Received: 10 /10/2024
Review: 04/01/2025
Accepted: 10 /04/2025
DOI: 10.22054/jocl.2025.85062.1270

Journal of Cyber Law
No(1),Vol(2), 65-79
ISSN: 0972-6934
www.jocl.ir

Cyber Law in Confrontation with Facial Recognition Technologies and the Threats to Citizens' Privacy

Mahdi Rezvanfar[1], Negar Khosroshahi[2*]

1- Master's Student in Law, University of Isfahan, Isfahan, Iran
2- Master's Student in Law, University of Isfahan, Isfahan, Iran

ABSTRACT

Facial recognition technologies have rapidly expanded in recent years, with their applications in security, commercial, and social domains increasing significantly. While this technology enhances efficiency and security, it simultaneously poses serious threats to citizens' privacy and raises fundamental legal questions. Key issues include the collection, storage, and use of individuals' biometric data, which, without legal oversight, can violate fundamental rights. The necessity of examining cyber law in the context of facial recognition arises from the fact that existing legal frameworks in many countries are not yet equipped to address the emerging threats of this technology, and legal gaps can lead to misuse of personal information. This study aims to analyze the legal challenges to privacy posed by facial recognition technology and propose legal measures for protecting citizens' personal data. The research method in this article is descriptive–analytical and based on documentary studies, reviewing legal sources, scientific articles, and international documents. The findings indicate that implementing comprehensive regulations and updating existing laws can balance the utilization of advanced technologies with the protection of citizens' rights, and transparency in the use of biometric data enhances public trust. The innovation of this article lies in presenting a combined analytical framework between cyber law and privacy for facial recognition technology, enabling comparison and application in future policymaking.

Keywords:
facial recognition technology, cyber law, privacy, biometric data, legal regulations

How to Cite: rezvanfar, M. and khosroshahi, N. (2025). Cyber Law in Confrontation with Facial Recognition Technologies and the Threats to Citizens' Privacy. Journal of Cyber Law (JOCL), 2(1), 65-79.
doi: 10.22054/jocl.2025.85062.1270

* Corresponding Author: negar.khosroshahi@ui.ac.ir

نشریه حقوق سایبری
شماره (۱) 65-79
دوره ۱۴۰۴

تاریخ دریافت: ۱۴۰۳/۰۷/۲۰
تاریخ اصلاح: ۱۴۰۳/۱۰/۱۴
تاریخ پذیرش: ۱۴۰۴/۰۱/۲۲

بررسی حقوق سایبری در مواجهه با فناوری‌های تشخیص چهره و تهدید حریم خصوصی شهروندان

مهدی رضوان فر[۱]،نگار خسروشاهی[۳*]

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه اصفهان، اصفهان، ایران

۲- دانشجوی کارشناسی ارشد حقوق، دانشگاه اصفهان، اصفهان، ایران

چکیده

فناوری‌های تشخیص چهره در سال‌های اخیر به‌سرعت در حال گسترش بوده و کاربردهای آن در حوزه‌های مختلف امنیتی، تجاری و اجتماعی به‌طور چشمگیری افزایش یافته است. این فناوری، اگرچه کارایی و امنیت را ارتقاء می‌بخشد، اما به‌طور همزمان تهدیدات جدی برای حریم خصوصی شهروندان ایجاد می‌کند و موجب بروز پرسش‌های اساسی حقوقی می‌شود. از جمله مسائل مهم، نحوه جمع‌آوری، ذخیره‌سازی و استفاده از داده‌های زیست‌سنجی افراد است که بدون نظارت قانونی می‌تواند حقوق بنیادین شهروندان را نقض کند. ضرورت بررسی حقوق سایبری در مواجهه با فناوری‌های تشخیص چهره از آن جهت است که نظام‌های قانونی موجود در بسیاری از کشورها هنوز پاسخگوی تهدیدات نوظهور این فناوری نیستند و خلأهای قانونی می‌تواند باعث سوءاستفاده از اطلاعات شخصی شود. هدف این مقاله تحلیل حقوقی چالش‌های حریم خصوصی ناشی از فناوری تشخیص چهره و ارائه راهکارهای قانونی برای حفاظت از داده‌های شخصی شهروندان است. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی است، به‌طوری که منابع حقوقی، مقالات علمی و اسناد بین‌المللی مورد بررسی قرار گرفته‌اند. نتایج تحقیق نشان می‌دهد که اعمال مقررات جامع و به‌روزرسانی قوانین موجود می‌تواند تعادلی میان بهره‌برداری از فناوری‌های نوین و حفظ حقوق شهروندان برقرار کند و شفافیت در استفاده از داده‌های زیست‌سنجی، اعتماد عمومی را افزایش می‌دهد. نوآوری این مقاله در ارائه چارچوب تحلیلی ترکیبی میان حقوق سایبری و حریم خصوصی برای فناوری تشخیص چهره است که امکان مقایسه و کاربرد در سیاست‌گذاری‌های آینده را فراهم می‌کند.

کلیدواژه‌ها:

فناوری تشخیص چهره، حقوق سایبری، حریم خصوصی، داده‌های زیست‌سنجی، مقررات قانونی

نحوه استناد:

رضوان فر, مهدی و خسروشاهی, نگار . (۱۴۰۴). بررسی حقوق سایبری در مواجهه با فناوری‌های تشخیص چهره و تهدید حریم خصوصی شهروندان. حقوق سایبری, ۲(۱), ۶۵-۷۹.

* ایمیل نویسنده مسئول: negar.khosroshahi@ui.ac.ir

مقدمه

فناوری‌های تشخیص چهره به‌عنوان یکی از پیشرفته‌ترین ابزارهای شناسایی بیومتریک، در سال‌های اخیر تحولی شگرف در حوزه‌های مختلف نظیر امنیت عمومی، خدمات بانکی، تبلیغات هدفمند و مدیریت دسترسی ایجاد کرده‌اند (محمدی، ۱۴۰۱، ص. ۳۲). با این حال، استفاده گسترده از این فناوری‌ها، به‌ویژه در فضای عمومی، با چالش‌های حقوقی و اخلاقی متعددی مواجه است که تهدیدی جدی برای حریم خصوصی شهروندان محسوب می‌شود (کاظمی، ۱۴۰۰، ص. ۴۷). در نظام‌های حقوقی مختلف، از جمله اتحادیه اروپا، ایالات متحده و برخی کشورهای آسیایی، مقرراتی برای حفاظت از داده‌های بیومتریک تدوین شده است؛ اما در عمل، بسیاری از این قوانین با سرعت پیشرفت فناوری هم‌راستا نبوده و با خلأهای قانونی مواجه‌اند (Lee & Chen, 2021, p. 98; Patel, 2022, p. 65).

در نظام حقوقی ایران، با وجود تصویب «قانون حمایت از حقوق کاربران در فضای مجازی» در سال ۱۳۹۹، هنوز مقررات مشخصی برای استفاده از فناوری‌های تشخیص چهره وجود ندارد (صدر، ۱۴۰۰، ص. ۱۵). این امر موجب نگرانی‌هایی در خصوص نقض حریم خصوصی و سوءاستفاده از داده‌های بیومتریک شهروندان می‌شود. در این زمینه، ماده ۲۲ قانون اساسی جمهوری اسلامی ایران (حسینی، ۱۴۰۱، ص. ۴۵)، اصل ۲۲ قانون اساسی و ماده ۲ قانون حمایت از حقوق کاربران در فضای مجازی، به‌طور غیرمستقیم به حفاظت از حریم خصوصی اشاره دارند؛ اما هیچ‌یک به‌طور خاص به استفاده از فناوری‌های تشخیص چهره و چالش‌های حقوقی آن نپرداخته‌اند (یوسفی، ۱۳۹۹، ص. ۷۸).

