربارهٔ نقش صدا در سیستم‌های هویت بیومتریک به‌طور بایسته پژوهشی انجام نشده است. همچنین مباحث مربوط به استفاده از داده‌های بیومتریک ازطریق ضابطان قانونی و قضایی، به‌شدت درحال گمانه‌زنی است و البته ماهیت واقعی و شیوه‌های نظارت[2] مبتنی‌بر داده در این قرائت حائز اهمیت است (Brayne & Christin, 2021). از این حیث، تمرکز بر صدا، به‌منزلهٔ سیاست تشخیصی در سیستم‌های هویت بیومتریک، با هدف ارتباط صدا با رخدادهای عالم واقع، عینی و مناسب فرض می‌شود (Couldry, 2010).

درحالی‌که برداشت‌ها از سیاست تشخیص در رابطهٔ فنّاوری سیپ مبتنی‌بر سیستم‌های هویت بیومتریک است، اما برخی ویژگی‌های مربوط به نقش و ماهیت صدا در این سیستم حائز اهمیت است. از منظر حقوق و آزادی‌های بنیادین بشر، ازجمله حقوق مدنی و سیاسی مانند آزادی اطلاعات، باید دید که چگونه صدا به فنّاوری تشخیص و شناسایی ماهیت انسانی بدل می‌شود. براین‌اساس، اشکال تشخیص هویت، نفیاً یا اثباتاً بررسی می‌شوند. همچنین، قدرت و پویایی پیشرفت فنّاوری‌های بیومتریک در اجرای قانون تبیین می‌شود و ارتباط آن در تحقق «عدالت داده‌ها»،[3] که به چالش‌های عدیده انجامیده، تعیین می‌شود (Dencik et al., 2016; Taylor, 2017). استفادهٔ روزافزون از سیستم‌های هویت صوتی در اجرای قانون، مبارزات جدیدی را بر سر به‌رسمیت‌شناختن آن به ذهن متبادر می‌کند که به اطلاع‌رسانی ویژه دربارهٔ مسئلهٔ «عدالت داده» نیازمند است (Abdelwhab &Viriri, 2018; Dantcheva et al., 2015; Kak, 2020).

چالش حقوقی سیستم تشخیص صدا برای اجرای قانون

«تنها صداست که می‌ماند»[4] (Kroemer & Kittel, 1980). فنّاوری نوین سیپ، راه‌حلی پیش‌رو برای شناسایی مشکوک است که موتور جدید تشخیص هویت به نام (SID)[5] مبتنی است که چندین الگوریتم تحلیلی گفتار (مانند تشخیص صدا، جنسیت/ سن/ زبان/ لهجه، تکیه کلام و تکرار کلمهٔ کلیدی، طبقه‌بندی و تشخیص شبیه‌سازی صدا) را با هم ترکیب می‌کند (Khelif et al., 2018). سیاست ترکیبی تشخیص هویت با افزایش دقت تشخیص همراه است. این فنّاوری برای ردیابی شبکه‌های مشکوک ترور و جنایت، بسترسازی ایده‌آلی را رقم می‌زند؛ به‌ویژه هنگامی که افراد از برنامه‌های مبتنی‌بر اینترنت،[6] تلفن‌های ابری یا رسانه‌های اجتماعی، برای برنامه‌ریزی یک جنایت یا حملهٔ تروریستی استفاده می‌کنند. نتایج حاصل از فنّاوری سیپ به‌راحتی با مرکز اشتراک‌گذاری اطلاعات پایدار،[7] واقع در اینترپل[8]، به‌اشتراک گذاشته می‌شود. مرکز اشتراک‌گذاری اطلاعات پایدار افزایش ضریب اطمینان‌بخشی از نتایج حاصل از شناسایی و تشخیص را ازطریق فنّاوری‌های فوق‌پیشرفته و نمونه‌های صوتی موجود در پایگاه عظیم داده‌های جمع‌آوری‌شده از ۱۹۰ عضو اینترپل، که مبتنی‌بر روش‌های استاندارد عملیات/ حریم خصوصی داده‌هاست، تضمین می‌کند (Fieke et al., 2021).

فنّاوری سیپ اشتراک‌گذاری اطلاعات و همکاری مؤثر در جامعهٔ مشترک آنتن بزرگ اروپایی[9] را به چند برابر افزایش می‌دهد. استفاده از این فنّاوری در اروپا، نه‌فقط شناسایی فردی، بلکه احراز هویت قطعی افراد را سرعت می‌بخشد. فنّاوری سیپ در همهٔ منابع گفتاری (اینترنت،

1. Speaker Identification Integrated Project
2. Actual Nature and Practices of Data-based Surveillance
3. Data Justice

٤. نک: فروغ فرخزاد، *ایمان بیاوریم به آغاز فصل سرد*. «تنها صداست که می‌ماند». مجموعهٔ شعر امروز ایران. تهران: انتشارات مروارید. ۱۳۵۲.

5. Speaker-Identification
6. Voice Over Internet Protocol)VOIP(
7. SIIP Info Sharing Center (SISC)
8. INTERPOL

۹. Large European Antenna (LEA)؛ نک. اعلامیهٔ اروپا درخصوص جامعهٔ آنتن بزرگ اروپا. این برنامه ازطریق کمیسیون اروپا و در راستای تحقق اهداف برنامهٔ ۲۰۲۰ اروپا سازمان‌دهی و حمایت مالی می‌شود.

شبکه‌های مخابراتی عمومی،[1] شبکهٔ سلولار (تلفن همراه) و ماهوارهٔ ساتکام[2]) اجرا می‌شود و از آخرین برنامه‌های داده‌کاوی هوش باز[3]برای به‌دست‌آوردن نمونه‌های صوتی استفاده می‌کند. کنسرسیوم سیپ در اروپا از هفده شریک تشکیل شده که کاربران نهایی خود را، اعم از بنگاه‌های کوچک و متوسط،[4] شرکای صنعتی و دانشگاهی در زمینه‌های گوناگون، ازجمله تجزیه‌وتحلیل گفتار، تجزیه‌وتحلیل رسانه‌های اجتماعی و ادغام آنان، گردهم می‌آورد. برای اثربخشی هرچه بهتر فنّاوری سیپ، پروژهٔ نهایی سیپ با همکاری نهادهایی مانند اینترپل و نیروهای پلیس در بریتانیا و پرتغال طراحی، توسعه و آزمایش خواهد شد.[5]

گسترش روزافزون صنعت بیومتریک صدا برای مقاصد نظامی و غیرنظامی، ازجمله پایلوت‌های تشخیص چهره در مکان‌های عمومی، ایستگاه‌ها و فرودگاه‌ها در سراسر اروپا، نشان می‌دهد که استفاده از ویژگی‌های بدن انسانی مانند صورت، عنبیه یا شبکیهٔ چشم برای اغلب دولت‌ها امری رایج است (Fussey & Murray, 2019; Marciano, 2019). هویت یکی از ابزارهای حکمرانی و یکی از اجزای اصلی ظهور دولت‌داری مدرن است (Scott, 1998). بی‌تردید تبدیل دولت به دولت تنظیم‌گر[6] یا حکمران تنظیم‌گر به‌جای دولت‌های رفاه و پلیس در سده‌های قبلی، اهمیت روش‌های نظارت و کنترل را به شیوهٔ تنظیم‌گری نمایان می‌کند (هداوند و جم، ۱۴۰۰). رژیم تنظیم‌گری متشکل از استانداردها، قواعد و سازوکارهای پایش و بازخورد و اجرای این قواعد است و به‌زعم آلفونس بورا[7] (2017) تنظیم‌گری جامعه‌گرا عبارت است از هرنوع عملکرد سیستم اجتماعی که قاصدانه درپی تصمیم‌گیری و تبیین سیستم هدف و به قصد حصول خیر مشترک[8] جوامع و منفعت عموم[9] است (هداوند و جم، ۱۴۰۰). این امر، به دولت‌های اروپایی پیشرو[10]اجازه می‌دهد که اقدامات آگاهانه‌تری را برای خیر عموم و پیشبرد اهداف خاص مانند فرارهای مالیاتی[11] و امنیت داخلی[12] خود انجام دهند. از زمان تأسیس این جامعهٔ پیش‌رو، سیستم‌های هویتی تکامل‌یافته‌تر و پیچیده‌تر شده‌اند تا با افزایش جابه‌جایی تجارت جهانی کالاها و خدمات و ایمن‌سازی سیاست امنیت انسانی پس از پایان جنگ سرد[13] هماهنگی داشته باشند. بنابراین، سیستم‌های تشخیص هویت و ابزارهای حکومتی مهم به‌منظور نظارت بر ورود و خروج افراد به سرزمین‌های مستقل و نحوهٔ رفتار افراد در داخل قلمرو کشور است. تعابیری مانند «حکمرانی بر هویت»[14] از مفاهیم نوظهوری هستند که به‌موجب آن‌ها وضعیت مشروع در جامعه، دسترسی به خدمات اساسی، فضای عمومی و خصوصی به‌طور فزاینده‌ای با توانایی تولید و تأیید هویت شخصی مرتبط است (Gates, 2011; Lyon, 2008). ازاین‌نظر، سیستم‌های تشخیص «هویت» وسیله‌ای حیاتی هستند که ازطریق آن‌ها، دولت‌ها به‌طور مؤثر در امور دولتی، کنترل مرزها، تحقیقات پلیسی و ادارهٔ خدمات عمومی مشارکت می‌کنند (Van Zoonen, 2013).

