Comparative Evaluation of Legal Mechanisms in Iran and the European Union in Addressing Deepfake Pornography

Abstract

The emergence of deepfake technology, particularly in the form of digital pornography, poses serious threats to privacy and human dignity in the online environment. Produced through artificial intelligence and deep learning techniques, this phenomenon inflicts substantial psychological and social harm on victims. Accordingly, addressing such content, particularly from a legal perspective, requires the development of effective legislative and enforcement mechanisms. This article undertakes a comparative analysis of the legal frameworks of Iran and the European Union for combating deepfake pornography. Using a descriptive and analytical method, and drawing on library sources and reputable scholarly articles, the study examines the existing laws in Iran and the European Union in terms of their responses to deepfake related challenges. Within the Iranian legal system, provisions such as Article 14 of the Computer Crimes Act and Article 16 of the same statute, particularly with respect to defamation through alteration of digital content, address this threat. In the European Union, the Artificial Intelligence Act and the Digital Services Act establish frameworks for the removal of illegal content and the liability of platforms. The findings indicate that in Iran, despite existing regulations, challenges persist, including the lack of clear criteria for reputational harm and insufficient technical infrastructure for detecting deepfakes. In the European Union, although the legal frameworks are comparatively more comprehensive in relation to content removal and platform responsibility, issues such as technical divergences in detection and the transnational enforcement of rules remain. Finally, the study analyzes how combining the legal capacities of Iran and the European Union can generate innovative solutions for the evolution of legislative mechanisms to counter deepfakes in Iran, and on this basis, the Union's framework, relying concurrently on the Artificial

Intelligence Act, the Digital Services Act, and the General Data Protection Regulation, outlines an integrated scheme for the regulation of illegal content and the reinforcement of victim protection. Through mechanisms of transparency, labeling, and on platform reporting, this scheme promotes platform accountability and responsiveness, although its implementation faces cross border and technical challenges. In Iran, criminal categories addressing obscene and manipulated content provide initial coverage, yet practical effectiveness remains limited due to conceptual ambiguity and the absence of clear criteria for identifying deepfakes. Deficiencies in enforcement mechanisms and limited technical capacity for detection hinder the effectiveness of legal responses, underscoring the need to strengthen infrastructure and specialized institutions. Optimizing the national response requires revising and adopting context sensitive rules aligned with the European Union approach, with a focus on content governance and victim support. The development of diagnostic tools, the education and empowerment of law enforcement and judges, and the drafting of protocols for the preservation of digital evidence provide the operational foundation for this transformation. Advancing this trajectory becomes feasible and measurable through a time bound roadmap, the designation of a single coordinating authority, and periodic regulatory impact assessments.

Keywords:Pornography,Deepfake,Artificial Intelligence, Artificial Intelligence Law, Privacy, Human Dignity.

ارزیابی تطبیقی سازوکارهای حقوقی ایران و اتحادیه اروپا در مقابله با پورنوگرافی (هرزه‌نگاری) دیپ‌فیک (جعل عمیق)

چکیده

ظهور پدیده دیپ‌فیک، به‌ویژه در قالب پورنوگرافی دیجیتال، تهدیدات جدی برای حریم خصوصی و کرامت انسانی افراد در فضای دیجیتال به همراه دارد. این پدیده که با استفاده از فناوری‌های هوش مصنوعی و یادگیری عمیق تولید می‌شود، موجب آسیب‌های روانی و اجتماعی فراوانی برای قربانیان می‌گردد. ازاین‌رو، مقابله با این نوع محتوا، به‌ویژه در حوزه‌های حقوقی، نیازمند تدوین سازوکارهای تقنینی و اجرایی مؤثر است. در این مقاله، سازوکارهای حقوقی ایران و اتحادیه اروپا برای مقابله با پورنوگرافی دیپ‌فیک موردبررسی تطبیقی قرار گرفته است. این پژوهش با استفاده از روش توصیفی – تحلیلی و مراجعه به اسناد کتابخانه‌ای و مقالات علمی معتبر، قوانین موجود در ایران و اتحادیه اروپا را از نظر پاسخ به چالش‌های مرتبط با دیپ‌فیک تحلیل کرده است. در سیستم حقوقی ایران، قوانین چون ماده ١٤ قانون جرائم رایانه‌ای و ماده ١٦ همان قانون به‌ویژه در زمینه هتک حیثیت از طریق تغییر محتوای دیجیتال، به مقابله با این تهدید پرداخته‌اند. در اتحادیه اروپا، «قانون هوش مصنوعی» و «قانون خدمات دیجیتال» چارچوب‌هایی را برای حذف محتوای غیرقانونی و مسئولیت پلتفرم‌ها در نظر گرفته‌اند. نتایج این مقاله نشان می‌دهد که در ایران، باوجود قوانین موجود، چالش‌هایی همچون عدم شفافیت معیارهای هتک حیثیت و کمبود زیرساخت‌های فنی برای تشخیص دیپ‌فیک وجود دارد. در اتحادیه اروپا نیز، اگرچه چارچوب‌های قانونی به‌ویژه در زمینه حذف محتوا و مسئولیت پلتفرم‌ها به طور جامع‌تر هستند، اما مشکلاتی چون تفاوت‌های فنی در تشخیص و اجرای قوانین در سطح فراملی همچنان مطرح است. در نهایت، این پژوهش به تحلیل این نکته می‌پردازد که چگونه ترکیب ظرفیت‌های قانونی ایران و اتحادیه اروپا می‌تواند راه‌حل‌های نوآورانه‌ای را در جهت تکامل سازوکارهای تقنینی برای مقابله با دیپ‌فیک‌ها در ایران فراهم آورد براین‌اساس، چارچوب اتحادیه اروپا با اتکای هم‌زمان به «قانون هوش مصنوعی»، «قانون خدمات دیجیتال» و «مقررات عمومی حفاظت از داده‌ها»، منظومه‌ای یکپارچه برای تنظیم محتوای غیرقانونی و تقویت حمایت از قربانیان ترسیم می‌کند. این منظومه با سازوکارهای شفاف‌سازی، برچسب‌گذاری و گزارش‌دهی درون سکویی، مسئولیت‌پذیری و پاسخ‌گویی

سکوها را ارتقا می‌دهد، هرچند اجرای آن با چالش‌های فرامرزی و فنی مواجه است. در ایران، عناوین کیفری ناظر بر محتوای مستهجن و دست‌کاری‌شده پوشش اولیه را فراهم می‌کنند؛ اما به سبب ابهام مفهومی و فقدان معیارهای شناسایی دیپ‌فیک، کارایی عملی محدود می‌ماند. کاستی در سازوکارهای اجرایی و کمبود ظرفیت فنی تشخیص، مانع اثربخشی پاسخ حقوقی شده و ضرورت تقویت زیرساخت‌ها و نهادهای تخصصی را پررنگ می‌سازد. بهینه‌سازی پاسخ ملی مستلزم بازنگری و تصویب قواعد بومی‌سازی‌شده هم‌تراز با رویکرد اتحادیه اروپا با تمرکز بر مدیریت محتوا و حمایت از زیان‌دیدگان است. توسعه ابزارهای تشخیصی، آموزش و توانمندسازی ضابطان و قضات و تدوین پروتکل‌های حفظ ادله دیجیتال، پایه اجرایی این تحول را فراهم می‌کند. پیشبرد این مسیر با نقشه راه زمان‌بندی‌شده، تعیین متولی هماهنگی واحد و ارزیابی‌های دوره‌ای اثرسنجی مقررات، امکان‌پذیر و سنجش‌پذیر می‌شود.

کلیدواژه‌ها: پورنوگرافی، دیپ‌فیک، هوش مصنوعی، قانون هوش مصنوعی، حریم خصوصی، کرامت انسانی.

مقدمه

در دنیای معاصر، با پیشرفت‌های روزافزون در زمینه‌های هوش مصنوعی و یادگیری عمیق، فناوری‌هایی همچون دیپ‌فیک ظهور کرده‌اند که به‌ویژه در تولید محتوای دیجیتال جعلی، از جمله تصاویر و ویدئوهای دست‌کاری‌شده، نقش مهمی ایفا می‌کنند. دیپ‌فیک‌ها، به‌ویژه در زمینه پورنوگرافی و محتوای مستهجن، تهدیدات جدی برای حریم خصوصی و کرامت انسانی افراد ایجاد کرده‌اند. این نوع محتوا، با توانایی بازنمایی غیرواقعی افراد در موقعیت‌های جنسی یا توهین‌آمیز، می‌تواند آسیب‌های جبران‌ناپذیری به حیثیت اجتماعی افراد وارد کند. در این راستا، توجه به سازوکارهای تقنینی برای مقابله با این پدیده، امری ضروری به نظر می‌رسد، چرا که چالش‌های حقوقی و اجتماعی متعددی را پیشروی جوامع و نظام‌های حقوقی می‌گذارد. این ضرورت، به‌ویژه برای کشورهایی مانند ایران که با این پدیده مواجه هستند، نیازمند تحلیل دقیق قوانین موجود و بررسی راهکارهای عملی برای بهبود وضعیت است.

در سطح جهانی، بسیاری از کشورها به‌ویژه اتحادیه اروپا، با تدوین قوانین و مقرراتی همچون «قانون هوش مصنوعی»، «قانون خدمات دیجیتال» و «مقررات عمومی حفاظت از داده‌ها»، به مقابله با تهدیدات دیپ‌فیک پرداخته‌اند. این قوانین باهدف ایجاد توازن میان حفاظت از حقوق فردی و مقابله با محتوای مضر، سازوکارهای حقوقی و اجرایی مشخصی را برای شناسایی، حذف و جلوگیری از انتشار محتوای غیرقانونی فراهم کرده‌اند. این اقدامات از منظر حقوق بشری و آزادی‌های فردی نیز بادقت زیادی تدوین شده‌اند تا از سوءاستفاده‌های احتمالی جلوگیری کنند.

در ایران، باوجود پیشرفت‌های قانونی در زمینه حقوق دیجیتال، خلأهایی در مقوله مقابله با دیپ‌فیک‌های پورنوگرافیک وجود دارد. از جمله این قوانین، می‌توان به «قانون جرائم رایانه‌ای» و «قانون مجازات اسلامی» اشاره کرد که در برخی موارد، به‌ویژه در مواجهه با پدیده‌های نوین مانند دیپ‌فیک، پاسخ‌گویی کافی ندارند. این مسئله ضرورت دارد که قوانین ایران باتوجه‌به

تحولات جهانی و به‌ویژه سازوکارهای قانونی در اتحادیه اروپا، بازنگری و به‌روزرسانی شوند تا بتوانند با تهدیدات دیجیتال همگام شوند.

بر اساس این مباحث، هدف این پژوهش بررسی تطبیقی سازوکارهای حقوقی ایران و اتحادیه اروپا برای مقابله با پدیده دیپ‌فیک است. این تحقیق بر آن است تا خلأهای قانونی موجود در نظام حقوقی ایران را شناسایی کرده و پیشنهاداتی برای تقویت و به‌روزرسانی پاسخ‌های قانونی به این پدیده نوظهور ارائه دهد. پژوهش حاضر با استفاده از روش توصیفی – تحلیلی و با بررسی قوانین موجود در ایران و اتحادیه اروپا، به تحلیل و مقایسه سازوکارهای اجرایی و تقنینی در هر دو حوزه پرداخته است.

