فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲
وبگاه مجله: https://cyberlaw.maragheh.iau.ir

Situational Measures to Prevent Cybercrimes in in the Light of the Dominant Pathology

Amin Amirian Farsani*
Assistant Professor, Department of Law, Shahid Ashrafi Isfahani University, Isfahan, Iran.
amirian.amin@yahoo.com
DOI: 10.30495/CYBERLAW.2023.706601

Keywords:
Preventive Pathology, Situational Prevention, Measures, Cybercrimes, Cyber Space

Abstract

Considering the huge changes that have been happening in the field of technology and the various revolutions that we have witnessed in the field of information and communication technology in the last few years, and considering the positive function of this technology, it is sometimes observed that some profit-seeking and opportunistic people try to abuse the users and to create a series of problems by learning and having the necessary skills. The cyber space provides new and highly advanced opportunities for breaking the law, as well as the potential to commit conventional and classic types of crimes in unconventional and very new ways so that the cyber criminals can do whatever they want and have in their mind in this *zero and one* galaxy. Considering this issue, the present study aims to explain the status of the situational prevention of cybercrimes in the light of the dominant pathology. Through the descriptive and analytical research methodology the current research has reached this important achievement that preventive measures such as restricting or denying access, regulatory measures, licensing measures, anonymizing tools, and encryption can be helpful in situational prevention of crimes in the cyberspace.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

تدابیر پیشگیری وضعی از جرائم سایبری در بوته آسیب‌شناسی حاکم بر آن

امین امیریان فارسانی*

استادیار گروه حقوق دانشگاه شهید اشرفی اصفهانی ، اصفهان ، ایران.

amirian.amin@yahoo.com

تاریخ دریافت: ۱۷ فروردین۱۴۰۲ تاریخ پذیرش: ۱۸ تیر ۱۴۰۲

چکیده

با توجه به تحولات عظیمی که در عرصه تکنولوژی به وقوع پیوسته و انقلاب‌های مختلفی که در زمینه فن‌آوری اطلاعات و ارتباطات در طی چند سال اخیر شاهد آن بوده‌ایم و با توجه به کارکرد مثبت این فن‌آوری اما گاه دیده می‌شود که بعضی از افراد سودجو و فرصت‌طلب با فراگرفتن داشتن و مهارت لازم در پی سوءاستفاده از کاربران و هم‌چنین ایجاد و بروز یک سری مشکلات هستند. فضای سایبر، فرصت‌های تازه و بسیار پیشرفته‌ای را برای قانون‌شکنی در اختیار انسان می‌گذارد، هم‌چنین توان بالقوه ارتکاب گونه‌های مرسوم و کلاسیک جرائم را به شیوه‌های غیرمرسوم و بسیار جدید سوق می‌دهد تا مجرمان سایبری بتوانند در این کهکشان صفر و یک، هرآن چه می‌خواهند و در اندیشه دارند، به منصه ظهور برسانند با توجه به این مساله پژوهش حاضر باهدف تبیین جایگاه پیشگیری وضعی از جرائم سایبری در بوته آسیب‌شناسی با روش تحقیق توصیفی و تحلیلی به این دستاورد مهم رسیده است که تدابیر پیشگیری وضعی ازجمله؛ تدابیر محدودکننده یا سلب‌کننده دسترسی، تدابیر نظارتی، تدابیر صدور مجوز، ابزارهای ناشناس کننده و رمزگذاری، می‌توانند به پیشگیری وضعی کمک شایانی کنند.

.

کلید واژگان: آسیب‌شناسی پیشگیری، پیشگیری وضعی، تدابیر، جرائم سایبری، فضای سایبری.

مقدمه

ویژگی‌های محیط سایبر از قبیل عدم وابستگی به زمان و مکان خاص، امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف، به همراه ماهیت جرائم سایبری، وسعت جغرافیایی کشور و گسترش ارتکاب جرائم سایبری؛ عواملی هستند که شیوه‌های ارتکاب جرائم سایبری را متنوع‌تر و کشف جرائم سایبری و به دام انداختن مجرمان را سخت‌تر کرده است. در شرایط حاضر ضرورت و اهمیت کشف جرائم سایبری در برابر انواع تهدیدات و تهاجمات بر کسی پوشیده نیست و برای حفظ امنیت عمومی ضروری است. با توجه به پیچیدگی‌های مسیر کشف جرم و لزوم تسریع کشف و دستگیری مجرمان و تأثیر آن در کاهش میزان وقوع جرائم، لازم است در حیطه جرم یابی، راهکارهای علمی متعدد و متنوعی جهت کشف جرم مطرح‌شده و بکار گرفته شود در این راستا نهاد پلیس در طول زمان با توجه به تغییر و تحولات محیط‌های پیرامونی و انتقال جرائم به محیط سایبر دچار تغییرات و دگرگونی‌هایی در جهت پاسخ‌دهی به جرائم شده‌اند و راهبردها، ساختارها و مدل‌های مختلفی را در پیش‌گرفته و اجرا نموده‌اند. بدین ترتیب در کشف جرائم سایبری، به دلیل پیچیدگی‌ها و مشکلات پیش روی آن، روش‌ها و ابزارهای مختلفی نیاز است و مقابله جدی و مؤثر پلیس را می‌طلبد که با توسل به مدرن ترین وسایل و روش‌ها، بتواند توان مقابله با مجرمانی که مرتکب این جرائم می‌شوند را داشته باشد (داوری، ۱۴۰۰: ۳۶). بنابراین شناسایی عوامل تأثیرگذار بر کشف جرائم سایبری از اهمیت ویژه‌ای برخوردار است، به‌طوری‌که بر سرعت کشف این جرائم می‌افزاید و بدون توجه به این موضوع نمی‌توان در جهت کاهش آمار رو به رشد جرائم سایبری گام برداشت و به‌منظور ردیابی، تعقیب و تحت پیگرد قرار دادن و کشف ادله و اثبات جرم مجهز شد؛ درحالی‌که مجرمان هرچه بیشتر تلاش خواهند نمود از این ظرفیت عظیم سایبری در عرصه ناامنی‌های اجتماعی استفاده نمایند. بررسی‌ها نیز نشان می‌دهد که علی‌رغم تشکیل پلیس مبارزه با جرائم سایبری ضابط تخصصی تحت عنوان ضابط کشف جرائم سایبری که به‌صورت تخصصی به مقابله با جرائم سایبری بپردازد وجود ندارد که دلیل آن می‌تواند خلأ قانونی و عدم تصویب قوانین اختصاصی باشد. لذا با توجه به اینکه ادله اثبات جرم در فضای سایبری به علت الکترونیکی بودن و ویژگی‌های خاص آن‌که متفاوت از ادله‌های جرائم سنتی هست و پلیس به‌منظور بررسی و کشف جرائم سایبری با مسائلی مواجه می‌شود که در سایر جرائم مطرح نیست، لذا با توجه به وضعیت و شرایط خاص جرائم سایبری و ادله‌ها و ابزارهای ارتکاب جرائم سایبری و امکان جعل و دست‌کاری ادله جرائم سایبری باید به‌طور مفصل نقش ضابطان در کشف و تعقیب این جرائم و آسیب‌هایی که با آن مواجه هستند بررسی شود. پژوهش حاضر درصدد پاسخگویی به این سؤالات است که راهبردهای پیشگیری وضعی کدامند؟ آسیب‌های حاکم بر پیشگیری سایبری کدامند؟

