



Police Biometric Surveillance and the Right to Privacy in Light of European Case Law: Implications for the Iranian Legal System

Abbas Shiri^{*1}, Ali Afrasiyabi², Mohammadreza Baregar³

1. Associate Professor, Faculty of Law and Political Sciences, University of Tehran, Tehran, Iran. (Corresponding Author)

2. Department of Criminal Law and Criminology, Amin University of Police Sciences, Tehran, Iran.

3. Ph.D Student of Criminal Law and Criminology, University of Tehran, Tehran, Iran. .

ARTICLE INFORMATION

Type of Article: Original Research

Pages: 161-176

Corresponding Author's Info

ORCID: 0000-0001-8052-2607

TELL: +989121187100

Email: ashiri@ut.ac.ir

Article history:

Received: 07 Apr 2026

Revised: 13 Jun 2026

Accepted: 15 Jun 2026

Published online: 22 Jun 2026

Keywords:

Facial Recognition, Biometric Surveillance, Privacy, European Case Law, Artificial Intelligence.

ABSTRACT

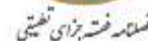
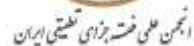
Police forces in a number of countries have deployed AI-based facial recognition technology in publicly accessible spaces, and the Iranian police likewise intend to make use of this technology. Employing a descriptive-analytical method and drawing on documentary sources, the present article seeks to answer the following question: on what reasoning has European case law treated police biometric surveillance as an interference with the right to privacy, and — on the basis of that same reasoning — what criteria must the legal basis authorizing such surveillance satisfy if it is not to result in a violation of citizens' rights? The first finding is that such surveillance, insofar as it entails the automated capture and processing of the facial data of all passers-by, suspects and non-suspects alike, without their knowledge or consent, constitutes an interference with the right to privacy and cannot be equated with ordinary police observation in public places. The second finding is that European judicial and legislative practice has formulated a set of constraints governing the basis for such interference, including: satisfying the "quality of law" requirement; limiting police discretion in determining the persons and locations placed under surveillance; exhaustive specification of permissible purposes; regulated data retention; prohibition of indiscriminate mass collection; prior authorization by a judicial authority; and independent institutional oversight. The implication of these criteria for the Iranian police is that the legitimacy of deploying this technology requires a specific legislative basis incorporating the safeguards outlined above.



This is an open access article under the CC BY license.

© 2026 The Authors.

How to Cite This Article: Shiri, A; Afrasiyabi, A & Baregar, M (2026). "Police Biometric Surveillance and the Right to Privacy in Light of European Case Law: Implications for the Iranian Legal System". *Journal of Comparative Criminal Jurisprudence*, 6(2): 161-176.



مقدمه

نظام‌های پلیسی در نیم‌قرن اخیر مسیری پیموده‌اند که از گشت‌زنی واکنشی و تحقیقات پسینی آغاز شد و به الگوهای پیشگیرانه و داده‌محور انجامید؛ پژوهشگران با نشان دادن اثر اندک راهبردهای واکنشی بر نرخ جرم، زمینه چرخش به سوی پلیسی مبتنی بر شواهد و متمرکز بر کانون‌های جرم‌خیز را فراهم آوردند (Brayne, 2017: 981) و هوش مصنوعی نیز، به اقتضای توانایی‌اش در تحلیل داده‌های انبوه، در امتداد همین چرخش به ابزار مرجع نهادهای انتظامی بدل شد. بدین‌سان دامنه بهره‌برداری از این فناوری از تحلیل الگوهای جرم به شناسایی اشخاص تسری یافت و سامانه‌های تشخیص چهره که هویت افراد را از رهگذر تطبیق الگوی بیومتریک چهره با فهرست‌های از پیش تعیین‌شده احراز می‌کنند، در شمار ابزارهای متعارف پلیس در ایالات‌متحده، اروپا و چین درآمد. جمهوری اسلامی ایران نیز از این تحول برکنار نمانده است، چه اینکه فرمانده انتظامی کشور در سال از تمایل پلیس بر به‌کارگیری فناوری تشخیص چهره در شناسایی مرتکبان جرائم خبر داده و سند ملی هوش مصنوعی نیز توسعه کاربردهای این فناوری را در زمره اهداف کلان نظام حکمرانی نشانده است و البته که همان سند «رعایت حریم خصوصی» را از جمله اصول و مبانی ارزشی خود قرار داده است (سند ملی هوش مصنوعی جمهوری اسلامی ایران، ۱۴۰۳: بند هشتم ماده ۲). با این وصف، استفاده از این روش نظارتی از منظر حقوقی پرسشی مبنایی در پی دارد که پاسخ آن در نظم حقوقی کنونی ایران روشن نیست.

خاستگاه این پرسش آن است که تصویر چهره انسان، بر خلاف تصور رایج که آن را داده‌ای در معرض دید و لذا بی‌حریم می‌انگارد، داده‌ای شخصی است و پردازش خودکار آن به‌وسیله سامانه تشخیص چهره نیز پردازش داده شخصی به‌شمار می‌آید و از این‌رو جز با وجود توجیهی قانونی روا نیست (Buckley & Hunter, 2011: 639). حساسیت این توجیه آنگاه دوچندان می‌شود که به یاد آوریم فناوری‌های داده‌محور مرز میان قلمرو عمومی و خصوصی زندگی شهروندان را چنان

کم‌رنگ ساخته و ظرفیت تعقیب، پروفایل‌سازی و بازشناسی افراد را چندان گسترانده‌اند که برخی پژوهشگران وضع کنونی را عصر پوچ‌گرایی حریم خصوصی خوانده‌اند (Manheim & Kaplan, 2019: 119). وانگهی شناسایی بیومتریک در معابر عمومی، به خلاف دوربین نظارتی متعارف که ناظری منفعل بیش نیست، هر عابر را بالقوه موضوع یک عملیات احراز هویت قرار می‌دهد، بی‌آنکه وی مظنون به ارتکاب جرمی باشد یا از این پردازش آگاهی یابد. صحت این تمایز و آثار حقوقی مترتب بر آن، خود از مسائلی است که در این نوشتار در پرتو رویه قضایی سنجیده خواهد شد؛ لکن همین اندازه پیداست که اگر چنین تمایزی پذیرفته شود، سخن از مداخله‌ای در حق‌های بنیادین در میان خواهد بود و در قانون اساسی ایران، مداخله در این حق‌ها جز «به حکم قانون» روا نیست. بهره‌برداری از فناوری‌های نظارتی مبتنی بر هوش مصنوعی بدون نظارت و چارچوب قانونی متناسب، مستعد آن دانسته شده است که به سوءاستفاده گسترده و نقض آزادی‌های فردی بینجامد (ظفریان و همکاران، ۱۴۰۴: ۵۰). بدین قرار، مسأله این پژوهش آن نیست که آیا پلیس اساساً می‌تواند از فناوری تشخیص چهره بهره‌گیرد یا نه، بلکه واکاوی شرایط و الزامات این بهره‌برداری بدون خدشه در حق بر حریم خصوصی است.

پیش از ورود به بحث، تحدید دقیق موضوع ضروری است، چه اینکه فناوری تشخیص چهره کاربردهایی متنوع دارد که آثار حقوقی یکسانی بر آن‌ها مترتب نیست. آنچه در این نوشتار «پایش بیومتریک پلیسی» خوانده می‌شود، ناظر بر عملیاتی است که قانون هوش مصنوعی اتحادیه اروپا از آن به «شناسایی بیومتریک از راه دور به اغراض انتظامی» تعبیر می‌کند و ارکان آن را تعریف کرده است. از منظر این قانون شناسایی بیومتریک، یعنی بازشناسی خودکار ویژگی‌های شخص به منظور احراز هویت او از رهگذر تطبیق داده بیومتریکش با داده اشخاص ذخیره‌شده در یک پایگاه داده؛ وصف «از راه دور»، یعنی وقوع این شناسایی بدون مشارکت فعال شخص و نوعاً از فاصله؛ و «فضای در دسترس عموم»، یعنی هر مکانی که شمار نامعینی از اشخاص بدان دسترسی

را که رویه قضایی اروپایی برای سنجش مشروعیت چنین مداخله‌ای صورت‌بندی کرده است — از «کیفیت قانون» و تحدید صلاح‌دید پلیسی تا ضرورت، تناسب و منع گردآوری انبوه — استخراج می‌کند و نشان می‌دهد که این ضوابط سرانجام در قانون هوش مصنوعی اتحادیه اروپا متبلور شده‌اند.

