

نقش دولت با محوریت قرآن در پیشگیری از جعل هویت رایانه‌ای در فضای مجازی

عاطفه حسینی فرد*

تاریخ دریافت: ۹۷/۲/۸

نقیسه نکویی مهر**

تاریخ پذیرش: ۹۷/۵/۱۳

محمد جواد عبداللهی***

چکیده

مهم‌ترین مسأله در مقابله با جرایم سایبری پیشگیری اجتماعی است که از جمله راهکارهای پیشگیری از جرایم رایانه‌ای محسوب می‌گردند و همچنین تهیه پیش‌نویس قانون مبارزه با جرائم رایانه‌ای که در دستور کار قوه قضاییه، مجلس و دولت قرار گرفته است. با توجه به این امر موفقیت هر سیاستی اهتمام به آموزش خانواده و آموزش کودکان و نوجوانان، تربیت نیروی انسانی متخصص در مقابله با این جرایم و در نهایت سازماندهی جدید نیروی انتظامی و قوه قضاییه برای تأسیس پلیس سایبر و دادسرای جرایم سایبر است. این تحقیق از نوع کاربردی و روش انجام تحقیق توصیفی-تحلیلی است. این پژوهش با توضیح مختصری پیرامون مفاهیم، نظریه‌های مرتبط با جرم جعل هویت اشاره و رویکردها و کارکردهای پیشگیری وضعی را مورد کنکاش قرار داده است و مهم‌ترین راهبردهای سیاستگذاری اجتماعی در حوزه فضای مجازی با رویکرد پیشگیری وضعی را مورد بحث قرار می‌دهد، و سرانجام با پرداختن به حق استفاده شهروندان از فضای مجازی از منظر قرآن به این مهم دست یافته شده است که دولت باید با توجه به تأکید آیات قرآنی، فرهنگ استفاده از فضای مجازی را در کشور نهادینه سازد تا بتواند گامی در جهت کاهش جرایم رایانه‌ای بردارد.

کلیدواژگان: فضای مجازی، نظارت، جعل هویت، دولت، پیشگیری، آیات قرآن.

* دانشجوی دکتری، گروه فقه و حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

atefehoseinifard@gmail.com

** دانشجوی دکتری، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

*** عضو هیأت علمی، گروه حقوق، واحد خمینی شهر، دانشگاه آزاد اسلامی، خمینی شهر، ایران.

نویسنده مسئول: عاطفه حسینی فرد

مقدمه

یکی از بزرگ‌ترین چالش‌های فضای مجازی (به خصوص در ایران) هویت نامشخص بسیاری از کاربران و به تعبیری هویت جعلی آنان است. با این هویت جعلی ارتباطات جعلی شکل می‌گیرد! این خطر بزرگی برای امنیت جامعه سایبری ماست. به همین جهت می‌شود ادعا کرد که اولین و مهم‌ترین شاخص اخلاق در فضای مجازی، هویت واقعی است چراکه با همین هویت است که ارتباطات بعدی ما شکل می‌گیرد و اگر این هویت دروغین باشد ارتباطات ما هم دروغین خواهد بود. البته بسیاری از شبکه‌های اینترنتی مثل توئیتر و فیسبوک، آمادگی بررسی هویت حقیقی کاربران از طریق دریافت برخی مدارک شناسایی را دارند اما قسمت عمده کاربران از این ویژگی استفاده نمی‌کنند. برخی وبگاه‌های فارسی نظیر تبیان و دونیت هم تلاش‌های مشابهی را برای تأیید هویت کاربران خود انجام داده‌اند.

در کنار اهمیت هویت واقعی، مسأله‌ای به نام «سرقت هویت» هم مطرح می‌شود. سرقت هویت یعنی کسی بدون اجازه دیگری از هویت او در فضای مجازی استفاده کند. سرقت هویت هم باعث کاهش امنیت در فضای مجازی می‌شود. نمونه‌های گسترده‌ای از این دست هم در بین ایرانیان یافت می‌شود. البته اگر بگوییم در ایران استفاده از هویت جعلی و آدرس‌های آی پی تقلبی به خاطر استفاده از ابزارهایی نظیر فیلترشکن‌ها رایج است اما سرقت هویت دیگر هیچ راه توجیهی ندارد. یادمان باشد که اعلام هویت درست و حقیقی در فضای اینترنت، علاوه بر اینکه به اعتماد دیگران درهم‌تنیدگی بیش‌تر و امن شدن جامعه مجازی منجر می‌شود، به خود ما نیز کمک می‌کند تا اطرافیان حقیقی را سریع‌تر بیابیم و کنترل بیش‌تری بر روابط مجازی خود داشته باشیم. می‌شود ادعا کرد که اولین و مهم‌ترین شاخص اخلاق در فضای مجازی، هویت واقعی است. چراکه با همین هویت است که ارتباطات بعدی ما شکل می‌گیرد و اگر این هویت، دروغین باشد ارتباطات ما هم دروغین خواهد بود. همه ما در زندگی حقیقی خودمان با مجموعه‌ای از ارتباطات مواجه هستیم و خودمان هم یکی از ذرات تشکیل دهنده این تار ارتباطی هستیم. ما روزانه با اعضای خانواده و دوستان و حتی با افرادی که خیلی از ما دور هستند در ارتباط هستیم و همین ارتباط شالوده و پایه اجتماع انسانی ماست. در فضای

مجازی هم ارتباطات ماست که تشکیل‌دهنده شبکه‌ها، گروه‌ها، اجتماعات مجازی و به طور کلی هر نوع فعالیت مجازی می‌شود. همان‌طور که در ارتباطات عالم حقیقی، هویت ما به عنوان یکی از ارکان مهم ارتباط و یا حتی شاید مهم‌ترین رکن به کار می‌آید، در فضای مجازی نیز هویت مجازی ما نقش اساسی در ارتباطات دارد. این هویت، خواه حقیقی و خواه مجازی، می‌تواند شامل مشخصات زیادی نظیر نام، نام خانوادگی، شماره تلفن همراه، آدرس، کد پستی، نام مدرسه دوران کودکی و... باشد. بر اساس همین هویت است که ما از دیگران تشخیص داده می‌شویم و آشنایان خود را یافته و ارتباطات خود با آنان را سامان می‌دهیم. بارها خودتان با استفاده از همین هویت در مدرسه یا دانشگاه ثبت نام کرده‌اید، خود را به دیگران معرفی کرده‌اید و حتی آنان را برای ارتباط با خود ترغیب کرده‌اید. در فضای مجازی هم هر فرد با یک هویت معین، خود را به دیگران معرفی می‌کند و در شبکه‌های اجتماعی و گروه‌ها ثبت نام می‌کند. در اینترنت هیچ کس بدون هویت نیست و حتی در وب گردی از طریق شناسه‌ای عددی که به آن آدرس آی پی گفته می‌شود معرفی می‌شود اما هنگامی که بخواهد از این سطح معمولی فراتر رفته و ارتباطات مجازی‌اش را از طریق شبکه‌ها و در گستره وب جهانی شکل دهد، لازم است تا این هویت بیش از پیش مشخص باشد. همان‌طور که برای ثبت یک رایانامه معمولی در گوگل یا یاهو لازم است تا نام، نام خانوادگی و شماره تلفن خود را اعلام کنید. این‌ها به جامعه مجازی ما کمک می‌کند تا در هم تنیده‌تر و امن‌تر باشد.

دو معنای اصلی هویت، تمایز و تشابه مطلق است (جنکینز، ۱۳۹۱: ۵). هویت را این‌گونه تعریف می‌کنند: هویت ریشه در زبان لاتین و دو معنای اصلی دارد. اولین معنای آن مفهوم تشابه مطلق را بیان می‌کند؛ این با آن مشابه است. معنای دوم آن تمایز است که با مرور زمان سازگاری و تداوم را فرض می‌گیرد. به این ترتیب، به مفهوم شباهت از دو زاویه مختلف راه می‌یابد. مفهوم هویت، هم‌زمان میان افراد یا اشیاء دو نسبت محتمل برقرار می‌سازد؛ شباهت و تفاوت. هویت داشتن یعنی یگانه بودن، ولی از دو جنبه متفاوت: همانند دیگران بودن در طبقه خود و همانند خود بودن در گذر زمان. از طرفی، فضای سایبر با برخورداری از ویژگی‌های منحصر به فردی چون بدون مرز بودن، امکان هنجارشکنی را به تمامی نقاط دنیا گسترش داده است.

همچنین با گمنام‌سازی کاربرهای سایبری، امکان شناسایی هویت هنجارشکنان، تعقیب و پیگرد آن‌ها را با مشکلات جدی مواجه کرده است. بنابراین ضرورت دارد فضای سایبر را تبیین نموده و سعی داریم راهکارهای الزامی و ضروری پیشگیری از جرم در فضای مجازی را جهت سیاستگذاری اجتماعی ارائه نموده و به این سوالات پاسخ دهیم:

۱. جرم جعل هویت چیست و انواع آن کدام‌اند؟ ۲. پیشگیری وضعی، کارکردها و رویکردهای آن کدام‌اند؟ همچنین در این نوشتار نیز با تبیین آیات قرآنی مشخص گردیده است که استفاده از فضای مجازی جزئی از حقوق شهروندی است و دولت باید با آموزش شهروندان و بالابردن فرهنگ استفاده از فضای مجازی گامی در راستای کاهش جرایم رایانه‌ای بردارد.

۱. پیشینه پژوهش

در بیان پیشینه پژوهش می‌توان گفت به طور کلی هیچ یک از تحقیقات تجربی پیشین به طور خاص به بررسی نظارت دولت (نیروی انتظامی به‌خصوص پلیس فتا) نپرداخته است. در این مقاله با توجه به مراجعه به سازمان کتابخانه ملی، کتابخانه دانشگاه آزاد، کتابخانه دانشگاه علوم انتظامی، سایت‌های مگیران، مطالعه پایان‌نامه‌ها و مقالات مرتبط، تحقیقاتی که به مطالعه نظارت دولت جهت پیشگیری جرم جعل پرداخته اشاره شده است.

/خگری (۱۳۸۸) به توصیف جرم جعل هویت در فضای مجازی پرداخته است و با بیان اینکه بیش‌ترین مجرمان از جوانان تشکیل شده‌اند به پیشگیری از جرم از جهت آگاه‌سازی جوانان پرداخته است.