۱. مفهوم لغوی پیشگیری از وقوع جرم

واژه پیشگیری ازنظر لغوی جلوگیری کردن، مانع‌شدن، دفع، صیانت، جلو بستن و نیز اقدامات احتیاطی برای جلوگیری از حوادث بد و ناخواسته معنا کرده‌اند (معین، ۱۳۷۷: ۹۳۳). یا به معنای منع کردن، دفع، به نگهداری برخاستن نیز آمده است (دهخدا، ۱۳۷۷: ۵۹۹۱). بنابراین، پیشگیری در علم لغت به معنای مانع یا سدی است که جلوی اتفاق افتادن یک امر یا موضوع بد و ناخوشایند را می‌گیرد. ازنظر ریشه‌شناسی، کلمه پیشگیری در دو بعد به معنای پیش‌دستی کردن و به جلوی چیزی رفتن و همچنین به معنی آگاه کردن، خبر دادن و هشدار دادن آمده است. همچنین این واژه در مفهوم جرم‌شناسی، خارج از گستره نظام کیفری تحقق پیدا می‌کند و عبارت است از «هرگونه اقدامی که جلوگیری از ارتکاب جرم را موردتوجه قرار دهد» (نجفی ابرندآبادی، ۱۳۹۸: ۵۲۵). باید گفت درواقع از منظر جرم‌شناسی

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

پیشگیرانه، پاسخ‌های پیشگیرانه به پدیده مجرمانه، اقدام‌هایی است که جنبه کنشی داشته و با ماهیت غیر قهرآمیز یا در مقام سالم‌سازی جامعه یا برای رفع بحران‌های جرم‌زا و یا برای برهم زدن اوضاع‌واحوال ماقبل بزهکاری اتخاذ می‌شود.

۲. اصطلاح‌شناسی پیشگیری از وقوع جرم

پیشگیری یکی از وسایل و امکانات سیاست جنایی برای کنترل جرم است. ازنظر علمی و اصطلاحی، مفهوم پیشگیری به مفاهیم مختلفی تعلق دارد؛ یعنی ترکیبی از تئوری و تجربه است. در ابتدا پیشگیری به‌صورت نظری مطرح می‌شد. انریکو فری یکی از پیشگامان مکتب تحققی و از بانیان نظریه عوامل محیطی بزهکاری، پیشنهادهایی در زمینه دفاع جمعی در مقابل بزهکاری- که درواقع طرح تغییر جامعه است- را ارائه می‌کند، یعنی عرف و عادات باید دگرگون شود. پاره‌ای از این نظریات کم‌وبیش به اجرا گذاشته‌شده و تجربه می‌شوند. به دنبال این تجربه، ارزیابی تأثیر این تجربیات مطرح می‌شود. به دنبال ارزیابی این تجربیات، امکان اصلاح و جرح‌وتعدیل نظریه قبل فراهم می‌شود و به‌این‌ترتیب، مفهوم پیشگیری یک مفهوم منطقی و عملی به خود می‌گیرد (نجفی ابرندآبادی، ۱۳۹۳: ۷۴۱).

در اصطلاح‌شناسی، بنابراین، می‌توان گفت: مجموعه تدابیر و اقداماتی است که هدف از اعمال آن کاهش جرم و بزه، ترس و ارعاب در مجرمان برای عدم تکرار جرم‌های بعدی، جلوگیری از مجرم شدن مجرمان بالقوه، تأدیب افراد جامعه علی‌الخصوص مجرمان، باهدف افزایش نظم و امنیت عمومی و فردی، کاهش انگیزه‌ها و فرصت‌های مجرمانه در افراد جامعه، دفاع از حقوق قربانیان جرم، در چارچوب قانون است.

۳. پیشگیری وضعی جرم‌شناختی

در پیشگیری وضعی جرم شناختی،[1] که مبنای نظری آن در جرم‌شناسی، وضعیت ماقبل بزهکاری است، با فرآیند گذار از اندیشه به عمل[2] مواجه هستیم و درصدد تغییر وضعیت مشرف بر جرم هستیم تا معادله جرم به ضرر مجرم شود. به‌بیان‌دیگر، هدف اتخاذ اقداماتی است که فرآیند گذار از اندیشه به عمل را قطع کند (نجفی ابرندآبادی، ۱۳۹۳: ۷۸۸-۷۵۱). اقدام‌های وضعی در این نوع پیشگیری، ناظر به اوضاع، احوال و شرایطی است که مجرم را در آستانه ارتکاب جرم قرار می‌دهند. این اوضاع‌واحوال که در جرم‌شناسی وضعیت‌های ماقبل بزهکاری یا وضعیت‌های پیش جنائی نام دارند، فرایند گذار از اندیشه به عمل مجرمانه را تحریک یا تسهیل کرده و نقش تعیین‌کننده‌ای در آن ایفا می‌کند در پیشگیری وضعی جرم‌شناختی، اندیشه اساسی این است که گذار به عمل مجرمانه نه‌فقط به انگیزه‌های مجرم بستگی دارد، بلکه به خصوصیات وضعی، شرایط موضعی، شرایط موجود در اوضاع‌واحوال قبل از جرم بستگی دارد. هدف، چیره شدن به اوضاع قبل از جرم که فرد را در آستانه جرمی قرار داده است.