انقلاب بیومتریک در قرن اخیر و اشاعهٔ تفکر حکمرانی ازطریق هویت، از تمایل دولت‌ها به پیوندزدن هویت واحد و باثبات به یک شخص نشأت می‌گیرد (Leese, 2022). فرض غالب آن است که استفاده از نمایشی دیجیتالی متشکل از اثر انگشت، صورت یا چهره همراه با صدا، امکان خلق هویتی واحد و تشخیص‌پذیر و البته یکپارچه را به‌طور مطمئن محقق می‌دارد که در طول زمان مترصد تغییر نمی‌شود و نسبت به سایر اشکال شناسایی، کمتر در معرض سوءاستفاده قرار می‌گیرد (Gates , 2011, p. 14). بنابراین، سیستم‌های تشخیص هویت از مرحلهٔ تخصیص

1. Public Switched Telephone Network (PSTN)
2. SATCOM Satellite
3. Open-Source Intelligence (OSINT)
4. Small and Medium-Sized Enterprises (SME)
5. https://cordis.europa.eu/project/id/607784
6. Regulatory State
7. Alfonse Bora
8. Common Good
9. Common Utility
10. The Early European Nation States
11. Tax Evasion
12. Internal Security
13. Cold War
14. ‘Governing by Identity’

صرف یک شمارهٔ شناسایی به افراد، به سازمان‌دهی عظیم، نظام‌مند و پیچیده حول ویژگی‌های خاص بدن انسان بدل شده‌اند (Kak, 2020؛ Van Zoonen, 2013).

از نگاه مجریان قانون،[1] این سیستم‌ها از منظر تاریخی در تحقیقات پلیس نقش محوری داشته‌اند. از دیرباز به این موضوع ـ هم از نظر شناسایی آثار باقی‌مانده در صحنهٔ جرم و هم از نظر ساختارهای هنجاری که مجرم کیست و جرم چیست ـ توجه شده است؛ به‌طوری که ارتباط موضوع با فقرا، کارگران مهاجر و جوامع سیاه به‌منزلهٔ اولویت‌های خاص جرم و جنایت، در بررسی‌های تجسس‌محور پلیس تحلیل شده است. تلاقی میان نژاد، طبقه و جرم در تحقیقات انجام‌شده، درحکم مفروض اصلی، حاکی از آن است که مجری قانون از سیستم‌های تشخیص هویت بهره می‌گیرد تا به‌طور مؤکد از قدرت و اقتدار خود در انتساب دسته‌هایی از جرم[2] به افراد[3] یا جرم‌انگاری برای جوامع و گروه‌های خاص استفاده کند (Williams & Clarke, 2016). بنابراین، این شیوهٔ انتساب جرم در سیستم‌های جدید، محل مناقشه است. استفاده از فنّاوری‌های بیومتریک جدید در اجرای قانون، دچار انحراف و عدول در مسیر و هدف مشروع شده است؛ برای مثال در بریتانیا، پلیس استفاده از تشخیص چهرهٔ زنده[4] را برای نظارت بر محافل خرید، رویدادها و اعتراض‌ها بررسی می‌کند (Watch. B. B, 2018; Liberty, 2020) و یا در ایالات متحده، مقرر است اطلاعات نیمی از جمعیت کشور در پایگاه‌های اطلاعاتی تشخیص چهره ازطریق مجریان قانون ضبط و نگه‌داری شود. رواج چنین کاربردهایی در تشخیص هویت نشان‌دهندهٔ آن است که حساسیت نظارتی بر جمعیت‌های خاص و محیط‌های خاص جرم‌زا در شرف شکل‌گیری است که به نوبهٔ خود، انگیزه‌های تبعیض‌نژادی را به ذهن متبادر می‌کند (Valentino-DeVries, 2020).

درحالی‌که بزرگ‌ترین پایگاه داده‌های بیومتریک شناخته‌شده در جهان، براساس اثر انگشت[5] و الگوهای چهره[6] هستند، تحقیقات کمتری درمورد استفاده از خصیصهٔ «صدای آدمی» به‌منزلهٔ ویژگی بیومتریک در ساخت سیستم‌های پیچیدهٔ فنّاورمحور در مقیاس کلان انجام شده است.(Algere,Soldi&Evans, 2014) پیشرفت‌های موجود در فنّاوری‌های شناسایی صدا و سخن‌گو به دههٔ ۱۹۵۰ بازمی‌گردد که با هدف حمایت از آژانس‌های امنیتی و تحقیقات پزشکی قانونی[7] انجام شد و شامل ترکیبی از دستگاه‌های الکترونیکی و کارشناسان آموزش‌دیده بود که می‌توانست خروجی این دستگاه‌ها برای فاش‌کردن هویت افراد را تجزیه و تحلیل کند (Pollack, 1954). در دههٔ ۱۹۹۰، اولین سیستم‌های صوتی خودکار برای شناسایی افراد در دسترس قرار گرفت که هم‌اکنون نیز برای شناسایی هویت کاربر و کلید کنترل دسترسی، تبدیل متن به گفتار و گفتار به متن استفاده می‌شود (Abramowitz et al., 2011; Rashid et al., 2008). اخیراً توجه به «صدا» به‌منزلهٔ فنّاوری بیومتریک برای ارتباط با سایر سیستم‌ها و خدمات آنلاین، فرصت‌های جدیدی را برای جمع‌آوری اطلاعات و داده‌ها به‌ویژه در تشخیص هویت فراهم کرده است (Turow, 2021). درحال حاضر، ارتقای سیستم‌های تشخیص صدا در حوزهٔ کار مجریان قانونی ازجمله ضابطان قضایی رایج شده است. براساس نظرسنجی که اینترپل در سال ۲۰۱۶ انجام داد، ٤٤ سازمان مجری قانون در سراسر جهان، که نیمی از آن‌ها در اروپا مستقرند، دارای قابلیت شناسایی سخن‌گو یا گوینده‌اند که ازطریق پایگاه‌های دادهٔ صوتی، گویندگان را به‌طور خودکار یا تحت نظارت انسانی شناسایی می‌کنند (Morrison et al., 2016).

موانع و محدودیت‌های به‌کارگیری سیستم‌های شناسایی و فنّاوری هویت بیومتریک

تحول دیجیتال در دنیای امروز اجتناب‌ناپذیر است، تحولی که تمامی جوامع انسانی را در سراسر جهان دربر گرفته است. ایجاد «هویت» ازطریق فنّاوری‌های تشخیص مبتنی‌بر فنّاوری بیومتریک با نحوهٔ تشکیل «هویت» صرف متفاوت است (Burke & Stets, 2009, p. 3). به‌نظر می‌رسد

1. Law Enforcement
2. Criminality
3. Criminalize Specific Individuals
4. Live
5. Fingerprints
6. Face
7. Forensic Investigation

هویت[1] به‌منزلهٔ مجموعه‌ای از مفاهیم تعریف می‌شود که فرد با تصاحب نقشی خاص در جامعه، در مقام عضوی از گروهی خاص، آن را ادعا می‌کند و نیز ویژگی‌های خاصی را به‌مثابهٔ «شخصیت» تبیین می‌کند. باید اشاره کرد که هویت‌های انسانی ثابت نیستند؛ بلکه به‌طور پیوسته به‌دست افراد مختلف خلق می‌شوند و حتی با قبول نقش‌های مجدد و متنوع در جامعهٔ انسانی تغییر می‌یابند. تغییر مذکور از آن روی است که فرد با قبول نقش‌های متعدد در جامعه، هویت جدید برگزیند و با آن سازگار شود. توانایی، تمتع و تشکیل هویت اغلب برای افراد در ارتباط با یکدیگر با عضویت در اجتماع و گروه و ارتباط با محیط نمایان می‌شود (Young, 2011). در فنّاوری‌های مبتنی‌بر داده،[2] هویت به‌طور خاص، تابعی از یک «الگوریتم» است (Cheney-Lippold, 2017) و اغلب به‌صورت دیجیتالی، ازطریق پلتفرم‌ها و برنامه‌های رسانه‌های اجتماعی ساخته و ازطریق شکل‌های پروفایل مبتنی‌بر داده خلق می‌شود. کثرت هویت‌های ایجادی از این منظر برای احراز هویت ناممکن است (Haggerty & Ericson, 2000). تشکیل هویت‌های الگوریتمی، که امکان دسته‌بندی و طبقه‌بندی اجتماعی متعدد را فراهم می‌کند، اغلب خارج از آگاهی و کنترل افراد، جوامع و گروه‌ها اتفاق می‌افتد و در بعد کلان، قابلیت نظارتی پیچیده دارد (Andrejevic, 2012).