سبحانی‌جو (۱۳۸۳) به توصیف جرم جعل به عنوان بحران پیش روی جامعه پرداخته و از این رو نقش دولت در پیشگیری از این جرم را حائز اهمیت شمرده است.

دوران (۱۳۸۳) برای پیشگیری از جرایم رایانه‌ای نقش آگاه‌سازی خانواده‌ها و جوانان را مهم برشمرده و نیز طی بررسی‌های به عمل آمده مشخص شده بیش از ۷۸ درصد خانواده‌ها از جرایم رایانه‌ای بی‌خبر هستند و باید آگاه‌سازی رخ دهد.

معینی (۱۳۸۴) به بررسی پیشگیری وضعی از جرایم رایانه‌ای پرداخته است.

فضلی (۱۳۸۹) برای مبارزه با مجرمان به بررسی قوانینی که در خصوص جرایم رایانه‌ای وجود دارد پرداخته و لزوم کامل‌سازی قوانین در این راستا را مورد بررسی قرار داده است.

جلالی‌فراهانی (۱۳۸۶) به تدابیر امنیتی برای مبارزه با این جرم پرداخته است. از منابع دیگر در این تحقیق در جهت تعیین و نقش جرم جعل هویت در فضای مجازی استفاده شده است.

مبانی مفهومی تحقیق

الف) فضای مجازی و هویت

اینترنت دارای قابلیت است که به واسطه آن افراد می‌توانند خودهای جدیدی را در دنیاهای جدید بسازند. این امور ممکن است در دنیای مادی اصلاً وجود خارجی نداشته باشند یا فرد به زعم خودش قادر به دستیابی به آن نباشد. این‌ها استفاده از فضای مجازی را برای کاربران جذاب‌تر می‌کند. بدین ترتیب، وب به مکانی برای معرفی و نمایش شخصیت فرد تبدیل می‌شود. البته قضیه به همین جا ختم نمی‌شود؛ زیرا امکان دارد که تصویر ارائه‌شده از سوی یک فرد بر روی وب، توسط دیگران به صورت‌هایی غیر از شکل مورد نظر وی تفسیر شود (اسلوین، ۱۳۸۰: ۱۵۶). حتی امکان معرفی خود در سایت‌های مختلف به صورت‌های گوناگون وجود دارد. به طوری که افراد بتوانند در جربان ارتباط‌گیری «هویت الکترونیک چندگانه‌ای» برای خود بسازند و هر بار خود را به یک صورت نشان دهند. تلویزیون و سایر رسانه‌ها فاقد این ویژگی خاص فضای مجازی‌اند. در مجموع، هویت اینترنتی یا هویت مجازی با دیدگاه‌های متعارف درباره هویت جور نیست. دیدگاه‌های متعارف درباره هویت به دنبال کلیت‌سازی درباره مفهوم هویت و یکپارچه نشان دادن آن هستند و تأثیر کلی آن را بر فرد در نظر می‌گیرند (بل، ۲۰۰۱: ۱۱۴). اما با این اوصاف در فضای مجازی استفاده از چنین تعاریفی برای هویت دشوار می‌شود و با گسترده‌تر شدن مرزهای هویتی، مرزبندی هویت واقعی و تخیلی در اینترنت محدود می‌شود به هر حال، اینترنت و شبکه‌های اجتماعی اینترنتی محصول درهم شکستگی هستی‌شناختی و پیچیده‌تر شدن فزاینده تفاوت‌های فردی هستند و با

آن سنخیت تام دارند. امروزه حتی اعضای خانواده‌ها و همسایگان نیز به ندرت معنای واحدی از هویت در ذهن دارند. این امر تشخیص اصالت‌ها را روز به روز دشوارتر می‌سازد. آلن تورن به خوبی این شرایط به ظاهر تناقض‌آمیز انسانی را توصیف کرده است: «ما در سکوت زندگی می‌کنیم، در شلوغی به سر می‌بریم، منزوی هستیم، در دریای خلق گم شده‌ایم» (تورن، ۱۳۸۰: ۱۶۰). از این حیث، هویت مجازی را می‌توان با فرایند اساساً مدرن تشکیل هویت به وسیله خویشتن و رسیدن به فهمی از خود و هویت‌یابی مربوط دانست. فرد در دوره مدرنیته از جا کنده می‌شود و اضطراب‌های وی افزایش پیدا می‌کند. اینترنت نه تنها این وضع را متحول کرد؛ بلکه به آن شدت بخشید. در اینجا ساختار و فردیت به هم می‌رسند و توأم‌اً مهم‌ترین جنبه پست‌مدرنیستی اینترنت را می‌سازند.

امکانات موجود برای انتخاب انواع متفاوت خروجی‌های اینترنت نه تنها فردیت کاربران را تقویت می‌کند؛ بلکه موجب تکثر بیش‌تر می‌شود. در عین حال، هم‌زمان با افزایش میزان تفاوت‌ها در اثر رشد استفاده عمومی از اینترنت، جهان‌بینی‌های افراد واگراتر می‌شود (گیبیز و ریمر، ۱۳۸۸: ۷۸). اینترنت شبیه یک بازار ارتباطی است و همین به تکثر هویتی و رشد فردیت کمک می‌کند و اشکال ابراز وجود شخصی را متنوع‌تر می‌کند، اما در عین حال نمی‌توان از این ایراد چشم‌پوشی کرد که وسایل ارتباطی به تدریج نقش فزاینده‌ای در سست کردن انسجام اجتماعات واقعی و ذره‌ای کردن جوامع انسانی دارد. همچنین اینترنت باعث رشد یک فرهنگ شخصی شده و حاصل تخیلات و تصورات و پندارهای فردی است. این امر به قیمت کاهش نفوذ کلیت‌های سیاسی بر هویت‌سازی‌های فردی تمام می‌شود و می‌تواند به شکل‌گیری منابع جدید هویتی بینجامد (معینی‌علمداری، ۱۳۸۴: ۱۱۶-۱۱۵). علاوه بر اینترنت، شبکه‌های اجتماعی مجازی همچون فیسبوک، به دنبال ایجاد جوامع مجازی هستند. این جوامع مجازی بر اساس ساختار و تعاریف خود به طبع دارای ارزش‌های مختلف فرهنگی، سیاسی و اجتماعی هستند. به طوری که این جوامع مجازی توانسته‌اند مفاهیمی چون «دوست»، «ارتباط»، «خانواده»، «هویت» و حتی مسائلی جزئی مانند نحوه احوالپرسی کردن را بازتعریف کنند. اگرچه کاربران خود در شکل‌دهی این جوامع نقش چشمگیری ایفا

می‌کنند اما قوانین این جوامع مجازی و گفتمان حاکم بر آنان در تأثیرگذاری و شکل‌دهی هویت اعضای خود نقش مهمی ایفا می‌کنند. ابتدایی‌ترین تأثیر شبکه‌های اجتماعی اینترنتی بر کاربران این است که هویت فعلی او را به چالش می‌کشند؛ ابتدا کاربر را از خود واقعی تهی می‌کنند و سپس به او فرصت می‌دهند خود ایده‌آلش را بروز دهد، در حالی که به طور ناخودآگاه، این خود جدید در فضای گفتمانی شبکه‌های اجتماعی برساخته شده است. شبکه‌های اجتماعی صحنه‌ای فراهم می‌آورند که کاربران می‌توانند از هر جنسیت، سن، طبقه اجتماعی، نژاد و قومیتی که باشند، در آن ظاهر شوند و نقش دلخواه خود را بازی کنند. در این سطح، شبکه‌های اجتماعی مجازی، کاربر را به هویتی فردمدار شده با مشخصات منحصر به فرد سوق می‌دهند (خلقتی، ۱۳۸۷: ۹). در واقع با شبکه‌های اجتماعی مجازی این قابلیت به فرد داده می‌شود تا خود را هر گونه که می‌خواهد، فراتر از هویت واقعی خود در جهان فیزیکی بازتعریف و روایت کند. بنابراین با قبول این فرض که شبکه‌های اجتماعی اینترنتی در درون جامعه مصرفی خلق شده‌اند، خود منشأ بازتولید مکرر چنین جامعه‌ای می‌شوند. ریچارد بارتل (۲۰۰۴: ۱۶۴) اینگونه استدلال می‌کند که دنیاهای مجازی برای مردم آینه‌ای را فراهم می‌آورند که هرچه فرد تصویر خود را در آن مأنوس‌تر با خود واقعی یا ایده‌آلش بیابد، بیش‌تر با آن ارتباط برقرار می‌کند. در واقع، راز موفقیت و جذب کاربر برای وبسایت‌های عمده این است که کاربر خود را در آینه جهان مجازی پیش رویش ببیند. بدین ترتیب، در باب هویت در دنیای مجازی، مسأله این است که کاربر چه میزان انعکاس تصویر خود را در این آینه می‌پسندد. زمانی این تلقی وجود داشت که هویت افراد در فضای مجازی، هویتی ناشناخته و چندگانه است، اما اکنون کاربران ادامه هویت تعریف‌شده خود در فضای مجازی را به صورت آفلاین پی می‌گیرند و یا در فعالیت‌های آفلاین در بسیاری از مواقع برای خود نام و نشان تعریف می‌کنند و با آن همزادپنداری زیادی دارند (عاملی، ۱۳۸۸: ۷). بنابراین، معادلات پیشین هویت دچار تحول شده است. بدین ترتیب، بازتعریف هویت فردی و اجتماعی در فضای مجازی در ابعاد گوناگون قابل بررسی است. در این فضا، همگرایی جامعه مصرفی و تخصص حرفه‌ای تولیدکنندگان و تجار به بازآفرینی مفاهیم انسانی چون بلوغ، سن و مراحل مختلف زندگی انجامیده است.

