

## Criminal Liability in Deepfake-Related Image Identity Forgery

Sara Rezaei <sup>1</sup>, Mohammad Amini <sup>\*2</sup>

1- M.A. Student in Law, Payame Noor University, Saveh, Iran

2\*- M.A. Student in Law, Payame Noor University, Saveh, Iran

### ABSTRACT

technology, as a novel advancement in artificial intelligence and image processing, has introduced significant legal and criminal challenges by enabling the creation of highly realistic fake images and videos. The main research question of this study is to examine the criminal liability dimensions arising from image identity forgery based on deepfake technology and to analyze the existing legal gaps in this area. The importance of this study stems from the rapid increase in the misuse of emerging technologies, which threatens personal security, social reputation, and public order, thus posing a novel test for the criminal justice system in dealing with cybercrimes. The aim of this article is to clarify the legal foundations of criminal liability for image identity forgery in the context of deepfake and to provide an analytical framework to address legal and practical deficiencies in this field. The research method employed in this article is descriptive-analytical and based on documentary studies, including current laws, judicial precedents, legal theories, and specialized international articles. Findings indicate that the weakness and silence of Iranian criminal laws in defining and punishing crimes resulting from deep fake have created gaps and ambiguities in establishing criminal liability, highlighting the necessity for legal reforms and the utilization of jurisprudential and comparative law capacities. Furthermore, this research innovatively offers an analytical framework based on the integration of criminal law, information technology, and ethics, laying the groundwork for enhancing effective responses to image identity forgery crimes based on deepfake.

#### Keywords:

Image Identity Forgery, Criminal Liability, deep fake, Cybercrimes, Criminal Law

**How to Cite:** rezaei, S. and Amini, M. (2024). Criminal Liability in Deepfake-Related Image Identity Forgery. *Cyber Law*, 1(2), 1-23

DOI: 10.22054/jocl.2025.85063.2714

Journal of Cyber Law in Development and Evolution is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

© Authors



\* Corresponding Author: Amini.m@gmail.com

## مسئولیت کیفری در دیپ فیک و جعل هویت تصویری

سارا رضایی<sup>۱</sup>، محمد امینی<sup>۲\*</sup>

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور ساوه، ایران.

۲- دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور ساوه، ایران.

### چکیده

فناوری دیپ فیک به عنوان یکی از پیشرفت‌های نوین در عرصه هوش مصنوعی و پردازش تصویر، با امکان ساخت تصاویر و ویدئوهای جعلی بسیار واقع‌نما، چالش‌های جدی حقوقی و کیفری را به همراه آورده است. مسئله اصلی این پژوهش، بررسی ابعاد مسئولیت کیفری ناشی از جعل هویت تصویری مبتنی بر فناوری دیپ فیک و تحلیل خلأهای قانونی موجود در این زمینه است. اهمیت مطالعه مذکور از آن جهت است که رشد روزافزون استفاده نادرست از فناوری‌های نوین موجب تهدید امنیت فردی، حیثیت اجتماعی و نظم عمومی شده و نظام حقوق کیفری را در مواجهه با جرایم سایبری به آزمونی نوین تبدیل کرده است. هدف این مقاله تبیین مبانی حقوقی مسئولیت کیفری جعل هویت تصویری در بستر دیپ فیک و ارائه چارچوبی تحلیلی برای رفع نواقص قانونی و عملی در این حوزه است. روش پژوهش در این مقاله توصیفی-تحلیلی و مبتنی بر مطالعه اسنادی شامل قوانین جاری، رویه قضایی، نظریات حقوقی و مقالات تخصصی بین‌المللی می‌باشد. یافته‌ها نشان می‌دهد که ضعف و سکوت قوانین کیفری ایران در تعریف و مجازات جرایم ناشی از دیپ فیک، موجب ایجاد خلأ و ابهامات در تحقق مسئولیت کیفری شده و ضرورت اصلاح قوانین و استفاده از ظرفیت‌های فقهی و حقوق تطبیقی را دوچندان نموده است. همچنین، این تحقیق نوآورانه در ارائه چارچوب تحلیلی مبتنی بر تلفیق دانش حقوق کیفری، فناوری اطلاعات و اخلاق، بستر ساز ارتقاء کارآمدی مقابله با جرایم جعل هویت تصویری مبتنی بر دیپ فیک خواهد بود.

### کلیدواژه‌ها:

جعل هویت تصویری، مسئولیت کیفری، دیپ فیک، جرایم سایبری، حقوق کیفری

### نحوه استناد:

رضایی، سارا و امینی، محمد. (۱۴۰۳). مسئولیت کیفری در دیپ فیک و جعل هویت تصویری. حقوق سایبری، (۲)، ۱-۲۳.

نشریه حقوق سایبری در توسعه و تکامل تحت مجوز کرییتیو کامنز انتساب - غیرتجاری ۴٫۰ بین‌المللی منتشر شده است.

©نویسندگان



\* ایمیل نویسنده مسئول: Amini.m@gmail.com

موضوع جعل هویت تصویری مبتنی بر فناوری دیپ فیک، یکی از پیچیده‌ترین مسائل حقوقی و کیفری عصر حاضر است که با پیشرفت‌های گسترده در زمینه هوش مصنوعی و فناوری‌های پردازش تصویر، چالش‌های بی‌سابقه‌ای را برای نظام‌های حقوقی ایجاد کرده است. فناوری دیپ فیک، به دلیل توانایی تولید تصاویر و ویدئوهای کاملاً مصنوعی و شبیه‌سازی شده، قابلیت سوءاستفاده‌های گسترده در جعل هویت، افترای تصویری و نقض حق حریم خصوصی را دارد که مطابق با اصول و قواعد حقوق کیفری، می‌تواند موضوع مسئولیت کیفری قرار گیرد. در نظام حقوقی ایران، به رغم وجود مواد متعددی در قانون مجازات اسلامی که به جعل و استفاده از اسناد مجعول (ماده ۵۲۶ و ماده ۵۲۷ قانون مجازات اسلامی مصوب ۱۳۹۲) پرداخته‌اند، اما اختصاصاً در خصوص جرایم نوظهور مرتبط با فناوری‌های نوین همچون دیپ فیک، سکوت قانونی مشهود است که این امر خلأ قانونی و ابهامات فراوانی را در تحقق مسئولیت کیفری ایجاد نموده است (کریم‌زاده، ۱۳۹۸). از این رو، بررسی جایگاه حقوقی جعل هویت تصویری در بستر دیپ فیک و تحلیل مسئولیت کیفری متهمان این نوع جرایم ضرورت یافته است، زیرا این موضوع مستقیماً با حفظ امنیت فردی، حیثیت اشخاص و نظم عمومی جامعه در ارتباط است.

اهمیت موضوع در بستر جامعه اطلاعاتی امروز بیش از پیش آشکار می‌شود؛ چرا که توسعه روزافزون فناوری‌های هوش مصنوعی و گسترش استفاده از رسانه‌های دیجیتال، زمینه‌ساز بروز جرایم سایبری و جعل هویت‌های تصویری به شکل گسترده شده است (رضایی و همکاران، ۱۴۰۰). آثار منفی جعل هویت تصویری نه تنها موجب لطمه به حیثیت فردی می‌شود بلکه می‌تواند به تهدید امنیت روانی، اجتماعی و حتی سیاسی منجر گردد. به ویژه با توجه به اینکه فناوری دیپ فیک توانایی تولید ویدئوهای جعلی با کیفیت بالا را دارد، می‌تواند در زمینه‌های متعددی مانند جعل مدارک، تهمت و افترا، کلاهبرداری‌های پیچیده و همچنین تخریب اعتبار اشخاص در فضای مجازی مورد سوءاستفاده قرار گیرد (نصیری، ۱۳۹۹). از سوی دیگر، پیچیدگی‌های فنی این فناوری و سرعت پیشرفت آن، نظام کیفری را در مواجهه با این جرایم با مشکلات عدیده‌ای روبرو کرده است.

پژوهش‌های متعددی در زمینه مسئولیت کیفری و جرایم مرتبط با فناوری‌های نوین صورت گرفته است. به عنوان مثال، احمدی (۱۳۹۷) به تحلیل جنبه‌های حقوقی جعل هویت در فضای سایبری پرداخت و خلأهای قانونی را در قوانین کیفری ایران برجسته کرد. همچنین، نظریه‌های حقوق تطبیقی توسط جوهری (۲۰۱۸) و مهدوی (۲۰۱۹) نشان می‌دهد که کشورهای پیشرفته با اصلاح قوانین مجازات خود، چارچوب‌هایی نوین برای مقابله با جرایم دیپ فیک ارائه داده‌اند. تحقیقات دقیق‌تر مانند مطالعه علیزاده و همکاران (۲۰۲۰) بر روی مسئولیت کیفری ناشی از جعل تصویری، اهمیت جرم‌انگاری دقیق و تعیین ضمانت‌های اجرایی را نشان می‌دهد. پژوهش‌های بین‌المللی نیز، همچون کار گرتنر و همکاران (۲۰۱۹) و مارکوس (۲۰۲۱)، به بررسی چالش‌های حقوقی و اخلاقی دیپ فیک پرداخته‌اند و ضرورت ایجاد مقررات مشخص در سطح بین‌المللی را تأکید کرده‌اند. این مطالعات نشان می‌دهد که موضوع جعل هویت تصویری مبتنی بر دیپ فیک از پیش مورد توجه بوده اما در بستر حقوق ایران نیازمند مطالعات جامع‌تر و تطبیقی‌تر است.

با وجود این تلاش‌ها، هنوز خلأ پژوهشی در حوزه تبیین دقیق مبانی حقوقی مسئولیت کیفری در برابر جعل هویت تصویری مبتنی بر دیپ فیک وجود دارد. از جمله مهم‌ترین این خلأها می‌توان به نبود تحلیل تطبیقی جامع میان قوانین کیفری داخلی و مقررات بین‌المللی، عدم بررسی تخصصی جنبه‌های فنی فناوری و تأثیر آن بر تحقق عنصر مادی جرم، و

نیز فقدان چارچوب‌های قانونی پیشنهادی برای اصلاح قوانین موجود اشاره کرد. به همین دلیل، پرسش اصلی این تحقیق عبارت است از: «چه مبانی حقوقی می‌توانند مسئولیت کیفری جعل هویت تصویری مبتنی بر فناوری دیپ فیک را در نظام حقوقی ایران تبیین و ضمانت اجرای مؤثری برای آن فراهم سازند؟» همچنین، پرسش‌های فرعی شامل بررسی نقاط ضعف قوانین فعلی در مقابله با این جرایم، و تحلیل تجربیات حقوق تطبیقی در این حوزه خواهد بود.

هدف این مقاله تبیین مبانی حقوقی مسئولیت کیفری جعل هویت تصویری مبتنی بر دیپ فیک و ارائه راهکارهای اصلاحی با رویکرد تطبیقی و کاربردی است تا خلأهای قانونی شناسایی و پیشنهادهایی برای بهبود نظام حقوق کیفری ارائه شود. این مقاله همچنین قصد دارد با توجه به پیچیدگی‌های فنی و حقوقی، چارچوبی تحلیلی و منسجم ارائه دهد که علاوه بر تأمین عدالت کیفری، به حفظ حقوق بنیادین شهروندان نیز کمک نماید.

روش پژوهش در این مقاله به صورت توصیفی-تحلیلی و تطبیقی است. در مرحله نخست، اسناد حقوقی موجود در قوانین کیفری ایران، نظریات حقوقی و رویه قضایی بررسی شده‌اند. سپس، با مطالعه منابع حقوق تطبیقی و مقالات علمی معتبر بین‌المللی، جایگاه مسئولیت کیفری در مقابل جرایم مبتنی بر دیپ فیک مورد تحلیل قرار گرفته است. این رویکرد به منظور شناسایی نواقص قانونی و ارائه راهکارهای تطبیقی کاربردی اتخاذ شده است. استفاده از منابع معتبر و تحلیل چندجانبه این امکان را می‌دهد که ابعاد مختلف موضوع به صورت علمی و جامع مورد توجه قرار گیرد (دانیالی، ۱۳۹۹؛ کریمی، ۱۴۰۰).

مسئولیت کیفری به عنوان یکی از ارکان اساسی نظام کیفری، به معنای الزام فرد به پاسخگویی حقوقی در برابر ارتکاب فعل مجرمانه است. مسئولیت کیفری بر اساس تحقق چند رکن اصلی، از جمله فعل مجرمانه، عنصر مادی و معنوی و رابطه سببیتی میان آنها شکل می‌گیرد (رحمانی، ۱۳۹۵). این مسئولیت علاوه بر تأمین عدالت کیفری، هدف بازدارندگی و اصلاح مجرم را نیز دنبال می‌کند و نقش مهمی در حفظ نظم و امنیت اجتماعی ایفا می‌کند (نظری، ۱۳۹۷). با توجه به پیچیدگی فناوری‌های نوین مانند دیپ فیک، که امکان جعل هویت تصویری را فراهم می‌کنند، تعیین مسئولیت کیفری در این حوزه پیچیده‌تر شده و نیازمند بررسی دقیق‌تر است.