در سیستم‌های تشخیص بیومتریک، ساخت و تشکیل هویت‌ها بر روند انتساب بیومتریک نرم[3] متکی است که به استنتاج ویژگی‌های جمعیت‌شناختی، مردم‌شناسی، انسان‌شناسی و حالات عاطفی و ویژگی‌های شخصیتی از داده‌های بدنی[4] اشاره دارد (Kak, 2020, p. 6). بیومتریک، اندازه‌گیری و تجزیهٔ خصوصیات فیزیکی و رفتاری فرد است که برپایهٔ داده‌های بیومتریک یا مجموعه‌ای از ویژگی‌های فیزیکی و رفتاری همچون اثر انگشت و صدا و غیره استوار شده‌اند. هدف اصلی فنّاوری اشاره‌شده، گره‌زدن هویتی ثابت و واحد به نمایش دیجیتالی حاصل از اثر انگشت، چهره و صدا در ثبت، احراز هویت و شناسایی است و ضمن آن، استنتاج ویژگی‌های خاصی از یک ویژگی بیومتریک با هدف طبقه‌بندی مجاز افراد، مزید امعان نظر است (Gates, 2011, p. 15). بنابراین، به فنّاوری‌های تشخیص می‌توان به‌منزلهٔ تجسم هدف مفید توجه کرد (Amoore, 2019). الگوریتم‌های خودکار رژیم تشخیص را متصور و منعکس می‌کند و در بستر آن، وقایع و شخصیت‌ها را در رخدادها و رویدادها معین می‌کند (Browne, 2015). با تکیه بر مفهوم «پوستی‌سازی»[5] برای فردیت رنگین، به سیستم‌های بیومتریک جدید درحکم «پوستی‌سازی دیجیتال» اشاره می‌شود که برای انتساب معانی به اجسام خاص از نگاهی «غیرمادی» عمل می‌کنند. به‌طور خاص، فنّاوری‌های بیومتریک، که در اندیشه‌های تبعیض‌مابانه و با رجحانیت نژاد سفید[6] ریشه دارند، در طرح‌واره‌های نژادپرستانه[7] گنجانده شده‌اند که برخی افراد[8] را دچار مشکل و برخی دیگر را از مشکل بری می‌کنند. به‌زعم فرانتس فانون،[9] مفهوم درونی‌شدهٔ تحقیر[10] افراد رنگین‌پوست مانند سیاه‌پوستان، تداعی‌گر آن است که چون افراد رنگین‌پوست از حقیقت تحقیر و تبعیض خود آگاه‌اند و چنین معرفت‌شناسی نتیجهٔ نگاه خیرهٔ سفیدپوستان است، برای آنان ماهیتی ثابت مانند اشیا قائل شده و آنان را با انحراف وجودی پیوند می‌زند. بنابراین، در این قرائت قومیت‌گرایی و نژادپرستی تمایز روانی را در انواع نژادی بازتاب می‌دهد و فردیت و هویت واقعی سیاه‌پوست را زائل می‌کند. فانون بر این باور است که پوستی‌سازی نهادینه شده و سیاه‌پوستان را گونه‌ای کهتر معرفی کرده است؛ بنابراین سیاه‌پوست هرکجا می‌رود، سیاه‌پوست باقی می‌ماند (Fanon, 2008, p. 133). سیستم‌های هویت بیومتریک نیز بر مفروض شناسایی و تشخیص نژادهای خاص و تمایز آنان مبتنی‌بر اصل ثابت یعنی سفیدپوستان استوار است.

با وجوداین، فرایند استفاده از داده‌های بیومتریک برای تأیید هویت فرد به‌مثابهٔ شناسایی بیومتریک است و سیستم‌های تشخیص هویت مبتنی‌بر بازنمایی «صدا» بخشی از مجموعهٔ پیچیده‌ای از فنّاوری‌های بیومتریک هستند که شرایط خاصی را برای تشخیص افراد انسانی، درحکم

1. Identity
2. Data
3. Soft Biometric
4. Demographic Characteristics Emotional States and Personality Traits from Bodily Data
5. Fanon's Concept of 'Epidermalization'
6. Prototypical Whiteness
7. Racializing Schemas
8. Bodies
9. Frantz Fanon
10. Inferiority

امری کاملاً سیاسی[1] تعیین می‌کنند (Amoore, 2020, p. 4). سیستم‌های معنون صرفاً برای اعتباربخشی یا انتساب حقیقت به یک هویت موجود نیستند، بلکه به‌طور فعال، سیستم‌های طبقه‌بندی را در انتساب صدا به فرد تولید و نهادینه می‌کنند.(Garland, 2004) در زمینهٔ اجرای قانون، فنّاوری‌های تشخیص بیومتریک اسناد مربوط به افراد را با تأثیرپذیری در موقعیت آنان در اجتماع اشاعه داده و طبقه‌بندی هدف را مقرر می‌دارند و درمجموع، چالش‌های هویتی مبارزه بر سر طبقه‌بندی[2] را تشکیل می‌دهند (Bourdieu, 1982; 2018). تحقق این مهم، مستلزم پاسخ به این پرسش است که چه کسانی را طبقه‌بندی می‌کنیم و اصولاً چگونه افراد را طبقه‌بندی می‌کنیم. رژیم حقوقی حاکم بر سیاست تشخیصی اشاره‌شده از مناظر متعدد محل چالش است؛ زیرا شاخص و معیارهای طبقه‌بندی در هویت شناختی جوامع گوناگون از حیث نظام‌های حقوقی و الزامات قانونی و ارزش‌های موجود در جامعه و معیارهای شناختی متفاوت است (Taylor, 1994).

هرچند محققان متعددی شناسایی رژیم‌های حقوقی ناظر بر این فنّاوری را ارائه کرده‌اند (MacBride, 2013)، اما استفاده از فنّاوری‌های بیومتریک در اجرای قانون، بر بینش افراد از خود واقعی‌شان و دربارهٔ دیگران و نابرابری‌های مادی نمادین در شکل‌گیری شناخت هویتی تأثیر می‌گذارد (Herzig, 2017). پردازش الگوریتمی داده‌ها به‌منزلهٔ ابزار امتیازدهی، طبقه‌بندی و رتبه‌بندی، به انباشت اطلاعات کمک می‌کند تا موقعیت اجتماعی، فرهنگی و اقتصادی عاملی انسانی[3] را در جامعه شکل دهد (Fourcade & Healy, 2017). در این رویکرد، ارزش نهادینه برای هر فرد، صرفاً ازطریق مفاهیمی که سیستم‌های طبقه‌بندی الگوریتمی ارائه می‌دهند تفسیر می‌شود. باوجوداین، سیاست شناسایی و تشخیص هویت به‌منزلهٔ ابزار قدرت اجتماعی در به‌دست‌آوردن اقتدار[4] دولت‌ها و رفع معضل «فقد حکمرانی مبتنی‌بر هویت» به‌کار می‌رود. این امر، به‌ویژه برای سیستم‌های الگوریتمی که برای اهداف قضایی و کیفری مستقر شده‌اند، مناسب است. بنابراین، اقتدار یک نظام سیاسی مبتنی‌بر تشخیص هویت مقتدرانه، خود نشانهٔ قدرت والای دولت تنظیم‌گر است (MacBride, 2013).

شناسه‌های بیومتریک متنوع‌اند؛ ازجمله شناسه‌های فیزیکی مانند اثر انگشت، خصایص زیست‌شناختی و دی‌ان‌ای و نیز الگوهای رفتاری و پیمایشی و حتی تعاملات افراد با فنّاوری‌های آنلاین. بنابراین، در تحقق عدالت محض، ضرورت رعایت عدالت در استفاده از فنّاوری‌های تشخیص هویت و استفاده از داده‌ها حیاتی است (Couldry, 2010). همچنین «حکمرانی مبتنی‌بر هویت» در طبقه‌بندی افراد به ضرورت اخلاق نیازمند است (Van Zoonen, 2013).