شاید این تعجب‌برانگیز باشد که مفاهیم انسانی با ابعاد زیست‌شناختی مانند بلوغ نیز در دنیای مجازی تعبیر جدید بیابند، اما ریشه استحاله این مفاهیم ناشی از تأثیرگذاری قوی فضای مجازی بر نوع تفکر کاربران است (کاتز و مارشال، ۲۰۰۶). همان‌گونه که *بارتل* (۲۰۰۴) خاطر نشان می‌کند: «هویت، حاصل تفکر است که در قالب‌های گوناگون (در عمل یا در قالب لغات) ظهور می‌کند» و با توسعه عرصه مجازی زندگی بشر، این حقیقت غیر قابل انکار است که این فضای مجازی با کاربرد ارتباطی دوسویه قرار دارد؛ نحوه تفکر او را تحت تأثیر قرار می‌دهد و در مقابل گستره وسیعی را فراهم می‌آورد که کاربر هویت خود را در آن بر اساس ترجیحات خود ابراز می‌کند و به منصفه ظهور می‌رساند. به عبارت دیگر، فضای مجازی امروز تنها آیینه منعکس‌کننده کاربر مقابل خود نیست، بلکه تا حد زیادی چگونگی کیفیت کاربر خود را نیز تعریف می‌کند. زمانی، تلقی منتقدین فرهنگی این بود که چون فضای مجازی عرصه‌ای است که مهندسان فنی و نه مهندسان فرهنگی آن را ساخته‌اند، بنابراین نقطه ضعف آن عدم وجود روایت است (بل و کندی، ۲۰۰۰). اما امروز دنیای مجازی آن‌چنان با زندگی و فرایند هویت‌سازی بشر درآمیخته است که نه تنها روایت‌های بی‌شمار در آن قابل درک است، بلکه این روایت‌ها بر روایت دنیای واقعی پیشی گرفته‌اند؛ چنان‌که بودریار از «فراواقعیت» مجازی سخن می‌گوید و به قول *آنجل آدریان* (۲۰۰۸: ۳۶۶)، همان‌قدر که تجارت الکترونیک از تجارت جدا نیست، هویت‌های الکترونیکی در فضای مجازی نیز از هویت‌های واقعی قابل بازشناسایی نیستند.

ب) فضای مجازی و بحران هویت در ایران

در بررسی بحران هویت ناشی از فضای مجازی شبکه‌های اجتماعی در ایران، نمی‌توان بحران‌های هویتی ناشی از دوران گذار جامعه ایران را نادیده گرفت. به اعتقاد نگارندگان، جامعه ایران امروز با دو گونه بحران هویتی با دو منشأ و علل مختلف رو به رو است. مطالعات گسترده در خصوص بحران‌های دوران صنعتی شدن در جوامع مختلف نشان می‌دهد این گونه جوامع در معرض بحران‌های ناشی از تغییرات ساختاری در عرصه‌های اقتصادی، فرهنگی، سیاست و اجتماع قرار می‌گیرند. جامعه امروز ایران در

عین حال که بحران‌های هویت ناشی از یک دوره تاریخی را با خود حمل می‌کند، در سه دهه اخیر با بحران‌های دوره تاریخی فراصنعتی بدون آنکه به طور طبیعی وارد این دوره شده باشد نیز رو به رو شده است. با توجه به خاصیت و کارکردهای فناوری‌های نوین ارتباطی به خصوص شبکه‌های اجتماعی، ورود آثار کنترل‌ناپذیر و بحران زای این دوره از سوی حاکمیت به سهولت صورت گرفته و عواقب ناشی از آن وارد جامعه امروز شده است. این شرایط در مجموع وضعیتی را پدید آورده است که می‌توان گفت در حال حاضر، با نوعی از بحران‌های هویت هم‌پوشان مواجه هستیم. استفاده از اینترنت و این اواخر مخصوصاً شبکه‌های اجتماعی در میان ایرانی‌ها به طور قابل توجهی افزایش یافته و بررسی‌ها نشان می‌دهد این روند کماکان ادامه دارد (دوران، ۱۳۸۳: ۳). اینترنت، به ویژه در میان جوانان ایرانی شیوع زیادی دارد و فاصله آن با سایر نسل‌های قدیم‌تر فاحش می‌باشد. بنابراین، عجیب نیست که بیش‌تر تحقیقات انجام‌شده در مورد اینترنت نشان می‌دهد اکثریت کاربران اینترنت در ایران به نسل جوان تعلق دارد؛ بنا بر یک تقسیم‌بندی نسلی، نسل سوم بیش‌ترین کاربران اینترنتی در ایران بوده و بیش از نسل‌های دیگر در معرض آثار ناشی از اینترنت، از جمله مسائل هویتی و بحران هویتی قرار می‌گیرند. فارغ از شکاف‌های به وجود آمده ناشی از فرایند رسانه‌های نوین، شکاف نسلی موجود ناشی از تحولات ساختاری و جمعیتی جامعه ایران باعث شده است انتقال ارزش‌ها و آموزه‌ها در قالب سنت از نسلی به نسل دیگر با اختلال رو به رو شود. این پدیده از یک سو، به روند انتقال فرهنگ آسیب می‌رساند و از سوی دیگر، حافظه تاریخی را مختل می‌سازد و بدین ترتیب، انتقال تجربیات سیاسی و فرهنگی دوره‌های پیشین به زمان حاضر با دشواری انجام می‌شود (ربیعی، ۱۳۸۷: ۱۶۶-۱۶۵). یکی از ویژگی‌ها و نیازهای ضروری جامعه جوان ایرانی، کسب هویت اجتماعی (دینی و ملی) است و هویت اجتماعی جوانان، در صورتی کسب می‌شود که نظام اجتماعی از طریق نهادهای واسط خانواده، مدرسه، رسانه‌های جمعی و دولت، زمینه‌های لازم را برای کسب هویت اجتماعی آنان فراهم کند. در این صورت، آحاد جامعه نسبت به نظام اجتماعی خود، احساس هویت اجتماعی خواهند کرد و به طور طبیعی، گرایش‌های آنان که به سه سطح ایستاری (شناختی و ارزشی)، کنشی (هنجاری و رفتاری) و نمادی (ظاهری) تقسیم

می‌شود بر اساس الگوها و هنجارهای نظام اجتماعی شکل خواهد گرفت (اوت و شومیکر، ۱۳۷۶).

حال اگر نظام اجتماعی، در فرایند زمینه‌سازی کسب هویت اجتماعی آحاد خود، به خوبی عمل نکند و نتواند الگوها و هنجارهای نظام اجتماعی را برای آنان ساخته و درونی کند، افراد نسبت به نظام اجتماعی خود احساس بی‌هویتی خواهند کرد و در نتیجه برای جبران هویت اجتماعی از دست رفته، به منابع دیگری که در فضای زندگی پیرامون آن‌ها در دسترس است رجوع خواهند کرد. در این صورت گرایش‌های ایستاری، کنشی و نمادی آن‌ها نیز متناسب با الگوهای فرهنگ غربی شکل خواهد گرفت. در واقع، در دنیای کنونی که انفجار اطلاعات در آن به وقوع پیوسته و بخش عظیمی از انسان‌ها و به‌ویژه جوانان در معرض پیامدهای آن قرار گرفته‌اند، هویت مبنا و معنای گذشته خود را از دست داده است و شدت و دامنه تغییرات هویتی در نسل‌های جدید به حدی است که در برخی موارد چالش‌ها و بحران‌های هویتی را پدید آورده است و بر خلاف گذشته، فرآیند انتقال هویت بیش از آن که در زمینه ارزش‌ها، باورها و رفتارها و خلاصه هویت‌شان از والدین خویش متأثر باشند از رسانه‌ها، صنعت فرهنگ، هم‌سالان و جوانان دیگر که چه بسا از دیگر کشورها باشند تأثیر می‌پذیرند.

یافته‌های پژوهش عدلی‌پور (۱۳۹۱) در رساله کارشناسی ارشد (که به بررسی تأثیرات و پیامدهای شبکه‌های اجتماعی مجازی بر هویت اجتماعی جوانان پرداخته) خود حاکی از آن است که شبکه‌های اجتماعی مجازی به عنوان یک پدیده نوظهور هم دارای آثار مثبت و هم آثار منفی می‌باشند. آثار منفی آن شامل تکه‌پاره گشتن سریع جوامع، دگرگونی مفاهیم مکان، زمان، فضا و منابع فرهنگی، به چالش کشیده شدن هویت‌های اصیل و سنتی، رواج هویت‌های سیال و ناپایدار، گمنامی و ناشناس ماندن و سرقت هویت است. علی‌رغم این نکات منفی که این پدیده به همراه دارد نمی‌توان از آثار مثبت آن نیز غافل ماند. افزایش منابع هویتی و آزادی عمل افراد برای کسب منابع مورد نیاز، رهایی و آزادی افراد از چنگال عوامل و متولیان فرافردی هویت‌سازی، فراهم آمدن واقعیت به‌گونه‌ای مجازی و غیره از آثار مثبت این پدیده هستند که اگر از آن‌ها استفاده درستی به عمل آید، باعث رشد و پویایی هویت اجتماعی در میان افراد جامعه خواهد

