بررسی جرم‌شناختی بزهکاری سایبری با تأکید بر نظریه‌ی فعالیت روزمره

سید علی شریفی[۱]

[۱]دانشجوی کارشناسی ارشد حقوق کیفری اطفال و نوجوانان، دانشکده حقوق و علوم سیاسی، دانشگاه تهران
sharifi1997@ut.ac.ir

چکیده

گسترش فنّاوری و استفاده از فضای سایبر، کوچ بزهکاران دنیای واقعی به دنیای مجازی را به دنبال داشته و جرائم نوینی را در بستر اینترنت ایجاد نموده است. منظور از بزه سایبری مجموعه فعالیت‌های مجرمانه‌ای است که در آن‌ها رایانه یا شبکه به عنوان ابزار، هدف یا بستری برای انجام این فعالیت‌ها به کار گرفته می‌شود. نظریه‌ی فعالیت روزمره به عنوان یکی از نظریه‌های مهم جرم‌شناسی در حوزه‌ی جرایم سایبری وجود سه عامل مهم یعنی وجود بزهکار بالقوه، حضور آماج مناسب به‌عنوان بزه‌دیده‌ی جرم و نیز فقدان نگهبان توانا را در ارتکاب جرم اینترنتی مؤثر می‌داند. این مقاله با تکیه بر مفاهیم مذکور در این نظریه با استفاده از روش توصیفی-تحلیلی و از طریق منابع کتابخانه‌ای به دنبال تبیین مؤلفه‌های مربوط به بزهکاری سایبری بوده و اقدامات لازم از جمله تدابیر مربوط به پیشگیری وضعی را به‌عنوان راه‌حل کاهش نرخ جرایم سایبری پیشنهاد می‌نماید.

کلمات کلیدی: فضای سایبری، بزهکاری سایبری، فعالیت روزمره، جرم‌شناسی، پیشگیری وضعی.

۱ مقدمه

در طی دهه‌های اخیر و با پیشرفت و توسعه‌ی فناوری، ابنای بشر به‌موازات زندگی در دنیای واقعی، تجربه‌ی زیست نوینی را در دنیای سایبر به دست آورده است. این فضا علیرغم منافع بسیاری که برای زندگی انسان فراهم داشته، چالش‌های جدیدی را نیز پیش روی او قرار داده است. یکی از این چالش‌ها، مهاجرت بزهکاران دنیای واقعی به فضای سایبر و نیز شکل‌گیری انواع و اقسام جدیدی از جرایم مخصوص به فضای مجازی است. ویژگی‌هایی همچون ناشناس بودن هویت افراد و فقدان امکانات مناسب جهت شناسایی متهمین، سرعت بسیار زیاد تبادل و تغییر اطلاعات، عدم حضور کنترل گران بیرونی و اجتماعی، جهانی بودن و عدم وابستگی به منطقه‌ی جغرافیایی خاص و... فضای مجازی را به محلی ایمن برای ارتکاب جرم بدل ساخته است.