بررسی سیپ در اروپا

درحالی‌که از صدا به‌منزلهٔ یکی از داده‌های بیومتریک استفاده شده است، تشخیص هویت سخن‌گو حوزهٔ نوپایی است که ازطریق پیشرفت‌های فنّاورانه و تکثیر سریع نمونه‌های صوتی، که به‌کمک پلتفرم‌های ویدیویی، رسانه‌های اجتماعی و تلفن‌های همراه مجهز به فنّاوری سیپ استخراج‌شدنی می‌شوند، به‌مثابهٔ موردی مناسب در تحقق توسعهٔ فنّاوری معرفی شده است.

ظهور فنّاوری سیپ و نظام حقوقی حاکم بر آن

همان‌گونه که هر سیستم بیومتریک از سه مؤلفهٔ سنسور و رایانه و نرم‌افزار تشکیل شده است، در پروژهٔ سیپ نیز داده‌های بیومتریک (صدا) باید ذخیره شوند. فنّاوری تشخیص هویت سیپ به‌منزلهٔ سیستم هویت بیومتریک جدید در دسترس مجریان قانونی قرار گرفته است. این فنّاوری برای رفع نیازهای مبرم سازمانی و افزایش توانایی پاسخ‌گویی به اولویت‌های امنیتی جرایم سازمان‌یافته و تروریسم ساخته شده است. سیپ، به‌منزلهٔ پروژه‌ای تحقیقاتی، ازطریق اتحادیهٔ اروپا تحت برنامهٔ امنیتی خاص[5] و با هدف راه‌اندازی اولین پایگاه بین‌المللی و تعاملی، بیومتریک صوتی برای حمایت از تحقیقات دربارهٔ تهدیدهای فراملّی، تروریسم و جرایم سازمان‌یافته تأمین شد. به‌منظور ضمانت اجراهای قانون در تشخیص

1. Fully Political
2. Struggles Over Classification
3. Agent
4. Authority
5. FP7-Security

اصوات انسانی، اینترپل در پروژهٔ توسعهٔ فنّاوری نوین صدا وارد شد. سیپ توسط کنسرسیوم بین‌المللی متشکل از نوزده عضو و کاربران نهایی، صنعت و دانشگاه از سال ۲۰۱۴ تا ۲۰۱۸ تشکیل شد. [1] این کنسرسیوم در پیشنهاد بودجهٔ خود به کمیسیون اروپا، اظهار می‌دارد که یکی از برجسته‌ترین راهکارهای کنونی در مبارزه با جرایم سازمان‌یافته و تروریسم این است که تروریست‌ها و جنایتکاران را در استفاده از هویت‌های متعدد و خودسرانه عقیم و متوقف کند (Fieke Jansen et al., 2021).

ادعای سیپ مبنی‌بر نظارت بر فعالیت مجرمانه، نشان می‌دهد که این فنّاوری نوین، شناسایی مجرمان و مظنونان تروریستی و ردیابی شبکه‌های مشکوک آتی دربارهٔ مظنونان را تسهیل می‌کند. پروژهٔ سیپ با هدف توسعهٔ «سیستم یا نظامی است که اصواتی را که از ارتباطات و رسانه‌های اجتماعی به طور قانونی رهگیری می‌شوند، شناسایی می‌کند» (Interpol, 2018b) این فنّاوری به مجریان قانون در شناسایی مظنونان تروریسم و عاملان پورنوگرافی کودکان[2] کمک می‌کند. در این فنّاوری، درصورتی که مظنونان تروریستی هنگام انجام عملی خشونت‌آمیز صورت خود را پوشانده‌اند و ردی از چهره‌شان در دوربین‌ها باقی نمانده است، به‌واسطهٔ تمییز صدا دستگیر می‌شوند. نمونه‌های صدای مظنونان ناشناس به پایگاه اطلاعاتی داده‌های ذخیره‌شده حاوی داده‌های موثق از مجرمان و تروریست‌ها، لینک و ارجاع داده می‌شوند. هنگامی که یک فرد نقاب‌دار ناشناس ویدئویی از خود را درحال انجام عملی تروریستی منتشر کند، سیستمی مانند سیپ به مجریان و ضابطان قضایی اجازه می‌دهد که مرجع صوتی ناشناختهٔ مزبور را، که از رسانه‌های اجتماعی جمع‌آوری شده، با سایر ویدئوهای رسانهٔ اجتماعی، که در دسترس عموم است، مقایسه کند. همچنین در جرایم سازمان‌یافته و استفاده از وضعیت هویت متعدد و متکثر در حالت آنلاین و آفلاین نیز به این فنّاوری اتکا می‌شود. سیپ قابلیت تشخیص افرادی که با هویت جعلی وارد کشور می‌شوند دارد. هنگامی که افسران پلیس مرزی به استفاده از هویت جعلی مشکوک می‌شوند، به‌سادگی با به‌کارگیری نمونه‌صدای مصاحبه و انطباق آن با نمونه‌های صوتی مجرمان کشف‌شده و نیز نمونه‌های صوتی ذخیره‌شده در اینترپل، مقایسه و ردیابی می‌شوند. انطباق دقیق نمودارهای ارتعاش صدا با مظنون یا مظنونان، نتیجهٔ شناسایی را قطعیت می‌بخشد (Interpol, 2018b). سیپ با استفاده از نمونه‌های صوتی در شناسایی عاملان یا قربانیان استثمار جنسی از کودکان و تطبیق صدای مجرمان ناشناس براساس شواهد ویدئویی[3] از یک پایگاه دادهٔ بزرگ‌تر موفق عمل کرده است (Fieke Jansen et al., 2021).

ویژگی‌های فنّاوری سیپ

مهم‌ترین ویژگی استفاده از بیومتریک نرم افزایش دقت تشخیص مبتنی‌بر صداست. سیپ استفاده از هفت موتور[4] مختلف را برای شناسایی مظنون ارائه می‌کند که عبارت‌اند از: تشخیص چاپ صوتی، تشخیص کلمهٔ کلیدی، تشخیص شبیه‌سازی صدا، و شناسایی سن، زبان، لهجه و جنسیت (European Commission, 2017). این مسئله به‌منزلهٔ ارتقای شایان توجه سیستم‌های شناسایی صوتی است که فقط قابلیت ترکیب دو موتور مانند «سن و زبان یا لهجه» را داشتند. نیل به توسعه و ترکیب ویژگی‌های عدیدهٔ بیومتریک نرم یکی از راه‌های حصول اطمینان بیشتر در شناسایی جنایتکاران یا تروریست‌هاست. همچنین فنّاوری سیپ نمونه‌های صوتی اعضای خانواده یا افرادی را که از تلفن مظنونان[5] استفاده می‌کنند فیلتر می‌کند و درنتیجه، تفحص و ظن بر بی‌گناهان[6] را کاهش می‌دهد (European Commission, 2017). افزایش دقت با بیومتریک نرم به ضابطان قانونی اجازه می‌دهد برخی صداها را محرز[7] و برخی دیگر را نامحرز[8] تلقی کنند؛ زیرا قطعیت یا عدم قطعیت

1.https://www.interpol.int/en/who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Speaker-Identification-Integrated-Project-SIIP
2. Perpetrators of Child Pornography
3. the Background of Confiscated Video Evidence Against a Larger Database
4. Engines
5. The Suspects' Phone
6. Innocents
7. Visible
8. Invisible

تشخیص هویت برمبنای صدا، به عواملی مانند زمان روز یا شب بودن، میزان و سطح استرس و سایر عوامل خارجی (مانند سیگارکشیدن) وابسته است.

