هفتمین همایش ملی بنیاد علمی قانون یار
همایش پژوهش های علمی علوم اسلامی و انسانی در عصر نوین
بنیاد علمی قانون یار - آموزش و پرورش استان کرمانشاه – واحد پژوهش سپاه پاسداران
(با همکاری و حمایت معنوی دانشگاه رازی، دانشگاه آزاد، دانشگاه فرهنگیان، دانشگاه پیام نور کرمانشاه، دانشگاه علمی و کاربردی، جهاد دانشگاهی واحد کرمانشاه، دانشگاه صنعتی کرمانشاه، بنیاد شهید و سازمان ارشاد و ....
سردبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی (نمایه مقالات در پایگاه های ملی و بین المللی)
تاریخ برگزاری همایش: ۸ اسفندماه ۱۴۰۳ شماره مقاله: ۲۸/۵۰۲ رده بندی کنگره: ب ۶۰/۵۶

مطالعه تطبیقی جرم‌شناسی و چالش‌های حقوقی ناشی از استفاده از تکنولوژی دیپ‌فیک و هوش مصنوعی در ارتکاب جرایم سایبری

میرامیرمحمد میرجعفری ترکی
کارشناس ارشد حقوق جزا و جرم شناسی،واحد تهران شمال،دانشگاه آزاد اسلامی، تهران

چکیده

استفاده روزافزون از تکنولوژی‌های نوین مانند دیپ‌فیک و هوش مصنوعی در فضای سایبری، منجر به ظهور و گسترش انواع جدیدی از جرایم سایبری شده است که به‌ویژه در زمینه جعل و سوءاستفاده از هویت افراد، تهدیدات جدی به همراه دارد. دیپ‌فیک، که به ایجاد ویدیوها و تصاویری می‌پردازد که به‌طور مصنوعی واقعی به نظر می‌رسند، به‌ویژه در زمینه‌های سیاسی، اجتماعی و اقتصادی آسیب‌های قابل توجهی ایجاد کرده است. این مقاله به مطالعه تطبیقی جرم‌شناسی و چالش‌های حقوقی ناشی از استفاده از این تکنولوژی‌ها در ارتکاب جرایم سایبری می‌پردازد. هدف اصلی این تحقیق بررسی ابعاد مختلف جرم‌شناسی، تحلیل مشکلات حقوقی موجود در برخورد با این گونه جرایم و ارائه پیشنهادات عملی برای مقابله با آن‌ها است. در این راستا، تطبیق رویکردهای مختلف حقوقی و جرم‌شناسی در کشورهای مختلف بررسی خواهد شد تا راهکارهای مؤثری برای پیشگیری و مقابله با تهدیدات ناشی از دیپ‌فیک و هوش مصنوعی ارائه گردد. در کنار دیپ‌فیک، هوش مصنوعی نیز به‌طور گسترده در زمینه تحلیل داده‌ها، پیش‌بینی رفتارها و حتی خلق محتواهای جعلی به کار می‌رود، که موجب پیچیدگی‌های فراوانی در شناسایی و مقابله با جرایم سایبری می‌شود. از آنجا که تکنولوژی‌های نوین در بسیاری از موارد قوانین موجود را پشت سر می‌گذارند و مشکلات جدی در تطبیق آن‌ها با اصول حقوقی ایجاد می‌کنند، ضرورت دارد تا به بررسی جامع این موضوع پرداخته و چالش‌های حقوقی آن شناسایی شود.

واژگان کلیدی: جرم شناسی ،جرائم سایبری ، هوش مصنوعی ، دیپ فنگ

مقدمه

تکنولوژی‌های نوین به‌ویژه هوش مصنوعی و دیپ‌فیک، انقلابی در عرصه‌های مختلف علمی و صنعتی به‌وجود آورده‌اند، اما در کنار مزایای فراوان، تهدیدات جدی نیز برای امنیت اجتماعی، سیاسی و اقتصادی به دنبال داشته‌اند. دیپ‌فیک، به‌عنوان یکی از پیشرفته‌ترین تکنولوژی‌های موجود در زمینه تغییر تصاویر و ویدیوها، می‌تواند هویت افراد را به‌طور کامل جعل کرده و برای اهداف مخرب مورد استفاده قرار گیرد. این امر به‌ویژه در عرصه‌های مختلف سیاسی و اجتماعی، موجب ایجاد بحران‌های جدی و از بین بردن اعتماد عمومی می‌شود. این مقاله به‌طور خاص به مطالعه تطبیقی بین سیستم‌های حقوقی مختلف در برخورد با این گونه جرایم می‌پردازد و تلاش می‌کند تا ضمن تحلیل ابعاد جرم‌شناسی این جرایم، راهکارهای قانونی و پیشگیرانه برای مقابله با آن‌ها ارائه دهد. در این مسیر، بررسی نقش نهادهای دولتی، سازمان‌های بین‌المللی و بخش خصوصی در مقابله با این جرایم اهمیت ویژه‌ای خواهد داشت. یکی از ویژگی های دهه های اخیر توسعه کمی و کیفی انواع فناوری خایی است که به جامعه بشری معرفی می شود . اصولا هر پدیده اجتماعی به دلیل فرآیند تاثیر و تاثر در جامعه تابع یک سری قوانین و مقررات حقوقی است . رایانه و تلفن همراه یا دارک وب ها به عنوان یکی از اجزای لاینفک اجتماعی در عصر حاضر از این اصل پیروی می کند .(محمدی فردوئی ؛ ۱۳۹۷ ، ۴۹۵)

با معرفی فضای مجازی ؛ جامعه انسانی هر از چندگاهی شاهد عرضه یک نرم افزار با قابلیت های جدیدی است . این برنامه ها عمدتا دو هدف تسهیل انجام بخشی از کارهای روزمره انسان با فراهم ساختن یک قابلیت جدید برای وی دنبال می کند. هرچند این نرم افزار ها با هدف بهبود کیفیت زندگی بشر انجام میپذیرد ، تنوع قابلیت های آنها این امکان را نیز فراهم میسازد تا بتوان این کارکرد های سوئی را نیز به خدمت گرفت . در کنار فواید بسیار این پدیده هم چون هر پدیده دیگر موجبات سواستفاده برخی را نیز فراهم نموده است. (گرایلی ؛ ۱۳۸۹، ۱۵۹)

دیپ فیک ها یا همان جعل عمیق، ترکیبی از کلمه‌های «یادگیری عمیق» و «جعلی»، یک تکنیک برای ترکیب تصویر انسان مبتنی بر هوش مصنوعی است. جعل عمیق تصاویر و فیلم‌های موجود را بر روی تصاویر یا فیلم‌های منبع قرار می‌دهد و از یک تکنیک یادگیری ماشین به نام «شبکه‌های زایای

دشمنگونه (GAN) «استفاده می‌کند. ویدیوی جعلی، ترکیب فیلم‌های موجود و منبع است که فرد یا افرادی را درحال انجام یک کار در موقعیتی نشان می‌دهد که هرگز در واقعیت اتفاق نیفتاده است.