پیشینه پژوهش نشان می‌دهد که آثار زیادی در زمینه دیپ‌فیک و چالش‌های حقوقی آن منتشر شده است. به‌عنوان نمونه، مقاله اکبری و همکاران (۱۴۰۱) با عنوان: «تحلیل پدیده مجرمانه دیپ‌فیک‌ها (جعل‌های رایانه‌ای پیچیده) با نگاهی به سیاست کیفری ایران و چالش‌های حقوق بشری» به تحلیل ابعاد مختلف پدیده دیپ‌فیک در سیاست کیفری ایران پرداخته است و بر لزوم اصلاحات قانونی در این حوزه تأکید دارد. در همین راستا، مقاله شیری (۱۴۰۱) با عنوان: «دیپ‌فیک یا همانندسازی صوتی یا تصویری غیرواقعی در حقوق کیفری» نیز به تحلیل جنبه‌های حقوق کیفری دیپ‌فیک‌ها پرداخته و بر نیاز به بازنگری در قوانین ایران برای جرم‌انگاری دقیق‌تر این پدیده تأکید می‌کند. اما در این تحقیق، توجه اصلی به مقایسه تطبیقی و بررسی ظرفیت‌های حقوقی اتحادیه اروپا در مقابله با دیپ‌فیک‌ها است که در مقالات پیشین کمتر موردتوجه قرار گرفته است.

این پژوهش در تلاش است تا با استفاده از تجربیات قانونی اتحادیه اروپا، راهکارهای عملی برای تقویت و به‌روزرسانی نظام حقوقی ایران در مقابله با دیپ‌فیک‌های پورنوگرافیک ارائه دهد. در این راستا، سؤالات اصلی پژوهش عبارت‌اند از: نخست، چه سازوکارهایی در حقوق ایران برای مقابله با دیپ‌فیک‌ها وجود دارد و آیا این سازوکارها می‌توانند به طور مؤثر با تهدیدات این

فناوری مقابله کنند؟ دوم، اتحادیه اروپا چه اقداماتی را در زمینه مقابله با دیپ‌فیک‌ها به کار گرفته است و چقدر این اقدامات می‌توانند برای ایران باتوجه‌به ویژگی‌های خاص فرهنگی و حقوقی آن مناسب و قابل‌اجرا باشند؟

در پایان از حیث ساختار، ابتدا به واکاوی و تبیین مفاهیم بنیادین دیپ‌فیک و پورنوگرافی پرداخته می‌شود تا حدود و ثغور مفهومی روشن گردد، سپس بنیادهای نظری جرم‌انگاری پورنوگرافی مبتنی بر دیپ‌فیک بررسی و نسبت آن با آزادی‌های مشروع و صیانت از کرامت انسانی تبیین می‌شود و در ادامه سازوکارهای حقوقی ایران از حیث تقنینی و اجرایی تحلیل و ارزیابی می‌گردد، آنگاه چارچوب‌های اتحادیه اروپا با رویکردی تحلیلی و انتقادی واکاوی می‌شود تا ظرفیت‌ها و محدودیت‌های آن آشکار شود، و سرانجام نتیجه‌گیری با جمع‌بندی یافته‌ها و ترسیم مسیرهای سیاست‌گذاری و اصلاح تقنینی و اجرایی پیشنهاد می‌شود.

۱. تبیین مفاهیم

۱-۱. پورنوگرافی[1](هرزه‌نگاری)

اصطلاح «پورنوگرافی» ریشه‌ای تاریخی دارد که از زبان یونانی باستان به زبان‌های معاصر منتقل شده است. بخش نخست آن، پورنو، در زبان یونانی کلاسیک به معنای «فاحشه» یا «برده جنسی» بوده و در متون ادبی یونان باستان برای توصیف فعالیت‌های جنسی خارج از چهارچوب اخلاق غالب جامعه به کار می‌رفته است (Löfgren-Mårtenson, 2008: 306) . بخش دوم، «گرافی»، از فعل graphein به معنای «نوشتن» یا «ثبت‌کردن» مشتق شده و در زبان امروزی نشانگر «نمایش» یا «بازنمایی» است (Hayes & Paul, 2007: 517) . در گذار معنا، پورنوگرافی به نمایش صریح کنش‌های جنسی گفته می‌شود؛ صحنه‌هایی که هدف اصلی آن‌ها تحریک مخاطب است نه انتقال پیام هنری یا آموزشی. این هدف‌گذاری برانگیختگی جنسی، نقطهٔ تمایز این محتوا از

[1]. Pornography.

آثار ادبی و علمی است و در بسیاری از نظام‌های حقوقی بر مبنای معیارهای «تمایل به شهوت» و «فاقد ارزش روشنگرانه» جرم‌انگاری یا محدود می‌شود (رضایی، ۱۳۹٦: ۱۰۵؛ موسوی، ۱۳۹٤:۵۰).

در ادبیات تقنینی ایران، واژه «پورنوگرافی» به طور صریح به کار نرفته است، اما قوانین مرتبط با آن در چارچوب‌هایی همچون «منافی عفت عمومی»، «مبتذل»، «مستهجن» و «جریحه‌دار کردن عفت و اخلاق عمومی» مطرح شده‌اند. به‌ویژه، در فصل هجدهم قانون مجازات اسلامی مصوب ۱۳۹۲ (ماده ٦۳۹)، نشر تصاویر یا مطالب مستهجن به‌عنوان «عمل مخالف عفت عمومی» شناخته شده و مرتکبان آن به حبس و شلاق محکوم می‌شوند. همچنین، ماده ۲۵ قانون جرائم رایانه‌ای مصوب ۱۳۸۸، هرگونه «محتوای مبتذل و مخل عفت عمومی» را جرم اعلام کرده و برای مرتکبان مجازات‌هایی از جمله حبس و جزای نقدی در نظر گرفته است. علاوه بر این، تبصره ٤ ماده ۷٤۲ قانون مجازات اسلامی مقرر می‌دارد: «انتشار، توزیع یا معامله محتویات مستهجن، اعم از واقعی یا غیرواقعی، جرم محسوب می‌شود.» ذکر قید «واقعی یا غیرواقعی» در این تبصره به‌وضوح دامنهٔ شمول آثار مستهجن را توسعه داده و محتوای جعلی دیجیتال همچون پورنوگرافی دیپ‌فیک را نیز در بر می‌گیرد؛ زیرا حتی در صورت فقدان برهنگی واقعی یا آمیزش واقعی، بازنمایی واقع‌نما و گمراه‌کننده همچنان مشمول جرم‌انگاری است.

همچنین، تبصره ۵ بند (الف) ماده ۲ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌کنند مصوب ۱۳۸٦، «آثار سمعی و بصری مستهجن» را چنین تعریف کرده است: «آثاری که محتوای آن‌ها نمایش برهنگی زن و مرد یا اندام تناسلی یا نمایش آمیزش جنسی باشد». این تعریف، معیار صریحی برای تشخیص «مستهجن» ارائه می‌دهد و در صورت انطباق محتوای دیپ‌فیک با این ویژگی‌ها، قابلیت تطبیق کامل دارد.

نکته قابل‌توجه آن است که قانون‌گذار در برابر اصطلاح «مبتذل» تعریف روشنی ارائه نکرده است. در دکترین حقوقی، «مبتذل» به آثاری گفته می‌شود که فاقد ارزش هنری و فرهنگی بوده و بیشتر به تحریک شهوت سطحی منجر می‌شوند (بابایی، ۱۳۹۷: ۱۵٤). بنابراین دیپ‌فیک‌هایی که فاقد نمایش کامل جنسی‌اند، اما از طریق دست‌کاری چهره یا حرکات بدن القای محتوای جنسی

می‌کنند، ذیل این عنوان قرار می‌گیرند. ضعف این اصطلاح در نسبیت و وابستگی آن به عرف اجتماعی است که باعث ناامنی قضایی می‌شود.

در خصوص «مستهجن»، همان‌گونه که اشاره شد، معیار نمایش صریح برهنگی و آمیزش جنسی (اعم از واقعی یا غیرواقعی) دقیق‌ترین ملاک در قوانین ایران است. به همین دلیل، مصادیق پورنوگرافی دیپ‌فیک درصورتی‌که شامل برهنگی یا آمیزش باشند، حتی به شکل الگوریتمی[1] و جعلی، به‌روشنی مشمول این تعریف می‌شوند.

اصطلاح «منافی عفت عمومی» مفهومی فراگیر و کلی است که قانون‌گذار در ماده ٦٣٩ قانون مجازات اسلامی برای جرم‌انگاری کلی‌تر به کار گرفته است. این اصطلاح هم مصادیق مبتذل و هم مستهجن را در بر می‌گیرد. هرچند کارکرد آن انعطاف‌پذیری در پوشش موارد متنوع است، اما کلی بودن آن با اصل تفسیر مضیق قوانین کیفری تعارض دارد و ممکن است دست قاضی را برای برداشت‌های موسع باز گذارد (الله‌وردی، ۱۳۹۹: ٤٥).

«جریحه‌دار کردن عفت و اخلاق عمومی» نیز از تعابیر عام و سیالی است که به‌ویژه در فقه و رویه قضایی برای مواردی به کار می‌رود که الزاماً برهنگی یا آمیزش در کار نیست، اما شأن عمومی جامعه از بازنمایی آن آسیب می‌بیند. در حوزه دیپ‌فیک، این عنوان می‌تواند شامل ویدئوهایی باشد که فرد را حتی بدون نمایش اندام جنسی، در وضعیت‌های تحقیرآمیز یا خلاف شأن نشان می‌دهند (عبدی و دیگران، ۱۳۹۲: ٤٨).

این قوانین در تلاش‌اند تا با برخورد قاطع با نشر محتوای مستهجن، حفاظت از اخلاق عمومی را تضمین کنند. در مقایسه، دیوان عدالت اتحادیه اروپا رویکردی متوازن در مواجهه با پدیده‌هایی چون پورنوگرافی دیپ‌فیک اتخاذ کرده است که به‌ویژه بر حقوق بشر و آزادی‌های

---

[1]. الگوریتم در معنای فنی، مجموعه‌ای متناهی از قواعد دقیق است که در قالب کد اجرا می‌شود و به رایانه می‌گوید چگونه داده‌ها را پردازش کند و ورودی‌های تصویری یا صوتی را به خروجی تبدیل نماید.

در زمینه این پژوهش، الگوریتم‌های مبتنی بر یادگیری عمیق با استخراج الگوهای آماری از هزاران نمونه آموزشی، ساختار چهره و حرکت را می‌آموزند و می‌توانند چهره فردی را بر پیکره دیگری بنشانند یا صحنه‌ای جعلی بسازند که واقعی به نظر می‌رسد.این سازوکار مبنای فنی تولید رسانه‌های دیپ‌فیک است و مدل‌های مولد رایج مانند شبکه‌های مولد خصمانه و مدل‌های انتشار از همین جنس‌اند، و در این مقاله هرجا از «الگوریتم» سخن می‌رود همین معنا اراده شده است.

فردی تأکید دارد (Peguera, 2020: 115–118) . درحالی‌که قوانین ایران بر مقابله با محتوای مخل عفت عمومی تمرکز دارند، در اتحادیه اروپا، تلاش برای حفظ آزادی‌های فردی و حقوق بشر در کنار مقابله با چنین محتوای دیجیتال آسیب‌زا، موردتوجه قرار گرفته است. هر دو نظام حقوقی در صدد توازن میان حقوق فردی و منافع عمومی هستند[1] .