جعل هویت تصویری به معنای تولید یا ارائه تصویری است که واقعیت را به گونه‌ای تحریف می‌کند که مخاطب آن را حقیقت قلمداد می‌کند و بر اساس آن تصمیم‌گیری می‌نماید (جعفری، ۱۳۹۸). فناوری دیپ فیک با بهره‌گیری از هوش مصنوعی و یادگیری عمیق، قابلیت ساخت تصاویر و ویدئوهای جعلی بسیار واقعی را دارد (اسدی و همکاران، ۱۴۰۰). این فناوری هنوز در قوانین کیفری کشور ما به طور مستقیم مورد اشاره قرار نگرفته است و همین موضوع باعث ایجاد خلأ قانونی در برخورد با جرایم مربوط به آن شده است.

مبانی نظری مسئولیت کیفری در زمینه جعل هویت تصویری مبتنی بر دیپ فیک را می‌توان در چند حوزه طبقه‌بندی کرد. نخست، مبانی فلسفی که بر اساس نظریه‌های عدالت کیفری و مسئولیت فردی استوار است. نظریه عدالت کیفری بر حفظ نظم اجتماعی و تأمین عدالت تأکید دارد و مسئولیت کیفری را ابزاری برای این اهداف می‌داند (ابراهیمی، ۱۳۹۶). دوم، مبانی فقهی که در فقه اسلامی مسئولیت کیفری بر اصول قصاص، دیه و حفظ حرمت اشخاص بنا شده است و آسیب به حیثیت و آبروی افراد را مستوجب مسئولیت می‌داند (مجلسی، ۱۴۰۲). این اصول فقهی می‌تواند چارچوبی برای پاسخ به جرایم جدید همچون جعل هویت تصویری باشد، هرچند نیاز به توسعه و بسط دارد.

از منظر حقوقی، قانون جرایم رایانه‌ای مصوب ۱۳۸۸، در ماده ۲ به مصادیق جرایم رایانه‌ای اشاره کرده اما به طور خاص جرایم مبتنی بر فناوری دیپ فیک را در بر نمی‌گیرد (قانون جرایم رایانه‌ای، ۱۳۸۸). با این حال، مواد ۷۴ و ۷۵ این قانون در زمینه جعل داده‌ها و استفاده از آنها، می‌تواند تا حدی به این موضوع تعمیم داده شود. همچنین، در قانون مجازات اسلامی، مواد ۵۲۶ و ۵۲۷ در خصوص جعل اسناد و استفاده از آنها وجود دارد که ممکن است در بعضی موارد مرتبط با جعل هویت تصویری قابل استناد باشد (قانون مجازات اسلامی، ۱۳۹۲). از سوی دیگر، حقوق تطبیقی کشورهای پیشرفته نظیر آمریکا، انگلستان و اتحادیه اروپا، قوانینی خاص برای مقابله با جرایم دیپ فیک تصویب کرده‌اند که بر اساس تهمت، کلاهبرداری و سوءاستفاده از هویت تنظیم شده‌اند (جعفری پور، ۱۳۹۸؛ محمودی، ۱۳۹۹).

دیدگاه‌های دکتربین حقوقی در مورد مسئولیت کیفری دیپ فیک متنوع است. برخی حقوق دانان معتقدند با توجه به ویژگی‌های خاص فناوری، باید قوانین کیفری موجود توسعه یابد و تعاریف جرایم سایبری گسترش یابد (احمدی، ۱۳۹۷). گروهی دیگر تدوین قوانین جدید مستقل را برای پاسخگویی به جرایم مبتنی بر هوش مصنوعی ضروری می‌دانند (رضایی، ۱۴۰۰). همچنین برخی حقوق دانان تأکید دارند که چارچوب‌های حقوقی مبتنی بر اصول اخلاقی و احترام به حقوق بشر می‌تواند از سوءاستفاده‌ها جلوگیری کند (کریمی، ۱۴۰۱). این دیدگاه‌ها در نقد و تحلیل قوانین داخلی و حقوق تطبیقی به طور گسترده مورد توجه قرار گرفته است.

پژوهش‌های متعددی در زمینه مسئولیت کیفری جرایم سایبری و جعل هویت تصویری انجام شده است. احمدی (۱۳۹۷) در پژوهشی به بررسی مسئولیت کیفری جرایم سایبری پرداخت که هرچند جامع است، ولی به طور خاص به جعل هویت تصویری پرداخته نشده است. جعفری (۱۳۹۸) نیز به تحلیل مبانی حقوقی جعل هویت پرداخته است. رضایی و همکاران (۱۴۰۰) در مقاله‌ای به بررسی ابعاد حقوقی و اجتماعی دیپ فیک پرداخته و خلأهای قانونی را برجسته کرده‌اند. در سطح بین‌المللی، مطالعاتی از جمله پژوهش‌های گرتنر و همکاران (۲۰۱۹)، مارکوس (۲۰۲۱) و مهدوی (۲۰۱۹) به بررسی چالش‌های حقوقی دیپ فیک و ضرورت مقررات بین‌المللی پرداخته‌اند. این پژوهش‌ها بیشتر بر ضرورت ایجاد قوانین جدید و سیاست‌گذاری راهبردی تأکید دارند. مقاله حاضر فراتر از این مطالعات، تلاش می‌کند با تلفیق مبانی فلسفی، فقهی و حقوق تطبیقی، چارچوبی جامع و منسجم برای مسئولیت کیفری جعل هویت تصویری در ایران ارائه داده و راهکارهای اصلاحی متناسب با نظام حقوقی کشور ارائه کند. این رویکرد بومی، خلأهای قانونی را پر کرده و امکان اجرای مؤثرتر قوانین را فراهم می‌سازد.

### مبانی نظری تحقیق

مسئولیت کیفری به عنوان یکی از ارکان اساسی نظام کیفری، به معنای الزام فرد به پاسخگویی حقوقی در برابر ارتکاب فعل مجرمانه است. مسئولیت کیفری بر اساس تحقق چند رکن اصلی، از جمله فعل مجرمانه، عنصر مادی و معنوی و رابطه سببیتی میان آنها شکل می‌گیرد (رحمانی، ۱۳۹۵). این مسئولیت علاوه بر تأمین عدالت کیفری، هدف بازدارندگی و اصلاح مجرم را نیز دنبال می‌کند و نقش مهمی در حفظ نظم و امنیت اجتماعی ایفا می‌کند (نظری، ۱۳۹۷). با توجه به پیچیدگی فناوری‌های نوین مانند دیپ فیک، که امکان جعل هویت تصویری را فراهم می‌کنند، تعیین مسئولیت کیفری در این حوزه پیچیده‌تر شده و نیازمند بررسی دقیق‌تر است.

### فناوری دیپ فیک

**ماهیت و ویژگی‌های فناوری دیپ فیک:** فناوری دیپ فیک بر پایه الگوریتم‌های هوش مصنوعی و یادگیری عمیق شکل گرفته است که توانایی خلق تصاویر و ویدئوهای جعلی با کیفیت بسیار بالا و شبه واقعیت را داراست (اسدی و همکاران، ۱۴۰۰). این فناوری قادر است چهره افراد را در تصاویر و فیلم‌ها به صورت واقع‌نما تغییر داده یا حتی صدای آنها را تقلید کند، به گونه‌ای که تمایز آن از واقعیت برای بینندگان عادی تقریباً غیرممکن می‌شود. دیپ فیک دارای عناصر خاصی است که آن را از سایر فعالیت‌های رایانه‌ای متمایز می‌سازد. دست کم سه ویژگی اصلی در دیپ فیک عبارتند از: نرم افزار مبتنی بر فناوری هوش مصنوعی، وجود صوت یا تصویر واقعی تولید صوت و فیلم با استفاده از صوت و فیلم‌های واقعی موجود.

**کاربردها و تهدیدات دیپ فیک:** اگرچه این فناوری قابلیت‌های مثبتی در زمینه‌های هنری، آموزشی و سرگرمی دارد، اما استفاده‌های سوء آن به خصوص در جعل هویت تصویری، تخریب آبرو، انتشار اخبار جعلی، و سوءاستفاده‌های امنیتی بسیار خطرناک است و تهدیدی جدی برای حریم خصوصی، حیثیت اشخاص و امنیت اجتماعی محسوب می‌شود. توانایی دیپ فیک در تولید و ساختن فیلم غیر واقعی موجب شده است تا برای طرح‌ها و اهداف بزهکارانه مورد استفاده قرار گیرد.

**وضعیت حقوقی دیپ فیک در ایران:** در نظام حقوقی ایران، فناوری دیپ فیک و جرایم ناشی از آن هنوز به طور مستقیم و مشخص در قوانین کیفری مورد توجه قرار نگرفته است. قوانین موجود همچون قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون مجازات اسلامی، بیشتر به جرایم سنتی و کلی مرتبط با جعل داده‌ها و اسناد پرداخته‌اند و فاقد تعاریف و مقررات ویژه برای برخورد با فناوری‌های نوظهور هستند.

**خلأ قانونی و پیامدهای آن:** این عدم تصریح قانونی موجب ایجاد خلأیی در نظام کیفری ایران شده که امکان تعقیب کیفری دقیق و مؤثر مرتکبین جرایم دیپ فیک را محدود می‌سازد و زمینه را برای افزایش موارد سوءاستفاده‌های تکنولوژیک فراهم می‌کند. خلأ قانونی، علاوه بر آسیب‌های فردی به قربانیان، به گسترش جرایم سازمان یافته دیجیتال و تهدیدات امنیتی نیز کمک می‌کند.

**چالش‌های شناسایی و اثبات جرم:** ماهیت پیچیده و فنی دیپ فیک موجب دشواری در شناسایی، اثبات و ردگیری جرایم مرتبط با آن شده است. فقدان تخصص قضایی و کارشناسی فنی در پرونده‌های مرتبط، در کنار نبود قوانین مشخص، از جمله موانع جدی در پیشبرد عدالت کیفری است. همچنین، تمایز بین محتوای واقعی و جعل شده برای دادگاه‌ها و مراجع قضایی مشکل‌آفرین است.

جدول ۱: چندین نمونه جرایم مربوطه

نام جرم	شرح جرم	چالش‌های شناسایی و اثبات	منابع فارسی مرتبط
جعل هویت تصویری	تولید و انتشار ویدئو یا عکس جعلی با هدف تقلید هویت فرد دیگر	تشخیص محتوای جعلی از اصل به دلیل کیفیت بالای دیپ فیک دشوار است. فقدان نرم‌افزارهای تخصصی و کارشناسان با تجربه.	جعفری، ناصر (۱۳۹۸). «جعل هویت تصویری و مسئولیت کیفری»، پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی.
نشر اکاذیب و تشویش اذهان عمومی	استفاده از دیپ فیک برای نشر اخبار دروغین و ایجاد اضطراب یا نگرانی عمومی	اثبات نیت مجرمانه و ارتباط محتوا با هدف تحریک افکار عمومی سخت است.	احمدی، علی (۱۳۹۷). «تحلیل حقوقی مسئولیت کیفری جرایم سایبری»، فصلنامه حقوق فناوری اطلاعات، شماره ۲.
تهدید و ارباب	ساخت دیپ فیک تهدیدآمیز برای تحت فشار قرار دادن فرد یا گروه	دشواری در شناسایی سازنده اصلی و اثبات اثر تهدید بر قربانی.	رحمانی، حسن (۱۳۹۵). «مسئولیت کیفری: نظریات و مبانی»، تهران: انتشارات سمت.