گشت. وی همچنین در پژوهش خود هم‌راستا با تحقیقات رفعت‌جاه و شکوری (۱۳۸۷)، عباس‌قادی (۱۳۹۰)، مهدی‌زاده و عنبرین (۱۳۸۸) و احمدپور و قادرزاده (۱۳۸۹) نشان می‌دهد که شبکه‌های اجتماعی عاملی تأثیرگذار بر هویت اجتماعی جوانان هستند و با افزایش مدت زمان عضویت، میزان استفاده، میزان مشارکت و فعالیت و واقعی تلقی کردن محتوای مطالب ارائه شده در این شبکه‌ها هویت ملی و دینی کاربران تضعیف می‌شود (رفعت، ۱۳۸۷: ۸). وی در تحلیل این امر معتقد است که احتمالاً استفاده آزاد از امکاناتی چون اینترنت و شبکه‌های اجتماعی مجازی در خانواده‌هایی بیش‌تر رواج دارد که اعتقادات و باورها و در نهایت هویت دینی آن‌ها ضعیف‌تر از دیگر خانواده‌ها است. اما این مسأله از عامل دیگری نیز سرچشمه می‌گیرد و آن این است که چون در جامعه ما از اینترنت، شبکه‌های اجتماعی مجازی و ماهواره اکثراً به صورت منطقی استفاده نمی‌شود و این رسانه‌ها و امکانات اطلاعاتی و ارتباطاتی، بیش‌تر مروج فرهنگ مادی‌نگر و لذت‌جو و فردگرایانه غربی هستند، یکی از جنبه‌های آسیب‌زای آن کاهش تعلقات دینی و اخلاقی در نوجوانان و جوانان است. همچنین تعامل در فضای مجازی تأثیر دوگانه‌ای بر ابعاد هویت دینی جوانان دارد؛ به طوری که با افزایش دسترسی و بهره‌مندی از مجاری نوین اطلاعاتی و ارتباطی و افزایش مدت زمان استفاده و نوع مصرف به دلیل تلطیف افق ذهنی و بینشی و ارتقاء و گسترش جهت‌گیری‌های شناختی، عاطفی و عملی، از یک سو، از شدت ابعاد پیامدی و تجربی کاسته می‌شود و از سوی دیگر، هویت دینی جوانان در بعد شناختی تقویت می‌شود. در واقع اطلاعات یادشده بر این واقعیت دلالت دارد که جوانان متناسب با نوع نیازهای دینی و مذهبی خود از اینترنت و شبکه‌های اجتماعی مجازی استفاده می‌کنند و به همان ترتیب استفاده از شبکه‌های اجتماعی اینترنتی بر شیوه و سبک دینداری آن‌ها تأثیر می‌گذارد و انعطاف‌پذیری نسبت به قرائت‌های دینی مختلف را افزایش می‌دهد (اخگری، ۱۳۸۸: ۲۵). یافته‌های پژوهش وی همچنین با آنچه در زمینه همسان‌سازی فرهنگ کشورهای جهان سوم با کشورهای غربی صورت می‌گیرد نیز همخوانی دارد. از آنجا که ایجادکنندگان و پیام‌فرستندگان و برنامه‌سازان این تکنولوژی ارتباطی و اطلاعاتی عمدتاً کشورهای توسعه‌یافته غربی هستند تعجبی هم ندارد که انبوه فیلم‌ها و سایت‌های پرمخاطب آن‌ها هویت فرهنگی، قومی و ملی

کشورهای مصرف‌کننده را تحت تأثیر قرار داده و تضعیف نماید. با این حال در سال‌های اخیر در اینترنت مقاومت‌هایی در برابر این جریان به چشم می‌خورد که نشان از ظهور و احیای هویت‌های قومی و ملی در اینترنت و ماهواره است. سایر پژوهش‌های انجام شده توسط محققان دیگر به‌ویژه تحقیق *ساروخانی و رضایی‌قادی* (۱۳۹۱)، *کوهی و حسنی* (۱۳۹۱)، نشان‌دهنده آن‌اند که با گسترش روزافزون رسانه‌های نوین همچون شبکه‌های اجتماعی مجازی، به‌ویژه در جوامع در حال گذار، روند نوسازی به تضعیف پیوندهای سنتی می‌انجامد. این رسانه‌ها می‌توانند در نگرش‌ها و رفتار شهروندان تأثیر گذارده و باعث کاهش همدلی، احساس تعلق ملی و انسجام اجتماعی شوند. *اینگله‌هارت* با طرح مفهوم انقلاب خاموش، بر این نظر است که ورود سریع ارزش‌ها و ایده‌های جدید از طریق تکنولوژی‌های نوین اطلاعاتی و ارتباطی می‌تواند گسست‌های جدی در مبانی هویتی جامعه ایجاد کند. هم‌چنان که *کاستلز* بیان کرده است ماهواره و اینترنت با دگرگون ساختن بنیادین ماهیت ارتباطات، نقش تعیین‌کننده‌ای در تغییر و شکل‌دهی فرهنگ‌ها و هویت ملی شهروندان ایفا می‌کنند (*کاستلز*، ۱۳۸۰: ۳۸۴-۳۸۳). علاوه بر آن، پاستر بر نقش اینترنت در گسترش فرهنگ و هویت و روش جدید ساخته شدن هویت ملی تأکید کرده است. در این ارتباط، وی فرایند جهانی شدن رسانه‌ها را با به وقوع پیوستن افول هویت ملی تحلیل کرده است (*پاستر*، ۱۳۷۷: ۵۲). *گیدنز* اینترنت و ماهواره را عامل سردرگمی و بی‌ثباتی و بی‌نظمی فرهنگی قلمداد کرده است. گستره بحران هویت به موارد یادشده محدود نمی‌شود. نوعی از بحران هویت که خاص فضای مجازی است، مربوط به تغییر اجتماعی سریع است. بر اثر ارتباطات این چنین و تعامل با فضای مجازی، سنت‌های قدیمی به سرعت در حال سست شدن بوده و احساس سردرگمی هویتی در تعدادی از گروه‌های اجتماعی شکل گرفته است. استفاده از اینترنت و شبکه‌های اجتماعی تأثیرات عمیقی بر ارزش‌های جوانان داشته و موجب شده نیازهایی که قبلاً توسط خانواده بر طرف می‌شود، امروزه از سوی این رسانه جدید مرتفع گردد؛ مثلاً در گذشته دوست‌یابی تحت نظر والدین صورت می‌گرفت؛ اما امروزه برخی جوانان با استفاده از سیاست‌های دوست‌یابی، گفت‌وگو (چت) و امثال آن‌ها قادرند با افراد گوناگون و با فرهنگ‌های مختلف آشنا شوند (*حاجیانی*، ۱۳۸۸: ۵۶). کاربران اینترنت بر خلاف

نسل اول که در فضایی واقعی و حقیقی فعالیت می‌کردند، امروزه در فضایی مجازی مشغول هستند. بر همین اساس، بسیاری از کارکردهای خانواده در جامعه پذیری افراد به وسیله این رسانه تعاملی در محیطی مجازی صورت می‌گیرد (بوره‌سین بیگی، ۱۳۸۳: ۵۶). پدیده مهم دیگری که از بحران هویت به وجود می‌آید، ترکیبی از بحران هویت فردی و اجتماعی است. شواهد نشان می‌دهد وقتی افراد در معرض فضای مجازی قرار می‌گیرند، به نوعی از دگرخودپنداری از خویش مبتلا می‌شوند. این پدیده که در روان‌شناسی از آن به بیماری امپاتی یاد می‌شود، وضعیتی پدید می‌آورد که افراد در فضای مجازی، خود را در شرایطی ایده‌آل و دست نیافتنی‌تر تعریف می‌کنند و در مواجهه با واقعیت دچار نوعی بحران می‌شوند. به نظر می‌رسد این بحران، پایه‌ساز بحران‌های سیاسی و اجتماعی در جوامع در حال توسعه می‌باشد.

انواع جرم‌های مربوط به جعل هویت

سرقت ایمیل‌ها یا گشتن در بین زباله‌های حاوی اطلاعات شخصی؛ بازیابی اطلاعات از وسیله دور انداخته شده، همچون رایانه‌های سرورهایی که بدون رعایت اصول بهداشتی در سایت‌های زباله عمومی رها شده است؛ جست‌وجو درباره قربانیان در مراکز ثبت دولتی و موتورهای جست‌وجوی اینترنتی؛ سرقت کارت‌های بانکی و شناسایی از طریق جیب‌بری یا کارت‌خوان‌ها؛ اطلاعات‌خوانی از راه دور از طریق چیپ‌های RFID روی کارت‌های هوشمند، اعتباری یا پاسپورت‌ها؛ استراق سمع تعاملات عمومی برای کسب اطلاعات (نگاه از روی دست دیگران)؛ سرقت اطلاعات شخصی از رایانه‌ها و پایگاه‌های رایانه‌ای (تروجان‌ها، هک کردن)؛ باگ‌های تبلیغات شغلی برای اینکه کاربران اطلاعات خود را ارسال کنند؛ جست‌وجو در شبکه‌های اجتماعی برای به دست آوردن اطلاعات جزئی که کاربران در آنجا گذاشته‌اند. سرقت هویت ممکن است اشکال مختلفی به خود بگیرد. بر اساس گزارش مرکز غیر انتفاعی منبع سرقت هویت و دیگر منابع، سرقت هویت به پنج دسته زیر تقسیم می‌شود. سرقت هویت کاری/تجاری (استفاده از نام تجاری شخص دیگر برای کسب اعتبار)؛ سرقت هویت جنایی (معرفی خود به عنوان فرد دیگر هنگام ارتکاب جرم)؛ سرقت هویت مالی (استفاده از هویت دیگری برای کسب کالاها

و خدمات)؛ تکثیر هویت (استفاده از اطلاعات فرد دیگر برای استفاده از هویت او در زندگی روزانه)؛ سرقت هویت پزشکی (استفاده از اطلاعات فرد دیگر برای کسب مراقبت‌های بهداشتی یا داروها)، جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی.

الف. جعل رایانه‌ای و استفاده از داده‌های مجعول

۱. جعل رایانه‌ای

رکن قانونی بزه جعل رایانه‌ای ماده ۶ قانون جرایم رایانه‌ای (م ۷۳۴ ق.م.ا) می‌باشد. بستر انجام بزه جعل رایانه‌ای، فضای سایبر است و فضای سایبر فضایی غیرمادی و ناملموس است که توسط رایانه‌ها و شبکه‌های رایانه‌ای به وجود آمده است و دنیایی مجازی را در کنار دنیای واقعی ما به وجود آورده است. در واقع فضای سایبر همان فضای مجازی بیکرانی است که از طریق اتصال شبکه‌های رایانه‌ای به هم به وجود آمده است.

به لحاظ فنی «شبکه رایانه‌ای در پایه‌ای‌ترین سطح خود شامل دو کامپیوتر می‌باشد که به وسیله کابل به یکدیگر متصل شده‌اند به گونه‌ای که بتوانند از داده‌ها به طور مشترک استفاده نمایند». این ارتباط در حال حاضر از طریق کابل مسی است، البته ارتباط رایانه‌ها با یکدیگر ممکن است از طریق کابل خطوط تلفن نباشد و از طریق «فیبر نوری، میکروویو، اشعه مادون قرمز و ماهواره‌های ارتباطی نیز می‌توان برای ارتباط استفاده کرد».