برای مثال چنین فیلم‌های تقلبی‌ای می‌تواند فرد را در حال انجام اقدامات جنسی نشان دهد که هرگز در آن شرکت نکرده‌است یا می‌تواند برای تغییر کلمات یا حرکات یک سیاستمدار مورد استفاده قرار گیرد تا به نظر برسد آن فرد چیزی را گفته که هرگز به زبان نیاورده‌است. به دلیل این قابلیت‌ها، جعل عمیق می‌تواند برای ایجاد فیلم‌های پورن افراد مشهور، پورن انتقامی، اخبار جعلی و کلاهبرداری‌های مخرب استفاده شود.(ویکیپدیا) در انجام هر پژوهش علمی مطالعه و بررسی تحقیقاتی که در ارتباط با موضوع است ضروری خواهد بود که در این بخش به بررسی آن¬ها پرداخته می شود :

- صالحی و محترم قلاتی (۱۳۹۷) ؛ در مقاله ای با عوان {گستره و ویژگی های دادهای مجعول رایانه ای در حقوق ایران } به این نتیجه رسیده است که به موازات پیشرفت سزیع فناوری های اطلاعات و ارتباطات ؛ طیف گسترده و متنوعی از داده ها و اسناد الکترئنیک موضوع جعل و تحریف قرار گرفته .

- شیری ورنامخواستی ، عباس (۱۴۰۱) : در مقاله ای با عوان {دیپ فیک یا همانندسازی صوتی یا تصویری غیر واقعی در حقوق کیفری } به این نتیجه رسیده است که مصادیق بزهکارانه دیپ فیک تا کنون جرم انگاری نگردیده است . امکان تطبیق جرائم جعل رایانه ای ، تولید محتوای نبتذل ، مستهجن ، و هرزه نگاری ، افترا و نشر اکاذیب با دیف فیک مورد بررسی قرار گرفته است .

- علی ین ، آرش (۱۴۰۰) : در مقاله ای با عوان { جرم انگاری دیپ فیک ها از منظر تعهدات حقوق بشری دولت ها } به این نتیجه رسیده است که دیپ فیک ها تعرض به حقوق اشخاص و جامعه محسوب می شوند .

- فلسفی ، سیدغلامرضا (۱۳۹۸) ؛ در مقاله ای با عوان {دیپ فیک تیغی در کف زنگیان مست} به این نتیجه رسیده است که روند شناسایی دیپ فیک ها همچونم رابطه موش و گربه دچار می شود .

آنچه پژوهش حاضر را از سایر تحقیقات در این حوزه جدا می کند و جنبه نوآوری این پژوهش این است که به موضوع مذکور پرداخته نشده است لذا ضرورت پژوهش در این حوزه بیش از پیش لازم است.

در این بخش از پژوهش به مفهوم مهم جرم‌شناسی و چالش‌های حقوقی ناشی از استفاده از تکنولوژی دیپ‌فیک پرداخته می شود:

بخش اول: تعریف و بررسی دیپ فیک و هوش مصنوعی

در این بخش به تئضیح و بررسی ماهیت و عملکرد تکنولوژی دیپ فیم و هوش مصنوعی میپردازد ؛ دیپ فیک ها به عنوان ویدیوهای جعلی که با استفاده از الگوریتم های هوش مصنوعی ساخته می شوند و به نوعی ارتباط مستقیم با یک دیگر دارند توانایی ایجاد تصویر و ویدئو های واقعی از افرادی که هیچ گاه آن را تولید نکرده اند دارند. (۲۰۲۱).kietzmann,J.H.,&Angell, l

دیپ فیک (Deepfake) و هوش مصنوعی (AI) دو موضوع مهم و جذاب در دنیای فناوری و رسانه هستند که ارتباط نزدیکی با یکدیگر دارند. در اینجا، هر دو مفهوم را به طور مفصل بررسی می‌کنیم.

بند اول: هوش مصنوعی(AI)

هوش مصنوعی به شاخه‌ای از علوم کامپیوتر اطلاق می‌شود که هدف آن ایجاد سیستم‌هایی است که می‌توانند مانند انسان‌ها فکر کنند، یاد بگیرند، استدلال کنند و تصمیم‌گیری‌های پیچیده انجام دهند. هوش مصنوعی شامل بسیاری از زیرشاخه‌ها و روش‌هاست که می‌توانند در حل مسائل مختلف کاربرد داشته باشند، از جمله:

الف)یادگیری ماشین :(Machine Learning) یکی از مهم‌ترین زیرشاخه‌ها، جایی که سیستم‌ها می‌توانند از داده‌ها یاد بگیرند و به مرور زمان عملکرد خود را بهبود دهند. این روش‌ها معمولاً بر اساس الگوریتم‌هایی عمل می‌کنند که با داده‌های آموزشی پردازش می‌شوند و پیش‌بینی‌ها یا تصمیمات جدید می‌سازند.

ب)یادگیری عمیق :(Deep Learning) یک روش خاص از یادگیری ماشین که از شبکه‌های عصبی عمیق (شبکه‌های مصنوعی با لایه‌های متعدد) برای مدل‌سازی و پیش‌بینی استفاده می‌کند. یادگیری عمیق در زمینه‌های مختلفی مانند شناسایی تصاویر، تشخیص صدا و حتی پردازش زبان طبیعی به کار می‌رود.

ج)پردازش زبان طبیعی :(Natural Language Processing) به‌کارگیری الگوریتم‌ها برای درک و تولید زبان انسانی، که شامل ترجمه، تحلیل احساسات و پاسخ به سوالات است

د) .رؤیهٔ کامپیوتری :(Computer Vision) این شاخه به شبیه‌سازی توانایی‌های بینایی انسان در سیستم‌های کامپیوتری می‌پردازد. کاربردهای آن شامل شناسایی اشیاء در تصاویر و ویدئوها و تشخیص چهره است.

هوش مصنوعی به سرعت در حال پیشرفت است و در بسیاری از صنایع از جمله بهداشت، خودروسازی، آموزش، بانکداری، و امنیت کاربردهای فراوانی دارد.