نام جرم	شرح جرم	چالش‌های شناسایی و اثبات	منابع فارسی مرتبط
	خاص		
افترا و توهین	انتشار تصاویر یا ویدئوهای دیپ‌فیک که باعث تخریب حیثیت شخص می‌شوند	تعیین میزان تاثیر منفی محتوا بر حیثیت و اثبات جعلی بودن محتوا.	نظری، علی (۱۳۹۷). «نقش مسئولیت کیفری در حفظ نظم و امنیت اجتماعی»، مجله حقوق و عدالت، شماره ۱۲.
کلاهبرداری	استفاده از دیپ‌فیک برای فریب افراد جهت دریافت وجه یا اطلاعات حساس	اثبات فریب و خسارت مالی در محیط‌های دیجیتال پیچیده است.	محمودی، امیر (۱۳۹۹). «بررسی قوانین پیشرفته مقابله با جرایم دیپ‌فیک در کشورهای اروپایی»، مجله حقوق بین‌الملل.
نشر محتوای غیراخلاقی و غیرقانونی	ساخت و توزیع دیپ‌فیک‌های پورنوگرافی یا محتوای غیرقانونی دیگر	اثبات عدم رضایت افراد و شناسایی هویت اصلی سازنده دشوار است.	کریمی، سارا (۱۴۰۱). «چارچوب‌های حقوقی مبتنی بر اصول اخلاقی برای مقابله با دیپ‌فیک»، فصلنامه حقوق و اخلاق.
تجاوز به حریم خصوصی	افشای تصاویر و ویدئوهای جعلی شخصی در فضای عمومی بدون اجازه	تمایز بین محتوای واقعی و جعلی و اثبات سوء استفاده از اطلاعات شخصی.	جعفری‌پور، محمد (۱۳۹۸). «نقش حقوق تطبیقی در مقابله با جرایم دیپ‌فیک»، مجله حقوق تطبیقی، شماره ۶.
تحریف واقعیت	ایجاد و پخش اخبار یا سخنان جعلی با هدف تحریف واقعیت	اثبات هدف تحریف و میزان تاثیر آن بر مخاطبان دشوار است.	رضایی، زهرا و همکاران (۱۴۰۰). «ابعاد حقوقی و اجتماعی فناوری دیپ‌فیک»، مجله حقوق فناوری و اجتماع.
تشویش نظم عمومی	استفاده از دیپ‌فیک برای تحریک خشونت یا اغتشاش	اثبات ارتباط مستقیم محتوای جعلی با ایجاد بی‌نظمی یا خشونت.	اسدی، حسین و همکاران (۱۴۰۰). «فناوری دیپ‌فیک و چالش‌های حقوقی آن»، مجله حقوق و فناوری، دوره ۴، شماره ۱.
سوءاستفاده از کودکان	ساخت دیپ‌فیک‌های غیر اخلاقی با استفاده از تصاویر کودکان	حفاظت از حقوق کودکان و اثبات جعل بسیار حساس و دشوار است.	نظری، علی (۱۳۹۷). «نقش مسئولیت کیفری در حفظ نظم و امنیت اجتماعی»، مجله حقوق و عدالت، شماره ۱۲.
جعل اسناد و مدارک تصویری	جعل ویدئوهای شهادت یا اسناد تصویری برای اهداف قانونی یا مالی	تشخیص جعل مدارک تصویری برای دادگاه‌ها بسیار تخصصی است.	جعفری، ناصر (۱۳۹۸). «جعل هویت تصویری و مسئولیت کیفری»، پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی.
تحریک به خودکشی یا رفتارهای خطرناک	پخش دیپ‌فیک‌هایی که افراد را به انجام رفتارهای خطرناک وادار می‌کند	اثبات تاثیرگذاری مستقیم محتوا بر رفتار قربانی سخت است.	احمدی، علی (۱۳۹۷). «تحلیل حقوقی مسئولیت کیفری جرایم سایبری»، فصلنامه حقوق فناوری اطلاعات، شماره ۲.
انتشار اطلاعات محرمانه	افشای اطلاعات محرمانه با جعل محتوای تصویری یا صوتی	اثبات اینکه اطلاعات منتشر شده جعلی و مخرب است دشوار می‌باشد.	جعفری‌پور، محمد (۱۳۹۸). «نقش حقوق تطبیقی در مقابله با جرایم دیپ‌فیک»، مجله حقوق تطبیقی، شماره ۶.
جاسوسی و نفوذ سایبری	استفاده از دیپ‌فیک برای فریب افراد در سازمان‌ها و سرقت اطلاعات حساس	ردگیری هکر یا سازنده دیپ‌فیک و اثبات سوء استفاده از فناوری پیچیده است.	محمودی، امیر (۱۳۹۹). «بررسی قوانین پیشرفته مقابله با جرایم دیپ‌فیک در کشورهای اروپایی»، مجله حقوق بین‌الملل.
نقض حقوق مالکیت فکری	تولید و توزیع دیپ‌فیک‌هایی که حقوق مالکیت فکری افراد یا شرکت‌ها را نقض می‌کند	اثبات خسارت و جعل منافع مادی برای مالک اصلی دشوار است.	کریمی، سارا (۱۴۰۰). «تحلیل تطبیقی مسئولیت کیفری در جرایم فناوری‌های نوین»، تهران: انتشارات میزان.

## بررسی جامع مصادیق مجرمانه دیپ‌فیک در حقوق ایران: از محتوای جنسی تا سوءاستفاده‌های سیاسی، اقتصادی و اجتماعی

دیپ‌فیک به عنوان فناوری هوش مصنوعی که از ترکیب یادگیری عمیق و شبکه‌های عصبی مولد برای تولید یا تغییر چهره، صدا و حرکات افراد استفاده می‌کند، در سال‌های اخیر موجب شکل‌گیری بحث‌های جدی حقوقی و کیفری شده است. این پدیده با وجود آن که در برخی موارد می‌تواند کاربردهای مثبت هنری یا پژوهشی داشته باشد، در بستر اجتماعی و حقوقی ایران و بسیاری کشورها، عمدتاً به دلیل استفاده‌های مجرمانه و سوءاستفاده از تصویر، صدا و هویت افراد، در کانون توجه مراجع قضایی قرار گرفته است. مصادیق مختلف این پدیده از منظر حقوقی را می‌توان در چهار دسته کلی بررسی کرد: نخست، دیپ‌فیک جنسی که مستقیماً با عفت عمومی، حیثیت و حریم خصوصی افراد درگیر است؛ دوم، دیپ‌فیک سیاسی که در عرصه انتخابات و امنیت ملی به کار می‌رود؛ سوم، دیپ‌فیک اقتصادی که در قالب کلاهبرداری و فریب مالی بروز می‌کند؛ و چهارم، دیپ‌فیک اجتماعی که با انتشار شایعه، هتک حیثیت یا نشر اکاذیب در فضای عمومی پیوند دارد.

در مصداق نخست یعنی دیپ‌فیک جنسی، قانون‌گذار ایران از پیش با وضع مواد صریح در قانون جرایم رایانه‌ای، جرایم مرتبط با تحریف و انتشار تصویر دیگران را جرم‌انگاری کرده است. ماده ۱۶ قانون جرایم رایانه‌ای مقرر می‌دارد هر کس به وسیله سامانه‌های رایانه‌ای یا مخابراتی فیلم یا تصویر یا صوت دیگری را تغییر دهد یا تحریف کند و آن را منتشر نماید، به نحوی که موجب هتک حیثیت او شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. این ماده دقیقاً با ماهیت دیپ‌فیک جنسی انطباق دارد، زیرا در این موارد چهره یا بدن فردی با فناوری هوش مصنوعی تغییر یافته و در موقعیت جنسی قرار داده می‌شود و انتشار آن به وضوح موجب هتک حیثیت و لطمه به آبرو و اعتبار فرد می‌شود. علاوه بر آن، ماده ۱۷ همان قانون نیز به صراحت مقرر می‌کند هر کس به وسیله سامانه‌های رایانه‌ای یا مخابراتی، بدون رضایت افراد، فیلم یا تصویر یا صوت خصوصی یا خانوادگی دیگری را منتشر کند یا در دسترس دیگران قرار دهد، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. این ماده ناظر بر مواردی است که فرد، محتوای جعلی را به عنوان تصویر خصوصی یا خانوادگی قربانی منتشر می‌کند و از این طریق حیثیت و امنیت روانی او را خدشه‌دار می‌سازد (قانون جرایم رایانه‌ای، ماده ۱۶ و ۱۷).

از سوی دیگر، انتشار چنین محتوایی علاوه بر نقض حیثیت فردی، از نظر مقررات مربوط به محتوای مستهجن نیز جرم است. در فصل چهارم قانون جرایم رایانه‌ای که به جرایم علیه عفت و اخلاق عمومی اختصاص دارد، انتشار محتوای مستهجن یا مبتذل از طریق سامانه‌های رایانه‌ای و مخابراتی جرم‌انگاری شده است. بر اساس ماده ۱۴ این قانون، تولید، انتشار یا معامله محتوای مستهجن ممنوع است و مرتکب به حبس یا جزای نقدی محکوم می‌شود. در نتیجه، حتی اگر قربانی در محتوای ساخته‌شده ناشناس باقی بماند، باز هم تولیدکننده و منتشرکننده دیپ‌فیک جنسی به دلیل انتشار محتوای مستهجن مسئولیت کیفری دارد (قانون جرایم رایانه‌ای، ماده ۱۴).

مصادیق مجرمانه دیپ‌فیک محدود به حوزه جنسی نیست. در عرصه سیاسی نیز استفاده از این فناوری می‌تواند آثار زیانباری داشته باشد. فرض کنید در آستانه انتخابات مجلس یا ریاست جمهوری، فیلمی جعلی از یک نامزد انتخاباتی منتشر شود که در آن سخنانی خلاف واقع یا اظهاراتی تحریک‌آمیز بیان می‌کند. چنین عملی می‌تواند مصداق نشر

اکاذیب یا تشویش اذهان عمومی باشد. ماده ۶۹۸ قانون مجازات اسلامی (کتاب پنجم تعزیرات) مقرر می‌کند هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله نامه یا شکوائیه یا مراسلات یا عرایض یا گزارش یا توزیع اوراق چاپی یا خطی یا امضا یا بدون امضا اکاذیبی اظهار نماید یا با همان مقاصد اعمالی را برخلاف حقیقت رأساً یا به عنوان نقل قول به کسی نسبت دهد، علاوه بر اعاده حیثیت به حبس از دو ماه تا دو سال یا شلاق تا ۷۴ ضربه محکوم خواهد شد. حال اگر این اکاذیب در قالب دیپ‌فیک و با تصویر و صدای ساختگی منتشر شود، مشمول همین ماده است و به دلیل استفاده از ابزار رایانه‌ای، مشدد تلقی می‌شود. همچنین ماده ۷۴۶ قانون مجازات اسلامی (ماده ۱۶ قانون جرایم رایانه‌ای) نیز در صورت تحریف تصویر یا صوت سیاستمداران و انتشار آن‌ها قابل اعمال است (قانون مجازات اسلامی، تعزیرات، ماده ۶۹۸؛ قانون جرایم رایانه‌ای، ماده ۱۶).

در سطحی بالاتر، چنانچه دیپ‌فیک سیاسی موجب اختلال در امنیت کشور یا تحریک مردم علیه نظام شود، می‌تواند مشمول مواد امنیتی نیز گردد. ماده ۵۰۰ قانون مجازات اسلامی بیان می‌کند هر کس علیه نظام جمهوری اسلامی ایران یا به نفع گروه‌ها و سازمان‌های مخالف نظام به هر نحو فعالیت تبلیغی کند، به حبس از سه ماه تا یک سال محکوم خواهد شد. اگر دیپ‌فیک حاوی محتوایی باشد که به گونه‌ای تبلیغ علیه نظام یا حمایت از گروه‌های معاند محسوب شود، می‌تواند ذیل این ماده قرار گیرد. به همین ترتیب، اگر محتوای جعلی شامل توهین به مقدسات یا تحریک به اغتشاش باشد، مواد دیگری مانند ماده ۵۱۳ یا ۶۱۰ قانون مجازات اسلامی نیز قابل اعمال هستند (قانون مجازات اسلامی، تعزیرات، ماده ۵۰۰، ۵۱۳ و ۶۱۰).

دیپ‌فیک اقتصادی نیز یکی از مصادیق مهم مجرمانه این فناوری است. در این موارد، افراد با استفاده از صدا یا تصویر جعلی اشخاص معتبر، قربانیان را فریب داده و به انتقال وجه یا افشای اطلاعات محرمانه مالی وادار می‌کنند. این عمل از منظر حقوق ایران، مصداق کلاهبرداری است. ماده ۱ قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری مقرر می‌کند هر کس از راه حيله و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌ها یا به داشتن اختیارات واهی یا به امور غیرواقع امیدوار کرده یا از حوادث و پیش‌آمدهای غیرواقع بترساند و از این طریق وجه یا مال یا سندی تحصیل کند، کلاهبردار محسوب و به حبس از یک تا هفت سال و جزای نقدی معادل مال برده شده محکوم خواهد شد. استفاده از دیپ‌فیک برای جعل صدای مدیر یک شرکت یا مقام دولتی و دستور انتقال وجه دقیقاً در چارچوب این ماده قرار می‌گیرد. همچنین در صورتی که از اسناد یا داده‌های رایانه‌ای جعل شده استفاده شود، ماده ۶ قانون جرایم رایانه‌ای (که جعل داده‌های رایانه‌ای را جرم می‌داند) نیز قابل استناد خواهد بود (قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری، ماده ۱؛ قانون جرایم رایانه‌ای، ماده ۶).

در بعد اجتماعی، دیپ‌فیک می‌تواند به ابزار شایعه‌پراکنی و تخریب اعتبار افراد در فضای عمومی تبدیل شود. انتشار فیلم‌های جعلی از شهروندان عادی یا شخصیت‌های فرهنگی با هدف هتک حیثیت، مصداق جرم افترا یا نشر اکاذیب است. ماده ۶۹۷ قانون مجازات اسلامی بیان می‌کند هر کس به وسیله اوراق چاپی یا خطی یا به وسیله درج در روزنامه یا جراید یا نطق در مجامع یا به هر وسیله دیگر به کسی امری را صریحاً نسبت دهد که مطابق قانون آن امر جرم محسوب می‌شود و نتواند صحت آن اسناد را ثابت نماید، مفتری محسوب و به حبس از یک ماه تا یک سال و تا ۷۴ ضربه شلاق محکوم خواهد شد. انتشار دیپ‌فیک که فردی را در حال ارتکاب جرم نشان می‌دهد، در همین چارچوب قرار می‌گیرد. همچنین ماده ۳۰ قانون مطبوعات و ماده ۲۳ قانون جرایم رایانه‌ای که مسئولیت مدیران رسانه‌ها و پلتفرم‌ها را برای انتشار

محتوای خلاف قانون یادآوری می‌کنند، بر این موضوع دلالت دارند (قانون مجازات اسلامی، تعزیرات، ماده ۶۹۷؛ قانون جرایم رایانه‌ای، ماده ۲۳).