بنابراین همه رفتارهای پیش بینی شده در این ماده باید از رهگذر کنش‌های رایانه‌ای و در بستر رایانه و مخابرات انجام شود. بنابراین اگر کسی داده رایانه‌ای را چاپ کند یا از روی صفحه نمایشگر رایانه عکس بگیرد و سپس بر روی کاغذ چاپ شده، تغییراتی را ایجاد کند، جعل رایانه‌ای محقق نیست و ممکن است با وجود تمام شرایط جعل سنتی باشد. همچنین انجام رفتارهای موضوع جعل رایانه‌ای، باید به صورت غیرمجاز باشد یعنی یا اجازه نداشته و یا بر خلاف قانون و قرارداد بوده است.

۱. رکن مادی: (۱-۱) موضوع جرم: موضوع جعل رایانه‌ای، داده و یا حامل داده و یا

جای انباشت داده می‌باشد مانند علامت، کارت حافظه و تراشه.

داده‌های موضوع جعل رایانه‌ای باید قابلیت استناد داشته باشند و به همین دلیل است که دیگری نیازی به ایراد ضرر برای تحقق این جرم نیست و اگر زبانی حاصل شود می‌تواند باعث افزایش کیفر شود.

۲-۱) رفتار مرتکب: در بند الف ماده ۶ ق جرایم رایانه‌ای دو بخش جداگانه در انجام رفتار جعل رایانه‌ای پیش بینی شده است: اول، تغییر یا ایجاد داده‌های قابل استناد که در واقع تغییر باید در داده‌های قابل استناد انجام شود و ایجاد نیز باید پدید آوردن داده‌ای باشد که توانایی استناد پذیری داشته باشد. دوم، ایجاد یا وارد کردن متقلبانه داده به آن‌ها بند ب ماده ۶ ق جرایم رایانه‌ای، تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها با ایجاد یا وارد کردن متقلبانه داده‌ها یا علایم به آن‌ها را به عنوان رفتار مجرمانه برای جرم جعل رایانه‌ای مطرح می‌کند.

البته به نظر می‌رسد که رفتارهای مندرج در بند ب تفاوتی با بند الف ندارد و نیازی به آوردن بند ب نبود. لیکن برای بند ب، قانونگذار شرط استناد پذیری را بیان نکرده است.

بنابراین وارد کردن، تغییر، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور و اهداف سیاسی و اقتصادی صورت می‌گیرد. جعل رایانه‌ای جعل داده‌هاست. در جعل رایانه‌ای عمل ارتكابی بر داده‌ها اثر می‌گذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.

۲. رکن روانی: عمد مرتکب در پدید آوردن دگرگونی در داده‌های قابل استناد و

سایر رفتارهای مندرج در ماده، رکن روانی این بزه را تشکیل می‌دهد.

۳. مجازات: کسی که مرتکب جرم جعل رایانه‌ای می‌شود بنا به تصریح ماده ۶ ق

جرایم رایانه‌ای به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم می‌شود.

بند دوم: استفاده از داده مجعول: ماده ۷ ق جرایم رایانه‌ای (ماده ۷۳۵ ق.م.ا)، رکن قانونی بزه استفاده از داده مجعول به شمار می‌رود.

۱. رکن مادی: (۱-۱) موضوع جرم: داده، کارت‌های الکترونیکی و تراشه‌ها موضوع رفتار مجرمانه در این جرم می‌باشند.

(۲-۱) رفتار مرتکب: استفاده کردن از داده مجعول که باید در فضای سایبر و سامانه‌های رایانه‌ای و مخابراتی یا داده‌برها و کارت‌های حافظه انجام شود، رفتار مرتکب در بزه استفاده از داده مجعول را تشکیل می‌دهد.

بنابراین اگر کسی در فضای بیرونی و فیزیکی از داده مجعول استفاده کند، این بزه رخ نمی‌دهد. به عنوان مثال اگر فردی جعل رایانه‌ای کند و متن یک قرارداد الکترونیکی را تغییر دهد و یا اینکه چنین قرارداد مجعولی را بیابد یا دریافت دارد و سپس آن را چاپ کرده و به نهاد یا کسی ارائه دهد مرتکب جرم استفاده از سند مجعول شده است نه جرم استفاده از داده مجعول، چراکه استفاده کردن در فضای بیرونی انجام شده است.

۲. رکن روانی: آگاهی مرتکب به جعلی بودن، برجسته‌ترین عنصر رکن روانی است. همچنین لازم است که مرتکب عمد در استفاده کردن از داده مجعول را نیز داشته باشد.

۳. مجازات: بر اساس ماده ۷ ق جرایم رایانه‌ای هر کس با علم به مجعول بودن داده‌ها یا کارت‌ها یا تراشه‌ها از آن‌ها استفاده کند، بنا به تصریح ماده ۶ ق جرایم رایانه‌ای به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم می‌شود.

۲. خرابکاری رایانه‌ای

خرابکاری رایانه‌ای در بردارنده هر رفتاری است که داده را به طور کلی یا جزئی از میان ببرد یا کارکرد داده یا سامانه را به هر نحو بر هم بزند (۲۱۶: ۱۳). استفاده از عنوان تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی برای مبحث دوم از فصل یکم در بخش نخست قانون جرایم رایانه‌ای برای این است که چهار عنوان مجرمانه تخریب، اخلال، ممانعت از دستیابی و تروریسم سایبری را در بر گیرد. از آنجایی که ویژگی‌های تخریب و اخلال نزدیک به هم هستند آن‌ها را در یک بند بررسی می‌کنیم.

بند یکم: تخریب یا اخلال داده: تخریب به معنای از بین بردن تمام یا قسمتی از یک چیز و اخلال در معنای ایجاد آشفتگی و ناتوانی در کارکرد چیزی است. م ۸ ق جرایم رایانه‌ای (م ۷۳۶ ق م ا) این جرم را پیش‌بینی کرده است.

۱. رکن مادی: (۱-۱) موضوع جرم: موضوع بزه تخریب یا اخلال، «داده» می‌باشد. این داده باید از آن دیگری باشد. خواه مالیت داشته باشد، خواه نداشته باشد و خواه استاندارد پذیر نباشد، خواه شخصی باشد خواه دولتی. اما اگر موضوع بزه، داده‌های دولتی باشد مطابق بند ج ماده ۲۶ ق جرایم رایانه‌ای مرتکب با افزایش مجازات مواجه خواهد بود. (۲-۱) رفتار مرتکب: چهار رفتار حذف، تخریب، مختل و غیر قابل پردازش کردن در ماده ۸ ق جرایم رایانه‌ای پیش‌بینی شده است که زیر دو رفتار تخریب و اخلال قرار می‌گیرند. دو رفتار حذف و تخریب نسبت به خود داده و دو رفتار مختل کردن و غیر قابل پردازش نمودن نسبت به کارکرد و توانایی داده رخ می‌دهد.

هر چهار رفتار باید در فضای سایبر رخ دهد این مسأله با بکار بردن عبارت «سامانه‌های رایانه‌ای یا مخابراتی یا حامل داده» در متن ماده روشن می‌شود و رفتارهای بزهکارانه باید رایانه‌ای و سایبری باشد. به عنوان مثال اگر کسی به قصد از بین بردن داده دیگری، رایانه‌اش را از بلندی پرت کند یا آن را بسوزاند یا لوح فشرده را بشکند یا آن را بخرشد یا سنگ، بر روی حامل داده بزند، هیچ یک تخریب یا اخلال رایانه‌ای نیست بلکه حسب مورد تخریب یا اخلال سنتی است.

۲. رکن روانی: علم و عمد در انجام رفتارهای مرتکب که در قسمت قبل عنوان شد، رکن روانی بزه را تشکیل می‌دهد، همچنین بزه تخریب و اخلال داده رایانه‌ای باید به طور غیرمجاز انجام گیرند و مرتکب آگاه به غیرمجاز بودن باشد بدیهی است که اگر رفتارهای موضوع ماده ۸ ق جرایم رایانه‌ای با اجازه دارنده آن باشد، بزهی در کار نخواهد بود و میان شخص حقوقی و حقیقی و فرد و دولت تفاوتی نمی‌باشد (مهدی زاده، ۱۳۸۸: ۴۱).

۳. مجازات: بر اساس ماده ۸ ق جرایم رایانه‌ای برای مرتکب بزه مزبور حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات در نظر گرفته شده است.

بند دوم: اخلال سامانه‌های رایانه‌ای یا مخابراتی

ماده ۹ قانون جرایم رایانه‌ای (م ۷۳۷ ق م ا) این بزه را بیان نموده است.

۱. رکن مادی: (۱-۱) موضوع جرم: موضوع بزه اخلال در ماده ۹ ق جرایم رایانه‌ای، سامانه‌های رایانه‌ای و مخابراتی است. سامانه ممکن است از آن شخص حقیقی یا حقوقی خصوصی باشد یا اینکه ممکن است از آن نهادها و سازمان‌های دولتی باشد. اخلال سامانه دولتی سبب افزایش کیفر می‌گردد. (۲-۱) رفتار مرتکب: در ماده ۹ قانون جرایم رایانه‌ای دو نوع رفتار پیش‌بینی شده است: اول، رفتارهای احصایی که شامل از کار انداختن و مختل کردن می‌شود و دوم رفتارهای تمثیلی که در صدر ماده آمده و عبارت‌اند از وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب و مانند آن‌ها.

رفتارهای تمثیلی بر روی سامانه رخ نمی‌دهند بلکه بر روی داده یا موج انجام می‌شوند و سپس به اخلال می‌انجامند. از کار انداختن و مختل کردن بر روی سامانه رایانه‌ای و مخابراتی انجام می‌شوند.

۲- رکن روانی: در اخلال سامانه، مرتکب باید عمد در انجام رفتار را داشته باشد. همچنین او باید به موضوع بزه آگاهی داشته باشد. یعنی هم نسبت به اینکه سامانه از آن دیگری است و یا اینکه از آن دولت است و هم نسبت به غیرمجاز بودن آن آگاه باشد.

۳. مجازات: بر پایه ماده ۹ ق جرایم رایانه‌ای (م ۷۳۷ ق م ا) برای بزه مزبور حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات، مقرر گردیده است.