با لحاظ مجموعهٔ تعاریف تاریخی، تقنینی و تحلیل‌های نظری، به نظر نگارندگان مناسب‌ترین تعریف از پورنوگرافی، آن است که علاوه بر نمایش صریح کنش‌های جنسی و هدف‌گذاری بر تحریک شهوانی، شامل بازنمایی‌های غیرواقعی و الگوریتمی نیز بشود، هرچند فاقد برهنگی واقعی باشد. نقطهٔ مشترک در همهٔ این تعاریف، تعرض به حریم جنسی و کرامت انسانی است؛ خواه از رهگذر مستهجن به معنای صریح قانونی (نمایش برهنگی و آمیزش)، خواه از طریق مبتذل به معنای فقدان ارزش و تحریک سطحی، یا حتی منافی عفت عمومی به‌مثابه مفهومی جامع و فراگیر. ازاین‌رو، در فضای نوین فناوری، «پورنوگرافی دیپ‌فیک» به‌عنوان بازنمایی واقع‌نما و بدون رضایت، مصداق بارز پورنوگرافی محسوب می‌شود و تعریف موسع قانون‌گذار ایران در تبصره ٤ ماده ٧٤٢ (واقعی یا غیرواقعی بودن) بهترین پشتوانهٔ حقوقی برای پوشش این پدیده است. بدین‌سان، تعریف مطلوب، آن است که میان سنت حقوقی ایران و تحولات دیجیتال پیوند برقرار کند و هم‌زمان بر اصل بنیادین حمایت از کرامت انسانی استوار باشد.

۱-۲. دیپ‌فیک[2](جعل عمیق)

---

[1]. با وجود این همسویی غایت، مراد از «توازن» برابری وزنی میان حقوق فردی و منافع عمومی نیست. در نظام ایران، صیانت از عفت و نظم عمومی پررنگ‌تر است و واکنش‌ها بیش‌تر معطوف به مهار مصادیق مخل است. در اتحادیه اروپا، پاسداشت حقوق بنیادین در کنار حکمرانی بر محتوای غیرقانونی برجسته است و مسئولیت‌پذیری سکوها محوریت دارد. بدین‌سبب، شیوه‌های وزن‌دهی و ابزارهای اجرا یکسان به دست نمی‌آید و نتایج عملی می‌تواند متفاوت باشد. ازاین‌رو، توازن به معنای توجه هم‌زمان به هر دو دسته منفعت در چارچوب‌های متمایز و متناسب با بستر نهادی هر نظام است.این بیان ناظر به مقررات و رویه‌های مورد بحث است و ادعای تعمیم فراتر از دامنه آن‌ها ندارد.

[2].Deepfake.

در ماده ۳ (٦٠) «قانون هوش مصنوعی»[1] اتحادیه اروپا ، «دیپ‌فیک» چنین تعریف شده است: «محتوای تصویری، صوتی یا ویدئویی که با هوش مصنوعی تولید یا دست‌کاری شده و شباهتی گمراه‌کننده با افراد، اشیاء، مکان‌ها، نهادها یا رویدادهای واقعی پیدا می‌کند، به‌گونه‌ای‌که بیننده آن را اصیل یا موثق تلقی می‌کند». از نظر ساختاری و محتوایی این تعریف تقریباً با بند (ک) (۱) ماده ۳۵ مقررات خدمات دیجیتال[2] همپوشانی دارد، اگرچه در آن قانون صراحتاً از عبارت «دیپ‌فیک» استفاده نشده است.

بااین‌همه در بند ۱۳٤ همان «قانون هوش مصنوعی اتحادیه اروپا» اصطلاح «شباهت محسوس[3]» به متن تعریف افزوده شده است تا بر میزان شباهت قابل‌رؤیت تأکید کند. به‌موجب این بند، «سامانهٔ هوش مصنوعی باید محتوایی را به‌گونه‌ای شبیه واقعیت بسازد یا دست‌کاری کند که بینندهٔ متعارف آن را به‌اشتباه به‌عنوان محتوای اصیل بپذیرد».

ورود واژه «شباهت محسوس» به قانون هوش مصنوعی اتحادیه اروپا معانی متفاوت و گاه متضادی را به همراه دارد؛ از یک‌سو می‌تواند معیار سخت‌گیرانه‌تری برای شناسایی دیپ‌فیک تعیین کند و از سوی دیگر ممکن است تنها توصیفی توضیحی باشد که کمکی به تعریف اصلی دیپ‌فیک نمی‌کند. این تفاوت واژگانی میان ماده و تبصره، مرز روشن‌بین محتوای قابل‌قبول و ممنوعه را مبهم می‌سازد و نشان می‌دهد که قانون‌گذاران اروپایی درباره آستانه شباهت «دیپ‌فیک» نیازمند دقت و یکپارچگی بیشتری هستند (Labuz, 2024:787) .

علاوه بر این، فقدان معیارهای فنی مشخص برای اندازه‌گیری «شباهت محسوس» موجب شده تا رویه‌های قضایی و ابزارهای تشخیص در کشورهای عضو به‌شدت متنوع باشد؛ از تحلیل‌های بیومتریک تا الگوریتم‌های تشخیص چهره، هر یک با استانداردهای متفاوتی تعریف «شباهت محسوس» را دست‌کاری می‌کنند و این خود چالش جدیدی درباره شفافیت و اعتبارسنجش خلق می‌کند (Labuz, 2024:787) .

---

[1]. Artificial Intelligence Act.
[2]. Digital Service Act.
[3].«appreciably».

باوجود هماهنگی نسبی میان «قانون هوش مصنوعی» و «مقررات خدمات دیجیتال» نبود یک تعریف مشترک و قابل‌اندازه‌گیری از «دیپ‌فیک» می‌تواند در عمل راه برای سوءاستفاده تولیدکنندگان محتوا باز کند و قضاوت نهایی درباره ماهیت ممنوعیت را به تشخیص موردی قاضیان و نهادهای فنی محول نماید؛ وضعیتی که نه‌تنها پیچیدگی‌های حقوقی را افزایش می‌دهد، بلکه اقتضای تصویب سریع‌تر و یکپارچه‌تر اصلاحات در چارچوب قوانین دیجیتال را بیش‌ازپیش آشکار می‌سازد (Labuz, 2024:788) .

باتوجه‌به تعاریف مختلف ارائه‌شده در مقررات اتحادیه اروپا و نقدهای وارده بر آن‌ها، به نظر نگارندگان جامع‌ترین تعریف از دیپ‌فیک آن است که نه صرفاً بر معیارهای فنی، بلکه بر مبنای اثرگذاری اجتماعی و حقوقی آن استوار باشد. معیار «شباهت محسوس» در قانون هوش مصنوعی اتحادیه اروپا، هرچند نقطهٔ قوتی در شمول بازنمایی‌های گمراه‌کننده است، اما به‌تنهایی برای تعیین حدود مسئولیت کیفری کافی نیست، زیرا همچنان ابهام در سنجش میزان شباهت باقی می‌ماند. ازاین‌رو، تعریف مطلوب باید علاوه بر اتکا بر واقع‌نمایی قابل‌ادراک برای مخاطب متعارف، به عنصر نقض کرامت انسانی و سلب اختیار از شخص نیز توجه کند. تنها در این صورت است که می‌توان دیپ‌فیک را به‌عنوان مصداق بارز محتوای دیجیتال جعلی مخل حقوق بشر و نظم عمومی به‌درستی شناسایی و جرم‌انگاری کرد.

۳. بنیادهای نظری جرم‌انگاری پورنوگرافی دیپ‌فیک (محتوای دیجیتال جعلی)

جرم‌انگاری دیپ‌فیک‌های پورنوگرافیک صرفاً واکنش به یک ابزار فناورانه نیست، بلکه بر اصولی ریشه‌دار در حقوق کیفری و حقوق بشر استوار است. این اصول، مبانی نظری مداخله قانون‌گذار را فراهم می‌کنند.

۳-۱. اصل آسیب و منطق حداقل‌گرایی کیفری

منطق جرم‌انگاری اقتضا می‌کند که تنها زمانی مداخله کیفری توجیه‌پذیر باشد که رفتار معین موجب زیان واقعی به دیگران شود. محتوای جعلی جنسی حتی بدون وقوع فعل جنسی واقعی،

آسیب‌های عمیق روانی، حیثیتی و اجتماعی بر بزه‌دیدگان وارد می‌کند و در نتیجه مصداق بارز «آسیب» است (Feinberg, 1984: 33–35) . این نوع زیان‌ها که اغلب به‌صورت غیرمادی‌اند، به‌خودی‌خود کفایت می‌کنند تا مداخله کیفری ضروری جلوه کند؛ بنابراین جرم‌انگاری دیپ‌فیک‌های پورنوگرافیک با اصل حداقل‌گرایی کیفری همساز است، زیرا تنها در مواردی وارد عمل می‌شود که مصالح فردی و اجتماعی جدی در معرض خطر قرار گیرد.

۳-۲. کرامت انسانی و منع ابزاری‌سازی بدن

یکی از مبانی مهم جرم‌انگاری، اصل کرامت انسانی است. تولید یا انتشار محتوای جنسی جعلی بدون رضایت فرد، در حقیقت به معنای فروکاستن شخص به «شیءانگاری جنسی» است. چنین فرایندی، انسان را نه به‌عنوان سوژه‌ای مختار بلکه به‌مثابه ابزاری برای ارضای جنسی یا تحقیر اجتماعی بازنمایی می‌کند (Citron, 2019: 1921–1924) . این عمل، نقض آشکار شأن ذاتی انسان است و توجیهی هنجاری قوی برای جرم‌انگاری فراهم می‌سازد.

۳-۳. آزادی بیان و مرزهای مشروع آن

آزادی بیان حقی بنیادین است، اما مطلق تلقی نمی‌شود. حقوق بشر معاصر پذیرفته است که این آزادی می‌تواند برای حمایت از حقوق و حیثیت دیگران یا حفظ اخلاق عمومی محدود شود. محتوای جنسی جعلی که بدون رضایت فرد تولید و منتشر می‌شود، نمونه‌ای روشن از جایی است که آزادی بیان باید در برابر حق بر حیثیت و کرامت انسانی عقب‌نشینی کند (دیوان اروپایی حقوق بشر، ۲۰۱۵: ۲۷).

در این چارچوب، جرم‌انگاری پورنوگرافی دیپ‌فیک، نه محدودسازی خودسرانه آزادی، بلکه اقدامی مشروع برای پاسداشت توازن میان آزادی و مسئولیت است.

۳-۴. حق بر حریم خصوصی و خودمختاری جنسی

یکی از جلوه‌های اساسی حقوق بنیادین بشر، حق بر حریم خصوصی و کنترل فرد بر بدن و تصویر خویش است. حفظ حریم خصوصی و حمایت از داده‌های شخصی، به ویژه داده‌های مرتبط با فناوری دیپ‌فیک حقی ضروری در راستای حفاظت از کرامت انسانی است (لطیف‌زاده، ۱۴۰۳: ۱۸۹). دیپ‌فیک‌های پورنوگرافیک این حق را در چند سطح نقض می‌کنند: در سطح

فردی با تحقیر و اضطراب روانی، در سطح اجتماعی با بی‌اعتبارسازی شغلی و خانوادگی، و در سطح ساختاری با بازتولید نابرابری‌های جنسیتی (Pascale, 2023: 338–341). این نقض چندوجهی نشان می‌دهد که جرم‌انگاری چنین محتواهایی ضرورتی برای حفاظت از خودمختاری جنسی و حق تعیین سرنوشت فرد بر بدن و تصویر خویش است (Rackley & Houghton, 2020: 2–3).