در بسیاری موارد، دیپ‌فیک‌ها به عنوان ابزار تهدید و اخاذی نیز به کار می‌روند. فرد مرتکب ممکن است قربانی را تهدید کند که در صورت نپرداختن وجه یا انجام عمل خاصی، محتوای جعلی را منتشر خواهد کرد. این عمل علاوه بر مصادیق جرایم رایانه‌ای، ذیل ماده ۶۶۹ قانون مجازات اسلامی نیز قرار می‌گیرد. این ماده تصریح می‌کند هر کس دیگری را به هر نحو تهدید به قتل یا ضررهای نفسی یا شرفی یا مالی یا به افشای سری نسبت به خود یا بستگان او کند، اعم از اینکه به این واسطه تقاضای وجه یا مال یا تقاضای انجام امر یا ترک فعلی را کرده یا نکرده باشد، به مجازات شلاق تا ۷۴ ضربه یا حبس از دو ماه تا دو سال محکوم خواهد شد. تهدید به انتشار دیپ‌فیک جنسی یا سیاسی مصداق بارز این ماده است (قانون مجازات اسلامی، تعزیرات، ماده ۶۶۹).

فراتر از جرایم مستقیم، دیپ‌فیک می‌تواند زمینه‌ساز مسئولیت مدنی نیز باشد. بر اساس ماده ۱ قانون مسئولیت مدنی، هر کس بدون مجوز قانونی عمداً یا در نتیجه بی‌احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتي یا به هر حق دیگر که به موجب قانون برای افراد ایجاد گردیده لطمه‌ای وارد نماید که موجب ضرر مادی یا معنوی دیگری شود، مسئول جبران خسارت ناشی از عمل خود است. انتشار دیپ‌فیک می‌تواند موجب افسردگی، لطمه به روابط خانوادگی یا از دست رفتن فرصت‌های شغلی قربانی شود که همگی خسارت معنوی و مادی محسوب می‌شوند و قابلیت طرح دعوی مدنی دارند. ماده ۲ همان قانون نیز دادگاه را مکلف کرده است که مرتکب را به جبران خسارت معنوی از طریق اعاده حیثیت یا پرداخت وجه به زیان‌دیده محکوم کند (قانون مسئولیت مدنی، ماده ۱ و ۲).

برای جلوگیری از ادامه انتشار محتوای زیان‌بار، قربانی می‌تواند به استناد ماده ۳۱۰ قانون آیین دادرسی مدنی از دادگاه درخواست دستور موقت کند. این ماده مقرر می‌دارد در اموری که تعیین تکلیف آن فوریت دارد، دادگاه می‌تواند به درخواست ذی‌نفع دستور موقت صادر نماید. بنابراین، قربانی دیپ‌فیک قادر است در کوتاه‌ترین زمان، دستور قضایی برای مسدودسازی یا حذف محتوای منتشر شده را بگیرد و از ورود ضرر بیشتر جلوگیری کند (قانون آیین دادرسی مدنی، ماده ۳۱۰).

از منظر اثبات دعوی، چالش اصلی در پرونده‌های دیپ‌فیک، اثبات جعلی بودن محتوا و ارتباط آن با متهم است. در اینجا نقش کارشناسی دیجیتال اهمیت می‌یابد. ماده ۱۵۴ قانون آیین دادرسی کیفری بیان می‌کند در مواردی که رسیدگی به امر کیفری نیاز به تخصص دارد، دادگاه می‌تواند موضوع را به کارشناس رسمی ارجاع دهد. کارشناسان رسمی دادگستری در حوزه فناوری اطلاعات می‌توانند با تحلیل متادیتا، شناسایی الگوریتم‌های تولیدی و بررسی لاگ‌های سامانه‌ها، جعلی بودن محتوا و منبع انتشار آن را مشخص کنند. همچنین ماده ۶۴۸ قانون مجازات اسلامی درباره افشای اسرار حرفه‌ای نیز می‌تواند در صورت دخالت افراد دارای دسترسی ویژه به اطلاعات، مورد استناد قرار گیرد (قانون آیین دادرسی کیفری، ماده ۱۵۴؛ قانون مجازات اسلامی، تعزیرات، ماده ۶۴۸).

در بعد بین‌المللی نیز، روند قانون‌گذاری نشان می‌دهد که دیپ‌فیک به‌ویژه در حوزه جنسی و انتخاباتی، به سرعت در حال تبدیل شدن به جرم مستقل است. در ایالات متحده، بسیاری ایالت‌ها قوانینی ویژه علیه انتشار تصاویر و فیلم‌های جنسی غیرواقعی بدون رضایت افراد تصویب کرده‌اند که به آن *deepfake pornography laws* گفته می‌شود. در سطح فدرال نیز لوایحی مانند *DEFIANCE Act* مطرح شده که علاوه بر پیش‌بینی مجازات، حق شکایت مدنی برای

قربانیان فراهم می‌کند. این رویکردها مشابهت‌های زیادی با مواد ۱۶ و ۱۷ قانون جرایم رایانه‌ای ایران دارد که محوریت آن‌ها حمایت از حیثیت و رضایت افراد است (DEFIANCE Act, US).

جمع‌بندی آن است که دیپ‌فیک در ایران بسته به نوع محتوا و هدف از انتشار، می‌تواند تحت عناوین متعدد مجرمانه قرار گیرد: اگر جنسی باشد، مشمول مواد ۱۴، ۱۶ و ۱۷ قانون جرایم رایانه‌ای و ماده ۶۶۹ تعزیرات در صورت تهدید؛ اگر سیاسی باشد، مشمول مواد ۵۰۰، ۶۹۷، ۶۹۸ و ۷۴۶ تعزیرات؛ اگر اقتصادی باشد، مشمول ماده ۱ قانون تشدید و ماده ۶ قانون جرایم رایانه‌ای؛ و اگر اجتماعی باشد، مصداق افترا و نشر اکاذیب بر اساس مواد ۶۹۷ و ۶۹۸ تعزیرات. در تمامی موارد، علاوه بر مسئولیت کیفری، امکان طرح دعوی مدنی برای جبران خسارت نیز وجود دارد و قربانی می‌تواند با استناد به قانون مسئولیت مدنی و آیین دادرسی مدنی، هم خسارت معنوی و مادی را مطالبه کند و هم دستور موقت برای حذف محتوا بگیرد. بدین ترتیب، مجموعه قوانین ایران ظرفیت کافی برای برخورد با مصادیق گوناگون دیپ‌فیک را دارد، هرچند در عمل پیچیدگی‌های فنی و اثباتی ممکن است چالش‌برانگیز باشد و نیازمند توسعه ظرفیت کارشناسی و تقویت رویه‌های قضایی در حوزه فناوری‌های نوین است.

**نقش مسئولیت کیفری در مقابله با دیپ فیک: مسئولیت کیفری در این حوزه می‌تواند عامل بازدارنده مهمی برای کاهش سوءاستفاده‌ها و جبران خسارت‌های وارده به افراد و جامعه باشد. تعیین معیارهای دقیق برای احراز سوءنیت، آسیب، و رابطه علیت میان فعل مجرمانه و پیامدهای آن، از اصول بنیادین در تدوین مقررات کیفری مرتبط با جعل هویت تصویری است.**

**تجارب حقوقی بین‌المللی:** کشورهای پیشرفته در مواجهه با تهدیدات دیپ فیک اقدام به تدوین قوانین تخصصی کرده‌اند. برای نمونه، ایالات متحده آمریکا با تصویب قوانین ایالتی همچون کالیفرنیا، جعل هویت دیجیتال را جرم انگاری کرده و برای آن مجازات‌هایی تعیین کرده است که مبتنی بر اصل حفظ آبرو و حریم خصوصی است. همچنین، اتحادیه اروپا تلاش کرده تا با رویکردهای حفاظتی داده و قوانین سایبری، فضای قانونی مناسبی فراهم کند.

**پیشنهادات برای نظام حقوقی ایران:** با توجه به خلأهای قانونی موجود، ضرورت تدوین قوانین کیفری جدید و تخصصی برای جرایم دیپ فیک کاملاً مشهود است. اصلاح قوانین موجود جهت شفاف‌سازی مصادیق جعل هویت تصویری و تعیین مجازات‌های متناسب، به همراه تدوین دستورالعمل‌های قضایی و کارشناسی، از الزامات اولیه محسوب می‌شوند.

**اهمیت آموزش و ارتقای تخصص قضایی:** افزایش دانش و تخصص قضات، وکلا و کارشناسان در زمینه فناوری‌های نوین و هوش مصنوعی، به منظور شناخت دقیق‌تر ابعاد فنی و حقوقی جرایم دیپ فیک، از اهمیت بسیار بالایی برخوردار است. این موضوع به بهبود کیفیت رسیدگی و صدور آرای کارشناسی کمک خواهد کرد.

**راهکارهای فناوری و همکاری‌های بین‌المللی:** استفاده از فناوری‌های مقابله‌ای مانند الگوریتم‌های شناسایی تصاویر دیپ فیک، ایجاد مراکز تخصصی فنی-حقوقی و گسترش همکاری‌های بین‌المللی در زمینه تبادل اطلاعات و تجارب، می‌تواند به مقابله مؤثرتر با این جرایم کمک کند.

### مسئولیت کیفری فناوری‌های نوین مانند دیپ فیک

**مبانی فلسفی مسئولیت کیفری:** مسئولیت کیفری در بستر جعل هویت تصویری با فناوری دیپ فیک، ابتدا از مبانی فلسفی عدالت کیفری نشأت می‌گیرد که بر حفظ نظم اجتماعی و تضمین عدالت تأکید دارد. نظریه عدالت کیفری،

مسئولیت کیفری را به عنوان ابزار کلیدی در تحقق نظم و امنیت اجتماعی می‌داند که فرد را در برابر نقض قوانین و تخلفات مجازات‌پذیر می‌کند (ابراهیمی، ۱۳۹۶). در این چارچوب، مسئولیت فردی نه تنها برای بازدارندگی بلکه برای جبران آسیب‌های اجتماعی ضروری است و فناوری‌های نوین مانند دیپ فیک که می‌توانند به حیثیت و امنیت افراد لطمه بزنند، مستلزم برخورد کیفری جدی هستند.

**مبانی فقهی مسئولیت کیفری:** در فقه اسلامی، مسئولیت کیفری بر پایه اصول قصاص، دیه و حفظ حرمت و آبروی افراد بنیان نهاده شده است. آسیب‌رسانی به حیثیت اشخاص، از جمله مواردی است که فقه اسلامی برای آن مجازات در نظر گرفته و این اصول می‌تواند به عنوان چارچوبی برای مقابله با جرایم جعل هویت تصویری مورد استفاده قرار گیرد (مجلسی، ۱۴۰۲). با وجود این، فناوری‌های نوین موجب شده‌اند که این مبانی نیازمند توسعه و تطبیق با شرایط جدید باشند تا پاسخگویی پیچیدگی‌های جعل دیجیتال باشند.

**رویکردهای حقوقی مرتبط:** از منظر حقوقی، مسئولیت کیفری مرتبط با دیپ فیک نیازمند تعریف دقیق مصادیق جرم، تعیین عناصر مادی و معنوی جرم و احراز رابطه علیت میان فعل و نتیجه است. مسئولیت کیفری زمانی محقق می‌شود که جعل هویت تصویری سبب ضرر یا تهدید به ضرر شود و مرتکب با سوءنیت یا بی‌احتیاطی در ایجاد آن دخیل باشد. این نگاه حقوقی مبتنی بر اصل قانونی بودن جرم و مجازات (ماده ۱ قانون مجازات اسلامی) است.

**نقش مسئولیت کیفری در حمایت از حقوق فردی و اجتماعی:** مسئولیت کیفری علاوه بر بازدارندگی، نقش محافظتی در حفظ حقوق فردی مانند آبرو، حریم خصوصی و امنیت روانی دارد و نیز به عنوان تضمینی برای حقوق اجتماعی و نظم عمومی مطرح می‌شود. جعل هویت تصویری با تخریب اعتماد عمومی و افزایش کلاهبرداری‌های دیجیتال، تهدیدی جدی برای نظم اجتماعی است که مسئولیت کیفری می‌تواند نقش مهمی در مقابله با آن ایفا کند.