بند دوم: دیپ فیک (Deepfake)

دیپ فیک به تکنیک‌هایی اطلاق می‌شود که از هوش مصنوعی، به‌ویژه یادگیری عمیق، برای تولید یا تغییر محتوای تصویری و صوتی به‌گونه‌ای استفاده می‌کند که این محتوای جدید واقعی به نظر برسد، اما حقیقت ندارد. این تکنیک می‌تواند تصاویر و ویدئوهایی بسازد که در آن‌ها افراد به انجام کارهایی نمایش داده می‌شوند که در واقع هرگز انجام نداده‌اند.

الف) چگونگی ایجاد دیپ فیک

برای ایجاد یک دیپ فیک، از شبکه‌های عصبی مصنوعی مانند Generative Adversarial Networks (GANs)استفاده می‌شود. این شبکه‌ها دو مدل دارند: یکی مدل تولیدکننده (Generator)که محتوای جعلی را تولید می‌کند، و دیگری مدل تشخیص‌دهنده (Discriminator)که تلاش می‌کند تا تفاوت بین محتوای واقعی و جعلی را شناسایی کند. این دو مدل به‌طور همزمان آموزش داده می‌شوند تا مدل تولیدکننده بتواند محتوای هرچه واقعی‌تر بسازد.

ب) کاربردهای دیپ فیک

۱ .صنعت سرگرمی: در سینما و تلویزیون، برای ایجاد جلوه‌های ویژه، تغییر چهره بازیگران یا بازگرداندن بازیگران قدیمی به فیلم‌های جدید.

۲ .آموزش و آموزش‌های مجازی: ایجاد محتواهای آموزشی یا دوبله‌های مصنوعی برای زبان‌های مختلف.

۳ .تبلیغات و بازاریابی: استفاده از چهره افراد مشهور برای تبلیغات بدون حضور واقعی آن‌ها.

۴ .تولید محتوای کاذب: در بعضی مواقع از دیپ فیک‌ها برای ساخت اخبار دروغین یا جعل سخنان افراد استفاده می‌شود.

ج) چالش‌ها و مشکلات دیپ فیک

۱ .اطلاعات نادرست: یکی از بزرگ‌ترین تهدیدهای دیپ فیک‌ها، توانایی آن‌ها در ایجاد محتوای جعلی است که می‌تواند به گمراهی عمومی منجر شود. برای مثال، دیپ فیک‌ها می‌توانند سخنان یا رفتارهای افراد را تحریف کنند.

۲ .امنیت و حریم خصوصی: استفاده از چهره یا صداهای افراد بدون اجازه آن‌ها، می‌تواند تهدیدی برای حریم خصوصی باشد.

۳ .تشخیص و مقابله با دیپ فیک: تشخیص دیپ فیک‌ها چالش بزرگی است. برخی از ابزارها و الگوریتم‌ها در حال توسعه هستند تا بتوانند تشخیص دهند که یک ویدئو یا تصویر واقعی است یا خیر.

د) رابطه بین دیپ فیک و هوش مصنوعی

هوش مصنوعی و دیپ فیک به‌طور نزدیکی به هم مرتبط هستند، زیرا دیپ فیک‌ها معمولاً با استفاده از الگوریتم‌های یادگیری عمیق و شبکه‌های عصبی تولید می‌شوند. این تکنیک‌ها می‌توانند به سرعت پیشرفت کرده و محتوای با کیفیت بسیار بالا و شبیه به واقعیت ایجاد کنند، به طوری که تفکیک آن از واقعیت دشوار می‌شود.

بخش دوم: جرم شناسی و تحلیل تهدیدات ناشی از دیپ فیک و هوش مصنوع

این بخش به بررسی چالش های حقوقی مربوط به دیپ فیک و هوش مصنوعی می پردازد ، یکی از مهم ترین چالش عا تطبیق قوانین موجود با تکنولوژی های جدید است . ((Finck,M.(۲۰۲۰)

بند اول: جعل رایانه‌ای

جعل در لغت به معنای دگرگون کردن و ساختن می باشد در جرم جعل سنتی مرتکب نسبت به نوشته جات ،اسناد ،مهر و امضای اشخاص دخل و تصرف کرده و با تقلب آن ها را به قصد اضرار به دیگری تغییر می دهد.در قانون مجازات اسلامی و همچنین قانون جرایم رایانه ای جرم جعل بیان شده است.

تفاوتی که بین جرم جعل سنتی با جعل رایانه ای وجود دارد بستر ارتکاب می باشد جرم جعل رایانه ای درفضای دیجیتال مثل رایانه و نسبت به داده ها صورت می گیرد.قانون مجازات اسلامی در ماده ۵۲۳ بیان می دارد:

جعل و تزویر عبارتند از:ساختن نوشته یا سند یا ساختن مهر یا امضای اشخاص غیر رسمی یا رسمی ، خراشیدن یا تراشیدن یا قلم بردن یا الحاق یا محو یا اثبات یا سیاه کردن یا تقدیم یا تاخیر سند نسبت به

تاریخ حقیقی یا الصاق نوشته ای به نوشته دیگر یا به کار بردن مهر دیگری بدون اجازه صاحب آن و نظایر این ها به قصد تقلب.

* ماده ۶ قانون جرایم رایانه ای در خصوص جعل رایانه ای بیان می دارد:

هر کس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب می‌شود:

تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده به آنها.

تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علائم به آنها. بنابراین تفاوت جعل سنتی و جعل رایانه ای تفاوت در بستر ارتکاب می باشد زیرا برخلاف جعل سنتی که ملموس و مادی می باشد جعل رایانه ای ملموس نبوده و در فضای مجازی ودیجیتال و نسبت به داده ها اعمال می شود. تفاوت دیگر جعل رایانه ای و جعل سنتی در این است که جعل رایانه ای صرفا در قالب فعل مثبت واقع می شود و به صورت ترک فعل قابل ارتکاب نمی باشد .این نکته را می توان از عباراات قانونگذار متوجه شد که از عبارت تغییر دادن که فعلی مثبت می باشد در قانون جرایم رایانه ای استفاده کرده است. البته لازم به ذکر است که واژه قابل استناد که در ماده ۶ قانون جرایم رایانه ای از آن عنوان شده است بی دلیل و معنا نبوده و داده های تغییر یافته می بایست ارزشمند بوده و قابلیت ورود ضرر را داشته باشند.(موسسه حقوقی منشور دیدگاه سوم)

بند دوم: نقض حریم خصوصی

هرچند حریم خصوصی را مفهوم بسیار مبهم دانستند و تعریف آن را بسیار مشکل دانستند .(محسنی ، فرید (۱۳۸۹)) می‌توان گفت حریم خصوصی قلمرویی از زندگی اشخاص است که به هیچ وجه مایل نیستند دیگران بدون اجازه آنها وارد این قلمرو شوند یا از آنها آگاهی پیدا کنند .(هوسمن، کارل(ترجمه داوود حیدری۱۳۷۰ ؛ ص ۴۲) ؛ مطابق بند ۱ ماده ۲ لایحه حمایت از حریم خصوصی ، حریم خصوصی قلمرویی از زندگی هر شخص است که آن شخص عرفاً یا با اعلان قبلی در چهارچوب قانون انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن

