Justice Administration of Tehran Province

Judgment

https://www.Ghazavat.org

Online ISSN: 3060-7809
Print ISSN: 1735-1227
Volum:25 – Issue:124
Winter 2026

Analyzing the Necessity of Differential Criminalization of Deepfakes in the Iranian Criminal Law System (In light of the Study of the Approaches in US and Chinese Criminal Law)

Seyed Alireza Mirkamali[1] | Hamidreza Heydarpour[2] | Zhila Mehrara[1]

1. Associate Professor, Faculty of Law, Shahid Beheshti University, Tehran, Iran. a_mirkamali@sbu.ac.ir
2. Postdoctoral Researcher in Criminal Law and Criminology and University Lecturer, Tehran, Iran (Corresponding Author): hrh_1364@yahoo.com
3. Master of Criminal Law and Criminology from Allameh Tabatabaei University,Tehran, Iran, Zhila. Mehrara.1365@gmail.com

Article Info

Article type:
Scientific Article

Received:
2025/07/24
Received in revised form:
2025/11/19
Accepted:
2026/05/02

Keywords:
Deep Fake; Computer Forgery; Audiovisual Forgery; Extreme Manipulation of Audiovisual Computer Data; Differential Criminalization; Iranian Criminal Law.

Abstract

This article aims to analyze the nature of "deepfakes" and to establish the necessity for differential and aggravated sentencing for this specific and acute form of computer-related forgery within the Iranian criminal law system. The central questions addressed are: How does the nature of a deepfake differ from traditional computer forgery? What necessitates the imposition of aggravated penalties for deepfakes compared to simple computer forgery in Iranian penal system? And, from a comparative perspective, can instances of differential and aggravated criminalization of deepfakes be found in other penal systems? The findings indicate that, on the one hand, instances of deepfake commission—as a prominent manifestation of the misuse of emerging Artificial Intelligence (AI) technologies—are on the rise, leading to diverse ethical and security consequences. On the other hand, due to the extreme manipulation and distortion of audiovisual computer data inherent in deepfakes, this phenomenon must be regarded as far more complex than ordinary computer forgery. Furthermore, various ethical, economic, political, security, and technical grounds justify the determination of differential and aggravated punishment for deepfakes as opposed to ordinary computer forgery. Consequently, it is argued that the Iranian legislature, following the developments in other penal systems such as those of China and the United States, should move toward the differential and aggravated criminalization of deepfakes.

How To Cite

Mirkamali, Seyed Alireza, Heydarpour, Hamidreza, Mehrara, Zhila. (2026). Analyzing the Necessity of Differential Criminalization of Deepfakes in the Iranian Criminal Law System (In light of the Study of the Approaches in US and Chinese Criminal Law). Journal of Judgment, 125(1), 104-125.
http//doi.org/ 10.22034/judg.2026.2066883.1540

DOI

10.22034/judg.2026.2066883.1540

Publisher

Publications of the Judiciary of Tehran Province

آموزش دادگستری
استان تهران

فصلنامه قضاوت

https://www.Ghazavat.org

شاپای الکترونیکی: ۷۸۰۹-۳۰۶۰
شاپا چاپی: ۱۲۲۷-۱۷۳۵
دوره : ۲۵ ـ شماره: ۱۲۴
زمستان ۱۴۰۴

تحلیل ضرورت جرم انگاری افتراقی جعل عمیق در نظام کیفری ایران (در پرتو مطالعه رویکرد حقوق کیفری آمریکا و چین)

سید علیرضا میرکمالی[۱] | حمیدرضا حیدرپور[۲] | ژیلا مهرآرا[۳]

۱. دانشیار دانشکده حقوق دانشگاه شهید بهشتی، تهران، ایران، رایانامه: a_mirkamali@sbu.ac.ir
۲. پژوهشگر پسادکترای حقوق کیفری و جرم شناسی و مدرس دانشگاه، تهران، ایران، (نویسنده مسئول)، رایانامه: hrh_1364@yahoo.com
۳. کارشناس ارشد حقوق کیفری و جرم شناسی از دانشگاه علامه طباطبایی، تهران، ایران، رایانامه: Zhila.Mehrara.1365@gmail.com

اطلاعات مقاله

نوع مقاله: علمی

تاریخ دریافت:
۱۴۰۴/۰۵/۰۲
تاریخ بازنگری:
۱۴۰۴/۰۸/۲۸
تاریخ پذیرش:
۱۴۰۵/۰۲/۱۲

کلیدواژه:
جعل عمیق، جعل رایانه‌ای، جعل صوت و تصویر، دست کاری شدید داده‌های رایانه‌ای صوتی و تصویری، کیفر گذاریِ افتراقی، حقوق کیفری ایران.

چکیده

هدف این نوشتار، تحلیل ماهیت جعل عمیق از یک سو و تبیین ضرورت کیفرگذاری افتراقی و تشدیدیافته نسبت به این شکل خاص و حاد از جعل داده‌های رایانه‌ای در نظام کیفری ایران است. سؤال مشخص این مقاله آن است که جعل عمیق، چه ماهیت متفاوتی نسبت به جعل رایانه‌ای دارد و چه لزومی به تعیین مجازات مشدد برای آن در مقایسه با جعل سادهٔ داده‌های رایانه‌ای در نظام کیفری ایران وجود دارد و از حیث مطالعهٔ تطبیقی، آیا می‌توان نمونه‌ای از کیفرگذاری افتراقی و تشدیدیافته نسبت به جعل عمیق را در دیگر نظام‌های کیفری یافت؟ یافته‌های حاصل از این پژوهش، حاکی است که از یک سو، موارد ارتکاب جعل عمیق به‌منزلهٔ جلوهٔ بارزی از سوءاستفاده از فناوری نوظهور هوش مصنوعی و در نتیجه، تبعات گوناگون آن مانند پیامدهای اخلاقی و امنیتی، رو به افزایش است و از سوی دیگر، به علت دست‌کاری و تحریف بسیار شدید داده‌های رایانه‌ای صوتی و تصویری در جعل عمیق، آن را باید پدیده‌ای به مراتب پیچیده‌تر از جعل رایانه‌ای عادی محسوب کرد. همچنین دلایل متعددی از جمله دلایل اخلاقی، اقتصادی، سیاسی، امنیتی و فنی (تکنیکال) نیز تعیین مجازات افتراقی و مشدد نسبت به جعل عمیق در مقایسه با جعل رایانه‌ای عادی را توجیه می‌کنند. بنابراین، به نظر می‌رسد قانون‌گذار ایرانی، همسو با تحولات برخی دیگر از نظام‌های کیفری از جمله چین و آمریکا، باید درصدد کیفرگذاری افتراقی و تشدیدیافته نسبت به جعل عمیق برآید.

استناد
میرکمالی، سید علیرضا، حیدرپور، حمیدرضا ، مهرآرا، ژیلا. (۱۴۰۵). تحلیل ضرورت جرم انگاری افتراقی جعل عمیق در نظام کیفری ایران (در پرتو مطالعه رویکرد حقوق کیفری آمریکا و چین)، فصلنامه قضاوت، ۱۲۵(۱)، ۱۰۴-۱۲۵.
http//doi.org/ 10.22034/judg.2026.2066883.1540

DOI 10.22034/judg.2026.2066883.1540

ناشر انتشارات دادگستری کل استان تهران

مقدمه

هوش مصنوعی[1] فناوری نوظهور روزگار کنونی است که برای بشریت، مزیت‌ها و کارکردهای مثبت فراوانی داشته است. با این حال، مانند هر فناوری دیگری، امکان سوءاستفاده از آن در راستای ارتکاب رفتارهای مجرمانه وجود دارد. یکی از جلوه‌های مهم سوءاستفاده‌های مجرمانه از هوش مصنوعی، جعل عمیق[2] یا تغییر و تحریف عمیق صوت یا تصویر اشخاص است. بارها دیده و شنیده شده است که با بهره‌گیری از فناوری هوش مصنوعی، صوت یا تصویر متعلق به دیگری، به‌گونه‌ای تغییر یافته یا تحریف شده است که صوت یا تصویری در ظاهر، کاملاً شبیه با نمونهٔ واقعی ولی در باطن، کاملاً متفاوت با آن، ساخته و منتشر شده است. ماهیت خاص جعل عمیق و تفاوت‌های آشکار آن با جعل رایانه‌ای[3] عادی، ابعاد مهمی به آن می‌بخشد و در عین حال، ارتکاب آن، آثار و تبعات چشمگیری نیز در پی دارد. بر همین اساس، برخی نظام‌های کیفری از جمله آمریکا و چین، بر اساس رویکردی فرق‌گذارانه میان ماهیت جعل عمیق و جعل رایانه‌ای عادی (ساده)، در پی کیفرگذاری افتراقی و تشدیدیافته نسبت به جعل عمیق بوده‌اند.

با وجود این، چنین کیفرگذاری در نظام کیفری ایران نسبت به جعل عمیق صورت نگرفته است و رویکردهای ناظر بر چیستی‌شناسیِ جعل عمیق در حقوق کیفری ایران، بیشتر، آن را همچنان مشمول همان عنوان مجرمانهٔ جعلِ رایانه‌ای عادی می‌پندارند. حال آنکه، به نظر می‌رسد جعل عمیق، ماهیتی به مراتب خاص‌تر و در عین حال، پیچیده‌تر از جعل رایانه‌ای دارد و بر این اساس، نیازمند کیفرگذاری افتراقی و تشدیدیافته نسبت به جعل عمیق در نظام کیفری ایران هستیم.