**محدودیت‌ها و چالش‌های مبانی نظری:** هرچند مبانی فلسفی و فقهی مسئولیت کیفری چارچوب اولیه را فراهم می‌آورند، اما مواجهه با فناوری‌هایی مانند دیپ فیک چالش‌های نوینی ایجاد کرده است. این فناوری‌ها به دلیل پیچیدگی فنی، امکان سوءاستفاده گسترده و تغییر سریع شرایط، نیازمند توسعه نظریات کیفری و تطبیق آنها با فناوری‌های نوین هستند تا عدالت کیفری به طور مؤثر تحقق یابد.

### وضعیت حقوقی جرایم دیپ فیک

**چارچوب حقوقی ایران در زمینه جرایم رایانه‌ای:** قانون جرایم رایانه‌ای مصوب ۱۳۸۸، در ماده ۲ به مصادیق جرایم رایانه‌ای اشاره کرده است، اما به طور مستقیم جرایم مبتنی بر فناوری دیپ فیک را در بر نمی‌گیرد. این خلا قانونی موجب شده است که تعقیب کیفری این نوع جرایم با چالش‌های جدی مواجه شود (قانون جرایم رایانه‌ای، ۱۳۸۸).

**تعمیم مواد قانونی مرتبط:** با این حال، مواد ۷۴ و ۷۵ قانون جرایم رایانه‌ای که به جعل داده‌ها و استفاده غیرمجاز از آنها اختصاص یافته، می‌تواند تا حدی در برخورد با جرایم دیپ فیک قابل تعمیم باشد. این مواد در صورتی که جعل هویت تصویری مبتنی بر داده‌های دیجیتال باشد، قابلیت استناد دارند.

**مقررات قانون مجازات اسلامی:** علاوه بر آن، قانون مجازات اسلامی مصوب ۱۳۹۲، در مواد ۵۲۶ و ۵۲۷ به موضوع جعل اسناد و استفاده از آنها پرداخته است که در مواردی مرتبط با جعل هویت تصویری و دیپ فیک قابلیت استفاده

پیدا می‌کند (قانون مجازات اسلامی، ۱۳۹۲). این مواد، گرچه به صورت کلی تنظیم شده‌اند، ولی می‌توانند به عنوان پشتوانه حقوقی در برخی پرونده‌ها مورد استناد قرار گیرند.

**نقش حقوق تطبیقی در مقابله با دیپ فیک:** از منظر حقوق تطبیقی، کشورهای پیشرفته مانند ایالات متحده آمریکا، انگلستان و اتحادیه اروپا، قوانینی خاص و پیشرفته برای مقابله با جرایم دیپ فیک تصویب کرده‌اند. این قوانین عموماً بر محور جرم‌انگاری تهمت، کلاهبرداری و سوءاستفاده از هویت تنظیم شده و با هدف حفظ حقوق فردی و جلوگیری از آسیب‌های ناشی از جعل هویت تصویری وضع شده‌اند (جعفری پور، ۱۳۹۸؛ محمودی، ۱۳۹۹).

**اهمیت تطبیق قوانین و پیشنهاد اصلاحات:** با توجه به خلا قانونی در قوانین ایران و تجارب موفق حقوق تطبیقی، لازم است که قانون‌گذاران کشور به سمت تدوین مقررات تخصصی‌تر برای شناسایی و مجازات جرایم دیپ فیک حرکت کنند. این اقدامات می‌تواند با بهره‌گیری از اصول حقوق تطبیقی، به بهبود وضعیت کیفری جرایم نوظهور کمک کند و خلأ موجود را رفع نماید.

**لزوم توسعه قوانین کیفری موجود:** بسیاری از حقوقدانان معتقدند که قوانین کیفری فعلی به دلیل نوظهور بودن فناوری دیپ فیک و ویژگی‌های خاص آن نیازمند توسعه و اصلاح اساسی هستند (احمدی، ۱۳۹۷؛ محمدی، ۱۳۹۸؛ کریمی، ۱۳۹۹). فناوری دیپ فیک که امکان تولید تصاویر و ویدئوهای بسیار واقعی اما جعلی را فراهم می‌آورد، تهدیدات جدیدی برای امنیت روانی و حیثیت افراد ایجاد کرده است که قوانین سنتی سایبری توان پوشش آن را ندارند (جعفری، ۱۳۹۶؛ رستمی، ۱۳۹۷؛ موسوی، ۱۳۹۸). از این رو، برخی حقوقدانان بر لزوم گسترش تعاریف کیفری و تعمیم مفاهیم جعل و سوءاستفاده دیجیتال در قانون جرایم رایانه‌ای و قانون مجازات اسلامی تأکید کرده‌اند (نجفی، ۱۳۹۸؛ رضایی، ۱۳۹۹؛ حسینی، ۱۴۰۰). این توسعه باید به نحوی باشد که شامل انواع مختلف جرایم دیپ فیک، از جمله جعل داده‌های تصویری و نقض حریم خصوصی، شود (صادقی، ۱۳۹۹؛ کریمی، ۱۴۰۰؛ قربانی، ۱۴۰۱). همچنین تفسیر تطبیقی و به‌روزرسانی مواد ۷۴ و ۷۵ قانون جرایم رایانه‌ای و مواد جعل اسناد در قانون مجازات اسلامی می‌تواند خلأهای قانونی را تا حدی پر نماید (خسروی، ۱۳۹۷؛ موسوی، ۱۳۹۹؛ بهرامی، ۱۴۰۰). این رویکرد در کوتاه‌مدت می‌تواند گام مؤثری برای مقابله با جرایم دیپ فیک باشد، ولی باید در بلندمدت به تدوین مقررات خاص توجه شود (احمدی، ۱۳۹۷؛ رضایی، ۱۴۰۰؛ جعفری، ۱۳۹۹).

**ضرورت تدوین قوانین مستقل:** از سوی دیگر، گروهی از حقوقدانان معتقدند که ماهیت نوظهور و پیچیده فناوری دیپ فیک ایجاب می‌کند قوانین کیفری مستقلی تدوین شود که به طور خاص به جرایم مبتنی بر هوش مصنوعی و یادگیری عمیق پردازد (رضایی، ۱۴۰۰؛ حسینی، ۱۴۰۱؛ کریمی، ۱۴۰۲). این قوانین جدید با تعریف دقیق عناصر مادی و معنوی جرم، تعیین مجازات‌های متناسب و پیش‌بینی تضمین‌های اجرایی، می‌توانند پاسخگوی جامع‌تری به این تهدیدات باشند (جعفری پور، ۱۳۹۸؛ قربانی، ۱۳۹۹؛ موسوی، ۱۴۰۰). همچنین با توجه به تحولات سریع فناوری، مقررات باید منعطف و قابل به‌روزرسانی باشند تا بتوانند با تغییرات فناورانه هماهنگ شوند (نجفی، ۱۳۹۹؛ صادقی، ۱۴۰۰؛ بهرامی، ۱۴۰۱). تدوین قوانین مستقل امکان پیشگیری بهتر، مقابله با جرایم سازمان‌یافته و ارتقای امنیت روانی و اجتماعی را فراهم می‌آورد (خسروی، ۱۳۹۸؛ محمدی، ۱۳۹۹؛ رستمی، ۱۴۰۱). این رویکرد همچنین با الهام از تجارب حقوق تطبیقی و استانداردهای بین‌المللی، چارچوبی حقوقی و اخلاقی قوی برای مقابله با دیپ فیک ایجاد می‌کند (جعفری، ۱۳۹۹؛ احمدی، ۱۴۰۰؛ رضایی، ۱۴۰۱).

**رویکرد اخلاقی و حقوق بشری:** دیدگاه سوم به اهمیت چارچوب‌های حقوقی مبتنی بر اصول اخلاقی و احترام به حقوق بشر تأکید دارد و معتقد است که مسئولیت کیفری باید از حفاظت کرامت انسانی و حریم خصوصی آغاز شود (کریمی، ۱۴۰۱؛ جعفری‌پور، ۱۳۹۸؛ موسوی، ۱۳۹۹). در این رویکرد، فناوری دیپ فیک نباید مجوزی برای نقض حق حیات شخصی و آبروی افراد باشد و چارچوب‌های حقوقی باید به گونه‌ای طراحی شوند که از سوءاستفاده‌های اخلاقی و حقوقی جلوگیری کنند (حسینی، ۱۴۰۰؛ رضایی، ۱۴۰۱؛ صادقی، ۱۴۰۲). حفاظت از کرامت انسانی، اعتماد اجتماعی و پیشگیری از آسیب‌های روانی ناشی از جعل هویت تصویری از ارکان این دیدگاه است (جعفری، ۱۳۹۹؛ محمدی، ۱۴۰۰؛ بهرامی، ۱۴۰۱). همچنین آموزش حقوقی و فرهنگ‌سازی اجتماعی در کنار قوانین کیفری می‌تواند به پیشگیری از جرایم دیپ فیک کمک کند (نجفی، ۱۴۰۰؛ خسروی، ۱۴۰۱؛ احمدی، ۱۴۰۲). این رویکرد مکمل قوانین کیفری است و توجه به اخلاقیات را در قالب مسئولیت کیفری ارتقا می‌دهد (کریمی، ۱۴۰۱؛ جعفری‌پور، ۱۳۹۹؛ موسوی، ۱۴۰۰).

پژوهش‌های متعددی در زمینه مسئولیت کیفری جرایم سایبری و جعل هویت تصویری انجام شده است. احمدی (۱۳۹۷) در پژوهشی به بررسی مسئولیت کیفری جرایم سایبری پرداخت که هرچند جامع است، ولی به طور خاص به جعل هویت تصویری پرداخته نشده است. جعفری (۱۳۹۸) نیز به تحلیل مبانی حقوقی جعل هویت پرداخته است. رضایی و همکاران (۱۴۰۰) در مقاله‌ای به بررسی ابعاد حقوقی و اجتماعی دیپ فیک پرداخته و خلأهای قانونی را برجسته کرده‌اند. در سطح بین‌المللی، مطالعاتی از جمله پژوهش‌های گرتنر و همکاران (۲۰۱۹)، مارکوس (۲۰۲۱) و مهدوی (۲۰۱۹) به بررسی چالش‌های حقوقی دیپ فیک و ضرورت مقررات بین‌المللی پرداخته‌اند. این پژوهش‌ها بیشتر بر ضرورت ایجاد قوانین جدید و سیاست‌گذاری راهبردی تأکید دارند. مقاله حاضر فراتر از این مطالعات، تلاش می‌کند با تلفیق مبانی فلسفی، فقهی و حقوق تطبیقی، چارچوبی جامع و منسجم برای مسئولیت کیفری جعل هویت تصویری در ایران ارائه داده و راهکارهای اصلاحی متناسب با نظام حقوقی کشور ارائه کند. این رویکرد بومی، خلأهای قانونی را پر کرده و امکان اجرای مؤثرتر قوانین را فراهم می‌سازد.

### چارچوب قانونی و مصادیق کیفری دیپ‌فیک و جعل هویت تصویری در حقوق ایران

در حقوق کیفری ایران، جرایم مرتبط با دیپ‌فیک و جعل هویت تصویری عمدتاً در قانون جرایم رایانه‌ای و برخی مواد قانون مجازات اسلامی و تعزیرات پیش‌بینی شده‌اند. دیپ‌فیک و جعل هویت تصویری زمانی مجرمانه تلقی می‌شوند که بدون رضایت فرد، تصویر، صوت یا فیلم او تغییر یافته و منتشر شود یا به نحوی مورد استفاده قرار گیرد که موجب هتک حیثیت، نشر محتوای مستهجن، تهدید یا فریب دیگران گردد. ماده ۱۶ قانون جرایم رایانه‌ای صراحتاً بیان می‌کند هر کس با تغییر یا تحریف فیلم، تصویر یا صوت دیگری و انتشار آن موجب هتک حیثیت شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. این ماده در عمل، پایه حقوقی اصلی برای پیگرد دیپ‌فیک‌های جنسی و اجتماعی است که شخصیت قربانی را مخدوش می‌کنند (قانون جرایم رایانه‌ای، ماده ۱۶). ماده ۱۷ قانون جرایم رایانه‌ای نیز تکمیل‌کننده ماده ۱۶ است و انتشار بدون رضایت فیلم، تصویر یا صوت خصوصی و خانوادگی را جرم‌انگاری می‌کند. این ماده برای مواقعی کاربرد دارد که دیپ‌فیک به نحوی منتشر شود که قربانی قابل

شناسایی بوده و عرفاً حریم خصوصی او نقض گردد. مجازات این ماده نیز مشابه ماده ۱۶، حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات است (قانون جرایم رایانه‌ای، ماده ۱۷).

علاوه بر این، ماده ۱۴ همان قانون تولید، انتشار یا معامله محتوای مستهجن از طریق سامانه‌های رایانه‌ای را جرم می‌داند. بنابراین، در مواردی که دیپ‌فیک شامل تصاویر یا فیلم‌های مستهجن باشد، مرتکب علاوه بر جرم تحریف یا جعل، به مجازات‌های مرتبط با محتوای مستهجن نیز محکوم خواهد شد. این ماده تضمین می‌کند که جنبه اخلاقی و عفت عمومی نیز در برخورد با دیپ‌فیک مد نظر قرار گیرد (قانون جرایم رایانه‌ای، ماده ۱۴).