اهمیت این موضوع در دنیای امروز به‌ویژه با توجه به گسترش استفاده از فناوری‌های تشخیص چهره در مکان‌های عمومی، مدارس، فرودگاه‌ها و مراکز تجاری، دوچندان می‌شود. مطالعات مختلف نشان داده‌اند که این فناوری‌ها می‌توانند به‌راحتی برای شناسایی و ردیابی افراد بدون اطلاع یا رضایت آن‌ها استفاده شوند. برای مثال، در پژوهشی که در سال ۲۰۲۴ منتشر شد، به بررسی چالش‌های حقوقی و اخلاقی استفاده از فناوری‌های تشخیص چهره در مکان‌های عمومی پرداخته شده است (Wang, 2024, p. 45).پیشینه پژوهش‌های انجام‌شده در این حوزه نشان می‌دهد که موضوع حقوق سایبری در مواجهه با فناوری‌های تشخیص چهره و تهدید حریم خصوصی شهروندان، پیش‌تر نیز مورد توجه محققان قرار گرفته است. برای نمونه، در مطالعه‌ای که در سال ۲۰۲۳ منتشر شد، به بررسی تأثیرات استفاده از فناوری‌های تشخیص چهره بر حقوق بشر و حریم خصوصی پرداخته شده است (Qandeel, 2023, p. 112). همچنین، در پژوهشی دیگر در سال ۲۰۲۲، به تحلیل چالش‌های حقوقی استفاده از فناوری‌های تشخیص چهره در نظارت‌های عمومی پرداخته شده است (Simmler, 2022, p. 78).

با وجود این پیشینه، هنوز خلأهای پژوهشی قابل‌توجهی در این زمینه وجود دارد. بیشتر مطالعات موجود، به‌صورت پراکنده به جنبه‌های مختلف این موضوع پرداخته‌اند و تحلیل جامعی از ابعاد حقوقی، اجتماعی و فنی آن ارائه نکرده‌اند. بنابراین،

پژوهش حاضر با هدف پرکردن این خلأ و ارائه تحلیلی جامع از چالش‌های حقوقی استفاده از فناوری‌های تشخیص چهره در ایران، انجام می‌شود.

پرسش‌های اصلی تحقیق عبارت‌اند از:

۱. چه چالش‌های حقوقی در استفاده از فناوری‌های تشخیص چهره در ایران وجود دارد؟

۲. نظام حقوقی ایران تا چه اندازه توانایی مقابله با تهدیدات ناشی از این فناوری‌ها را دارد؟

۳. چه راهکارهایی برای تقویت مقررات حقوقی در این زمینه پیشنهاد می‌شود؟

هدف این مقاله، تحلیل حقوقی چالش‌های استفاده از فناوری‌های تشخیص چهره در ایران و ارائه پیشنهادهایی برای تقویت مقررات حقوقی در این حوزه است. روش پژوهش در این مقاله تحلیلی-توصیفی و مبتنی بر مطالعه اسنادی است. در این روش، ابتدا به بررسی قوانین و مقررات موجود در ایران و سایر کشورها پرداخته می‌شود و سپس با تحلیل آن‌ها، چالش‌ها و خلأهای موجود شناسایی می‌شوند. در نهایت، با ارائه پیشنهادهایی برای تقویت نظام حقوقی، سعی می‌شود راهکارهایی برای حفاظت از حریم خصوصی شهروندان در برابر تهدیدات ناشی از فناوری‌های تشخیص چهره ارائه گردد.

فناوری تشخیص چهره

فناوری تشخیص چهره به‌عنوان یکی از پیشرفته‌ترین شاخه‌های فناوری‌های بیومتریک، بر اساس تحلیل ویژگی‌های فیزیکی صورت افراد عمل می‌کند و امکان شناسایی یا تایید هویت افراد را با دقت بالا فراهم می‌آورد (محمدی، ۱۴۰۱، ص. ۳۲). این فناوری با استفاده از الگوریتم‌های پیچیده یادگیری ماشین و شبکه‌های عصبی مصنوعی، قادر است الگوهای منحصر به فرد صورت هر فرد را استخراج کرده و با پایگاه داده موجود مقایسه کند (Lee & Chen, 2021, p. 98). در عمل، فناوری تشخیص چهره به دو روش اصلی مورد استفاده قرار می‌گیرد: شناسایی یک‌به‌یک (verification) که برای تأیید هویت شخص کاربرد دارد و شناسایی یک‌به‌چند (identification) که برای یافتن هویت یک فرد در میان گروه بزرگی از افراد استفاده می‌شود (Patel, 2022, p. 63).یکی از مهم‌ترین مزایای این فناوری، افزایش امنیت در فضاهای عمومی و خصوصی است. استفاده از سیستم‌های تشخیص چهره در فرودگاه‌ها، بانک‌ها، مراکز تجاری و حتی در کنترل دسترسی به محیط‌های حساس، به کاهش تقلب و سوءاستفاده‌ها کمک می‌کند (کاظمی، ۱۴۰۰، ص. ۴۹). علاوه بر این، فناوری تشخیص چهره در تبلیغات هدفمند و ارائه خدمات شخصی‌سازی شده نیز کاربرد دارد؛ شرکت‌های فناوری از این ابزار برای تحلیل رفتار کاربران، پیش‌بینی نیازها و ارائه خدمات متناسب با ویژگی‌های هر فرد استفاده می‌کنند (محمدی، ۱۴۰۱، ص. ۳۵).

با وجود این مزایا، استفاده گسترده از فناوری تشخیص چهره با چالش‌ها و نگرانی‌های جدی مواجه است. یکی از اصلی‌ترین مسائل، تهدید حریم خصوصی و امنیت داده‌های شخصی است. جمع‌آوری و ذخیره‌سازی اطلاعات بیومتریک افراد، بدون رضایت صریح و چارچوب قانونی، می‌تواند به سوءاستفاده‌های گسترده و نقض حقوق شهروندان منجر شود (نجفی، ۱۴۰۱، ص. ۵۲). از منظر حقوقی، بسیاری از کشورها برای مقابله با این تهدیدها، مقررات خاصی تدوین کرده‌اند. به عنوان نمونه، مقررات عمومی حفاظت از داده‌ها (GDPR) در اتحادیه اروپا، داده‌های بیومتریک را به عنوان داده‌های حساس طبقه‌بندی کرده و شرایط سختگیرانه‌ای برای پردازش آن‌ها تعیین می‌کند (Smith & Johnson, 2019, p.

112). این مقررات شامل الزام به رضایت صریح، محدودیت استفاده، شفافیت و ایجاد مکانیزم‌های جبران خسارت برای افراد است.

در ایالات متحده، قوانین حریم خصوصی متفاوت و ایالتی هستند و برخی ایالات مانند ایلینوی با تصویب « Biometric Information Privacy Act»، جمع‌آوری و استفاده از داده‌های بیومتریک را مشروط به رضایت افراد کرده‌اند (Wang, 2024, p. 46). کشورهای آسیایی نیز به تدریج به تدوین مقررات اختصاصی پرداخته‌اند، اما غالباً این مقررات با سرعت رشد فناوری هم‌راستا نبوده و خلأهای قانونی وجود دارد (Patel, 2022, p. 65).

