**مطالعات فقهی و فلسفی**
**سال ششم، شماره ۲۳، پاییز ۱۳۹۴**
**صفحات ۳۲ ـ ۷**

# بررسی شیوه‌های پیشگیری از سرقت‌های اینترنتی

**سیدمحسن رضوی‌اصل*، احمد مرادخانی**، سیدمحمدمهدی احمدی***، سیدحسن عابدیان‌کلخوران*****

(تاریخ دریافت: ۱۳۹۵/۰۴/۳۰؛ تاریخ پذیرش: ۱۳۹۵/۰۵/۲۵)

## چکیده

فضای سایبری در کنار کارکردهای مهم و حیاتی‌اش، محل فعالیت انسان‌های فرصت‌طلب نیز می‌باشد. یکی از جرایمی که در فضای سایبری توسط این افراد رخ می‌دهد، سرقت داده‌ها و اطلاعات متعلق به دیگران می‌باشد. برای جلوگیری و هر چه کمتر نمودن ارتکاب این جرم، بالاخص توسط افرادی که سابقه‌دار نبوده و ویژگی‌های فضای مجازی آن‌ها را به ارتکاب جرم ترغیب می کند، استفاده از راه‌کارهای پیشگیری از جرم مؤثر می‌باشد. این راه‌کارها که شامل دو روش پیشگیری وضعی و پیشگیری اجتماعی می‌شوند، از جمله شیوه‌های تأثیرگذار در کاهش وقوع جرم سرقت اینترنتی هستند که هر چند در اصل برگرفته از شیوه‌های پیشگیری از سرقت‌های سنتی می‌باشند، لیکن با تطبیق آن‌ها با شرایط فضای سایبری، می‌توانند موجب کاهش سرقت‌های اینترنتی گردند.

## کلیدواژگان

پیشگیری، جرم، سایبر، سرقت اینترنتی، فضای مجازی.

---

* مسئول مکاتبات: دانشجوی دکتری فقه و مبانی حقوق اسلامی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران
رایانامه: Mohsen.razavy@gmail.com

** نویسنده مسئول: استادیار گروه فقه و حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران
رایانامه: Ah_moradkhani@yahoo.com

*** استادیار گروه فقه و حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران

**** استادیار گروه فقه و حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران

این مقاله مستخرج از پایان‌نامه است.

## مقدمه

پیشینه مقابله با جرم قدمتی برابر با تمدن بشری دارد. علی‌رغم این که همیشه میان اندیشمندان اختلاف نظر بر سر مجازات‌کردن یا اصلاح بزهکاران وجود داشته است، لیکن هیچ ابهامی در این خصوص وجود ندارد که بهترین راه حل برای از بین بردن یا کاهش رفتارهای غیرقانونی، پیشگیری است (محمدنسل، ۱۳۹۱، ص۱۱۲). اقدامات پیشگیرانه به منزله واکسیناسیون جامعه در مقابل جرایم می‌باشند و می‌توانند به دو صورت متجلّی شوند: ۱. اقدامات مربوط به زمان پیش از تحقق جرم؛ و ۲. اقدامات مربوط به زمان پس از وقوع جرم. آن بخشی که به نظر مهم‌تر رسیده و می‌بایست بیش از هر اقدام دیگری مورد توجه قرار گیرد، اقدامات پیش از وقوع جرم است، زیرا این مرحله است که می‌تواند در سالم‌سازی جامعه و هدایت افراد نقش عمده و اساسی ایفا نماید (ایرانشاهی، ۱۳۸۹، ص۵۷). برخلاف سرقت‌های سنتی، علل و عوامل و همچنین شیوه‌های ارتکاب سرقت‌های اینترنتی بسیار متنوع و مختلف می باشند. سرقت‌های سنتی به روش‌هایی مانند سرقت از بانک، جیب‌بری، کیف‌قاپی و ... ارتکاب می‌یابند و متناسب با نحوه ارتکاب سرقت، قانونگذار اقدام به جرم‌انگاری انواع مختلف سرقت نموده است. اما در سرقت‌های اینترنتی با شیوه‌های نوین ارتکاب جرم و به تعبیر دیگر با ریزومیک شدن جرایم روبه رو هستیم. در فضای سایبری، جرایم دیگر در یک جهت خاص و در جایی مشخص رخ نمی‌دهند، بلکه بیش از اندازه متکثر و پراکنده شده‌اند و قلمرو خاصی را نمی توان برای آن‌ها در نظر گرفت. این امر را می توان ناشی از سرعت بالای پیشرفت فن‌آوری در حوزه اطلاعات و ارتباطات دانست و شاید بتوان گفت به دلیل سرعت بالای این پیشرفت، قانونگذار همیشه یک گام عقب تر از فن‌آوری بوده و پس از قربانی شدن افراد بسیاری در فضای مجازی، به جرم‌انگاری و و اعمال اقدامات پیشگیرانه می پردازد (سلیمی، ۱۳۹۱، ص۱۷).

اگرچه آماری قطعی از سرقت‌های اینترنتی منتشر نشده است، لیکن تحقیقات انجام شده

بوسیله اداره تحقیقات فدرال آمریکا[1] و مؤسسه امنیت رایانه[2] نشان می‌دهند که شیوه‌های پیشگیری از سرقت‌های سنتی، در پیشگیری از سرقت‌های اینترنتی نیز مؤثر می‌باشند. (Turrini, 2010, p.369) لذا به نظر می‌رسد که برای مقابله همه جانبه و کارآمد با سرقت‌هایی که در فضای مجازی رخ می‌دهند، اتخاذ یک سیاست جنایی فراگیر و مبتنی بر مشارکت همه آحاد جامعه، بالاخص کاربران فضای مجازی و سازمان‌های مردم نهاد ضروری می‌باشد. در یک سیاست جنایی گسترده و مشارکتی، همه گروه‌ها باید در مراحل مختلف فرآیند پیشگیری و مقابله با جرم شرکت داشته باشند تا بتوانند به مقابله هر چه گسترده‌تر و دقیق‌تر با سرقت‌های اینترنتی بپردازند، چرا که پیشگیری از این جرم به جهات مختلف فراتر از ظرفیت نهادهای رسمی مجری عدالت است و باید به واگذاری بخشی از سازوکارهای تأمین‌کننده امنیت و عدالت به مردم، سازمان‌های مردم نهاد و نهادهای غیردولتی پرداخت (حاجی‌ده‌آبادی، ۱۳۹۳، ص۸۳). واقعیت این است که مبارزه و کشف این گونه جرایم کاری بسیار دشوار است، چرا که به واسطه ویژگی‌های خاص فضای مجازی، ظرفیت سوءاستفاده از آن بالا می‌رود. واحد ملی مبارزه با جرایم رایانه ای FBI[3] برآورد می کند که ۸۵ تا ۸۹ درصد از تهاجمات رایانه‌ای حتی کشف نمی‌شوند (آیکاو، ۱۳۸۳، ص٤٢). ویژگی‌هایی چون گمنامی و ناشناخته بودن کاربران در فضای مجازی، بدون مرز بودن آن، کم هزینه بودن فعالیت در این محیط و در عین حال پرثمر بودن آن به نسبت فضای فیزیکی، پایین بودن احتمال دستگیری یا مجازات، امکان وارد آوردن خسارات بالا در زمانی بسیار کم‌تر از جرایم فیزیکی، آسان بودن تهیه امکانات و وسایل مورد نیاز جرم و ... از مواردی هستند که موجب افزایش ارتکاب جرایم در فضای مجازی می‌شوند.

## تعریف پیشگیری از جرم

هرچند تعاریف متعددی از پیشگیری از جرم ارائه شده است، لیکن ارائه تعریفی دقیق از پیشگیری

1. Federal Bureau of Investigation (FBI)
2. Computer Security Institute (CSI)
3. The FBI’s National Computer Crimes Squad

کار آسانی نیست، زیرا غالب نویسندگان به بررسی پیشگیری می‌پردازند بدون آن که از قبل، نسبت به تعریف و توجیه آن اقدام کنند. در یک تعریف عام «پیشگیری شامل هر رویدادی است که نتیجه اعمال آن کاسته شدن از نرخ بزهکاری باشد.» اما در تعریف خاص، برخی پیشگیری از جرم را «نوعی مداخله از طریق اتخاذ تدابیری برای جلوگیری یا کاهش ارتکاب جرم یا کاهش نتایج احتمالی آن» می‌دانند. موریس کوسن، جرم‌شناس کانادایی، پیشگیری را چنین تعریف می‌کند :«مجموعه اقدام‌ها و تدابیر غیرقهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال رخ دادن و وخامت جرم، پیرامون علل وقوع جرایم اتخاذ می‌شوند.» (ابراهیمی، ۱۳۹۱، ج۱، ص۳۸). برخی دیگر آن را این‌گونه تعریف می‌کنند: «پیشگیری از جرم، پیش‌بینی، شناسایی و برآورد خطر جرم و ابداع اقداماتی برای حذف یا کاهش آن است.» این تعریف از جرم توسط مرکز پیشگیری از جرم در استافورد انگلستان ارائه شده و توسط مرکز ملی پیشگیری از جرم ایالات متحده مورد پذیرش قرار گرفته است (مک‌نیل، ۱۳۸۷، ص٤٨٧) این واقعیت مورد تأیید قرار گرفته است که جرم از تقارن تمایل به ارتکاب بزه با باور مهیا بودن فرصت ارتکاب بزه حاصل می‌شود. در حالی که وجود نیروی انتظامی و سایر نیروهای اجتماعی ممکن است میل به ارتکاب جرم در بزهکاران را کاهش دهند، اعمال تکنیک‌های پیشگیری از جرم نیز مجرمین را به کاهش مؤثر ارتکاب جرم وادار می‌سازد. فرصت مجرمانه در هشدارهای جرم یا خطرات جرم آشکار می‌شود. با درک این نکته که مباشرین جرم، عموماً کم‌مقاومت‌ترین مسیرهای منتهی به جرم را طی می‌کنند، این باور منطقی است که رابطه‌ای مستقیم میان تعداد فرصت‌ها در یک محل و شمار اقدامات بزهکارانه در آن محل وجود داشته باشد (محمدنسل، ۱۳۹۱، ص۱۵۲-۱۵۳) در ماده ۱ قانون پیشگیری از وقوع جرم پیشگیری این‌گونه تعریف شده است: «پیشگیری از وقوع جرم عبارت است از پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدامات لازم برای از میان بردن یا کاهش آن».