۴. سازوکارهای حقوقی ایران برای مقابله با پورنوگرافی(هرزه-نگاری) دیپ‌فیک(جعل عمیق)

این بخش به تحلیل سازوکارهای حقوقی ایران برای مقابله با پورنوگرافی دیپ‌فیک اختصاص‌یافته است و تلاش دارد ظرفیت قانونی موجود و کارآمدی آن را ارزیابی کند. بررسی بر دو رویکرد متمرکز است: نخست، جرم‌انگاری تولید و انتشار محتوای مستهجن با تمرکز بر شمول محتوای دیجیتال دست‌کاری‌شده؛ دوم، حمایت از حیثیت افراد از طریق ارزیابی مقررات مرتبط با هتک حیثیت در فضای دیجیتال. این تحلیل با اتکا بر مفاد قانونی و رویه‌های قضایی موجود، نقاط قوت، محدودیت‌ها و ظرفیت‌های بالقوه قوانین ایران را برای مقابله با دیپ‌فیک نشان می‌دهد و زمینه ارائه پیشنهادهایی برای افزایش کارآمدی آن‌ها را فراهم می‌کند.

۴-۱. جرم‌انگاری تولید و انتشار محتوای مستهجن

مادهٔ ١٤ قانون جرائم رایانه‌ای ۱۳۸۸ (اصلاحی ۱۳۹۹) با جرم‌انگاری تولید، انتشار، توزیع، معامله و نیز نگهداری به‌قصد افساد یا تجارت، چارچوب هنجاری صیانت از عفت عمومی و حیثیت فردی را سامان می‌دهد و تبصره ٤ همان ماده با تصریح به شمول «اعم از واقعی یا ساختگی»، قلمرو ماهوی قاعده را به محتوای دست‌کاری‌شده دیجیتال نیز تسری می‌دهد؛ بدین ترتیب، بازنمایی‌های مبتنی بر جعل عمیق که با الصاق چهرهٔ اشخاص به پیکره‌های برهنه یا صحنه‌های آمیزشی ساخته می‌شوند، ذیل عنوان «مستهجن» قرار می‌گیرند، هرچند مادهٔ مزبور برهنگی واقعی شخص مورد انتساب را شرط نکرده است. همان قانون، با انتقال تمرکز از «ماهیت محتوا» به «نحوهٔ اشاعه»، رفتارهای تسهیل‌گر از قبیل تحریک، ترغیب،

تهدید، تطمیع، فریب یا آموزش شیوه‌های دسترسی را مستقل از فعل تولید، قابل‌تعقیب می‌داند؛ از این حیث، بسترهای آموزش ساخت دیپ‌فیک یا شبکه‌های توزیع پیوندهای دسترسی می‌توانند در قلمرو این قانون قرار گیرند. این دو ماده در کنار هم، از منطق «عنصر جنسی غالب و فقدان رضایت معتبر» بهره می‌گیرند: تمایزی که در ادبیات جزایی داخلی نیز برای افتراق میان آثار مستهجن و مصادیق دارای ارزش ادبی—هنری پذیرفته شده است (رزمان، ۱۳۹۵: ۵۳). بر این مبنا، می‌توان بیان داشت روایت‌های دیپ‌فیکی که کارکرد غالب آن‌ها تحریک جنسی یا تحقیر جنسی شخص قابل‌شناسایی است و هیچ نشانی از رضایت معتبر او در مرحله‌ی تولید، انتساب یا انتشار ندارد، قابلیت شمول در ماده ۱۴ و ۱۵ قانون جرائم رایانه‌ای را خواهند داشت.

رویهٔ قضائی موجود هرچند عموماً ناظر به محتوای سنتی‌تر است، ظرفیت انطباق خود با بسترهای نوین را نشان داده است: در دادنامهٔ شمارهٔ ۹۲۰۹۹۷۰۲۷۰۲۰۰۰۶۶ دادگاه تجدیدنظر تهران (۱۳۹۲)، انتشار محتوای مستهجن در شبکه‌های اجتماعی به استناد مادهٔ ۱۴ جرم تلقی و محکومیت صادر شد؛ و دیوان عالی کشور در رأی شمارهٔ ۹۴۰۹۹۸۲۹۲۵۴۰۱۴۰۷ (۱۳۹۵)، نشر محتوای مستهجن در پیام‌رسان تلگرام را در صلاحیت مادهٔ یادشده قرارداد. باوجود این، از منظر کارآمدی، چند کاستی اساسی پابرجاست: نخست آنکه اتکای مفهومی «مبتذل/مستهجن» به «عرف» اگرچه انعطاف تفسیری فراهم می‌کند، اما به ناهمگونی در آراء و کاهش پیش‌بینی‌پذیری می‌انجامد؛ امری که در ادبیات جزای عمومی، به‌عنوان تهدیدی برای امنیت قضایی مورد اشاره قرار گرفته است (نوری، ۱۳۸۶: ۴۲). دوم آنکه تناسب میان ضمانت اجراهای فعلی (حبس‌های کوتاه‌مدت و جزای نقدی سبک) با منطق شبکه (سرعت انتشار، اثر حیثیتی ماندگار و انگیزهٔ انتفاع اقتصادی) چشمگیر نیست و کارکرد بازدارندگی را کاهش می‌دهد (عزیزی، ۱۴۰۲: ۸۹). سوم آنکه به گزارش عملیاتی پلیس فتا، باوجود ثبت صدها پرونده دربارهٔ انتشار تصاویر خصوصی و محتوای دست‌کاری‌شده، محدودیت ظرفیت تخصصی در تشخیص فنی و نبود سازوکار حذف فوری در سکوهای برخط، روند حمایت مؤثر از بزه‌دیدگان را کند می‌کند (پلیس فتا، ۱۴۰۰؛ نیز نک: سازمان پدافند غیرعامل، ۱۴۰۰).

از دید نگارندگان، مفاد مواد ١٤ و ١٥ «ظرفیت هنجاری» کافی برای پوشش پورنوگرافی دیپ‌فیک را دارند، اما برای انتقال این ظرفیت به «کارآمدی عینی»، دو اصلاح لازم می‌نماید: نخست، درج تعریف قانونی «محتوای دست‌کاری‌شدهٔ دیجیتال (دیپ‌فیک)» با سه سنجهٔ آزمون‌پذیر (شباهت محسوس برای ناظر متعارف، قابلیت انتساب به شخص قابل‌شناسایی، و فقدان رضایت معتبر) به‌منظور کاهش ناهمگونی قضایی و دوم، الزام قانونی سکوها به اقدام فوری توأم با ایجاد واحدهای تخصصی تشخیص دیپ‌فیک در پلیس فتا و دادسراها. در غیاب این اصلاحات، کارکرد مواد مذکور عمدتاً اعلامی باقی خواهد ماند نه حمایتی.

۴-۲. هتک حیثیت از طریق فناوری دیجیتال

مادهٔ ١٦ قانون جرائم رایانه‌ای ١٣٨٨ (اصلاحی ١٣٩٩) مقرر می‌دارد: «هرکس به‌وسیلهٔ سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به‌نحوی‌که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پانزده میلیون تا یک‌صد میلیون ریال یا هر دو مجازات محکوم خواهد شد». نسبت این ماده با دیپ‌فیک مضاعف است: از یک‌سو، عنصر مادی «تغییر یا تحریف» دقیقاً با ماهیت فنی جعل عمیق انطباق دارد؛ و از سوی دیگر، معیار نتیجه‌محور «هتک حیثیت عرفی» اجازه می‌دهد مواردی که فاقد برهنگی کامل‌اند، اما به اعتبار اجتماعی شخص لطمه می‌زنند، مشمول حمایت کیفری قرار گیرند. در عمل، دست‌کاری‌های واقع‌نما (از قبیل الصاق چهرهٔ شخص به بدن دیگری در بافت‌های جنسی یا تحقیرآمیز، یا هم‌لب‌ساز صدا برای القای گفتار موهن) به طور نوعی قابلیت نقض حیثیت دارند، مشروط بر آنکه انتشار (حتی در محیط‌های نیمه عمومی) تحقق‌یافته باشد (عزیزی، ١٤٠٢: ١٠١). رویهٔ قضایی نیز این جهت‌گیری را تأیید کرده است: در دادنامهٔ شمارهٔ ٩٧٠٩٩٧٢٢٩٤١٠٠٤٨٢ شعبهٔ ٤١ دادگاه تجدیدنظر تهران (١٣٩٧)، ارسال تصاویر دست‌کاری‌شده در گروه محدود پیام‌رسان، «انتشار» تلقی و محکومیت اعلام شد؛ و دیوان عالی کشور در رأی شمارهٔ ٩٤٠٩٩٨٢٩٢٥٤٠١٤٠٧ (١٣٩٥) تصریح کرد که فقدان برهنگی کامل مانع از شمول مادهٔ ١٦ نیست، مادام که معیار عرفی لطمهٔ حیثیتی احراز گردد.

باوجود این ظرفیت تفسیری، کارآمدی عملی مادهٔ ۱۶ به سه سبب محل تردید است. نخست، اتکای معیار نهایی به «عرف» (بی‌آنکه شاخص‌های عینی راهنما (مانند «شباهت محسوس» یا «انتساب معتبر» در متن قانون تصریح شده باشد) به ناهمگونی در داوری‌ها می‌انجامد و پیش‌بینی‌پذیری را می‌کاهد (عزیزی، ۱۴۰۲: ۷۸) . دوم، فرایند اثبات در فقدان استانداردهای ملی تشخیص دیپ‌فیک، کند و پرهزینه است؛ گزارش‌های عملیاتی پلیس فتا حاکی از افزایش پرونده‌های تهدید و اخاذی با تصاویر دست‌کاری‌شده و هم‌زمان محدودیت توان کارشناسی در مواجهه با مدل‌های پیشرفتهٔ جعل عمیق است (پلیس فتا، ۱۴۰۰؛ سازمان پدافند غیرعامل، ۱۴۰۰). سوم، عدم تناسب ضمانت‌اجراها با آسیب‌های حیثیتی پایدار و با محاسبه هزینه–فایده از سوی مرتکبان، کارکرد بازدارندگی را مخدوش می‌سازد؛ مجازات‌های کوتاه‌مدت و جزای نقدی سبک، در مواجهه با چرخهٔ اقتصادی تولید و توزیع محتوا، بازدارندگی قوی ایجاد نمی‌کند (تبریزی، ۱۴۰۳: ۹۷).