در این نوع پیشگیری وضعی، دو اقدام اساسی می‌توان انجام داد: کاهش وضعیت‌های جرم‌زا یا وضعیت‌های موجود در آستانه ارتکاب جرم یا وضعیت‌هایی که زمینه ارتکاب جرم را فراهم می‌کند و افزایش خطر دستگیری مجرم یا بالا بردن هزینه کیفری ارتکاب جرم برای مجرم.

۴. پیشگیری وضعی بزه‌دیده‌شناختی

امروزه، شکل جدیدی از پیشگیری، موسوم به «پیشگیری بزه دیده شناختی»[3] که خود از شاخه‌های «پیشگیری وضعی» از بزهکاری محسوب می‌شود، در سیاست جنایی موردتوجه و استفاده قرارگرفته است. تدابیر و اقدام‌ها در پیشگیری بزه دیده شناسانه ناظر به اجتناب

[1] Criminological Preventional
[2] Acting Out
[3] Victim logical Prevention

از بزه دیده واقع‌شدن یا به‌عبارت‌دیگر، جلوگیری از بزه دیدگی افراد یا اموال به‌عنوان آماج یا هدف جرم، است. در این چارچوب، بحث مصون‌سازی، ایمن‌سازی و تقویت آن دسته از آماج‌هایی مطرح می‌شود که بزهکاران نوعاً به آن‌ها تعرض می‌کنند. با اتخاذ و اعمال این اقدامات، هدف آن است که هزینه روانی، جسمانی و کیفری جرم برای شخص بزهکار تا حداکثر ممکن بالا رود و لااقل خود بزه دیده، به‌عنوان عنصری از وضعیت ماقبل بزهکاری یا وضعیت پیش جنایی، زمینه جذابی را برای بزهکاران فراهم نیاورد (نجفی ابرندآبادی، ۱۳۹۲: ۱۱). به دیگر سخن، در پیشگیری وضعی بزه دیده شناختی، هدف مداخله در وضعیت پیش جنایی به شکلی است که از بزه دیده واقع‌شدن هدف و یا موضوع جرم جلوگیری شود.

بنابراین، این نوع پیشگیری با تغییر وضعیت‌های ماقبل بزهکاری، مثلاً از طریق حفاظت یا تقویت حمایت از بزه دیده یا آماج بالقوه جرم با استفاده از دستاورد فناوری‌های نوین، دشوار کردن ارتکاب جرم، بالا بردن خطر شناسایی و دستگیری بزهکار و کاهش سود و لذت مورد انتظار مجرم از تعرض به هدف یا بزه دیده خاص را دنبال می‌کند و بدین ترتیب فرض بر این است که در چنین شرایطی، بزهکار از عملی ساختن اندیشه خود نسبت به آن بزه دیده یا آماج حمایت‌شده صرف‌نظر خواهد کرد. به‌عبارت‌دیگر، پیشگیری وضعی، «شامل مسئول کردن کل جامعه در قبال خطر مجرمانه و خطر بزه دیده شناختی می‌شود؛ به‌گونه‌ای که اعضای آن، خود، در مراقبت از خود و اموال مشارکت کنند.» (ابراهیمی، ۱۳۹۱: ۹۲). ازاین‌رو، تفاوت پیشگیری وضعی با سایر پیشگیری‌ها در این است که در سایر پیشگیری‌ها عمده اقدامات ما ناظر به این است که افراد مجرم نشوند و عوامل جرم‌زا خنثی شوند؛ اما در پیشگیری وضعی، علاوه بر این بُعد، بُعد دیگری وجود دارد که ناظر به بزه دیده نشدن افراد و اموال است.

۵. مبانی نظری حاکم بر بزه دیدگی سایبری

۱،۵. نظریه فراگیری و بزه دیدگی سایبری

طبق این نظریه فعالیت‌های روزمره افراد به‌طور بالقوه تحت تأثیر جرائم سایبری قرار دارد؛ و ازآنجایی‌که استفاده از فضای سایبر در بین افراد مختلف جامعه فراگیر شده است، افراد از هر قشر و یا گروهی که باشند خواه یا ناخواه به‌نوعی با این جرائم مواجه خواهند شد. به‌عبارت‌دیگر در جامعه امروز افراد چه مستقیماً با فضای سایبر در ارتباط باشند و چه غیرمستقیم و باواسطه، به‌نوعی امکان بزه دیده شدنشان وجود دارد. امکان بزه دیده شدن در فرض ارتباط مستقیم با فضای سایبر کاملاً ملموس هست و نیازی به توضیح بیشتر نیست اما در فرضی که ارتباط با فضای سایبر غیرمستقیم هست، نیاز به توضیح بیشتر دارد که با ذکر مثالی روشن خواهد شد. فرض کنید فردی برای ثبت‌نام اینترنتی خود به یک کافی‌نت مراجعه و از مسئول آن تقاضا می‌کند تا فرایند ثبت‌نام وی را انجام دهد و در همین حال شخص ثالثی با توجه به دانش پایین مسئول کافی‌نت اقدام به استخراج اطلاعات متقاضی نموده و در فعالیت‌های مجرمانه خود از آن سوءاستفاده می‌کند، در این فرض فرد متقاضی بدون اینکه در فعالیت سایبری نقش مستقیم داشته باشد قربانی جرم سایبری شده و به تعبیری بزه دیده سایبری است. با این وصف دامنه شمول بزه دیدگی سایبری با توجه به مطالب مطرح‌شده، بسیار گسترده بوده و افراد بسیاری را در برمی گیرد. بااین‌وجود نکته حائز اهمیت در بررسی جرم شناسانه بزه دیدگی سایبری همین فراگیری استفاده از فضای سایبر در میان اقشار مختلف جامعه است، که مبنای شکل‌گیری نظریه فعالیت‌های روزمره و بزه دیدگی سایبری است، که در ادامه به آن می‌پردازیم.