## شیوه‌های پیشگیری از سرقت اینترنتی

دیدگاه‌های مختلفی در مورد دسته‌بندی انواع اقدامات پیشگیرانه از جرم وجود دارد که طبق یکی از این دیدگاه‌ها، اقدامات پیشگیرانه را می‌توان تحت دو عنوان کلی پیشگیری اجتماعی و

پیشگیری وضعی مورد بررسی قرار داد (استانویک، ۱۳۸۷، ص۵۰٤). لیکن فارغ از انواع دسته‌بندی‌های بیان شده در این خصوص، نکته مهم توجه به این مسئله می‌باشد که برای ارتکاب هر عمل مجرمانه، دو عامل اصلی انگیزه مجرم و شرایط و فضای مناسب در وقوع جرم دخیل هستند. البته از بین بردن انگیزه مجرمان، وظیفه‌ای فراتر از حیطه توان مسئولیت‌های یک شهروند عادی و در محدوده اختیارات و توانایی‌های سازمان‌های کلان کشوری است، اما جلوگیری از ایجاد فضا و بستر مساعد برای بروز یک عمل مجرمانه توسط بزهکاران، تا حد زیادی وابسته به نوع عملکرد هر یک از قربانیان بالقوه، یعنی شهروندان است که می‌تواند آنان را در برابر مجرمان فرصت‌طلب حفظ کرده و موجب ناکامی آنان شود. در کشور ما وظیفه پیشگیری از وقوع جرم، در راستای اجرای بند ۵ اصل ۱۵٦ قانون اساسی، از طرف رئیس قوه قضاییه به دادستان کل کشور تفویض شده است و در نتیجه او را می‌توان مرجع ذی‌صلاح برای رسیدگی به مسأله سالم‌سازی و پیشگیری از وقوع جرایم در فضای سایبر دانست، زیرا باید این نکته را در نظر داشت که بسیاری از نیروهایی که در راستای اجرای روش‌های پیشگیری از سرقت سنتی اعمال می‌شوند، در خصوص سرقت‌های اینترنتی دارای کارآیی لازم نیستند، چرا که اینترنت، یک فن‌آوری وارداتی است و جامعه ما، یک جامعه مصرف‌کننده و بهره‌گیرنده از امکانات این فضا بوده و توان اعمال اراده لازم در این مورد را ندارد. لذا وظیفه کنترل و نظارت بر این فضا و فعالیت‌های انجام شده در آن در مرحله نخست متوجه دادسرا می‌باشد، چرا که دادسرا باید به عنوان نهاد متولی امر کشف جرایم و همچنین تعقیب مجرمان، آماده انجام اقدامات لازم بوده و در برابر هر نوع جرم، اعم از آن که در فضای فیزیکی رخ دهد یا در فضای مجازی، مبادرت به انجام فرآیندهای قضایی لازم نماید. بنابراین در مواردی مانند جرایم فضای سایبر که جرم دارای جنبه عمومی بوده و در معرض دید میلیون‌ها نفر رخ می‌دهند و تمامی ویژگی‌های جرم عمومی را دارا می‌باشند، از حقوق افراد جامعه صیانت کرده و به عنوان مدعی‌العمومی نقش خود را ایفا کند. در سال ۱۳۷۰ مرکزی با عنوان «دفتر مطالعات و پیشگیری از وقوع جرم» به دستور رئیس قوه قضائیه و با مسئولیت دادستان کل کشور، به منظور مطالعه راجع به پیشگیری از ارتکاب جرم تشکیل شد. اهداف این مرکز یافتن

شیوه‌ها و راه‌های مؤثر در پیشگیری از وقوع جرم و اصلاح از طریق: ۱. بررسی روند بزه‌کاری و علل وقوع جرایم؛ ۲. بررسی تدابیر مقابله با مجرمین؛ و ۳. اتخاذ اقدامات ضروری مبارزه با بزه‌کاری و مقابله با مجرمین می‌باشد (ایرانشاهی، ۱۳۸۹، ص۹٤) در همین راستا، دادستانی کل کشور طرح تشکیل ستادی تحت عنوان «ستاد پیشگیری و مبارزه با جرایم فن‌آوری اطلاعات» را به ریاست قوه قضائیه ارائه کرد که به موجب آن، این ستاد در سطح کشوری اقدام به ایجاد وحدت رویه قضایی در مواجهه با موارد مجرمانه مذکور و همچنین ارائه طریق در زمینه پیشگیری از وقوع جرایم در فضای سایبر بنماید. با تصویب قانون پیشگیری از وقوع جرم در تاریخ ۲۱ شهریورماه ۱۳۹٤ و اجرایی شدن آن از سوم دی ماه همین سال، شورای عالی پیشگیری از وقوع جرم تشکیل شد که طبق ماده ۳ این قانون، وظایف این شورا عبارت است از:

- تقسیم کار و اتخاذ تدابیر مناسب برای هماهنگی و توسعه همکاری بین دستگاه‌های مسئول در امر پیشگیری؛
- تعیین راهبردها، سیاست‌های اجرایی و برنامه‌های ملی پیشگیری از وقوع جرم؛
- بررسی و تصویب برنامه‌های کلان برای گسترش فرهنگ، ایجاد زمینه‌های مشارکت مردم و نهادهای دولتی و غیردولتی در امر پیشگیری از وقوع جرم و حمایت از آنها؛
- بررسی و اتخاذ تصمیم جهت شناسایی زمینه‌ها و علل وقوع جرم، کاهش آسیب‌های اجتماعی و ... ؛
- اتخاذ سیاست‌های موردنیاز در جهت حمایت از بزه‌دیدگان و محکومان و خانواده آنان و....

اما اجرای این قانون و انجام وظایف این شورا نیازمند تشکیل دبیرخانه‌ای می‌باشد تا عهده‌دار تشکیل جلسات، اجرایی نمودن وظایف تصریح شده در بندهای ماده ۳ فوق‌الذکر و همچنین مصوبات این شورا باشد. به همین دلیل در ماده ۵ این قانون، تشکیل دبیرخانه شورای عالی در قوه قضاییه پیش‌بینی شده است. اما آن‌چه مهم است توجه به این مطلب است که تصویب این قانون نشان دهنده درک اهمیّت و ضرورت پیشگیری از وقوع جرم توسط قانون‌گذار می‌باشد و اجرای صحیح و دقیق آن می‌تواند فضای ارتکاب جرم برای سارقان اینترنتی را با محدودیت مواجه کرده

و ارتکاب این جرم را در فضای سایبری کشور کاهش دهد که برخی از ایـن وظـایف مربـوط بـه پیشگیری‌های وضعی و برخی دیگر مربوط به پیشگیری‌های اجتماعی می‌باشند.

## پیشگیری اجتماعی از سرقت‌های اینترنتی

شیوه پیشگیری اجتماعی عوامل اجتماعی جرم‌زا و انحراف‌زا در یک جامعـه معـیّن را هـدف قـرار می‌دهد و به دنبال از بین بردن زمینه‌های اجتماعی بروز انگیزه‌های مجرمانه می‌باشد و به دو شـاخه پیشگیری اجتماعی جامعـه‌مـدار و فـردمـدار(رشـدمدار) تقسـیم مـی‌شـود (ذوالقـدر، ۱۳۹۱، ج۱، ص۱۰۹). در این شیوه از پیشگیری، ابتدا عوامل جرم‌زا شناسایی می‌شوند، آن‌گـاه اقـداماتی بـرای خنثی‌سازی یا کنار زدن آثار آن عوامل صورت می‌گیرد (عابدی، ۱۳۸۸، ص۲٤). توسعه روزافـزون زیرساخت‌های فن‌آوری اطلاعات و ارتباطات در کشور و افـزایش کـاربران و اسـتفاده‌کننـدگان از اینترنت و سایر فن‌آوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همـراه، شبکه‌های دیتای کشوری و محلّی و ارتباطات ماهواره‌ای، از جمله عواملی هستند که لزوم ایجاد و توسعه ساز و کاری برای برقـراری امنیـت در فضـای تولیـد و تبـادل اطلاعـات کشـور را توجیـه می‌نمایند. همچنین توسعه خـدمات الکترونیکـی در کشـور، نظیـر دولـت الکترونیـک، بانکـداری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و سـایر خـدمات از ایـن دسـت، لـزوم تـأمین امنیت و مقابله با جرایمی که در این فضا به وقوع می‌پیوندند را آشـکار مـی‌کنـد. از جملـه تـدابیر بسیار مؤثر در پیشگیری اجتماعی از سرقت‌های اینترنتی، ارائه آموزش‌های کافی و اطلاع‌رسانی بـه موقع به افراد جامعه است زیرا آگـاهی و دانـش موجـب رفـع بسـیاری از معضـلات و مشـکلات زندگی فردی و اجتماعی انسان می‌شود و اغلب معضلات اجتماعی، به ویـژه معضـل بـزه‌کـاری و بزه‌دیدگی، ناشی از جهل و ناآگاهی است (میرخلیلی، ۱۳۹۱، ج۱، ص٤۹). افراد یک جامعـه بایـد بتوانند مراقب افشای اطلاعات خود در فضای مجازی باشند و عدم اطلاع کافی فـرد از اینترنـت و قابلیت‌ها و مخـاطرات آن، موجـب انتشـار و افشـای اطلاعـات خصوصـی وی در فضـای سـایبر می‌شود. با ارائه آموزش‌های لازم می‌توان به افراد جامعه آموخت که بـه چـه شـیوه‌هـایی احتمـال آسیب‌دیدگی فردی و اجتماعی در مقابل فعالیت‌های مجرمانـه سـارقان اینترنتـی را کـاهش داده و