دسترسی نداشته یا در آن قلمرو وی مورد تعارض قرار ندهند . خسارت ناشی از نقض حریم خصوصی داده تحقق مسئولیت مدنی لازم است وجود ضرر و خسارت تقصیر یا فعل زیانبار و رابطه سببیت عرفی. هدف مسئولیت مدنی جبران ضرر است؛ بنابراین بدون ضرر مسئولیت نیز وجود نخواهد داشت. ضرر از نظر فقهی این چنین تعریف شده است : است که در مال یا آبرو یا نفس یا شأنی از شئون موجود انسان یا شأنی که مقتضی نزدیک آن وجود دارد به نحوی که عرف آن شأن را موجود می‌بیند (بجنوردی، سید محمد حسن (۱۴۱۹). حقوقدانان در تعریف ضرر گفته اند هرجا نقضی در اموال ایجاد شود یا منفعت مسلمی از دست برود یا به سلامت و حیثیت و عواطف شخص لطمه‌ای وارد آید ضرر به بار آمده است . (کاتوزیان، ناصر(۱۳۷۴)

حریم خصوصی را می‌توان در یک تقسیم‌بندی به حریم خصوصی اطلاعاتی (Information Privacy)، حریم خصوصی ارتباطی، (Communication privacy)، حریم خصوصی جسمانی (Bodily privacy)، حریم خصوصی مکانی (Territorial privacy) و حریم خصوصی شخصیتی (personality privacy) تقسیم نمود. رعایت این حق در مناسبات بین افراد یک جامعه و همچنین در خانواده و روابط خانوادگی و در ارتباط بین حاکمیت و مردم قابل تصور می‌باشد. برخلاف تصور برخی، مصادیق حریم خصوصی در بیان فقها متمایز از جان و مال انسان مورد توجه قرار گرفته است؛ به عبارت دیگر لزوم رعایت و دفاع از حریم در عبارات فقها منحصر به لزوم حفظ جان و مال نیست؛ بنابراین همان‌طور که انسان مکلف است در برابر متجاوز به مال و جان خود دفاع نماید در برابر تهدید کننده حریم نیز مسئولیت دارد. در عبارات شهید ثانی آمده است که انسان حق دارد در حد توان از جان و حریم و مال خویش دفاع کند. یا «اشکالی نیست در این‌که انسان، حق دارد از جان حریم و مالش در برابر محارب و مهاجم و دزد و مانند آن‌ها دفاع کند.»(شهید ثانی، زین‌الدین عاملی،ج۲، ص۵۹، ۱۴۱۰هق)

الف) اطلاعاتی

به هر نوع داده از جمله صوت، تصویر، فیلم، نوشته، نشانه، نقشه، اعداد و یا ترکیبی از آن‌ها که در اسناد مندرج باشد یا به صورت نرم‌افزاری ذخیره گردیده و یا با هر وسیله دیگری ضبط شده باشد، اطلاعات می‌گویند. اطلاعات مربوط به هویت، احوال شخصی، وضعیت فردی، عقاید و باورها، پست الکترونیکی،

عکس و فیلم و صوت و تصویر و عادات رفتاری و فردی از قبیل نام و نام خانوادگی، محل و تاریخ تولد، ازدواج، طلاق، مشخصات همسر، والدین و فرزندان، نسبت خانوادگی، ناراحتی‌های جسمی و روحی، شماره حساب بانکی و رمز عبور، محل کار و سکونت و همچنین اطلاعات شخصی مربوط به انجام امور تجاری، شغلی، تحصیلی، مالی، آموزشی، اداری، پزشکی و حقوقی اطلاعات شخصی گفته می‌شود. (ماده ۱، آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات) قواعد حاکم بر نحوه پردازش، داده‌ها و اطلاعات مربوط به اشخاص را حریم خصوصی اطلاعاتی می‌نامند (نوری و نخجوان، حقوق حمایت داده‌ها، ج۱، ص۳۴، ۱۳۸۳، تهران، گنج دانش).

بنابر اصول حمایت از داده‌ها کلیه اطلاعات شخصی نظیر اطلاعات پزشکی اشخاص، اطلاعات مالی، دولتی و... بایستی تحت قواعد مربوط به حمایت داده پردازش شوند و هرگونه تخلفی از قواعد مزبور به منزله نقض حریم اطلاعاتی اشخاص تلقی می‌شود(صادقی، حسین، مسئولیت مدنی در ارتباطات الکترونیک، ج۱، ص۱۱۷، ۱۳۸۸، تهران، میزان).

قانون تجارت الکترونیکی ایران مصوب ۱۳۸۴ هرچند صریحاً حریم خصوصی را تعریف نکرده ولی با بیان قواعد مربوط به بحث حمایت داده‌ها در قالب مواد مختلف مانند حمایت از داده‌های حساس (ماده ۵۸)، شرایط ذخیره، پردازش و توزیع داده‌ها با رضایت شخص (ماده ۵۹)، حمایت از داده‌های مربوط به سوابق پزشکی و بهداشتی (ماده ۶۰)، سعی در حمایت از حریم خصوصی از طریق برشمردن مصادیق آن نموده است.

رعایت حریم خصوصی اطلاعاتی افراد و عدم ورود و اشاعه اسرار آن‌ها به شدت مورد تأکید می‌باشد تا جایی که برخی از فقیهان افشای سر مؤمن را موجب سقوط عدالت دانسته‌اند. (مقدس اردبیلی، احمد، ص۳۴۹، ۱۴۱۱ هق) البته در مواردی که اطلاعات و اسرار نه در ارتباط با اشخاص، بلکه مرتبط با نظام و حاکمیت اسلامی باشد، رعایت حریم اطلاعاتی به مراتب مهم‌تر خواهد بود زیرا مفسده افشای اسرار نظام متوجه جمیع مؤمنین و افراد جامعه می‌گردد؛ بنابراین اگر نادیده گرفتن حریم خصوصی اطلاعاتی افراد جایز نمی‌باشد، به طریق اولی افشای اسرار نظام جایز نخواهد بود. «لاشک فی حرمۀ افشاء الاسرار، سیّما اذا کانت اسرار الدولۀ الاسلامیّۀ، حیثان ذلک یضرّ بمصالح المسلمین و دولتهم و کیانهم»