۲،۵. نظریه فعالیت‌های روزمره و بزه دیدگی سایبری

همان‌طور که گذشت نظریه فعالیت روزمره از سوی دو جامعه‌شناس به نام‌های لارنس کوهن و مارکوس فلسون مطرح شد. بر اساس نظریه کوهن و فلسون، زمانی بزه دیدگی احتمال بیشتر واقع‌شدن دارد که سه عامل در یک‌زمان و مکان جمع شود. این سه عامل عبارت‌اند

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

از: الف: وجود یک مجرم باانگیزه ب: وجود یک هدف مناسب ج: و نبود محافظ یا مدافع برای اهداف یا افراد یا آماج محافظت نشده در این نظریه برای جلوگیری از بزه دیدگی بر روی دو عامل یعنی هدف مناسب و عدم محافظت کافی تمرکز می‌شود. بدین معنی که ما در جامعه همیشه افرادی را داریم که برای ارتکاب جرم انگیزه دارند، حال برای پیشگیری از جرم اولاً باید اهداف مجرمانه را کاهش دهیم و ثانیاً نظارت‌ها و محافظت‌ها را بیشتر و کارآمدتر کنیم (خانیکی و بابائی، ۱۳۹۰: ۷۷-۷۸).

بنابر عقیده این دو دانشمند تغییر الگوی زندگی در جوامع کنونی و امروزی فرصت‌های مجرمانه را افزایش داده است. به‌عنوان نمونه در جوامع امروزی بر تعداد کلان‌شهرها روزبه‌روز افزوده می‌شود و همین امر باعث شده که افراد برای انجام اعمال روزمره و فعالیت‌های شغلی خود، فاصله بیشتری از منزل خود بگیرند، از طرف دیگر افزایش ساعات کاری و افزایش شمار زنان شاغل باعث کاهش نظارت بر خانه و اعضای خانواده شده است. کمبود وقت و کاهش روابط خانوادگی سبب شده که سالمندان به دلیل جدایی از بستگان خود و کودکان نیز در نبود والدین ساعات بیشتری را تنها زندگی کنند که هر دو گروه به دلیل ناتوانی اهداف مناسبی برای مجرمان هستند. بر این اساس برخی از افراد بر پایه تفاوت‌هایشان در مدل زندگی، بیش از دیگران برای بزه دیده شدن مناسب هستند.

حال با توجه به آشنایی مختصری نسبت به کلیات و مبانی نظریه فعالیت روزمره، در خصوص تطبیق این نظریه با فضای سایبر و بزه دیدگان سایبری نیز باید گفت در فضای سایبر برخلاف فضای واقعی که برای تحقق جرم نیاز به سه عامل داشتیم، صرف فقدان محافظ توانا منجر به تحقق بزه دیدگی می‌شود. درواقع دو عامل مجرم باانگیزه و هدف مناسب در فضای سایبر قابل‌دستیابی‌اند و مجرم به‌راحتی می‌تواند از میان کاربران این فضا هدف مناسب خود را بیابد. و مناسب بودن هدف در دیدگاه فلسون نشانگر چهار ضابطه است: ۱- ارزشمند بودن هدف جرم ۲- استیصال هدف جرم ۳-قابلیت رؤیت هدف جرم و ۴- دسترسی به هدف جرم، که بررسی این چهارعنصر در فضای سایبری به‌خوبی این واقعیت را که مناسب بودن هدف در فضای سایبر امری مفروض است، به اثبات می‌رساند (ابراهیمی، ۱۳۹۸: ۷۲).

به‌عنوان‌مثال اگر کاربر بنا بر هر دلیلی به اینترنت متصل شود، رایانه وی اطلاعاتی در فضای سایبر منتقل می‌کند که همین امر سبب جذب مجرمان سایبری می‌شود؛ و اگر مجرمان سایبری به‌اندازه کافی در سیستم‌های رایانه‌ای خبره و توانمند باشند، استیصال و به تعبیری گیر افتادن بزه دیده امری بدیهی خواهد بود. به‌عبارت‌دیگر از زمانی که کاربر به اینترنت متصل می‌شود و در فضای سایبر حضور پیدا می‌کند، نحوه عملکرد او و نوع و میزان تبادل اطلاعاتش مجرمان سایبری را به‌سوی این قبیل افراد می‌کشاند تا شاید با پیدا کردن راهی وی را قربانی نیات شوم و پلید خود کنند.

برای تقریب بیشتر موضوع به ذهن مثالی را ذکر می‌کنیم: به‌عنوان‌مثال اگر شما به‌عنوان یک محقق در فضای سایبر فعالیت کنید و در سایت‌های اینترنتی مرتبط باعلاقه‌تان عضو شوید، پس از گذشت مدتی با انبوهی از ایمیل‌ها و نامه‌های الکترونیکی در پست الکترونیک خود مواجه خواهید شد که با پرداختن به موضوعات موردعلاقه شما و تقاضای دریافت یکسری اطلاعات سعی در فریب دادن شما دارند. این در حالی است که هیچ‌یک از این ایمیل‌ها از سوی ارگان‌ها و مؤسسات معتبر ارسال نشده است. این موارد مصداق بارز سوءاستفاده بزهکاران از نحوه، نوع و میزان حضور افراد در فضای سایبر است. در رابطه بارویت پذیری نیز باید گفت، بزه‌کاران پس از مشاهده علائم و نشانه‌هایی از هدف موردنظر، حمله را به سمت آن آغاز می‌کنند. شاید هیچ محیطی به‌اندازه فضای سایبر قابل‌مشاهده نباشد. ازاین‌جهت بزه‌کاران احتمالی را به ارتکاب جرم برمی‌انگیزد. در خصوص در دسترس بودن نیز باید گفت، در فضای سایبر با توجه به ویژگی‌های آن، تمام داده‌ها و اطلاعات ازجمله فیلم و عکس و آهنگ و متن را می‌توان به اشتراک گذاشت و این مزیت در این فضا بیش از هرجای دیگری قابل‌توجه است. افراد علاوه بر اینکه به‌راحتی می‌توانند به داده‌ها دست یابند، به‌آسانی هم می‌توانند آن‌ها را تغییر داده و دست‌کاری کنند (امیریان، ۱۳۹۶: ۱۰).