بتوانند خانواده، اموال و حیثیت اجتماعی خود را تا حدّ زیادی از چنین مخاطراتی مصون دارند (معاونت‌کشف‌جرایم‌ناجا، ۱۳۷۹، ص۱۰۲). زیرا بزرگترین آسیب‌پذیری در هر سیستم رایانه‌ای و بزرگترین تهدیدی که متوجه حفاظت رایانه است، خود کاربران می‌باشند و مسائل حفاظتی مرتبط با آن‌ها موضوع گسترده‌ای است که چیزی بیشتر از جلوگیری از سرقت‌های اینترنتی را شامل می‌شود (آیکاو، ۱۳۸۳، ص۱۸۱). در جوامع مختلف برای ارائه آموزش‌های لازم به کاربران از شیوه‌های مختلفی استفاده شده است و علاوه بر آموزش‌های حضوری، ارائه آموزش‌ها به صورت غیرحضوری به شکل انتشار کتاب، جزوه‌های آموزشی و یا برنامه‌های آموزش از راه دور نیز کاربردهای فراوانی داشته است. در حال حاضر، بسیاری از سایت‌ها دارای صفحاتی جهت آموزش مخاطبان خود هستند که از این طریق به عموم افراد جامعه و یا اقشار خاصی که از آن سایت‌ها استفاده می‌کنند، آموزش داده می‌شود. در این قبیل صفحات راهنمایی‌های خاصی برای خسارت‌دیدگان از سرقت‌های اینترنتی و پشتیبانی از آن‌ها نیز مشاهده می‌گردد. گفتگو کردن با افراد ناآشنا و در دسترس آن‌ها قرار دادن اطلاعات شخصی خود، یکی از رایج‌ترین اشتباهات کاربران در فضای مجازی است. یکی دیگر از این اشتباهات ذخیره نمودن رمز کارت‌های اعتباری بر روی سایت‌هایی است که فرد در فضای مجازی از آن‌ها خرید نموده و یا از خدمات آن‌ها استفاده می‌نماید، زیرا این مسئله موجب سهولت کار سارقان اینترنتی می‌شود و آن‌ها می‌توانند به راحتی با هک نمودن آن وب‌سایت به اطلاعات موجود در آن دسترسی پیدا کنند. از دیگر ابعاد ضروری سیاست آموزشی برای مقابله با سرقت‌های اینترنتی، ارائه آموزش‌های مورد نیاز کارکنان و افراد شاغل در بخش‌های مختلف جامعه در زمینه‌های شغلی آن‌ها است. این آموزش‌ها که محوریّت اصلی آن‌ها در رابطه با وظایف شغلی افراد می‌باشد، مواردی را در برمی‌گیرند که عدم رعایت آن‌ها می‌تواند فرد را از نظر مسائل شغلی در مقابل سرقت‌های اینترنتی ضربه‌پذیر سازد، زیرا امروزه در اغلب مشاغل، رایانه و اینترنت به عنوان ابزارهایی توانمند و ضروری به کار گرفته می‌شوند. علاوه بر این، آموزش‌های ویژه‌ای نیز در ارتباط با مشاغل خاصی از جامعه ضروری است؛ به عنوان مثال طرح‌ریزی و اجرای آموزش‌های ویژه برای مسئولان حفاظت و امنیت

شبکه‌های رایانه‌ای، کارکنان نیروهای انتظامی که وظیفه تحقیق و تحت پیگـرد قـرار دادن سـارقان اینترنتی را بر عهده دارند و حقوقدانان و قضاتی که با پرونده‌هایی در این زمینه سر و کار دارند، از جمله تدابیری هستند که بایستی مورد توجه قرار بگیرند. لذا در هر جامعه‌ای لزوم آگاهی‌رسـانی و آموزش افراد در خصوص انواع سرقت‌های سایبری و راه‌های پیشگیری از آن‌هـا، مـی‌توانـد تـأثیر بسزایی در کاهش این گونه سرقت‌ها داشته باشد. از این رو ضروری است که علوم مختلـف را در شناسایی این جرم، سارقان و بزه‌دیدگان آن‌ها به کار گرفت و با یک مبنای علمی دقیق به مقابله بـا این جرم پرداخت و راهبردها، برنامه‌ها و اقدامات پیشگیرانه برای مقابله با این سرقت‌ها را بر پایـه تحقیقات علمی انجام شده در خصوص شناسـایی علـل وقـوع ایـن جـرم و راه‌کارهـای قطعـی و مقطعی پیشگیری از جرم بنا نهاد. اما در پیشگیری اجتماعی باید به این نکته مهم نیز توجه شود که بی‌تردید اقدامات پیشگیرانه اجتماعی از وقوع جرم و بزه‌کاری، بدون توجه به اصول و مبانی دینی، کامل نبوده و نیاز است تا از مجموعه راه‌کارهای سـازنده فرهنگـی، اجتمـاعی، تربیتـی و آموزشـی شرع مقدس برای تکمیل تمهیدات پیشگیرانه اجتماعی بهره جست. تأکید سیاست قضایی اسلام بر مشارکت عمومی در فرآینـد پیشـگیری از بـزه‌کـاری در تعـالیم اسـلامی، حکایـت از آن دارد کـه دولت‌ها امکان پیشبرد صحیح و کافی امر پیشگیری را بـدون اتکـاء بـه مـردم و نهادهـای مردمـی ندارند. خداوند متعال در آیه «وَلَولا دَفعَ اللهِ النَّاسَ بَعضَهُم بِبعضٍ لَفَسَدتِ الأَرضُ»(بقـره، آیـه۲۵۱) این موضوع را متذکر شده است که اگر مشارکت عموم مردم در امـر پیشـگیری از جـرم صـورت نگیرد، هرگز نتیجه مطلوب حاصل نخواهد شد و جرم و فساد همه جا را فرا خواهد گرفت و عدم استفاده از اراده عمومی در پیشگیری از جرم، موجب گسترش فساد در جامعه می‌شود (میرخلیلـی، ۱۳۹۱، ج۱، ص۲٦) آموزه‌های دینی و اخلاقی اگر بـه درسـتی از دوران کـودکی و پـیش از آغـاز دبستان و با روش‌های جدید علمی و آموزشی به افراد جامعه منتقل شوند، ساختار شخصیتی افـراد را به گونه‌ای شکل خواهند داد که به طور ناخودآگاه انگیزه لازم بـرای حرکـت بـه سـمت اعمـال خلاف را نخواهند اشت و میل او به سمت اعمال نیک و صحیح خواهد بود (رحمتی، ۱۳۹۲، ج۳، ص۱۵۹). واقعیت آن است که کارآمدی احکام دیـن در بسـتر مناسـب و طبیعـی خـود جلـوه‌گـر