در تحقیق پیشِ رو که رویکرد آن، توصیفی ـ تحلیلی است و با روش مطالعهٔ کتابخانه‌ای تدوین شده، مسئلهٔ اصلیِ موردتحقیق این است که تفاوت ماهوی میان جعل عمیق و جعل رایانه‌ای عادی چیست، چه توجیهاتی به منظور تبیین ضرورت کیفرگذاری افتراقی نسبت به آن در حقوق کیفری ایران وجود دارد و رویکرد حقوق کیفری آمریکا و چین که اقدام به کیفرگذاری تشدیدیافته نسبت به جعل عمیق کرده‌اند، دراین‌باره چه بوده است؟ فرضیهٔ متناظر با این پرسش نیز این است که با عنایت به ماهیت خاص جعل عمیق که مبتنی بر سوءاستفاده از صوت یا تصویر افراد به‌صورت تغییر، تحریف و ترکیب آن‌ها با استفاده از فناوری هوش مصنوعی و تولید صوت یا تصویر جدید است به نحوی که مخاطب، صوت یا تصویر ایجادشده را واقعی می‌پندارد و نیز به سبب دست‌کاری بسیار شدید داده‌های صوتی و تصویری در جعل عمیق، باید میان آن و جعل رایانه‌ای عادی (یا ساده) قائل به تفاوت شد. نظر به همین تفاوت ماهوی، جعل عمیق می‌تواند آثار گاه به‌شدت مخربی

1. Artificial Intelligence (AI)
2. Deep Forgery
3. Computer (Cyber/ Digital) Forgery

نسـبت به حریم خصوصی افراد و نیز نظام معاملاتی و ثبتی و اقتصادی کشـور داشته باشد و حتی قادر است لطمات گاه جبران‌ناپذیر به امنیت سیاسی و نظامی کشور وارد کند؛ مخاطراتی که به‌طور معمول، با این شـدت‌وحدت، چه‌بسا نسبت به جعل عادی رایانه‌ای مطرح نباشند. بر اساس همین رویکرد، نظام کیفری آمریکا و چین، اقدام به جرم‌انگاری و نیز کیفرگذاری افتراقی نسـبت به جعل عمیق در مقایسـه با جعل رایانه‌ای عادی کرده‌اند که اسـتفاده از این دستاورد و نگاه به این تحول، می‌تواند برای مقنن ایرانی نیز راهگشـا باشد. به نظر می‌رسـد مقررات کیفری در مورد جرم جعل رایانـه‌ای در قانـون جرایم رایانه‌ای مصوب ۱۳۸۸، تکافوی مقابلـهٔ کیفری با پدیدهٔ جعل عمیق را ندارند و بنابراین، لازم اسـت با جرم‌انگاری و کیفرگـذاری افتراقی برای این پدیده، رویکردی به مراتب شدیدتر و سخت‌گیرانه‌تر از جعل رایانه‌ای ساده (یا عادی)، نسبت به آن روا داشت.

گفتنی اسـت جعل عمیق، تا به حال در برخی پژوهش‌هـای داخلی و خارجی موضوع مطالعه بوده است،[1] اما وجه تمایز تحقیق حاضر با این پژوهش‌ها آن است که اساساً جعل عمیق را دارای ماهیتـی خاص و متفاوت با جعل رایانه‌ای عادی (یا سـاده) می‌دانـد. در پژوهش‌های موجود در ادبیـات حقوقی ایـران، در باب تبیین ماهیت متفاوت جعل عمیق بـا جعل‌های رایانه‌ای عادی (یا سـاده) و لزوم جرم‌انگاری و کیفرگذاری افتراقی و تشدیدیافته نسبت به جعل عمیق، بحث خاص و چندانی ارائه نشـده اسـت، حال آنکه مدعای نگارندگان حاضر، آن است که جعل عمیق، حالتی

---

۱. در میان پژوهش‌های داخلی، می‌توان به این موارد اشاره داشت:

- احسان‌پور، سیدرضا و امی، احمد. (۱۴۰۱). جرایم فناوری جعل عمیق از منظر فقه و حقوق کیفری، فصلنامهٔ فقه جزای تطبیقی، دورهٔ ۲، شمارهٔ ۴.
- اکبری، عباس‌علی؛ آقاپور، علی و آقاپور، کمال. (۱۴۰۱). تحلیل پدیدهٔ مجرمانه دیپ فیک‌ها (جعل‌های رایانه‌ای پیچیده) با نگاهی به سیاست کیفری ایران و چالش‌های حقوق بشری، فصلنامهٔ کارآگاه، دورهٔ ۱۶، شمارهٔ ۵۹.
- شیری، عباس. (۱۴۰۱). دیپ فیک یا همانندسازی صوتی یا تصویری غیرواقعی در حقوق کیفری، مجلهٔ تحقیقات حقوقی (ویژه‌نامهٔ حقوق و فناوری)، شمارهٔ ۹۴.
- علی ین، آرش. (۱۴۰۰). جرم‌انگاری دیپ فیک‌ها از منظر تعهدات حقوق بشری دولت‌ها، دوفصلنامهٔ بین‌المللی تحقیقات حقوق قضایی، دورهٔ ۲، شمارهٔ ۳.

و در میان پژوهش‌های خارجی، به این موارد می‌توان اشاره کرد:

1. Beebom, S. (2022). 10 Best Deep fake Apps and Websites You Can Try for Fun, Beebom.
2. Chesney, B and Citron, D. K. (2019). "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", California Law Review, Vol. 107.
3. Filimowicz, M. (Ed.). (2022). Deep Fakes: Algorithms and Society, Routledge.
4. Lees, D. (2023). Deep Fake Neighbor Wars: ITV's comedy shows how AI can transform popular culture, The Conversation. Retrieved.

در این پژوهش‌ها عمدتاً چیسـتی جعل عمیق موردتوجه قرار گرفته اسـت و پدیده‌های مرتبط با آن از جمله شهود دروغین که به نظر می‌رسـد به‌زودی، به چالشـی برای نظام‌های قضایی و عامل آشـکاری برای منحرف‌شدن روند دادرسی‌ها تبدیل می‌شود، بررسی شده‌اند.

به مراتب پیچیده‌تر و مخرب‌تر از جعل رایانه‌ای ساده (عادی) است. ضرورت رفع خلأ پژوهشیِ مورداشاره و نیز لزوم ارائهٔ پیشنهاد به مقنن ایرانی مبنی بر اتخاذ رویکرد افتراقی نسبت به جعل عمیق در مقایسه با جعل رایانه‌ای عادی و کیفرگذاری تشدیدی و ویژه در خصوص جعل عمیق در قانون جرایم رایانه‌ای، انگیزهٔ اصلی نگارندگان برای تدوین پژوهش حاضر بوده است.

در نتیجه، در پرتو بحث از رویکرد نظام کیفری آمریکا و چین که به کیفرگذاری تشدیدیافته برای جعل عمیق در مقایسه با جعل عادی رایانه‌ای روی آورده‌اند، ضرورت تعیین کیفر افتراقی برای جعل عمیق نسبت به جعل رایانه‌ای عادی در حقوق کیفری ایران، مهم‌ترین محور مطالعه و تحلیل در پژوهش حاضر است.

۱. چیستی جعل عمیق

«جعل عمیق»که با نام‌های دیگری چون «جعل عمیق صوتی و تصویری»،[1] «جعل باورپذیر»[2] و «دیپ فیک»[3] نیز شناخته می‌شود، فناوری‌ای مبتنی بر هوش مصنوعی است که برای تولید ویدئوهای تقلبی از تصاویر و صداهای پایه استفاده می‌کند. این فناوری قادر است به‌طور خودکار، صورت یک فرد را در ویدئوی دیگری جایگزین کند و حتی صدای او را نیز تغییر دهد (صالحی، ۱۳۹۷: ۴۷). مبنای عمدهٔ ارتکاب جعل عمیق، استفاده از فناوری‌های صوتی و تصویریِ مبتنی بر هوش مصنوعی است (السان، ۱۴۰۱: ۱۹۷).

امروزه، از جعل عمیق برای ساخت تصاویر و ویدئوهای جعلی و تولید محتوای دیجیتال در زمینه‌های مختلف از جمله تبلیغات، فیلم‌ها، سریال‌ها و اخبار استفاده می‌شود. در جعل عمیق، از الگوریتم‌های پیچیده برای تولید تصاویر و صداهای جعلی به‌گونه‌ای که مخاطب، نتواند میان نسخهٔ جعلی (فیک) و نسخهٔ اصلی (واقعی) تمایزی قائل شود، بهره گرفته می‌شود (آبید، ۱۳۹۹: ۴۱). بر این اساس، جعل عمیق، روشی نرم‌افزاری مبتنی بر هوش مصنوعی است که در محتوای صوتی و تصویری دست می‌برد و آن را به‌دلخواه تغییر می‌دهد؛ بنابراین نتیجهٔ نهایی که به دست می‌آید، چیزی کاملاً متفاوت از حقیقت خواهد بود، اما به واسطهٔ باورپذیری بالای تصویرها و صوت‌های ساخته‌شده به‌صورت جعل عمیق، تشخیص مرز واقعیت و دروغ، بسیار دشوار و چه بسا ناممکن خواهد شد (ترنج، ۱۳۹۷: ۴۱) (Brandon, 2018: 24).

باید افزود که واژهٔ دیپ[4] به معنای عمیق و گاه به مفهوم مبهم است و واژهٔ فیک[5] نیز در مفهوم

1. Deep Audio and Video Forgery
2. Believable Forgery
3. Deep Fake
4. Deep
5. Fake

جعلی، دروغین و غیرواقعی به کار می‌رود. بر این اساس، دیپ فیک یعنی ارتکاب جعل به‌صورت بسیار عمیق و پیشرفته به نحوی که میان نسخهٔ ساخته‌شده و نسخهٔ اصلی، شدیداً، شباهت ظاهری وجود دارد که در نگاه اول و چه بسا حتی با چشم‌های مسلح، نتوان هیچ تفاوت و تمایزی میان این دو نسخه احساس کرد (حیدری، ۱۳۹۰: ۲۴) (Filimowicz, 2022: 144; Beebom, 2022: 159).

البته جعل عمیق، می‌تواند استفاده‌های مشروع نیز داشته باشد از جمله در ساخت انیمیشن یا نماهنگ‌های تبلیغاتی. با این حال، مانند هر پدیدهٔ دیگری، ممکن است بتوان موارد انتفاع مجرمانه نیز برای آن در نظر گرفت (قناد، ۱۳۹۷: ۷۱؛ فلسفی، ۱۳۹۸: ۵۶؛ اکبری و همکاران، ۱۴۰۱: ۱۵۳). باید خاطرنشان کرد که انتفاع‌های مجرمانه از هوش مصنوعی برای ارتکاب جعل عمیق، گاه حتی می‌تواند باعث بروز و تشدید معضلات امنیتی نیز شود (صالحی و محترم قلاتی، ۱۳۹۷: ۱۷۳؛ محمدی فردوئی، ۱۳۹۷: ۴۶۱؛ علی ین، ۱۴۰۰: ۳۶۰) (Zhukava, 2020: 311).