۱- مبانی حق بر حریم خصوصی در نظام حقوقی ایران

سنجش هرگونه مداخله در حق بر حریم خصوصی، در گرو آن است که مشخص شود این حق در نظام حقوقی بر چه پایه‌هایی بنا شده است؛ چراکه معیارهای برآمده از رویه‌های بیگانه، تنها زمانی برای تحلیل کارآمد خواهند بود که نسبت آن‌ها با مبانی درونی نظام حقوقی میزبان روشن باشد. ازاین‌رو، مبحث حاضر پیش از ورود به تجربه اروپایی، مبانی حمایت از حریم خصوصی در حقوق ایران و همچنین منطق حاکم بر استثنائات آن را واکاوی می‌کند تا در پرتو همین مبانی، ماهیت مداخله‌گرانه پایش بیومتریک و اقتضائات تجویز آن ارزیابی شود.

در اندیشه اسلامی از منظر عقلی، فراهم شدن موجبات امنیت و آسایش نوع انسان مستقیماً در گرو مراعات حریم شخصی و منع تجسس است، چه اینکه انسان‌ها ذاتاً به خلوتی نیاز دارند که منحصرأ متعلق به خودشان باشد و هرگونه ورود غیرمجاز و افشای اطلاعات افراد، نوعی برتری‌جویی و تصرف در امور دیگران تلقی می‌گردد که عقل سلیم آن را مصداق ظلم و در نتیجه مذموم می‌شمارد (محسنی و میرعماد، ۱۳۹۸: ۲۷۰). در امتداد همین حکم عقل، متون و منابع اسلامی نیز حمایت از حریم خصوصی را مبتنی بر لزوم پاسداشت کرامت انسانی که اختصاص به گروهی خاص نداشته و تمام نسل بشر را در برمی‌گیرد، دانسته‌اند. این حمایت با لزوم امانت‌داری و حفظ اسرار پیوند می‌خورد، چنان‌که در منابع فقهی به‌شدت نسبت به افشای سخنان پنهانی و تبعات آن هشدار داده شده است. بر پایه همین مبانی است که حق خلوت یا حق داشتن زندگی خصوصی از حقوق اساسی شهروندان شمرده شده؛ و در منابع اسلامی نیز، از رهگذر ممنوعیت ورود به خلوت اشخاص و منع تجسس در امور دیگران، مورد تأکید است (ساریخانی، ۱۳۹۷: ۲۳۴).

در نظام حقوقی ایران، اصل بیست‌ودوم قانون اساسی حیثیت،

دارند، صرف‌نظر از عمومی یا خصوصی بودن مالکیت آن و صرف‌نظر از وجود شروط ورود (Artificial Intelligence Act, 2024, Art. 3, paras. 35, 41, 44). بر پایه همین تعریف اخیر، نه‌تنها معابر، بلکه ایستگاه‌های حمل‌ونقل، مراکز خرید و اماکن برگزاری اجتماعات نیز در قلمرو بحث می‌گنجند.

بر این پایه، نوشتار حاضر با روش توصیفی-تحلیلی و با تکیه بر منابع اسنادی، در پی پاسخ به پرسشی دوجبه‌ای است؛ نخست آنکه به‌کارگیری پایش بیومتریک در معابر عمومی، در پرتو رویه قضایی اروپایی، بنا بر چه استدلالی مداخله در حق بر حریم خصوصی به‌شمار می‌آید؛ و بر پایه همان استدلال، برای آنکه قانون تجویزکننده این پایش به نقض حقوق شهروندان نینجامد، باید واجد چه ویژگی‌ها، معیارها و تضمین‌هایی باشد. گزینش رویه قضایی اروپایی به‌عنوان محک این سنجش نیز نه از آن روست که الگوی اروپایی علی‌الطلاق قابل اقتباس باشد — چه اینکه مبانی حمایت از حریم خصوصی در نظام حقوقی ایران، چنان‌که خواهد آمد، ریشه در موازین اسلامی و اصول قانون اساسی دارد — بلکه از آن جهت است که دیوان اروپایی حقوق بشر، دیوان دادگستری اتحادیه اروپا و دادگاه‌های ملی اروپا طی دو دهه معیارهای قانونمندی، ضرورت و تناسب را بر مصادیق انضمامی نظارت بیومتریک تطبیق داده و از دل همین تطبیق، ضوابطی عینی استخراج کرده‌اند که فارغ از خاستگاه خود، پرسش‌هایی را پیش می‌نهد که هر نظام حقوقی در مواجهه با این فناوری ناگزیر از پاسخ‌گویی بدان‌هاست.

سامان این نوشتار بر همین پرسش استوار شده است. مبحث نخست به مبانی حق بر حریم خصوصی در نظام حقوقی ایران می‌پردازد تا روشن شود این حق بر چه پایه‌های عقلی، شرعی و اساسی استوار است، استثنائات وارد بر آن از چه منطقی پیروی می‌کند و از دل این منطق چه ضوابط درونی‌ای برای سنجش مداخله به دست می‌آید. مبحث دوم، در دو گفتار، نخست آستانه احراز مداخله را در رویه اروپایی می‌کاود و تفکیک میان مشاهده انسانی و پردازش خودکار داده را می‌سنجد، آنگاه اوصافی را برمی‌شمارد که شدت و گستره این مداخله را از نظارت تصویری متعارف فراتر می‌برد. مبحث سوم نیز، در دو گفتار، معیارهایی

جان، مال و حقوق اشخاص را از تعرض مصون داشته و اصل بیست‌وپنجم بازرسی و تجسس را ممنوع ساخته است، مگر آنکه مداخله «به حکم قانون» صورت گیرد. هرچند در قانون اساسی لفظ «حریم خصوصی» به کار نرفته اما دو ظرفیت تفسیری در همین اصول نهفته است که تسری آن‌ها بر مصادیق نوظهور را ممکن می‌سازد؛ نخست آنکه اصل بیست‌وپنجم هرگونه تجسس را به‌طور مطلق ممنوع ساخته و با احراز مفهوم «تجسس»، بسیاری از مصادیق نقض حریم خصوصی را می‌توان ذیل آن جای داد (زرکلام و عبدی، ۱۳۹۳: ۳۳)؛ و دوم آنکه واژه «حقوق» در اصل بیست‌ودوم، مفهومی کیفی و تفسیرپذیر است که حق بر حریم خصوصی را می‌توان با «تفسیر بر اساس مقتضیات زمان» مشمول آن دانست (زرکلام و عبدی، ۱۳۹۳: ۳۴)، علاوه بر این از باب مطلق بودن کلمه «حقوق» شمول آن بر حق بر حریم خصوصی به لحاظ اصولی نیز پذیرفته شده است.

قانون اساسی برای نقض و تحدید حریم خصوصی، هیچ مبنا و دلیلی جز حکم قانون را به رسمیت نمی‌شناسد؛ به عبارت دیگر، اصل بر مصونیت است و استثنای آن تنها در صلاحیت انحصاری مقنن قرار دارد. با این وصف، به موجب اصل چهارم قانون اساسی که بر تمامی اصول حاکمیت دارد، این اختیار قانون‌گذاری نیز مطلق نبوده و هرگونه وضع قاعده برای ایجاد محدودیت در حریم خصوصی، لزوماً باید ریشه در موازین دین اسلام داشته باشد (حسینی‌کاشانی و همکاران، ۱۳۹۸: ۶۰). تأمل در همین موازین اسلامی نشان می‌دهد که استثنائات وارد بر حریم خصوصی با هدف حفظ امنیت جامعه و جلوگیری از سوءاستفاده‌ها، کاملاً محدود، ضابطه‌مند و ناظر به ضرورت‌های قطعی است و عمدتاً در دو قالب نظارت پیشینی و پسینی تجلی می‌یابد. در عرصه نظارت پیشینی، جواز مداخله منحصر به مواردی نظیر اشراف اطلاعاتی بر کارگزاران حکومت، رصد تحرکات دشمنان خارجی، مقابله با منافقین و معاندین داخلی، محدود می‌گردد. در عرصه نظارت پسینی نیز، خروج از اصل

منع تجسس تنها در فروضی روا شمرده شده است که عمل ارتكابی محقق شده و پای مصلحتی برتر در میان باشد؛ نظیر مقابله با مخلانی که با ایجاد رعب و وحشت امنیت جامعه را تهدید می‌کنند (محسنی و میرعماد، ۱۳۹۸: ۲۶۵-۲۵۸). بر این اساس، دقت در این استثنائات مبرهن می‌سازد که جواز مداخله همواره ناظر به تهدیدات مشخص، افراد معین و شرایط استثنایی است. چنانکه احترام به حریم خصوصی امری مطلق دانسته نشده و در فرض تراحم مصلحت فردی با مصالح اجتماعی، امکان ورود برای اشخاص ذی‌صلاح منتفی شمرده نشده است، لکن این ورود جز به حکم قانون، با رعایت مقررات و تحت نظارت مقام قضایی روا ندانسته‌اند (ظفریان و همکاران، ۱۴۰۴: ۴۹). تأمل در منطق حاکم بر این استثنائات، آشکار می‌سازد که جواز مداخله به اشخاصی معین و مشخص تعلق می‌گیرد، همچنین خروج از اصل منع تجسس در مقام دفع مفسده‌ای برتر و برای غرضی محصور روا شمرده شده و به مصلحت‌سنجی موردی مجری واگذار نشده است. این مداخله وصفی عارضی و موقت دارد و نمی‌تواند به رویه‌ای مستمر و فراگیر بدل شود، چه اینکه در آن صورت استثنا جای اصل را خواهد گرفت.