می‌شود و بستر طبیعی اجرای احکام اسلامی جامعه‌ای را می‌طلبد که در آن قبل از مبارزه با معلول، با علّت و اساس آن مبارزه شود. ایمان به وجود خدا و اعتقاد به حضور او در همه احوال و شرایط، می‌تواند به عنوان یک اهرم بازدارنده قوی از ارتکاب جرم باشد و انسان را در مبارزه با وسوسه‌های شیطانی یاری دهد و این نقش ایمان و بازدارندگی درونی آن، چیزی است که قابل انکار نیست. قرآن کریم در این خصوص می‌فرماید: «أَلَمْ یَعلَم بِأَنَّ الله یَرَی؛ آیا انسان نمی‌داند که خداوند همه اعمال او را می‌بیند؟» (علق، آیه١٤). همچنین اعتقاد به معاد و حساب و کتاب روز قیامت می‌تواند موجب بازدارندگی از ارتکاب جرایم گردد زیرا ایمان به معاد یعنی اعتقاد به وجود جهان پس از مرگ و بررسی اعمال افراد در آن جهان است و این که عاقبت هر انسانی در گرو اعمال خود اوست. به همین دلیل است که این اعتقاد فرد را به ارتکاب نیکی‌ها و دوری از بدی‌ها سوق می‌دهد. خداوند متعال در آیه ۳۰ سوره مبارکه آل‌عمران می‌فرماید: «یَومَ تَجِدُ کُلُّ نَفسٍ مَا عَمِلَت مِن خَیرٍ مُحضراً وَ مَا عَمِلَت مِن سُوءٍ تَوَدُّ لَو أَنَّ بَینَها وَ بَینَهُ أَمَداً بَعیداً وَ یُحَذِّرُکُمُ اللهُ نَفسَهُ وَ اللهُ رَئُوفٌ بِالعِباد؛ یعنی روزی که هر نفسی آنچه را در دنیا کرده، چه خیر و چه شر، برابر خود حاضر می بیند در آن روز آرزو می کند ای کاش بین او و آنچه کرده زمانی طولانی فاصله بود (چون از اعمال خود برحذر است و شما مردمی که چنین ترسی در پیش دارید بدانید که) خدا شما را از کیفر خود می‌ترساند و خداوند به بندگانش مهربان است.» همچنین اهتمام به انجام فرائض دینی و عادت دادن افراد از کودکی به انجام عبادات، می‌تواند نقش بسیار مؤثری در پیشگیری از وقوع جرم داشته باشد و به همین علّت است که حضرت ابراهیم (علیه‌السلام) از پروردگار درخواست می‌نماید که به عنوان یک لطف الهی، خودش و برخی از ذریه‌اش را متمسّک به دین و برپا دارنده نماز گرداند: «رَبِّ اجعَلنِی مُقیمَ الصَّلوهِ وَ مِن ذُرِّیَّتِی رَبَّنا وَ تَقَبَّل دُعاءِ» (ابراهیم، آیه٤٠) تا از این طریق از راه راست منحرف نشده و مرتکب گناه نگردند. به دلیل همین تأثیر شگرف انجام عبادات در هدایت انسان‌ها و دوری آن‌ها از گناه و جرم است که خداوند مؤمنان را به استعانت جستن از صبر و نماز در مشکلات فرا می‌خواند تا مبادا فریب شیطان را خورده و از مسیر حق خارج شوند: «وَ استَعِینُوا بِالصَبرِ وَ الصَلوهِ وَ انَّها لَکبیره إلّا عَلی الخَاشِعین» (بقره، آیه٤٥) همچنین آیات ۳ تا ۵ سوره بقره اشاره

مستقیم به تأثیر اعتقاد به نبوت و معاد، اقامه نماز و اقدام بـه انفـاق در رسـیدن انسـان بـه فـلاح و رستگاری دارد و این گونه نتیجه می‌گیرد که رستگاری حاصـل نمـی‌شـود مگـر بـه وسـیله انجـام واجبات و دوری از انجام محرمات و گناهان: «اَلّذینَ یُؤمِنونَ بِالغَیبِ وَ یُقیمونَ الصَّلوهَ وَ مِمّا رَزَقناهُم یُنفِقونَ* وَ الَّذینَ یُؤمِنونَ بِما اُنزِلَ اِلَیکَ وَ ما اُنزِلَ مِن قَبلِکَ وَ بِالاخِرَهِ هُم یُوقِنونَ* اُولئِکَ عَلی هُدًی مِن رَبِّهِم وَ اُولئِکَ هُمُ المُفلِحُونَ؛ یعنی آن‌ها که به عالم غیب ایمان دارند و نماز را بر پا مـی‌کننـد و و از آن چـه بـه آن‌هـا روزی داده‌ایم انفاق می‌کنند و آنان که با آن چه بر تو نازل شده و بدان چه قبـل از تـو نـازل شـده ایمان، و به آخرت یقین دارند، چنین کسان بر طریق هدایتی از پروردگار خویش قرار دارند و آن‌ها هستند که رستگارانند.» علاوه بر این، خداونـد متعـال در آیـه ٤٥ سـوره عنکبـوت نیـز بـه نقـش پیشگیرانه و بازدارنده نماز از هر گونه گناه و جرم اشاره داشته وی می‌فرماید: « ... و اقم الصلوه ان الصلوه تنهی عن الفحشاء و المنکر ...؛ یعنـی و نمـاز را بـه پـادار کـه نمـاز از فحشـاء و منکـرات جلوگیری می کند.» رسول گرامی اسلام، حضرت محمد(صلی‌الله‌علیه‌وآله) نیـز در خصـوص تـأثیر نماز در جلوگیری از ارتکاب گناه و معصیت می‌فرماینـد: «لَایَزالُ الشَّیطانُ ذَعِراً مِنَ المؤمِنِ مَا حَافَظَ عَلی الصَّلَواتِ الخَمسِ فَإذا ضَیَّعَهُنَّ تَجَرَّأَ عَلَیه؛ یعنی مداومت بر حفظ نمازهای پنج‌گانه موجـب بـرآوردن نالـه شیطان و ترس و وحشت او از انسان مؤمن نمازگزار می‌شود، اما ضایع کردن نماز موجب جـرأت و جسارت شیطان در هجوم بر علیه انسان می‌شود.» (کلینی، ١٣٦٧، ج٣، ص٢٦٩) و به همین دلیل است که امیر مؤمنان علی(علیه‌السلام) در باب نقش دعا در حفاظت از مؤمن در برابر وسوسه‌هـای شیطان می‌فرماید: «الدُّعَاءُ تُرْسُ الْمُؤْمِنِ؛ یعنی دعا سـپر مـؤمن اسـت ...» (همـان، ص٢١٤، ح٤). لـذا فراگیر شدن عمل به آموزه‌های اخلاقی اسلام و توجه به تعالیم دینـی و الهـی در میـان افـراد یـک جامعه، همانند یک پشتوانه قـوی و مطمـئن، مـی‌توانـد جامعـه را در برابـر بسـیاری از امـراض و انحرافات فکری و عملی مصون دارد و این در حالی است که بی‌توجهی جوامع امروزی به اخـلاق و بالاخص خلاء اخلاقی موجود در فضای بدون مرز سایبری موجب شـده اسـت کـه بسـیاری از افراد، سرقت اینترنتی را به عنوان یک عمل قبیح که در عرف اجتمـاعی جـرم تلقـی مـی‌شـود، بـه حساب نیاورند. بنابراین آگاه ساختن افراد جامعه در این زمینه و ارائه آموزش‌های دینی و اخلاقـی لازم به آن‌ها می‌تواند نقش شایان توجهی در پیشگیری از سرقت‌های اینترنتی داشته باشد (معاونت

کشف جرایم ناجا، ۱۳۷۹، ص۱۰۲) زیرا با آموزش مبانی فقهی و اخلاقی مرتبط با استفاده از رایانه و اینترنت می‌توان از ناظری مطمئن به نام پرهیزگاری و تقوا استفاده نمود و در همین راستا، لازم است قبح سرقت داده‌ها و اطلاعات دیگران در فضای مجازی و جرم بودن آن از همان کودکی برای افراد آشکار شود تا در کنار آموزش شیوه‌های صحیح استفاده از امکانات فضای مجازی، بدانند که چگونه می‌توان از این فن‌آوری اطلاعاتی و ارتباطی بدون وارد کردن هیچ گونه آسیبی به خود و دیگران استفاده مفید نمود. این مطلبی است که امروزه با عنوان خودکنترلی مطرح بوده و در برخورد با انواع جرایم، از جمله سرقت‌های اینترنتی، به عنوان یک راه‌حل کارآمد ترویج می‌شود (بنی‌هاشمی، ۱۳۹۰، ص۲۰۹). لذا با وجود تمام پیشرفت‌های علمی و صنعتی، همچنان شاهد آن هستیم که اخلاق و آموزه‌های دینی و همچنین توجه به تذهیب نفس از مسائلی می‌باشند که تمامی افراد جامعه، در همه سطوح، به آن نیازمند بوده و نمی‌توان فن‌آوری‌های نوین را بدون در نظر گرفتن این عوامل به درستی به کار گرفت.

### پیشگیری وضعی از سرقت‌های اینترنتی

پیشگیری وضعی عبارت است از: «ایجاد تغییر نظام‌مند و دائمی در محیط، به منظور کاهش فرصت‌های مجرمانه و افزایش خطر ارتکاب جرم». پیشگیری وضعی، رویکردی موقعیت‌مدار داشته و «موقعیت ارتکاب جرم» را یکی از عوامل اساسی جرم محسوب می‌کند و به همین دلیل در صدد از بین بردن موقعیت جرم از طریق برهم زدن عناصر تشکیل‌دهنده موقعیت است (مقیمی، ۱۳۹۱، ج۱، ص۳۸۲) در این روش، با هدف حمایت و تقویت بزه‌دیده بالقوه، اقدام به تغییر وضعیت‌های ماقبل بزه‌کاری شده و وضعیت فرد یا شرایط بیرونی مانند مکان، زمان و ... به گونه‌ای تغییر داده می‌شوند تا از ارتکاب جرم پیشگیری گردد. در حقیقت می‌توان گفت که این شیوه از پیشگیری، متوجه وضعیت «پیش از وقوع جرم» است و تلاش می کند فرآیند تبدیل از «اندیشه مجرمانه» به «عمل مجرمانه» قطع شود. در پیشگیری وضعی دو جهت‌گیری اصلی «مداخله در وضعیت پیش از جرم» و «ایمن‌سازی اهداف جرم» وجود دارد که دو هدف عمده را دنبال می‌کنند: یکی دشوار یا ناممکن‌سازی وقوع جرم، در حالی که انگیزه مجرمانه وجود دارد؛ و دیگری