از منظر نگارندگان، کارآمدی ماده ۱۶ هنگامی تضمین می‌شود که برای مهار ناهمگونی مبتنی بر عرف و تسهیل اثبات، دو اقدام مکمل در خود قانون و در آیین کار رسیدگی نهادینه گردد؛ نخست، تصریح معیارهای عینی در متن ماده، از قبیل «شباهت محسوس برای ناظر متعارف» و «انتساب قابل اعتماد به شخص معین»، تا سنجش «هتک حیثیت عرفی» از حد تفسیر موردی فراتر رفته و پیش‌بینی‌پذیری قضایی افزایش یابد. دوم، تدوین «راهنمای فنی ملی تشخیص دیپ‌فیک» با مشارکت قوه قضائیه، پلیس فتا و مراکز دانشگاهی، نه برای تحدید قلمرو کیفری، بلکه برای تعیین شاخص‌های فنی احراز «تغییر یا تحریف» موضوع ماده ۱۶، تنظیم پروتکل‌های زنجیره نگهداری و استنادپذیری ادله الکترونیکی مطابق قانون آیین دادرسی کیفری ۱۳۹۲ و آیین‌نامه جمع‌آوری، حفظ و ارائه ادله الکترونیکی ۱۳۹۳، و یکنواخت‌سازی گزارش‌های کارشناسی برای دادسرا و دادگاه. به این ترتیب کارکرد راهنما روشن است: در پرونده‌ای که محتوای مورد نزاع «دست‌کاری‌شده» احراز می‌شود، مسیر رسیدگی ذیل ماده ۱۶ ادامه می‌یابد؛ و هرگاه بررسی فنی نشان دهد محتوا «واقعی» و متعلق به حریم خصوصی است و بدون رضایت منتشر شده، عنوان صحیح، حسب مورد، ماده ۱۷

قانون جرائم رایانه‌ای مصوب ۱۳۸٦ در خصوص انتشار داده‌ها و تصاویر خصوصی بدون رضایت و نیز مقررات خاص قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌کنند است. این تفکیک به معنای خروج رفتار زیان‌بار از قلمرو جرم یا تخفیف خودکار پاسخ کیفری نیست، زیرا در فرض انطباق چند عنوان یا ارتکاب رفتارهای متعدد، قواعد تعدد جرم و اعمال مجازات اشد بر پایه ماده ۱۳٤ قانون مجازات اسلامی ۱۳۹۲ قابل اجرا است؛ افزون بر این، در صورت تحقق عناصر تهدید یا اخاذی، عناوین مرتبط نیز قابل انطباق خواهد بود. جای بحث حاضر دقیقاً همین‌جاست، زیرا نسبت ماده ۱٦ با سایر عناوین در گرو تشخیص فنی «واقعی در برابر دست‌کاری‌شده» است و بدون تعیین این نسبت، هم معیار «هتک حیثیت عرفی» دچار پراکندگی می‌ماند و هم وحدت رویه در استناد به قوانین مرتبط حاصل نمی‌شود. بدین نحو، راهنمای فنی ملی نقشی اثبات‌محور و هماهنگ‌کننده ایفا می‌کند و با ارتقای کیفیت ادله، کاهش ناهمگونی در داوری‌ها و هدایت پرونده به عنوان مجرمانه صحیح، ماده ۱٦ را به ابزاری مؤثرتر برای صیانت از حیثیت اشخاص در مواجهه با رسانه‌های دست‌کاری‌شده تبدیل می‌سازد.

۵. رویکرد اتحادیه اروپا برای مقابله با پورنوگرافی(هرزه‌نگاری) دیپ‌فیک(جعل عمیق)

در این بخش، نظام تقنینی اتحادیه اروپا برای مقابله با پورنوگرافی دیپ‌فیک موردبررسی قرار می‌گیرد تا توانایی آن در مدیریت محتوای دیجیتال آسیب‌رسان و حمایت از قربانیان تحلیل شود. بررسی بر دو محور متمرکز است: نخست، مکانیسم‌های اجرایی قانون هوش مصنوعی و نقش نهادهای هماهنگ‌کننده در ایجاد توازن میان نظارت ملی و هماهنگی اتحادیه‌ای؛ و دوم، ابزارهای قانونی برای حذف محتوا و تضمین حقوق بزه‌دیدگان، از جمله قوانین خدمات دیجیتال و مقررات عمومی حفاظت از داده‌ها. این بخش قصد دارد با ارزیابی کارآمدی، محدودیت‌ها و ظرفیت‌های موجود، تصویر روشنی از توان عملیاتی و چالش‌های اتحادیه اروپا در مقابله با دیپ‌فیک‌های پورنوگرافیک ارائه کند.

۵-۱. مکانیسم‌های اجرایی

مقررات اجرایی اتحادیه اروپا در قالب «قانون هوش مصنوعی» کوشیده‌اند میان اقتدار ملی و هماهنگی اتحادیه‌ای توازن برقرار کنند. ماده ۷٤ این قانون کشورها را مکلف به تعیین مرجع نظارتی مستقل کرده که اختیار بازرسی، مطالبه اسناد فنی و صدور دستورات اصلاحی را دارد، درحالی‌که ماده ۷۵ از طریق «مساعدت متقابل»، امکان پیگیری تخلفات فرامرزی را فراهم می‌سازد. افزون بر این، هیئت اروپایی هوش مصنوعی[1] (ماده ٦۵) و دفتر اروپایی هوش مصنوعی[2] که در سال ۲۰۲٤ تأسیس شد، نقش هماهنگ‌کننده و کارشناسی را ایفا می‌کنند (کمیسیون اروپا، ۲۰۲٤: ملاحظه‌های ٦ تا ۷). این ساختار به‌ویژه در حوزه دیپ‌فیک‌های پورنوگرافیک کارآمد می‌نماید، زیرا از یک سو مرجع ملی می‌تواند نزدیک به محل وقوع زیان مداخله کند و از سوی دیگر، هماهنگی اتحادیه‌ای مانع پراکندگی رویه‌ها می‌شود.

از حیث ضمانت اجرا، ماده ۹۹ قانون هوش مصنوعی مجازات‌های اداری سنگینی را پیش‌بینی کرده که برای نقض‌های جدی، تا ٦ درصد گردش مالی جهانی شرکت را شامل می‌شود. چنین سقفی در مقایسه با سایر قوانین رقابتی و داده‌محور اتحادیه بی‌سابقه نیست و هدف آن ایجاد بازدارندگی واقعی است. در این میان، تجربه‌های قضایی اتحادیه نشان داده‌اند که سازوکارهای اداری باید با ابزارهای قضایی تکمیل شوند. در رأی «پرونده اوا گلاویشنیگ-پیشچک علیه شرکت فیسبوک ایرلند[3]»، دیوان عدالت اتحادیه اروپا پلتفرم میزبان را ملزم کرد نه‌تنها محتوای غیرقانونی شناسایی‌شده بلکه نسخه‌های «اساساً معادل» آن را نیز حذف کند (دیوان عدالت اتحادیه اروپا، ۲۰۱۹، بندهای ٤۵ تا ٤۹ رأی).

این حکم در عمل اهمیت زیادی برای مقابله با دیپ‌فیک‌های پورنوگرافیک دارد، زیرا همین نسخه‌های معادل غالباً بلافاصله بازتولید می‌شوند .درعین‌حال، تحلیل‌های نظری تأکید دارند که بازدارندگی تنها در صورتی تحقق می‌یابد که توان فنی برای تشخیص و اثبات تخلف نیز فراهم باشد، وگرنه جریمه‌های سنگین در عمل به تهدیدی کاغذی تبدیل می‌شوند (Schuett, 2024: 16–17) .

---

1. European Artificial Intelligence Board.
2. European Artificial Intelligence Office.
3. Glawischnig-Piesczek v. Facebook.

باوجود این نقاط قوت، ضعف‌هایی نیز قابل‌مشاهده است: نخست، محدودیت صلاحیت سرزمینی در مواجهه با توزیع جهانی محتوا، که حتی با سازوکارهای مساعدت متقابل نیز موجب کندی می‌شود؛ دوم، کمبود ظرفیت فنی برخی ناظران ملی برای شناسایی دیپ‌فیک‌های پیشرفته؛ و سوم، احتمال ناهمگونی در اجرای مواد میان کشورهای عضو پیش از تثبیت رویه‌های مشترک. گزارش پژوهشی پارلمان اروپا نیز همین چالش‌ها را برشمرده و بر لزوم تقویت ابزارهای فنی و هماهنگی فراملی تأکید کرده است (خدمات پژوهشی پارلمان اروپا، ۲۰۲۱: ۳۰–۳۳) .

هرچند مقررات اتحادیه اروپا به‌ویژه «قانون هوش مصنوعی» ظرفیت‌های چشمگیری برای کنترل سوءاستفاده از فناوری‌های نوین دارند، اما از منظر انتقادی نمی‌توان نادیده گرفت که ماهیت فرامرزی فضای دیجیتال، تفاوت سطح توانمندی نهادهای ملی و محدودیت ابزارهای فنی در شناسایی دیپ‌فیک‌های پیچیده، تحقق کامل اهداف این قانون را با دشواری مواجه می‌سازد (Leins et al., 2023: 114) . افزون بر این، ابهام در معیارهای ارزیابی ریسک و دشواری‌های اجرایی در زمینه همکاری میان مراجع کشورهای عضو، ناهمگونی در اعمال مقررات را به همراه دارد. باوجود این، نوآوری اصلی این چارچوب در طراحی ضمانت اجراهای مالی متناسب با سطح خطر و نیز پیش‌بینی همکاری فراملی در قالب «هیئت اروپایی هوش مصنوعی» است که با هماهنگی رویه‌های نظارتی و تسهیل تحقیقات مشترک، کاستی‌های اجرایی را تا حدی جبران می‌کند (Schuett, 2023: 370) .

از حیث سازوکار اجرایی، قانون خدمات دیجیتال پلتفرم‌ها را موظف می‌کند سازوکاری کارآمد برای «اعلان و اقدام» فراهم کنند تا هر کاربر بتواند به‌سادگی محتوای غیرقانونی را گزارش دهد و پلتفرم موظف باشد «بدون تأخیر ناموجه» آن را حذف یا دسترسی به آن را مسدود کند. این تکلیف در کنار انتشار گزارش‌های شفافیت دوره‌ای (ماده ۱۹) و ممیزی‌های اجباری برای پلتفرم‌های بسیار بزرگ (ماده ۲۶) نظامی را ایجاد می‌کند که به‌جای واکنش منفرد، به‌دنبال پیشگیری سیستماتیک است (Helberger et al., 2021: 146).

رویه‌های قضایی دیوان عدالت اتحادیه اروپا نیز با تثبیت اصولی همچون الزام به شفافیت و مسئولیت‌پذیری ارائه‌دهندگان فناوری، ابعاد هنجاری این چارچوب را تقویت کرده است؛ بنابراین، اگرچه خلأها و محدودیت‌های عملی همچنان پابرجاست، اما کارآمدی نسبی این نظام تقنینی در مهار محتوای مضر و حمایت از قربانیان، برتری آشکاری نسبت به بسیاری از الگوهای مشابه دارد. از دید نگارندگان، نقطه قوت اصلی این سازوکار در هم‌نشینی قواعد هنجاری سخت‌گیرانه، ضمانت اجراهای مالی بازدارنده و نهادهای نظارتی فراملی است؛ مدلی که در صورت تقویت زیرساخت‌های فنی و ارتقای ظرفیت‌های ملی، قابلیت تبدیل‌شدن به الگویی پایدار برای مدیریت خطرات دیپ‌فیک‌های پورنوگرافیک در سطح بین‌المللی را داراست.

۵-۲. حذف محتوا و حمایت از بزه‌دیدگان در چارچوب اتحادیه اروپا

رویکرد اتحادیه اروپا در زمینه حذف محتوای غیرقانونی، به‌ویژه پورنوگرافی‌های مبتنی بر جعل عمیق، بر ترکیب چندین سند تقنینی استوار است. «قانون هوش مصنوعی» نقش پیشگیرانه و شفافیتی دارد، اما تکلیف حذف سریع و حمایت از بزه‌دیده را به مقررات مکمل، به‌ویژه «قانون خدمات دیجیتال[1]» و «مقررات عمومی حفاظت از داده‌ها[2]»، واگذار می‌کند. این ساختار چندوجهی، به لحاظ هنجاری تلاشی است برای‌آنکه هم پلتفرم‌ها در قبال محتوای مضر پاسخگو باشند، هم قربانی ابزار مستقیمی برای ترمیم وضعیت حقوقی و حیثیتی خود در اختیار داشته باشد (European Union, 2022: arts. 8–9) .