در نظام حقوقی ایران، فناوری تشخیص چهره هنوز با قوانین مشخص مواجه نشده است. تصویب «قانون حمایت از حقوق کاربران در فضای مجازی» در سال ۱۳۹۹، اقدامی در جهت حفاظت از داده‌های شخصی محسوب می‌شود، اما به طور مستقیم به داده‌های بیومتریک و فناوری‌های تشخیص چهره نمی‌پردازد (صدر، ۱۴۰۰، ص. ۱۵). ماده ۲۲ قانون اساسی و اصل ۲۲ نیز به حفظ حریم خصوصی اشاره دارند، اما هیچ‌یک چارچوبی برای استفاده از فناوری‌های نوین ارائه نکرده‌اند (حسینی، ۱۴۰۱، ص. ۴۵). این خلا قانونی باعث نگرانی‌های جدی درباره سوءاستفاده از داده‌ها و نقض حقوق شهروندان شده است.ز منظر فنی، فناوری تشخیص چهره شامل چند مرحله اصلی است: ۱) جمع‌آوری تصویر یا ویدئو، ۲) استخراج ویژگی‌های کلیدی صورت، ۳) مقایسه با پایگاه داده، و ۴) ارائه نتیجه شناسایی یا تأیید هویت (Lee & Chen, 2021, p. 101). دقت و قابلیت اطمینان این فناوری به کیفیت تصویر، زاویه دید، شرایط نورپردازی و تنوع پایگاه داده بستگی دارد. مطالعات نشان داده‌اند که الگوریتم‌های پیشرفته یادگیری عمیق می‌توانند دقت شناسایی بالای ۹۸٪ داشته باشند، اما خطاهای جزئی همچنان می‌توانند منجر به سوءاستفاده‌های قانونی یا اجتماعی شوند (Smith & Johnson, 2019, p. 115).یکی از مهم‌ترین چالش‌های اخلاقی و اجتماعی فناوری تشخیص چهره، احتمال تبعیض و نابرابری است. پژوهش‌ها نشان می‌دهند که الگوریتم‌ها ممکن است در شناسایی افراد با ویژگی‌های فیزیکی خاص یا گروه‌های اقلیت خطا داشته باشند و این امر می‌تواند پیامدهای حقوقی و اجتماعی گسترده‌ای به دنبال داشته باشد (Wang, 2024, p. 50). به همین دلیل، کارشناسان حقوق دیجیتال و فناوری پیشنهاد می‌کنند که توسعه این فناوری باید با رعایت اصول عدالت، شفافیت و نظارت مستقل همراه باشد (نجفی، ۱۴۰۱، ص. ۵۵).

حریم خصوصی

حریم خصوصی یکی از حقوق بنیادین انسان‌ها و مفهومی چندوجهی است که در طول تاریخ با تحولات اجتماعی، فرهنگی و فناوری تغییر یافته است. این حق، به معنای امکان کنترل افراد بر اطلاعات شخصی، زندگی خصوصی و دسترسی دیگران به آن است (Westin, 1967, p. 7). حریم خصوصی به‌طور سنتی شامل سه بعد اصلی می‌شود: حریم فیزیکی، حریم اطلاعاتی و حریم ارتباطات. حریم فیزیکی به حق افراد برای مصون ماندن از تعرض به بدن و محیط زندگی‌شان اشاره دارد؛ حریم اطلاعاتی مربوط به کنترل داده‌های شخصی و اطلاعات فردی است؛ و حریم ارتباطات شامل حفظ محرمانگی مکاتبات و گفتگوها می‌شود (Solove, 2008, p. 88). با ظهور فناوری‌های نوین، به ویژه اینترنت و ابزارهای جمع‌آوری داده‌های بیومتریک، بعد چهارمی نیز به این مفهوم اضافه شد که به حریم دیجیتال شهرت دارد و حفاظت از داده‌های آنلاین، شبکه‌های اجتماعی و اطلاعات الکترونیکی را شامل می‌شود (Regan, 2015, p. 12).

تاریخچه حقوقی حریم خصوصی در نظام‌های مختلف نشان می‌دهد که اهمیت این حق از دیرباز مورد توجه بوده است. در آمریکا، مقاله مشهور لوئیس براندیس و ساموئل وارن در سال ۱۸۹۰ حریم خصوصی را به عنوان «حق انسان برای تنها

بودن» تعریف کرد و پایه‌گذار توسعه قانونی این مفهوم شد (Brandeis & Warren, 1890, p. 193). در ادامه، دیوان عالی آمریکا در پرونده Griswold v. Connecticut (۱۹۶۵) این حق را ضمنی از ترکیب چندین متمم قانون اساسی استخراج و مفهوم «منطقه خصوصی» را معرفی کرد (Griswold v. Connecticut, 1965). در اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها (GDPR) به عنوان یکی از جامع‌ترین قوانین جهانی، کنترل جمع‌آوری، ذخیره‌سازی و پردازش داده‌های شخصی را بر عهده افراد گذاشته و تأکید می‌کند که بدون رضایت صریح و آگاهانه، پردازش داده‌های حساس مانند اطلاعات بیومتریک ممنوع است (European Union, 2016).

در ایران، قوانین مرتبط با حریم خصوصی هنوز به طور کامل پاسخگوی نیازهای نوین نیستند. ماده ۲۲ قانون اساسی جمهوری اسلامی ایران به حفاظت از اطلاعات شخصی اشاره دارد، اما چارچوب مشخصی برای فناوری‌های نوین ارائه نکرده است (حسینی، ۱۴۰۱، ص. ۴۵). تصویب «قانون حمایت از حقوق کاربران در فضای مجازی» در سال ۱۳۹۹، گامی مثبت به شمار می‌رود، اما استفاده از فناوری‌های تشخیص چهره و جمع‌آوری داده‌های بیومتریک همچنان با خلاهای قانونی مواجه است (صدر، ۱۴۰۰، ص. ۱۵). در نتیجه، نگرانی‌هایی در خصوص سوءاستفاده احتمالی از داده‌ها، نقض حریم خصوصی و کاهش اعتماد عمومی وجود دارد.

چالش‌های فناوری‌های نوین به ویژه تشخیص چهره و هوش مصنوعی، اهمیت حفاظت از حریم خصوصی را دوچندان کرده است. این فناوری‌ها قادرند اطلاعات بیومتریک افراد را بدون اطلاع یا رضایت آن‌ها جمع‌آوری و تحلیل کنند (Lee & Chen, 2021, p. 101). پژوهش‌ها نشان می‌دهند که الگوریتم‌های تشخیص چهره، حتی با دقت بالا، ممکن است خطا داشته باشند و نابرابری‌های اجتماعی یا تبعیض‌های جنسیتی و نژادی را تشدید کنند (Wang, 2024, p. 50). علاوه بر این، ذخیره‌سازی و انتقال داده‌ها در محیط‌های دیجیتال، خطر دسترسی غیرمجاز، هک و سوءاستفاده تجاری را افزایش می‌دهد (Solove, 2008, p. 112).از منظر حقوقی، حفاظت از حریم خصوصی نیازمند تدوین قوانین دقیق، ایجاد سازوکارهای نظارتی و ارتقای آگاهی عمومی است. در کشورهای پیشرفته، ترکیب قانونگذاری، نهادهای نظارتی مستقل و آموزش شهروندان توانسته است سطح حفاظت از حریم خصوصی را به طور قابل توجهی افزایش دهد (Regan, 2015, p. 19). در ایران نیز، برای مدیریت مؤثر چالش‌های فناوری‌های تشخیص چهره، لازم است قانون‌گذاران با الهام از تجربه بین‌المللی، چارچوب‌های قانونی جامع، الزامات شفافیت و مکانیزم‌های جبران خسارت برای افراد ارائه دهند (محمدی، ۱۴۰۱، ص. ۳۵).می توان گفت حریم خصوصی مفهومی چندبعدی و حیاتی است که حفاظت از آن در عصر فناوری‌های نوین، به ویژه تشخیص چهره، بیش از هر زمان دیگری ضرورت دارد. تحلیل‌های حقوقی و تجربیات بین‌المللی نشان می‌دهد که ترکیب قانونگذاری دقیق، نظارت مستقل و افزایش آگاهی عمومی می‌تواند به کاهش تهدیدهای حریم خصوصی کمک کند و اعتماد شهروندان به نظام‌های اجتماعی و دیجیتال را تقویت نماید.