دانشگاه آزاد اسلامی واحد مراغه

درنهایت اینکه تنها رکنی که در بزه دیدگی افراد مؤثر است میزان نظارت و حفاظت است. به دیگر عبارت، عامل اصلی در بزه دیدگی سایبری از دیدگاه نظریه فعالیت روزمره، نبود تدابیر امنیتی و حفاظتی در فضای سایبر است. بر اساس نظریه فعالیت‌های روزمره، بهترین روش برای جلوگیری از بزه دیدگی افراد در فضای سایبر، دشوار کردن دسترسی به هدف یا همان بزه دیده است، چراکه امکان آشنایی و آموزش افراد به‌صورت حرفه‌ای جهت مقابله با حملات سایبری کاری غیرممکن و پرهزینه است، اما می‌توان با آموزش‌های ابتدایی و آشنایی به استفاده از نرم‌افزارهای امنیتی و از طرفی نظارت بر کار کاربران فضای سایبر به‌نوعی دسترسی به بزه دیده را دشوار کرد و از این طریق بزه دیدگی سایبری و از طرفی از تحقق جرائم سایبری که بزه دیده می‌تواند در آن نقش داشته باشد، پیشگیری کرد.

نظریه فعالیت روزمره از بعد فعالیت روزانه افراد نیز قابل‌تحلیل و بررسی است، درواقع تفاوت افراد در رفتارها و فعالیت روزانه سبب تفاوت سطح خطرپذیری و بزه دیدگی آنان و نقشی که می‌توانند در تحقق جرائم داشته باشند، می‌شود. در حقیقت میزان و نوع عملکرد کاربران در فضای سایبر در بزه دیدگی آنان کاملاً مؤثر است به‌گونه‌ای که در این فرض کاربران آنلاین و خصوصاً افرادی که علاقه‌مند به بازدید از سایت‌های ناشناس هستند، آهنگ‌ها، فیلم‌ها و یا نرم‌افزارهای رایگان را از هر سایتی دانلود می‌کنند و یا اینکه روی آیکون‌ها و تبلیغات اینترنتی بدون اندیشه و احتیاط کلیک می‌کنند، به‌احتمال‌زیاد درنتیجه اقدام و عملکرد خود، قربانی مجرمان سایبری می‌شوند. درواقع «سایت‌های اراده دهنده موزیک، ویدئو و نرم‌افزار، گنجینه‌ای از نرم‌افزارهای مخرب در لباس مبدل هستند. بسیاری از متخصصان امنیتی معتقدند وب سایت‌های این‌چنینی یکی از خطرناک‌ترین محیط‌ها برای بازدید هستند، چراکه اغلب این وب‌سایت‌ها یک مدل مشخصی از کسب‌وکار و همچنین اعتبار امنیتی کافی ندارند. اگرچه به علت محتوای خطرناک و غیرقابل‌اعتماد این‌گونه وب‌سایت‌ها، کاربران باید از بازدید آن‌ها صرف‌نظر کنند اما اگر به هر دلیلی به سراغ این وب‌سایت‌ها رفتند، بهتر است به‌منظور حفاظت از سیستم خود، از یک آنتی‌ویروس کاملاً به‌روز استفاده کنند و یا به‌عنوان‌مثال کاربرانی که به وب‌سایت‌های نامشروع و دارای محتوای غیراخلاقی سر می‌زنند نیز در معرض خطر هستند» چراکه وب‌سایت‌های نامشروع به‌خودی‌خود نسبت به سایر سایت‌های فعال و عمومی از درجه امنیت کمتری برخوردار هستند. اگرچه بازدید از این وب سایت‌ها به دلیل محتوای آن‌ها، به‌طورکلی مخرب است اما به دلیل اینکه هیچ خط‌مشی امنیتی مشخصی ندارند علاوه بر محتوای مخرب می‌توانند حاوی برنامه‌های آلوده و بدافزار هم باشند. ازاین‌رو کاربران بهتر است به هیچ دلیلی به هر یک از این وب سایت‌ها وارد نشوند. باید گفت مطابق نظریه فعالیت روزمره، فعالیت‌های افراد در فضای سایبر و نوع عملکرد آنان در این فضا در بزه دیدگی آنان کاملاً مؤثر است. به‌گونه‌ای که تفاوت افراد در رفتارهای روزمره در فضای سایبر سبب تفاوت سطح خطرپذیری بزه دیدگی آنان می‌شود.

۳،۵. نظریه سبک زندگی و بزه دیدگی سایبری

همان‌طور که گذشت این نظریه در پی مطالعات دانشمندانی چون گات فردسن، هیندلنگ و گارفالو توسعه پیدا کرد. مطابق این نظریه جرم یک واقعه اتفاقی نیست بلکه بزه دیدگی بر اساس شیوه، سبک و مدل زندگی افراد و عملکرد زندگی آنان متغیر است. برخی از دانشمندان معتقدند که افراد ممکن است به این دلیل بزه دیده شوند که نوع زندگی، آنان را در معرض ارتکاب جرم قرار داده است. بر اساس این نظریه می‌توان گفت: نوع زندگی افراد نقش کلیدی در آسیب‌پذیری آن‌ها دارد، هرچه افراد شیوه زندگی بازتری داشته باشند خطر و احتمال بزه دیدگی‌شان نیز بیشتر می‌شود. نظریه شیوه یا سبک زندگی به‌واسطه عواملی تحت تأثیر قرار می‌گیرد. یکی از این عوامل نقشی است که افراد در جامعه ایفا می‌کنند و این نقش، بعضاً کمابیش آن‌ها را به‌سوی بزه دیدگی می‌کشاند. برای مثال جوانان بیشتر در معرض خطر بزه دیدگی قرار دارند. زیرا نقش‌های اجتماعی آن‌ها سبب می‌شود بیشتر در محیط‌های مجرمانه و خطرناک و یا در زمان‌های خطرناک رفت‌وآمد کنند (کوهساری، ۱۳۹۹ :۶۵).