۴. راه‌های پیشگیری از جرم

۴-۱. پیشگیری وضعی

مبانی پیشگیری وضعی بر این فرض استوار است که یک انسان متعارف، در همه زمینه‌ها، خواسته یا ناخواسته به طور منطقی و حساب‌شده عمل کرده و از خطرات شدید دوری می‌کند؛ یعنی در صورتی تن به خطر می‌دهد که عایدات یا منافع حاصل از آن عمل ارزشمند باشد. حال اگر این فرض در مورد مجرمان درست باشد، می‌توان گفت اگر

به هر شکل بتوان خطرپذیری جرم را افزایش داد یا جاذبه و منفعت حاصل از آن «را کاهش داده یا از بین برد، قاعدتاً مجرمان بالقوه از ارتکاب جرم منصرف می‌شوند» (نجفی ابرندآبادی، ۱۳۸۲: ۲۴۲). کالرک، جرم شناس معروف انگلیسی، پیشگیری وضعی از جرم را به عنوان اقدامات قابل سنجش و ارزیابی مقابله با جرم می‌داند. این اقدامات معطوف به اشکال خاص از جرائم بوده و از طریق مدیریت یا مداخله در محیط بالواسطه به شیوه‌ای پایدار و سیستماتیک منجر به کاهش فرصت‌های جرم و افزایش خطرات جرم که همواره مد نظر تعداد بسیاری از مجرمان بوده است می‌شود (رزنبام و سایرین، ۱۳۸۲: ۳۴۲). پیشگیری وضعی از جرم قابل مقایسه با مفهوم عامل روان‌شناسان، یعنی کنترل محرک است. آن‌ها معتقدند احتمال وقوع جرم بر اساس کیفیت قرارگرفتن محرک در محیط، تقویت یا تضعیف می‌شود. محرک را می‌توان از طریق اعمال مدیریت، طراحی یا مداخله در محیط، توسط طراحان پیشگیری از جرم تغییر داد. همچنین پیشگیری وضعی از جرم، بر این نظریه استوار است که موقعیت‌ها قابل پیش‌بینی‌تر از افراد هستند. تحقیقات انجام‌شده نشان می‌دهد که درصد زیادی از حوادث و وقایع مجرمانه در محل‌های خاصی متمرکز شده‌اند که جرم‌شناسان از آن‌ها به عنوان نقاط جرم‌خیز یاد می‌کنند. بنابراین اقدامات پیشگیری از جرم برای کاهش فرصت‌های جرم‌زایی که در محیط پدید می‌آیند، به کار برده می‌شود (جلالی فراهانی، ۱۳۸۶: ۳۴۰). پیشگیری وضعی شامل مجموعه اقدامات و تدابیری است که به سمت تسلط بر محیط و شرایط پیرامونی جرم (وضعیت مشرف بر جرم) و مهار آن متمایل است. این امر از یک سو، از طریق کاهش وضعیت‌های مقابل بزهکاری یعنی وضعیت‌های پیش‌جنایی که وقوع جرم را مساعد و تسهیل می‌کنند انجام می‌شود و از سوی دیگر، با افزایش خطر شناسایی و احتمال دستگیری بزهکاران، از وقوع جرم جلوگیری می‌کند. بنابراین پیشگیری وضعی، بیش‌تر با حمایت از آماج‌های جرم و نیز بزه‌دیدگان بالقوه و اعمال تدابیر فنی، به دنبال پیشگیری از بزه‌دیدگی افراد یا آماج‌ها در برابر بزهکاران است که در نهایت به طور غیرمستقیم منجر به کاهش بزهکاری می‌شود. در صورتی که پیشگیری اجتماعی به طور مستقیم در مقام جلوگیری از تبدیل شدن بزهکاران بالقوه به بزهکاران بالفعل است. رویکردهای پیشگیری وضعی با توجه به رویکرد کلی مقابله با جرائم که در دهه‌های اخیر شاهد تحولات

شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد که عبارت‌اند از اقدامات کیفری و غیرکیفری. در زمینه اقدامات کیفری سعی می‌شود از طریق جرم‌انگاری هنجارشکنی‌ها و سوء استفاده‌های جدید و یا تجدید نظر در قوانین کیفری گذشته، ارباب پذیری مؤثری درباره مجرمان بالقوه یا مکرر صورت می‌گیرد که به این ترتیب، از ارتکاب جرم باز داشته شوند.

اما رویکرد دوم که در بستر جرم‌شناسی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان‌شناسی، جامعه‌شناسی پدید آمده، اتخاذ تدابیر پیشگیرانه را در دستور کار خود قرار داده است. در این زمینه، تا کنون الگوهای مختلفی در عرصه جرم‌شناسی پیشگیرانه ارائه شده و مورد آزمون قرار گرفته است.

از مهم‌ترین و مؤثرترین این الگوها می‌توان به پیشگیری اجتماعی و پیشگیری وضعی اشاره کرد. به طور خلاصه، در پیشگیری اجتماعی سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آن‌ها، به ویژه قشر جوان و نوجوان جامعه، و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم (مانند فقر و بیکاری) انگیزه‌های مجرمانه از مجرمان سلب شود. امام در پیشگیری وضعی، هدف سلب فرصت ابزار ارتکاب جرم از مجرم با انگیزه است.

۲-۴. کارکرد پیشگیری وضعی

کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. توجه به مثلث جرم می‌تواند به درک این موضوع کمک کند. برای ارتکاب یک جرم، سه عامل باید جمع شوند؛ مهم‌ترین آن‌ها که قاعده مثلث جرم را هم تشکیل می‌دهد، انگیزه مجرمان است. انگیزه باعث بیدار شدن میل درونی در افراد و به تبع آن قصد مجرمانه می‌شود. برای از بین بردن این عامل ضروری است تدابیر پیشگیرانه اجتماعی اتخاذ شود.

اما اگر به هر دلیل مجرمان دارای انگیزه شدند، باید از اجتماع دو ضلع دیگر این مثلث، یعنی فرصت و ابزار ارتکاب جرم جلوگیری کرد. از میان این دو، سلب فرصت از مجرمان اهمیت بیش‌تری دارد، زیرا متصدیان امر هرچه بکوشند ابزار ارتکاب جرم را از

سطح جامعه جمع‌آوری کنند، بازهم مجرمان بانگیزه خواهند توانست به آن‌ها دست یابند. هرچند در عین حال نباید اهمیت جمع‌آوری این ابزارها را در کاهش جرائم نادیده گرفت. به هر حال، آنچه در پیشگیری وضعی از جرائم اولویت دارد، حفظ آماج‌ها و بزه‌دیدگان از تعرض مجرمان است.

۳-۴. سیاستگذاری‌های اجتماعی و تدابیر پیشگیرانه وضعی در فضای مجازی

سیاستگذاری‌های اجتماعی را می‌توان با بکارگیری تدابیر پیشگیرانه وضعی در فضای سایبر، در چهار گروه طبقه‌بندی کرد: تدابیر نظارتی، تدابیر صدور مجوز، ناشناس‌کننده‌ها و رمزنگارها، تدابیر محدودکننده دسترسی (فیلترینگ).

۱. تدابیر نظارتی: به طور خلاصه این تدابیر در دوشاخه اصلی قرار می‌گیرند. یک شیوه این است که با اتخاذ تدابیر نظارتی در دنیای فیزیکی، از ارتکاب جرایم در فضای سایبر جلوگیری شود. برای مثال، به والدین آموزش داده می‌شود سیستم‌های رایانه‌ای را در نقاطی از منازل قرار دهند که در معرض دید عموم باشد تا فرزندانشان فرصت سوء استفاده از خلوت در فضای سایبر را پیدا نکنند. شیوه دیگر نظارت که با ویژگی‌های این فضا نیز سازگار است، نظارت الکترونیکی نام دارد. در اینجا با بکارگیری تجهیزات برنامه‌های خاص، فعالیت‌های شبکه‌ای افراد تحت نظر قرار می‌گیرد. نظارت الکترونیکی نیز به دو شکل انجام می‌شود: هم‌زمان و غیر هم‌زمان. در حالت اول، ابزار الکترونیکی مسئول یا متصدی مربوطه را از فعالیت‌های غیرمجاز شبکه‌ای کاربر در همان زمان آگاه می‌کند. به این ترتیب، او می‌تواند اقدامات الزامی را انجام دهد. اما در نظارت غیر زنده، بسته به میزان دقت ابزار تمام یا بخش‌گزینه‌های از فعالیت‌های شبکه‌ای را ثبت می‌کند (Lin.S & Thornburgh, 2004:305).

۲. تدابیر صدور مجوز: این تدابیر از الگوبرداری از دنیای فیزیکی به اجرا در می‌آیند. یکی از شیوه‌های رایج سلب فرصت مجرمانه یا حتی جلوگیری از بزه‌دیدگی و افراد، کنترل دسترسی است. به عبارت دیگر، تنها کسانی می‌توانند به محیط‌هایی با ویژگی‌های خاص وارد شوند که تأییدیه مورد نظر را داشته باشند. لذا چنانچه تدابیر کنترل دسترسی به خوبی اجرا شود از ورود مجرمان بالقوه و همچنین کسانی که به هر

دلیل مطابق قانون نمی‌توانند وارد آن محیط شوند جلوگیری به عمل می‌آید (48:2004, children on board).

۳. ناشناس کننده‌ها و رمزنگارها: کارکرد ناشناس کننده‌ها این است که پیوندهای هویتی را قطع می‌کنند. این ابزارها تنها آن چیزی را که به طور تصادفی ایجاد شده به عنوان هویت اشخاص ارائه می‌دهند و کاربران قادر خواهند بود در تعاملات شبکه‌ای خود از آن استفاده کنند. به این ترتیب، هر کس از هویت ناشناس کاربر مورد نظر آگاه شود، با موانعی مواجه خواهد شد. این اقدام به ویژه برای زنان و کودکان یا به طور کلی اشخاص آسیب پذیر سودمند است. زیرا بی آنکه فرصت شناسایی خود را به مجرمان سایبر بدهند، می‌توانند به فعالیتهای شبکه‌ای بپردازند. رمزنگاری اطلاعات فرد را از مقابل دیدگان تمامی اشخاص (به استثناء آن‌هایی که مجاز شمرده می‌شوند) پنهان می‌کند. در اکثر فعالیتهای کلی رمزگذاری، اصل ساز (Originator) پیامی را برای مخاطب خود ایجاد می‌کند و سپس آن را طی مراحل رمزنگاری محفوظ کرده و به عنوان یک رمز نوشته ارسال می‌کند. مخاطب نیز به محض دریافت آن را رمزگشایی و به متن اصلی تبدیل می‌کند (Shinder, 2002: 353).