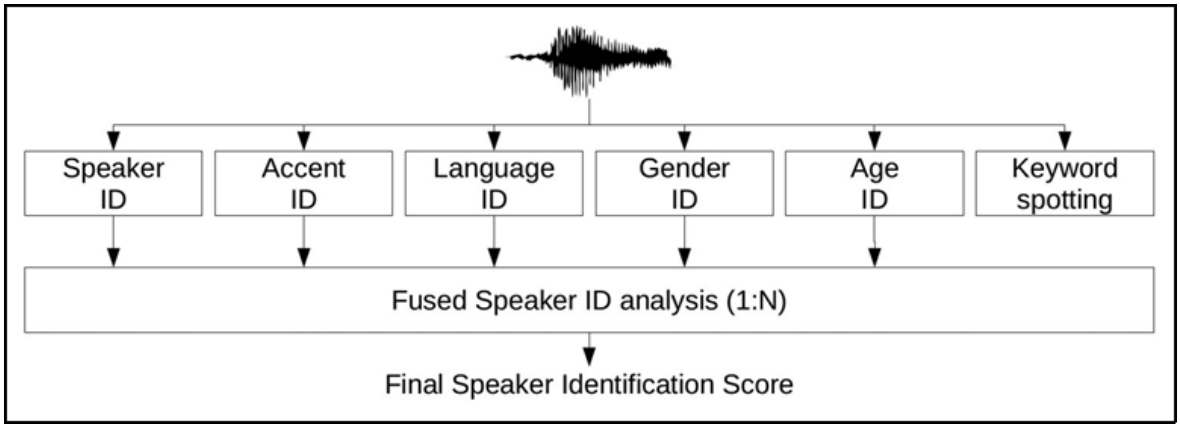
محققان بر بیومتریک نرم تأکید دارند؛ یعنی نسبت‌دادن ویژگی‌هایی مانند سن، زبان، لهجه و جنسیت به یک چاپ صوتی که براساس آن، تجزیه‌وتحلیل صدای ناشناخته و سازوکار پیش‌انتخاب برای محدودکردن مجموعه‌داده‌های جمع‌آوری‌شده از فنّاوری به‌صورت هوش منبع باز انجام می‌شود. این روش جست‌وجوی پیشرفته در منابع آزاد اطلاعات است؛ مثلاً اگر به دنبال گوینده‌ای هستید که عربی صحبت کند، مرد و بزرگ‌سال باشد و لهجهٔ رایج در عربستان سعودی را داشته باشد، می‌توانید فضای جست‌وجو را به این ویژگی‌ها محدود کنید؛ امید است که بتوان آن را محدود کرد و شاید فرصت بهتری نصیب جوینده شود تا واقعاً این ماهی نادر را در دریای بی‌کران بیابد (Interpol, 2018a).

سیستم‌های تأیید و شناسایی سخن‌گو، شامل استخراج ویژگی، مدل‌سازی گوینده، امتیازدهی، راستی‌آزمایی و تصمیم‌گیری است. ابتدا استخراج ویژگی مبتنی‌بر هدف انجام می‌شود تا سیگنال گفتاری را به‌صورت صوتی، به مجموعه‌ای از بردارهای مفروض تبدیل کند. رایانه این امر را پردازش می‌کند. بردارهای مربوط به ویژگی‌های بیومتریک برای ایجاد متن و نمایش‌های مستقل از یک شخص به نام «مدل‌های سخن‌گو» پردازش می‌شوند. دراین‌میان، هر سیستم قابل اعتماد باید مدل‌های سخن‌گوی بسیار مشابه را از نمونه‌های صوتی مختلف از یک شخص تولید کند و معمولاً چندین بردار برای هر فرد به‌وجود می‌آید که تنوع بین چند سخن‌گو را نشان دهد (Dehak et al., 2011). فنّاوری نرم‌افزاری سیپ از تکنیکی به نام بردارهای هویت[1] به‌منزلهٔ مدل‌های سخن‌گو همراه با تکنیک‌های آماری و ماشینی برای مقایسه و امتیازدادن به شباهت این مدل‌ها استفاده می‌کند (Khelif et al. 2017). مدل‌های بیومتریک نرم، به طرز مشابه، ازطریق مدل‌های جهانی[2] کدگذاری و تنظیم می‌شوند، مدل‌هایی که مستقل از سخن‌گو هستند و می‌توانند با مدلی خاص مقایسه شوند (Li & Jain, 2015).

اگرچه فنّاوری سیپ تکنیک‌های مختلف آماری خودکار را برای هر مرحله بررسی می‌کند، اما می‌توان به مفروضات و منطق کلی این نوع تکنیک‌ها در هنگام ساختن نمایش‌های محاسباتی هویت‌ها و بیومتریک نرم اشاره کرد. برای بهبود دقت فنّاوری سیپ، تکنیک موصوف از دو اصل کلی پیروی می‌کند: نمایش محاسباتی آیتم‌های هر طبقه باید مشابه باشد؛ درحالی‌که نمایش نمونه‌های طبقه‌های مختلف با گروه‌های دیگر بسیار متفاوت است. بنابراین، برای جست‌وجوی این اصول، از تکنیک‌های آماری مانند تحلیل عامل و از تحلیل متمایز خطی، برای یافتن یک نمایش برداری استفاده می‌شود که در آن بین واریانس بین‌طبقاتی (گروه‌های جمعیتی مختلف برای مثال نمونه‌های بزرگ‌سالان در مقابل کودکان) و واریانس درون‌طبقه‌ای رابطه معنا دار وجود دارد (Li & Jain, 2015). این اصل عمومی برای تبدیل داده‌ها در روش‌های خودکار در راستای ساخت ابزارهای امتیازدهی نهایی مانند ماشین‌های بردار پشتیبان و شبکه‌های عصبی استفاده می‌شود. به‌عبارت‌دیگر، ویژگی‌های صوتی، که در میان گروه‌های انسانی مشابه‌اند، از مدل حذف می‌شوند؛ درحالی که ویژگی‌هایی خاص عموماً تأثیر قوی‌تری در امتیازدهی دارند که میزان احتمال تعلق یک فرد به یک گروه جمعیتی را اندازه‌گیری می‌کند (Li & Jain, 2015)

در سیپ برای شناسایی جنسیت، سن، زبان و لهجه از سیستم‌های ناهمگن استفاده می‌شود که با رونویسی گفتار به متن با نقطه‌گذاری کلمهٔ کلیدی گسترش می‌یابد و ادغام بین وظیفه‌ای[3] نامیده می‌شود. نمای کلی ترکیب اطلاعات هویت، که در سیپ استفاده می‌شود، در شکل ۱ نشان داده شده است.

1. I-Vectors
2. Universal Background Models
3. Inter-task



شکل ١: سازوکار ترکیب اطلاعات مربوط به تشخیص هویت در سیپ

استفاده از مدل‌های طبقه‌بندی بیومتریک نرم پیش‌تر در زمینهٔ تشخیص چهره برای بهبود روش‌های تشخیص بصری توسعه یافته است (Park & Jain, 2010). اطلاعات مربوط به جمعیت‌های انسانی و کلمات کلیدی استفاده‌شده در سیپ عموماً درحکم ابردادهٔ مرتبط با یک سخن‌گو در چارچوب تحقیق و جست‌وجو در دسترس خواهد بود. منطق حاکم بر این فنّاوری آن است که هنگام مقایسهٔ دو مدل سخن‌گو، اگر ویژگی‌های استنباط‌شده مشابه باشند، باید آن‌ها را در فضای مدل نزدیک‌تر در نظر گرفت؛ برای مثال سیپ در فرایند تشخیص هویت فردی، که مردی بالغ با لهجهٔ هندی شناسایی می‌شود، به احتمال زیاد نمونه‌های صوتی را با ویژگی‌های مدنظر مطابقت می‌دهد. توسعه‌دهندگان سیپ چندین روش را برای ترکیب اطلاعات گوینده با لهجه، زبان و جنسیت و سن در ابرداده‌ها بررسی کردند (Ferras et al., 2016; Madikeri et al., 2019). در مطالعات تجربی این نتیجه حاصل شد که افزودن این قبیل اطلاعات جانبی، میزان خطا را تا ٠/٥ درصد در مجموعه‌داده‌های معیار کاهش می‌دهد (Ferras et al., 2016).

فنّاوری شناسایی زبان سیپ ٢٢ زبان مختلف را تشخیص می‌دهد و چندین لهجهٔ انگلیسی (بومی، چینی، روسی، هندی و کره‌ای) را تفکیک و شناسایی می‌کند. این ماژول‌ها به‌گونه‌ای آموزش داده شده‌اند که بین زبان‌ها و لهجه‌ها تمایز قائل شوند و از شناسایی ویژگی‌های صوتی از گویندگان جلوگیری کنند. ویژگی دیگر سیپ، ساده‌سازی[1] برای کاربران درخصوص انواع منابع و پایگاه‌های داده، مانند ادغام جمع‌آوری داده‌ها ازطریق هوش منبع باز، ضبط داده‌های صوتی ازطریق ضبط صدا با تلفن همراه و ماهواره و استفادهٔ بهینه از آن‌هاست. تلفن‌های همراه برای ضبط نمونه‌های صوتی و ارجاع متقابل آن‌ها به پایگاه‌های اطلاعاتی قانونی و اینترپل، ویژگی‌های محصولات هوش مصنوعی[2] را در امکان‌سنجی استخراج صدا فراهم می‌کند که مستلزم گروه‌بندی صداهای گوینده‌های مشابه در یک پایگاه داده است تا داده‌های ناشناخته را در مجموعه‌های بزرگی از اطلاعات در کانال‌های گوناگون ارتباطی و مخابراتی مرتبط کند (Ferras et al. 2016).