در همین راستا، خود «قانون هوش مصنوعی» نیز سطحی از شفافیت و قابلیت پیگیری را بر ارائه‌دهندگان سیستم‌های هوش مصنوعی تحمیل می‌کند؛ به بیان دیگر، اتحادیه اروپا تنها به حذف محتوا بسنده نمی‌کند، بلکه می‌خواهد منبع و سازوکار تولید آن محتوا نیز قابل فهم و قابل نظارت باشد. این ایده در تعهدات مرتبط با شفافیت عملکرد سیستم‌ها بازتاب پیدا می‌کند:

---

[1].Digital Services Act.
[2].General Data Protection Regulation.

با توجه به ماده ۱۳ قانون هوش مصنوعی اتحادیه اروپا، سیستم های هوش مصنوعی پر خطر باید طوری طراحی و توسعه داده شوند که عملکرد آنها به اندازه ی کافی شفاف باشد (پارسا، ۱٤۰۳: ۱۲٦).

در زمینه پیشینه قضائی، پرونده‌های دیوان عدالت اتحادیه اروپا به تبیین مسئولیت پلتفرم‌ها در حذف محتوای غیرقانونی کمک می‌کنند. در پرونده «لورئال علیه ای بی اینترنشنال ای جی[1]»، دیوان حکم داد که پلتفرم‌ها در صورت ایفای نقش فعال در میزبانی محتوای غیرقانونی، از مسئولیت مدنی معاف نیستند و باید اقدامات مؤثری برای جلوگیری از نقض حقوق مالکیت معنوی انجام دهند (دیوان عدالت اتحادیه اروپا، ۲۰۱۱) . هرچند موضوع دعوی نقض حقوق مالکیت معنوی بود، نسبت آن به بحث حاضر ازاین‌جهت است که دیوان «نقش فعال» پلتفرم را معیار زوال مصونیت میزبانی و ایجاد تکلیف به اقدام مؤثر در قبال هر نوع محتوای غیرقانونی دانست، نه صرفاً محتوای ناقض مالکیت معنوی، به همین قیاس، در مواجهه با دیپ‌فیک‌های پورنوگرافیک نیز هرگاه پلتفرم نقشی فعال ایفا کند یا از غیرقانونی بودن محتوا آگاه شود، تعهد به اقدام به‌موقع برای حذف و پیشگیری از بازنشر برقرار است، هرچند ماهیت محتوای غیرقانونی با پرونده مرجع متفاوت باشد.

همچنین، در «پرونده شرکت یو پی سی تله‌کابل وین علیه شرکت کنستانتین فیلم فِرلاینخ[2]»، دیوان تأکید کرد که ارائه‌دهندگان خدمات اینترنتی می‌توانند دسترسی به محتوای غیرقانونی حتی به‌صورت پیشگیرانه و بدون دستور قضائی قبلی را محدود کنند (دیوان عدالت اروپا، ۲۰۱٤).

مقررات عمومی حفاظت از داده‌ها ابزار مکمل دیگری را از مسیر «حق پاک‌سازی» (حق فراموش‌شدن) پیش‌بینی کرده است. ماده ۱۷ این مقرره به افراد حق می‌دهد داده‌های شخصی

[1]. L’Oréal SA v. eBay International AG (C-324/09).
[2]. UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH (C-314/12).

خود را که بدون رضایت معتبر یا برخلاف حقوق اساسی پردازش شده است، حذف کنند.

در پرونده «گوگل اسپانیا[1]»، دیوان عدالت اتحادیه اروپا «حق پاک‌سازی یا حق فراموشی» را درباره نتایج موتورهای جست‌وجو به رسمیت شناخت، یعنی شخص می‌تواند در شرایط معین درخواست کند پیوندهایی که با جست‌وجوی نام او ظاهر می‌شوند از فهرست نتایج حذف شوند و پذیرش یا رد این درخواست بر پایه ارزیابی موردی میان حریم خصوصی فرد و حق دسترسی عموم به اطلاعات انجام می‌شود (دیوان عدالت اتحادیه اروپا، ۲۰۱٤: بندهای ۹۳ تا ۹۹).

پس از آن، در پرونده «گوگل علیه نهاد حفاظت از داده‌های فرانسه[2]» تصریح شد که دامنه جغرافیایی این حق اصولاً به قلمرو اتحادیه محدود است، اما موتورهای جست‌وجو باید تدابیر مؤثری اتخاذ کنند تا کاربران اروپایی نتوانند از نسخه‌های خارج از اتحادیه به نتایج حذف‌شده دسترسی پیدا کنند (دیوان عدالت اتحادیه اروپا، ۲۰۱۹: بندهای ۷۲ تا ۷٦).

باوجود این محدودیت سرزمینی، این سازوکار همچنان در سطح اتحادیه ابزار مؤثری برای کنترل محتوای مضر و حمایت از بزه‌دیدگان محسوب می‌شود (Kulk & Borgesius, 2014: 94).

باوجود نقاط قوت مقررات اتحادیه اروپا، کاستی‌هایی نیز مشهود است. از جمله، وابستگی گسترده قانون خدمات دیجیتال به سازوکار گزارش و اقدام که موجب می‌شود قربانی در عمل بار اولیهٔ اثبات و اطلاع‌رسانی را بر دوش کشد، امری که می‌تواند موجب تأخیر در حذف محتوا و استمرار آسیب شود (Lynskey, 2022: 218–219) . همچنین، تعارض میان حق پاک‌سازی تحت ماده ۱۷ مقررات عمومی حفاظت از داده‌ها و آزادی بیان در ماده ۱۱ منشور حقوق بنیادین اتحادیه اروپا همواره محل مناقشه است؛ مبنای این تعارض آن است که ماده ۱۷ مقررات عمومی حفاظت از داده‌ها مطلق نیست و در بند ۳ خود استثنائاتی برای آزادی بیان و حق دسترسی به اطلاعات، اهداف آرشیوی در منافع عمومی، پژوهش علمی

---

[1]. Google Spain (C-131/12).
[2]. Google v. CNIL (C-507/17).

یا تاریخی، و تکالیف قانونی پیش‌بینی کرده است، بنابراینِ عمال حق پاک‌سازی نیازمند سنجشِ موردی میان منافع داده موضوع و حق دسترسی عمومی است .در این سنجش، معیارهای راهنما شامل نقش و جایگاه عمومی فرد، ماهیت و حساسیت داده، صحت و به‌روز بودن، سهم اطلاعات در گفت‌وگوی عمومی، فاصله زمانی از انتشار، زمینه اولیه انتشار و دامنه دسترس‌پذیری، و نیز اثر نمایه‌سازی موتورهای جست‌وجو بر شدت مداخله در حریم خصوصی است .علاوه بر این، ماده ۸۵ مقررات عمومی حفاظت از داده‌ها کشورهای عضو را مکلف می‌کند برای فعالیت‌های روزنامه‌نگاری، هنری یا ادبی معافیت‌ها و محدودیت‌های لازم را وضع کنند که خود دامنه حق پاک‌سازی را در برابر آزادی بیان تنظیم می‌نماید .برآیند این چارچوب آن است که «حق پاک‌سازی» و «آزادی بیان» در نسبتِ تعارض ـ تطبیق قرار دارند، نه تقدم مطلق یکی بر دیگری، و نتیجه هر پرونده بر پایه اصول ضرورت و تناسب و ارزیابیِ موردی تعیین می‌شود.

دیوان عدالت اتحادیه اروپا در پرونده «جی سی و دیگران علیه کمیسیون ملی انفورماتیک و آزادی‌ها در فرانسه[1]» تصریح کرد که حذف داده‌های حساس باید در چارچوب مصلحت عمومی و آزادی اطلاع‌رسانی سنجیده شود. این محدودیت نشان می‌دهد که حتی سازوکارهایی که به‌ظاهر مطلق به نظر می‌رسند، در عمل با توازن حقوق بنیادین همراه‌اند. علاوه‌برآن، اجرای مؤثر این مقررات در سطح فراملی با چالش جدی مواجه است؛ زیرا بسیاری از پلتفرم‌های اصلی خارج از حوزه قضایی اتحادیه فعالیت دارند و اجرای تصمیمات قضایی یا اداری اتحادیه در برابر آن‌ها نیازمند همکاری‌های بین‌المللی است (Kuner, 2021: 45–47).

بااین‌حال، ظرفیت‌های کارآمد این نظام انکارناپذیر است. ترکیب «حق پاک‌سازی» در مقررات عمومی حفاظت از داده‌ها با تکالیف شفافیت و حذف فوری محتوا در قانون خدمات دیجیتال الگویی پیشرفته از حمایت بزه‌دیدگان فراهم کرده که در سایر حوزه‌های قضایی کمتر نظیری برای آن می‌توان یافت. پژوهش‌های اخیر نشان داده‌اند که نرخ موفقیت قربانیان

[1]. Google v. CNIL (C-507/17).

در حذف محتوای غیرقانونی تحت این چارچوب به‌مراتب بیشتر از نظام‌های صرفاً مبتنی بر قواعد جزایی است (Hijmans, 2020: 132) . از دید نگارندگان، مزیت بنیادین این سازوکارها در آن است که علاوه بر ضمانت اجراهای مالی و تعهدات شفافیتی، بر توانمندسازی بزه‌دیدگان برای کنترل داده‌های شخصی خود تأکید دارند؛ امری که در جرایم مبتنی بر دیپ‌فیک که هویت و حیثیت فردی به طور مستقیم در معرض تعرض است، نقشی اساسی ایفا می‌کند. درعین‌حال، تردیدی نیست که برای تحقق کامل اهداف، نیاز به سرمایه‌گذاری بیشتر بر ابزارهای فنی تشخیص دیپ‌فیک و ایجاد سازوکارهای الزام‌آور همکاری فرامرزی باقی است. به‌طورکلی، می‌توان گفت مقررات اتحادیه اروپا در این حوزه علی‌رغم محدودیت‌ها، کارآمدترین چارچوب تقنینی موجود در سطح بین‌المللی را تشکیل می‌دهد و الگویی ارزشمند برای سایر نظام‌های حقوقی محسوب می‌شود.