۲. تحلیل چرایی و توجیه کیفرگذاری افتراقی نسبت به جعل عمیق در مقایسه با جعل رایانه‌ای عادی

جرم‌انگاری و کیفرگذاری یک پدیده در قوانین کیفری، امری عقلایی است و باید به حد کفایت، مبتنی بر اصول و موازین و توجیهات و مستندات عقلانی باشد. در مورد پدیدهٔ جعل عمیق نیز این واقعیت، صادق است. به سبب تغییرات و تحریفات پیچیده در جعل عمیق، مرز واقعیت و غیرواقعیت، به‌شدت خلط می‌شود و تشخیص و تفکیک این دو در بسیاری از موارد، به‌سادگی امکان‌پذیر نیست (شیری، ۱۴۰۱: ۱۴۸؛ ابوذری، ۱۴۰۱: ۲۴).

همین مسئله، چه بسا در بسیاری از پرونده‌ها و دعاوی، مراجع قضایی را به اشتباه اندازد و آن‌ها را به انحراف از مسیر درست دادرسی بکشاند و به صدور آرای قضایی اشتباه، سوق دهد. بر این اساس، یکی از بسترهای آشکار ارتکاب جعل عمیق، پیدایش شهود دروغین است. کافی است تصور کنیم در پرونده‌ای قضایی، قاضی رسیدگی‌کننده، به اقرار یا شهادت شهود نیاز داشته باشد و ذی‌نفع، با استفاده از جعل عمیق، تصاویر یا اصوات کاملاً جعلی و ساختگی مبنی بر اقرار یا شهادت، تهیه و به مرجع قضایی ارائه کند. با این حال، مرجع قضایی نیز نتواند جعلی و ساختگی‌بودن اصوات و تصاویر را تشخیص دهد و در نهایت، از مسیر منطقی دادرسی منحرف شود و بر اساس یک سری اطلاعات و داده‌های جعلی، ساختگی و غیرواقعی، رأی صادر کند. توالی فاسد ارتکاب جعل عمیق در چنین مواردی، کاملاً آشکار و مبرهن است. بنابراین، جعل عمیق، به‌زودی، به معضلی اساسی در حقوق کیفری و نظام‌های عدالت جزایی تبدیل خواهد شد و چالش‌های فراوانی را برای کشورها به وجود می‌آورد. بر این اساس، کیفرگذاری افتراقی برای این

رفتار، از جمله ضروری‌ترین اقداماتی است که در راستای مقابله با آن، باید انجام شود.

بـه نظر می‌رسـد با رویکردی تحلیلی، می‌تـوان در مجموع، پنج توجیه را بـرای تبیین چراییِ جرم‌انگاری و کیفرگذاری افتراقی نسبت به جعل عمیق برشمرد که در ادامه، بررسی خواهند شد.

۲-۱. توجیه اخلاقی

یکـی از توجیهات اصلی جرم‌انگاری و کیفرگذاری افتراقی نسـبت به جعل عمیق، توجیه اخلاقی اسـت. جعل عمیق در صوت و تصویر افراد، مصداق بارز سوءاسـتفاده از فناوری‌های دیجیتال و پدیده‌ای به‌شـدت غیراخلاقی، به‌ویژه اگر به واسـطهٔ ارتکاب این جرم، نقـض و تجاوز به حریم خصوصی افراد رخ دهد، قلمداد شـده اسـت (Chesney, 2019: 1179). از منظر تحلیلی، می‌توان گفت که لزوم حمایت کیفری از مسـائل اخلاقی از جمله روابط و تعاملات اجتماعی میان مردم و جلوگیری از ارتکاب رفتارهای غیراخلاقی که حریم روابط و تعاملات روزمرهٔ افراد را با خدشـهٔ جدی مواجه می‌سازد، یکی از مهم‌ترین ضرورت‌هایی است که جرم‌انگاری و کیفرگذاری افتراقی نسـبت به جعل عمیق را توجیه می‌کند. بدین ترتیب، اخلاق حکم می‌کند که زمینه‌ها و بسـترهای سوءاستفاده از فناوری‌های نوین دیجیتال به منظور ارتکاب جعل عمیق، با مداخلهٔ سرسختانهٔ نظام حقوق کیفری مواجه شود.

۲-۲. توجیه اقتصادی

گاه سوءاسـتفاده از فناوری‌هـای و ابزارهـای مبتنی بـر هوش مصنوعی در قالـب ارتکاب جعل عمیق، به ورود ضررهای اقتصادی هنگفت به منافع ملی کشـورها منتهی می‌شود (Bregler, 2016: 353–360). تصـور کنیم فـرد یا افرادی با مقاصد و اهداف خاص سیاسـی و به قصد لطمه‌زدن به رقبـای خود، درصدد جعـل عمیق صوت و تصویر برآیند و با این کار، زمینه‌ها و بسـترهای وقوع مسـائلی نظیر قطع روابط همکاری‌های اقتصادی و سیاسی، اتهام‌زنی‌ها، دسیسه‌چینی‌های سیاسی، غرض‌ورزی‌ها و تسویه‌حساب‌های شخصی و سودجویانه و مواردی از این دست را میان کشورها و رهبران نظام‌های سیاسـی فراهم کنند. در اینجا، چه بسـا لطمات این امر، به‌شدت، نظام‌های کلی حاکم بر کشور به‌ویژه نظام اقتصادی را دستخوش تحولاتی کند.

بر این اساس، با دیدگاهی تحلیل‌گرانه و واقع‌گرایانه از رقابت‌هایی که به‌ویژه نظام‌های اقتصادی پویا و پیشرفته در جهان کنونی با یکدیگر دارند، می‌توان حدس زد که این نظام‌ها برای ربودن گوی سبقت از یکدیگر و ایجاد یا تشدید سیطره بر بازارهای مالی و پولی دیگر کشورها، ممکن است به جعل‌هـای عمیق صوتی و تصویری روی آورند و با تولید محتوای کذب، درصدد واردکردن ضربه

به نظام‌های اقتصادی رقیب برآیند. در چنین وضعیتی، از حیث اقتصادی و بنابر ضرورت صیانت از استحکام و سلامت عملکرد نظام‌های اقتصادی، مالی و پولی و به قصد پیشگیری از تولید و انتشار محتواهـای کذب و دروغین در فضای مجازی، جرم‌انگاری و کیفرگذاری افتراقی نسـبت به جعل عمیق در مقایسه با جعل رایانه‌ای ساده، توجیه کافی دارد.

۲-۳. توجیه سیاسی

از جمله مهم‌ترین عناصر موردنظر دولت‌ها در ساختاربندی تعاملاتشان با شهروندان، جلب اعتماد عمومی و همراه‌داشـتن مقبولیت همگانی در تصمیمات و سیاسـت‌گذاری‌ها است. ارتکاب جعل عمیق به‌ویژه اگر مبتنی بر نشـر اکاذیب و یا افترا به مقامات سیاسـی باشـد، به‌شدت می‌تواند این اعتماد را خدشـه‌دار سـازد (Zollhöfer, 2016: 233). از سـوی دیگر، عرصهٔ رقابت‌های سیاسی می‌تواند بسـتر مساعدی برای ارتکاب جعل عمیق باشـد. دروغ‌پراکنی‌های گوناگون رقبا، احزاب و شـخصیت‌ها نسبت به یکدیگر، سـلامت و بهداشت نظام‌های سیاسی و حوزه‌های سیاست‌گری و سیاسـت‌گذاری را بـا چالش مواجه می‌کند و جعـل عمیق، به‌مثابهٔ یکـی از مهم‌ترین ابزارهای پمپاژ دروغ در عرصهٔ سیاسـی شناخته می‌شود. بر این اسـاس، یکی از مهم‌ترین توجیهات مدنظر قانون‌گذاران در جرم‌انگاری و کیفرگذاری افتراقی نسبت به جعل عمیق، توجیه سیاسی است.

می‌تـوان پیش‌بینی کرد در آینده‌ای نه چندان دور، چه بسـا رقبای انتخاباتی، برای فریب افکار عمومی و برای جلب و جذب آرای شـهروندان، از طریق سوءاستفاده از فناوری‌های نوین به‌ویژه هـوش مصنوعی و با تولید و انتشـار تصاویر یـا اصوات دروغین، وجههٔ رقبـای خود را تخریب کنند. از منظر تحلیلی و با دیدگاهی واقع‌گرا، می‌توان لطمه به اسـتحکام و ثبات نظام‌های سیاسی و انتخاباتی، برهم‌خوردن نظم و آرامش عمومی در جامعه در نتیجهٔ انتشار گستردهٔ کلیپ‌های دیداری یا شنیداری کذب از سوی رقبای انتخاباتی و سیاسی علیه همدیگر و نیز ایجاد یا تشدید بی‌اعتمادی به ساختارهای سیاسی حاکم را از جمله پیامدهای جدی و مخاطره‌آمیز جعل عمیق محسوب کرد. بر این اسـاس، به نظر می‌رسـد باید باور به برخورد متفاوت و افتراقیِ مقنن کیفری با این شکل از جعل صوت و تصویر در مقایسه با جعل عادی رایانه‌ای بود.

۲-۴. توجیه امنیتی

از جمله توجیهات جرم‌انگاری و کیفرگذاری افتراقی نسبت به جعل عمیق، توجیه امنیتی است. این مـورد، به‌ویژه به این علت اهمیت دارد که ارتکاب جعـل عمیق می‌تواند افراد یا نهادهای مخاطب را با مخاطرات جدی امنیتی مواجه سازد (Mirsky, 2020: 333). با رویکردی تحلیلی و با توجه به

برخی واقعیت‌های مستند و مبتنی بر شواهد عینی، می‌توان گفت تولید تصاویر یا اصوات غیرواقعی و قلابی به‌صورت جعل عمیق، به‌ویژه در شرایط خاصی مانند وضعیت‌های جنگی، می‌تواند موجبات تشویش شدید اذهان عمومی، دروغ‌پراکنی‌های گسترده، تحریک نیروهای خودسر به مقابله و رویارویی، شکل‌گیری وضعیت‌های خشونت‌بار و جنگ‌های شهری و نیز در قلمرویی وسیع‌تر، تشدید درگیری‌های فراشهری، القای شکست‌ها و پیروزی‌های کاذب، گسسته‌شدن انتظام و انسجام نیروهای نظامی و دفاعی و دیگر موارد شود. بدیهی است که هریک از این پیامدها، چه به‌صورت مستقل و چه در پیوند با یکدیگر، می‌تواند بنیان‌های امنیتی کشور را به‌طور جدی متزلزل سازد.[۱]

می‌توان مدعی بود که پیامدهای مخاطره‌آمیز جعل عمیق از حیث امنیتی، برای نظام‌های سیاسی، دامنه‌ای بسیار گسترده دارد و آن‌ها را در تنگناهای سخت قرار می‌دهد. بر این اساس، یکی از عرصه‌هایی که به‌طور جدی می‌تواند از ارتکاب جعل عمیق، موردتهدید عملی قرار گیرد، حوزهٔ امنیتی است. تصور کنیم جنگی میان دو کشور رخ داده است و هکرهای سایبری از هر دو طرف درگیر در مخاصمه، با ساخت صوت یا تصاویر جعلی، اذعان به شکست در برابر دشمن کنند و به نیروهای خودی، دستور عقب‌نشینی یا تحویل مواضع حساس به طرف مخاصمه صادر کنند. تبعات و لطمات جبران‌ناپذیر انتشار این صوت یا تصویر جعلی، قابل پیش‌بینی است. لذا به نظر می‌رسد لزوم صیانت از امنیت ملی در همهٔ کشورها ضرورت جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق در مقایسه با جعل رایانه‌ای عادی را توجیه می‌کند.