به بیانی دیگر نسل جوان و نوجوان امروز نه‌تنها برای کارهای مهمی چون عملیات بانکی، ثبت‌نام مؤسسات و دانشگاه‌ها، انجام تکالیف درسی و... از امکانات این فضا استفاده می‌کنند. بلکه بسیاری از تفریحات و سرگرمی‌شان را نیز در این فضا جستجو می‌کنند. حال اینکه قشر سالخورده و نسل دیروز به این خاطر که با این فضا رشد نکردند، به‌ندرت در این فضا به فعالیت می‌پردازند. درنتیجه اینکه حضور

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

بیشتر در این فضا، احتمال بزه دیدگی جوانان و نوجوانان امروز را که بیشترین کاربران این فضا را تشکیل می‌دهند، افزایش می‌دهد. در کنار نقش‌های اجتماعی می‌توان به موقعیت فرد در ساختار اجتماع نیز اشاره کرد. موقعیت فرد در ساختار اجتماع نیز می‌تواند در احتمال بزه دیدگی مؤثر باشد چراکه اغلب، هرچه افراد دارای موقعیت اجتماعی بالاتری باشند به دلیل فعالیت‌هایی که انجام می‌دهند و محیط‌هایی که به آن رفت‌وآمد می‌کنند خطر بزه دیدگی‌شان پایین می‌آید. هرچه افراد با اشخاص بزهکار و یا محیط‌هایی مجرمانه و خطرناک و یا زمان‌های خطرناک بیشتر رفت‌وآمد کنند، شانس بزه دیدگی خود را افزایش می‌دهند. موقعیت‌های احتمالی به وجود آمده بین بزهکار و بزه دیده بالقوه با توجه به سبک زندگی آن‌ها تغییر می‌کند. بنابراین با توجه به تصمیماتی که افراد برای برگزیدن انواع شیوه‌های زندگی اتخاذ می‌کنند احتمال بزه دیدگی نسبتاً قابل پیش‌بینی است و می‌توان گفت علل بزه دیدگی برخی افراد انتخاب نوع سبک زندگی آنان است که خطر بزه دیدگی را کم یا زیاد می‌کند.

بنابراین تئوری سبک زندگی بیان می‌کند که احتمال قربانی شدن افراد در اجتماع بیشتر است. مردان، جوانان و افراد مستمند بیشترین ریسک و خطر را برای قربانی شدن دارند. زیرا این‌گونه افراد شرایط پرخطری نسبت به زنان، سالمندان و افراد مرفه دارند. به نظر می رسد تفاوت‌های فردی از قبیل زیاد بیرون بسر بردن از خانه به‌ویژه در شب، درگیری در فعالیت‌های عمومی و معاشرت باکسانی که درگیر رفتار مجرمانه‌اند و از آن رضایت دارند، احتمال بزه دیده شدن یک شخص را افزایش می‌دهد. در فضای سایبر نیز موقعیت اجتماعی افراد ازجمله میزان تحصیلات به‌ویژه دانش رایانه‌ای، اشتغال، نوع شغل کاربران و ... در میزان بزه دیدگی آنان مؤثر است. برای مثال کاربری که از میزان تحصیلات بالایی برخوردار نیست و به‌صورت تجربی نحوه فعالیت در اینترنت و فضای سایبر را فراگرفته است به‌طورمعمول در هنگام خطر و نفوذ رخنه گران و هکرها به سیستم رایانه‌ای یا گوشی همراهش خیلی دیر متوجه بزه دیدگی خود می شود، وقتی‌که اطلاعات او در اختیار رخنه گران قرارگرفته و عملاً دیگر کاری نمی‌توان کرد.

البته باید این نکته را هم اشاره کرد که صرف تحصیلات بالا برای حضور در این فضا کافی نیست بلکه آنچه لازم است فراگیری دانش رایانه‌ای متناسب با میزان فعالیت هر کاربر در فضای سایبر است. این نکته را هم باید خاطرنشان کرد که افرادی که درگیر فعالیت‌های مجرمانه در فضای سایبر شده‌اند، اغلب خودشان به هدفی مناسب برای بزهکاران بدل می‌شوند چراکه این افراد در اندیشه‌های مجرمانه خویش غرق‌شده و گمان می‌کنند که بر فعالیت‌های مجرمانه تسلط کامل دارند و ازاین‌رو هیچ‌وقت بزه دیده نخواهند شد. البته ناگفته نماند که این افراد جزء مجرمان حرفه‌ای سایبری نیستند و غالباً کسانی هستند که از روش‌های رده خارج بزهکاری سایبری استفاده می کنند یا از راه‌های ارائه‌شده توسط مجرمان سایبری به‌منظور گریز از برخی محدودیت‌های موجود در فضای سایبر بهره می‌گیرند. به‌عنوان‌مثال به افرادی که از نرم‌افزارهای هک که به‌صورت عمده در بازار فروخته و یا از سایت‌های ناشناس بارگذاری می‌شوند، بهره می گیرند در زمره همین افراد است و در غالب موارد از سوی طراحان اصلی نرم‌افزار مورد سوءاستفاده قرارگرفته یا اطلاعاتشان توسط آن‌ها به سرقت می‌رود.