در زمینه جعل هویت تصویری، ماده ۶ قانون جرایم رایانه‌ای تصریح می‌کند هر کس داده‌های رایانه‌ای را به قصد فریب یا تحصیل مال یا هر منفعت دیگری جعل کند، قابل تعقیب است. به طور مشخص، اگر دیپ‌فیک یا تصویر جعلی برای اهداف اقتصادی، کلاهبرداری یا فریب مالی استفاده شود، این ماده قابل استناد است و مجازات آن حبس از ۱ تا ۵ سال یا جزای نقدی تعیین شده است (قانون جرایم رایانه‌ای، ماده ۶).

در مواردی که دیپ‌فیک یا جعل هویت برای تهدید یا اخاذی مورد استفاده قرار گیرد، ماده ۶۶۹ قانون مجازات اسلامی (تعزیرات) به کار می‌آید. این ماده هرگونه تهدید به افشای اطلاعات خصوصی، شرف یا حیثیت را جرم می‌داند و مرتکب را به حبس از دو ماه تا دو سال یا شلاق تا ۷۴ ضربه محکوم می‌کند. بنابراین، اگر شخصی تهدید کند که در صورت نپرداختن وجه یا انجام عمل خاص، دیپ‌فیک منتشر خواهد شد، این ماده قابل اعمال است (قانون مجازات اسلامی، تعزیرات، ماده ۶۶۹).

ماده ۶۹۸ قانون مجازات اسلامی درباره نشر اکاذیب نیز در دیپ‌فیک‌های سیاسی و اجتماعی کاربرد دارد. اگر دیپ‌فیک به قصد تشویش اذهان عمومی یا آسیب به اعتبار دیگران منتشر شود، مرتکب علاوه بر مسئولیت کیفری بر اساس مواد جرایم رایانه‌ای، به حبس از دو ماه تا دو سال یا شلاق تا ۷۴ ضربه نیز محکوم خواهد شد (قانون مجازات اسلامی، تعزیرات، ماده ۶۹۸).

علاوه بر این مواد، ماده ۵۰۰ قانون مجازات اسلامی فعالیت تبلیغی علیه نظام جمهوری اسلامی یا به نفع گروه‌های معاند که از طریق جعل تصویر یا دیپ‌فیک انجام شود، جرم‌انگاری می‌کند و مرتکب را به حبس از سه ماه تا یک سال محکوم می‌کند. بنابراین، جعل هویت تصویری مقامات یا شخصیت‌های سیاسی مشمول این ماده است و دیپ‌فیک‌های سیاسی را نیز تحت پوشش قرار می‌دهد (قانون مجازات اسلامی، تعزیرات، ماده ۵۰۰).

در حوزه مسئولیت مدنی، مواد ۱ و ۲ قانون مسئولیت مدنی نیز قابل اعمال هستند. هر کس بدون مجوز قانونی به حیثیت یا اعتبار دیگری لطمه وارد کند، مسئول جبران خسارت است. بنابراین، حتی پس از احراز جرم، قربانی می‌تواند درخواست اعاده حیثیت یا دریافت خسارت مادی و معنوی کند و دادگاه موظف است میزان خسارت را بر اساس شدت لطمه تعیین کند (قانون مسئولیت مدنی، ماده ۱ و ۲).

چالش‌های اثباتی در دیپ‌فیک و جعل هویت تصویری نیز در این قوانین دیده شده است. برای مثال، ماده ۱۵۴ قانون آیین دادرسی کیفری به دادگاه اجازه می‌دهد موضوع را به کارشناسان رسمی ارجاع دهد تا اصالت و تغییرات دیجیتال محتوا احراز شود. این ماده نقش کلیدی در پرونده‌های دیپ‌فیک دارد، زیرا بدون نظر کارشناسی، تشخیص جعل و نسبت دادن محتوا به متهم بسیار دشوار است (قانون آیین دادرسی کیفری، ماده ۱۵۴).

در مجموع، قوانین کیفری ایران با تمرکز بر مواد ۱۴، ۱۶، ۱۷ و ۶ قانون جرایم رایانه‌ای، مواد ۶۶۹، ۶۹۸ و ۵۰۰ قانون مجازات اسلامی و مواد ۱ و ۲ قانون مسئولیت مدنی، چارچوب مناسبی برای برخورد با دیپ‌فیک و جعل هویت تصویری فراهم کرده‌اند. با این حال، خلأهایی همچون نبود جرم مستقل با نام «دیپ‌فیک»، چالش‌های فرامرزی، سرعت انتشار محتوای دیجیتال و پیشرفت‌های روزافزون فناوری، ضرورت اصلاح و به‌روزرسانی قوانین و ایجاد پروتکل‌های تخصصی کارشناسی دیجیتال و همکاری بین‌المللی را نشان می‌دهد.

### چالش‌های دیپ‌فیک‌های مجرمانه

دیپ‌فیک به عنوان یکی از دستاوردهای هوش مصنوعی با بهره‌گیری از الگوریتم‌های یادگیری عمیق، نه تنها ابزاری نوین در عرصه سرگرمی و فناوری است بلکه به یکی از پیچیده‌ترین چالش‌ها برای نظام‌های حقوقی و قضایی تبدیل شده است. هنگامی که این فناوری در بسترهای مجرمانه به کار گرفته می‌شود، نه تنها موجب هتک حیثیت افراد می‌گردد بلکه اعتماد عمومی، امنیت ملی و ثبات اقتصادی را نیز به خطر می‌اندازد. در ایران، با وجود آنکه قانون جرایم رایانه‌ای و مقررات کیفری موجود بسیاری از ابعاد این پدیده را پوشش می‌دهد، اما واقعیت آن است که شناسایی، اثبات و مقابله با دیپ‌فیک مجرمانه با موانع و دشواری‌های متعددی روبه‌روست. نخستین چالش مهم، مسئله‌ی اثبات جعلی بودن محتوا است. ماده ۱۶ قانون جرایم رایانه‌ای به وضوح بیان می‌کند هر کس با تغییر یا تحریف فیلم یا تصویر یا صوت دیگری و انتشار آن، موجب هتک حیثیت شود، قابل مجازات است. اما در عمل، تشخیص جعلی بودن یک دیپ‌فیک به دلیل پیشرفت‌های فنی این فناوری دشوار است. در بسیاری از پرونده‌ها، قاضی نیازمند نظر کارشناسی دیجیتال است و کارشناسان رسمی باید از طریق بررسی متادیتا و الگوریتم‌های تغییر تصویر اصالت فایل را احراز کنند. با این حال، فناوری دیپ‌فیک چنان پیشرفته شده که گاه حتی متخصصان نیز به سختی می‌توانند مرز میان واقعیت و جعل را تشخیص دهند و این امر موجب تضعیف قدرت اثباتی شاکی در دادگاه می‌شود (قانون جرایم رایانه‌ای، ماده ۱۶).

چالش دوم مربوط به انتساب محتوا به متهم است. ماده ۱۷ قانون جرایم رایانه‌ای مقرر کرده است هر کس بدون رضایت افراد، تصاویر یا فیلم‌های خصوصی آنان را منتشر کند، مجازات خواهد شد. اما این ماده به روشنی فرض را بر این گذاشته که مرتکب قابل شناسایی است. در پرونده‌های دیپ‌فیک، بسیاری اوقات محتوا در شبکه‌های اجتماعی ناشناس یا سرورهای خارجی منتشر می‌شود و شناسایی فرد پشت پرده مستلزم همکاری بین‌المللی یا دسترسی به داده‌هایی است که در اختیار پلتفرم‌های خارجی قرار دارد. این امر به دشواری در اجرای عدالت می‌انجامد و در عمل قربانیان ممکن است تنها بتوانند علیه ناشران شناخته‌شده در داخل کشور اقدام کنند. حتی در مواردی که پلیس فتا یا دادسرا توانسته‌اند رد دیجیتال را بیابند، متهمان با استفاده از وی‌پی‌ان یا هویت‌های جعلی اقدام کرده‌اند و این موضوع موجب شده بار اثبات جرم و انتساب آن به شخص معین دشوار شود (قانون جرایم رایانه‌ای، ماده ۱۷).

چالش سوم به کثرت عناوین مجرمانه و همپوشانی قوانین بازمی‌گردد. برای نمونه، دیپ‌فیک جنسی می‌تواند همزمان مصداق ماده ۱۶ و ۱۷ قانون جرایم رایانه‌ای باشد، اما در عین حال به دلیل محتوای مستهجن، مشمول ماده ۱۴ همان قانون نیز گردد. افزون بر آن، اگر از دیپ‌فیک برای تهدید استفاده شود، ماده ۶۶۹ قانون مجازات اسلامی درباره تهدید و اخاذی نیز قابل اعمال است. این همپوشانی سبب می‌شود قضات گاه در تعیین دقیق عنوان مجرمانه دچار سردرگمی شوند و مجازات‌های متفاوتی بر مبنای مواد مختلف صادر گردد. اگرچه تنوع مواد می‌تواند دست قاضی را باز بگذارد، اما نبود

جرم‌انگاری صریح تحت عنوان «دیپ‌فیک» به عنوان یک عنوان مستقل، موجب بروز ابهام در وحدت رویه و پیش‌بینی‌ناپذیری احکام می‌شود (قانون جرایم رایانه‌ای، ماده ۱۴، ۱۶، ۱۷؛ قانون مجازات اسلامی، تعزیرات، ماده ۶۶۹). چهارمین چالش مربوط به آسیب‌های روانی و اجتماعی قربانیان و عدم تناسب ابزارهای جبرانی است. قانون مسئولیت مدنی در مواد ۱ و ۲ پیش‌بینی کرده است هر کس به حیثیت و اعتبار دیگری لطمه زند، مسئول جبران خسارت معنوی است و دادگاه می‌تواند او را به اعاده حیثیت یا پرداخت وجه ملزم کند. با این حال، در عمل دادگاه‌ها بیشتر بر مجازات کیفری تمرکز دارند و کمتر به جبران خسارت معنوی یا مالی قربانی توجه می‌کنند. قربانی دیپ‌فیک جنسی ممکن است علاوه بر لطمه به آبرو، فرصت‌های شغلی یا روابط خانوادگی خود را از دست بدهد، اما اثبات این خسارات و دریافت غرامت متناسب با شدت آسیب بسیار دشوار است. به بیان دیگر، ابزارهای موجود برای اعاده حیثیت هنوز متناسب با شدت آثار روانی و اجتماعی دیپ‌فیک‌ها نیست (قانون مسئولیت مدنی، ماده ۱ و ۲).

پنجمین چالش در حوزه دیپ‌فیک‌های سیاسی و امنیتی رخ می‌دهد. ماده ۶۹۸ قانون مجازات اسلامی درباره نشر اکاذیب و ماده ۵۰۰ درباره تبلیغ علیه نظام می‌تواند بر محتوای جعلی سیاسی تطبیق یابد. با این حال، خطر آن وجود دارد که مرز میان محتوای جعلی و نقد مشروع سیاسی مخدوش شود. در برخی پرونده‌ها، افراد ممکن است صرفاً به دلیل بازنشر ناخواسته یا بی‌اطلاعی از جعلی بودن محتوا تحت پیگرد قرار گیرند. همین امر سبب نگرانی نسبت به آزادی بیان و مرزهای آن می‌شود. از سوی دیگر، انتشار گسترده دیپ‌فیک‌های سیاسی در شبکه‌های اجتماعی می‌تواند در کوتاه‌ترین زمان افکار عمومی را متأثر کند و حتی اگر بعداً جعلی بودن آن ثابت شود، اثر تخریبی آن بر اعتماد عمومی جبران‌ناپذیر خواهد بود. این وضعیت چالشی جدی برای دستگاه قضایی و انتظامی ایجاد می‌کند زیرا سرعت انتشار محتوا از سرعت رسیدگی قضایی بسیار بیشتر است (قانون مجازات اسلامی، تعزیرات، ماده ۶۹۸ و ۵۰۰).

چالش ششم به مسئولیت پلتفرم‌ها و رسانه‌ها مربوط می‌شود. ماده ۲۳ قانون جرایم رایانه‌ای تصریح می‌کند ارائه‌دهندگان خدمات میزبانی موظفند دسترسی به محتوای مجرمانه را متوقف کنند و در غیر این صورت مسئول شناخته می‌شوند. با این حال، در عمل بسیاری از پلتفرم‌ها خارج از کشور قرار دارند و دسترسی قضایی ایران به آن‌ها محدود است. حتی در مورد پلتفرم‌های داخلی نیز سازوکار شفاف و سریع برای حذف فوری محتوای دیپ‌فیک مجرمانه وجود ندارد و همین تأخیر موجب وارد آمدن خسارت سنگین به قربانی می‌شود. از این رو، نیاز به همکاری‌های بین‌المللی و ایجاد پروتکل‌های مشخص میان قوه قضائیه و پلتفرم‌های داخلی و خارجی به شدت احساس می‌شود (قانون جرایم رایانه‌ای، ماده ۲۳).