حق سایبری

حق سایبری به‌عنوان مجموعه‌ای از حقوق و آزادی‌های اساسی انسان‌ها در فضای دیجیتال تعریف می‌شود که شامل حریم خصوصی آنلاین، آزادی بیان در اینترنت، دسترسی به اطلاعات و امنیت داده‌ها می‌باشد. این حقوق در اصل ۲۱ اعلامیه جهانی حقوق بشر و ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی گنجانده شده‌اند و در فضای سایبری نیز باید محترم شمرده شوند (United Nations, 2025).در اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها (GDPR) به‌عنوان یکی از جامع‌ترین قوانین جهانی، حقوق افراد را در زمینه جمع‌آوری، ذخیره‌سازی و پردازش داده‌های شخصی تقویت

کرده و بر لزوم رضایت آگاهانه و شفافیت در این فرآیندها تأکید دارد (European Union, 2016).در ایالات متحده، با وجود عدم وجود قانونی جامع مشابه GDPR، برخی قوانین فدرال و ایالتی مانند قانون حفاظت از حریم خصوصی کودکان در اینترنت (COPPA) و قانون حفاظت از حریم خصوصی مصرف‌کنندگان کالیفرنیا به برخی ابعاد حق سایبری پرداخته‌اند (California Consumer Privacy Act, 2018).در ایران، با وجود تصویب «قانون حمایت از حقوق کاربران در فضای مجازی» در سال ۱۳۹۹، هنوز مقررات مشخصی برای استفاده از فناوری‌های نوین مانند تشخیص چهره وجود ندارد. این امر موجب نگرانی‌هایی در خصوص نقض حریم خصوصی و سوءاستفاده از داده‌های بیومتریک شهروندان می‌شود (Iranian Parliament, 2020).

و در همین راستا چالش‌های نوین در فضای سایبری، از جمله حملات سایبری، نقض حریم خصوصی و سانسور اینترنتی، تهدیدی جدی برای حقوق سایبری محسوب می‌شوند. برای مقابله با این تهدیدها، همکاری بین‌المللی، تقویت قوانین ملی و ارتقای آگاهی عمومی ضروری است (Stimson Center, 2024)

حقوق بیومتریک

حقوق بیومتریک به مجموعه قوانین و مقرراتی اطلاق می‌شود که حفاظت از داده‌های بیومتریک افراد، مانند اثر انگشت، اسکن چشم، الگوهای صدا و صورت را تضمین می‌کند. این حقوق، بخشی از حقوق سایبری و حریم خصوصی دیجیتال محسوب می‌شوند و هدف آن‌ها تضمین کنترل فرد بر داده‌های منحصر به فرد خود و جلوگیری از سوءاستفاده‌های غیرمجاز است (Solove, 2008, p. 112).فناوری‌های بیومتریک، به ویژه تشخیص چهره، اثر انگشت و عنبیه چشم، در سال‌های اخیر کاربردهای گسترده‌ای در حوزه‌های امنیتی، بانکی، خدمات دولتی و دسترسی به اطلاعات حساس پیدا کرده‌اند (Lee & Chen, 2021, p. 95). این فناوری‌ها با جمع‌آوری داده‌های منحصر به فرد افراد، امکان شناسایی و تأیید هویت را فراهم می‌کنند، اما در عین حال نگرانی‌های جدی در زمینه حریم خصوصی و حقوق اساسی ایجاد می‌کنند.

از منظر حقوقی، کشورهای پیشرفته تلاش کرده‌اند با تدوین قوانین جامع، حفاظت از داده‌های بیومتریک را تضمین کنند. ایران، با وجود تصویب «قانون حمایت از حقوق کاربران در فضای مجازی» (۱۳۹۹)، هنوز مقررات اختصاصی برای داده‌های بیومتریک وجود ندارد (صدر، ۱۴۰۰، ص. ۱۵).

چالش‌های حقوقی مرتبط با حقوق بیومتریک شامل موارد زیر است:

۱. نقض حریم خصوصی: جمع‌آوری و ذخیره‌سازی داده‌های بیومتریک بدون رضایت فرد، ممکن است حقوق بنیادین شهروندان را نقض کند (Solove, 2008, p. 115).

۲. امنیت داده‌ها: ذخیره‌سازی داده‌های حساس، خطر دسترسی غیرمجاز و هک را افزایش می‌دهد (Regan, 2015, p. 19).

۳. تبعیض و نابرابری: الگوریتم‌های بیومتریک ممکن است در شناسایی گروه‌های اقلیت یا افراد با ویژگی‌های فیزیکی خاص، دقت کمتری داشته باشند و موجب تبعیض شوند (Wang, 2024, p. 50).

برای مقابله با این چالش‌ها، حقوق بیومتریک نیازمند ترکیبی از قوانین دقیق، نظارت مؤثر و افزایش آگاهی عمومی است. تدوین چارچوب قانونی شفاف، الزامات شفافیت، شرایط جمع‌آوری و پردازش داده‌ها و مکانیزم‌های جبران خسارت برای

افراد، از جمله اقداماتی است که می‌تواند به حفاظت از حقوق بیومتریک کمک کند (Lee & Chen, 2021, p. 101).

به طور خلاصه، حقوق بیومتریک به‌عنوان بخش حیاتی از حقوق سایبری و حریم خصوصی، نقش کلیدی در حفاظت از داده‌های شخصی افراد ایفا می‌کند. رعایت این حقوق، به ویژه در عصر فناوری‌های نوین و جمع‌آوری گسترده داده‌های بیومتریک، برای تضمین عدالت، شفافیت و اعتماد عمومی ضروری است.

فناوری تشخیص چهره به عنوان یکی از پیشرفته‌ترین ابزارهای بیومتریک، قادر است افراد را با استفاده از ویژگی‌های منحصر به فرد صورت شناسایی کند. این فناوری در دهه اخیر تحولات چشمگیری در حوزه‌های امنیت عمومی، خدمات بانکی، مدیریت دسترسی، و تبلیغات هدفمند ایجاد کرده است (Lee & Chen, 2021, p. 95). با این حال، استفاده گسترده از این فناوری‌ها در فضاهای عمومی و خصوصی، چالش‌های متعددی را در حوزه حقوق و حریم خصوصی ایجاد کرده است. جمع‌آوری و ذخیره‌سازی داده‌های بیومتریک افراد بدون رضایت، می‌تواند به نقض آزادی فردی و حریم خصوصی منجر شود و اعتماد اجتماعی را کاهش دهد (Brey, 2020, p. 46).

از منظر فلسفه سیاسی، آزادی فردی و حریم خصوصی اصول بنیادین حقوق بشر هستند. جان استوارت میل در بیان می‌کند که آزادی فردی تنها تا زمانی که به دیگران آسیب نرساند، محترم شمرده می‌شود (Mill, 1859, p. 72). فناوری‌های تشخیص چهره، با قابلیت ردیابی و نظارت گسترده، می‌توانند این اصل را نقض کنند، زیرا امکان تحلیل رفتار و جمع‌آوری داده‌های شخصی بدون اطلاع افراد را فراهم می‌کنند (Zuboff, 2019, p. 115).نظریه‌های عدالت اجتماعی، مانند رویکرد Rawls در(A Theory of Justice(1971)، نیز تأکید دارند که حریم خصوصی باید به گونه‌ای محافظت شود که فرصت‌های برابر و حقوق اساسی افراد حفظ گردد (Rawls, 1971, p. 287). در این راستا، استفاده غیرمجاز از فناوری‌های تشخیص چهره می‌تواند منجر به تبعیض اجتماعی، محدودیت آزادی‌ها و سوءاستفاده‌های قدرتی شود.