۲-۵. توجیه فنی (تکنیکال)

مقصود از این توجیه، در واقع، صیانت و مراقبت از کارکردهای مثبت فناوری‌های نوین است. توضیح اینکه امروزه، سوءاستفاده از فناوری‌های نوین از جمله هوش مصنوعی، یکی از مهم‌ترین چالش‌ها و مخاطراتی است که نظام‌های حقوقی با آن‌ها مواجه‌اند (عطازاده و انصاری، ۱۳۹۸: ۸۰). در واقع، ضرورت بهره‌برداری بهینه و غیرمجرمانه از کارکردهای مثبت فناوری‌های نوین، به‌ویژه هوش مصنوعی، اقتضا می‌کند که حتی‌الامکان از سوءاستفاده از این فناوری‌ها جلوگیری کرد تا امکان استفاده و انتفاع بشر از آن‌ها به‌صورت مسالمت‌آمیز، کارآمد، غیرمجرمانه و غیرمنحرفانه فراهم آید.[۲] باید افزود که آمریکا به‌عنوان کشوری که برای نخستین بار، مفاهیم و کاربردهای

۱. نمونهٔ بارز این سردرگمی را می‌توان در سخنان شهردار نیویورک یا فرماندار آریزونا در نوامبر ۲۰۲۱ میلادی مشاهده کرد. هر دو حتی مدعی نفوذ در رخنه‌های امنیتی پنتاگون (وزارت دفاع آمریکا) نیز شدند و اعلام داشتند فناوری‌های مبتنی بر هوش مصنوعی و به‌ویژه جعل عمیق، به‌زودی، به چالش امنیتی گسترده‌ای برای ایالات متحده آمریکا تبدیل خواهد شد (Lees, 2023: 244).

۲. حقیقت آن است که فناوری هوش مصنوعی، به‌منزلهٔ جلوهٔ جدیدی از فناوری‌ها، موارد استفاده و انتفاع مشروع

فناوری هوش مصنوعی در آن شکل گرفت و گسترش یافت، سعی کرده است از منافع و کارکردهای صلح‌جویانه و مسالمت‌آمیز فناوری‌های نوین حداکثر صیانت را به عمل آورد، اما شواهد موجود دلالت بر این واقعیت دارند که در برخی موارد، این تلاش‌ها موفقیت‌آمیز نبوده است و بهره‌برداری از فناوری‌های نوین، به‌ویژه فناوری‌های مبتنی بر هوش مصنوعی، گاه، به‌صورت کاملاً مجرمانه و منحرفانه بوده است. در این میان، پدیدهٔ جعل عمیق را می‌توان یکی از بارزترین مصادیق و مظاهر این انتفاع مجرمانه و منحرفانه از فناوری هوش مصنوعی در آمریکا دانست (Perov, 2020: 391). بنابراین، از حیث فنی نیز می‌طلبد که زمینه‌های سوءاستفاده از فناوری هوش مصنوعی از جمله در راستای ارتکاب جعل عمیق، محدود شود و این سوءاستفاده‌ها با ضمانت اجراهای کیفری کارآمد، مواجه شوند. در حقیقت، با دیدگاهی تحلیلی باید گفت فناوری‌های نوین، به‌ویژه هوش مصنوعی، در کنار همهٔ انتفاعات مثبت و کارکردهای سازنده‌ای که برای بشر دارند، ممکن است ابزار ارتکاب جرم نیز قرار گیرند. بنابراین، وجههٔ همت دولت‌ها و نظام‌های حقوقی باید مقابله با بهره‌برداری‌های مجرمانه از این فناوری‌ها و در عوض، حمایت از استفاده‌های نامجرمانه از آن‌ها باشد. جعل عمیق، گاه، حالت مجرمانه به خود می‌گیرد و از آنجا که مراتب شدید جعل در داده‌های صوتی و تصویری در آن رخ می‌دهد، باید موضوع رویکرد افتراقی قانون‌گذاران کیفری از حیث جرم‌انگاری و کیفرگذاری نیز واقع شود و اکتفا به جرم‌انگاری‌ها و کیفرگذاری‌های عادی، برای مقابلهٔ مؤثر با آن و مبارزه با انتفاعات مجرمانه از آن، کافی نیست.

مقولهٔ دیگری که باید بحث و اشاره شود این است که در برخی نظام‌های کیفری، جرم‌انگاری و کیفرگذاری افتراقی و ویژه نسبت به جعل عمیق در مقایسه با جعل‌های رایانه‌ای عادی، صورت گرفته است. نمونهٔ بارز این نظام‌ها آمریکا و چین هستند. در بخش بعدی نوشتار حاضر، از یک سو با هدف مطالعهٔ تطبیقی موضوع مقاله و بهره‌برداری از تجربیات و دستاوردهای این دو کشور در مواجهه با پدیدهٔ جعل عمیق در نظام کیفری داخلی آن‌ها و از سوی دیگر، به منظور تقویت غنای علمی این نوشتار، فرایند جرم‌انگاری و کیفرگذاری افتراقی نسبت به این پدیده در نظام کیفری این دو کشور، موردمطالعه و تحلیل قرار گرفته است.

فراوانی دارد که از آن جمله می‌توان به «عملیات پزشکی و درمانی از راه دور» (موسوم به تله مدیسین) و استفاده از «ربات‌های جراح» در این عملیات اشاره داشت. دیده و شنیده شده است که برخی بیماران که توان اقتصادی و مالی کافی برای سفر به کشورهای دیگر برای درمان بیماری یا انجام معالجات جراحی پیچیده را ندارند، با استفاده از فناوری‌های نوین، به‌ویژه ربات‌های جراح مبتنی بر هوش مصنوعی، توانسته‌اند از مزایای این فناوری‌ها به‌خوبی بهره‌مند شوند (هالوی، ۱۳۹۸: ۴۴). با این حال، در کنار مزایا و انتفاعات حاصل از فناوری هوش مصنوعی، قابلیت‌های این تکنولوژی در ارتکاب جعل عمیق و آثار ناگوار حاصل از آن در عرصه‌های مختلف، به‌روشنی آشکار است.

۳. ارزیابی و تحلیل جرم‌انگاری و کیفرگذاری افتراقی نسبت به جعل عمیق در حقوق کیفری آمریکا و چین

۳-۱. حقوق کیفری آمریکا

در حقــوق کیفری آمریکا، با توجه به همهٔ توجیهاتی که پیش‌تر اشــاره شــد، در کنار جعل رایانه‌ای ســاده یا عادی، جعل عمیق نیز جرم‌انگاری شده است. قانون‌گذار آمریکایی در مقدمهٔ قانونی که در راستای جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق به تصویب رسانده است و به «قانون مجازات مرتکبــان جعل عمیق و محافظت از حفظ حریم خصوصی افراد»[1] مصوب ۲۰۲۱ میلادی موســوم اســت، تصریح می‌کند که یکی از تعهدات دولت آمریکا نســبت به شــهروندان این کشور و نیز همهٔ افراد حاضر در قلمرو این کشور، صیانت از حریم خصوصی آن‌ها است و جعل عمیق از رفتارهای اخلاقاً ممنوعی است که این حریم را به‌طور جدی به مخاطره می‌اندازد. همچنین، از آنجا که مقولهٔ امنیت، از مؤلفه‌های بنیادین تضمین قدرت و هژمونی آمریکا به شــمار می‌آید و پدیدهٔ جعل عمیق، این امر را با مخاطرات جدی مواجه می‌ســازد، قانون‌گــذار آمریکایی، پدیدهٔ جعل عمیق را در کنار جرم جعل رایانه‌ای جرم‌انگاری و کیفرگذاری افتراقی کرده است. به علاوه در بخش دیگری از مقدمهٔ مورداشــاره، اعلام داشته اســت که یکی از مهم‌ترین اهداف موردنظر از جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق، صیانت و حراست از امنیت ملی آمریکا است (Reid, 2021: 229-244).

در فراینــد تصویب «قانون مجازات مرتکبان جعل عمیق و محافظت از حفظ حریم خصوصی افراد» مصوب ۲۰۲۱ میلادی در آمریکا، بسیاری از سناتورهای آمریکایی به وقایعی اشاره کرده‌اند کــه در جریــان رقابت‌های انتخاباتی اخیر این کشــور میان بایدن و ترامــپ رخ داد؛ وقایعی که در آن‌ها با سوءاستفاده از فناوری هوش مصنوعی، ویدئوهای جعلی منتسب به این دو نامزد و خطاب به طرفداران و مخالفانشــان، تولید و منتشر شد. ســناتورها در نهایت به این جمع‌بندی رسیدند که فقدان مقابلهٔ مؤثر کیفری با پدیدهٔ جعل عمیق می‌تواند پیامدهای سیاســی وخیمی برای دموکراسی آمریکا در بر داشــته باشــد. نظر به مراتب پیش‌گفته، میزان مجازات جعل در داده‌های رایانه‌ای، که در مقایســه بــا مقررات کیفریِ خاص مربــوط به جعل عمیق، می‌توان آن را «جعل عادی و ســادهٔ داده‌های رایانه‌ای» نامید، به موجب قانون «کلاهبرداری و سوءاســتفاده‌های رایانه‌ای»[2] (اصلاحی ۲۰۱۱ میلادی)، جریمهٔ نقدی پنج‌هزار دلاری به همراه برخی ممنوعیت‌ها از حقوق اجتماعی تعیین شده است. این در حالی است که در خصوص جعل عمیق صوتی و تصویری، در قانون «مجازات مرتکبــان جعل عمیق و محافظت از حفــظ حریم خصوصی افراد» (مصوب ۲۰۲۱ میلادی)، میزان

1. «Punishing Perpetrators of Deep Fake and Protecting People's Privacy Act (2021)»
2. Computer Fraud and Abuse Act (CFAC) (Amended 2011)

جریمهٔ نقدی، بین دو تا چهار برابر است. همچنین در صورتی که شرکت‌ها یا مؤسسات فعال در زمینهٔ تولید و تبادل نرم‌افزارهای رایانه‌ای مرتکب جرم جعل عمیق شوند، در مرحلهٔ نخست با ممنوعیت موقت پنج‌ساله از فعالیت و در صورت تکرار به ممنوعیت دائمی از فعالیت مواجه می‌شوند. البته برخی مجازات‌های تکمیلی دیگر از جمله الزام به ارائهٔ خدمات عمومی نیز نسبت به مرتکبان جعل عمیق در این قانون در نظر گرفته شده است (Beebom, 2022: 159).