همچنین صاحب جواهر در مقایسه فرار از جنگ، که از گناهان کبیره شمرده می‌شود، با افشای اسرار مسلمین نزد کفار که منجر به قتل و اسارت و غارت ایشان می‌شود، گناه و مفسده دومی را بسیار بیش‌تر می‌داند(نجفی، محمدحسن، جواهر الکلام، ج۱۳، ص۳۲۱). امام خمینی (رحمۀالله‌علیه) نیز در فرمان هشت ماده‌ای سال ۱۳۶۱ خطاب به مسئولین اجرایی و قضایی به صراحت دیدگاه خود را در خصوص رعایت موازین این موضوع حیاتی برای جامعه و مردم بیان داشته است. «هیچ کس حق ندارد به تلفن یا نوار ضبط صوت دیگری به نام کشف جرم یا کشف مرکز گناه، گوش کند و یا برای کشف گناه و جرم، شنود بگذارد و یا دنبال اسرار مردم باشد و تجسّس از گناهان غیر نماید، یا اسراری را که از غیر به او رسیده فاش کند. تمام این‌ها جرم و گناه است و بعضی از آن‌ها چون اشاعه فحشا و گناهان، از کبائر بسیار بزرگ است و مرتکبین هریک از امور فوق، مجرم و مستحقّ تعزیر شرعی هستند و بعضی از آن‌ها موجب حدّ شرعی می‌باشد (موسوی خمینی، روح الله، صحیفه نور، ج۱۷، ص۱۰۶، ۱۳۸۵، تهران، مؤسسه تنظیم و نشر آثار امام خمینی)

ب) ارتباطی

براساس قواعد حاکم بر این نوع حریم، هر شخص در برخی از انواع ارتباطات فردی و اجتماعی خویش می‌تواند جنبه‌هایی از سری بودن روابط و ارتباطات را از جامعه انتظار داشته باشد به نحوی که از دید عموم محفوظ مانده و افراد غیرمجاز حق تجسس و پایش و رهگیری آن‌ها را نداشته باشند. این نوع حریم شامل کلیه ارتباطات انسانس از قبیل پست عادی و پست الکترونیک، مکالمات تلفنی، تلگراف و... می‌شود. در این نوع حریم قواعدی حاکم است که چگونگی ارتباطات فیمابین اشخاص از طریق فیزیکی و الکترونیکی را تنظیم و تحت قاعده در می‌آورد(صادقی، حسین، مسئولیت مدنی در ارتباطات الکترونیک، ج۱، ص۱۱۷، ۱۳۸۸، تهران، میزان) اصل ۲۵ قانون اساسی جمهوری اسلامی ایران به رعایت حریم ارتباطی افراد در مکالمات تلفنی، الکترونیکی و نامه‌ها تصریح نموده است. مبتنی بر این اصل بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون.

ج) جسمانی

این‌گونه حریم خصوصی در باب حمایت از تمامیت جسمانی در مقابل هرگونه تعرض و تجاوز و نیز در مقابل آزمایش‌های ژنتیکی، دارویی و نظایر آن است. تمامیت جسمانی هر شخص اولین و مهم‌ترین داشته اوست که تجاوز به آن در همه نظام‌های حقوقی جهان با شدیدترین مجازات‌های کیفری مواجه می‌باشد و به همین دلیل کامل‌ترین حریم از جهت حمایتی، حریم جسمانی است(صادقی، حسین، مسئولیت مدنی در ارتباطات الکترونیک، ج۱، ص۱۱۷، ۱۳۸۸، تهران، میزان) تجاوز به حریم جسمانی افراد در تعالیم قرآنی منع شده و اعمال نامشروعی مانند زنا و لواط مورد نهی و حرمت قرار گرفته است. «وَ لاَ تَقْرَبُوا الزِّنَی إِنَّهُ کَانَ فَاحِشَةً وَ سَاءَ سَبِیلاً (اسراء/سوره۱۷، آیه۳۲)

متأسفانه امروزه برخی مدعیان دفاع از حقوق بشر با تمسک به حق حریم خصوصی به دنبال حرمت‌شکنی از این روابط نامشروع می‌باشند به طوری که در برخی کشورهای غربی و اخیراً در ایالات متحده به قانونی‌کردن روابط هم‌جنس‌خواهانه اقدام شده است. باید توجه داشت آزادی روابط جنسی در اجتماع نه تنها حق مشروعی برای انسان نیست بلکه در تزاحم با حقوق اجتماع و همچنین مغایر با حقوق الهی است.

د) مکانی

حریم خصوصی مکانی در واقع به قواعدی می‌پردازد که آرامش و آسایش شخصی را در یک مکان متعلق به خود تضمین می‌کند به نحوی که اطمینان حاصل نماید که هیچ‌کس نظاره‌گر وی در مکان مزبور نیست. به عبارت دیگر افراد این انتظار متعارف را از جامعه دارند که در نحوه استفاده از ملک خود آزادی کامل داشته باشند و از یک طرف هیچ‌کس به ملک مزبور متعرض نشود و از طرفی دیگر هیچ شخصی بر نحوه فعالیت در آن ملک نظارت و تجسس ننماید.

قرآن کریم در آیه ۲۷ و ۲۸ سوره نور می‌فرماید: «ای اهل ایمان هرگز به خانه‌ای غیر از خانه خودتان وارد نشوید مگر آن‌که با اهل آن خانه انس گیرید و (چون رخصت یافتید داخل شوید)، به اهل آن خانه سلام کنید و این برای شما بهتر است که متذکر شوید و اگر در خانه کسی را نیافتید وارد خانه نشوید، تا

به شما اجازه داده شود و اگر گفتند برگردید، برگردید که این برای پاکی شما بهتر است و خدا به هرچه می‌کنید، داناست.» چنان‌چه از شأن نزول این آیات نیز فهمیده می‌شود این آیات مؤمنان را به رعایت حریم خصوصی افراد در منازلشان امر می‌نماید.

عدّی بن ثابت می‌گوید علت نزول آیه چنین بوده که زنی از انصار نزد رسول خدا آمد و گفت: یا رسول‌الله، اوقات و حالاتی بر من می‌گذرد که نمی‌خواهم پدرم یا فرزندم مرا در آن اوقات و حالات ببینند، در صورتی که اینان هر وقت سرزده به خانه من می‌آیند و من از این حیث در زحمت و کراهت می‌باشم، بنابراین چه کاری می‌توانم بکنم؛ سپس این آیه نازل گردید (احدی، علی بن احمد، اسباب نزول القرآن، ج۱، ص۳۲۴، ۱۴۱۱ هق).