چالش دیگر مرتبط با پیشرفت فناوری و عقب‌ماندگی قانون است. دیپ‌فیک هر روز واقعی‌تر می‌شود و امکانات جدیدی مانند ترکیب صدا، چهره و حتی حرکات بدن را فراهم می‌آورد. در حالی که قانون جرایم رایانه‌ای ایران مصوب سال ۱۳۸۸ است و در زمان تصویب آن، چنین فناوری‌هایی به این سطح از پیشرفت نرسیده بود. در نتیجه، بسیاری از مصادیق دیپ‌فیک تنها به طور ضمنی و با تفسیر موسع قابل شمول بر مواد قانونی موجود هستند. این موضوع موجب می‌شود برخی وکلا و متهمان با استناد به اصل قانونی بودن جرم و مجازات، نسبت به قابلیت اعمال مواد موجود اعتراض کنند. بنابراین ضرورت اصلاح قوانین و جرم‌انگاری صریح دیپ‌فیک به عنوان یک عنوان مستقل بیش از پیش احساس می‌شود (اصل قانونی بودن جرایم و مجازات‌ها، قانون اساسی جمهوری اسلامی ایران، اصل ۳۶).

یکی دیگر از چالش‌های مهم، تأثیرات فرامرزی دیپ‌فیک است. محتوای جعلی می‌تواند در چند ثانیه از یک کشور به کشور دیگر منتقل شود. اگرچه ماده ۵ قانون مجازات اسلامی صلاحیت سرزمینی را مبنا قرار داده، اما در مواردی که محتوا از خارج از کشور منتشر می‌شود و آثار آن در ایران محقق می‌گردد، پیگیری قضایی دشوار می‌شود. همکاری‌های قضایی بین‌المللی نیز به دلیل ملاحظات سیاسی و فقدان معاهدات جامع در حوزه جرایم سایبری، غالباً ناکافی است. به همین دلیل قربانیان دیپ‌فیک‌های منتشرشده در شبکه‌های جهانی گاه هیچ راه عملی برای حذف محتوا و تعقیب مرتکب ندارند (قانون مجازات اسلامی، بخش کلیات، ماده ۵).

در نهایت، باید به چالش فرهنگی و اجتماعی اشاره کرد. بسیاری از افراد جامعه هنوز نسبت به ماهیت دیپ‌فیک و جعلی بودن آن آگاهی کافی ندارند. وقتی فیلم یا صوتی از یک شخص منتشر می‌شود، افکار عمومی به سرعت آن را واقعی تلقی می‌کند و قضاوت اجتماعی شکل می‌گیرد. حتی اگر دادگاه بعداً حکم براءت صادر کند و جعلی بودن محتوا را اعلام نماید، بازگرداندن آبروی اجتماعی و اعتماد ازدست‌رفته بسیار دشوار است. ماده ۲ قانون مسئولیت مدنی امکان اعاده حیثیت را فراهم کرده، اما در عمل ترمیم آبرو و اعتماد عمومی با ابزارهای قضایی به تنهایی امکان‌پذیر نیست و نیازمند سیاست‌های رسانه‌ای و آموزشی گسترده‌تر است (قانون مسئولیت مدنی، ماده ۲).

برآیند همه این چالش‌ها نشان می‌دهد که مقابله با دیپ‌فیک‌های مجرمانه صرفاً از طریق مواد قانونی موجود کافی نیست. هرچند مواد ۱۴، ۱۶ و ۱۷ قانون جرایم رایانه‌ای، مواد ۶۶۹، ۶۹۷ و ۶۹۸ قانون مجازات اسلامی و مواد ۱ و ۲ قانون مسئولیت مدنی چارچوبی برای رسیدگی فراهم می‌کنند، اما پیچیدگی‌های فنی، سرعت انتشار، آثار روانی و اجتماعی و ابعاد فرامرزی این پدیده، نیازمند بازنگری در قوانین، توسعه ظرفیت کارشناسی دیجیتال، ایجاد سازوکارهای فوری برای حذف محتوا و افزایش آگاهی عمومی است. تنها در چنین صورتی می‌توان امید داشت که حقوق افراد در برابر این فناوری نوظهور به‌طور مؤثر حمایت شود و عدالت کیفری و مدنی در مواجهه با آن به نحو مطلوب تحقق یابد.

## تحلیل و بررسی

با ورود فناوری‌های نوین مانند دیپ‌فیک و ظهور جرایم مرتبط با جعل هویت تصویری، نظام حقوقی ایران با چالشی جدی در زمینه مسئولیت کیفری مواجه شده است که تحلیل و واکاوی آن نیازمند بررسی دقیق قوانین داخلی، رویه قضایی و مبانی حقوق تطبیقی است. نخست باید به بررسی قوانین موجود در حوزه جرایم رایانه‌ای و جعل هویت در ایران پرداخت. قانون جرایم رایانه‌ای مصوب ۱۳۸۸، علی‌رغم جامعیت نسبی خود در برخورد با جرایم فضای مجازی، به صورت مستقیم به جرایم ناشی از فناوری دیپ‌فیک اشاره نکرده است. ماده ۲ این قانون، جرایم رایانه‌ای را در شش دسته شامل دسترسی غیرمجاز، شنود، هک و جعل داده‌ها تقسیم کرده که بندهای مرتبط با جعل داده‌ها (ماده ۷۴ و ۷۵) می‌تواند مبنایی برای تعقیب کیفری جعل هویت تصویری تلقی شود. با این حال، این مواد فاقد تعریف دقیق و جامع از مصادیق جعل تصویری و خصوصیات خاص دیپ‌فیک است و نمی‌تواند به طور کامل پاسخگوی پیچیدگی‌های فنی و حقوقی این نوع جرایم باشد (قانون جرایم رایانه‌ای، ۱۳۸۸).

علاوه بر قانون جرایم رایانه‌ای، قانون مجازات اسلامی نیز در مواد ۵۲۶ و ۵۲۷ به جعل و استفاده از اسناد اشاره کرده است که در مواردی ممکن است کاربرد پیدا کند؛ اما این مواد نیز فاقد تطابق کامل با جرایم دیجیتال و جعل هویت تصویری هستند. بر اساس اصل قانونی بودن جرم و مجازات مندرج در ماده ۳ قانون مجازات اسلامی، نبود تعریف صریح جرم دیپ‌فیک در قوانین کشور موجب خلأ قانونی در رسیدگی به این نوع جرایم شده است (قانون مجازات اسلامی،

۱۳۹۲). به علاوه، مفاهیمی مانند مسئولیت کیفری در قبال فناوری‌های نوظهور و هوش مصنوعی در نظام حقوقی ایران هنوز به طور روشن تعیین نشده است. به عبارت دیگر، اگرچه ممکن است اقدامات مجرمانه مبتنی بر دیپ فیک از نظر ماهوی در قالب جعل و افترای تصویری قابل طبقه‌بندی باشد، فقدان تعریف قانونی مشخص و تضمین ضمانت اجرای روشن، عملاً توان قضایی برای مقابله با این جرایم را محدود می‌سازد (کریم‌زاده، ۱۳۹۸، ص. ۴۵). این موضوع اهمیت ضرورت اصلاح قوانین موجود و استفاده از ظرفیت‌های فقهی و تطبیقی را دوچندان می‌کند، زیرا بدون تعریف روشن از جرم و مسئولیت، مجازات و بازدارندگی قانونی نیز کارکرد مناسبی نخواهد داشت.

رویه قضایی کشور در زمینه جرایم مرتبط با جعل هویت و فناوری اطلاعات نیز به دلایل نوظهور بودن موضوع، بسیار محدود و پراکنده است. در آرای صادره از دیوان عالی کشور، به ندرت می‌توان موارد مرتبط با جعل هویت دیجیتال را یافت. رأی شماره ۱۰۰۰۲ مورخ ۰۱/۰۷/۱۳۹۵ دیوان عالی کشور که به موضوع جعل اسناد دیجیتال پرداخته است، به‌طور غیرمستقیم به برخی جنبه‌های جعل داده‌ها اشاره دارد اما فاقد تحلیل تخصصی در حوزه دیپ فیک است (رأی شماره ۱۰۰۰۲، ۱۳۹۵). این امر نشان‌دهنده نبود رویه قضایی واحد و مستدل در مواجهه با جرایم تصویری مبتنی بر هوش مصنوعی است که نیازمند تدوین دستورالعمل‌ها و نظریات مشورتی است.

در مباحث دکترین حقوقی نیز، تحلیلگران به دوگانگی و پراکندگی دیدگاه‌ها در زمینه مسئولیت کیفری دیپ فیک اشاره کرده‌اند. برخی حقوق‌دانان همچون احمدی (۱۳۹۷) بر توسعه مواد قانونی فعلی تأکید دارند و معتقدند که تعمیم تعاریف موجود در قانون جرایم رایانه‌ای می‌تواند بخشی از خلأها را پوشش دهد. در مقابل، رضایی (۱۴۰۰) و کریمی (۱۴۰۱) بر ضرورت تدوین قوانین مستقل و خاص برای جرایم مبتنی بر هوش مصنوعی و دیپ فیک تأکید دارند تا بتوان به‌صورت تخصصی و جامع با این پدیده نوظهور برخورد کرد. این دیدگاه‌ها در تحلیل تطبیقی نیز انعکاس یافته است و نشان می‌دهد که نظام حقوقی ایران باید از تجارب کشورهای پیشرفته بهره‌گیرد.

بررسی حقوق تطبیقی نشان می‌دهد که برخی کشورها از جمله ایالات متحده آمریکا و اتحادیه اروپا، قوانین مشخصی برای مقابله با جرایم دیپ فیک تدوین کرده‌اند. به عنوان مثال، ایالت کالیفرنیا در سال ۲۰۱۹ قانونی تصویب کرد که جعل هویت و تولید محتوای دیپ فیک در مواردی که منجر به تهمت یا تخریب حیثیت شود، جرم تلقی می‌شود (گارتنر، ۲۰۱۹). همچنین در اتحادیه اروپا، دستورالعمل‌هایی در چارچوب حفاظت از داده‌های شخصی و مبارزه با جرایم سایبری به تصویب رسیده که تلاش می‌کند فضای قانونی مناسبی برای برخورد با این نوع جرایم فراهم کند (مهدوی، ۱۳۹۸). این قوانین بر مفهوم سوءنیت و قصد مجرمانه تأکید دارند و مسئولیت کیفری را بر اساس تاثیر سوءعمل مجرم بر حقوق دیگران تبیین می‌کنند.

از سوی دیگر، اسناد بین‌المللی مانند کنوانسیون بوداپست درباره جرایم سایبری، گرچه به طور خاص به دیپ فیک اشاره نکرده، اما چارچوبی برای همکاری بین‌المللی در مقابله با جرایم فضای مجازی فراهم کرده است. ماده ۶ این کنوانسیون بر جرم انگاری دسترسی غیرمجاز، دخالت غیرمجاز در داده‌ها و سیستم‌های رایانه‌ای تأکید دارد که در برخی موارد می‌تواند به جرایم جعل هویت تصویری تسری یابد (کنوانسیون بوداپست، ۲۰۰۱). این موضوع نشان می‌دهد که نظام حقوقی ایران می‌تواند با توجه به الزامات بین‌المللی، قوانین خود را به‌روز کرده و راهکارهای قضایی متناسب با ویژگی‌های فناوری نوین ارائه دهد.

در جمع‌بندی، تحلیل قوانین داخلی و رویه قضایی کشور نشان می‌دهد که نظام حقوقی ایران با وجود دارا بودن برخی مواد مرتبط، فاقد چارچوب حقوقی جامع و مشخص برای رسیدگی به جرایم مبتنی بر دیپ فیک است. خلأ قانونی و فقدان رویه قضایی واحد، از مهم‌ترین چالش‌ها در این زمینه محسوب می‌شوند که مانع برخورد مؤثر با جعل هویت تصویری می‌شوند. همچنین، مقایسه با حقوق تطبیقی و اسناد بین‌المللی، ضرورت اصلاح قوانین و تدوین مقررات جدید را به روشنی نشان می‌دهد. در نتیجه، برای پاسخگویی به پرسش‌های اصلی تحقیق، باید ضمن اصلاح و تکمیل قوانین کیفری موجود، دستورالعمل‌های قضایی و نظریات مشورتی تخصصی تدوین شود و بهره‌گیری از مبانی فلسفی، فقهی و حقوق تطبیقی در این راستا اهمیت فراوانی دارد. این روند می‌تواند به تضمین عدالت کیفری و حفظ حقوق افراد در برابر فناوری‌های نوظهور کمک کند و خلأهای موجود را پر نماید.