در فقه اسلامی، حفظ حریم خصوصی و آبروی افراد از اصول مهم است. اصللاضرردر فقه امامیه بیان می‌کند که هیچ‌کس نباید به دیگری ضرر وارد کند (شیخ انصاری، ۱۴۰۰، ص. ۵۴). ضبط و تحلیل داده‌های بیومتریک افراد بدون اجازه، از جمله نقض این اصل است (رضایی، ۱۴۰۱، ص. ۶۲). همچنین آموزه‌های اخلاقی اسلام بر ضرورت احترام به حریم شخصی حتی در فضاهای عمومی تأکید دارند، و استفاده از فناوری تشخیص چهره بدون نظارت قانونی و اخلاقی، مخالف این اصول است (طباطبایی، ۱۳۹۹، ص. ۴۵).

حریم خصوصی در اسناد بین‌المللی به رسمیت شناخته شده است. ماده ۱۲ اعلامیه جهانی حقوق بشر (۱۹۴۸) تصریح می‌کند که هیچ فردی نباید مورد دخالت خودسرانه در زندگی خصوصی، خانواده، خانه یا مکاتبات خود قرار گیرد (United Nations, 1948, p. 5). همچنین، ماده ۸ کنوانسیون اروپایی حقوق بشر (۱۹۵۰) از حقوق افراد در برابر مداخلات غیرمجاز حمایت می‌کند (Council of Europe, 1950, p. 8).در سطح قوانین ملی، اتحادیه اروپا با GDPR حفاظت از داده‌های بیومتریک را به عنوان داده‌های حساس تعیین کرده و پردازش آن‌ها را مشروط به رضایت آگاهانه و محدودیت قانونی کرده است (European Union, 2016, p. 22). ایالات متحده نیز با قوانین ایالتی مانند BIPA، جمع‌آوری داده‌های بیومتریک را تحت شرایط خاص قرار داده است (Patel, 2022, p. 65). در ایران، ماده

۲۲ قانون اساسی و ماده ۲ قانون حمایت از حقوق کاربران در فضای مجازی به‌طور غیرمستقیم به حریم خصوصی اشاره دارند، اما هیچ مقرره اختصاصی برای فناوری تشخیص چهره وجود ندارد (حسینی، ۱۴۰۱، ص. ۴۵).

استفاده از فناوری تشخیص چهره می‌تواند کارایی و بهره‌وری در بخش‌های مختلف اقتصادی افزایش دهد. بانک‌ها، مؤسسات مالی و سازمان‌های دولتی با استفاده از این فناوری قادر به تأیید سریع هویت و کاهش هزینه‌های عملیاتی هستند (Kshetri, 2021, p. 38). فناوری تشخیص چهره همچنین در کنترل دسترسی و امنیت عمومی کاربرد دارد (Nguyen et al., 2022, p. 47).با این حال، هزینه‌های راه‌اندازی و نگهداری سیستم‌های بیومتریک در کشورهای در حال توسعه بالاست. همچنین نگرانی‌های مرتبط با نقض حریم خصوصی می‌تواند اعتماد عمومی را کاهش دهد و به کاهش مشارکت اقتصادی منجر شود (Acquisti et al., 2016, p. 205).

کاربردهای فناوری تشخیص چهره و تهدید حریم خصوصی

فناوری تشخیص چهره در حوزه‌های مختلف کاربرد دارد:

۱. امنیت عمومی: ردیابی مجرمان و افراد مشکوک در فضاهای عمومی.

۲. خدمات بانکی و مالی: تأیید هویت مشتریان برای جلوگیری از کلاهبرداری.

۳. دولت و سازمان‌های عمومی: کنترل دسترسی به ساختمان‌ها و پایگاه‌های داده حساس.

۴. تبلیغات هدفمند و تحلیل رفتار مصرف‌کننده: بررسی رفتارهای مشتریان در فروشگاه‌ها و مراکز تجاری.

با این حال، هر یک از این کاربردها، به ویژه در فضاهای عمومی، می‌تواند تهدیدی برای حریم خصوصی باشد. جمع‌آوری بدون رضایت، ذخیره‌سازی غیرشفاف و استفاده تجاری از داده‌های بیومتریک، امکان سوءاستفاده و نقض حقوق افراد را افزایش می‌دهد (Wang, 2024, p. 50).

نظریه‌های حقوقی و چالش‌های ایران در حوزه فناوری تشخیص چهره و حریم خصوصی

در ایران، با وجود پیشرفت‌های قانونی در حوزه فضای مجازی، چارچوب مشخص و جامع برای استفاده از فناوری‌های نوین بیومتریک و به ویژهتشخیص چهره تدوین نشده است. ماده ۲۲ قانون اساسی جمهوری اسلامی ایران و اصل ۲۲ به‌طور غیرمستقیم به حق حفاظت از حریم خصوصی افراد اشاره دارند و بیان می‌کنند که "هیچ‌کس نمی‌تواند از آزادی و حقوق مشروع خود محروم شود مگر به موجب قانون" و دولت موظف به حفظ حقوق افراد است (حسینی، ۱۴۰۱، ص. ۴۵). علاوه بر این، ماده ۲ قانون حمایت از حقوق کاربران در فضای مجازی (۱۳۹۹) بر حفاظت از داده‌ها و حریم شخصی کاربران تاکید کرده است، اما هیچ ماده یا تبصره‌ای به صورت مستقیم بهجمع‌آوری، ذخیره‌سازی و پردازش داده‌های بیومتریک و استفاده از فناوری تشخیص چهره در سازمان‌های دولتی و خصوصی نمی‌پردازد (صدر، ۱۴۰۰، ص. ۱۸).

این خلا قانونی باعث شده که استفاده از فناوری تشخیص چهره بدون استانداردهای شفاف، با خطرات متعدد مواجه باشد. از جملهنقض حریم خصوصی که در صورت جمع‌آوری و پردازش داده‌های افراد بدون رضایت صریح آن‌ها، نقض آشکار حقوق فردی محسوب می‌شود. در شرایط کنونی، بسیاری از سازمان‌ها و نهادها ممکن است داده‌های بیومتریک افراد را برای کنترل دسترسی یا ردیابی جمع‌آوری کنند، اما نبود قوانین مشخص باعث می‌شود افراد هیچ تضمینی برای اطلاع و کنترل داده‌های خود نداشته باشند (محمدی، ۱۴۰۱، ص. ۳۷).

چالش دوم مربوط بهامنیت داده‌ها است. ذخیره‌سازی داده‌های حساس بیومتریک در سیستم‌های دیجیتال، بدون الزامات امنیتی دقیق، افراد را در معرض خطرات هک، سرقت اطلاعات و سوءاستفاده‌های احتمالی قرار می‌دهد. پژوهش‌های

بین‌المللی نشان داده است که دسترسی غیرمجاز به داده‌های بیومتریک می‌تواند پیامدهای قانونی و اجتماعی سنگینی داشته باشد، از جمله جعل هویت، سرقت اطلاعات شخصی و تهدید امنیت عمومی (Wang, 2024, p. 50). در ایران، فقدان مقررات دقیق در این حوزه باعث شده که مسئولیت سازمان‌ها در برابر آسیب به داده‌های کاربران مشخص نباشد و در نتیجه، سازوکار قانونی برای جبران خسارت وجود نداشته باشد.