بند سوم: افترا و نشر اکاذیب

با گسترش ارتباطات و ترویج استفاده از رایانه ها و فضای مجازی، زمینه تازه ای برای اقدامات افراد سودجو و کلاهبردار، فراهم شده و جرائمی، تحت عنوان جرائم رایانه ای پدیدار شده اند. به همین دلیل قانون گذار با تصویب قانونی تحت عنوان «قانون جرائم رایانه ای» در سال ۱۳۸۸، اقدام به جرم انگاری برخی اعمالی که با استفاده از رایانه قابل تحقق هستند، نموده است.

اغلب افراد، بدون آگاهی از صحت اخباری که در تلگرام یا اینستاگرام به دست آن ها رسیده است، اقدام به بازنشر و ارسال آن برای دوستان و آشنایان خود می کنند. این افراد اغلب گمان می کنند، چون خودشان ایجاد کننده مطلب نبوده اند، در صورتی که مطلب منتشر شده کذب باشد، مسئولیتی متوجه آن ها نمی شود. در صورتی که این تصور درست نیست.

اگر ثابت شود، مطالب پخش شده، کذب بوده و فرد با قصد ضربه زدن به دیگری و با داشتن سوء نیت، اقدام به نشر آن در فضای مجازی کرده است، با وجود اینکه خودش تولید کننده آن نبوده، مطابق قانون، مجرم شناخته شده و به مجازات مندرج در قانون محکوم می شود. در ادامه، به بیان ماده قانونی و مجازات جرم انتشار دروغ در تلگرام و اینستاگرام و به طور کلی، نشر اکاذیب در فضای مجازی، می

پردازیم. در ماده ۱۸ قانون جرائم رایانه ای، به جرم تشویش اذهان عمومی و نشر اکاذیب به وسیله سامانه های رایانه ای اشاره شده که متن این ماده به شرح زیر است:

«هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی، به وسیله سامانه رایانه ای یا مخابراتی، اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد، اعمالی را بر خلاف حقیقت، راسا یا به عنوان نقل قول، به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یاد شده، به نحوی از انحاء، ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت (در صورت امکان)، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.» (سایت مشاوره حقوقی دینا)

بخش سوم: جرائم سایبری

توصیف رفتارهای انحرافی مرتبط با رایانه، اصطالحات گوناگونی از قبیل جرم رایانهای، تخلفات رایانهای، جرایم سایبر وجرایم مجازی وجود دارد که اغلب به جای یکدیگر مورد استفاده میگیرند و تمایز و تفکیکی در به کارگیری این اصطالحات وجود ندارد. (مک کواد،۲۰۰۶) جرایم سایبری به جرایمی گفته میشود که در محیطی غیر فیزیکی علیه فناوری اطالعات با حاالت شبیهسازی و مجازی سازی ارتکاب مییابد (بیابانی و همکاران، ۱۳۸۴)سایبر در اصطالح به همه چیزهایی گفته می شود که اساس فعالیت آنها بر مبنای پردازش و طبق سامانه صفر و یک کار میکنند (زندی، ۱۳۸۹)جرایم سایبری فعالیتهایی هستند که در آنها رایانهها، تلفنها و تجهیزات خانگی و سایر امکانات تکنولوژیک برای اهداف نامشروعی چون کلاهبرداری، سرقت، خرابکاری الکترونیکی، تجاوز به حقوق مالکیت افراد، سوء استفاده جنسی از زنان و کودکان و شکستن و وارد شدن به سیستمهای کامپیوتری و شبکهها مورد استفاده قرار میگیرد (Spper, ۲۰۰۰)فناوری اطالعات موجب تغییر در تعامل افراد با یکدیگر میشود وافراد همچنین به گونهای دیگر وقت خود را صرف میکنند و حتی میتوانند برای منفعت شخصی خود نیز از آن بهره مند شوند (Pole, ۲۰۰۷) .

بند اول: دو نسل از جرایم سایبری و ارتباط آن با دیپ فیک و هوش مصنوعی

الف) نسل اول جرایم سایبری با هدف سود مالی و یا تخریب اطلاعات محدود صورت گرفته است که شامل بمب و مت آمفتامین می شود.

ب) نسل دوم جرایم سایبری از طریق پیشرفت تکنولوژی صورت گرفته است، هدف آن تبهکاری و جرم و جنایت اینترنتی بوده است و سرقت از راه دور. این جرم شامل هک، انتشار پورنوگرافی، میشود. و نسل سوم جرایم سایبری که از پیشرفت تکنولوژی اینترنتی صورت گرفته، شامل: انتشار نرم افزارهای مخرب مانند ویروسها یا کرمهای تروجان می شود (Donner ۲۰۱۴,)جرایم سایبری، به فرد اجازه میدهد که ارتباطی گمنام برقرار کند (Higgins, ۲۰۰۹)از این رو، ویژگی مهم فضای سایبر از جمله عدم تماس چهره به چهره و عدم وجود پلیس و نهادهای نظارتی، باقی نماندن آثاری از رد پای مجرمین و آزادی بی حد و حصر در اینترنت شرایط مناسبی را برای مجرمان فراهم می سازد تا مرتکب جرم شوند. فضای سایبر شرایطی را به وجود آورده است که بزهکاران با کمترین هزینه و اضطراب، بیشترین خسارت و صدمه را به وجود آورند (باستانی، ۱۳۸۲) .حجم خسارات حاصله از جرایم سایبری بسیار زیاد است مثال: برای دستبرد زدن الکترونیکی به یک بانک یک نفر میتواند با نفوذ به سیستم بانک میلیاردها دالر پول الکترونیکی را به حساب خود یا دیگری انتقال دهد(کوشا؛ ۱۳۸۶.)نوع مجرمین سایبری اکثرا از طبقات روشنفکر و تحصیلکرده میباشند. سرعت وقوع جرم، تعداد زیاد بزهدیده در فضای سایبر از دیگر ویژگیهای جرایم سایبری است(جاللی فراهانی،۱۳۸۴) جرایم سایبری امروزه گسترش یافته است، سرقت هویت افراد، جنایات جنسی مثل پورنوگرافی کودکان، قاچاق جنسی انسان و حتی فحشا، کشف رمز عبور خصوصی و آزار و اذیت های اینترنتی از جمله جرایم در فضای مجازی می باشند و انسان ها از آن در امان نیستند (Donner, ۲۰۱۴) .