از ابتدای ایجاد اصطلاح جرم سایبری و ارتکاب اولین جرایم در این فضا، جرم شناسان با استفاده از نظریه‌های گوناگون به بررسی ابعاد مختلف این‌گونه جرایم پرداخته و درصدد تبیین عوامل مؤثر بر ارتکاب این جرایم و نهایتاً کاهش نرخ بزهکاری سایبری برآمدند. هرچند که به‌واسطه‌ی جدید بودن موضوع، نظریات مترقیانه‌ی جرم‌شناسی آنچنان که باید هنوز شکل نگرفته است لکن نوآوری‌های جرم شناسان در این زمینه قابل‌توجه می‌باشد. نظریه‌ی «انتقال فضا» یکی از این ابتکاراتی است که با عبور از جرم‌شناسی سنتی، به دنبال بررسی علل و عوامل وقوع جرم در فضای مجازی با تکیه‌بر ساختارها و ویژگی‌های مرتبط با فضای سایبری است. نظریات نوین جرم‌شناسی، مانع از به‌کارگیری نظریات سنتی جرم‌شناسی برای تبیین علل و عوامل بزهکاری در این حوزه نخواهد بود. چرا که باوجود تفاوت‌های عمده میان دنیای واقعی و مجازی با یکدیگر، بسیاری از مؤلفه‌های مربوط به بزهکاری به‌صورت مشترک میان این دو فضا وجود دارد. مکاتب جرم‌شناسی سنتی، به‌طورکلی عوامل وقوع بزهکاری در سه گروه علل زیستی، علل روانی و علل محیطی- اجتماعی تقسیم‌بندی نموده و نظریات خود را ذیل هر یک از این سه گروه بیان می‌نماید. نظریه‌ی فعالیت روزمره یکی از نظریات سنتی جرم‌شناسی است که ذیل علل محیطی- اجتماعی قرار گرفته و وقوع بزه را از منظرهای گوناگون مورد بررسی قرار می‌دهد. در این نوشتار، ابتدائاً به شناخت انواع جرایم سایبری (بخش اول) پرداخته؛ سپس با تبیین نظریه‌ی فعالیت روزمره در ساحت محیط سایبری (بخش دوم)، راهکارهایی برای کاهش نرخ بزه سایبری (بخش سوم) ارائه خواهد شد.

۲ جرایم سایبری

جرایم سایبری، همچون دیگر حوزه‌های مرتبط با فنّاوری سیر تطور و تکامل خود را از شکل بسیط و مضیق، به اشکال پیچیده و گسترده طی نموده است. تا اواخر دهه‌ی ۱۹۸۰ میلادی، جرایم تنها در حوزه‌ی کامپیوتر و به‌صورت ساده در خصوص داده‌ها و برنامه‌های رایانه‌ای از طریق سرقت و کپی برنامه‌ها انجام می‌گرفت. پس از آن، در دهه‌ی ۱۹۹۰ میلادی، جرایم علیه داده‌ها شکل پیچیده‌تری به خود گرفت و جرایم علیه فنّاوری اطلاعاتی و ماهواره‌های مخابراتی نیز ارتکاب می‌یافت. در نهایت با گسترش اینترنت و در اختیار عموم قرار گرفتن فنّاوری مفهوم جرم سایبری نیز ایجاد شد (ابوذری،۱۳۹۱: ۲۰).

جرم سایبری به صورت‌های گوناگون توسط اندیشمندان تعریف شده است. مارکو گرکی، هرگونه فعالیت که در آن رایانه یا شبکه ابزار، هدف یا مکانی برای فعالیت تبهکاری بکار می‌رود را جرم سایبری تعریف نموده است. (ابوذری،۱۳۹۱: ۲۱) کنوانسیون جرایم سایبری نیز با احصای مصادیق مرتبط، اقدام به تعریف جرم سایبری نموده است؛ از نگاه این کنوانسیون، ۵ گروه از جرایم سایبری وجود دارد که عبارت است از: الف) جرایم علیه محرمانگی، تمامیت و دسترسی‌پذیری ب) جرایم مرتبط با رایانه ج) محتوای هرزه‌نگاری د) نقض حق نشر ه) محتوای ضد بیگانه و نژادپرستانه. لازم به ذکر است که قانون جرایم رایانه‌ای مصوب ۱۳۸۸ مجلس شورای اسلامی نیز با پیروی از کنوانسیون جرایم رایانه‌ای، تقسیم‌بندی مشابهی را برای این‌گونه جرایم ذکر نموده است. از میان تعاریف گوناگون در مجموع می‌توان جرم سایبری را معطوف به جرایمی دانست که در یکی از سه حوزه‌ی زیر ارتکاب می‌یابد: الف) جرایمی که رایانه در آن به‌مثابه‌ی موضوع و آماج جرم مورد