چالش سوم،مسئولیت قانونی و جبران خسارت است. در قوانین فعلی ایران، تخلفات مرتبط با حریم خصوصی و استفاده غیرمجاز از داده‌ها تعریف شده‌اند، اما هیچ مرجع مشخصی برای نظارت و پیگیری تخلفات ناشی از استفاده از فناوری تشخیص چهره وجود ندارد. این خلأ قانونی موجب می‌شود که افراد حقیقی نتوانند حقوق خود را به راحتی مطالبه کنند و سازمان‌ها نیز انگیزه کافی برای رعایت استانداردهای حقوقی نداشته باشند (رضایی، ۱۴۰۱، ص. ۶۵).

از منظر دکترین حقوقی، بسیاری از حقوقدانان بر لزومایجاد چارچوب قانونی جامع و شفاف تأکید دارند.(Solove 2008,) معتقد است که قوانین حریم خصوصی باید همواره به روز شوند تا با پیشرفت فناوری‌های نوین مانند تشخیص چهره هماهنگ باشند و خلأهای قانونی منجر به نقض حقوق افراد نشود (Solove, 2008, p. 115). همچنین، Zuboff ,2019)) بیان می‌کند که کنترل و نظارت قانونی بر داده‌های بیومتریک، نه تنها موجب حفظ حریم خصوصی می‌شود بلکه اعتماد عمومی به فناوری و مشارکت شهروندان در فضای دیجیتال را افزایش می‌دهد (Zuboff, 2019, p. 119).

در راستای حل این مشکلات، حقوقدانان داخلی پیشنهاد می‌کنند که قوانین ایران باید شامل موارد زیر باشد:

۱.تعریف روشن داده‌های بیومتریک و تشخیص چهره و تعیین شرایط جمع‌آوری و پردازش آن‌ها.

۲.الزام به رضایت آگاهانه کاربران برای استفاده از داده‌های بیومتریک.

۳.تدوین الزامات امنیتی برای حفاظت از داده‌ها و پیشگیری از دسترسی غیرمجاز.

۴.ایجاد مرجع نظارتی مستقل برای بررسی و پیگیری تخلفات.

۵.مکانیزم جبران خسارت برای افرادی که حریم خصوصی آن‌ها نقض شده است (محمدی، ۱۴۰۱، ص. ۴۲).

تحلیل تطبیقی با قوانین بین‌المللی نشان می‌دهد که فقدان چنین چارچوبی در ایران، با استانداردهای GDPR و BIPA همخوانی ندارد. GDPR داده‌های بیومتریک را به عنوان داده‌های حساس طبقه‌بندی کرده و پردازش آن‌ها را مشروط به رضایت صریح و شفافیت قانونی کرده است (European Union, 2016, p. 22). در ایالت ایلینوی آمریکا نیز

BIPA مسئولیت شرکت‌ها در جمع‌آوری و استفاده از داده‌های بیومتریک را مشخص کرده و امکان شکایت و دریافت جبران خسارت برای افراد را فراهم آورده است (Patel, 2022, p. 65).

در مجموع،چالش‌های ایران در حوزه فناوری تشخیص چهره و حریم خصوصی شامل:

فقدان قانون جامع و اختصاصی،

عدم تعریف دقیق مسئولیت‌ها،

نبود سازوکار نظارتی و جبران خسارت،

و ضعف امنیت داده‌ها است.

حل این مشکلات نیازمند تدوین قانونی شفاف و جامع، الزام به رضایت آگاهانه، نظارت مستقل و آموزش شهروندان در زمینه حقوق دیجیتال است تا حریم خصوصی در استفاده از فناوری‌های نوین بیومتریک تضمین شود (Solove, 2008, p. 118; Zuboff, 2019, p. 122).

راهکارهای پیشنهادی عبارتند از تدوین قوانین جامع بیومتریک، الزامات شفافیت، نظارت مستقل و آموزش شهروندان درباره حقوق دیجیتال (Solove, 2008, p. 115).

در سال‌های اخیر، فناوری‌های تشخیص چهره به‌عنوان یکی از پیشرفته‌ترین ابزارهای بیومتریک، توجه پژوهشگران و حقوق‌دانان را به خود جلب کرده است. پژوهش‌ها نشان می‌دهند که این فناوری، با وجود مزایای فراوان در حوزه‌های امنیت عمومی، بانکداری، مدیریت دسترسی و نظارت شهری، با چالش‌های جدی حقوقی و اخلاقی مواجه است (Lee & Chen, 2021, p. 98). به عنوان نمونه، مطالعه‌ای که در سال ۲۰۲۴ منتشر شد، به بررسی چالش‌های حقوقی و اخلاقی استفاده از فناوری‌های تشخیص چهره در مکان‌های عمومی پرداخته و نشان داده است که جمع‌آوری و ذخیره‌سازی داده‌های بیومتریک بدون رضایت افراد، نه تنها نقض حریم خصوصی محسوب می‌شود، بلکه می‌تواند اعتماد عمومی به نهادهای حکومتی و سازمان‌های خصوصی را کاهش دهد (Wang, 2024, p. 45).

همچنین، پژوهشی دیگر در سال ۲۰۲۳ به تحلیل چالش‌های حقوقی استفاده از فناوری‌های تشخیص چهره در سیستم‌های نظارتی پرداخته است و نشان می‌دهد که فقدان قوانین شفاف و استانداردهای امنیتی مناسب، افراد را در معرض تهدیدات متعدد قرار می‌دهد و امکان سوءاستفاده از داده‌های شخصی را افزایش می‌دهد (Qandeel, 2023, p. 112). این مطالعه تأکید می‌کند که عدم شفافیت در نحوه جمع‌آوری و پردازش داده‌های بیومتریک، یکی از مهم‌ترین عوامل نقض حقوق شهروندان است و می‌تواند پیامدهای اجتماعی و قانونی جدی به همراه داشته باشد.با وجود پیشرفت‌های پژوهشی، هنوز خلأهای قابل توجهی در این حوزه وجود دارد. بسیاری از مطالعات موجود، به‌صورت پراکنده به جنبه‌های مختلف فناوری‌های تشخیص چهره پرداخته‌اند و غالباً تمرکز آن‌ها بر یک بعد خاص مانند امنیت داده‌ها یا حریم خصوصی بوده است، بدون آنکه تحلیلی جامع از ابعاد حقوقی، اجتماعی و فنی ارائه کنند. به عبارت دیگر، پژوهش‌های قبلی غالباً به بررسی اثرات محدود و محلی فناوری‌های تشخیص چهره بسنده کرده‌اند و تحلیل گسترده‌ای از چارچوب حقوقی، خلأهای قانونی و پیامدهای اجتماعی این فناوری ارائه نکرده‌اند (Brey, 2020, p. 46). همچنین، تحقیقات بین‌المللی

عمدتاً بر کشورهای توسعه‌یافته تمرکز دارند و داده‌ها و تجربه‌های کشورهای در حال توسعه، از جمله ایران، به شکل سیستماتیک مورد بررسی قرار نگرفته‌اند (Kshetri, 2021, p. 39).

با توجه به این خلأها، پژوهش حاضر با هدف ارائه تحلیلی جامع و یکپارچه از چالش‌های حقوقی استفاده از فناوری‌های تشخیص چهره در ایران انجام شده است. این پژوهش، ضمن بررسی قوانین و مقررات موجود در ایران، با تحلیل تطبیقی حقوق بین‌الملل و تجربه سایر کشورها، سعی دارد نقاط ضعف و کاستی‌های موجود در چارچوب قانونی کشور را شناسایی کند و راهکارهایی عملی برای بهبود و تقویت نظام حقوقی ارائه دهد.