جلوگیری از پیدایش و شدت گرفتن انگیزه مجرمانه (عابدی، ۱۳۸۸، ص۲۵-۲۶). امروزه شاهد آن هستیم که بین وابستگی روزافزون جوامع به فن‌آوری‌های اطلاعاتی و ارتباطاتی[1] و توانایی دولت‌ها در نظارت و اعمال نفوذ بر فعالیت‌های انجام شده در فضای سایبر، فاصله‌ای پدید آمده است که بزهکاران را ترغیب به انتقال فعالیت‌های خود به دنیای سایبر نموده است، زیرا آن‌ها دریافته‌اند که در این محیط، روش‌های نظارتی مرسوم کارآیی لازم را نداشته و دلایل دیجیتالی به دست آمده، تاب پیگرد آن‌ها را ندارند. همچنین نوظهور بودن این فن‌آوری سبب شده تا اقدامات مقطعی و کوتاه‌مدت برای مقابله با سرقت‌های اینترنتی، در نظر سیستم‌های قضایی کشورها مطلوب جلوه کنند، چرا که این اقدامات کم‌هزینه سبب می‌شوند تا چنین به نظر آید که دستگاه قضایی برای برخورد با مجرمین فاقد برنامه لازم نمی‌باشد. نمونه بارز این گونه اقدامات، تدابیر وضعی است که با اثرگذاری بر موقعیت‌های جرم‌زا به دنبال آن است که در سایه تدابیر محدود کننده و نظارتی، ارتکاب جرم را برای بزه‌کاران دشوار جلوه دهد و با کم کردن سود حصل از فعالیت‌های مجرمانه برای تبهکاران، آن‌ها را از ارتکاب جرم باز دارد. البته دستگاه‌های قضایی برای مبارزه با جرم، همواره از کیفر بهره جسته‌اند، اما ادامه فعالیت‌های مجرمان و روند رو به افزایش آن‌ها، بالاخص درفضای مجازی، نشان می‌دهد که در کنار مجازات مجرمان باید به پیشگیری از وقوع جرم نیز اهتمام ویژه شود. درباره سرقت‌های اینترنتی به دلیل ویژگی‌های متفاوت فضای مجازی در مقایسه با فضای فیزیکی، جرم‌شناسان دریافته‌اند که الگوهای بازدارندگی سنتی، بدون تطبیق با شرایط حاکم بر سرقت‌های اینترنتی، در پیشگیری از این جرم و ارعاب سارقان اینترنتی مؤثر واقع نمی‌شوند (معاونت کشف جرایم ناجا، ۱۳۷۹، ص۱۷۱-۱۷۳). یکی از جامع‌ترین برنامه‌های پیشگیری وضعی، بکارگیری رهنمودهای کلارک است که شامل راه‌کارهای بیست و پنج‌گانه‌ای می‌باشد که وی آن‌ها را در خصوص جرایم سنتی مطرح کرده است، لیکن می‌توان با اجرای آن‌ها در فضای مجازی تا حد زیادی از جرایم سایبری و بالاخص سرقت‌های اینترنتی

1. ICT's

پیشگیری نمود. کلارک پیشگیری وضعی را اقدامات و روش‌هایی بـرای کـاهش فرصـت ارتکـاب جرم می‌داند که اولاً به سوی شکل کاملاً خاصی از جرم نشانه می روند؛ ثانیـاً متضـمن طراحـی و مدیریت محیط بلاواسطه جرم، اعم از صحنه و محل وقوع جرم، یا همـان نظـارت و تحـت نفـوذ درآوردن هرچه پایدارتر و سازمان‌یافته‌تر محل وقوع جرم هستند؛ و ثالثاً زحمات و خطرات ناشـی از اقدام برای ارتکاب جرم را افزایش داده و سود حاصله، آن‌گونه که در نظر اکثر مرتکبین جلوه‌گر می‌شود، را کاهش دهند (صفاری، ۱۳۸۰، ص۲۹۲). تدابیر پیشگیری وضـعی در کنـار برنامـه‌هـای پیشگیری اجتماعی، می‌توانند سبب پیشگیری و کنترل سرقت‌های اینترنتی شوند و برخی ایرادهای گرفته شده به آن، ناشی از به کار بستن نادرست این تدابیر و راهبردها می‌باشند، زیرا به عنوان مثال انتقاد درباره ایجاد محدودیت‌های اخلاقی و حقوق بشـری و همچنـین مسـئله هزینـه‌هـای بـالای اقتصادی اجرای آن‌ها، که به اعتقاد برخی این پیشـگیری‌هـا را تنهـا بـه سـود طبقـه مرفـه جامعـه می‌نماید، بیشتر به نحوه اجرای این تدابیر برمی‌گردند و دولت‌ها می‌توانند برای رفع این مشکل بـا اجرای طرح‌های حمایتی و اختصاص بودجه مناسب، توازن امنیتی را میان اقشـار مختلـف جامعـه برقرار سازند. در همین راستا، کلارک پنج راهبرد اصلی را برای پیشگیری وضعی از جرایم پیشنهاد می‌کند که هر یک از این راهبردها، پنج راهکار را شامل می‌شوند و مجموعاً راهکارهـای بیسـت و پنج‌گانه پیشگیری وضعی را تشکیل می‌دهند. پنج راهبرد اصلی وی برای مقابله با جـرم کـه بـه دو گروه راهبردهای ایجابی و راهبردهای سلبی تقسیم می‌شوند، عبارتند از:

**الف) راهبردهای ایجابی**

راهبردهای ایجابی شامل موارد زیر است:

۱. افزایش میزان تلاش به منظور ارتکاب جرم؛

۲. افزایش خطرهای ارتکاب جرم؛

**ب)راهبردهای سلبی**

راهبردهای ایجابی شامل موارد زیر است:

۱. کاهش دست‌آوردها؛

۲. کاهش عوامل محرک؛

۳. سلب توجیه‌ها.

فراگیر بودن این راهبردها سبب می‌شود تا جرایم نوینی مانند سرقت‌های اینترنتی نیز بتوان آن‌ها را به کار بست (Clarke, 1997, P.4). البته باید توجه داشت که اعمال تدابیر وضعی پیشگیری از جرم، زمانی عادلانه خواهند بود که حقوق بشر مطلق شهروندان مخدوش نشده و یا در سطح محدودی با محدودیت روبرو گردد. به عبارت دیگر، در همه انواع پیشگیری، مداخله دولت از یک سو باید حداقلی و از سوی دیگر همراه با احتیاط‌ها و ملاحظات حقوق بشری باشد (ابراهیمی، ۱۳۹۱، ج۱، ص۸۸). البته باید به این نکته توجه نمود که اگر چه تاکنون راه‌حل قطعی برای پیشگیری صد در صد از سرقت‌های اینترنتی یافت نشده است و تمامی روش‌های پیشگیری دارای موفقیت نسبی بوده‌اند و هیچ‌گاه نتوانسته‌اند ارتکاب جرم را به صفر برسانند، لیکن با بکارگیری صحیح این روش‌ها و انجام یک سری اقدامات کلیدی می‌توان از داده‌ها و اطلاعات، بالاخص اطلاعات مالی، در مقابل حملات سایبری حفاظت نمود. از جمله مهم‌ترین تدابیر لازم برای پیشگیری از سرقت‌های اینترنتی، که نقش محوری در کاهش این گونه از سرقت‌ها را ایفا می‌کند، بهره‌گیری از روش‌های حفاظتی و امنیتی است. در حال حاضر تمامی فرآیندهای حفاظت از سیستم‌ها و شبکه‌های رایانه‌ای نسبی بوده و تعداد کمی از سازمان‌ها، مؤسسات و شرکت‌ها هستند که می‌توانند نسبت به پرداخت هزینه لازم برای حفاظت کامل از دارائی‌هایشان اقدام کنند. در عوض، بیشتر آنان با پرداخت هزینه انواع مختلف حفاظت، به مقابله با خطرات ناشی از بی‌توجهی می‌روند که این مرحله را مرحله تجزیه و تحلیل و تصمیم در مورد خطرات احتمالی و سطحی را که سازمان می‌تواند انجام دهد، خطر قابل قبول می‌نامند (آیکاو، ۱۳۸۳، ص۱٤۹). شیوه‌های حفاظتی نه تنها جزء روش‌های مناسب برای مقابله با سرقت‌های اینترنتی می‌باشند، بلکه تأثیر بسزایی در پیشگیری از خطراتی دارند که ممکن است از خطاهای انسانی، مشکلات اجرایی و یا حوادث غیرمترقبه ناشی شوند (معاونت کشف جرایم ناجا، ۱۳۷۹، ص۱۰۰). اجرای تدابیر حفاظتی و امنیتی دامنه بسیار گسترده‌ای را در برمی‌گیرند. نخستین اقدام برای اتخاذ تدابیر حفاظتی

سیستم‌ها و شبکه‌های رایانه‌ای، بررسی جهت تعیین خطرات احتمالی سیستم و یا به تعبیری ارزیابی میزان ریسک است. در تجزیه و تحلیل خطر، سه گزینه مطرح می‌باشند که عبارتند از: تهدیدها، آسیب‌پذیری‌ها و اقدامات متقابل. تجزیه و تحلیل خطر در واقع مرحله پرسیدن سؤالاتی درباره تهدیدها، آسیب‌پذیری‌ها و در نهایت درباره اقدامات متقابلی است که برای مقابله با این تهدیدها و آسیب‌پذیری‌ها انجام می‌شوند. برخی از این سؤالات عبارتند از:

- چه افراد یا گروه‌هایی در صدد حمله به سیستم یا شبکه رایانه‌ای مورد نظر می‌باشند و چرا؟
- مهاجمان در صورت موفقیت، چه چیز ارزشمندی را در آن سیستم یا شبکه رایانه‌ای به دست خواهند آورد؟
- آیا سیستم و شبکه رایانه‌ای مورد نظر حاوی اطلاعات علمی، صنعتی یا دولتی حساس می‌باشد که برای سارقان دارای ارزش هستند؟
- آیا این سیستم یا شبکه رایانه‌ای حاوی اطلاعات مالی است که مجرمین حرفه‌ای به دنبال آن‌ها می‌باشند؟
- آیا این سیستم یا شبکه رایانه‌ای اطلاعاتی مانند بازی‌های رایانه‌ای جدید را شامل می‌شود که برای مهاجمان جذابیت دارند؟
- آسیب‌پذیری‌های این سیستم یا شبکه رایانه‌ای چه چیزهایی هستند؟ (آیکاو، ۱۳۸۳، ص۱۵۰)

**شناسایی تهدیدها و خطرات بالقوه**

نتایج منتشر شده از بررسی‌های انجام شده توسط مراکز گوناگون در سطح جهان، نشان‌دهنده آن است که عوامل ایجاد خسارات ناشی از جرایم و اتفاقات رخ داده در مورد سیستم‌ها و شبکه‌های رایانه‌ای، مختلف می‌باشند. در حالی که خطاهای انسانی و مشکلات فیزیکی مانند وقوع بلایای طبیعی و قطع شدن منبع تغذیه، به ترتیب ۵۵ و ۲۰ درصد خسارات وارده به سیستم‌ها و شبکه‌های رایانه‌ای را تشکیل می‌دهند، تخلفات کارکنان ناراضی ٤٤ درصد، ورود ریزبرنامه‌های مخرب ٤

درصد و حملات افراد بیگانه ۲ درصد از موارد را موجب می‌گردند (معاونت کشف جرایم ناجا، ۱۳۷۹، ص۱۰۱) تهدیدهای یک سیستم یا شبکه رایانه‌ای می‌تواند یک شخص مانند یک نفوذگر غیرمجاز، یا یک شیء مثل یک نرم افزار ناقص و یا یک اتفاق مانند آتش سوزی و یا زلزله باشد که خطر بالقوه برای این سیستم‌ها و شبکه‌ها محسوب شده و ممکن است به سیستم یا شبکه رایانه‌ای آسیب برسانند. (آیکاو، ۱۳۸۳، ص۱۵۰) در نتیجه مرحله شناسایی تهدیدات و خطرات بالقوه، گامی اساسی در جهت پیشگیری از وقوع جرایم سایبری و از جمله سرقت‌های اینترنتی می‌باشد که نیازمند توجهی دقیق و همه جانبه می‌باشد.

**شناسایی نقاط ضعف و آسیب‌پذیری سیستم**

آسیب‌پذیری نقطه‌ای است که می‌توان از آن جا سیستم را مورد حمله قرار داد؛ مانند سطح دسترسی‌هایی که در اختیار اشخاصی قرار دارند که با سیستم کار می‌کنند ولی آموزش‌های لازم را ندیده‌اند. همچنین نقاط اتصال به اینترنت از دیگر نقاط آسیب‌پذیر سیستم‌ها و شبکه‌های رایانه‌ای می‌باشند. ارزیابی خطر احتمالی، در واقع هم حفاظت فیزیکی و هم حفاظت ارتباطی را شامل خواهد شد. به علاوه طبق بررسی‌های به عمل آمده توسط مراکز مختلف، تعداد زیادی از سرقت‌های اینترنتی، به وسیله کارمندانی انجام شده‌اند که از عوامل گوناگون نارضایتی شغلی تأثیر پذیرفته‌اند. آن‌ها با خنثی‌سازی کنترل‌های اجتماعی درونی و بیرونی، خود را قانع می‌سازند که برداشت داده‌ها و اطلاعات مربوط به کارفرمایشان، سرقت نمی‌باشد (متزا، ۱۳۹۰، ص۲۰۱) لذا بایستی سوابق کارمندان قبل از استخدام به دقت بررسی شوند و یک مدیر خوب باید رفتار کارمندان خود را کنترل کرده و به این پرسش به درستی پاسخ دهد که آیا کارمندان دارای حسن سابقه بوده و آموزش‌های لازم را دیده‌اند تا اشتباهاتی را که موجب دسترسی افراد غیرمجاز می‌شوند را انجام ندهند؟(آیکاو، ۱۳۸۳، ص۱۸۲) بهره‌برداری از نقاط ضعف و آسیب‌پذیری‌های یک سیستم یا شبکه رایانه‌ای، شیوه عملی نمودن یک تهدید می‌باشد. در نتیجه می‌توان این مرحله را مرحله مشخص نمودن نحوه عملکرد سیستم در هنگامی که مورد حمله قرار می‌گیرد، نامید.

**شناسایی روش هایی برای حفاظت از سیستم و پوشاندن نقاط ضعف آن**

این مرحله شامل شناسایی نقاط ضعف یک سیستم و استفاده از روش‌های کنترل و حفاظت یک سیستم می‌شود، مانند ایجاد گذرواژه‌ها، بهره‌گیری از شیوه‌های ارتباطات امن و استفاده از کارشناسان حفاظت سیستم‌های رایانه‌ای که معمولاً انواع مختلفی از تدابیر حفاظتی را برای این سیستم‌ها ضروری می‌دانند. مسدود کردن درگاه‌های ورودی و خروجی رایانه‌ها در ادارات و سازمان‌ها یکی دیگر از این راه‌کارهای سریع، کم هزینه و در عین حال مؤثر در پیشگیری از سرقت‌های اینترنتی می‌باشد. در این روش، درگاه‌های ورودی و خروجی سیستم‌های رایانه‌ای از قبیل درایورها، پورت‌های USB و ... بسته شده و به این ترتیب کاربران نمی‌توانند هیچ اطلاعاتی را بدون مجوز مدیر سیستم[1] وارد رایانه کرده و یا از آن خارج کنند. در این حالت کاربر تنها به داده‌هایی که به منظور انجام وظایف محوله در اختیار وی قرار داده شده، دسترسی خواهد داشت. همچنین می‌توان برای انجام امور مالی و دسترسی به حساب‌های بانکی از یک رایانه مجزا استفاده نمود که به شبکه اینترنت متصل نمی‌باشد و این یکی از اساسی‌ترین اقداماتی است که می‌توان جهت حفاظت از داده‌ها و اطلاعات مالی انجام داد. سارقان اینترنتی تلاش می‌کنند داده‌ها و اطلاعاتی را هک کنند که فقط به کاربر اصلی اجازه دسترسی و استفاده از آن‌ها داده می‌شود. کاربران با کلیک کردن بر روی لینک‌های دانلود، تبلیغات و یا عکس، به سارقان اجازه دسترسی به حساب مالی خود را می‌دهند. یکی دیگر از اقدامات پیشگیرانه وضعی در برابر سرقت‌های اینترنتی این است که کاربر با نصب یک برنامه ضدویروس[2] معتبر و به روزرسانی شده روی سیستم خود، نرم‌افزارهای مخرب را که هکرها برای نیل به مقاصد و اهداف خود برای کاربران هدف ارسال می کنند، شناسایی کرده و جلوی ورود آن‌ها را به سیستم خود می‌گیرد. همچنین در فضای مجازی بایستی از نام کاربری و رمز عبور ایمن استفاده نمود. کاربران اینترنت باید از نام‌های کاربری و رمزهای عبوری استفاده کنند که به راحتی قابل حدس و شناسایی نباشند، زیرا یکی از اولین خطوط دفاعی در برابر سرقت‌های اینترنتی، نام کاربری و رمز عبور کاربران می‌باشد و ضعف آن‌ها

1. Administrator
2. Antivirus

می‌تواند رایانه کاربر اینترنت را به یک هدف آسان برای سارقان و نفوذگران اینترنتی تبدیل کند. به همین دلیل نام کاربری و رمز عبور باید هر چند وقت یک بار، در بازه‌های زمانی ٦٠ تا ٩٠ روز عوض شده و کاربران سعی کنند رمز عبوری را که انتخاب می‌کنند بیشتر از ٦ کاراکتر بوده و در انتخاب رمز عبور خود از ترکیب حروف بزرگ، حروف کوچک، اعداد و علائم، آن هم به صورت تصادفی استفاده کنند. همچنین کاربران اینترنت باید سعی کنند هرچند وقت یک بار، تمام گزارشات مالی خود را رصد کنند و حتی اگر فکر می‌کنند در آن ماه انتقال وجه و یا فعالیتی در حساب مالی خود نداشته‌اند، باز هم این کار را انجام دهند. به علاوه کاربران می‌توانند با فعال کردن هشدار امنیتی سیستم خود، از هرگونه فعالیت غیرمعمول مثل انتقال وجه، تنظیمات جدید و انتقالات خارجی، از طریق هشدار آگاه شوند. از آنجا که آدرس‌های اینترنتی کوتاه شده[1] هیچ اشاره‌ای به مقصد ندارند، هکرها از این موضوع استفاده کرده و از این طریق لینک‌های ویروسی و بدافزارها را برای کاربران اینترنتی ارسال می‌کنند. به علاوه کاربران باید هنگام خرید اینترنتی از معتبر بودن فروشگاه اینترنتی مورد نظر اطمینان حاصل نمایند، زیرا در هنگام خرید اینترنتی اطلاعات حساب بانکی خود را در اختیار فروشگاه مورد نظر قرار می‌دهند. پس انجام کمی تأمل و تحقیق در مورد سیستم امنیتی آن‌ها و کسب اطمینان از فعال بودن آن، زمان چندانی از کاربر نمی‌گیرد و در مقابل، می‌تواند مانع سرقت‌های اینترنتی بشود زیرا مهم‌ترین قسمت یک پرداخت آنلاین مطمئن، اطمینان از صحیح بودن درگاه پرداخت بانکی است که کاربر وارد آن شده است. اگر کاربر وارد یک سایت جعلی با ظاهر و آدرسی شبیه درگاه پرداخت بانک اصلی شده باشد، بقیه کارهای امنیتی مانند وارد کردن رمز عبور با استفاده از صفحه کلید مجازی، استفاده از رمزهای عبور طولانی و ترکیبی و ... هیچ سودی برای کاربر نخواهند داشت. به همین دلیل در دوره‌های آموزش اینترنت، به کاربران یاد داده می‌شود که تمام درگاه‌های پرداخت بانک ها با کمک گرفتن از پروتکل تبادل اطلاعات امن SSL کار می‌کنند و نشانه آن حضور https به جای http است و