۳-۲. حقوق کیفری چین

در نظام کیفری چین، آخرین اقدام تقنینی در راستای جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق، در سال ۲۰۲۱ میلادی صورت گرفت که به تصویب قانونی موسوم به «قانون جرم‌انگاری جعل‌های عمیق صوتی و تصویری و مقابله با رفتارهای ضد امنیت ملی»[1] انجامید. در این چهارچوب، رویکرد اخلاقی یکی از مهم‌ترین مبانی موردتوجه در سیاست‌گذاری کیفری این کشور در مواجهه با پدیدهٔ جعل عمیق بوده است؛ به نحوی که در مقدمهٔ این قانون آورده شده است: «... حفاظت از حریم خصوصی افراد که در پرتو بهره‌گیری از فناوری جعل عمیق، به‌شدت می‌تواند موردتهدید قرار گیرد، واجد اهمیتی بنیادین و مبتنی بر ملاحظات اخلاقی است... بر این اساس، جرم‌انگاری جعل عمیق، بر ضرورتی اخلاقی استوار است... و اقتضا دارد با اشخاصی که داده‌های صوتی و تصویری را در معرض تحریف‌های عمیق و گمراه‌کننده قرار می‌دهند، به نحو متناسب و کارآمدی مقابله کرد... صوت‌ها و تصویرهای تولیدشده در قالب جعل عمیق، از مهم‌ترین ابزارهای آسیب‌رسان به حریم خصوصی افراد و نیز امنیت ملی کشورند...» (Filimowicz, 2022: 144).

باید افزود که در حقوق کیفری چین، توجیه اقتصادیِ جرم‌انگاری و کیفرگذاری جعل عمیق نیز موردتوجه ویژه بوده است. این کشور که به‌تدریج در حال تبدیل‌شدن به یکی از قدرت‌های بزرگ اقتصادی جهان است، طبعاً حساسیت خاصی برای صیانت از امنیت اقتصادی خود دارد و یکی از مهم‌ترین دلایل بهره‌گیری نظام کیفری چین از جرم‌انگاری افتراقی جعل عمیق نیز ناظر بر همین ملاحظه است. به نحوی که در جریان مذاکرات مربوط به تصویب «قانون مبارزه با جعل عمیق و استفادهٔ مجرمانه از هوش مصنوعی»[2] مصوب ۲۰۲۰ میلادی، امنیت اقتصادی یکی از مهم‌ترین حوزه‌های در معرض تهدید ناشی از ارتکاب جعل عمیق معرفی و اعلام شده است (Odonnell, 2021: 712–708). به موجب این قانون، میزان جزای نقدی برای جعل عمیق، در مقایسه با جعل‌های رایانه‌ای عادی، حداقل شش برابر تعیین شده است. همچنین، در صورت تکرار این

1. Criminalizing Deep Audio and Video Forgeries and Countering Anti-National Security Behaviors Act (2022)
2. «Combating Deep Fake and Criminal Use of Artificial Intelligence» Act (2020)

رفتار، حبس از چهار تا پانزده سال برای مرتکبان در نظر گرفته شده است، در حالی که در جعل‌های رایانه‌ای عادی، میزان حبس بین دو تا شش سال است (Gieseke, 2020: 144).

در تحلیل رویکرد دو نظام کیفری آمریکا و چین در زمینهٔ جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق و تمایز آن با جعل رایانه‌ای ساده، می‌توان گفت مقنن کیفری در هر دو کشور به‌درستی دریافته است که از حیث ماهیت و نحوهٔ ارتکاب، جعل عمیق تفاوت‌های بنیادینی با جعل رایانه‌ای عادی دارد؛ وگرنه، تشدید مجازات جعل عمیق در قوانین کیفری این دو کشور، اساساً محملی نداشت. جالب آنکه، این دو کشور اکنون، رقبای جدی یکدیگر در عرصهٔ تجارت و اقتصاد محسوب می‌شوند و به نظر می‌رسد یکی از انگیزه‌های مهم مقنن کیفری در هر دو کشور برای جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق، مقابله با تحرکات و رفتارهایی باشد که از طریق دست‌کاری صوت و تصویر و تولید و انتشار محتواهای دیداری و شنیداری از سوی طرف مقابل می‌تواند محقق شود. نکتهٔ دیگر اینکه، روابط دو کشور از حیث سیاسی نیز چندان دوستانه نیست و در بسیاری از محافل و گفتمان‌های سیاسی، چین نماد بارز اقتصاد و سیاست کمونیستی و آمریکا مصداق آشکار اقتصاد و سیاست سرمایه‌داری معرفی، و دو قطب کاملاً مخالف یکدیگر ارزیابی می‌شوند. بر این پایه، جرم‌انگاری و کیفرگذاری افتراقی و تشدیدی نسبت به جعل عمیق در قوانین کیفری دو کشور، شاید برای پیشگیری و مقابله با تبلیغات سوء و منفی طرف مقابل باشد. بنابراین، تمایزگذاری میان جعل عمیق و جعل رایانه‌ای عادی در نظام‌های کیفری آمریکا و چین، افزون بر ابعاد فنی و حقوقی، واجد صبغه‌ای سیاسی نیز هست.

اینک، در پرتو درک رویکرد مقنن کیفری در آمریکا و چین در خصوص جرم‌انگاری و کیفرگذاری افتراقی نسبت به جعل عمیق در مقایسه با جعل رایانه‌ای ساده، در بخش بعدی، جایگاه این مقوله در حقوق کیفری ایران، بحث و تحلیل می‌شود.

۴. مطالعه و تحلیل جایگاه پدیدهٔ جعل عمیق در مقایسه با جعل رایانه‌ای عادی در حقوق کیفری ایران

جعل رایانه‌ای در مادهٔ ۶ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ (معادل مادهٔ ۷۴۳ قانون تعزیرات مصوب ۱۳۷۵) جرم‌انگاری شده است. عنصر مادی این جرم، به تصریح مادهٔ یادشده، عبارت است از تغییردادن داده‌های قابل‌استناد، ایجاد یا واردکردن متقلبانهٔ این داده‌ها به داده‌های رایانه‌ای دیگر. در جعل رایانه‌ای، یا داده‌ای که از اساس وجود نداشته است، ایجاد می‌شود، یا در داده‌ای که پیش‌تر وجود داشته است، تغییر صورت می‌گیرد و یا اینکه داده‌ای که قبلاً تولید شده است، به‌طور متقلبانه وارد داده‌های قبلی می‌شود.

اما به نظر می‌رسد آنچه در قالب جعل عمیق ارتکاب می‌یابد، به مراتب، پیچیده‌تر و پیشرفته‌تر از جعل رایانه‌ای عادی (یا ساده) (موضوع مادهٔ ۶ قانون جرایم رایانه‌ای) است. با استفاده از جعل عمیق، می‌توان صدا و تصویر را به‌صورت حیرت‌انگیزی تحریف کرد؛ به نحوی که در بسیاری از موارد، تشخیص موارد جعلی از موارد اصلی، بسیار سخت و چه بسا حتی غیرممکن می‌شود. مبنای جعل عمیق، تحریف واقعیت و به‌طور خاص، تحریف صوت و تصویر است (سلطانی‌فر و همکاران، ۱۳۹۶: ۶۰).

از سوی دیگر، ممکن است جعل عمیق، مصداقی از جرایم علیه عفت و اخلاق عمومی در فضای سایبری (موضوع مادهٔ ۱۴ قانون جرایم رایانه‌ای و معادل مادهٔ ۷۴۲ قانون تعزیرات)، هتک رایانه‌ای حیثیت (موضوع دو مادهٔ ۱۶ و ۱۷ قانون جرایم رایانه‌ای و معادل مواد ۷۴۴ و ۷۴۵ قانون تعزیرات) یا نشر اکاذیب رایانه‌ای (موضوع مادهٔ ۱۷ قانون جرایم رایانه‌ای و معادل مادهٔ ۷۴۶ قانون تعزیرات) در نظر گرفته شود. همچنین ممکن است این فناوری به‌طور گسترده برای تولید و پخش فیلم‌ها و تصاویر منافی عفت عمومی، تصاویر مستهجن، هرزه‌نگاری کودکان و مانند این‌ها استفاده شود (تقی‌پور و زرینه، ۱۳۹۴: ۸۳؛ حبیب‌زاده و رحمانیان، ۱۳۹۰: ۱۲۰؛ نوری، ۱۳۸۶: ۴۱). اما در یک نکته نمی‌توان تردید داشت و آن اینکه، جعل عمیق پیش از آنکه مشمول هریک از این عناوین مجرمانه قرار گیرد و بخواهد مقدمه یا ابزاری برای ارتکاب نشر اکاذیب رایانه‌ای یا هتک رایانه‌ای حیثیت افراد در فضای مجازی باشد، رفتاری مبتنی بر تحریف و دست‌کاری داده‌های رایانه‌ای آن هم به شکلی پیچیده است. بنابراین، از حیث ماهیت، با عنوان مجرمانهٔ جعل رایانه‌ای (موضوع مادهٔ ۶ قانون جرایم رایانه‌ای و معادل مادهٔ ۷۳۴ قانون تعزیرات) سازگار است. در واقع، از حیث تحلیلی می‌توان گفت در جعل عمیق، قبل از آنکه هتک حیثیت یا نشر اکاذیب واقع شود، جعل رایانه‌ای مبتنی بر تحریف و دست‌کاری داده‌های رایانه‌ای محقق است و لذا شمول عنوان جعل رایانه‌ای بر جعل عمیق، منطقی‌تر و پذیرفتنی‌تر است. با این حال، شکلی خاص و به مراتب، آسیب‌زاتر از جعل رایانه‌ای عادی (ساده) در جعل عمیق واقع می‌شود.