۶. تفاوت نظام حقوقی ایران و اتحادیه اروپا در مواجهه با پورنوگرافی دیپ‌فیک

برای تکمیل بحث، باید به تفاوت مبنای هنجاری دو نظام نیز اشاره شود. در حقوق ایران، مواجهه با پورنوگرافی دیپ‌فیک عمدتاً ذیل مفاهیمی مانند «اخلال در عفت و اخلاق عمومی»، «مستهجن»، «مبتذل» و «جریحه‌دار کردن نظم و حیثیت عمومی» صورت‌بندی می‌شود و جرم‌انگاری نیز در همین چارچوب توجیه می‌گردد. در این چارچوب، تمرکز اصلی بر حمایت از نظم عمومی، صیانت از ارزش‌های اخلاقی و پیشگیری از تزلزل بنیان‌های اجتماعی است و به همین دلیل، پاسخ حقوقی در درجه اول ماهیت کیفری و سلبی پیدا می‌کند، با اتکا بر ممنوعیت نشر و توزیع محتوا و مجازات مرتکب. در مقابل، در اتحادیه اروپا نقطه عزیمت، حمایت از حقوق فردی است؛ از جمله حق بر کرامت انسانی، حق بر حریم خصوصی و حق بر کنترل بر داده‌ها و تصویر شخص، همراه با حق مطالبه حذف یا مسدودسازی محتوا. پیامد عملی این اختلاف مبنا آن است که در ایران، محور مداخله بیشتر «پیشگیری از اخلال در نظم عمومی» است و حمایت از شخص بزه‌دیده عمدتاً به‌صورت غیرمستقیم و در قالب منع کلی انتشار محتوای مستهجن تأمین می‌شود، حال‌آنکه در اتحادیه

اروپا، قربانی به‌مثابه دارنده حق مستقل مورد شناسایی قرار می‌گیرد و از سازوکارهای فعال حمایت می‌شود، از جمله حق درخواست حذف محتوا، حق مطالبه محدودسازی دسترسی، و حق پیگیری مسئولیت پلتفرم در صورت قصور در اقدام. این تفاوت مبنایی در عمل پیامدهای عینی دارد: در نظام ایران، بار اصلی واکنش بر تعقیب کیفری مرتکب و مجازات او متمرکز است و مسئولیت سکو عمدتاً به‌صورت فرعی و غیرمستقیم مطرح می‌شود، درحالی‌که در نظام اتحادیه، علاوه بر امکان پیگرد مرتکب، پلتفرم نیز به‌عنوان بازیگری با تکلیف مثبت برای حذف، مسدودسازی و پیشگیری از بازنشر مخاطب مستقیم تعهد قرار می‌گیرد و قربانی می‌تواند مطالبه اقدام فوری و ترمیم جایگاه حیثیتی خود را بنماید؛ بنابراین، تفاوت میان «نظم محوری» در ایران و «حق‌محوری» در اتحادیه اروپا صرفاً نظری نیست، بلکه بر اولویت‌های اجرایی (مجازات در برابر حذف فوری محتوا)، بر نوع ابزارهای حمایتی (تعقیب کیفری در برابر مکانیسم‌های جبرانی و حمایتی فردمحور) و بر تعیین طرف پاسخ‌گو (صرفاً تولیدکننده محتوا در برابر پلتفرم میزبان) اثر مستقیم می‌گذارد و در نهایت تعیین می‌کند که در هر نظام، صیانت از حیثیت و کرامت اشخاص چگونه و با چه سرعتی محقق می‌شود.

نتیجه‌گیری

با بررسی رویکرد اتحادیه اروپا در مقابله با پورنوگرافی دیپ‌فیک، مشاهده می‌شود که قوانین مختلف این اتحادیه به‌ویژه «قانون هوش مصنوعی» و «قانون خدمات دیجیتال»، به‌طورکلی به‌منظور تنظیم و نظارت بر تولید، انتشار و توزیع محتوای غیرقانونی از جمله دیپ‌فیک‌ها طراحی شده‌اند. این رویکردها، با ترکیب شیوه‌های پیشگیرانه و اصلاحی، در صدد ایجاد توازن میان آزادی بیان و حقوق فردی از یک سو و حمایت از منافع عمومی و کرامت انسانی از سوی دیگر هستند. در این چارچوب، مقررات اتحادیه اروپا از جمله «مقررات عمومی حفاظت از داده‌ها» که به‌ویژه بر «حق پاک‌سازی» (حق فراموش‌شدن) تأکید دارد، به قربانیان دیپ‌فیک امکان می‌دهد

که حقوق خود را باز پس گیرند و از نشر محتوای جعلی که بر حیثیت و حریم خصوصی‌شان آسیب می‌زند جلوگیری کنند. علاوه‌برآن، الزامات شفاف‌سازی و برچسب‌گذاری محتوای دست‌کاری‌شده و نیز تعبیه ابزارهای گزارش‌دهی درون سکوها (از جمله سازوکارهای «اعلام و اقدام» و جایگاه «پرچم‌داران مورداعتماد») در اتحادیه اروپا، بُعد اجرایی حمایت از قربانی را تقویت می‌کند.

در خصوص سازوکار اجرایی این قوانین، لازم به ذکر است که اتحادیه اروپا با استفاده از هیئت اروپایی هوش مصنوعی، مسئولیت‌پذیری پلتفرم‌ها را به‌صورت منظم و با جریمه‌های سنگین برای تخلفات جدی فراهم کرده است. این رویکرد به‌ویژه در مواجهه با دیپ‌فیک‌های پورنوگرافیک از اهمیت ویژه‌ای برخوردار است؛ چراکه این محتوای غیرقانونی غالباً به‌سرعت بازتولید می‌شود و به طور عمده در پلتفرم‌های آنلاین منتشر می‌شود. اما چالش‌هایی از جمله محدودیت‌های صلاحیت سرزمینی، ضعف در ظرفیت فنی تشخیص دیپ‌فیک و فقدان استانداردهای یکسان میان کشورهای عضو، مانع از اجرایی‌شدن کامل این مقررات شده است.

در همین راستا، یکی از مهم‌ترین ابعاد رویکرد اتحادیه اروپا، تضمین شفافیت و پاسخگویی پلتفرم‌ها از طریق ایجاد سازوکارهایی برای گزارش و حذف سریع محتوا است. باوجود این، چالش‌هایی نیز وجود دارد، از جمله اینکه وابستگی زیاد به سازوکار «گزارش و اقدام» که به طور عملی ممکن است باعث تأخیر در حذف محتوای غیرقانونی و در نتیجه استمرار آسیب به قربانیان شود. به‌ویژه در مقایسه با سیستم‌های مبتنی بر قوانین جزایی، این رویکرد نشان‌دهندهٔ کارآمدی بالاتر در حمایت از قربانیان دیپ‌فیک‌ها است. به همین دلیل، ارتقای کیفیت فرایندهای رسیدگی (مانند تعیین بازه زمانی «اقدام به‌موقع»، مستندسازی تصمیمات پلتفرم و امکان اعتراض مؤثر قربانی) در اتحادیه اروپا به‌عنوان مکمل ابزارهای نظارتی اهمیت می‌یابد.

در بررسی قوانین ایران و چگونگی مقابله با پورنوگرافی دیپ‌فیک در این کشور، می‌توان دید که در حال حاضر قوانین موجود در ایران بیشتر بر مقابله با محتوای «مستهجن» و «منافی عفت عمومی» تمرکز دارند. به‌ویژه مواد ١٤ و ١٥ قانون جرائم رایانه‌ای ١٣٨٨، با جرم‌انگاری تولید و انتشار محتوای مستهجن، می‌تواند شامل محتوای دست‌کاری‌شده دیجیتال از جمله

دیپ‌فیک‌ها می‌شود. این قوانین با اتکا بر مفاهیم «مستهجن» و «مبتذل»، و همچنین باتوجه‌به قوانین شفاف‌تری همچون تبصره ٤ ماده ٧٤٢ قانون مجازات اسلامی، تلاش دارند تا محتواهای غیرقانونی را تحت پوشش قرار دهند.

بااین‌حال، مشکلاتی در عمل مشاهده می‌شود که موجب کاهش کارآمدی این قوانین می‌گردد. به طور خاص، اتکای مفهومی «مستهجن» به «عرف» می‌تواند به ناهمگونی و ابهام در برداشت‌های قضائی منجر شود. همچنین، عدم وجود استانداردهای واضح برای شناسایی محتوای دیپ‌فیک و ضعف در سازوکارهای اجرایی برای حذف سریع محتوای مضر، به‌ویژه در فضای اینترنتی، از مشکلات عمده به شمار می‌آید، به‌ویژه، یکی از مهم‌ترین انتقادها نسبت به رویکرد کنونی ایران، عدم امکان حذف فوری و مؤثر این‌گونه پیام‌ها و محتواها در سطح پلتفرم‌هاست؛ امری که مستلزم واکاوی چالش‌های اجرایی در ایران، از جمله هماهنگی میان ضابطان، مراجع قضایی و پلتفرم‌ها، ظرفیت پاسخ‌گویی مستمر، ایجاد سازوکارهای الزام‌آورِ «اعلام و اقدام»، و تضمین دسترسی به ادله دیجیتال و ارائه راه‌حل‌های عملی برای رفع این موانع است. در همین راستا، راهکارهای اجراییِ مکمل می‌تواند شامل تعیین ضرب‌الاجل‌های مشخص برای حذف، ایجاد «مرکز تماس واحد» برای مراجع داخلی، پیش‌بینی دستور موقت الکترونیکی ساری‌الاثر برای حذف فوری، انعقاد تفاهم‌نامه‌های اجرایی با پلتفرم‌های فرامرزی، و تعریف شاخص‌های عملکرد برای پلیس فتا و پلتفرم‌ها باشد. در این شرایط، توان فنی و ظرفیت‌های اجرایی برای شناسایی و برخورد با دیپ‌فیک‌ها در ایران به طور قابل‌ملاحظه‌ای محدود است و این امر کارآمدی قوانین را کاهش می‌دهد. افزون بر این، فقدان قانون جامع حفاظت از داده‌ها و نبود مرجع تخصصی واحد در این حوزه، خلأهای نهادی مهمی ایجاد کرده است.

برای بهبود این وضعیت، پیشنهاد می‌شود که ایران به‌منظور تقویت مقابله با تهدیدات دیجیتال، به‌ویژه دیپ‌فیک‌ها، از رویکردهای اتحادیه اروپا استفاده کند، اما باتوجه‌به شرایط فرهنگی، فنی و اجتماعی کشور، لازم است این رویکردها با اقتضائات بومی‌سازی شوند. این فرایند شامل طراحی و تصویب قوانین مشابه «قانون خدمات دیجیتال» و «قانون هوش مصنوعی» می‌شود که به‌ویژه بر حذف سریع محتوا و حمایت از قربانیان تأکید دارند. به طور خاص، ایران

می‌تواند از مدل‌های اتحادیه اروپا استفاده کرده و قوانین خود را برای مقابله با محتوای جعلی دیجیتال بازنگری کند.

در سطح اجرایی، ایران نیاز به تقویت زیرساخت‌های فنی و ایجاد واحدهای تخصصی در پلیس فتا و دادسراها دارد تا بتواند به طور مؤثر محتوای دیپ‌فیک را شناسایی و حذف کند. این امر مستلزم سرمایه‌گذاری در ابزارهای تشخیص دیپ‌فیک و همچنین آموزش و توانمندسازی نیروهای قضائی و پلیسی است. علاوه بر این، استفاده از مدل‌هایی نظیر «حق پاک‌سازی» در مقررات عمومی حفاظت از داده‌ها می‌تواند به‌عنوان یک ابزار مکمل در ایران مورداستفاده قرار گیرد، با این تفاوت که در ایران باید مرزهای دقیق‌تر و مناسبی برای پیاده‌سازی این حق باتوجه‌به شرایط فرهنگی و اجتماعی مشخص شود. به‌موازات آن، تدوین پروتکل‌های حفظ ادله دیجیتال و زنجیره نگهداری برای تسهیل پیگیری کیفری و حقوقی ضروری است.