سیاست‌های حقوقی تشخیص صدا در به‌کارگیری فنّاوری سیپ

استفاده از داده‌های بیومتریک به دنبال صبغهٔ برندسازی[3] است که در آن، کاربرد بیومتریک تأیید، شناسایی و شیوه‌های مکانیکی تشخیص هویت[4] است که بدن انسان را به‌منزلهٔ ادله و مدرک قابل قبول معرفی می‌کند. در تجزیه‌وتحلیل فنّاوری سیپ، اگرچه بحث‌ها عمدتاً حول استفاده از تشخیص چهره متمرکز شده است، شکل جدیدی از فنّاوری بیومتریک در زمینهٔ اجرای قانون را سبب شده که بدن انسان را بیشتر به‌منزلهٔ مدرک

1. Simplify
2. NUANCE Created the voice recognition space more than 20 years ago and has been building deep domain expertise across science and hygiene. See www.nuance.com
3. Genealogy of Branding
4. Automation Practices

و ادلهٔ اثبات نفیاً یا اثباتاً سوق می‌دهد و به افزایش سطح نظارت کمک شایان توجهی می‌کند. فنّاوری سیپ نه‌فقط به دنبال شناسایی صداها، بلکه درپی این حقیقت است که «به‌طور فعال قابلیت شناسایی و تشخیص هویت دقیق ایجاد کند» (Amoore, 2020, p. 69). هنوز دربارهٔ نحوهٔ استفادهٔ سازمان‌های مجری قانون از سیپ در عمل اطلاعات کمی موجود است، اما ادغام فنّاوری سیپ با سایر نهادهایی مانند اینترپل به پیشرفت شگرف سیستم‌های داده مبتنی‌بر صدا در پروژه‌های تحقیقاتی امنیتی [1] انجامیده است (Fieke et al., 2021).

آنچه از نظر قابلیت تشخیص هویت اهمیت دارد، نمایش دیجیتالی صداست. بحث دربارهٔ پیامدهای حقوقی و سیاسی ناظر بر سیستم‌های هویت بیومتریک مانند انگشت‌نگاری و تصویربرداری دیجیتال، براساس صورت‌نگاری و چهره‌شناسی افراد و یا ازطریق خصایص رفتاری و فیزیکی دیگر مانند نحوهٔ راه‌رفتن، نگرانی‌های جدی را در بروز خطا و پیامدهای تبعیض‌آمیز به وجود آورده است. این قبیل نگرانی‌ها با تأکید بر فردیت غیررنگین [2] یا تبعیض برپایهٔ رنگ پوست که تبارشناسی فنّاوری‌های بیومتریک را مشخص کرده است، به میزان جهت‌گیری در شناسایی یا سوء تعبیر از چهره‌های انسانی «دیگر» [3] مانند سیاه‌پوست، دورگه، زنان و اقلیت‌های جنسی و جنسیتی (دگرجنس‌گراها) [4] اشاره کرده است (Browne, 2015; Brayne, 2020; Buolamwini & Gebru, 2018). کالریسم [5] یا تبعیض براساس رنگ پوست نوعی پیش‌داوری است، که در قالب تبعیض نژادی، جوامع انسانی را برپایهٔ برخی معانی و ملاحظات اجتماعی مرتبط با رنگ پوست پیش‌داوری می‌کند. این امر با عدالت کیفری و حتی در سیستم‌های فنّاوری با پیش‌داده‌های مفروض بر این اساس مغایر است. به نظر می‌رسد از منظر حقوقی، به‌ویژه حقوق بنیادین انسان در تکریم وی به ماهو انسان و منع هرگونه تبعیض، رویکرد انتقادی نظریهٔ نژادی با تشخیص هویت مرتبط باشد. طبق این نظریهٔ جامعه‌شناختی، برتری سفید و قدرت نژادی به مرور زمان باقی می‌ماند و نژاد در این قرائت برخاسته از هویتی اجتماعی است (Bell, 1995).

شناسایی نادرست یا سوء تشخیص [6] ممکن است به افزایش نظارت پلیس و سایر اقدامات منجر شود؛ مهم‌ترازهمه، نشان‌دادن میزان «سوگیری یا جهت‌دهی» در سیستم‌های هویت بیومتریک باعث تضعیف مشروعیت استفاده از آن‌ها شده است. همچنین این نگرانی وجود دارد که به‌دنبال اصلاحات فنی، بهینه‌سازی تشخیص چهره صرفاً برای گروه‌هایی باشد که مستعد سوءشناسایی هستند. بنابراین این دغدغه، صرفاً درمورد فنّاوری سیپ به‌منزلهٔ سیستم تأیید شناسایی در تشخیص صدای صرف متصور نیست، بلکه بیم آن می‌رود که سایر فنّاوری‌هایی که برای تشخیص صدای جوامع خاص تعبیه می‌شوند نیز برچسب انتقادی تبعیض‌نژادی را داشته باشند. فرض الگوریتم‌های تشخیص براساس گویش، لهجه، زبان‌ها و جنسیت‌های خاص، که به‌خودی‌خود با شناسایی تروریست و مجرمان مرتبط است، می‌تواند بیانگر تجسس و تفحص افراد و جوامع خاصی برای انتساب جرم به آنان باشد؛ بنابراین ادغام نمونه‌های صوتی در پایگاه‌های اطلاعاتی برای اهداف قانونی، مشروط به بررسی گروه خاص نژادی است و بدین‌ترتیب ناامنی هستی‌شناسانه [7] را در رژیم تشخیص هویت ازطریق سیستم‌های هویت بیومتریک مقرر می‌دارد (Browne, 2015).

همچنین، براساس معیارهای داده‌ای پیش‌فرض، بعید است که منطق طبقه‌بندی در سیستم بیومتریک نرم با تنوع فرهنگی و اجتماعی جمعیت انسانی و عموم مطابقت داشته باشد. به نظر می‌رسد به‌کارگیری بیومتریک نرم اعتبار علمی ندارد و اغلب به فرضیات مورد مناقشه دربارهٔ ویژگی‌های فیزیولوژیکی و رابطهٔ بین افراد و داده‌ها متکی است (Sanchez-Monedero & Denick, 2022). گزینه‌های پیش‌فرض انتخاب در بازنمایی دیجیتالی برخی صداهای ذخیره‌شده از زیرساخت‌های داده‌محور، به‌منظور اطلاع از برچسب‌زنی مجرمان یا تروریست‌ها، رژیم خاصی از شناسایی را هویدا می‌کند که در آن اولویت‌بندی گروه‌های خاصی از افراد را شکل می‌دهند که به‌دست مجریان قانون در پردازش الگوریتمی، در قالب ویژگی‌های صوتی خاص اشتراک‌گذاری می‌شوند (Fieke et al., 2021).

1. See Roxanne Project.
2. Prototypical Whiteness
3. Misidentification of Othered Faces
4. Queer Communities
5. Colorism
6. Misidentification
7. Ontological Insecurities

استفاده از بیومتریک نرم به‌منزلهٔ سازوکار مبتنی‌بر گزینهٔ پیش‌انتخاب، نمونه‌های کلیشه‌ای[1] و یکنواخت را در نهادهای موجود مقرر می‌دارد و با جرم‌انگاری جوامع خاص،[2] ابهامات عدیده را رقم می‌زند (Williams, 2015). درصورتی که پردازش الگوریتمی صدا ـ بدون اطلاع از کسانی که تحت تأثیر قرار گرفته‌اند ـ محقق شود، ابهامات موجود در فرایندی را که ازطریق آن، جوامع خاص جرم‌انگاری می‌شوند تضمین می‌کند. در پروژهٔ سیپ، استفاده از بیومتریک نرم دقت شناسایی مظنونان را افزایش و نظارت بر افراد بی‌گناه را در اثبات بی‌گناهی‌شان کاهش می‌دهد. پیش‌فرض انتخاب صدا دربارهٔ تشخیص هویت جمعیت‌های انسانی، این دوگانگی[3] را به ذهن متبادر می‌کند که چگونه صدا درحکم تهدید جدی در مواجهه با جنایتکاران یا عاملان تروریستی و هم برای اثبات بی‌گناهی فرد استفاده می‌شود (Fieke et al., 2021).