باید افزود که جعل رایانه‌ای معمولاً نسبت به داده‌هایی رخ می‌دهد که به‌صورت صفر و یک در یک سامانهٔ رایانه‌ای یا مخابراتی تعریف شده‌اند، اما در جعل عمیق، صوت یا تصویر واقعی فرد به صورتی تغییر می‌یابد که تشخیص صوت و تصویر واقعی از غیرواقعی امکان‌پذیر نخواهد شد. بنابراین، به نظر می‌رسد جعل عمیق، مفهومی فراتر از جعل صرف در داده‌های رایانه‌ای باشد. بر این اساس، شاید ماهیت جعل رایانه‌ای عادی و جعل عمیق، همچنان مبتنی بر تغییر و تحریف داده‌ها باشد، اما به باور نگارندگان حاضر، نمی‌توان جعل عمیق را عیناً همان جعل رایانه‌ای عادی دانست. بنابراین، ماهیت پیچیده‌تر جعل عمیق نسبت به جعل رایانه‌ای ساده (یا عادی)، اقتضای

کیفرگـذاری افتراقی و مواجهه ایـن حالت خاص از جعل رایانه‌ای با مجازاتی شـدیدتر از جعل رایانه‌ای سـاده و عادی را دارد. از این رو، مجازات پیش‌بینی‌شده در مادهٔ ۶ قانون جرایم رایانه‌ای ناظر بر جرم جعل رایانه‌ای، برای مقابله با جعل عمیق، آن‌گونه که باید و شاید کافی نیست.

باید به این نکته نیز اذعان داشـت که فقدان جرم‌انگاری و کیفرگذاری افتراقی نسـبت به جعل عمیق در نظام کیفری ایران، چه بسـا به عقب‌ماندن این نظام از دیگر نظام‌های کیفری منتهی شـود کـه در پی جرم‌انگاری و کیفرگـذاری افتراقی جعل عمیق تجربه کرده‌اند؛ وضعیتی که در نوع خود، واجد زیانی قابل‌توجه است.

در تحلیـل دقیق‌تر می‌تـوان گفت، مجموعه‌ای از ملاحظات بنیادیـن، ضرورت جرم‌انگاری و کیفرگـذاری افتراقی نسـبت به جعل عمیـق را در نظام کیفری ایران توجیـه می‌کند؛ از جمله لزوم صیانـت از حریم خصوصی افراد به‌مثابهٔ قاعده‌ای برتر در جامعـهٔ ایرانی و اهتمام قانون‌گذاران و سیاسـت‌گذاران کلان کشـور در خصوص این مقوله، ضرورت همگامی با رشد و توسعهٔ اقتصادی در سـطح جهان و عقب‌نماندن از چرخهٔ تولید و تجارت بین‌المللی، لزوم پیشگیری از سوءاستفادهٔ بزهکاران برای ایجاد تنش، ناامنی و یا اختلاف‌افکنی میان اقوام و مذاهب گوناگون ساکن در کشور یا ایجاد تشت میان سیاسیون در ایران و دامن‌زدن به اختلافات سیاسی. افزون بر این، محافظت از مرزها و تمامیت ارضی کشور و ضرورت مقابله با تحرکات ضدامنیتی و نیز سامان‌بخشی تقنینی به استفاده از فناوری‌های نوظهور به‌ویژه هوش مصنوعی که دیر یا زود به مؤثرترین فناوری در ابعاد و عرصه‌های مختلف زندگی جوامع انسانی تبدیل خواهد شد، همگی بر ضرورت پیش‌بینی واکنشی کیفری افتراقی نسبت به جعل عمیق در حقوق کیفری ایران دلالت دارند.

بحث مهم دیگری در ارتباط با پدیدهٔ جعل عمیق که می‌تواند موردتوجه باشـد، امکان ارتکاب این نوع جعل برای «دلیل‌سازی‌های واهی» در پرونده‌های قضایی است. با توجه به توضیحاتی که در ارتباط با ماهیت جعل عمیق و نحوهٔ ارتکاب آن در نوشـتار حاضر ارائه شـد، تردیدی نیست که امکان سوءاسـتفاده از فناوری‌های مبتنی بر هوش مصنوعی برای سـاخت صداها و یا تصویرهای دروغین دال بر ادای اقرار، شهادت و سوگند و ارائهٔ این دلیل‌های کاذب به مراجع قضایی و یا دیگر مراجع قانونی در مقام نفی یا اثبات موضوعات مختلف، وجود دارد.

تصور کنیم فردی در پرونده‌ای، از ادای شـهادت شـخصی منتفع می‌شود و با توسل به فناوری جعـل عمیق، کلیپی از ارائهٔ شـهادت آن فـرد تولید می‌کند؛ به‌گونه‌ای که مقـام قضایی یا قانونی را به‌طور مؤثر گمراه کند و وی شـاهد و محتوای شـهادت ارائه‌شـده را واقعی بپندارد و بر مبنای آن، رأی به سـود فرد منتفع صادر کند؛ حال آنکه توسـل به این شـهادت و ارائهٔ آن به مرجع قضایی، از اساس کذب و خلاف حقیقت بوده است. به نظر می‌رسد صرفاً از رهگذر جرم‌انگاری جعل عمیق

به نحو افتراقی اســت که می‌توان با چنین رفتارهایی که صراحتاً، فرایند دادرســی کیفری را دچار انحــراف می‌کنند و قابلیت قرارگرفتن در زمرهٔ جرایم علیه عدالت قضایی را دارند، برخوردی مؤثر و متناسب به عمل آورد؛ وگرنه اکتفا به مقررات فعلی موجود در زمینهٔ جعل رایانه‌ای ساده در مقام واکنش نســبت به دلیل‌سازی‌های واهی و کاذبانه در مراجع قضایی چه بسا کافی و وافی به مقصود نباشــد. حقیقت آن است که جعل عمیق، «قابلیت واقعی جلوه‌دادن همهٔ پدیده‌های غیرواقعی»[1] را دارد و این ویژگی، برای عرصه‌های مختلف زندگی فردی و اجتماعی بشــر امروز خطرناک اســت و به‌ســادگی می‌تواند حریم حقوق و آزادی‌های بنیادین شــهروندان و نیز امنیت سیاســی و نظامی حاکمیت‌هــا را به‌طــور جدی، تهدید و تحدیــد کند.[2] از این رو، نگارندگان بــر این باورند که نگاه قانون‌گــذار ایرانی به پدیدهٔ جعــل رایانه‌ای، چندان با واقعیات و الزامــات مربوط به جعل عمیق، همخوانی ندارد و باید درصدد رفع این خلأ تقنینی مهم برآمد.

۵. توجیه و تحلیل چرایی و ضرورت کیفرگذاری افتراقی جعل عمیق در مقایسه با جعل رایانه‌ای عادی در نظام کیفری ایران

بــه بــاور نگارندگان این مقاله، عنوان مجرمانهٔ «جعل رایانه‌ای» مذکــور در قانون جرایم رایانه‌ای، در وضعیت کنونی، کفایت لازم برای شــمول بر پدیدهٔ جعل عمیق را ندارد و از همین رو ضروری اســت قانون‌گذار ایرانی در مقام جرم‌انگاری مســتقل و کیفرگذاری افتراقی نســبت به جعل عمیق اقدام تقنینی مقتضی به عمل آورد.

چند دلیل عمده می‌تواند ضرورت جرم‌انگاری و کیفرگذاری افتراقی نســبت به جعل عمیق در نظام کیفری ایران را توجیه کند:

۱. از حیــث ماهوی، جعل عمیــق پدیده‌ای به مراتب پیچیده‌تر از جعل رایانه‌ای مقرر در قانون جرایم رایانه‌ای است. همین تفاوت ماهوی، ضرورت تفاوت‌گذاری در نوع واکنش و پاسخ کیفری به جعل عمیق نســبت به جعل‌های رایانه‌ای ســاده را تقویت می‌کند. بر این اساس، می‌تــوان گفت جرم‌انگاری و کیفرگذاری افتراقی نســبت به جعل عمیق به‌صورت خاص، می‌توانــد خلأهــای تقنینی و قضایی را برطرف کند؛ خلأهایی کــه در آن‌ها، جرم‌انگاری و

1. Fake - Building

۲. برای مطالعهٔ بیشــتر در مورد قابلیت «فیک‌ســازی» جعل عمیق، بنگرید به: (Helmus, 2022: 30-35). آقای هلموس کــه متخصص فناوری اطلاعات و امنیت شــبکه در پلیس فدرال آمریکا اســت، در این گــزارش، مهم‌ترین قابلیت فناوری هوش مصنوعی به منظور ارتکاب جعل عمیق صوتی و تصویری را وارونه جلوه‌دادن همه‌چیز اعلام می‌کند. بــه نظــر وی، این خصیصه امکان رســوخ و نفوذ به همهٔ جنبه‌ها و حریم‌های شــخصی و جمعی زندگی بشــر را به سوءاستفاده‌کننده‌ها و بزهکاران خواهد داد.

کیفرگذاری نسبت به جعل ساده و عادی، قدرت مقابلهٔ مؤثر با جعل‌های عمیق را ندارد.

۲. از سوی دیگر، قانون جرایم رایانه‌ای، در سال ۱۳۸۸ به تصویب رسیده است. در آن زمان، جعل عمیق صوتی و تصویری، یا به کلی در عرصهٔ بین‌المللی ارتکاب نیافته بود و یا اساساً تصور نمی‌شد که این پدیده، بتواند به مراتب، آسیب‌ها و خسارت‌های شدیدتری نسبت به جعل‌های رایانه‌ای ساده و عادی، ایجاد کند. حال آنکه این پدیده در سال‌های اخیر رخ داده و به‌مثابهٔ جلوهٔ پیچیده و خاصی از جعل رایانه‌ای، موردتوجه قرار گرفته است. بر این اساس، لزوم همگامی و همسویی نظام کیفری ایران با تحولات جرم‌انگارانه و کیفرگذارانه در سطح بین‌المللی در مواجهه با جعل عمیق و ضرورت انطباق بیشتر نظام کیفری ایران در قانون جرایم رایانه‌ای با این تحولات، می‌تواند توجیه‌کنندهٔ ضرورت جرم‌انگاری و کیفرگذاری افتراقی نسبت به جعل عمیق در کنار جعل رایانه‌ای عادی باشد.