بند دوم: جرایم سایبری در ایران

در ایران بر اساس آمارهای موجود در سال۱۳۸۴ ، ۵۰ مورد پرونده مربوط به جرایم اینترنتی تشکیل شد که کشف جرایم آمار۵۰ درصدی را نشان می دهد. از مهمترین موارد سایبری در این سال، ۱۱ مورد سوء

استفاده از کارتهای اعتباری، ۳۲ مورد کلاهبرداری اینترنتی، ۷ مورد ایجاد مزاحمت از طریق اینترنت، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوعات متفرقه بوده است. با توجه به آمارهای سال ۸۴ میزان کشفیات مربوط به کلاهبرداری، جعل و سایر جرایم سایبری ۱۱درصد را نشان می دهد. در سال ۸۷ ، ۱۲۴هزار پرونده جرم سایبری در کشور موجود بود که افزایش ۲۶ درصدی نسبت به سال ۸۶ را نشان می داد. نسبت جرایم در ۸۷ نسبت به سال ۸۶ افزایش ۱۵۰ درصدی داشته است. از ۱۲۴هزارپرونده جرایم سایبری در سال ۸۷ ، ۲۶ درصد مربوط به دسترسی غیر مجاز به شبکههای رایانه های (هک) ۲۶ درصد مربوط به هتک حیثیت و نشر اکاذیب، ۷ درصد مربوط به تکثیر غیر مجاز نرم افزار، ۵ درصد مربوط به کالهبرداری، ۳ درصد مربوط به تخریب و اختالل سیستم ها و داده های رایانه ای و ۲۹ درصد نیز مربوط به موضوعات متعددی مثل اخاذی، تهدید و شناسایی سیستم های غیر مجاز مربوط میشود(امامی، ۱۳۸۹) در ایران بیش از ۴۵میلیون نفر کاربر اینترنت وجود دارد که ۲۳ میلیون نفر آنان جوانان هستند. بیشترین جرایم در ایران مربوط به کالهبرداریهای رایانهای، سرقتهای بانکی و نشر اکاذیب می باشند (.پلیس فتا؛ به نقل از، خبرگزاری تحلیلی ایران، ۱۶ خرداد ۱۳۹۳) . در سال ۳۱ برداشت غیرمجاز، ۱۳۹۵ درصد از جرایم سایبری در کشور را به خود اختصاص داده است.

نتیجه‌گیری

با توجه به سرعت پیشرفت تکنولوژی‌های دیپ‌فیک و هوش مصنوعی، چالش‌های حقوقی ناشی از این فناوری‌ها به موضوعی پیچیده و اضطراری در دنیای دیجیتال تبدیل شده است. این تکنولوژی‌ها به‌طور گسترده در بسیاری از حوزه‌ها مانند رسانه، تبلیغات، سیاست و حتی جنایت‌های سازمان‌یافته به‌کار می‌روند، و به همین دلیل، تهدیدات جدیدی در سطح جهانی ایجاد کرده‌اند. دیپ‌فیک، به‌ویژه، از توانایی ایجاد محتوای جعلی با کیفیتی شبیه به واقعیت برخوردار است که می‌تواند برای اهداف منفی مانند جعل هویت، تهدیدات سیاسی و اجتماعی، و حتی ایجاد شواهد کاذب در محاکم قضائی استفاده شود. همچنین، هوش مصنوعی در زمینه‌های مختلفی مانند حملات سایبری، هک‌های پیچیده، سرقت داده‌ها و تهدیدات امنیتی به‌طور روزافزون در حال گسترش است.

این فناوری‌ها در کنار مزایای خود، تهدیدات زیادی به همراه دارند که نظام‌های حقوقی و قضائی قادر به مقابله با آن‌ها نیستند. یکی از مهم‌ترین مشکلات در این زمینه، دشواری شناسایی متخلفان و اثبات جرم است. در بسیاری از موارد، محتوای جعلی به‌راحتی قابل تولید و انتشار است، اما شناسایی منبع و هویت واقعی تولیدکنندگان آن، به دلیل ویژگی‌های خاص دیجیتال و ناشناسی فضای اینترنت، بسیار پیچیده است.

در این شرایط، مبارزه با این تهدیدات نیازمند یک رویکرد جامع است که در آن، قوانین حقوقی جدید و به‌روز برای مقابله با جرایم مرتبط با این فناوری‌ها تدوین و به اجرا درآید. همچنین، لازم است که ابزارهای پیشرفته برای شناسایی محتوای جعلی و مقابله با حملات سایبری توسعه داده شوند. این امر تنها از طریق همکاری‌های بین‌المللی و هماهنگی میان کشورها و نهادهای مختلف ممکن است. در این راستا، سازمان‌های دولتی و غیردولتی باید به‌طور فعال در ایجاد و اجرای این قوانین و فناوری‌ها همکاری کنند تا از بروز آسیب‌های گسترده‌تری در آینده جلوگیری شود.

علاوه بر این، نیاز به آموزش و آگاهی‌رسانی عمومی نیز به‌شدت احساس می‌شود. بسیاری از کاربران اینترنت هنوز از خطرات و تهدیدات ناشی از این فناوری‌ها آگاه نیستند و در نتیجه، بیشتر در معرض آسیب‌پذیری قرار دارند. بنابراین، برنامه‌های آموزشی و آگاهی‌دهنده در مورد نحوه شناسایی و برخورد با محتوای جعلی و تهدیدات سایبری می‌تواند تاثیر زیادی در کاهش آسیب‌ها داشته باشد.

در نهایت، برای ایجاد یک فضای دیجیتال امن و حقوقی پایدار، لازم است که قوانین و مقررات موجود با سرعت و دقت به‌روز شوند، تا بتوانند از تهدیدات ناشی از تکنولوژی‌های نوظهور به‌طور موثر جلوگیری کنند و متخلفان را تحت تعقیب قرار دهند. این مسئله نیازمند توجه ویژه دولت‌ها، شرکت‌های فناوری و جوامع بین‌المللی است تا همکاری‌های لازم برای ایجاد یک نظام حقوقی و امنیتی قوی در برابر این تهدیدات انجام گیرد.

با توجه به پیشرفت تکنولوژی و شناختن جرائم دیپ فیک و هوش مصنوعی این مقاله در ذیل به چند راهکار و پیشنهاد جهت پیشگیری جرم مذکور پرداخته است :

- تقویت قوانین سایبری و به‌روز رسانی آن‌ها: برای مقابله با چالش‌های حقوقی ناشی از استفاده از دیپ‌فیک و هوش مصنوعی در ارتکاب جرایم، لازم است که قوانین ملی و بین‌المللی در زمینه جرایم سایبری به‌روزرسانی شوند. این امر به خصوص در زمینه‌های شناسایی و مقابله با جرایم جدید ناشی از این فناوری‌ها ضروری است.

- آموزش و آگاهی عمومی: ترویج آگاهی عمومی از خطرات دیپ‌فیک و هوش مصنوعی در ارتکاب جرایم سایبری می‌تواند به کاهش آسیب‌های احتمالی کمک کند. این آموزش‌ها باید شامل نحوه شناسایی اطلاعات جعلی و نحوه محافظت از خود در برابر تهدیدات سایبری باشد.