امروزه اهمیت بازنمایی دیجیتالی صدا بر همگان مشخص است که البته مستعد تداخلات محیطی است؛ به‌همین‌منظور آن‌ها را نامعتبر می‌کند. دست‌اندرکاران پروژهٔ سیپ سعی دارند با تکیهٔ بیشتر بر برخی داده‌ها به‌جای شنود تلفنی (مانند هوش منبع باز یا اوسینت) بر این مشکل غلبه کنند (Amoore, 2019) و آن را به‌منزلهٔ پیش‌شرط یقین الگوریتمی[4] توصیف کنند؛ بنابراین سیستم‌های الگوریتمی موارد شک را می‌زدایند و هم‌زمان «پارامترهایی را که عدم قطعیت براساس آن‌ها قضاوت می‌شود» بازتولید می‌کند تا نتیجه به واحدی متراکم تبدیل شود. خروجی نهایی با حذف موارد مشکوک و با حصول یقین و البته با نادیده‌گرفتن خطاپذیری الگوریتم درمورد امور پیرامونی مفروض محقق می‌شود (Amoore, 2019).

سیستم‌های هویت بیومتریک با تأکید بر صدای انسان به‌منزلهٔ رژیم‌های تشخیص هویت بهینه قلمداد می‌شوند. صدا به‌منزلهٔ عنصر مؤثر در فنّاوری نوین تشخیص، تفاوت‌ها را طبقه‌بندی می‌کند (Bourdieu, 1982; 2018)؛ گرچه منطق طبقه‌بندی افراد هدف در این سیستم با مشکل روبه‌روست؛ اما سازوکار طبقه‌بندی پتانسیل لازم را دارد تا موقعیت اجتماعی، فرهنگی و اقتصادی فرد را در جامعه شکل دهد (Fourcade & Healy, 2017). در فنّاوری سیپ، جمع‌آوری نمونه‌های صوتی در میان سایر منابع داده‌ای (رسانه‌های اجتماعی، تلفن‌های همراه و غیره) انجام می‌شود و ادغام داده‌های صوتی در یک پایگاه مشترک داده‌ای متعلق به سازمان‌های مجری قانون محقق می‌شود که در داده‌کاوی ابعاد جهانی دارد؛ بنابراین استفاده از مجموعهٔ نمونه‌صداهای انسانی، به زیرساخت داده این اجازه را می‌دهد تا به صحنهٔ جرم تبدیل شود و سایتی پویا و قانونی را برای تحقیق از یک شخص محقق بدارد. برای مثال، پلتفرم‌های رسانه‌های اجتماعی[5] شرایطی را فراهم می‌کنند که در آن تشخیص هویت مکانی موثق برای شکل‌گیری هویت تشخیص است که اهمیت خاص برای نهادهای قانونی و جنایی دارد (Fieke, 2021)؛ بنابراین استفاده از فنّاوری صدا به تشخیص مجرمان با دقت بالا منجر می‌شود که درنهایت به‌عنوان مدرکی مستدل، برای احراز بی‌گناهی مظنونانی به‌کار می‌رود که به ناحق وارد وادی مجازات می‌شوند. این امر، به علم قاضی کمک می‌کند تا ظن را به یقین تبدیل کنند (Couldry & Mejias, 2019).

عدالت داده[6] مفهومی نوین همراه با توسعهٔ فنّاوری است. در این قرائت، بر تحقق عدالت دربارهٔ افرادی که ازطریق سیستم‌های داده شناسایی می‌شوند تأکید می‌شود. صدا، در هر دو شکل نمادین و مادی خود، در واقعیت اغلب برای اعادهٔ حق به‌کار می‌رود که در مقام دفاع کاربرد دارد (Couldry, 2010). ظهور سیستم‌های هویت بیومتریک، مانند فنّاوری سیپ، به رابطهٔ بین صدا و تشخیص هویت فردی اشعار دارد. به‌عبارت‌دیگر، به‌جای این‌که صدا مجرایی باشد که ازطریق آن، سیاست تشخیص بتواند مبتنی‌بر تجربیات افراد از دنیای اجتماعی‌شان باشد، سیپ فرایندی از بیگانگی و تفرق[7] میان صدا و تشخیص را مقرر می‌دارد. صدای تجسم‌یافته دیگر هیچ ارتباط معناداری با شرایط تشخیص و نحوهٔ نسبت‌دادن صدا ندارد و سیپ این نوع رابطه را با ترکیب صدا و تخصیص فضا به فضای طبقه‌بندی صدا برای اهداف مجریان قانون تغییر

1. Stereotyping
2. Criminalization of Specific Communities
3. Duality
4. Algorithmic Doubt & Certainty
5. Social Media Platforms
6. Data Justice
7. Alienation

می‌دهد. ازاین‌منظر، سیستم‌های هویت بیومتریک ذاتاً نادرست و در امر تشخیص هویت با سوگیری همراه است؛ زیرا افرادی را که ویژگی‌های صوتی مشترکی دارند به اولویت تشخیصی جرم نسبت داده و آنان را در مقام مجرم پیش‌فرض می‌داند (Fieke et al., 2021).

نتیجه‌گیری

استفاده از داده‌های بیومتریک در بررسی جرم و اعمال غیرقانونی، سابقهٔ طولانی دارد. نهادهای مجری قانون اغلب چنین فنّاوری‌هایی را با نوید عملکرد کارآمدتر و دقیق‌تر توسعه داده‌اند؛ بااین‌حال نگرانی‌هایی درمورد تأثیر سوء سیستم‌های هویت بیومتریک در عملکرد ضابطان قضایی وجود دارد که اغلب بر ماهیت و مقیاس نظارتی در استفاده و به‌کارگیری، از حیث تزاحم حق حریم خصوصی فردی، آزادی بیان و آزادی تجمع بیان شده است؛ به‌ویژه در میان گروه‌های اقلیت که در معرض افزایش خطر جرم‌انگاری هستند. امروزه سیستم‌های هویت بیومتریک نوین ابزاری برای حکمرانی قلمداد می‌شوند که بیم عدول از عدالت داده در حفظ و استفاده را تداعی می‌کنند.

فنّاوری سیپ در اروپا به‌منزلهٔ روشی پیشرفته با تکیه بر پیش‌فرض‌های مقرر مبتنی‌بر بیومتریک نرم، مانند جنسیت، زبان و گویش و لهجه‌های گوناگون، با فرض افزایش دقت و رفع نیازهای اصلی سازمانی ایجاد شده است. دقت سیپ نه‌فقط از نظر تشکیل هویتی واحد، بلکه برای راه‌اندازی یک سیستم طبقه‌بندی براساس تطبیق ویژگی‌های صوتی با اولویت‌های جرم فرض می‌شود. این سیستم طبقه‌بندی، به دسترسی داده‌ها به شکل نمایش دیجیتالی صدا در پلتفرم‌های آنلاین و تلفن‌های همراه مشروط است.

ازآنجاکه فنّاوری‌های تشخیص صدا در حوزهٔ قانونی و قضایی و مستند بر اصل حاکمیت قانون اهمیت دارد، بررسی دقیق رژیم‌های حقوقی نوظهور تشخیص هویت و نحوهٔ تأثیر آن‌ها در شیوه‌های نوین تحقیقات پلیسی باید مبتنی‌بر عدالت داده باشد؛ بنابراین رویکردهای حقوقی در تبیین ماهیت این قبیل فنّاوری‌ها در استفادهٔ بهینه در امور قانونی مؤکداً توصیه می‌شود تا تبیین عدالت داده‌ها در حفظ آن‌ها به‌سوی انصاف و عدل سوق داده شود.

منابع

هداوند، مهدی و جم، فرهاد (۱۴۰۰). مفهوم دولت تنظیم‌گر: تحلیل تنظیم‌گری به مثابهٔ ابزار حکمرانی. *راهبرد*، ۳۰(۹۹)، ۲۶۶-۲۲۷.

Abdelwhab, A., & Viriri, S. (2018). A survey on soft biometrics for human identification. *Machine Learning and Biometrics*, p. 37

Alegre, F., Soldi, G., & Evans, N. (2014, May). Evasion and obfuscation in automatic speaker verification. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 749-753). IEEE.

Amoore, L. (2019). Doubt and the algorithm: On the partial accounts of machine learning. *Theory, Culture & Society*, *36*(6), 147-169.

Amoore, L. (2020). *Cloud ethics: Algorithms and the attributes of ourselves and others*. Duke University Press.

Andrejevic, M. (2013). Exploitation in the data mine. In *Internet and surveillance* (pp. 71-88). Routledge.

Aronowitz, H., Hoory, R., Pelecanos, J., & Nahamoo, D. (2011). New developments in voice biometrics for user authentication. In *Twelfth Annual Conference of the International Speech Communication Association*., Florence, Italy, 28–31 August 2011, pp.17–20.