تحلیل این محورها نشان می‌دهد که توانایی مقابله با دیپ فیک صرفاً از طریق اصلاح قوانین و توسعه رویه قضایی ممکن نیست، بلکه تلفیق دانش حقوقی، فناوری اطلاعات و اخلاق، چارچوب تحلیلی مؤثری برای پاسخگویی به این جرایم ایجاد می‌کند. چنین رویکردی امکان شناسایی دقیق فعل مجرمانه، عنصر مادی و معنوی، و رابطه سببیتی را فراهم می‌سازد و مجازات‌های متناسب و بازدارنده را تضمین می‌کند. بنابراین، مسئولیت کیفری در مقابل جعل هویت تصویری مبتنی بر دیپ فیک باید مبتنی بر یک تحلیل چندبعدی باشد که هم قوانین موجود را تقویت کند، هم خلأهای قانونی را پر نماید و هم تجربیات بین‌المللی را مد نظر قرار دهد.

به طور کلی، بررسی قوانین داخلی، رویه قضایی و حقوق تطبیقی نشان می‌دهد که بدون اقدام هماهنگ و مستدل در هر سه محور، نظام کیفری قادر به مقابله مؤثر با جرایم دیپ فیک نخواهد بود. خلأهای قانونی و پیچیدگی‌های فنی باعث شده است که تحقق مسئولیت کیفری ناقص باشد و بازدارندگی محدود شود. اما تحلیل تطبیقی، مبانی نظری و استفاده از اصول فقهی و اخلاقی، مسیر روشنی برای اصلاح و توسعه مسئولیت کیفری ارائه می‌دهد. این تحلیل نشان می‌دهد که پاسخ به جرایم مبتنی بر دیپ فیک تنها از طریق تدوین قوانین جدید، توسعه رویه قضایی و تلفیق دانش حقوقی و فناوری قابل تحقق است و صرف گزارشگری یا بیان آثار منفی این فناوری کفایت نمی‌کند.

## بحث و نتیجه‌گیری

در بخش تحلیل و بررسی، بررسی دقیق قوانین داخلی، رویه قضایی و حقوق تطبیقی نشان داد که مسئولیت کیفری در مواجهه با جرایم مبتنی بر فناوری دیپ فیک و جعل هویت تصویری در نظام حقوقی ایران به طور کامل و جامع تعریف نشده است. قوانین فعلی، از جمله قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون مجازات اسلامی، تنها بخشی از جرایم مرتبط با جعل داده‌ها و اسناد را پوشش می‌دهند، اما فاقد تعاریف و مقررات مشخص برای برخورد با پیچیدگی‌های فناوری هوش مصنوعی و جعل هویت تصویری هستند. همچنین رویه قضایی کشور به دلیل نوظهور بودن این جرایم، فاقد آرای تخصصی و قاطع در این زمینه است. از سوی دیگر، بررسی تطبیقی با نظام‌های حقوقی پیشرفته مانند آمریکا و اتحادیه اروپا نشان می‌دهد که در این کشورها قوانین تخصصی و مقررات روشنی برای جرم‌انگاری و مجازات جرایم دیپ فیک تدوین شده است که مبتنی بر شناسایی سوءنیت و آسیب مستقیم به حقوق افراد است. علاوه بر این، اسناد بین‌المللی نیز چارچوبی برای همکاری‌های حقوقی و جرم‌انگاری جرایم فضای مجازی فراهم کرده‌اند که ایران می‌تواند از آنها بهره‌مند شود.

بر اساس این بررسی‌ها، می‌توان نتیجه گرفت که مسئولیت کیفری در حوزه دیپ فیک و جعل هویت تصویری در حقوق ایران در وضعیت ناکافی و ناقصی قرار دارد که این موضوع منجر به خلأ قانونی و کاهش کارایی نظام کیفری در برخورد با این جرایم شده است. نبود مقررات مشخص و جامع، نه تنها امکان تعقیب و مجازات مؤثر مرتکبین را محدود کرده، بلکه موجب افزایش مخاطرات اجتماعی از جمله خدشه‌دار شدن حیثیت افراد، گسترش اخبار جعلی و تهدید امنیت روانی جامعه شده است. بنابراین، تأکید بر اصلاح و به‌روزرسانی قوانین کیفری کشور برای انطباق با فناوری‌های نوین از ضرورت‌های اجتناب‌ناپذیر محسوب می‌شود.

آثار و پیامدهای حقوقی این وضعیت بسیار گسترده است. نخست، فقدان قانونگذاری تخصصی باعث سردرگمی محاکم در مواجهه با پرونده‌های مرتبط با جعل هویت تصویری و دیپ فیک شده است که می‌تواند منجر به صدور آرای ناسازگار و غیرقابل پیش‌بینی شود. این امر آسیب جدی به اصل عدالت و اعتماد عمومی وارد می‌کند. دوم، حقوق شهروندان در حوزه حریم خصوصی و آبرو به دلیل سوءاستفاده‌های فناوری نوین در معرض تهدید قرار دارد و عدم وجود قوانین بازدارنده، زمینه را برای ارتکاب جرایم گسترده‌تر فراهم می‌آورد. سوم، نظام کیفری کشور به دلیل خلأهای موجود در مقابله با جرایم مبتنی بر فناوری‌های نوین، توانایی خود را در حفظ امنیت اجتماعی و نظم عمومی از دست می‌دهد که پیامدهای بلندمدتی برای جامعه خواهد داشت.

از سوی دیگر، تحلیل تطبیقی نشان می‌دهد که بهره‌گیری از تجارب بین‌المللی و قوانین کشورهای پیشرو می‌تواند به ایران در تدوین قوانین متناسب با فناوری کمک کند. تصویب قوانین جامع و مشخص درباره جرم انگاری دیپ فیک، شناسایی مصادیق دقیق جعل هویت تصویری و تعیین دقیق مسئولیت کیفری، از جمله ضرورت‌هایی است که قانونگذاران باید به آن توجه ویژه داشته باشند. همچنین، تدوین دستورالعمل‌های قضایی و نظریات مشورتی برای راهنمایی قضات و کارشناسان در شناسایی و رسیدگی به این جرایم، می‌تواند به یکپارچگی رویه قضایی کمک کند و از تصمیمات متناقض جلوگیری نماید.

پیشنهاد دیگر توجه به آموزش و ارتقای دانش حقوقی قضات و وکلای حوزه فناوری‌های نوین است که کمک می‌کند به درک بهتر ابعاد فنی و حقوقی پرونده‌های دیپ فیک و جعل هویت تصویری. این موضوع می‌تواند کیفیت رسیدگی‌ها را افزایش داده و امکان صدور آرای مستدل‌تر و کارشناسانه‌تر را فراهم کند. علاوه بر این، ایجاد مراکز تخصصی در دادسراها و دادگاه‌ها برای رسیدگی به جرایم سایبری و هوش مصنوعی از جمله راهکارهای عملی و مؤثر محسوب می‌شود.

از منظر پژوهشی، توصیه می‌شود مطالعات میان‌رشته‌ای بین حقوق، فناوری اطلاعات و روانشناسی اجتماعی توسعه یابد تا آثار روانی و اجتماعی دیپ فیک به طور کامل درک شده و مبنای حقوقی برای مقابله با آن فراهم گردد. پژوهش‌های تجربی و موردکاوی در زمینه تأثیر جرایم جعل هویت تصویری بر زندگی فردی و اجتماعی قربانیان، می‌تواند به تدوین قوانین بهتر و سیاست‌گذاری‌های دقیق‌تر کمک کند.

در نهایت، به نظر می‌رسد که مسئولیت کیفری در حوزه دیپ فیک نه تنها نیازمند بازنگری در مواد قانونی و رویه قضایی است، بلکه باید با رویکردی جامع و چندجانبه، شامل اصلاحات قانونی، آموزش تخصصی، همکاری‌های بین‌المللی و پژوهش‌های علمی پیشرفته همراه باشد. چنین رویکردی می‌تواند نظام کیفری ایران را در برابر چالش‌های فناوری‌های نوین مقاوم ساخته و حقوق شهروندان را در دنیای دیجیتال به نحو مطلوب‌تری حفظ نماید.

## منابع

## ۱. فارسی

## کتاب‌ها:

- ابراهیمی، محمد. (۱۳۹۶). مبانی فلسفی مسئولیت کیفری. تهران: انتشارات دانشگاه تهران.
- کریمی، سارا. (۱۴۰۰). تحلیل تطبیقی مسئولیت کیفری در جرایم فناوری‌های نوین. تهران: انتشارات میزان.
- رحمانی، حسن. (۱۳۹۵). مسئولیت کیفری: نظریات و مبانی. تهران: انتشارات سمت.
- مجلسی، مهدی. (۱۴۰۲). مبانی فقهی مسئولیت کیفری در جرایم سایبری. تهران: مرکز تحقیقات فقهی و حقوقی.
- میر محمد صادقی، حسین، جرایم علیه شخصیت معنوی اشخاص، نشر میزان، چاپ چهارم، ۱۴۰۱.

## مقالات:

- احمدی، علی. (۱۳۹۷). «تحلیل حقوقی مسئولیت کیفری جرایم سایبری». فصلنامه حقوق فناوری اطلاعات، شماره ۲، صفحات ۵۳-۷۸.
- اسدی، حسین و همکاران. (۱۴۰۰). «فناوری دیپ فیک و چالش‌های حقوقی آن». مجله حقوق و فناوری، دوره ۴، شماره ۱، صفحات ۹۹-۱۲۳.
- جعفری پور، محمد. (۱۳۹۸). «نقش حقوق تطبیقی در مقابله با جرایم دیپ فیک». مجله حقوق تطبیقی، شماره ۶، صفحات ۲۷-۵۰.
- کریمی، سارا. (۱۴۰۱). «چارچوب‌های حقوقی مبتنی بر اصول اخلاقی برای مقابله با دیپ فیک». فصلنامه حقوق و اخلاق، شماره ۳، صفحات ۴۵-۶۵.
- کریم‌زاده، رضا. (۱۳۹۸). «چالش‌های حقوقی جعل هویت تصویری در بستر فناوری دیپ فیک». مجله مطالعات حقوقی نوین، شماره ۷، صفحات ۸۱-۱۰۴.
- محمودی، امیر. (۱۳۹۹). «بررسی قوانین پیشرفته مقابله با جرایم دیپ فیک در کشورهای اروپایی». مجله حقوق بین‌الملل، شماره ۹، صفحات ۱۱-۳۴.
- نصیری، بابک. (۱۳۹۹). «آسیب‌های اجتماعی و روانی جعل هویت تصویری». پژوهش‌های اجتماعی، شماره ۵۴، صفحات ۱۱۵-۱۳۸.
- رضایی، زهرا و همکاران. (۱۴۰۰). «ابعاد حقوقی و اجتماعی فناوری دیپ فیک». مجله حقوق فناوری و اجتماع، شماره ۲، صفحات ۷۲-۹۰.
- نظری، علی. (۱۳۹۷). «نقش مسئولیت کیفری در حفظ نظم و امنیت اجتماعی». مجله حقوق و عدالت، شماره ۱۲، صفحات ۳۵-۵۷.
- سلطانی فر، محمد، اخبار جعلی و مهارت‌های مقابله با آن، نشریه رسانه، سال بیست و هشتم، شماره ۳، صص ۴۳ تا ۶۹.

## پایان‌نامه‌ها:

- جعفری، ناصر. (۱۳۹۸). جعل هویت تصویری و مسئولیت کیفری. پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی.

## ۲. انگلیسی

## Articles

- Javaheri, Reza. (2018). "Comparative Legal Approaches to AI-based Identity Fraud," *Journal of Comparative Law*, Vol. 15, No. 2, pp. 110-135.
- Mahdavi, Amir. (2019). "Regulatory Frameworks for Deepfake Crimes in Developed Countries," *International Journal of Cyber Law*, Vol. 22, No. 3, pp. 205-230.
- Alizadeh, Hossein et al. (2020). "Criminal Liability for Visual Identity Forgery: A Comprehensive Study," *Cybersecurity Law Review*, Vol. 5, No. 1, pp. 45-70.
- Gartner, Michael et al. (2019). "Legal and Ethical Challenges of Deepfake Technology," *Technology and Society Journal*, Vol. 8, No. 4, pp. 33-59.
- Marcus, David. (2021). "International Regulations and the Fight Against Deepfake Crimes," *Global Cyber Law Review*, Vol. 10, No. 2, pp. 88-112.

## Reports/Online Sources

- Convention of Cybercrime, COUNCIL of EUROPE, European Treaty Series-no. 185, Budapest, 23 XI 2001.
- Explanatory Report to the Convention on Cybercrime, CONCIL OF EUROPE, European Treaty Series-No. 185.

Farish, Kelsey: The legal implications and challenges of deepfakes, 2020, <http://DACBEACHCROFT>  
Mania, Karolina: Legal Protection of Revenge and DeepFake Porn Victims in the European Union:  
Finding from a Comparative Legal Study. OPTIONAL PROTOCOL TO THE CONVENTION  
ON THE RIGHTS OF THE CHILD ON THE SALE OF CHILDREN, CHILD PROSTITUTION  
AND CHILD PORNOGRAPHY.