استفاده قرار می‌گیرد. برای مثال، در سرقت رایانه‌ای، اطلاعاتی که در یک رایانه ذخیره شده است مورد تجاوز و هتک قرار می‌گیرد و در آن رایانه به‌عنوان موضوع سرقت خواهد بود. ب) جرایمی که در آن رایانه به‌عنوان ابزار جرم بکار گرفته می‌شود. برای نمونه، پورنوگرافی اطفال و نوجوانان امری مستقل از رایانه و سامانه‌های رایانه‌ای می‌باشد لکن استفاده از رایانه و فضای سایبر در تسهیل ارتکاب این جرم بسیار مؤثر می‌باشد. ج) جرایمی که به‌طور خاص مرتبط با رایانه می‌باشد و مشابه آن در محیط واقعی قابل مشاهده نیست. جرم هک نمودن رایانه مثال خوبی برای این دسته از جرایم است.

۱.۲ بزهکاران سایبری

بزهکاران سایبری در مقایسه با افرادی که در فضای واقعی مرتکب جرم می‌شوند تفاوت‌های مهمی دارند. این تفاوت‌ها به دلیل آن است که ارتکاب بزه در محیط سایبری نیازمند توانمندی‌های خاصی از قبیل آشنایی با فناوری‌ها و فنّاوری‌های مرتبط با حوزه‌ی سایبر است و بزهکاران در این محیط دارای توانایی‌های فنی و تخصصی بیشتری نسبت به مجرمین عادی هستند. مجرمین این حوزه به دو دسته تقسیم می‌شوند. دسته‌ی اول، اشخاصی هستند که جرم را در محیط‌های واقعی نیز مرتکب می‌شوند و فعالیت‌های مجرمانه‌ی خود را به فضای سایبری انتقال داده‌اند. این افراد عمدتاً به دنبال کسب منفعت مالی از فضای سایبر هستند و با همین انگیزه نیز مرتکب جرم می‌گردند. دسته‌ی دوم، شامل اشخاصی است که در فضای واقعی شهروندان قانون‌مداری بوده و رفتار بهنجاری از آن‌ها انتظار می‌رود، لکن در محیط مجازی و به دلیل ویژگی‌های خاص این محیط مرتکب اعمال مجرمانه می‌شوند.

مطالعات نشان می‌دهد افرادی که محیط برخط را برای سرگرمی انتخاب کرده‌اند گرایش بیشتری به ارتکاب رفتارهای مجرمانه دارند؛ در مقابل، افرادی که فضای مجازی و به‌ویژه شبکه‌های اجتماعی را امری فراتر از سرگرمی‌های ناپایدار و زودگذر تلقی می‌نمایند و علقه‌های اجتماعی و نشانه‌های وفاداری به این محیط را از خود نشان می‌دهند، احتمال کمتری دارد که مرتکب جرایم در فضای مجازی شوند. گردشگران فضای مجازی که این محیط را صرفاً سرگرمی تلقی می‌کنند در جرایم کمتر فنی‌تری همچون توهین و هرزه‌نگاری را دنبال می‌کنند اما مجرمین با مهارت فنی بالا عمدتاً جرایم مهم‌تری از قبیل آزار سایبری، هک و ویرانگری را مرتکب می‌شوند. اساساً افرادی که به دلیل وجود علقه‌های اجتماعی و ساعات طولانی حضور در فضای مجازی و شبکه‌های اجتماعی شهروندان فضای مجازی قلمداد می‌شوند، نسبت به گردشگران این محیط بیشتر مرتکب نقض هنجارهای گروهی و بزه‌های جدی‌تر می‌گردند (ویلیامز، ۱۳۹۰: ۲۴).