همان‌گونه که مطرح شد برخی از افراد از روش‌های موجود برای رهایی از محدودیت‌های موجود در فضای سایبر، استفاده می‌کنند، به‌عنوان‌مثال از نرم‌افزارهایی تحت عنوان فیلترشکن یا (VPN)ها برای عبور از سد فیلترینگ اعمال‌شده از سوی دولت استفاده می‌کنند. ایشان نیز ناخواسته در دام بزه‌کاران سایبری می‌افتند، چراکه در برخی موارد سیستم‌های گریز از فیلترینگ خود حاوی بدافزارهایی هستند که اطلاعات و داده‌های شخصی کاربران را برای سازندگانشان ارسال می‌کنند. در این موارد استفاده‌کننده خود را فردی هوشمند می‌داند که از روش‌های نوین برای اعمال غیرقانونی بهره می‌گیرد، غافل از اینکه خود به بازیچه‌ای در دست دیگری تبدیل‌شده است. به تعبیری این شخص بزه دیده جرمی شده، که خود زمینه سازش بوده است.

۶. تدابیر و راهبردهای پیشگیری وضعی از جرائم سایبری

مبنای پیشگیری وضعی بر این فرض استوار است که یک انسان متعارف، در همه زمینه‌ها خواسته یا ناخواسته به‌طور 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.

دانشگاه آزاد اسلامی واحد مراغه

حال اگر این فرض در مورد مجازات 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 به‌این‌ترتیب این نوع پیشگیری، برخلاف پیشگیری اجتماعی رویکردی بزه دیده محور یا آماج محور دارد. هرچند عنصر مهم مجرم نیز به‌نوعی همچنان جایگاه خود را حفظ کرده است. درواقع یکی از اهداف مهم پیشگیری وضعی، تأثیرگذاری مستقیم برگزینش مجرم و تغییر عقلانیت اوست. در اینجا تلاش می‌شود در فرایند گزار از اندیشه به عمل مجرمانه وقفه ایجاد شود، بنابراین هدف اصلی، انصراف قطعی مجرم بالقوه از ارتکاب جرم نبوده و کوششی جهت جلوگیری از شکل‌گیری شخصیت مجرمانه‌اش صورت نمی‌گیرد و همان‌طور که گفته شد این مهم به پیشگیری اجتماعی واگذارشده است.

درباره تدابیر پیشگیرانه وضعی از وقوع جرم، مطالعات و پژوهش‌های گسترده و مفصلی صورت گرفته و تقسیم‌بندی‌های گوناگونی از آن به‌عمل‌آمده است. همچنین نقاط قوت و ضعف هر یک از آن‌ها از جنبه‌های اقتصادی، اجتماعی، روان‌شناختی و حقوقی (به‌ویژه پایه موازین حقوق بشری) بررسی و تحلیل‌شده است. در خصوص مفهوم و شکل‌های به‌کارگیری تدابیر پیشگیرانه وضعی در فضای سایبر، به‌طورکلی می‌توان این‌گونه تدابیر را در چهار گروه طبقه‌بندی کرد:۱- تدابیر نظارتی. ۲- تدابیر صدور مجوز ۳- ناشناس کننده‌ها و رمزنگارها ۴- تدابیر محدودکننده دسترسی (فیلترینگ).

۱،۶. تدابیر نظارتی

به‌طور خلاصه این تدابیر در دوشاخه اصلی قرار می‌گیرند. یک شیوه این است که با اتخاذ تدابیر نظارتی در دنیای فیزیکی توسط پلیس، از ارتکاب جرائم 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 خانواده باشد تا فرزندان فرصت سوءاستفاده از خلوت در فضای سایبر را پیدا نکنند. شیوه دیگر نظارت که با ویژگی این فضا نیز سازگار است، نظارت الکترونیکی نام دارد (عالی پور، ۱۳۹۳: ۲۴۵). در اینجا با به‌کارگیری تجهیزات و برنامه‌های خاص توسط پلیس، فعالیت‌های شبکه‌ای افراد، تحت نظر قرار می‌گیرد. نظارت الکترونیکی نیز به دو شکل انجام می‌شود. هم‌زمان و غیر هم‌زمان. در حالت اول ابزار الکترونیکی، پلیس یا متصدی مربوطه را از فعالیت غیرمجاز شبکه‌ای کاربر در همان زمان آگاه می‌کند. به‌این‌ترتیب او می‌تواند اقدامات لازم را انجام دهد. اما در نظارت غیرزنده بسته به میزان دقت ابزار، تمام یا بخش گزینش‌شده‌ای از فعالیت‌های شبکه‌ای را ثبت می‌کند تا در فرصتی دیگر پلیس با بررسی آن‌ها موارد غیرمجاز را مشخص کند

۲،۶. تدابیر صدور مجوز

این تدابیر با الگوبرداری از دنیای فیزیکی به اجرا درمی‌آیند. یکی از شیوه‌های رایج سلب فرصت مجرمانه یا حتی جلوگیری از بزه دیدگی افراد که پلیس می‌تواند انجام دهد کنترل دسترسی است. به‌عبارت‌دیگر تنها کسانی می‌توانند به محیط‌هایی با ویژگی‌های خاص وارد شوند که تأییدیه موردنظر داشته باشند. بنابراین چنانچه تدابیر کنترل دسترسی به‌خوبی اجرا شود از ورود مجرمان بالقوه و همچنین کسانی که به هر دلیل مطابق قانون نمی‌توانند وارد آن محیط شوند، جلوگیری به عمل می‌آید. برای مثال، در اکثر کشورها میان مسائل جنسی بزرگسالان یا کودکان تفاوت قائل می‌شوند و حتی برای گروه اول قوانین حمایتی نیز وضع کرده‌اند. اما با دسترسی و مواجهه کودکان با مسائل مستهجن و مبتذل برخورد می‌کنند و حتی برای متخلفین مجازاتی را در نظر گرفته‌اند (حیدری، ۱۳۹۷: ۲۲). همچنین فناوری‌های تأیید سن یکی از مهم‌ترین این ابزارها هستند. در این فناوری با اخذ اطلاعات معتبر از کاربر، هویت او (به‌ویژه سنش) بررسی و در صورت تأیید اجازه دسترسی به سایت داده خواهد شد