از منظر سیاست‌گذاری، ایران باید تدابیر لازم برای حفظ توازن میان حقوق فردی و منافع عمومی را در نظر بگیرد. به‌ویژه، در قوانین جدید باید به این نکته توجه شود که دفاع از حقوق قربانیان دیپ‌فیک باید در کنار حفظ حقوق آزادی بیان، به طور دقیق و متوازن انجام پذیرد. به‌علاوه، توجه به تفاوت‌های فرهنگی و اجتماعی در طراحی این قوانین ضروری است؛ زیرا تغییرات فرهنگی می‌تواند بر نگرش‌های قضائی و عمومی نسبت به مفهوم «محتوای مستهجن» و «تهدید به حیثیت» تأثیر بگذارد. درعین‌حال، تفاوت رویکرد بنیادین میان دو نظام حقوقی نیز باید به‌صراحت مورد اشاره قرار گیرد: در ایران، غالباً مواجهه با این جرایم از منظر «نظم عمومی» صورت می‌گیرد، حال‌آنکه در اتحادیه اروپا محوریت با «حقوق فردی» و حمایت از قربانی است. این اختلاف مبنایی آثار عملی مهمی به دنبال دارد، از جمله در اولویت‌گذاری‌ها (جرم‌انگاری و کنترل محتوا در برابر جبران خسارت و ترمیم حقوقی)، بار اثبات و دسترسی قربانی به سازوکارهای سریع حذف محتوا، دامنه مسئولیت و پاسخ‌گویی پلتفرم‌ها، تعیین مرجع صالح (مثلاً نهاد حفاظت از داده‌ها در برابر دادستانی)، و طراحی ضمانت اجراها که لازم است در تحلیل تطبیقی به طور روشن بازتاب یابد. بر این مبنا، راهبردهای پیشگیری، آموزش سواد رسانه‌ای و

طراحی الزامات شفافیت الگوریتمی نیز در دو نظام مسیرهای متفاوتی را طی می‌کند که باید در سیاست‌گذاری‌های آینده مدنظر قرار گیرد.

در نهایت، به‌طورکلی می‌توان گفت که الگوبرداری از نظام تقنینی اتحادیه اروپا برای ایران، اگرچه نیازمند اصلاحات و بومی‌سازی است، می‌تواند به‌عنوان یک مدل پیشرفته و کارآمد برای مقابله با تهدیدات دیجیتال در کشور ما عمل کند. در صورت ایجاد زیرساخت‌های مناسب، توانمندسازی نهادهای نظارتی و قضائی و هم‌راستایی با نیازهای اجتماعی و فرهنگی، ایران قادر خواهد بود که یک چارچوب حقوقی متناسب با نیازهای خود برای مقابله با دیپ‌فیک‌ها و سایر تهدیدات مشابه دیجیتال ایجاد کند. تحقق این اهداف مستلزم نقشه‌راه زمان‌بندی‌شده، تعیین متولی واحد هماهنگی، و انجام ارزیابی‌های ادواری اثرسنجی مقررات است.

منابع و مآخذ

۱. الله‌وردی، فرهاد (۱۳۹۹). جرائم علیه عفت و اخلاق عمومی. تهران: تفکر آینده‌ساز.

۲. بابایی، جواد (۱۳۹۷). جرایم رایانه‌ای و آیین دادرسی حاکم بر آن. تهران: مرکز مطبوعات و انتشارات قوه قضائیه.

۳. پارسا،ناهید . (۱٤۰۳). نقش و الزامات نظارت انسانی بر هوش مصنوعی در قانون اتحادیه اروپا و قوانین ایران. دوفصلنامه تحقیق و توسعه در حقوق عمومی، ۱(۲)، ۱۱۲-۱٤۰. doi: 10.22034/jrpl.2025.721655

٤. پلیس فضای تولید و تبادل اطلاعات ناجا (پلیس فتا) (۱٤۰۰). گزارش سالانه عملکرد در حوزه جرایم سایبری. تهران.

۵. تبریزی، صادق (۱٤۰۳). آیین دادرسی پیشرفته جرایم سایبری. تهران: میزان.

٦. رزمان، علی (۱۳۹۵). بررسی کیفری جرائم جنسی و منافی عفت با نگاهی بر فضای سایبر. تهران: قانون‌یار.

۷. رضایی، محمد (۱۳۹٦). بررسی تطبیقی جرایم مستهجن در حقوق جزای ایران و اتحادیه اروپا. پژوهش‌های حقوقی، ۱۲(۳)، ۱۰۱–۱۲۰.

۸. سازمان پدافند غیرعامل (۱٤۰۰). گزارش تهدیدات نوین سایبری و راهکارهای مقابله. تهران.

۹. عبدی، میکائیل، فرهودی‌نیا، حسن، و شیخ‌زاده، محمود (۱۳۹۲). پایان‌نامه کارشناسی‌ارشد: بررسی مفهوم عفت عمومی باتکیه‌بر اصل قانونی‌بودن جرایم و مجازات‌ها در حقوق کیفری ایران. دانشکده حقوق، دانشگاه تبریز.

۱۰. عزیزی، امیرمهدی (۱٤۰۲). حقوق کیفری جرایم رایانه‌ای. تهران: مجد.

۱۱. لطیف‌زاده، مهدیه (۱٤۰۳). بررسی چگونگی اثرگذاری متقابل هوش مصنوعی خودمختار و حقوق اسلامی. دوفصلنامه تحقیق و توسعه در حقوق خصوصی، ۱ (۲)، ۲۰۵-۱۸۰. doi:10.22034/jpl.2025.720739

۱۲. موسوی، علی (۱۳۹٤). ماهیت و مصادیق محتوای مستهجن در قوانین ایران. فصلنامه حقوق و سیاست، ۲۷(۱)، ٤٥–٦۸.

۱۳. نوری، مسعود (۱۳۸٦). پروتکل الحاقی به پیمان‌نامه حقوق کودک دربارهٔ فروش، فحشا و هرزه‌نگاری کودکان و بررسی الحاق ایران به آن. دوفصلنامه بین‌المللی حقوق بشر، ۲(۳)، ۳۹–٥٦.

References

1. Abdi, Mikaeil, Farhoudinia, Hassan, & Sheikhzadeh, Mahmoud. (1392). Examination of the concept of public chastity with emphasis on the principle of legality of crimes and punishments in Iranian criminal law. Master's thesis, Faculty of Law, University of Tabriz. (in Persian)
2. Allahvardi, Farhad. (1399). Crimes against public chastity and morality. Tehran: Tafakkor Ayandehsaz. (in Persian)
3. Azizi, Amir-Mahdi. (1402). Criminal law of computer crimes. Tehran: Majd. (in Persian)
4. Babaei, Javad. (1397). Computer crimes and the rules of criminal procedure governing them. Tehran: Publications Center of the Judiciary. (in Persian)
5. Citron, D. K. (2019). Sexual privacy. Yale Law Journal, 128(7), 1870–1960.
6. Court of Justice of the European Union (CJEU). (2014). Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Case C-131/12), ECLI:EU:C:2014:317, paras. 93–99.
7. Court of Justice of the European Union (CJEU). (2019). Eva Glawischnig-Piesczek v. Facebook Ireland Limited (Case C-18/18), Judgment of 3 October 2019.
8. Court of Justice of the European Union (CJEU). (2019). GC and Others v. CNIL (Case C-136/17), ECLI:EU:C:2019:773.
9. Court of Justice of the European Union (CJEU). (2019). Google LLC v. Commission nationale de l'informatique et des libertés (CNIL) (Case C-507/17), ECLI:EU:C:2019:772, paras. 72–76.
10. European Commission. (2024). Proposal for an Artificial Intelligence Act (rec. 6–7). European Commission.
11. European Court of Human Rights. (2015). Guide on Article 8 of the European Convention on Human Rights (p. 27). Council of Europe.
12. European Parliament Research Service (EPRS). (2021). Artificial intelligence at EU borders: Overview of applications and key issues (pp. 30–33).
13. FATA Police of the Law Enforcement Force of Iran (NAJA). (1400). Annual report on performance in the field of cyber crimes. Tehran. (in Persian)
14. Feinberg, J. (1984). Harm to others. Oxford University Press.
15. Hayes, S. C., & Paul, P. (2007). The pornography "addiction" model: Evidence for false claims. Science and Engineering Ethics, 13(4), 515–533.
16. Helberger, N., Pierson, J., & Poell, T. (2021). Governing online platforms: From contested to cooperative responsibility. The Information Society, 37(3), 146–158.

17. Hijmans, H. (2020). The European Union as guardian of Internet privacy: The story of Art 16 TFEU. Springer.
18. Kulk, S., & Borgesius, F. Z. (2014). Google Spain v. González: Did the Court forget about freedom of expression? European Journal of Risk Regulation, 5(3), 389–398.
19. Kuner, C. (2021). The global reach of EU data protection law. International Data Privacy Law, 11(1), 35–52.
20. Łabuz, M. (2024). Deep fakes and the Artificial Intelligence Act—An important signal or a missed opportunity? Policy & Internet, 5(6), 783–800.
21. Latifzadeh, Mahdieh. (1403). Examining the mutual influence between autonomous artificial intelligence and Islamic law. Biannual Journal of Research and Development in Private Law, 1(2), 180–205. doi:10.22034/jpl.2025.720739 (in Persian)
22. Leins, K., Culnane, C., & Rubinstein, K. (2023). Tracking deepfakes: Legal and regulatory responses to synthetic media. International Journal of Law and Information Technology, 31(2), 101–120.
23. Löfgren-Mårtenson, L. (2008). Adolescents' perceptions of pornography. Journal of Sex Research, 45(3), 306–312.
24. Lynskey, O. (2022). The foundations of EU data protection law. Oxford University Press.
25. McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. Oxford Journal of Legal Studies, 37(3), 534–561.
26. McGlynn, C., Rackley, E., & Houghton, R. (2020). The harms of image-based sexual abuse. Social & Legal Studies, 29(6), 1–22.
27. Mousavi, Ali. (1394). The nature and instances of obscene content in Iranian law. Quarterly Journal of Law and Policy, 27(1), 45–68. (in Persian)
28. Nouri, Masoud. (1386). The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and an assessment of Iran's accession. International Human Rights Law (Biannual), 2(3), 39–56. (in Persian)
29. Parsa, Nahid. (1403). The role and requirements of human oversight of artificial intelligence in European Union law and Iranian law. Biannual Journal of Research and Development in Public Law, 1(2), 112–140doi: 10.22034/jrpl.2025.721655. (in Persian)
30. Pascale, E. (2023). Deeply dehumanizing, degrading, and violating: Deepfake pornography and the path to legal recourse. Syracuse Law Review, 73(2), 335–366.
31. Passive Defense Organization. (1400). Report on emerging cyber threats and countermeasures. Tehran. (in Persian)
32. Peguera, M. (2020). The European Court of Justice and intermediary liability for third-party content. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 11(2), 115–125.
33. Razman, Ali. (1395). A criminal analysis of sexual offenses and acts contrary to public chastity with a view to cyberspace. Tehran: Qanunyar. (in Persian)
34. Rezaei, Mohammad. (1396). A comparative study of obscene offenses in Iranian criminal law and the European Union. Legal Research, 12(3), 101–120. (in Persian)

35. Schuett, J. (2023). The EU Artificial Intelligence Act: Regulating high-risk AI systems. Computer Law & Security Review, 49, 369–380.
36. Schuett, J. (2024). Regulating artificial intelligence in the European Union: Risk, compliance, and enforcement. European Law Journal, 30(1), 1–23.
37. Tabrizi, Sadegh. (1403). Advanced criminal procedure for cyber crimes. Tehran: Mizan. (in Persian)