Bell, Derrick A. A. (1995). *Who's Afraid of Critical Race Theory University of Illino law reviw, 1995*(4), pp. 893-910.

Watch, B. B. (2018). Face off: The lawless growth of facial recognition in UK policing. *Obtenido de: bigbrotherwatch. org. uk/wp-content/uploads/2018/05/Face-Off-final-digital-1. pdf. Consultado el*, *22*. Available at: https://bigbrotherwatch.org.uk/wpcontent/uploads/2018/05/Face-Off-final-digital-1.pdf.

Bora, A. (2017). Semantics of ruling: reflective theories of regulation, governance and law. In Society, Regulation and Governance (pp. 15-37). Edward Elgar Publishing.

Bourdieu, P. (1982). *Classification Struggles*. Cambridge and Medford, MA: Polity.

Bourdieu, P. (2018). *Classification Struggles*. Cambridge and Medford, MA: Polity.

Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press, USA.

Brayne, S., & Christin, A. (2021). Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social problems*, *68*(3), 608-624.

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press.

Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77-91). PMLR.

Burke, P. J., & Stets, J. E. (2009). Identity theory: Oxford University Press. *New York, NY*.

Cheney-Lippold, J. (2017). We are data. In *We Are Data*. New York University Press.

Couldry, N. (2010). *Why voice matters: Culture and politics after neoliberalism*. Sage publications.

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4), 336-349.

Dantcheva, A., Elia, P., & Ross, A. (2015). What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security*, *11*(3), 441-467.

Dehak, N., Kenny, P.J., Dehak, R., Dumouchel, P., Ouellet, P. (2011). Front-end factor analysis for speaker verification. IEEE Transactions on Audio. *Speech, and Language Processing*, *19*(4), p. 788–798.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2), 1–12.

Edri (2020). Facial recognition & biometric surveillance: document pool. Available at: https://edri.org/our-work/facial-recognitiondocument-pool/ (accessed 4 June 2021).

European Commission (2017) Speaker identification integrated project. September 10th 2017. Available at: https://cordis. europa.eu/project/id/607784 (accessed 17 June 2021).

Fanon, F. (2008). *Black skin, white masks*. Grove press.

Ferras, M., Madikeri, S. R., Dey, S., Motlícek, P., & Bourlard, H. (2016). Inter-Task System Fusion for Speaker Recognition. In *INTERSPEECH* (pp. 1810-1814).

Jansen, F., Sánchez-Monedero, J., & Dencik, L. (2021). Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP. *Big Data & Society*, *8*(2), 20539517211063604.

Fourcade, M., & Healy, K. (2017). Seeing like a market. *Socio-economic review*, *15*(1), 9-29.

Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. Available at: https//: repository.essex.ac.uk/24946/1/London-Met-Police-Trial-ofFacial-Recognition-Tech-Report-2.pdf.

Garland, D. (2004). Beyond the culture of control. *Critical review of international social and political philosophy*, *7*(2), 160-189..

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance* (Vol. 2). NYU Press.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British journal of sociology*, *51*(4), 605-622.

Herzig, R. (2017). *The Role of Symbolic Capital in Digital Inequality: Lessons from The Student Room's Reputation System* (Doctoral dissertation, University of East Anglia).

Interpol (2018a). Speaker 04. Available at: https://www.youtube. com/watch?v=foXSJCtHSqs (accessed 18 June 2021).

Interpol (2018b). Speaker Identification Integrated Project. Available at: https://www.interpol.int/en/Who-we-are/Legalframework/Information-communications-and-technology-ICTlaw-projects/Speaker-Identification-Integrated-Project-SIIP (accessed 8 December, 2021).

Kak, A. (2020). Regulating biometrics: Global approaches and urgent questions. *AI Now Institute, September*, *1*.

Khelif, K., Mombrun, Y., Backfried, G., Sahito, F., Scarpato, L., Motlicek, P., Madikeri, S. R., Kelly, D, Hazzani, G. & Chatzigavriil, E. (2017, September). Towards a breakthrough speaker identification approach for law enforcement agencies: SIIP. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 32-39). IEEE.

Khelif, K., Mombrun, Y., Hazzani, G., Motlicek, P., Madikeri, S., Sahito, F., & Backfried, G. (2018). SIIP: An innovative speaker identification approach for law enforcement agencies. In *STO meeting proceedings paper, NATO-OTAN* (pp. 1-14).

Kind, C. (2019). Biometrics and facial recognition technology–where next. *Ada Lovelace Institute* .Available at: https://www.adalovelaceinstitute.org/blog/biometrics-and-facialrecognition-technology-where-next/ (accessed 4 July 2021).

Kindt, E. (2020). A first attempt at regulating biometric data in the European Union. *Regulating Biometrics: Global Approaches and Open Questions. New York: AI Now*, p. 62-69.

Kofman, A. (2018). Interpol rolls out international voice identification database using samples from 192 law enforcement agencies. *The Intercept*, *25*.

Kroemer, H., & Kittel, C. (1980). *Thermal Physics*. (2nd ed.) W.H. Freeman Company.

Leese, M. (2022). Fixing state vision: Interoperability, biometrics, and identity management in the EU. *Geopolitics*, *27*(1), 113-133. DOI: 10.1080/14650045.2020.1830764.

Li, S.Z. & Jain, A.K. (2015). *Encyclopedia of Biometrics*. Boston, MA: Springer

Liberty (2020) Liberty wins ground-breaking victory against facial recognition tech. In: *Liberty*. Available at: https://www. libertyhumanrights.org.uk/issue/liberty-wins-groundbreaking-victory-against-facial-recognition-tech/ (accessed 26 June 2021).

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, *22*(9), 499-508.

Madikeri, S., Motlicek, P., & Dey, S. (2019, May). A Bayesian approach to inter-task fusion for speaker recognition. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 5786-5790). IEEE.

Marciano, A. (2019). Reframing biometric surveillance: from a means of inspection to a form of control. *Ethics and Information Technology*, *21*(2), 127-136.

McBride, C. (2013). *Recognition*. Camridge, Malden: Polity.

Morrison, G. S., Sahito, F. H., Jardine, G., Djokic, D., Clavet, S., Berghs, S., & Dorny, C. G. (2016). INTERPOL survey of the use of speaker identification by law enforcement agencies. *Forensic science international*, *263*, 92-100.

Park, U., & Jain, A. K. (2010). Face matching and retrieval using soft biometrics. *IEEE Transactions on Information Forensics and Security*, *5*(3), 406-415.

Poddar, A., Sahidullah, M., & Saha, G. (2019). Quality measures for speaker verification with short utterances. *Digital Signal Processing*, *88*, 66-79.

Pollack, I., Pickett, J. M., & Sumby, W. H. (1954). On the identification of speakers by voice. *the Journal of the Acoustical Society of America*, *26*(3), 403-406.

Rashid, R. A., Mahalin, N. H., Sarijari, M. A., & Aziz, A. A. A. (2008, May). Security system using biometric technology: Design and implementation of Voice Recognition System (VRS). In *2008 international conference on computer and communication engineering* (pp. 898-902). IEEE.

Sánchez-Monedero, J., & Dencik, L. (2022). The politics of deceptive borders:'biomarkers of deceit'and the case of iBorderCtrl. *Information, Communication & Society*, *25*(3), 413-430. DOI: 10.1080/ 1369118X.2020.1792530.

Scott, J. C. (2020). *Seeing like a state: How certain schemes to improve the human condition have failed*. yale university Press.

Taylor, C. (1994). *Multiculturalism: Examining the Politics of Recognition*. Princeton, NJ: Princeton University Press.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2), 1-14.

Turow, J. (2021). *The Voice Catchers: How Marketers Listen In to Exploit Your Feelings, Your Privacy, and Your Wallet*. New Haven: Yale University Press.

Valentino-DeVries, J. (2020). How the Police Use Facial Recognition, and Where It Falls Short-The New York Times. *URL: https://www. nytimes. com/2020/01/12/technology/facial-recognition-police. html*.

Van der Ploeg, I. (1999). The illegal body:Eurodac'and the politics of biometric identification. *Ethics and Information Technology*, *1*, 295-302.

Van Zoonen, L. (2013). From identity to identification: fixating the fragmented self. *Media, Culture & Society*, *35*(1), 44-51.

Williams, P. (2015). Criminalising the other: Challenging the race-gang nexus. *Race & Class*, *56*(3), 18-35.

Williams, P., & Clarke, B. (2016). Dangerous associations: Joint enterprise, gangs and racism. *Centre for Crime and Justice Studies*, 1-24.

Young, I. M. (1990). *Justice and the Politics of Difference*. Princeton University Press.