۲- شمول حق بر حریم خصوصی بر پایش بیومتریک در رویه قضایی اروپایی

پیش از ورود به رویه، اشاره‌ای کوتاه به مبنای آن ضروری است. ماده هشتم کنوانسیون اروپایی حقوق بشر در بند نخست، حق هر شخص را بر احترام به زندگی خصوصی و خانوادگی، خانه و مکاتباتش به رسمیت می‌شناسد و در بند دوم مقرر می‌دارد که هیچ مقام عمومی نمی‌تواند در اعمال این حق مداخله کند، مگر آنکه مداخله «مطابق قانون» باشد، «در یک جامعه دموکراتیک ضرورت داشته باشد» و در تعقیب یکی از اغراض حصرشده در همان بند -از جمله امنیت ملی، ایمنی عمومی و پیشگیری از بی‌نظمی یا جرم- صورت گیرد (European Convention on Human Rights, 1950,)

^۱- تنها سند داخلی که به‌صراحت به کنترل‌های صوتی و تصویری در اماکن عمومی پرداخته، منشور حقوق شهروندی مصوب ۱۳۹۵ است که چنین کنترل‌هایی را در محیط‌های کار، اماکن عمومی و محیط‌های ارائه خدمت به عموم ممنوع شمرده و گردآوری و انتشار اطلاعات خصوصی شهروندان را جز با رضایت آگاهانه یا به حکم قانون روا ندانسته است (حسینی‌کاشانی و همکاران، ۱۳۹۸: ۴۷)؛ مع‌ذلک این سند از سنخ تجویز یا منع تقنینی نیست - چنان‌که در ارزیابی جایگاه آن در نظم حقوقی داخلی گفته شده که به اقتضای نحوه تنظیم و ابلاغ، بیش از یک برنامه اخلاقی برای دولت به‌شمار نمی‌آید (میرزاوند و معتمدنژاد، ۱۴۰۴: ۲۶۶).

فرض تطابق، سامانه به اپراتور هشدار دهد (Fussey & Murray, 2019: 19). بدین‌سان هر عبور از برابر دوربین، به یک عملیات خودکار پردازش داده بیومتریک بدل می‌گردد.

حال این تقابل را می‌توان از زاویه دید رویکرد داده‌محور بازگو کرد که مبتنی بر آن کسی که به معبر عمومی گام می‌نهد، دانسته و خواسته خود را در معرض دید دیگران نهاده است؛ چهره او را هر رهگذری می‌بیند و هر مأمور گشتی می‌تواند او را بنگرد و در صورت شناختن، شناسایی کند و به این دلیل، نظارت از رهگذر ابزار فناورانه تفاوتی ماهوی با مشاهده مستقیم ندارد و صرفاً همان کاری را که چشم مأمور می‌کند با دقت و سرعتی افزون‌تر به انجام می‌رساند؛ پس ادعای نقض حریم خصوصی در جایی که شخص خود حریمی برای چهره‌اش قائل نشده، فاقد وجهت به نظر می‌رسد. این استدلال را نباید دست‌کم گرفت، چه اینکه خود دیوان اروپایی حقوق بشر نیز صرف مشاهده یا نظارت بر فرد در مکان عمومی را، بدون تحلیل بیشتر، مداخله در حریم خصوصی نمی‌شمارد و همین موضع، به حسب الظاهر مؤید این دیدگاه است.

مع‌ذلک تأمل در همان رویه، دیوان میان «مشاهده انسانی» و «ثبت و پردازش خودکار و نظام‌مند» تفکیک نهاده، نقطه عزیمت این تفکیک آن است که قلمرو زندگی خصوصی به «حلقه درونی» زندگی شخص محدود نمی‌شود و میان فرد و دیگران، حتی در بستری عمومی، عرصه‌ای از تعامل برجاست که در دامنه این حق می‌گنجد؛ و از همین رو انتظار متعارف شخص از رعایت حریمش، عاملی درخور اعتنا اما به‌تنهایی قاطع نیست (Antović and Mirković v. Montenegro, 2017, paras. 41-43). دیوان در پرونده بی.جی. و جی.اچ. علیه بریتانیا تصریح کرد که ملاحظات حریم خصوصی آنگاه پدیدار می‌شود که از نظارت صرف فراتر رفته، ثبتی نظام‌مند یا ماندگار از داده‌های برآمده از قلمرو عمومی صورت گیرد (P.G.).

Art. 8). ساختار همین بند است که آزمون سه‌مرحله‌ای دیوان را شکل داده و سامان دو قسمت پیش رو نیز بر آن استوار است. احراز اینکه پایش بیومتریک در معابر عمومی به قلمرو حق بر حریم خصوصی راه می‌یابد، دو پرسش متمایز را پیش می‌نهد نخست آنکه اساساً و از چه حیث می‌توان ثبت و پردازش خودکار چهره عابران را -به خلاف مشاهده متعارف پلیسی- «مداخله» نامید، و دوم آنکه چه اوصافی این مداخله را از سایر گونه‌های نظارت متمایز و شدت آن را مضاعف می‌سازد. دو گفتار پی‌آمده به همین ترتیب سامان یافته‌اند.

۲-۱- تفکیک «مشاهده انسانی» از «ثبت و پردازش خودکار»
برای درک ابعاد تقابل میان نظارت‌های نوین انتظامی و حقوق بنیادین شهروندان، نخست باید این انگاره تحلیل شود که شناسایی بیومتریک در معابر عمومی، فی‌حد ذاته یک مداخله سیستماتیک در حق بر حریم خصوصی است و لذا چالش‌های توجیه‌پذیری خاص خود را به همراه دارد. وقوع این تعارض به هیچ روی بدیهی انگاشته نمی‌شود و اتفاقاً قوی‌ترین استدلالی که در دفاع از رویکرد پیشگیرانه پلیس می‌توان اقامه کرد، در نقطه مقابل این مدعا ریشه دارد؛ مع‌ذلک پیش از طرح آن رویکرد، ارائه تصویری روشن از موضوع بحث ضروری است. اگرچه به گفته پژوهشگران این حوزه و نیز دیوان اروپایی حقوق بشر، ارائه تعریفی حقوقی و جامع از موضوع حمایت حریم خصوصی میسر نیست (Tzanou & Karyda, 2022: 123)، فی‌الجملة می‌توان گفت این حق ناظر بر زیستن به میل و سلیقه خود با کمترین مداخله دیگران است و از همین رو مالکیت بر اطلاعات شخصی، از جمله تصویر چهره و اختیار بر اینکه چه کسی بدین اطلاعات دسترسی یابد، در قلمرو آن می‌گنجد (Miller & Bossomaier, 2024: 173). از سوی دیگر، سازوکار سامانه‌های مبتنی بر هوش مصنوعی در تشخیص چهره زنده از این قرار است که دوربین تصویر چهره عابران را ثبت می‌کند، الگوریتم از هر چهره الگویی بیومتریک استخراج می‌سازد و این الگو با الگوهای موجود در پایگاه داده‌ای موسوم به فهرست مراقبت تطبیق داده می‌شود تا در

۱- گام مهم در شکل‌گیری مفهوم حریم خصوصی، انتشار مقاله «حق بر حریم خصوصی» اثر ساموئل وارن و لویی براندیس در سال ۱۸۹۰ بود. نویسندگان در این مقاله، حق بر حریم خصوصی را به عنوان «حق به حال خود رها شدن» تعریف کردند. از آن زمان تاکنون، این مفهوم تکامل یافته و با پذیرش گسترده در نظام‌های حقوقی، به یکی از حقوق بنیادین بشر در عصر حاضر تبدیل شده است (Warren & Brandeis, 1890).

17, 15, 14, 8. paras.) آنچه بر اعتبار این ضابطه می‌افزاید آن است که دیوان خود بعدها در رأی اس. و مارپر علیه بریتانیا بدان استناد کرد و همین تفکیک را مبنای تحلیل قرار داد (S. and Marper v. the United Kingdom, 2008, para. 82). مفهوم مخالف این استدلال روشن است، چه اینکه آنجا که تصویر به سامانه پردازش وارد شود و غرض، شناسایی شخص از رهگذر پردازش خودکار داده باشد، مداخله محقق است؛ حال آنکه سامانه تشخیص چهره زنده، چنان که گذشت، بذاته و بنا بر تعریف چیزی جز همین ورود تصویر به سامانه الگوریتمی به قصد شناسایی نیست. به دیگر سخن، درست همان عنصری که در فریدل مفقود بود و فقدانش مبنای نفی مداخله شد، در تشخیص چهره مقوم ماهیت فناوری است.