در تقسیم‌بندی دیگری، مجرمین سایبری به چهار گروه تقسیم می‌شوند. گروه اول، مجرمین کینه‌جو هستند که دارای شخصیتی بدذات بوده و بیشتر از دیگران اقدام به تهدید و آزار بزه دیدگان می‌نمایند؛ در رفتار این گروه تداوم فعالیت‌های آزاردهنده به‌وفور یافت می‌شود. گروه دوم، مجرمینی هستند که قربانیان را به‌صورت آرام و به دور از هیاهو تعیین کرده و از طریق رفتارهای تهدیدآمیز اقدام به آزار آن‌ها می‌نماید. گروه سوم، با ایجاد رابطه‌ی صمیمانه با بزه دیده به دنبال عقده‌گشایی و حل مشکلات روحی خود هستند و درنهایت گروه چهارم، مجرمینی هستند که دارای مهارت بالای فنی بوده و به‌صورت جمعی مرتکب جرایم سایبری می‌شوند. این گروه از حیث جرم‌شناسی و عمق خساراتی که وارد می‌نمایند، از اهمیت بالاتری

برخوردار هستند (رستگار صولتی، ۱۳۹۴: ۳۷).

۲.۲ بزه‌دیدگی سایبری

قربانیان در فضای سایبری ویژگی‌های متمایزکننده‌ای نسبت به بزهکاران فضای واقعی دارد. بر اساس آمار مراجع رسمی در سال ۱۳۹۶ استفاده‌کنندگان زیر ۱۸ سال از اینترنت در ایران، نزدیک به بیست میلیون نفر بوده است (اقتصاد نیوز، کد خبر:۱۶۸۵۲۰). این امر نشان‌دهنده‌ی حضور بسیار پررنگ اطفال و نوجوانان در اینترنت و به‌خصوص شبکه‌های اجتماعی به‌مثابه‌ی افرادی بدون توان حفاظت از خود در میان انبوهی از بزهکاران بالقوه می‌باشد. در یک تقسیم‌بندی کلی از دیدگاه هنتینگ، بزه دیدگان فضای سایبری را می‌توان به دو گروه بزه دیدگان بی‌گناه یا معصوم و بزه دیدگان مقصر یا بی‌احتیاط تقسیم‌بندی نمود. بزه دیدگان بی‌گناه افرادی هستند که حضور در این فضا را با اقداماتی ازجمله نصب آنتی‌ویروس، عدم مراجعه به لینک‌های نامعتبر و مشکوک و... تأمین نموده و هوشیاری نسبتاً مطلوبی را نسبت به مخاطرات موجود در فضای مجازی از خود نشان می‌دهند. در مقابل این افراد، گروهی از استفاده‌کنندگان از اینترنت و فضای مجازی با خواندن هرزنامه‌ها، دانلود بدافزارها، نصب فیلترشکن، گشت‌وگذار بی‌مورد در سایت‌های غیرقانونی بی‌احتیاطی خود را در استفاده‌ی از این فضا نشان می‌دهند. از نگاه شیندر، بزه دیدگان سایبری در شش گروه کلی تقسیم‌بندی می‌شوند: ۱- تازه‌واردان سایبری و افرادی که آشنایی با مخاطرات و ویژگی‌های فضای مجازی ندارند. ۲- افراد ساده‌لوح و زودباور که عمدتاً شامل دو گروه اطفال و افراد مسن و کهن‌سال می‌شوند. ۳- اشخاص ناتوان و آسیب‌پذیر که شرایط ویژه‌ی فردی آن‌ها منجر به بزه‌دیدگی آن‌ها می‌شود. ۴- افرادی که با اعمال و رفتارهای خود ازجمله حضور دائم در چت‌روم‌ها، سایت‌های مستهجن و ... زمینه‌ی بزه‌دیدگیشان را فراهم می‌کنند. ۵- قربانی‌نماهایی که با حیله و فریب به مقامات پلیس اعلام بزه‌دیدگی می کنند در حالی که واقعاً بزه دیده نشده‌اند. ۶- بزه‌دیدگان بدشانس که به‌صورت اتفاقی مورد بزه دیدگی واقع می‌شوند (ابوذری، ۱۳۹۱: ۳۴).