1. URL

باید هنگام ورود به درگاه پرداخت اینترنتی متعلق به یک بانک از وجود آن در ابتدای آدرس صفحه پرداخت اطمینان حاصل نمایند. در کشور ما نیز مانند سایر کشورهای جهان، رشد قارچ‌گونه جرایم در فضای مجازی، مثل کلاهبرداری‌ها و سرقت‌های اینترنتی و همچنین تصویب قانون جرایم رایانه‌ای و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوّبات کمیسیون فتای دولت مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، ضرورت تشکیل یک پلیس تخصصی که توان پیگیری و تعقیب مجرمان فضای سایبری، با بکارگیری فن‌آوری در سطوح بالا را داشته باشد، احساس می شد. در همین راستا، در بهمن‌ماه ۱۳۸۹ و به دستور فرمانده نیروی انتظامی جمهوری اسلامی ایران، پلیس فضای تولید و تبادل اطلاعات (فتا) تشکیل گردید. باید توجه نمود که تشکیل این نیرو در پلیس به معنی ایجاد محدودیت برای مردم و مداخله در حریم خصوصی آن‌ها نیست، بلکه وظیفه این نیرو پیش‌بینی، پیشگیری و مقابله با جرایم اینترنتی در تمامی حوزه‌های فضای سایبری است و عمده فعالیت‌های آن شامل مبارزه با جرایم اقتصادی، اخلاقی، امنیتی و تروریستی است که در بستر فضای مجازی رخ می‌دهند و یکی از آن‌ها نیز سرقت اینترنتی است. البته توجه به این نکته ضروری می‌باشد که فعالیت‌های این نیرو در زمینه نظارت بر فضای مجازی و اعمال راه‌کارهایی جهت کاهش آزادی عمل مجرمان جهت ارتکاب جرم در این فضا، در زمره پیشگیری‌های وضعی می باشند و برخی دیگر از فعالیت‌های پلیس سایبری مانند ارائه آموزش به افراد جامعه از طریق برگزاری کارگاه‌های آموزشی و چاپ کتاب و بروشور در زمره پیشگیری اجتماعی هستند.

## نتیجه

از مجموع آن‌چه گفته شد می‌توان چنین نتیجه گرفت که برای مقابله همه‌جانبه و کارآمد با سرقت‌های اینترنتی و کاهش ارتکاب آن توسط کاربران، استفاده و بکارگیری تمامی شیوه‌های مقابله با جرم به صورت توأمان تأثیرگذار بوده و استفاده از یک روش به تنهایی از کارآیی لازم برخوردار نخواهد بود. همچنین در اجرای روش‌های پیشگیری از جرم برای مقابله با سرقت‌های اینترنتی، باید خلاقیت به خرج داده و استفاده از این روش‌ها، آن‌گونه که در شکل سنتی جرایم

استفاده می‌شوند، در جرایم سایبری به طور اعم و در سرقت‌های اینترنتی به طور اخص، از کارآیی لازم برخوردار نبوده و می‌بایست نسبت به تطبیق این شیوه‌ها با شرایط موجود در سرقت‌هایی که در فضای مجازی انجام می‌شوند، اقدام نمود. به علاوه باید به این نکته توجه کرد که هر چند در نهایت هیچ یک از این شیوه‌ها، ارتکاب جرم را به صفر نمی‌رسانند، زیرا هیچ جامعه‌ای نیست که بتواند سازگاری کامل با دستورات اجتماعی را بر همه اعضایش تحمیل نماید، ولی موجب کاهش وقوع جرم شده و مهم‌تر از همه، جلوی ارتکاب جرم توسط افرادی که سابقه دار نیستند را می‌گیرد، زیرا عدم مقابله و پیشگیری از جرم موجب می‌شود تا افرادی که تاکنون، چه در فضای فیزیکی و چه در فضای مجازی، مرتکب جرم نشده‌اند، وسوسه شده و از گمنامی و پیچیدگی‌های فضای مجازی استفاده نموده و مرتکب جرم شوند و بدین ترتیب در زمره بزه‌کاران جامعه قرار بگیرند. در نتیجه به نظر می‌رسد که اجرای دقیق، هوشمندانه و خلاقانه شیوه‌های پیشگیری از جرم در سرقت‌های اینترنتی می تواند آمار سارقان مبتدی را به شدت کاهش داده و رغبت حرفه‌ای‌ها را نیز به ارتکاب جرم کم نموده و فضای مجازی را از یک فضای شلوغ، بدون مرز و ناامن، به یک فضای قانون‌مدار، منظم و ایمن تبدیل نماید.

## منابع و مآخذ


۱. ابراهیمی، شهرام(۱۳۹۱)، *جرم شناسی پیشگیری*، ج۱، تهران: میزان.

۲. اردبیلی، محمد علی(۱۳۸۱)، *حقوق جزای عمومی*، تهران: میزان.

۳. استانویک، جان(۱۳۸۷)، الزامات پیشگیری از جرم اوان کودکی بر کار پلیس، *مجموعه مقالات پلیس و پیشگیری از جرم*، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری ناجا، صفحات ۵۰۱-۵۲۵.

٤. الهی منش، محمدرضا و سدره نشین، ابوالفضل(۱۳۹۱)، *محشای قانون جرایم رایانه‌ای*، تهران: مجد.

۵. ایرانشاهی، حمید(۱۳۸۹)، *پیشگیری از وقوع جرم و نقش سازمان‌های مسئول در قوانین ایران*، تهران: جاودانه، جنگل.

٦. ایزدی فرد، علی‌اکبر و پیردهی حاجی‌کلا، علی(۱۳۸۹)، تأملی بر چالش‌های جرم‌انگاری جرائم مجازی (رایانه‌ای)، *مجموعه مقالات اولین همایش ملی فقه و مسائل مستحدثه (نوظهور)*، ساری: مرکز انتشارات توسعه علوم، صفحات ۱۵۵-۱٦٦.

۷. ایزدی فرد، علی‌اکبر و پیردهی حاجی‌کلا، علی(۱۳۸۹)، سرقت اینترنتی: حدی یا تعزیری؟، *مجله مطالعات اسلامی: فقه و اصول*، شماره ۸٤/۱، بهار و تابستان، صفحات ٤۵-٦۸ .

۸. آیکاو، دیوید جی. و سیگرو، کارل الف. و واناستروچ، ویلیام آ. ( ۱۳۸۳)، *راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای*، مترجمان اکبر سترگی و ...[و دیگران]، تهران: دانشگاه علوم انتظامی، معاونت پژوهش، اداره چاپ و نشر.

۹. باستانی، برومند(۱۳۸۳)، *جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری*، تهران: بهنامی.

۱۰.بای، حسینعلی، پورقهرمانی، بابک(۱۳۸۸)، *بررسی فقهی حقوقی جرایم رایانه‌ای*، قم: دفتر تبلیغات اسلامی حوزه علمیه قم، معاونت پژوهش، پژوهشگاه علوم و فرهنگ اسلامی.

۱۱.بجنوردی، سیدمحمد، بنی هاشمی، مریم(۱۳۹۲)، بررسی فقهی سرقت رایانه‌ای (اینترنتی) با

رویکردی بر نظر امام خمینی(س)، *پژوهشنامه متین*، سال پانزدهم، فصل پاییز، شماره ٦٠، صفحات ٢٩ – ٤٠.

١٢.بنی‌هاشمی، مریم(١٣٩٠)، *بررسی فقهی جرایم رایانه‌ای*، قم: دانشگاه قم، دانشکده الهیات.

١٣.بهره‌مند، حمید، کوره پز، حسین محمد و سلیمی، احسان(١٣٩٣)، راهبردهای وضعی پیشگیری از جرایم سایبری، *مجله آموزه های حقوق کیفری، دانشگاه علوم اسلامی رضوی*، بهار و تابستان، شماره ٧، صفحات ١٤٧-١٧٦.

١٤.پاکزاد، بتول(١٣٧٥)، *جرایم رایانه‌ای*، تهران: دانشگاه شهید بهشتی.

١٥.پاکزاد، بتول(١٣٨٤)، اقدام‌های سازمان‌های بین‌المللی و منطقه‌ای در خصوص جرم‌های رایانه‌ای، *مجموعه مقالات همایش بررسی جنبه های حقوقی فن‌آوری اطلاعات*، تهران: سلسبیل، صفحات ٧٠-٨٩.

١٦.جاوید نیا، جواد(١٣٨٧)، *جرایم تجارت الکترونیکی: جرایم رایانه‌ای در بستر تجارت الکترونیکی*، تهران: خرسندی.