در ادامه همین استدلال، دیوان در پرونده گاوران علیه بریتانیا نخست یادآور شد که کمیسیون اروپایی حقوق بشر پیش‌تر در آرائی چند -از جمله همان فریدل- نگهداری و استفاده از عکس‌های گرفته‌شده به وسیله مقامات انتظامی را مداخله در حریم خصوصی نمی‌شمرد، آنگاه با تصریح به اینکه در احراز مداخله باید بستر ثبت و نگهداری داده، ماهیت سوابق، شیوه استفاده و پردازش آن‌ها و نتایجی که ممکن است از این پردازش حاصل شود ملاحظه گردد، از آن رویه پیشین فاصله گرفت؛ و آنچه در این فاصله‌گیری نقش تعیین‌کننده داشت، در کنار نگهداری نامحدود عکس در پایگاه داده پلیس، این بود که عکس متقاضی می‌توانست به پایگاه داده ملی پلیس بارگذاری شود و در آنجا در معرض اعمال فناوری تشخیص چهره و نقشه‌برداری از چهره قرار گیرد؛ چندان که دیوان اعلام داشت در مداخله‌آمیز بودن گرفتن و نگهداری این عکس تردیدی ندارد (Gaughran v. the United Kingdom, 2020, paras. 65-70). دلالت این استدلال بر موضوع بحث حاضر دوچندان است؛ عامل دگرگون‌کننده وصف حقوقی، نه مکان گرفتن تصویر بود و نه ماهیت آن، بلکه پیوستن ظرفیت

57 (and J.H. v. The United Kingdom, 2001, para. 57) و در پرونده پک علیه بریتانیا نیز همین ضابطه را بر تصاویر ضبط‌شده از فضاهای عمومی تطبیق داد و به موازات آن، دیوان تصویر چهره را داده شخصی و حق شخص بر کنترل استفاده از تصویر خویش را از مؤلفه‌های حق بر حریم خصوصی و رشد شخصیت شمرده است (Peck v. The United Kingdom, 2003, para. 59,78). در همین راستا دیوان در پرونده آنتوویچ و میرکوویچ علیه مونته‌نگرو پایش تصویری آمفی‌تئاترهای دانشگاه را -با آنکه محل کار و در معرض دید دانشجویان بود و پایش نیز پنهانی صورت نمی‌گرفت- مداخله‌ای درخور اعتنا در زندگی خصوصی استادان شمرد، چه اینکه حاصل چنین پایشی، مستندسازی ضبط‌شده و بازتولیدپذیر رفتار شخص در مکانی است که وی به اقتضای تکلیف خود‌گزینی از حضور در آن ندارد (Antović and Mirković v. Montenegro, 2017, paras. 44,45). دلالت این رأی بر موضوع بحث به‌طریق اولی است، چه اینکه اگر گریزناپذیری حضور در محل کار مبنای احراز مداخله باشد، رهگذری که برای دسترسی به خدمات و اماکن شهری ناگزیر از عبور از معابر تحت پایش است، به‌مراتب کمتر از استاد دانشگاه اختیار پرهیز دارد.

روشن‌ترین معیار و محک این تفکیک از پرونده فریدل علیه اتریش به دست آمده است. کمیسیون اروپایی حقوق بشر در گزارش خود در این پرونده به‌اتفاق آرا بر آن شد که گرفتن و نگهداری عکس‌های ناشناس از یک تظاهرات عمومی نقض ماده هشتم نیست، اما نه علی‌الاطلاق، بلکه از آن جهت که عکس‌ها به هیچ سامانه پردازش داده‌ای وارد نشده و مقامات نیز در پی شناسایی اشخاص عکس‌برداری‌شده از رهگذر پردازش داده نبودند؛ پرونده سپس در دیوان با سازش دوستانه -که امحای تمامی عکس‌ها و نگاتیوها را نیز در بر داشت- مختومه و از فهرست خارج شد (Friedl v. Austria, 1995).

¹⁻ “57. There are a number of elements relevant to a consideration of whether a person’s private life is concerned by measures effected outside a person’s home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain...”

²⁻ data-processing system

پردازش بیومتریکی به آن، علاوه بر این دیوان برای احراز مداخله به تحقق فعلی شناسایی نیازی ندید و صرف ظرفیت سامانه را کافی شمرد.

همین منطق در دو ضابطه مکمل نیز بازتاب یافته است؛ دیوان اروپایی حقوق بشر صرف ذخیره داده مرتبط با زندگی خصوصی را مداخله می‌داند و استفاده بعدی از داده ذخیره شده را در این احراز بی‌تأثیر می‌شمارد (*S. and Marper v. the United Kingdom*, 2008, para. 67) و دیوان دادگستری اتحادیه اروپا نیز تصریح کرده است که در احراز مداخله در حق بر حریم خصوصی، حساس بودن اطلاعات و اینکه اشخاص ذی‌ربط از این اقدام دچار زحمتی شده باشند یا نه، تأثیری ندارد (*Digital Rights Ireland and Others*, C-293/12, 2014, para. 33). بدین ترتیب آن دو استدلال رایج نیز که «داده‌ای حساس در میان نیست» و «تا وقتی تطابقی رخ نداده زیانی به کسی نرسیده است»، در سنجش با رویه اروپایی مجالی برای طرح نمی‌یابند. جمع این آرا ضابطه‌ای واحد به دست می‌دهد مبنی بر اینکه متغیر تعیین‌کننده در احراز مداخله، عمومی یا خصوصی بودن مکان نیست، بلکه ورود تصویر به سامانه‌ای است که ظرفیت پردازش خودکار و شناسایی را داراست. شایان توجه آنکه همین ضابطه در سطح تقنینی نمود دارد؛ چنان‌که در تحلیل مقررات عمومی حفاظت از داده‌های اتحادیه اروپا آمده که تصویر تنها آنگاه ذیل تعریف داده بیومتریکی جای می‌گیرد که از رهگذر ابزار فنی خاصی پردازش شود که امکان شناسایی یا احراز هویت منحصر به فرد شخص را فراهم آورد (میرزاوند و معتمدنژاد، ۱۴۰۴: ۲۵۴-۲۵۵).

۲-۲- شدت و گستره مداخله؛ نفی رضایت، حساسیت داده، فراگیری نسبت به غیرمظنونان و خطر گسترش کارکرد

احراز نفس مداخله، حداقل آنچه از رویه اروپایی به دست می‌آید است؛ اهمیت این رویه در آن است که اوصافی را نیز برمی‌شمارد که شدت این مداخله را از نظارت تصویری متعارف فراتر می‌برد و -چنان‌که در مبحث پسین خواهد آمد- آستانه توجیه‌پذیری آن را نیز بالا می‌برد. نخستین وصف، اصل رضایت آگاهانه است که اقتضا می‌کند که اشخاص از زمان و نحوه گردآوری و پردازش داده‌های شخصی خود، از جمله اطلاعات بیومتریکی و از اغراض این اقدامات آگاه باشند، حال

آنکه فناوری تشخیص چهره در مکان‌های عمومی غالباً بی‌اطلاع و بی‌رضایت اشخاص به کار گرفته می‌شود و با ترکیب شناسه‌های بیومتریکی همچون تصویر چهره با شناسه‌های بیوگرافیک و انتسابی همچون نشانی و نام، بی‌نیاز از هرگونه رضایت یا حتی اطلاع، پروفایل‌هایی دقیق از اشخاص فراهم می‌آورد (Dul, 2022: 4). رهگذری که در برابر چشم مأمور از خیابان می‌گذرد، می‌داند که دیده می‌شود و همین آگاهی بخشی از انتخاب اوست؛ اما همو نمی‌داند و نمی‌تواند بداند که تصویرش در کدام سامانه با کدام فهرست تطبیق می‌خورد و حاصل این تطبیق به کجا می‌رود و همین واقعیت است که ادعای «در معرض دید نهادن خویش» را در فرض پردازش بیومتریکی بلاوجه می‌سازد.

این تحلیل در رویه دیوان مبنایی صریح دارد. دیوان در پرونده *Reklos and Davourlis v. Greece* (2009, para. 40) و انگهی دیوان در همان رأی بی‌ضرر بودن مدلول تصویر را مانع احراز نقض ندانست و تصریح کرد که مسأله اصلی نه ماهیت زیان‌بار یا بی‌آزار تصویر، بلکه نگهداری آن به شکلی قابل‌شناسایی و با امکان استفاده بعدی برخلاف خواست شخص است (*Reklos and Davourlis v. Greece*, 2009, para. 42). تطبیق این ضابطه بر پایش بیومتریکی روشن است؛ چنانکه ضابطه اینست که رضایت باید در لحظه ثبت تصویر احراز شود و اختیار اعتراض به نگهداری آن جزئی از حق شمرده می‌شود و سامانه‌ای که الگوی چهره

هزاران عابر را بی‌اطلاع و بی‌رضایت ایشان استخراج و پردازش می‌کند، فاصله‌ای مشهود از این ضابطه دارد.