مسئله‌ی دیگری که در خصوص بزه دیدگان سایبری باید به آن توجه نمود آن است که این افراد درصورتی‌که یک‌بار موضوع بزه قرار بگیرند، احتمال بزه دیدگی ثانویه در آن‌ها بسیار زیاد است. در سال ۱۹۹۲، ۶۳ درصد بزه‌دیدگان جرایم مالی و ۷۷ درصد جنایات علیه اشخاصی انجام شد که دارای سابقه‌ی بزه دیدگی بودند (ابوذری، ۱۳۹۱: ۴۴).

بررسی موارد فوق نشان می‌دهد که در اینگونه جرایم، توجه به بزه دیده نیز به‌موازات توجه به بزهکار اهمیت دارد؛ بنابراین دستیابی دقیق‌تر به عوامل و علل وقوع بزه نیازمند آن است که نظریاتی از جرم‌شناسی مورد استفاده قرار گیرد که نگاه خود را بیش از بزهکار به شرایط وقوع جرم و قربانی بالقوه‌ی جرم به‌عنوان یکی از ارکان مداخله‌گر معطوف دارد. نظریه‌ی فعالیت روزمره یکی از این نظریات است که با تکیه‌بر عناصر سه‌گانه‌ی وقوع جرم اقدام به تحلیل عوامل مداخله‌گر می‌نماید.

۳ نظریه‌ی فعالیت روزمره

در تعریفی ساده و کلی، عوامل محیطی مؤثر در وقوع جرایم سایبری علیه اطفال و نوجوانان را مجموعه‌ی عوامل به وجود آورنده‌ی جرم می‌دانند که مستقل از شخص بزهکار تعریف می‌شود. این عوامل، بر اراده‌ی شخصی افراد تأثیرگذار بوده و آن‌ها را به سمت ارتکاب جرایم و تخلفات و سرپیچی از هنجارهای جامعه دعوت می‌نماید. گستردگی مصادیق این تعریف، فراگیر بودن و مهم‌تر از همه در معرض بودن همه‌ی افراد جامعه در برابر این عوامل باعث شده است تا آن‌ها را مهم‌ترین و اصلی‌ترین عامل وقوع جرایم بدانیم. بدیهی است که بسیاری از اختلالات روانی منجر به ارتکاب جرایم در افراد، زاییده‌ی شرایط محیطی و اجتماعی آن‌ها بوده و در مقابل، عوامل زیستی در صورتی به پدیده‌ی مجرمانه منجر می‌گردد که شرایط و عوامل محیطی بستر مناسب ظهور و بروز آن‌ها را مهیا نماید. این امر، خود نمایانگر اهمیت عوامل محیطی و تأثیر بسیار آن‌ها بر سایر عوامل و مؤلفه‌های مؤثر در وقوع جرایم است.

از اوایل دهه ۱۹۷۰ میلادی، جرم شناسان تمرکز خود را از مطالعات مربوط به بزهکاران، به مطالعات مربوط تأثیر جرم بر روی بزه دیدگان تغییر دادند. نظریه فعالیت‌های روزمره نیز در زمانی مطرح شد که نظام عدالت کیفری تأکید خود بر روی موضوعات بزه دیدگی را آغاز کرده بود. در این زمان نظریه‌ی سبک زندگی و نظریه‌ی فعالیت‌های روزمره به‌عنوان دیدگاه‌های نظری عقلانی در جامعه‌شناسی ارائه شدند. این دو نظریه برای تحلیل علت وجود احتمال بیشتر بزه دیده شدن افراد با توجه به فعالیت‌ها، تعاملات و ساختار اجتماعی سبک‌های زندگی خویش مورد استفاده قرار گرفتند (Williams & McShane, 1999: 134).