- توسعه ابزارهای تشخیص هوش مصنوعی و دیپ‌فیک: استفاده از فناوری‌های پیشرفته برای شناسایی محتوای جعلی و نظارت بر فعالیت‌های مشکوک در فضای دیجیتال می‌تواند ابزار موثری برای مبارزه با جرایم سایبری باشد. این ابزارها باید به‌طور مداوم به‌روز شوند تا با تغییرات تکنولوژی همگام باشند.

- تقویت همکاری‌های بین‌المللی: با توجه به جهانی بودن فضای اینترنت و استفاده گسترده از فناوری‌ها در سراسر جهان، لازم است که کشورها همکاری‌های بیشتری در زمینه مبارزه با جرایم سایبری داشته باشند. این همکاری‌ها می‌توانند شامل به اشتراک‌گذاری اطلاعات، هماهنگی قوانین و اقدامات مشترک در برابر تهدیدات سایبری باشند.

- نظارت دقیق‌تر بر شرکت‌های فناوری: دولت‌ها باید نظارت‌های بیشتری بر شرکت‌های توسعه‌دهنده فناوری‌های دیپ‌فیک و هوش مصنوعی اعمال کنند تا از سوءاستفاده از این فناوری‌ها در ارتکاب جرایم جلوگیری کنند. این نظارت‌ها باید شامل الزام به رعایت اصول اخلاقی و امنیتی در طراحی و استفاده از این فناوری‌ها باشد.

و در آخر کلام جهت جمع بندی مطالب فوق پژوهش حاظر ، استفاده از تکنولوژی‌های دیپ‌فیک و هوش مصنوعی در ارتکاب جرایم سایبری به‌طور جدی چالش‌های حقوقی و اخلاقی زیادی را ایجاد کرده است. از یک سو، این فناوری‌ها تهدیدات جدیدی در زمینه امنیت سایبری و اطلاعات شخصی ایجاد کرده‌اند و از سوی دیگر، شناسایی و مجازات مرتکبین جرایم مرتبط با آن‌ها به دلیل پیچیدگی و تغییرپذیری سریع این فناوری‌ها دشوار شده است. به‌منظور مقابله با این چالش‌ها، به‌روز کردن قوانین، تقویت نظارت‌ها، و ایجاد آگاهی عمومی می‌تواند از جمله راه‌حل‌های موثر در این زمینه باشد.

منابع و مآخذ

الف) فارسی

۱. قرآن کریم

۲. نهج البلاغه

۳. محمدی فردوئی،عطاالله . (۱۳۹۷). بررسی جزایی عناصر بزه جعل رایانهای در حقوق ایران. قانون یار،۴۵۹- ۴۷۶، (۸)- ۲

۴. گرایلی ، محمدباقر.(۱۳۸۹) . بررسی جعل و تخریب و اخلال رایانه ای . آموزه های حقوق کیفری , ۷(۱۴) , ۱۸۸_۱۵۹.

۵. محسنی ، فرید . (۱۳۸۹) ؛ حریم خصوصی اطلاعات . مطالعه کیفری در حقوق ایران

۶. کاتوزیان، ناصر، (۱۳۸۶)، الزام‌های خارج از قرارداد (ضمان قهری)، تهران: انتشارات دانشگاه تهران

۷. شهید ثانی، زین‌الدین عاملی،ج۲، ص۵۹، ۱۴۱۰هجری قمری

۸. نوری و نخجوان، حقوق حمایت داده‌ها، ج۱، ص۳۴، ۱۳۸۳، تهران، گنج دانش

۹. صادقی، حسین، مسئولیت مدنی در ارتباطات الکترونیک، ج۱، ص۱۱۷، ۱۳۸۸، تهران، میزان

۱۰. احدی، علی بن احمد، اسباب نزول القرآن، ج۱، ص۳۲۴، ۱۴۱۱ هجری قمری

۱۱. زندی، محمدرضا، ۱۳۸۹، تحقیقات مقدماتی در جرائم سایبری، چاپ اول، تهران، انتشارات جنگل

۱۲. جعفر کوشا، ۱۳۸۶ جرایم رایانه ای در بستر تجارت الکترونیکی، چاپ سوم، تهران، انتشارات خرسندی

۱۳. بیابانی، غالم حسین و هادیانفر، سید کمال، ۱۳۸۴، فرهنگ توصیفی علوم جنایی، چاپ اول، تهران، انتشارات مرکز تحقیقات کاربردی کشف جرایم و امنیت معاونت آگاهی ناجا.

۱۴. رومند باستانی، جرایم کامپیوتری و اینترنتی جلوه ای از بزهکاری، مجله تحقیقات حقوقی، ؛ ۱۳۸۹

۱۵. مامی، حسن، بررسی ابعاد جرایم اینترنتی، مطالعات بین المللی پلیس، شماره ۱۳۸۹، ؛ ۳۶-۱

۱۶. .(هوسمن، کارل(ترجمه داوود حیدری۱۳۷۰ ؛ ص ۴۲)

۱۷. قانون مجازات اسلامی

۱۸. قانون جرائم رایانه ای

ب) لاتین

Donner, Christopher M. Marcum b, Catherine D. Jennings c, Wesley G. Higgins d, George E. Banfield, Jerry.

(۲۰۱٤). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital

piracy. Computers in Human Behavior. ۳٤ (۲۰۱٤) ۱٦٥_۱۷

۱. *Poole, Dawn (۲۰۰۷). A Study of Beliefs and Behaviors Regarding Digitalv Technology. New Media & Society. ۱۹(٥): ۷۷۱_۷۹۳.*

۲. -Spper. D(۲۰۰۰). R edefining borders: The challenges of cyber crime. Marquette university. Political science department. Crime. Law & Social change. ۲٤- ۳٤.

۳. Mcquade, S.C.(۲۰۰٦). Understanding and Managing Cybercrime. Boston. MA: Pearson.

٤. Finck, M. (۲۰۲۰). "Regulating AI and Deepfakes: Legal Challenges and Solutions." Journal of Technology in Society, ۱۳(۲), ۹۳-۱۰٥

٥. Kietzmann, J. H., & Angell, I. (۲۰۲۱). "Deepfakes: A New Threat in the Digital Era." Business Horizons.

ج) سایت

۱. ویکی پدیا

۲. موسسه حقوقی منشور دیدگاه سوم . daadappir@gmail.com

۳. مشاوره حقوقی دینا

لوگو سازمان ها و نهادهای علمی، سیاسی و دولتی حامی معنوی

هفتمین همایش ملی پژوهش‌های علمی علوم اسلامی و انسانی در عصر نوین