۴. تدابیر محدودکننده دسترسی (فیلترینگ): این تدابیر شامل اقداماتی می‌شود که از ورود یا ارسال برخی داده‌های غیرمجاز جلوگیری می‌کند، بعضی یکسویه عمل می‌کنند، یعنی فقط از ورود یا خروج موارد غیرمجاز جلوگیری می‌کنند، اما بعضی دیگر عمل دوسویه دارند. با توجه به موقعیت و مبنای عمل فیلترها، می‌توان برای آن‌ها تقسیماتی قایل شد که به دلیل اهمیت موضوع به آن‌ها اشاره می‌شود:

۱. فیلتر از سوی مشتری: فیلترهایی که می‌توان بر روی رایانه‌های شخصی رومیزی یا قابل حمل نصب کرد که نقطه دسترسی به اینترنت را برای کاربر پایانی فراهم می‌آورند.

۲. فیلتر از سوی ارائه دهنده خدمات دسترسی حضوری (کافی نت) یا ارائه دهنده خدمات اینترنتی: کم‌تر اتفاق می‌افتد کسی بر روی سیستم کامپیوتری خود فیلتر نصب کند و غالباً ارائه دهنده خدمات دسترسی کاربران را از دسترسی به سایت‌ها محروم می‌کند. کاربر مجبور است که برای برقراری ارتباط شبکه‌ای به یک ارائه دهنده خدمات

دسترسی مراجعه کند یا از منزل و محل کار خود با یک ISP ارتباط برقرار کند. به این ترتیب این دو مرجع می‌توانند با نصب فیلتر از دسترسی وی جلوگیری کنند (Lin.S, 271: Thornburgh, 2004).

۳. فیلتر از سوی سرور: این نوع فیلترها در مؤسسات یا نهادهایی کاربری دارند و معمولاً بر روی سیستم کامپیوتری‌ای نصب می‌شوند که امکان دسترسی شبکه‌ای را برای کامپیوترهای واقع در مجموعه خود فراهم می‌آورد.

۴. فیلتر از سوی ایجادکننده نقطه تماس بین المللی: این مراکز شاهراه اصلی برقراری ارتباطات شبکه‌ای داخل با خارج محسوب می‌شوند. مسأله قابل تأمل و تدبیر جدی از سوی سیاستگذاران و تصمیم‌گیران دولتی است. زیرا با مزیت‌های قابل توجه سایبر، نظیر خلوت، گمنامی و بدون مرز بودن کاربری رایانه‌ای که جرأت قابل توجهی را در مجرمان و منحرفان بالقوه پدید می‌آورد همراه می‌شود (جلالی فراهانی، ۱۳۸۶: ۲۵).

حقوق شهروند فضای مجازی از منظر قرآن

• اولین حق مردم در فضای مجازی آن است که مطالب و اخبار به شکل صحیح و مستند در اختیار آنان قرار گیرد، نه بر اساس حدس و گمان، توهین و تهمت، یا شایعه و برداشت شخصی.

قرآن می‌فرماید: ﴿إِنْ جَاءَكَ فَاسِقٌ بِنَبَأٍ فَتَبَيَّنْهُ﴾ (حجرات/۶): «اگر یک فاسق خبری آورد، تحقیق کنید». پخش اخبار بدون تحقیق در درست و غلط بودن آن، مسئولیت‌آفرین است. هدهد به حضرت سلیمان (ع) گفت: ﴿أَخَطْتُ بِمَا لَمْ تُحِطْ بِهِ وَجِئْتُكَ مِنْ سَبَإٍ بِنَبَأٍ يَقِينٍ﴾ (نمل/۲۲): «من بر چیزی آگاهی یافته‌ام که تو بر آن آگاهی نیافتی؛ من از سرزمین سبا یک خبر قطعی و یقینی برای تو آورده‌ام».

• مسأله دوم اینکه هر محتوایی باید به اهلش گفته شود و مسایل و مطالب، به روز و به موقع باشد؛ چون همه مردم ظرفیت هر محتوایی را ندارند. موسی (ع) پیامبر اولو العزم بود، اما در ماجرای همراهی با خضر نشان داد که ظرفیت و تحمل دیدن و شنیدن همه چیز را ندارد. قرآن می‌گوید همه مردم ظرفیت یکسان ندارند: ﴿لَا تَسْأَلُوهُنَّ عَنْ شَيْءٍ إِنَّهُنَّ

لَكَرُّ تَسْوُكُمْ﴾ (مائده/۱۰۱). بر این اساس خبر و مطلبی را نقل نکنیم که امنیت فکری و روانی جامعه به هم بخورد.

قرآن در ماجرای فرار موسی (ع) از مصر می‌فرماید: ﴿وَجَاءَ رَجُلٌ مِّنْ أَقْصَى الْمَدِينَةِ يَسْعَى﴾ (قصص/۲۰). وقتی دربار فرعون تصمیم گرفت موسی را بگیرند و او را بکشند شخصی با سرعت به شهر آمد و این خبر را به موسی داد. اگر او به موقع نمی‌آمد، کار موسی تمام شده بود.

• مسأله بعد اینکه باید فعالیت‌ها و حرکات دشمنان را رصد کنیم. ببینیم در دیگر سایت‌ها و فضاها چه می‌گذرد و چه گفته می‌شود؟ از دشمنان دین و کشور غافل نباشیم. البته این کار خواص است. کسانی که مسئول هستند، مثل نیروی انتظامی، وزارت اطلاعات، سازمان تبلیغات، حوزه‌ها، دانشگاه‌ها و

در قرآن می‌خوانیم که وقتی مادر موسی، نوزادش را در صندوقی گذارد و آن را به نیل انداخت، آن را رها نکرد، بلکه به دخترش گفت: ﴿وَقَالَتْ لِأُخْتِهِ قُصِّيهُ فَبَصَّرَتْ بِهِ عَنْ جُنْبٍ وَهُمْ لَا يَشْعُرُونَ﴾ (قصص/۱۱): «بدون آنکه کسی متوجه شود، این صندوق را دنبال کن». ما نیز باید همه چیز را رصد کنیم. خیلی وقت‌ها از مسایل مهم، زمانی خبردار می‌شویم که کار از کار گذشته است.

خبرها باید توسط افراد بصیر تحلیل و کارشناسی شود. در این باره قرآن می‌فرماید: ﴿وَلَوْ رَدُّوهُ إِلَى الرَّسُولِ وَإِلَى أُولِي الْأَمْرِ مِنْهُمْ لَعَلِمَهُ الَّذِينَ يَسْتَنْبِطُونَهُ مِنْهُمْ﴾ (نساء/۸۳): «اگر اخبار جامعه به پیامبر و پیشوایان که قدرت تشخیص کافی دارند- بازگردانده شود، مردم از ریشه‌های مسائل آگاه خواهند شد».

• فضای مجازی باید سالم باشد و حب و بغض شخصی در آن نباشد. قرآن می‌فرماید: ﴿شُهَدَاءُ لِلَّهِ وَلَوْ عَلَىٰ أَنْفُسِكُمْ أَوِ الْوَالِدِينَ وَالْأَقْرَبِينَ﴾ (نساء/۱۳۵): «برای خدا شهادت دهید، اگرچه (این گواهی) به زیان خود شما، یا پدر و مادر و نزدیکان شما بوده باشد! این بدین معناست که در درج اخبار و مطالب قبل از رعایت مصالح شخصی، خدا را در نظر بگیریم».

• باید مواظب بود به افراد بی‌گناه آسیبی نرسد و با آبروی اشخاص بازی نشود. شنیده می‌شود که در سایت‌ها تصاویر و فیلم‌هایی از افراد معروف و غیرمعروف بدون در

نظر گرفتن حریم خصوصی و شخصی افراد دست به دست می‌شود. قرآن می‌فرماید: ﴿أَنْ تَصِيبُوا قَوْمًا بَٰجِهَالَةٍ﴾ (حجرات/۶): «مبادا به گروهی از روی نادانی آسیب برسانید».

• باید مراقب باشیم مطلبی که منتشر می‌کنیم، بازتاب منفی نداشته باشد و مورد سوء استفاده و بهره‌برداری غلط قرار نگیرد. قرآن می‌فرماید: يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَقُولُوا رَاعِنًا وَقُولُوا انظُرْنَا وَاسْمَعُوا (بقره/۴۰). ای افراد باایمان! (هنگامی که از پیغمبر تقاضای مهلت برای درک آیات قرآن می‌کنید) نگوئید: «راعنا»؛ بلکه بگوئید: «انظرنا» (زیرا کلمه اول، هم به معنی «ما را مهلت بده!» است و هم به معنای «ما را تحمیق کن!»؛ و دستاویزی برای دشمنان است).

نتیجه بحث

در این پژوهش مهم‌ترین سؤال این است که نظارت‌های لازم دولت در حوزه فضاهای مجازی در مقابله با جرم جعل هویت با رویکرد پیشگیری وضعی کدام‌اند؟ با افزایش گسترش و بکارگیری فناوری‌های جدید، پدیده جرایم مرتبط با این فناوری‌ها نیز به سرعت و تصاعدی افزایش می‌یابند. هم اکنون مجرمان به ویژه در کشورهای پیشرفته کم‌تر به خودشان زحمت می‌دهند به بانکی، مسلحانه دستبرد بزنند و خطر دستگیری و زندانی شدن و مرگ را به جان بخرند. آنان قادرند با جعل هویت از خانه خود و با کمی امکانات، پول بانک‌ها را از نقطه‌ای به نقطه دیگر جهان انتقال دهند. این در حالی است که آنان سعی می‌کنند با اقدامات بسیار پیچیده از خود رد پایی به جای نگذارند. از این رو اطلاع و آگاهی از آخرین شیوه‌های تخریبی و مجرمانه رایانه‌ای برای پیشگیری، ردیابی و پی‌جویی و کنترل این نوع جرایم کاملاً ضروری می‌باشد. جهان مجازی شکل دیگری از جهان واقعی است که بر فراز آن قرار گرفته است.