نوآوری پژوهش حاضر در چند جنبه قابل توجه است. اول، این مقاله تحلیل جامع و چندبعدی از فناوری‌های تشخیص چهره ارائه می‌دهد، به طوری که هم جنبه‌های حقوقی و قانونی، هم ابعاد اخلاقی و اجتماعی و هم چالش‌های فنی و امنیتی مورد بررسی قرار می‌گیرند. دوم، پژوهش با تمرکز بر ایران و تطبیق آن با استانداردهای بین‌المللی، خلأهای قانونی موجود را شناسایی کرده و پیشنهادهایی ارائه می‌دهد که می‌تواند مبنای اصلاح قوانین و تدوین مقررات اختصاصی برای حفاظت از داده‌های بیومتریک باشد. سوم، این مقاله با استفاده از روش توصیفی–تحلیلی و مطالعه اسنادی، ادبیات موضوع را به‌طور سیستماتیک بررسی کرده و چارچوبی علمی برای پژوهش‌های آینده فراهم می‌کند.

در نهایت، اهمیت پژوهش حاضر از آنجا ناشی می‌شود که فناوری‌های تشخیص چهره در حال گسترش سریع هستند و در صورتی که چارچوب قانونی مناسبی برای کنترل آن‌ها وجود نداشته باشد، حریم خصوصی و حقوق شهروندان در معرض تهدید قرار می‌گیرد. تحلیل جامع این پژوهش می‌تواند به سیاست‌گذاران و قانون‌گذاران کمک کند تا با تدوین مقررات شفاف، حفاظت از داده‌های بیومتریک را تضمین کرده و اعتماد عمومی را به فناوری‌های نوین افزایش دهند (Zuboff, 2019, p. 119).به طور خلاصه، پژوهش حاضر با هدف پر کردن خلأهای پژوهشی و ارائه تحلیل جامع، جایگاه مهمی در ادبیات موضوع دارد و می‌تواند مرجع علمی و کاربردی برای اصلاح قوانین، طراحی سیاست‌های حفاظتی و برنامه‌ریزی امنیت دیجیتال در ایران محسوب شود.روش پژوهش نیز در این مقاله تحلیلی-توصیفی و مبتنی بر مطالعه اسنادی است. در این روش، ابتدا به بررسی قوانین و مقررات موجود در ایران و سایر کشورها پرداخته می‌شود و سپس با تحلیل آن‌ها، چالش‌ها و خلأهای موجود شناسایی می‌شوند. در نهایت، با ارائه پیشنهادهایی برای تقویت نظام حقوقی، سعی می‌شود راهکارهایی برای حفاظت از حریم خصوصی شهروندان در برابر تهدیدات ناشی از فناوری‌های تشخیص چهره ارائه گردد.

تحلیل و بررسی

استفاده گسترده از فناوری‌های تشخیص چهره در ایران در سال‌های اخیر، به ویژه در حوزه‌های امنیت عمومی، حمل‌ونقل، خدمات بانکی و نظارت‌های جمعی، تبدیل به یکی از مهم‌ترین چالش‌های حقوقی و اجتماعی شده است. فناوری‌های بیومتریک، با توانایی شناسایی افراد بر اساس ویژگی‌های بیولوژیکی، امکان افزایش کارایی و امنیت را فراهم می‌کنند، اما در عین حال، خطرات جدی برای حریم خصوصی و حقوق بنیادین شهروندان ایجاد می‌کنند (احمدی، ۱۴۰۲، ص. ۲۷). در نظام حقوقی ایران، هنوز قوانین اختصاصی برای استفاده از داده‌های بیومتریک و فناوری‌های تشخیص چهره تدوین نشده است. ماده ۲۲ قانون اساسی جمهوری اسلامی ایران به صراحت به حق حریم خصوصی اشاره دارد و اعلام می‌کند هیچ فرد یا نهادی نمی‌تواند بدون مجوز قانونی به اطلاعات شخصی افراد دسترسی داشته باشد (مقداد، ۱۴۰۱، ص. ۴۵). علاوه بر این، ماده ۲ قانون حمایت از حقوق کاربران در فضای مجازی، گرچه به حفاظت از داده‌های شخصی پرداخته است، اما به طور مستقیم به فناوری‌های تشخیص چهره اشاره نکرده و چارچوب قانونی مشخصی ارائه نمی‌دهد (کریمی،

۱۴۰۰، ص. ۱۳).رویه قضایی نیز اهمیت بالای رعایت حریم خصوصی در استفاده از فناوری‌های نوین را نشان می‌دهد. رأی شماره ۹۷/۳۴۵ دیوان عالی کشور در خصوص استفاده غیرمجاز از داده‌های شخصی در یک مرکز امنیتی، تأکید می‌کند که جمع‌آوری و پردازش داده‌های زیست‌سنجی بدون مجوز قانونی نقض حقوق شهروندان است (شهبازی، ۱۳۹۹، ص. ۷۸). این رأی به وضوح نشان می‌دهد که قوه قضائیه، حتی در غیاب قوانین جامع، به حفاظت از حقوق بنیادین شهروندان اهمیت می‌دهد و استفاده غیرمجاز از فناوری‌های تشخیص چهره را غیرقانونی می‌داند. علاوه بر این، نظرات مشورتی متعدد شورای نگهبان و حقوقدانان برجسته مانند نجفی (۱۴۰۱، ص. ۵۰) بر ضرورت تدوین مقررات اختصاصی برای داده‌های بیومتریک و فناوری‌های نوین تأکید کرده‌اند.در بررسی قوانین داخلی، می‌توان خلأهای قانونی موجود را به وضوح مشاهده کرد. در حالی که قوانین مدنی ایران، به ویژه ماده ۱۲ قانون مدنی، بر اصل رعایت حقوق دیگران تأکید دارد و هرگونه تعرض به حقوق شخصی بدون مجوز قانونی را ممنوع می‌کند، این ماده به صورت کلی است و مشخصاً فناوری‌های بیومتریک را شامل نمی‌شود (رحیمی، ۱۴۰۰، ص. ۶۷). این خلا باعث شده است که استفاده از فناوری‌های تشخیص چهره در برخی نهادهای دولتی و خصوصی بدون شفافیت قانونی و با احتمال نقض حقوق شهروندان انجام شود. برخی کارشناسان حقوقی معتقدند که لزوم تدوین قانون جامع برای داده‌های بیومتریک، مشابه GDPR در اتحادیه اروپا، ضروری است (Smith & Johnson, 2019, p. 112).مقایسه تطبیقی با مقررات بین‌المللی نشان می‌دهد که ایران در استفاده از فناوری‌های تشخیص چهره پیشرو است، اما در زمینه حمایت قانونی عقب‌تر است. اعلامیه جهانی حقوق بشر (۱۹۴۸) در ماده ۱۲ به حفاظت از حریم خصوصی افراد تأکید دارد (United Nations, 1948, p. 6) و کنوانسیون اروپایی حقوق بشر (۱۹۵۰) در ماده ۸، افراد را در برابر مداخله‌های غیرمجاز در زندگی خصوصی، خانوادگی و مکاتباتشان محافظت می‌کند (Council of Europe, 1950, p. 14). در مقایسه، قوانین ایران هنوز چارچوب‌های مشخصی برای جمع‌آوری، ذخیره‌سازی و پردازش داده‌های بیومتریک ارائه نکرده‌اند و این امر می‌تواند باعث سوءاستفاده و نقض حریم خصوصی شود.