وصف دوم به جنس داده موضوع پردازش بازمی‌گردد. دیوان در اس. و مارپر علیه بریتانیا اثر انگشت را از آن جهت که اطلاعاتی منحصر درباره شخص را در خود دارد و شناسایی دقیق او را در گستره‌ای وسیع از اوضاع و احوال ممکن می‌سازد، داده‌ای دانست که نگهداری آن بدون رضایت شخص را نمی‌توان بی‌طرف یا کم‌اهمیت شمرد (S. and Marper v. the United Kingdom, 2008, para. 84)؛ استدلالی که به‌طریق اولی بر الگوی بیومتریکی چهره منطبق است، دیوان در همان رأی افزود که ضرورت پیش‌بینی تضمین‌های مناسب در قانون داخلی آنگاه بیش‌ازپیش احساس می‌شود که پای پردازش خودکار داده شخصی در میان باشد، خاصه آنکه این پردازش برای اغراض پلیسی صورت گیرد؛ و ماهیت ذاتا خصوصی چنین اطلاعاتی مقتضی آن است که دیوان هر تدبیر دولتی را که نگهداری و استفاده از آن‌ها را بدون رضایت شخص تجویز می‌کند، به‌دقت واریسی نماید (S. and Marper v. the United Kingdom, 2008, paras. 103,104).

وصف سوم که مهم‌ترین وجه تمایز پایش بیومتریکی از مداخلات متعارف است، بر دامنه اشخاص موضوع پردازش نظر دارد. در نظارت متعارف، مداخله بر شخص یا اشخاصی معین و بر پایه ظنی مشخص اعمال می‌شود، حال آنکه سامانه تشخیص چهره زنده به اقتضای سازوکار خود الگوی بیومتریکی تمامی عابران را استخراج و تطبیق می‌دهد و از این حیث میان مظنون و غیرمظنون تفاوتی نمی‌نهد. دیوان دادگستری اتحادیه اروپا در رأی دیجیتال رایتس آیرلند، نگهداری عام داده را از آن جهت مردود شمرد که دامنه آن تمامی اشخاص و تمامی وسایل ارتباطی را بدون هرگونه تفکیک، تحدید یا استثنا دربر می‌گرفت و حتی اشخاصی را نیز مشمول می‌ساخت که هیچ قرینه‌ای بر ارتباط -حتی غیرمستقیم و دور- میان رفتار ایشان و جرم مهم در میان نبود (Digital Rights Ireland and Others, C-293/12, 2014, paras. 57,58) و در رأی اشرمز نیز تصریح کرد که مقرره‌ای که به مقامات عمومی اجازه دسترسی عام به محتوای ارتباطات را بدهد، «گوهر» حق بر

احترام به زندگی خصوصی را مخدوش می‌سازد (Schrems, C-362/14, 2015, para. 94). دیوان اروپایی حقوق بشر نیز در اس. و مارپر از وصف فراگیر و بدون تفکیک اختیار نگهداری داده به شگفت آمد و افزون بر آن بر خطر انگ‌زنی برآمده از این وضع انگشت نهاد، چه اینکه اشخاصی که به هیچ جرمی محکوم نشده و مستحق اصل برائت‌اند، به همان شیوه محکومان مورد رفتار قرار می‌گیرند (S. and Marper v. the United Kingdom, 2008, paras. 119,122). مقایسه این ضوابط با سازوکار پایش بیومتریکی نشان می‌دهد که در اینجا حتی از فرض نگهداری داده مظنونان نیز فراتر می‌رویم، زیرا آنچه پردازش می‌شود داده تمام رهگذرانی است که هیچ نسبتی با هیچ تحقیقی ندارند. شایان توجه آنکه این وصف، پیش از آنکه با معیارهای اروپایی سنجیده شود، با ضابطه برآمده از موازین فقهی -یعنی تعیین اشخاص موضوع مداخله- ناسازگار است، چه اینکه در آن منطق نیز جواز تجسس هرگز به عموم مردم تعلق نمی‌گیرد.

وصف چهارم مرتبط با آثار جمعی این پایش است. حق بر حریم خصوصی پیوندی نزدیک با مفهوم خودمختاری دارد و یکی از کارکردهای اصلی آن، تضمین این امر است که تصور یا واقعیت تحت نظر بودن به خودسانسوری و جهت‌دهی به اعمال شخص نبینجامد (Smith & Miller, 2022: 171-172). دیوان دادگستری اتحادیه اروپا در همان رأی دیجیتال رایتس آیرلند تصریح کرد که نگهداری داده و استفاده بعدی از آن، بی‌آنکه شخص ذی‌ربط از این امر آگاه شود، مستعد آن است که در اذهان اشخاص این احساس را بیافریند که زندگی خصوصی ایشان موضوع پایشی پیوسته است (Digital Rights Ireland and Others, C-293/12, 2014, para. 37). اثری که دقیقا همان کارکرد را هدف می‌گیرد و لذا نه فقط حریم خصوصی، بلکه آزادی‌های وابسته به آن را نیز در معرض خطر می‌نهد.

در کنار این موارد، خطر گسترش کارکرد نیز وجود دارد؛ بدین معنا که سامانه‌ای که برای شناسایی اشخاصی معین برپا می‌شود، به اقتضای ساختار فنی خود، ظرفیت آن را دارد که به سامانه دسته‌بندی جمعیتی بدل گردد. نمونه این خطر را در

است و گفتار دوم شروط ضرورت و تناسب را در دو تجلی عینی آن، یعنی ضابطه‌مندی نگهداری داده و منع گردآوری انبوه، می‌کاود.

۳-۱- از مبنای قانونی تا «کیفیت قانون» و تحدید صلاح‌دید پلیسی

چنان‌که در پایان مبحث پیشین گذشت، احراز نفس مداخله تنها نقطه آغاز مواجهه با این پدیده است و گام اساسی، یافتن الگوها و معیارهایی است که نظام‌های حقوقی به یاری آن‌ها این تقابل را مدیریت و مهار می‌کنند. نقطه عزیمت این جست‌وجو در نظام حقوقی اروپا، ماده هشتم کنوانسیون اروپایی حقوق بشر است که پس از شناسایی حق بر احترام به زندگی خصوصی، در بند دوم خود مداخله مقام عمومی را تنها در فرضی روا می‌شمارد که مطابق قانون باشد، هدفی مشروع همچون پیشگیری از جرم را دنبال کند و در جامعه‌ای دموکراتیک ضروری به‌شمار آید؛ و همین کنوانسیون و رویه دیوان ناظر بر آن، منبع اصلی موازین حقوق بشری برای اتحادیه اروپاست (Barfield & Pagallo, 2020: 5-34). مفاهیم ضرورت، تناسب و پیش‌بینی‌پذیری که از دل همین بند استخراج شده‌اند، بر برقراری توازنی منصفانه میان رویکرد داده‌محور نهادهای انتظامی و حقوق فردی شهروندان نظر دارند و مقتضای تناسب آن است که دولت با دلایلی کافی متقاعد سازد که تحدید حق، هدف مشروع را برمی‌آورد، کم‌مزاحمت‌ترین وسیله را برگزیده و کمترین تعرض را به حقوق فردی روا می‌دارد (Oswald et al., 2018: 226).

با این وصف، اگر مدیریت این چالش به همین عبارات کلی بسنده می‌کرد، حاصلی جز توصیه‌های انتزاعی در میان نبود، چه اینکه هیچ نهاد پلیسی نظارت خود را غیرضروری نمی‌خواند. اهمیت رویه قضایی اروپایی - به‌عنوان یک آزمایشگاه حقوقی پیشرو در مواجهه با فناوری - از آن روست

تجربه‌ای بیرون از قلمرو اروپا می‌توان دید؛ دولت چین، با افزایش نظارت شخصی در منطقه سین‌کیانگ، از سیستم‌های تشخیص چهره مبتنی بر هوش مصنوعی برای شناسایی اقلیت اویغور بر اساس ویژگی‌های ظاهری متمایزشان از اکثریت^۱ هان استفاده می‌کند. این سیستم‌ها در ایست‌های بازرسی پلیس و دوربین‌های نظارتی در سراسر منطقه، از جمله شهرهای مهم مانند اورومچی و کاشغر، به کار گرفته شده‌اند و به‌طور مداوم در حال توسعه و گسترش هستند. این فرآیند را «شناسایی اقلیت» می‌نامند. اطلاعات جمع‌آوری شده در یک پایگاه داده بزرگ به‌نام «پلتفرم عملیات مشترک یکپارچه» ذخیره می‌شود. این پایگاه داده از هوش مصنوعی برای ایجاد فهرست‌هایی از «افراد مشکوک» بر اساس این اطلاعات استفاده می‌کند (Stark, 2021: 162-163).