بکار بردن عباراتی چون دولت مجازی، پست الکترونیک، جرم الکترونیک، جرم اینترنتی، تجارت اینترنتی، دوستی مجازی و مانند آن، که همگی در درجه اول اشاره به جهان مجازی دارند، نشان‌دهنده تشابه میان عناصر هر یک از این دو جهان است. در فضای ارتباطی جدید، عامل زمان و مکان کم‌رنگ شده است و دوری و نزدیکی به عنوان عامل خنثی در ارتباطات محلی و جهانی محسوب می‌شوند. در واقع جهان جدیدی به

موازات جهان واقعی به وجود آمده است که جهان بی مرز، جهان بی مکان به تعبیر دقیق‌تر جهان مجازی نام گرفته است. پژوهش با توضیح کوتاهی پیرامون جرم جعل هویت و ویژگی‌های ارتباطات در فضای مجازی اشاره و در ادامه، نظریه‌هایی راجه به قوانین مرتبط با جرم جعل را مورد کنکاش قرار داده و رویکرد کلی مقابله با جرائم را در دو گزینه، اقدامات کیفری و غیرکیفری تقسیم بندی می‌نماید. در زمینه اقدامات کیفری سعی می‌شود از طریق جرم انگاری هنجارشکنی‌ها و سوء استفاده‌های جدید و یا تجدید نظر در قوانین کیفری گذشته، ارباب پذیری مؤثری درباره مجرمان بالقوه صورت گیرد، اما رویکرد غیر کیفری که در بستر جرم شناسی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان‌شناسی، جامعه‌شناسی پدید آمده، اتخاذ تدابیر پیشگیرانه را در دستور کار خود قرار داده است. از مهم‌ترین و مؤثرترین این الگوها می‌توان به پیشگیری وضعی اشاره کرد. در واقع کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. در گفتار پایانی پژوهش به راهبردها و تدابیر پیشگیرانه وضعی در فضای سایبر پرداخته و این‌گونه تدابیر را در چهار گروه مورد بحث قرار می‌دهد که در تدابیر نظارتی، این تدابیر را به طور خلاصه در دو شیوه مورد بررسی قرار می‌دهد. یک شیوه اتخاذ تدابیر نظارتی در دنیای فیزیکی است که قراردادن سیستم رایانه‌ای در نقاطی از منزل که در معرض دید عمومی باشد و توسط والدین صورت می‌گیرد و شیوه دیگر نظارت الکترونیکی است که با بکارگیری تجهیزات و برنامه‌های خاص، فعالیت‌های شبکه‌ای افراد تحت نظر قرار می‌گیرد. تدابیر صدور مجوز یکی از شیوه‌های رایج سلب فرصت مجرمانه یا حتی جلوگیری از بزه‌دیدگی و افراد، کنترل دسترسی است و تنها کسانی که می‌تواند به محیط‌هایی با ویژگی‌های خاص وارد شوند که تأییدیه مورد نظر را داشته باشند.

از دیگر تدابیر پیشگیرانه وضعی استفاده از ناشناس‌کننده‌ها و رمزنگارها است. رمزنگاری اطلاعات فرد را از مقابل دیدگان تمامی اشخاص (به استثناء آن‌هایی که مجاز شمرده می‌شوند) پنهان می‌کند. از دیگر اقدامات، تدابیر محدودکننده دسترسی (فیلترینگ) است که از ورود یا ارسال برخی داده‌های غیرمجاز جلوگیری می‌کند، بعضی یک‌سویه عمل می‌کنند، یعنی فقط از ورود یا خروج موارد غیرمجاز جلوگیری می‌کنند،

اما بعضی دیگر عمل دوسویه دارند. با توجه به موقعیت و مبنای عمل فیلترها، آن‌ها را به چهار گروه تقسیم بندی نموده که عبارت‌اند از فیلتر از سوی مشتری، فیلتر از سوی ارائه‌دهنده خدمات دسترسی حضوری (کافی نت) یا ارائه دهنده خدمات اینترنتی، فیلتر از سوی سرور و فیلتر از سوی ایجادکننده نقطه تماس بین المللی. در نتیجه با تدابیر فوق می‌توان آسیب‌های اجتماعی فضاهای مجازی نو پدید را به طور قابل ملاحظه‌ای کاهش داد.



کتابنامه

- جلالی فراهانی، امیرحسین. ۱۳۸۶ش، **تأملی بر فیلترینگ**، تهران: مرکز پژوهش‌های مجلس شورای اسلامی، شماره ۸۵۸۱.
- جنکینز، ریچارد. ۱۳۹۱ش، **هویت اجتماعی**، ترجمه تورج یار احمدی، تهران: نشر شیرازه.
- حاجیانی، ابراهیم. ۱۳۸۸ش، **جامعه‌شناسی هویت ایرانی**، تهران: پژوهشکده تحقیقات استراتژیک.
- خلقتی، مرضیه. ۱۳۸۷ش، **بحران‌های هویت‌های مجازی در گمنامی چت**، درس مدیریت بحران، دانشکده علوم اجتماعی دانشگاه تهران.
- عباسی‌قادی، مجتبی و خلیلی‌کاشانی، مرتضی. ۱۳۹۰ش، **تأثیر اینترنت بر هویت ملی**، تهران: پژوهشکده مطالعات راهبردی.
- فضلی، مهدی. ۱۳۸۹ش، **مسئولیت کیفری در فضای سایبر**، چاپ اول، تهران: انتشارات خرسندی.
- کاستلز، مانوئل. ۱۳۸۰ش، **عصر اطلاعات: اقتصاد، جامعه و فرهنگ**، ترجمه حسن چاوشیان، جلد ۲، تهران: طرح نو.
- گودرزی، حسین. ۱۳۸۴ش، **گفتارهایی درباره جامعه‌شناسی هویت در ایران**، تهران: مؤسسه مطالعات ملی.
- گیبیز، جان و ریمر، بو. ۱۳۸۸ش، **سیاست پست مدرنیته**، ترجمه منصور انصاری، تهران: گام نو.
- گیدنز، آنتونی. ۱۳۸۶ش، **جامعه‌شناسی**، ترجمه حسن چاوشیان، تهران: نشر نی.

منابع لاتین

- Adrian, A. (2008), "No One Knows You Are a Dog: Identity and Reputation in Virtual Words", *Computer Law and Security Report*, Vol. 24: 366- 374
- Katz, S.; Marshal, B. (2006), "New Sex for Old: Life Style, Consumerism and the Ethics of Aging Well", *Journal of Agibg Studies*, Vol. 17: 3- 16
- Bartle, R. (2004), *Designing Virtual Worlds*, London: Routledge.
- Pempek, T., & et al. (2009), "College students' social networking experiences on Facebook", *Journal of Applied Developmental Psychology*, 30: 227-238.
- Bell, D. (2001), *An Introduction to Cyberspace*, London: Rutledge.
- Shinder, D. L. (2002), *Scene of the Cyber Crime*, Computer Forensics Hand Book; Syngress Publication.
- Board on Children, Youth and Families (2004), *Technical, Business and Legal Dimensions of Protecting Children from Pornography on the Internet*, National Academy Press.
- Thornburgh, D. & S.Lin, H. (Eds.) (2004), *Youth, Pornography and the Internet*, National Academy Press.

مقالات

- اخگری، محمد. ۱۳۸۸م، «**اطلاعات حکمت و معرفت**»، فلسفه کلام و عرفان: مجلات، هویت انسانی در رسانه‌های مجازی، شماره ۴۰.

- جهانگیر. ۱۳۸۴ش، «هویت و مجاز: تأثیر هویت اینترنتی»، فصلنامه مطالعات ملی، شماره ۴، صص ۱۰۷-۱۲۴.
- دوران، بهزاد. ۱۳۸۳ش، «هویت خانوادگی و تعامل در فضای سایبر»، مجله زبان و ادبیات، شماره ۴۴.
- ربیعی، علی. ۱۳۸۷ش، «رسانه‌های نوین و بحران هویت»، فصلنامه مطالعات ملی، سال نهم، شماره ۴، صص ۱۴۹-۱۷۶.
- رفعت جاه، مریم و علی شکوری. ۱۳۸۷ش، «اینترنت و هویت اجتماعی»، فصلنامه جهانی رسانه، شماره ۵، صص ۱-۱۷.
- ساروخانی، باقر و رضایی‌قادی. ۱۳۹۱ش، «اینترنت و هویت ملی در میان کاربران»، فصلنامه فرهنگ ارتباطات، سال دوم، شماره ۵، صص ۵۱-۷۰.
- سبحانی جو. ۱۳۸۳ش، «هویت و بحران هویت»، مجله پیوند، شماره ۳۰۱.
- عاملی. ۱۳۸۸ش، «جزوه کلاسی درس مطالعات فضای مجازی»، مقطع کارشناسی ارشد مطالعات فرهنگی و رسانه.
- عاملی، سعیدرضا. ۱۳۸۲ش، «دو جهانی شدن‌ها و جامعه جهانی اضطراب»، نامه علوم اجتماعی، شماره ۲۱، صص ۱۴۳-۱۷۴.
- عدلی‌پور، صمد. ۱۳۹۱ش، «تحلیل جامعه‌شناختی پیامدهای شبکه‌های اجتماعی مجازی بر هویت اجتماعی کاربران جوان شهر اصفهان»، رساله کارشناسی ارشد جامعه‌شناسی، دانشگاه اصفهان.
- عمیدی، مهدی. ۱۳۸۷ش، «مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران»، پایان نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز.
- کوهی، کمال و حسنی، محمدرضا. ۱۳۹۱ش، «رابطه استفاده از رسانه‌های نوین با ابعاد هویتی در نوجوانان و جوانان ۱۴ تا ۲۹ ساله شهر تبریز»، فصلنامه پژوهش‌های ارتباطی، سال نوزدهم، صص ۱۰۹-۱۳۰.
- معینی‌علمداری، جهانگیر. ۱۳۸۴ش، «هویت و مجاز: تأثیر هویت اینترنتی»، فصلنامه مطالعات ملی، شماره ۴، صص ۱۰۷-۱۲۴.
- مهدی‌زاده، شراره و عنبرین، زینب. ۱۳۸۸ش، «بررسی رابطه میزان و نحوه استفاده از اینترنت و هویت فرهنگی جوانان»، فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات، شماره ۱۷، صص ۲-۲۸.