تحقیقات پیشین هیندلینگ و همکارانش به مسئله نقش سبک زندگی روزانه افراد چه در محل کار و چه در منزل بر بزه دیده شدن افراد می‌پرداخت. مسئله‌ی تأثیر نقش موقعیت اجتماعی فرد بر الگوهای سبک زندگی نیز مورد بحث این دو محقق بوده است؛ بنابراین به نظر می‌رسد که سه عامل اصلی در پیش‌بینی بزه دیده شدن یک فرد وجود داشته باشد. اول، ضرورت وجود یک فرد با انگیزه به‌عنوان بزهکار. دوم، ضرورت وجود هدفی مناسب به‌عنوان آماج جرم و بزه دیده‌ی بالقوه. سوم، عدم وجود یک نگهبان توانا برای محافظت از بزه دیده در مقابل رفتار مجرمانه‌ی بزهکار. برای تحقق بزه دیدگی نبود هرکدام از این عوامل احتمال ارتکاب جرم علیه فرد یا افراد را کاهش می‌دهد. بنابراین، ارتکاب یک بزه چه در محیط واقعی و چه در محیط مجازی مستلزم ترکیب این سه عامل با یکدیگر می‌باشد (Cohen & Felson, 1979: 590).

نظریه‌ی فعالیت روزمره به‌نوعی به دنبال گسترده‌تر نمودن یافته‌های نظریه‌ی سبک زندگی است که علاوه بر رفتارهای روزمره‌ی انسان‌ها، به بررسی فعالیت‌های شغلی و تفریحی افراد نیز می‌پردازد. فلسن، برای مناسب بودن یک فرد به‌عنوان آماج جرم، چهار ملاک را ارائه می‌کند: ۱-ارزش هدف جرم ۲- میزان تحرک هدف جرم ۳- مرئی بودن فیزیکی هدف جرم ۴- در دسترس بودن هدف جرم. (جیشانکار، ۱۳۹۵: ۳۳۶) آنچه در مورد جرایم سایبری وجود دارد آن است که هدف به‌صورت فیزیکی در مرئی و منظر بزهکار قرار ندارد.

بزهکار رایانه‌ای با استفاده از فنون ارتکابی جرم در فضای سایبری باعث می‌شود که هدف تحرک خود را از دست بدهد؛ همچنین، در دسترس بودن افراد واجد شرایط بزه دیدگی در محیط سایبر بسیار زیاد است؛

بنابراین باید جهت کنترل بزه دیدگی در این محیط، سطح توان نگهبانی را افزایش داد. این امر با استفاده از استراتژی سخت کردن هدف صورت می‌گیرد (Yar, 2005: 410) به گفته‌ی هیندلینگ و همکاران، فعالیت‌های کاری و تفریحی مهم‌ترین عوامل در سبک زندگی افراد محسوب می‌شوند که مستقیماً احتمال بزه دیدگی افراد را تحت تأثیر قرار می‌دهند. در مورد نوجوانان حاضر در فضای مجازی باید فعالیت‌های آموزشی و تحصیلی را نیز به حوزه‌های فوق اضافه نمود. از طرف دیگر، افراد درگیر در فعالیت‌های مرتبط با زندگی بزهکارانه با احتمال بیشتری به اهداف مناسب برای بزه دیدگی تبدیل می‌شوند و دلیل بزه دیدگی آن‌ها عدم تمایل به‌مواجهه با نظامات حقوقی و کیفری است (جیشانکار،۱۳۹۵: ۳۳۷).

با تحول فناوری جدید، فعالیت‌های روزمره‌ی کودکان از بازی‌هایی همچون دوچرخه‌سواری و بازی با عروسک‌ها به بازی‌های ویدئویی و اینترنت تغییر یافته است. در سال ۲۰۰۶، حدود ۸۷ درصد از جوانان از اینترنت استفاده می‌نمودند که این آمار به طرز شگفت‌انگیزی افزایش داشته است. همگام با ظهور فناوری‌های جدید بزه دیدگی این افراد در فضای مجازی نیز افزایش داشته است. از نگاه سمپسون، کاهش احتمال بزه دیدگی با استفاده از تمهیدات حفاظتی است. این پژوهش بیان می‌دارد که نمی‌توان فعالیت‌های نوجوانان را در اینترنت از جهت زمانی محدود نمود و تمهیدات حفاظتی نیز برای کاهش بزه دیدگی این افراد کافی نیست؛ بنابراین بهتر است آموزش مخاطرات به نوجوانان را هم‌زمان با استفاده از اقدامات حفاظتی افزایش داد (جیشانکار، ۱۳۹۵: ۳۵۸).