۳. از جانب دیگر، به نظر می‌رسد جعل عمیق در آینده‌ای نزدیک به یکی از چالش‌های مهم و فراگیر نظام‌های کیفری تبدیل شود. گسترش روزافزون فناوری‌های مبتنی بر هوش مصنوعی به بسیاری از عرصه‌های مختلف زندگی فردی و اجتماعی در دوران فعلی، امکان سوءاستفادهٔ مجرمانه از این فناوری را برای ارتکاب جعل عمیق آسان‌تر خواهد کرد. جعل عمیق به‌سادگی می‌تواند ابزاری برای تشدید مناقشات سیاسی و حزبی و برهم‌زدن امنیت ملی بدل شود و به‌ویژه در جامعه‌ای مانند ایران که از تنوع قومی، اقلیت‌های دینی و فرهنگ‌های قومیتی گوناگون برخوردار است، بستر مناسبی را برای انواع سوءاستفاده‌ها و انتقام‌جویی‌های سیاسی، فرهنگی و مذهبی از سوی افراد و گروه‌های سودجو و فرصت‌طلب فراهم آورد.[۱]

بر این اساس، با فرض اینکه جرم‌انگاری و کیفرگذاری ناظر بر جعل رایانه‌ای ساده در نظام کیفری فعلی، تکافوی پاسخ‌دهی کیفری کارآمد به جعل عمیق را ندارند، به نظر می‌رسد می‌توان مدعی شد که جرم‌انگاری و کیفرگذاری افتراقی برای جعل عمیق در ایران، چه بسا آثار پیشگیرانه و بازدارنده نیز داشته باشد. این جرم‌انگاری و کیفرگذاری ویژه، از منظر لزوم صیانت همه‌جانبه از امنیت داخلی و بین‌المللی کشور بسیار اهمیت دارد.

به نظر می‌رسد همهٔ توجیه‌هایی که پیش‌تر در راستای جرم‌انگاری و کیفرگذاری افتراقی نسبت

---

۱. به باور برخی نویسندگان، استفاده از فناوری هوش مصنوعی برای ارتکاب جعل‌های عمیق صوتی و تصویری، هرگز به استفاده‌های تفریحی و سرگرم‌کننده محدود نبوده است و نخواهد بود، بلکه جنبه‌های مجرمانه و سوءاستفاده‌جویانهٔ بسیاری را می‌توان برای این رفتار در نظر گرفت. بر همین اساس، باید درصدد همسان‌سازی قوانین کیفری با این پدیدهٔ جدید و رو به رشد بود. برای مطالعهٔ بیشتر، بنگرید به: (احسان‌پور و امی، ۱۴۰۱: ۱-۹).

به جعل عمیق، به آن‌ها اشـاره شـد و عمده مبانی موردتوجه قانون‌گذاران کیفری در کشورهایی که اقدام به جرم‌انگاری و کیفرگذاری افتراقی، ویژه و تشدیدیافته نسبت به جعل عمیق کرده‌اند (یعنی توجیـه اخلاقی، توجیه اقتصادی، توجیه سیاسـی، توجیه امنیتـی و توجیه فنی)، در خصوص نظام کیفری ایران نیز صادق هسـتند. از این رو، مجموع این توجیهات می‌توانند مبنای مناسـبی را برای تبیین نحوهٔ مقابله و مواجههٔ نظام کیفری ایران با پدیدهٔ جعل عمیق فراهم آورند.

در مقـام جمع‌بندی می‌توان گفت که کشـور ما نیز به‌مثابهٔ یکـی از دولت‌های حاضر در عرصهٔ تعامـلات بین‌المللـی، هرگز نمی‌تواند خود را از تحولات فناورانه دور نگاه دارد. از سـوی دیگر، امکان سوءاستفاده‌های مجرمانه از فناوری‌های نوین به‌شدت افزایش یافته است و نمونهٔ بارز این سوءاستفاده‌ها نیز ارتکاب جعل عمیق با استفاده از فناوری‌های مبتنی بر هوش مصنوعی است. به نظر می‌رسد قوانین کیفری موجود در ایران، به‌ویژه مقررات راجع به جرم جعل رایانه‌ای در قانون جرایم رایانه‌ای مصوب ۱۳۸۸، توان پاسـخ‌دهی کیفری متناسـب و کارآمد به پدیدهٔ جعل عمیق را ندارند. این نارسـایی هم از حیث ماهیتی و هم از حیث آثار و تبعات جعل عمیق مشـهود اسـت، چراکه جعل عمیق در مقایسـه با جعل رایانه‌ای، پیچیدگی‌های فنی بیشـتری دارد و اساساً تغییرات و تحریفاتـی که در جعل عمیق رخ می‌دهند و قابلیـت «باورپذیری»[1] داده‌های صوتی و تصویریِ حاصـل از ارتـکاب جعل عمیق، به مراتب از داده‌های صوتی و تصویری ناشـی از ارتکاب جعل رایانه‌ای، بیشـتر اسـت. دقیقاً همین قابلیت اسـت که به فناوری هوش مصنوعی، ظرفیت مجرمانهٔ بالایی داده است.

جعـل رایانه‌ای آن‌گونه که در گفتمـان قانون‌گذار ایرانی در قانون جرایـم رایانه‌ای تجلی یافته است، بیشتر ناظر بر تغییر داده‌ها و یا تحریف آن‌ها است که چه بسا در بسیاری از موارد نیز با رفتار مختصـری (مثـل تغییر دندانهٔ عدد یک و تبدیل آن به عـدد دو) صورت می‌گیرد؛ حال آنکه در جعل عمیق، همان‌گونه که از ظاهر عنوان این پدیده نیز برمی‌آید، تغییرات و تحریفات صورت‌گرفته، بسیار شـدیدتر و پیچیده‌تر از تغییرات و تحریفات مورداشـاره در جعل رایانه‌ای است. بنابراین، تفاوت ماهوی میان جعل رایانه‌ای و جعل عمیق مبرهن اسـت. از سـوی دیگر، دامنهٔ تأثیرگذاری و قلمرو تبعـات حاصل از ارتکاب جعل عمیق نیز به مراتب بیشـتر از جعـل رایانه‌ای مقرر در قانون جرایم رایانه‌ای است. دامنهٔ این تبعات حتی ممکن است نظام اقتصادی و سیاسی کشور را در برگیرد و یا در مخاصمه‌ای مسلحانه، به شکست در برابر جبههٔ مقابل منتهی شود. بر این اساس، به نظر نگارندگان، جعل عمیق (دیپ فیک)، با هیچ‌یک از عناوین ظاهراً مشـابهی که در قانون جرایم رایانه‌ای به آن‌ها اشـاره شـده اسـت، انطباق ندارد و نمی‌توان آن را معادل این جرایم دانست. بنابراین این موضوع

1. Believability

لزوم روزآمدشـــدن قوانین کیفری را با استانداردهای بین‌المللی و فراملی در راستای جرم‌انگاری و کیفرگذاری افتراقی نسبت به جعل عمیق در حقوق کیفری ایران توجیه و تبیین می‌کند.

نتیجه‌گیری

جعل عمیق یکی از مهم‌ترین جلوه‌های انتفاع مجرمانه از فناوری نوظهور هوش مصنوعی اســت. در جعــل عمیــق، صوت یا تصویر متعلق به دیگری با اســتفاده از ابزارهای مبتنی بر فناوری هوش مصنوعی، به‌گونه‌ای دچار تغییر و تحریف می‌شــوند که نســخه‌ای در ظاهر، کاملاً مشــابه با نمونهٔ واقعی، اما در ماهیت، کاملاً متفاوت با آن تولید، ارائه و منتشــر می‌شــود. روشــن اســت که چنین سوءاســتفاده‌ای از فناوری هوش مصنوعی و چنین تغییــر و تحریفی در صوت یا تصویر متعلق به دیگری، افزون بر گمراه‌ســازی و فریب مخاطبان در واقعی پنداشــتن محتوای ارائه‌شده، می‌تواند پیامدهای زیان‌بار جدی از حیث تعرض به حریم خصوصی و حیثیت افراد به همراه داشته باشد.

علاوه بر آن، امروزه، پیامدهای منفی جعل عمیق صرفاً به حوزه‌های فردی محدود نمی‌شــود و حتی می‌تواند جنبه‌های امنیتی نیز به خود بگیرد. برای مثال، چنانچه صوت یا تصویر مقام عالی‌رتبهٔ سیاســی‌ای، موضوع جعل عمیق قرار بگیرد و نسخه‌ای جعلی از وی با ظاهری کاملاً مشابه، اما در واقع، کاملاً متفاوت با واقعیت ساخته و منتشر شود که در آن، او کشور همسایه را به جنگ یا تجاوز به تمامیت ارضی تهدید می‌کند، این امر می‌تواند با واقعی‌پنداشــتن محتوا از ســوی طرف مقابل، واکنش‌های نظامی یا امنیتی متقابل و بحران‌زا را در پی داشته باشد. همانند واقعه‌ای که در انتخابات اخیر ریاســت‌جمهوری آمریکا (رقابت بین جو بایدن و دونالد ترامپ)، شــاهد آن بودیم؛ صوت یا تصویــر نامزدهای انتخاباتی، موضوع سوءاســتفاده و جعل عمیق قــرار گیرد و کلیپ‌های صوتی و ویدئوهایی با محتوای تخریب یکدیگر یا اتهام‌افکنی نسبت به هم، منتشر شوند.

بر این اســاس، دامنه و قلمــرو آثار و پیامدهای منفی جعل عمیق بــه حوزه‌های فردی محدود نمی‌مانــد و گاه تبعــات امنیتی و نظامــی نیز به خود می‌گیرد. با توجه به این مســئله، امروزه، برخی کشــورها (از جمله چین یا آمریکا)، اقدام به جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق به‌مثابهٔ جرمــی فناورانه در فضای ســایبری و اســتفاده از ابزارهای تکنیکی کرده‌اند. بــا این حال، به نظر می‌رســد ضعف بزرگ نظام کیفری کشــور ما فقــدان جرم‌انگاری و کیفرگذاری افتراقی نســبت به جعــل عمیق اســت. با اینکه برخی رویکردها جعل عمیق را همچنــان همان جعل رایانه‌ای مذکور در قانــون جرایــم رایانه‌ای می‌پندارند، جرم‌انگاری و کیفرگــذاری افتراقی جعل عمیق می‌تواند به نحو مؤثرتری، مقابلهٔ کیفری با آن را تحقق بخشــد و از این رو، اکتفا به قواعد و احکام جرم جعل رایانه‌ای، کافی نخواهد بود.