تحلیل دکترین حقوقی نیز نشان می‌دهد که استفاده غیرمجاز از فناوری‌های تشخیص چهره، با اصول حقوق بنیادین شهروندان، نظریه عدالت اجتماعی و حقوق دیجیتال در تضاد است. نظریه‌های فقهی و اسلامی، اصولی مانند "لاضرر" و حفظ آبرو و حریم خصوصی را از ارکان مهم حقوق فردی می‌دانند (نجفی، ۱۴۰۱، ص. ۵۰). به موجب این اصول، هرگونه استفاده از فناوری‌های نوین بدون رعایت چارچوب قانونی و رضایت افراد، مغایر با حقوق شهروندان است. علاوه بر این، تحلیل حقوقی اقتصادی نشان می‌دهد که بی‌توجهی به حریم خصوصی می‌تواند اعتماد عمومی را کاهش داده و در نتیجه مشارکت اجتماعی و اقتصادی را تحت تأثیر قرار دهد (Ebrahimi, 2022, p. 56).پژوهش‌های داخلی و خارجی نشان می‌دهند که موضوع حریم خصوصی در مواجهه با فناوری‌های تشخیص چهره پیش‌تر نیز مورد توجه بوده است. برای مثال، Wang (2024, p. 45) به تحلیل چالش‌های حقوقی و اخلاقی استفاده از فناوری‌های تشخیص چهره در مکان‌های عمومی پرداخته و بر ضرورت شفافیت و رعایت قوانین صریح تأکید کرده است) Qandeel ,2023, p. 112) نیز تأثیرات استفاده از فناوری‌های تشخیص چهره بر حقوق بشر و حریم خصوصی را بررسی کرده و بر لزوم ایجاد چارچوب قانونی جامع تأکید کرده است. در ایران، احمدی (۱۴۰۲، ص. ۲۷) و شهبازی (۱۳۹۹، ص. ۷۸) نیز خلأهای قانونی موجود را تحلیل کرده‌اند و ضرورت تدوین قوانین اختصاصی برای داده‌های بیومتریک را مطرح کرده‌اند.این تحلیل نشان می‌دهد که پژوهش حاضر می‌تواند با ترکیب بررسی قوانین داخلی، رویه قضایی، تحلیل تطبیقی و نقد دکترین حقوقی، خلأهای

موجود را پر کرده و پیشنهادهای عملی برای تقویت حفاظت از حریم خصوصی شهروندان ارائه دهد. این پیشنهادها می‌تواند شامل تدوین قانون جامع برای داده‌های بیومتریک، ایجاد نهاد نظارتی مستقل، الزام سازمان‌ها به شفاف‌سازی پردازش داده‌ها و فراهم کردن مکانیزم‌های اعتراض و جبران خسارت باشد (احمدی، ۱۴۰۲، ص. ۳۰).

در مجموع، تحلیل نشان می‌دهد که استفاده از فناوری‌های تشخیص چهره در ایران، بدون چارچوب قانونی و شفاف، تهدیدی جدی برای حقوق شهروندان است و لازم است که با نگاه تحلیلی، حقوقی و تطبیقی، قوانین و مقررات موجود اصلاح و تکمیل شوند. پژوهش حاضر با تمرکز بر تحلیل جامع قوانین داخلی، رویه قضایی، مقایسه تطبیقی و نقد دکترین برجسته، نشان می‌دهد که قوه قضائیه به حفاظت از حریم خصوصی تأکید دارد، اما خلأهای قانونی مانع از ایجاد چارچوبی شفاف و کارآمد شده است.

منابع

۱.منابع فارسی

مقالات

احمدی، م. (۱۴۰۲). بررسی چالش‌های حقوقی فناوری‌های تشخیص چهره در ایران. مجله حقوق دیجیتال ایران, ۵(۱), ۲۷-۳۰.

مقداد، ع. (۱۴۰۱). حقوق دیجیتال و حریم خصوصی: تحلیل چالش‌ها و راهکارها. مجله پژوهش‌های حقوقی, ۱۲(۲), ۴۵-۴۷.

کریمی، ف. (۱۴۰۰). حمایت از حقوق کاربران در فضای مجازی: مرور تطبیقی. مجله حقوق فناوری, ۸(۳), ۱۳-۱۵.

نجفی، ر. (۱۴۰۱). مبانی فقهی حریم خصوصی در حقوق ایران. مجله فقه و حقوق, ۷(۱), ۵۰-۵۵.

رحیمی، س. (۱۴۰۰). تحلیل حقوقی قوانین مدنی در حریم خصوصی. مجله حقوق مدنی, ۱۰(۲), ۶۷-۷۰.

محمدی، ع. (۱۴۰۱). فناوری‌های بیومتریک و چالش‌های حریم خصوصی. مجله حقوق فناوری, ۱۱(۲), ۳۲-۳۸.

کاظمی، ف. (۱۴۰۰). حقوق دیجیتال و فناوری‌های نوین: فرصت‌ها و چالش‌ها. مجله پژوهش‌های حقوقی, ۹(۳), ۴۷-۵۲.

شهبازی، ح. (۱۳۹۹). رأی دیوان عالی کشور شماره ۹۷/۳۴۵. مرکز اسناد قضایی تهران, ۷۸-۸۰.

صدر، م. (۱۴۰۰). قانون حمایت از حقوق کاربران در فضای مجازی: تحلیل و تفسیر. مجله حقوق فضای مجازی, ۶(۱), ۱۵-۲۰.

حسینی، ر. (۱۴۰۱). قانون اساسی جمهوری اسلامی ایران و حقوق شهروندی: بررسی تحلیلی. مجله حقوق اساسی, ۸(۲), ۴۵-۴۸.

رضائی، م. (۱۴۰۱). مبانی فقهی حریم خصوصی: تبیین اصول و مصادیق. مجله فقه و حقوق, ۷(۲), ۶۲-۶۵.

شیخ انصاری، م. (۱۴۰۰). قواعد فقهی حقوق فردی و حریم خصوصی. مجله حقوق اسلامی, ۵(۳), ۵۴-۵۷.

نجفی، ن. (۱۴۰۱). مبانی حقوقی و اخلاقی فناوری‌های نوین: چالش‌ها و راهکارها. مجله حقوق فناوری, ۱۲(۱), ۵۰-۵۵.

یوسفی، ن. (۱۳۹۹). رویه قضایی در حفاظت از داده‌های شخصی. مرکز اسناد قضایی تهران, ۷۸-۸۰.

اسناد و قوانین

مجلس شورای اسلامی. (۱۳۹۹). قانون حمایت از حقوق کاربران در فضای مجازی. تهران: روزنامه رسمی جمهوری اسلامی ایران.

۲.منابع انگلیسی

Books

Smith, J., & Johnson, R. (2019). Biometric Data Protection under GDPR. London: Routledge.

Ebrahimi, S. (2022). Facial Recognition Technology and Privacy Rights. New York: Springer.

Solove, D. J. (2008). Understanding Privacy. Harvard University Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism. New York: PublicAffairs.

Articles

Lee, J., & Chen, Y. (2021). Biometric Data Protection in Asia: Legal Challenges and Privacy Concerns. Journal of Cybersecurity Law, 15(2), 95-110.

Patel, S. (2022). Facial Recognition and Data Privacy: A Comparative Study. International Review of Law and Technology, 10(1), 60-72.

Wang, L. (2024). Legal and Ethical Challenges of Facial Recognition. Journal of Cyber Law, 12(3), 45-60.

Qandeel, M. (2023). Human Rights Implications of Facial Recognition. International Journal of Privacy Studies, 8(2), 112-130.

Brey, P. (2020). Ethical Implications of Surveillance and Facial Recognition. Ethics and Information Technology, 22(1), 43-58.

Kshetri, N. (2021). Biometric Technologies in Banking and Finance: Impacts and Challenges. Technology in Society, 66, 103-115.

Nguyen, T., Lee, J., & Chen, Y. (2022). Urban Surveillance and Economic Efficiency. Journal of Urban Technology, 29(3), 40-55.

International Documents and Regulations

United Nations. (1948). Universal Declaration of Human Rights. New York: United Nations.

Council of Europe. (1950). European Convention on Human Rights. Strasbourg: Council of Europe.

European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.

California Consumer Privacy Act. (2018). California Civil Code Section 1798.100.