در نگاه جرم‌شناسی سنتی می‌توان ۳ نگهبان توانا را برای کاربران اینترنت مفروض داشت. برنامه‌های ضدویروس، برنامه‌های ضد جاسوسی و تدابیر پیشگیری‌کننده از ورود (فایروال) (Moore, 2005: 2) درصورتی‌که برنامه‌های ضدویروس، بدافزاری را شناسایی نمایند که امنیت کاربر را به مخاطره بیندازد آن را منزوی نموده و یا از بین می‌برد. نرم‌افزارهای ضد جاسوسی نیز در راستای حذف توانمندی‌های بدافزارهای جاسوسی هستند که با استفاده از رهگیری اطلاعات کاربری و رمزهای عبور کاربران، اقدام به ارتکاب جرم سرقت رایانه‌ای می‌نمایند. تدابیر پیشگیری‌کننده از ورود نیز، اجازه‌ی ورود بدافزارها را به درون سامانه‌های کامپیوتری را نمی‌دهد و از این طریق حفاظت و امنیت کاربر را تأمین می‌نماید. به‌طورکلی، احتمال بزه دیدگی سایبری برای افرادی که به شکل منظم و روزآمد نرم‌افزارهای امنیتی خود را بروزرسانی می‌نمایند، استفاده‌ی آن‌ها از اینترنت دائمی و مداوم نبوده و رفتارهای خطرناک آنلاین را نیز انجام نمی‌دهند بسیار کمتر از سایر افراد است. این موضوع نشان می‌دهد که تدابیر حفاظت کننده نیز تا حد زیادی تحت تأثیر رفتارها و آموزش‌های قبلی داده‌شده به کاربران فضای مجازی است. در ادامه، راهکارهای مستقل از کاربران اینترنت برای کاهش احتمال بزه دیدگی سایبری بررسی خواهد شد.

۴ راهکار کاهش نرخ جرایم سایبری

همانگونه که در مباحث قبلی مطرح گردید، استفاده از تدابیر حفاظت کننده‌ی سنتی و وابسته به کاربر نمی‌تواند به‌اندازه‌ی کافی برای کاهش جرایم سایبری مؤثر واقع شود. چرا که استفاده از این تدابیر نیازمند آموزش کاربران این حوزه می‌باشد در حالی که بسیاری از کاربران این حوزه را اطفال و نوجوانان و یا افراد

فاقد دانش فنی شامل می‌گردد. در مقابل، استفاده از تدابیر حفاظت کننده‌ی هوشمند می‌تواند مستقل از اراده‌ی کاربر از وی حفاظت نموده و به‌عنوان نگهبانی توانا در عرصه‌ی فضای مجازی ظاهر گردد. اساساً از آنجایی که در جرایم فضای مجازی از عنصر فناوری استفاده می‌گردد الزاماً باید برای پیشگیری از آن‌ها نیز از فناوری کمک گرفت.

هوش مصنوعی به‌عنوان یکی از دستاوردهای فناوری که به‌عنوان هنر اندیشیدن ماشین و عمل نمودن آن مانند انسان تعریف می‌شود می‌تواند در پیشگیری از جرایم از طریق کارکردهای گوناگون آن بسیار مؤثر واقع شود. برای مثال، آزار و اذیت سایبری می‌تواند مشکلات زیادی را برای بزه دیدگان علی‌الخصوص افراد دارای ناپایداری عاطفی و اختلالات روانی ایجاد نماید؛ در اینگونه موارد هوش مصنوعی با به‌کارگیری الگوریتم‌های تشخیص خود، این افراد را شناسایی نموده و با تشخیص هوشمند محتواهای آزاردهنده از وصول اینگونه محتواها به بزه دیدگان بالقوه جلوگیری نماید (Rakhmator, 2022: 125).