اهمیت این نمونه در آن است که نشان می‌دهد فاصله میان یک سامانه شناسایی و یک سامانه دسته‌بندی جمعیتی، تنها به گستره اغراض مجاز و استحکام تضمین‌های حقوقی حاکم بر آن بازمی‌گردد؛ و از همین روست که سنجش مشروعیت این فناوری را نمی‌توان به کارکرد اعلامی آن محدود ساخت، بلکه باید ظرفیت‌های بالقوه آن را نیز در شمار آورد. این وصف نیز با ضابطه برآمده از مبحث نخست - استثنایی و موقت بودن مداخله - در تنش مستقیم است، چه اینکه سامانه‌ای که یک بار مستقر شود، به اقتضای طبیعت خود میل به استمرار و توسعه دامنه دارد مگر اینکه با ضوابط قانونی مشخص مهار شود.

۳- معیارهای سنجش مشروعیت مداخله در رویه قضایی اروپایی

مبحث حاضر بدین شرایط نظر دارد و در دو گفتار سامان یافته است؛ گفتار نخست بر شرط قانونمندی متمرکز است و نشان می‌دهد که رویه اروپایی چگونه از صرف وجود نص مجوزدهنده به سنجش «کیفیت» آن نص و تحدید صلاح‌دید پلیسی رسیده

^۱- Xinjiang

^۲- Uyghur

^۳- Han

^۴- Ürümqi

^۵- Kashgar

^۶- minority identification

^۷- Integrated Joint Operations Platform

که همین عبارات کلی را به ضابطه‌هایی عینی برای مهار مداخلات ناقض حریم خصوصی بدل کرده است. سرآغاز این تحول، تفسیری است که از قید «مطابق قانون» به دست داده شده. در منطق این رویه، برای پاسخگویی به چالش‌های هوش مصنوعی، صرف وجود نصی که مداخله را اجازه دهد کفایت نمی‌کند و آن نص باید از «کیفیت قانون» برخوردار باشد؛ به دیگر سخن در دسترس و پیش‌بینی‌پذیر باشد، دامنه اختیار مقام مجری را با دقتی به فراخور شدت مداخله ترسیم کند و در برابر خودسری تضمین بگذارد.

نمود این تحول و تلاش برای ضابطه‌مندسازی را در پرونده بریجز علیه رئیس پلیس ولز جنوبی می‌توان دید. پلیس از سال ۲۰۱۷ فناوری تشخیص چهره زنده را در اماکن عمومی برای شناسایی افراد مندرج در فهرست مراقبت به کار گرفته بود و شهروندی که تصویرش پردازش شده بود، به دادگاه شکایت برد (Gordon, 2021: 6-7). دادگاه بیان داشت که این بهره‌برداری ناقض حریم خصوصی است و آنچه این رأی را برای واکاوی این تعارض قابل توجه می‌سازد، جهت استدلال آن است؛ در نظام حقوقی انگلستان قانون حمایت از داده مصوب و مجری بود و پلیس نیز به اسناد راهنمای نظارت تصویری استناد می‌کرد، معذک دادگاه همین چارچوب را برای مهار یک مداخله بیومتریک کافی ندانست، زیرا تعیین اینکه چه کسانی در فهرست مراقبت جای گیرند و دوربین در کجا مستقر شود، یکسره به صلاح‌دید پلیس واگذار شده بود؛ نقصی که دادگاه آن را در دو حوزه صورت‌بندی کرد. نخست، در پاسخ به سؤال «چه کسی»، قوانین موجود مشخص نمی‌کنند که دقیقاً چه کسانی می‌توانند در فهرست مراقبت قرار گیرند.

دادگاه استدلال کرد که اگرچه برخی دسته‌بندی‌ها مانند افراد تحت تعقیب عینی هستند، اما گنجاندن دسته‌بندی مبهمی

مانند «افرادی که به دلایل اطلاعاتی مورد نیاز هستند»، بسیار ذهنی و گسترده بوده و عملاً به افسر پلیس اجازه می‌دهد هر کسی را که برایش جالب است در این فهرست قرار دهد (R (Bridges) v. Chief Constable of South Wales (Police, 2020, para. 124). دادگاه در خصوص نقص در پاسخ به سؤال «کدام مکان»، بیان کرد که هیچ معیار، ضابطه و محدودیت روشنی برای تعیین مکان‌هایی که پلیس مجاز است سیستم‌های تشخیص چهره را در آنجا مستقر کند، وجود ندارد (R (Bridges) v. Chief Constable of South (Wales Police, 2020, para. 91). به دلیل وجود این دو حوزه با صلاح‌دید بسیار وسیع و کنترل‌نشده برای پلیس، دادگاه حکم داد که این سطح از مداخله در حریم خصوصی افراد در ملاً عام، فاقد پشتوانه و چارچوب قانونی بوده و در نتیجه استقرار این سیستم‌ها غیرقانونی و ناقض ماده ۸ کنوانسیون است (R (Bridges) v. Chief Constable of South (Wales Police, 2020, para. 4) از این رأی ضابطه‌ای منقح به دست می‌آید که به موجب آن، در مواجهه با فناوری‌های نوین، وجود قانون کلی رافع چالش‌های ساختاری نیست و مدیریت این تقابل، نیازمند ضابطه‌مندی دقیق خود صلاح‌دید پلیسی است.

اقتضای همین شرط، حتی در وضعیت‌های اضطراری نیز تعلیق نمی‌پذیرد و به سامانه‌های ثابت نیز محدود نمانده است. از آغاز بحران کووید-۱۹، پلیس فرانسه برای نظارت بر شهروندان از پهپاد بهره می‌گرفت و سازمان حقوق دیجیتال اروپا با همکاری نهادهای دیگر، با استناد به فقدان هرگونه مبنای قانونی برای بهره‌برداری از تصاویر این پهپادها، علیه پلیس پاریس اقامه دعوا کرد؛ شورای دولتی فرانسه در مه ۲۰۲۰ پرواز هر پهپاد دوربین‌دار در ارتفاعی که شناسایی اشخاص از روی پوشش یا نشانه‌های ظاهری را ممکن سازد

^۱- Quality of Law

^۲- Who question

^۳- watchlist

^۴- PARA 124: "While we can readily understand that the first three of those categories are objective, the final category is not. In effect it could cover anyone who is of interest to the police. In our judgement, that leaves too broad a discretion vested in the individual police officer to decide who should go onto the watchlist."

^۵- PARA 91: "The fundamental deficiencies, as we see it, in the legal framework currently in place relate to two areas of concern. The first is what was called the "who question" at the hearing before us. The second is the "where question". In relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed."

ماده هشتم ندانست، رژیم حاکم بر آن را به سبب فقدان تضمین‌های سرتاسری -به‌ویژه نبود اجازه مستقل و پیشینی در مراحل کلیدی فرآیند و ضعف تضمین‌های ناظر بر گزینش و پردازش داده- ناقض این ماده شمرد (Big Brother Watch and Others v. the United Kingdom, 2021, paras. 350, 425). از این‌رو، هرچه دامنه پردازش خودکار داده گسترده‌تر شود، تضمین‌های آیینی باید در سراسر زنجیره پردازش و نه صرفاً در نقطه آغاز آن مستقر گردند، همچنین گستردگی دامنه، خود می‌تواند قرینه‌ای بر خروج از مدار ضرورت باشد، نه توجیه‌کننده کارآمدی سامانه و توارد این ضابطه با آنچه در مبحث نخست از موازین فقهی استخراج شد نیز درخور تأمل است، چه اینکه در هر دو منطق، عمومیت دامنه مداخله وصفی است که اصل جواز را منتفی می‌سازد.

تمامی این ضوابط سرانجام در رأی متبلور می‌شوند که باید آن را نقطه اوج رویه موجود در حل این تعارض دانست؛ رأی **گلوخین** علیه روسیه که یکی نخستین آراء دیوان اروپایی حقوق بشر با موضوع مستقیم تشخیص چهره پلیسی است. **نیکلای گلوخین** در متروی مسکو دست به اعتراضی انفرادی و مسالمت‌آمیز زده و پیکره مقوایی یک فعال سیاسی بازداشت‌شده را با خود حمل کرده بود؛ پلیس در پایش معمول اینترنت به تصاویر این حرکت در تلگرام برخورد، با پردازش تصاویر دوربین‌های مترو از رهگذر فناوری تشخیص چهره او را شناسایی و ظرف چند روز بازداشت کرد و به اتهام برگزاری تجمع بدون اطلاع قبلی به محکومیت اداری رساند (Glukhin v. Russia, 2023, paras. 6-9, 12, 13, 15). دیوان با احراز اینکه شناسایی سریع متقاضی جز با به‌کارگیری تشخیص چهره قابل تبیین نیست، پردازش داده بیومتریک او را مداخله در حق موضوع ماده هشتم دانست و آنگاه در مقام سنجش توجیه این مداخله تصریح کرد که درصدد داوری درباره جواز کلی پردازش داده بیومتریک با فناوری تشخیص چهره نیست و تنها می‌سنجد که پردازش داده‌های شخص متقاضی در این پرونده موجه بوده است یا نه (Glukhin v. Russia, 2023, paras. 72, 73, 85).