همان‌گونه که گفته شد، به سبب ماهیت پیچیدهٔ جعل عمیق، به نظر می‌رسد لزوم و الزامی به یکسان‌انگاری آن با جعل رایانه‌ای وجود ندارد. در واقع، رویکرد منطقی‌تر آن است که جعل عمیق، به‌منزلهٔ حالت پیچیده‌تری از جعل رایانه‌ای، موضوع جرم‌انگاری و کیفرگذاری افتراقی قرار گیرد. این وضعیت در برخی کشورها، که جعل عمیق را در کنار جعل رایانه‌ای، جرم‌انگاری و کیفرگذاری افتراقی کرده‌اند، مشهود است. از جمله در چین و آمریکا، قانون‌گذار کیفری در کنار جعل‌های رایانه‌ایِ «عادی»، جعل‌های عمیق را نیز به‌صورت افتراقی و تشدیدیافته، جرم‌انگاری و کیفرگذاری کرده است.

بر این اساس، پیشنهاد می‌شود که ماده یا دست‌کم تبصرهٔ جداگانه‌ای در قانون جرایم رایانه‌ای، به جرم‌انگاری و کیفرگذاری افتراقی جعل عمیق اختصاص یابد. پیشنهاد نگارندگان این پژوهش افزودن یک تبصره به مادهٔ ۶ قانون جرایم رایانه‌ای با این مضمون است: «جعل عمیق عبارت است از دست‌کاری و تحریف داده‌های صوتی و تصویری به نحوی که این داده‌ها به‌صورت متفاوت با حالت اولیهٔ آن‌ها ساخته شوند و متضمن مطالب و مسائل کذب نسبت به اشخاص حقیقی یا حقوقی و برخلاف حقیقت باشند. ارتکاب عمدی و غیرمجاز آن به هر شکل و با استفاده از هر ابزاری، مستوجب تشدید مجازات حبس و جزای نقدی مقرر در این ماده به میزان دو درجه نسبت به مرتکب است. در صورت ورود خسارت به اشخاص حقیقی یا حقوقیِ متضرر از این رفتار، جبران خسارت نیز موردحکم دادگاه قرار خواهد گرفت.» همچنین، این ویژه‌انگاری در شناسایی رفتار مجرمانهٔ جعل عمیق، موجبات کیفرگذاری افتراقی را در مورد این پدیده که نمود بارز آن، تشدید مجازات جاعل است، فراهم می‌کند. نکتهٔ مهم آن است که برخی حقوقدانانِ قائل به لزوم جرم‌انگاری خاص نسبت به جعل عمیق در مقایسه با جعل‌های رایانه‌ایِ عادی، ماهیت خاص جعل عمیق را که به مراتب از ماهیت جعل‌های رایانه‌ایِ عادی، پیچیده‌تر است و نیز آثار و تبعات ارتکاب جعل عمیق که در قیاس با جعل‌های رایانه‌ایِ عادی، شدیدتر است، دلیل این نگاه افتراقی می‌دانند و بر این مبنا، جرم‌انگاری مستقل جعل عمیق را ضرورت انکارناپذیری محسوب می‌کنند. به نظر می‌رسد نظام کیفری کشور ما از این رویکرد بی‌نیاز نیست.

منابع

۱. ابوذری، مهرنوش. (۱۴۰۱). **هوش مصنوعی و حقوق کیفری**، چاپ اول، تهران: میزان.

۲. احسان‌پور، سیدرضا و امی، احمد. (۱۴۰۱). **جرایم فناوری جعل عمیق از منظر فقه و حقوق کیفری**، فصلنامهٔ فقه جزای تطبیقی، دورهٔ ۲، شمارهٔ ۴.

۳. اکبری، عباس‌علی؛ آقاپور، علی و آقاپور، کمال. (۱۴۰۱). **تحلیل پدیدهٔ مجرمانه دیپ‌فیک‌ها (جعل‌های رایانه‌ای پیچیده) با نگاهی به سیاست کیفری ایران و چالش‌های حقوق بشری**، فصلنامهٔ کارآگاه، دورهٔ ۱۶، شمارهٔ ۵۹.

۴. آبید، محمد. (۱۳۹۹). **نگرش علمی و کاربردی به جعل رایانه‌ای**، چاپ اول، انتشارات پژوهشگاه قوهٔ قضائیه.
۵. ترنج مهرگان، رضا. (۱۳۹۷). **سیاست جنایی ایران در قبال جعل رایانه‌ای**، مجلهٔ آراء، دورهٔ ۲، شمارهٔ ۸.
۶. تقی‌پور، علی‌رضا و زرینه، مرتضی. (۱۳۹۴). **پاسخ کیفری در قبال هرزه‌نگاری سایبری در اسناد بین‌المللی و قانون جرایم رایانه‌ای**، مجلهٔ حقوقی دادگستری، سال ۸۱، شمارهٔ ۹۹.
۷. حبیب‌زاده، محمدجعفر و رحمانیان، حامد. (۱۳۹۰). **هرزه‌نگاری در حقوق کیفری ایران**، مجلهٔ حقوق دادگستری، دورهٔ ۷۵، شمارهٔ ۷۶.
۸. حیدری، علی‌مراد. (۱۳۹۰). **جعل رایانه‌ای در بستر تجارت الکترونیک**، مجلهٔ فقه و حقوق ارتباطات، دورهٔ ۲، شمارهٔ ۳.
۹. السان، مصطفی و دهستانی، سوور. (۱۴۰۱). **جنبه‌های حقوقی جعل عمیق**، مجلهٔ تحقیقات حقوقی (ویژه‌نامهٔ حقوق و فناوری)، شمارهٔ ۹۴.
۱۰. سلطانی‌فر، محمد؛ سلیمی، مریم و فلسفی، سیدغلامرضا. (۱۳۹۶). **اخبار جعلی و مهارت‌های مقابله با آن**، نشریهٔ رسانه، سال ۲۸، شمارهٔ ۳.
۱۱. شیری، عباس. (۱۴۰۱). **دیپ‌فیک یا همانندسازی صوتی یا تصویری غیرواقعی در حقوق کیفری**، مجلهٔ تحقیقات حقوقی (ویژه‌نامهٔ حقوق و فناوری)، شمارهٔ ۹۴.
۱۲. صالحی، محترم. (۱۳۹۷). **جعل رایانه‌ای**، پایان‌نامهٔ کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه تهران.
۱۳. صالحی، محمدخلیل و محترم قلاتی، ایمان. (۱۳۹۷). **گستره و ویژگی‌های داده‌های مجعول رایانه‌ای در حقوق ایران**، پژوهشنامهٔ حقوق کیفری، دورهٔ ۹، شمارهٔ ۱۷.
۱۴. علی ین، آرش. (۱۴۰۰). **جرم‌انگاری دیپ فیک‌ها از منظر تعهدات حقوق بشری دولت‌ها**، دوفصلنامهٔ بین‌المللی تحقیقات حقوق قضایی، دورهٔ ۲، شمارهٔ ۳.
۱۵. عطازاده، سعید و انصاری، جلال. (۱۳۹۸). **بازپژوهی مفهوم مسئولیت کیفری هوش مصنوعی در حقوق اسلام، ایران، آمریکا و آلمان**، مجلهٔ پژوهش تطبیقی حقوق اسلام و غرب، دورهٔ ۶، شمارهٔ ۴ (پیاپی ۲۲).
۱۶. فلسفی، سیدغلامرضا. (۱۳۹۸). **دیپ فیک؛ تیغی در کف زنگیان مست**، نشریهٔ رشد آموزش علوم اجتماعی، شمارهٔ ۸۲.
۱۷. قناد، فاطمه. (۱۳۹۷). **جعل در بستر فناوری‌های اطلاعات و ارتباطات**، چاپ اول، تهران: میزان.
۱۸. محمدی فردوئی، عطاءالله. (۱۳۹۷). **بررسی جزایی عناصر بزه جعل رایانه‌ای در حقوق ایران**، مجلهٔ قانون‌یار، دورهٔ ۲، شمارهٔ ۸.
۱۹. نوری، سیدمسعود. (۱۳۸۶). **پروتکل الحاقی به پیمان‌نامهٔ حقوق کودک دربارهٔ فروش، فحشا و هرزه‌نگاری کودکان و بررسی الحاق ایران به آن**، دوفصلنامه بین‌المللی حقوق بشر، دورهٔ ۲، شمارهٔ ۱.
۲۰. هالوی، گابریل. (۱۳۹۸). **مسئولیت کیفری ربات‌ها: هوش مصنوعی در قلمرو حقوق کیفری**، ترجمهٔ فرهاد شاهیده و طاهره قوانلو، چاپ اول، تهران: میزان.

21. Beebom, S. (2022). **10 Best Deep fake Apps and Websites You Can Try for Fun**, Beebom.
22. Brandon, J. (2018). **"Terrifying high-tech porn: Creepy 'deep fake' videos are on the rise"**, Fox News.
23. Bregler, C; Covell, M and Slaney, M. (2016). **Video Rewrite: Driving Visual Speech with Audio**, Proceedings of the 24th Annual Conference on Computer Graphics and Interactive Techniques.
24. Chesney, B and Citron, D. K. (2019). **"Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security"**, *California Law Review*, Vol. 107.
25. Filimowicz, M. (Ed.). (2022). **Deep Fakes: Algorithms and Society**, Routledge.
26. Gieseke, A. P. (2020). **The New Weapon of Choice: Law 's Current Inability to Properly Address**

Deep fake Pornography, *Vanderbilt Law Review*, Vol. 73.
27. Helmus, T. C. (2022). **Artificial Intelligence, Deepfakes, and Disinformation**, The RAND Corporation .
28. Lees, D. (2023). **Deep Fake Neighbor Wars: ITV's comedy shows how AI can transform popular culture**, The Conversation. Retrieved.
29. Mirsky, Y and Lee, W. (2020). **The Creation and Detection of Deep fakes: A Survey,** ACM Computing Surveys.
30. O'Donnell, N. (2021). **"Have we no decency? section 230 and the liability of social media companies for deep fake videos"**, *University of Illinois Law Review*, Vol. 2.
31. Perov, I. et al. (2020). **Deep Face Lab: A simple, flexible and extensible face swapping Framework**.
32. Reid, Sh. (2021). **"The Deep fake Dilemma: Reconciling Privacy and First Amendment Protections"**, *University of Pennsylvania Journal of Constitutional Law*, Vol. 23.
33. Zhukova, A. (2020). **7 Best Deep fake Apps and Websites**, Online Tech Tips, Retrieved, August.
34. Zollhöfer, M; Stamminger, M; Theobalt, Ch and Nießner, M. (2016). **Face 2 Face: Real-Time Face Capture and Reenactment of RGB Videos.**