استفاده از این روش تاکنون مورداستفاده‌ی بسیاری از کشورها نیز بوده است. در سال ۲۰۱۲ بانک‌های هلند ۸۰ میلیون یورو خسارت ناشی از جرایم سایبری را متحمل شدند؛ اما پس از آن با استفاده از فناوری نوین هوش مصنوعی و تجزیه‌وتحلیل داده‌ها و شناسایی رفتار غیرمعمول مشتریان اقدام به شناسایی و پیشگیری از ارتکاب دوباره‌ی جرایم مالی سایبری نمودند (J.Halt, 2019: 220).

۵ نتیجه‌گیری

جرایم سایبری امروزه از واقعیت‌های عصر حاضر در دنیای مجازی به شمار می‌آید که روزبه‌روز بر شمار افراد درگیر با این پدیده افزوده می‌شود. با توجه به نظریه‌ی فعالیت روزمره که یکی از نظریات مهم در جرم‌شناسی سنتی است، وجود یک نگهبان توانا در محیط مجازی می‌تواند از بروز بزهکاری جلوگیری و به‌عنوان سدی مستحکم در مقابل بزهکار بالقوه و بزه دیده‌ی بالقوه عمل نماید. تدابیر حفاظت کننده‌ی سنتی که نیازمند اعمال از طریق کاربر و یا افراد مرتبط با حوزه‌ی بزهکاری سایبری هستند نمی‌تواند در مقابل فناوری‌های پیچیده‌ی بکار رفته در اینگونه جرایم مؤثر واقع شود و پیشگیری از آن‌ها نیازمند استفاده از تدابیر فناورانه‌ای است که بتواند مستقل از اراده‌ی انسان عمل نماید. فناوری هوش مصنوعی که خود منبعث از گسترش و توسعه‌ی فنّاوری به‌ویژه در حوزه‌ی سایبری است می‌تواند به‌مثابه‌ی سدی مستحکم و مستقل از اراده‌ی افراد در مقابل بزهکاران فضای مجازی عمل نماید.

مراجع

[۱] ابوذری، مهرنوش، جرم‌شناسی جرایم سایبری، چاپ اول، نشر میزان، ۱۳۹۵.

[۲] پایگاه خبری تحلیلی اقتصاد نیوز، قابل‌دسترسی از: www.eghtesadnews.com

[۳] جیشانکار، کی، جرم‌شناسی فضای مجازی کشف جرایم اینترنتی و رفتار مجرمانه، ترجمه‌ی دکتر حمیدرضا ملک‌محمدی، چاپ اول، انتشارات میزان، ۱۳۹۴.

[۴] رستگار صولتی، محمد سعید، علت‌شناسی بزه دیدگی نوجوانان در فضای سایبر، پایان‌نامه کارشناسی ارشد، دانشکده حقوق دانشکدگان فارابی دانشگاه تهران، ۱۳۹۴.

[۵] ویلیامز، متیو؛ ترجمه: منفرد، محبوبه؛ جلالی فراهانی، امیرحسین، بزه‌کاری مجازی: بزه، انحراف و مقررات گذاری بر خط، چاپ اول، انتشارات میزان، ۱۳۹۱.

[6] Cohen,L.E. & Felson, M, "Special change and crime rate trends: A routine activity approach," American Sociological Review, 1979.

[7] Dilmurod,Rakhmatov, "Methods and Effectiveness of the Use of Artificial Intelligence in the Fight Against Cyberbullying," Journal of Academic Research and Trends in Educational Sciences. Volume1, Issue4, 2022.

[8] Moore,R, "Cyber crime: investigating high-technology computer crime," Philadelphia, PA: LexisNexis, 2005.

[9] Thomas,J.Holt, "Cybercrime Through an Interdisciplinary Lens," Routledge, 2019.

[10] Williams, F.P. & McShane, M.D, "Criminological theory," Upper Saddle River, NJ: Prentice Hall, 1999.

[11] Yar, M, "The novelty of cybercrime: An assessment in light of routine activity theory," European Journal of Criminology, 2005.