پاسخ دیوان منفی بود و مبنای آن، همان دو محوری که در پرونده بریجز و کت گذشت، از نظر دیوان، چارچوب حقوقی

غیرقانونی اعلام کرد و در همان سال، بهره‌گیری از پهنپاد برای نظارت بر تجمعات در معابر عمومی پاریس را نیز فاقد وجهت قانونی شمرد (O'Brien & Micek, 2020: 30). دلالت این آرا از آن جهت درخور تأمل است که حتی در وضعیت‌های اضطراری نظیر همه‌گیری -که رویکردهای امنیت‌محور گرایش به تسامح دارند- مراجع قضایی حاضر نشدند خلأ چارچوب حقوقی متناسب را نادیده بگیرند و بدین‌سان «کیفیت قانون» شرطی است که فقدانش با ضرورت‌های مقطعی جبران‌پذیر نیست.

۳-۲- ضرورت و تناسب: ضابطه‌مندی نگهداری و منع گردآوری انبوه داده

رویه دیوان نشان می‌دهد که حتی گذر از آزمون قانونمندی پایان کار نیست و مداخله باید از آزمون ضرورت نیز عبور کند؛ در همین راستا، در پرونده کت علیه بریتانیا، نام و اطلاعات شخصی یک فعال صلح‌طلب که هرگز به جرمی محکوم نشده بود در پایگاه داده پلیس موسوم به پایگاه داده افراط‌گرایی نگهداری می‌شد و دیوان با مناقشه‌آمیز خواندن تنوع تعاریف «افراط‌گرایی داخلی» حکم داد که نیاز مبرمی به نگهداری این داده‌ها وجود نداشته و به‌ویژه نگهداری داده‌های ناظر بر اعتراضات مسالمت‌آمیز او ضروری نبوده است (Catt v. The United Kingdom, 2019, paras. 123, 124).

ضابطه برآمده از این رأی مکمل ضابطه بریجز است، چه اینکه اگر آنجا ابهام در تعیین اشخاص پایش‌شونده به کیفیت قانون آسیب می‌زد، اینجا ابهام در معیار درج و نگهداری داده، احراز شرط ضرورت را منتفی می‌سازد. وانگهی منطق این رأی، در کنار آنچه در مارپر گذشت، اقتضایی روشن نیز در پی دارد؛ آنجا که نگهداری داده اشخاص فاقد ارتباط با تحقیق خود مداخله‌ای مستقل و مستمر شمرده می‌شود، تعیین تکلیف صریح در باب امحاء این داده‌ها از لوازم گذر از آزمون ضرورت است -اقتضایی که در پایش بیومتریک اهمیتی مضاعف می‌یابد، چه اینکه قاطبه پردازش‌شوندگان در این فناوری از همین دسته‌اند. دیوان همین رویکرد محدودکننده را در مقیاس کلان نیز اعمال کرده است؛ در پرونده بیگز برادر واچ علیه بریتانیا، شعبه عالی دیوان هرچند رهگیری انبوه ارتباطات را علی‌الاطلاق مغایر

نیستند، قانون‌گذار اروپایی به‌طور ایجاب مقرر داشت.

نتیجه‌گیری

پژوهش حاضر با واکاوی تقابل میان رویکرد نظارتی نهادهای انتظامی و حق بر حریم خصوصی شهروندان، نشان داد که بهره‌گیری پلیس از فناوری تشخیص چهره در معابر عمومی و پردازش خودکار و نظام‌مند داده‌های بیومتریک افراد توسط سامانه‌های هوشمند، با نظارت‌های بصری و متعارف انسانی قابل‌قیاس نیست و ماهیتاً مداخله در حقوق فردی محسوب می‌شود، این تفاوت ناشی از آن است که فناوری تشخیص چهره، تصویر عابران را به‌عنوان یک داده شخصی حساس، بدون آگاهی یا رضایت آن‌ها به‌صورت خودکار ثبت و پردازش می‌کند و با شمول فراگیر خود بر تمامی افراد حاضر در اماکن عمومی، اعم از مظنونان و افراد بی‌گناه، حق بر حریم خصوصی را مخدوش می‌سازد. دادگاه‌های اروپایی در پرونده‌های متعددی با تفکیک میان مشاهده انسانی و ثبت سیستماتیک داده‌ها، تأکید کرده‌اند که برای مشروعیت‌بخشی به چنین مداخله گسترده‌ای که مستعد ایجاد حس نظارت دائمی و پروفایل‌سازی جمعیتی است، وجود یک قانون عام یا اذن درون‌سازمانی کلی کفایت نمی‌کند. بر اساس این رویه، مبنای قانونی تجویزکننده این پایش باید از معیار «کیفیت قانون» برخوردار باشد؛ بدین معنا که دامنه صلاحدید پلیس در تعیین اشخاص تحت مراقبت و مکان‌های مجاز برای استقرار دوربین‌ها را به‌دقت و با صراحت ضابطه‌مند سازد.

علاوه بر این، استانداردهای برآمده از این آرا و قانون هوش مصنوعی اتحادیه اروپا، مقرر می‌دارند که این نظارت‌ها باید با ایجاد محدودیت‌های سخت‌گیرانه در زمینه مدت‌زمان نگهداری داده‌ها، حصر اغراض انتظامی، منع گردآوری انبوه و بی‌هدف اطلاعات و الزام به اخذ مجوزهای پیشین از مقامات مستقل قضایی، کنترل و مهار شوند. پیامد این دستاوردها برای نظام حقوقی ایران که در آن حق بر حریم خصوصی مبنای شرعی نظیر منع تجسس دارد و اصول قانون اساسی خروج از آن را تنها «به حکم قانون» مجاز شمرده‌اند تعیین‌کننده است؛ تأمل در منطق حاکم بر استثنائات وارد بر اصل منع تجسس نشان می‌دهد که جواز مداخله در حریم اشخاص همواره ماهیتی

روسیه، با آنکه قانون داده‌های شخصی و قانون پلیس را در خود داشت، به سبب کلیت و فقدان هرگونه تحدید دامنه و تضمین آیینی در برابر خودسری، فاقد کیفیت لازم برای مهار چنین مداخله شدیدی تشخیص داده شد. ماهیت «به‌شدت مداخله‌گر» این فناوری، سطحی بالاتر از توجیه و تضمین‌هایی قوی‌تر می‌طلبد. وانگهی دیوان از این نیز فراتر رفت و اعلام داشت که به‌کارگیری فناوری تشخیص چهره به‌شدت مداخله‌گر برای شناسایی و بازداشت شرکت‌کنندگان در اقدامات اعتراضی مسالمت‌آمیز می‌تواند اثری بازدارنده بر حق‌های بنیادین بر جای نهد و رفتار **گلوخین** متضمن هیچ عمل نکوهیده‌ای نبوده که نیازی اجتماعی و مبرم به پایش او پدید آورد (Glukhin v. Russia, 2023, paras. 88,89). بدین ترتیب **گلوخین** حلقه‌های پراکنده رویه پیشین را به زنجیره‌ای واحد پیوند می‌دهد که آن را می‌توان این‌گونه صورت‌بندی کرد که تصویر چهره داده شخصی است، پردازش بیومتریک آن مداخله است، مداخله محتاج قانونی واجد کیفیت است، کیفیت قانون با اذن عام و بی‌تضمین جمع نمی‌شود و شدت مداخله‌گری این فناوری، آستانه توجیه ضرورت را نیز بالا می‌برد.

آنچه بر اعتبار این آرا می‌افزاید آن است که قانون‌گذار اتحادیه اروپا تقریباً همین ضوابط قضایی را به قالب تقنینی نیز درآورده است. ماده پنجم قانون هوش مصنوعی اتحادیه، شناسایی بیومتریک از راه دور در زمان واقعی در فضاهای عمومی را برای اغراض انتظامی علی‌الاصول ممنوع ساخته و آن را تنها در مصادیقی حصری (همچون جست‌وجوی قربانیان آدم‌ربایی، دفع خطر قریب‌الوقوع تروریستی و ردیابی مظنونان جرائم مهم احصاشده) روا شمرده است (Artificial Intelligence Act, (2024, Art. 5, para. 1(h)(i-iii)) و حتی در همین مصادیق نیز بهره‌برداری را به ارزیابی پیشینی آثار بر حق‌های بنیادین (Artificial Intelligence Act, 2024, Art. 5, para. 2) و مهم‌تر از همه، کسب مجوز پیشینی مقام قضایی یا مقام اداری مستقل منوط کرده است (Artificial Intelligence Act, 2024, Art. 5, para. 3). به بیان روشن‌تر، آنچه دیوان در استدلال‌های خود به زبان سلبی بیان کرد مبنی بر اینکه که اذن عام و چارچوب‌های کلی برای مهار این فناوری کارآمد

- زرکلام، ستار و عبدی، قاسم (۱۳۹۳). «جایگاه حریم خصوصی در سیاست جنایی تقنینی ایران». *قضاوت*، ۱۴(۷۹): ۲۹-۴۷.