١٧.جرایم اینترنتی و سرقت از بانک‌ها(١٣٨٢)، *مجله بانک و اقتصاد*، شماره ٤٣، اسفندماه، صفحات ٤٨-٥١ .

١٨.جلالی فراهانی، امیرحسین(١٣٨٥)، صلاحیت کیفری در فضای سایبر، *مجله فقه و حقوق*، سال سوم، زمستان، شماره ١١، صفحات ٩١-١١٩.

١٩.جوان‌جعفری، عبدالرضا و سیدزاده ثانی، سیدمهدی(١٣٩١)، *رهنمودهای عملی پیشگیری از جرم*، تهران: میزان.

٢٠.حاجی‌ده‌آبادی، احمد و سلیمی، احسان(١٣٩٣)، اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرایم رایانه‌ای)، *فصلنامه مجلس و راهبرد*، سال بیست و یکم، زمستان، شماره ٨٠، صفحات ٦١-٨٨.

٢١.حبیب زاده، محمدجعفر(١٣٨٩)، *سرقت در حقوق کیفری ایران*، تهران: دادگستر.

٢٢.حضرتی‌شاهین‌دژ، صمد(١٣٩١)، ماهیت فقهی و حقوقی سرقت الکترونیکی، *ماهنامه کانون*، شماره ١٢٨، اردیبهشت ماه، صفحات ٧٥ – ٩٣.

۲۳.دهقان، حمید(۱۳۷۹)، *بررسی قانون سرقت: جرم شناسی سرقت و مطالعه تطبیقی آن در فقه و قوانین موضوعه*، قم: دفتر تبلیغات اسلامی حوزه علمیه قم، مرکز انتشارات.

۲٤.دی آنجلیز، جینا، ترجمه حافظی، سعید، و خرم آبادی، عبدالصمد(۱۳۸۳)، *جرایم سایبر*، تهران: دبیر خانه شورای عالی اطلاع رسانی.

۲۵.ذوالقدر، محمدباقر و جلالی فراهانی، امیرحسین(۱۳۹۱)، از آمار جنایی تا اطلس جنایی، *مجموعه مقالات همایش رهیافت‌های نوین پیشگیری از جرم*، ج ۱، صفحات۷۷-۲۲٤.

۲٦.ذوالقدر، محمدباقر(۱۳۹۱)، *رهیافت‌های نوین پیشگیری از جرم(مجموعه مقالات)*، ج ۱-۳، تهران: میزان.

۲۷.رحمتی، محمدجواد(۱۳۹۲)، پیش‌گیری از جرم و آموزه‌های دینی، *مجموعه مقالات همایش رهیافت‌های نوین پیشگیری از جرم*، ج۳، صفحات۱۵۷-۱۷٦.

۲۸.رحیمی، مسعود، مفهوم فقهی و حقوقی جرم سرقت، *مجله اصلاح و تربیت*، سال چهارم، شماره ۳۸، صفحات۳۳ - ۳۵.

۲۹.زیبر، اولریش(۱۳۹۰)، *جرایم رایانه‌ای*، ترجمه نوری، محمدعلی و ...، تهران: گنج دانش.

۳۰.ساریخانی، عادل و اکرمی سراب، روح‌الله(۱۳۹۲)، کارکردهای پیشگیرانه شفافیت در سیاست جنایی، *مجله حقوقی دادگستری*، تابستان، دوره۷۷، شماره۸۲، صفحات۹۱-۱۱٦.

۳۱.سلیمی، احسان(۱۳۹۱)، خطر مضاعف جرایم رایانه‌ای، *مجموعه مقالات اولین کنگره فضای مجازی و آسیب‌های اجتماعی نوپدید*، تهران: انتشارات وزارت رفاه و تأمین اجتماعی.

۳۲.شاهمرادی، خیرالله(۱۳۹۱)، *بررسی جرم سرقت رایانه‌ای و تطبیق آن با سرقت سنتی در نظام حقوقی ایران، دانشگاه قم*، مرکز آموزش الکترونیکی.

۳۳.صبحی شیشوان، بهنام(۱۳۸۳)، شیوه‌های گوناگون سرقت رایانه‌ای، *مجله وکالت*، شماره ۲۱ و ۲۲، مهرماه، صفحات ٦۸ – ۷۱ .

۳٤.صبری، نورمحمد(۱۳۷۸)، *جرم سرقت در حقوق کیفری ایران و اسلام*، تهران: ققنوس.

۳۵.صفاری، علی(۱۳۸۰)، مبانی نظری پیشگیری از جرم، *مجله تحقیقات حقوقی*، شماره ۳۳-۳٤، صفحات۲٦۷-۳۲۱.

۳۶.طارمی، محمدحسین(۱۳۸۷)، طبقه‌بندی و آسیب‌شناسی جرایم رایانه‌ای، *نشریه پگاه حوزه*، ۲۲ تیرماه، شماره ۲۳۵، صفحات ۱۶-۱۹.
۳۷.عالی‌پور، حسن(۱۳۹۲)، *حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)*، تهران: خرسندی.
۳۸.عایدی، محمد(۱۳۸۸)، *وظایف دولت در پیشگیری از جرم(در جامعه اسلامی)*، قم: نورالسجاد.
۳۹.فاضلی، حمید(۱۳۹۱)، *بررسی احکام سرقت رایانه‌ای در نظام کیفری ایران*، دانشگاه تبریز، دانشکده حقوق و علوم اجتماعی.
۴۰.فضلی، مهدی(۱۳۹۱)، *مسئولیت کیفری در فضای سایبر*، تهران: خرسندی.
۴۱.گلدوزیان، ایرج(۱۳۸۴)، *بایسته‌های حقوق جزای عمومی*، تهران: میزان.
۴۲.متزا، دیوید و سایکز، گرشام(۱۳۹۰)، فنون خنثی‌سازی کنترل‌های اجتماعی درونی و بیرونی، ترجمه حیدر فرهمندفر، *مجله تعالی حقوق*، سال چهاردهم، مهر، آبان، آذر، شماره ۱۳ و ۱۴، ۲۰۱-۲۱۳.
۴۳.محبوبی، فرخ(۱۳۸۱)، *دانش‌آموز نفوذگر*، تهران: ناقوس.
۴۴.محمدنسل، غلامرضا(۱۳۸۷)، *پیشگیری از جرم(مجموعه مقالات)*، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری ناجا.
۴۵.محمدنسل، غلامرضا(۱۳۹۱)، *مبانی پیشگیری از جرم(مجموعه مقالات)*، تهران: میزان.
۴۶.محمدنسل، غلامرضا(۱۳۹۱)، راهنمای کارگاه علمی-کاربردی مدیریت پیشگیری از وقوع جرم و آسیب‌های اجتماعی، تهران: میزان.
۴۷.مسکنی، زهره(۱۳۸۲)، بررسی پدیده جرایم اینترنتی در ایران و جهان: این جرایم نوپای بین‌المللی، *مجله اصلاح و تربیت*، شماره ۲۴، اسفندماه، صفحات ۱۵-۱۹ .
۴۸.مطهری بیدگلی، محسن(۱۳۸۸)، *نقش عدالت اجتماعی در پیشگیری از جرم*، قم: نورالسجاد.
۴۹.معاونت کشف جرایم ناجا(۱۳۷۹)، ابعاد حقوقی جرایم رایانه‌ای، *فصلنامه دانش انتظامی*، تابستان و پاییز، شماره ۲ و ۳، صفحات ۸۶-۱۰۹.
۵۰.مقیمی، مهدی و جعفری، سیداصغر(۱۳۹۱)، مؤلفه‌های مکانی پیشگیری وضعی و پلیسی از جرم، *مجموعه مقالات همایش رهیافت‌های نوین پیشگیری از جرم*، ج ۱، صفحات۳۷۹-۴۲۶.

۵۱. مک‌نیل، مایکل و ملوین، الویز ای (۱۳۸۷)، تکنیک‌های پیشگیری از جرم، *مجموعه مقالات پلیس و پیشگیری از جرم*، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری ناجا، صفحات ٤٧٣-٤٩٩.

۵۲. منسفیلد، ریچارد(۱۳۸۹)، *هکر (نفوذگر)*، ترجمه حمید اسحاق بیگی، تهران: سهادانش.

۵۳. مهدوی مقدم، محمد(۱۳۸۹)، *بررسی فقهی و حقوقی جرائم اینترنتی*، تهران: دانشگاه پیام نور، دانشکده الهیات و علوم اسلامی.

٥٤. میرخلیلی، سیدمحمود(۱۳۹۱)، سیاست جنایی مشارکتی اسلام، *مجموعه مقالات همایش رهیافت‌های نوین پیشگیری از جرم*، ج ۱، صفحات۱۹-۷٤.

55. Clarke, R. V.(1997*), Introduction Situational Crime Prevention: Successful Case Studies*, New York: Criminal Justice Press.
56. Jaishankar, k.(2011), *Cyber Criminology, Exploring Internet Crimes and Criminal Behavior*, Boca Raton, CRC Press.
57. McNeill, Michael & Melvin, Eloise E. (2007), *Crime Prevention Techniques*, North Carolina Justice Academy.
58. Smith, T.(2003), *Cybercrimes Super lab: Brazil*, NYT, 27 OCT, Article id: 115216.
59. Turrini, E.(2010), *Increasing Attack Costs and Risks and Reducing Attack Motivations*, London: Springer Publications Ltd.