- ساریخانی، عادل (۱۳۹۷). «حقوق شهروندی متهم در تعامل پلیس در قانون آیین دادرسی کیفری ۱۳۹۲ و اصلاحی ۱۳۹۴». *پژوهش‌های اطلاعاتی و جنایی*، ۱۳(۴۹): ۲۰۷-۲۳۲.

- ظفریان، طیبه؛ اسلامی فارسانی، رحیم و صادقی ده‌صحرایی، مرتضی (۱۴۰۴). «حفظ حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی». *مطالعات حقوقی فضای مجازی*، ۴(۱): ۴۲-۵۵.

- محسنی، فرید و میرعماد، محمدحسین (۱۳۹۸). «مبانی و استثنائات حریم خصوصی در اسلام و حقوق ایران از دیدگاه حقوق عمومی». *آموزه‌های حقوقی گواه*، ۵(۲): ۲۵۱-۲۷۶.

- میرزوند، رضوانه و معتمدنژاد، رؤیا (۱۴۰۴). «پردازش داده‌های بیومتریک و تأثیر آن بر زندگی خصوصی با تأکید بر قوانین اتحادیه اروپا و شورای اروپا». *پژوهش حقوق عمومی*، ۲۶(۸۶): ۲۳۵-۲۷۲.

ب. منابع لاتین (کتاب و مقالات)

- Barfield, W & Pagallo, U (2020). *Advanced Introduction to Law and Artificial Intelligence*. Edward Elgar Publishing.
<https://doi.org/10.4337/9781789905137>

- Miller, S & Bossomaier, T (2024). *Cybersecurity, Ethics, and Collective Responsibility*. Oxford University Press.

- Brayne, S (2017). "Big Data Surveillance: The Case of Policing". *American Sociological Review*, 82(5): 977-1008.
<https://doi.org/10.1177/0003122417725865>

- Buckley, B., & Hunter, M. (2011). "Say Cheese! Privacy and Facial Recognition". *Computer Law & Security Review*, 27(6): 637-640.
<https://doi.org/10.1016/j.clsr.2011.09.011>

- Dul, C. (2022). "Facial Recognition Technology VS Privacy: The Case of Clearview AI". *Queen Mary Law Journal*, 1.

استثنایی و محدود داشته و با ماهیت فراگیر و مستمر پایش بیومتریک در فضاهای عمومی در تضاد قرار دارد و همگام با اصول سند ملی هوش مصنوعی مبنی بر لزوم رعایت حریم خصوصی، پلیس ایران برای مشروعیت‌بخشی به استفاده از این فناوری و پیش از استقرار سامانه‌های شناسایی بیومتریک در اماکن عمومی، نیازمند تصویب یک مبنای تقنینی مشخص از سوی مجلس است و این قانون باید با گذر از رویکردهای صرفاً امنیت‌گرا، تضمین‌های عینی تحدید قدرت را به همراه داشته باشد؛ حصر جواز پایش به جرائم بسیار مهم و تهدیدات مسلم، الزام به اخذ مجوز موردی و پیشین از مقام قضایی برای هرگونه استقرار سامانه، تأسیس سازوکارهای نظارت مستقل فراسازمانی و تعیین تکالیف صریح در خصوص امحای فوری داده‌های عابران غیرمظنون، از مهم‌ترین الزامات پیشنهادی این قانون خواهد بود.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات مقاله تماماً رعایت گردید.

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافی بوده است.

سهم نویسندگان: نگارش مقاله به‌صورت مشترک توسط نویسندگان انجام گرفته است.

تشکر و قدردانی: بدین‌وسیله لازم است مراتب تقدیر و سپاس خود را از جناب آقای دکتر اکبر علیزاده، از معاونت حقوقی و امور مجلس فراجا، به‌پاس پیگیری‌های مجدانه و زحمات بی‌دریغ ایشان در مراحل مختلف این پژوهش ابراز نماییم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان‌یافته است.

منابع و مأخذ

الف. منابع فارسی

- حسینی‌کاشانی، سید روح‌الله؛ شریفی، عنایت و علوی، سید محمود (۱۳۹۸). «مبانی انسان‌شناختی حق بر حریم خصوصی از دیدگاه اسلام». *مطالعات حقوقی*، ۱۱(۳): ۴۱-۶۹.

د- آراء دیوان اروپایی حقوق بشر

- European Court of Human Rights (Chamber). (1995, January 31). *Friedl v. Austria* (Application no. 15225/89). Strasbourg. (Struck out Following Friendly Settlement; Commission Report of 19 May 1994).
- European Court of Human Rights (Third Section). (2001, September 25). *P.G. and J.H. v. the United Kingdom* (Application no. 44787/98). Strasbourg.
- European Court of Human Rights (Fourth Section). (2003, January 28). *Peck v. the United Kingdom* (Application no. 44647/98). Strasbourg.
- European Court of Human Rights (Grand Chamber). (2008, December 4). *S. and Marper v. the United Kingdom* (Applications nos. 30562/04 and 30566/04). Strasbourg.
- European Court of Human Rights (First Section). (2009, January 15). *Reklos and Davourlis v. Greece* (Application no. 1234/05). Strasbourg.
- European Court of Human Rights (Second Section). (2017, November 28). *Antović and Mirković v. Montenegro* (Application no. 70838/13). Strasbourg.
- European Court of Human Rights (First Section). (2019, January 24). *Catt v. the United Kingdom* (Application no. 43514/15). Strasbourg.
- European Court of Human Rights (First Section). (2020, February 13). *Gaughran v. the United Kingdom* (Application no. 45245/15). Strasbourg.
- European Court of Human Rights (Grand Chamber). (2021, May 25). *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15). Strasbourg.

- Gordon, B (2021). "Automated Facial Recognition in Law Enforcement: The Queen (on Application of Edward Bridges) V The Chief Constable of South Wales Police". *Potchefstroom Electronic Law Journal*, 24(1).
- Manheim, K & Kaplan, L (2019). "Artificial Intelligence: Risks to Privacy and Democracy". *Yale Journal of Law & Technology*, 21(106).
- Oswald, M; Grace, J; Urwin, S & Barnes, G. C (2018). "Algorithmic Risk Assessment Policing Models: Lessons From the Durham HART Model and 'Experimental' Proportionality". *Information & Communications Technology Law*, 27(2): 223–250.
<https://doi.org/10.1080/13600834.2018.1458455>
- Smith, M & Miller, S (2022). "The ethical Application of Biometric Facial Recognition Technology". *AI & Society*, 37(1): 167–175.
<https://doi.org/10.1007/s00146-021-01199-9>
- Stark, R (2021). "China's Use of Artificial Intelligence in Their War Against Xinjiang". *Tulane Journal of International & Comparative Law*, 29(153).
- Tzanou, M., & Karyda, S. (2022). "Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?" *European Public Law*, 28(1).
<https://doi.org/10.54648/euro2022007>
- Warren, S. D & Brandeis, L. D (1890). "The Right to Privacy". *Harvard Law Review*, 4(5): 193-220.

ج- گزارش‌ها

- Fussey, P & Murray, D (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. University of Essex Human Rights Centre.
- O'Brien, L & Micek, P (2020). *Defending Peaceful Assembly and Association in the Digital Age: Takedowns, Shutdowns, and Surveillance*. Access Now.

- European Court of Human Rights (Third Section). (2023, July 4). *Glukhin v. Russia* (Application no. 11519/20). Strasbourg.

و- آراء دیوان دادگستری اتحادیه اروپا

- Court of Justice of the European Union (Grand Chamber). (2014, April 8). *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others; Kärntner Landesregierung and Others* (Joined Cases C-293/12 and C-594/12). ECLI:EU:C:2014:238.
- Court of Justice of the European Union (Grand Chamber). (2015, October 6). *Maximillian Schrems v. Data Protection Commissioner* (Case C-362/14). ECLI:EU:C:2015:650.

ه- آراء دادگاه‌های ملی

- Court of Appeal of England and Wales (Civil Division). (2020, August 11). *R (Bridges) v. Chief Constable of South Wales Police and Others* (Case No. C1/2019/2670; Neutral Citation Number: [2020] EWCA Civ 1058). Royal Courts of Justice.

ی- اسناد و مقررات

- Council of Europe. (1950, November 4). Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), ETS No. 005. Rome.
- European Parliament and Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L Series. <http://data.europa.eu/eli/reg/2024/1689/oj>