۳،۶. ناشناس کننده‌ها و رمزنگارها

این تدابیر نیز فرایند مشابهی را اجرا می‌کنند. کارکرد اصلی‌شان این است که با پنهان کردن هویت یا محتوای اطلاعات افراد، از بزه دیدگی شان جلوگیری می‌کنند. کارکرد ناشناس کننده‌ها این است که پیونده‌ای هویتی را قطع کنند. این ابزارها تنها آنچه را که به‌طور تصادفی ایجادشده به‌عنوان هویت اشخاص ارائه می‌دهند و کاربران قادر خواهند بود در تعاملات شبکه‌ای خود از آن استفاده کنند. به‌این‌ترتیب هرکس بخواهد از هویت ناشناس کاربر موردنظر آگاه شود با موانعی مواجه خواهد شد. این اقدام به‌ویژه برای زنان و کودکان یا به‌طورکلی اشخاص آسیب‌پذیر سودمند است. زیرا بی‌آنکه فرصت شناسایی خود را به مجرمان سایبر بدهند، می‌توانند به فعالیت‌های شبکه‌ای بپردازند (قناد، ۱۳۹۵: ۱۲۵). به‌عبارت‌دیگر با ایجاد حریم بیشتر برای افراد از مقابل دیدگان تمامی اشخاص (به استثنا آن‌هایی که مجاز شمرده می شوند) پنهان می‌کند؛ بنابراین پلیس با به‌کارگیری این روش و در اختیار قرار دادن آن به کاربران خاص می‌تواند در پیشگیری از جرائم سایبری مؤثر واقع شود. در اکثر فعالیت‌های رمزنگاری، اصل ساز پیامی را برای مخاطب خود ایجاد می‌کند و سپس آن را طی فرایند رمزنگاری محفوظ کرده و به‌عنوان یک رمز نوشته ارسال می‌کند. مخاطب نیز به‌محض دریافت، آن را رمزگشایی و به متن اصلی تبدیل می کند. اگر فرد دیگری بخواهد به‌طور غیرمجاز به آن پیام دسترسی پیدا کند، یا باید از طریق فرایند رمزنگاری و تجزیه‌وتحلیل محتوای رمز نوشته و یا با تحصیل کلید رمزگشای مرتبط به هدفش برسد. همان‌طور که ملاحظه می‌شود، ماهیت اصلی این فرایند همانند ناشناس کننده‌هاست. با این تفاوت که به‌جای اطلاعات هویتی، محتوای ارتباطات را نامفهوم می‌کند (خرم‌آبادی، ۱۳۹۴: ۱۲۱).

۴،۶. تدابیر سالب 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 داده‌های غیرمجاز جلوگیری می‌کنند، اما بعضی دیگر عملی دوسویه دارند و علاوه بر ورودی‌ها، خروجی‌ها را هم تحت کنترل دارند. با توجه به موقعیت و مبنای عمل فیلترها، می‌توان برای آن‌ها تقسیماتی قائل شد که به دلیل اهمیت موضوع به آن‌ها اشاره می شود:

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

۲- فیلتر از سوی ارائه‌دهندگان خدمات دسترسی حضوری (کافی‌نت) یا ارائه‌دهندگان خدمات اینترنتی(ISP): کمتر اتفاق می‌افتد کسی بر روی سیستم کامپیوتری خود فیلتر نصب کند و غالباً ارائه‌دهندگان خدمات دسترسی کاربران را از دسترسی به سایت‌ها محروم می‌کنند. کاربر مجبور است برای برقراری ارتباط شبکه‌ای به یک ارائه‌دهنده خدمات دسترسی مراجعه کند یا از منزل و محل کار خود با یک ISP ارتباط برقرار کند. به‌این‌ترتیب این دو مرجع می‌توانند با نصب فیلتر از دسترسی وی جلوگیری کنند

۳- فیلتر از سوی سرور: این نوع فیلترها در مؤسسات یا نهادها کارایی دارند و معمولاً بر روی سیستم کامپیوتری نصب می‌شوند که امکان دسترسی شبکه‌ای را برای کامپیوترهای واقع در مجموعه خود فراهم می‌آورند.

۴- فیلتر از سوی ایجادکننده نقطه تماس بین‌المللی: این مراکز شاهراه اصلی برقراری ارتباطات شبکه‌ای داخل با خارج محسوب می‌شوند که بدیهی است بهترین نقطه برای نصب و اجرای انواع فیلترینگ هم هستند.

۵- فیلتر بر روی موتور جستجو: این طبقه بخش خاصی از فیلتر از سوی سرور را شامل می‌شود و بر روی موتورهای جستجو بزرگی نظیر گوگل یا آلتاویستا قرار می‌گیرد. بر روی موتورها گزینه‌ای به نام (safe search) وجود دارد که به کاربر امکان می‌دهد جستجو تصفیه‌شده‌ای به عمل آورد درباره مبنا عمل فیلترینگ به‌ویژه ازلحاظ نحوه فهرست برداری از موضوعات به‌اصطلاح سفید یا سیاه، نکات جالب‌توجه پیشگیرانه‌ای مطرح است که تحلیل و بررسی آن‌ها خارج از بحث پیش رو است؛ بنابراین پلیس می‌تواند ضمن معرفی این فیلترها کاربران را تشویق به دریافت و نصب آن‌ها کند و موجب پیشگیری از وقوع جرائم سایبر شود.

۷. آسیب‌شناسی تدابیر فنی پیشگیرانه وضعی در جرائم سایبری

۱،۷. کمبود تجهیزات و امکانات پلیس

شاید اگر به گوییم وسایل، امکانات و تجهیزاتی که می‌بایست در اختیار پلیس به‌خصوص آن دسته از کارکنان نیروی انتظامی که مستقیماً در سطح شهر با مردم در تماس هستند، به گشت زنی مشغول‌اند و از وقوع جرائم پیشگیری می‌کنند، قرار گیرد. بسیار کمتر از میزان ایدئال و مطلوب است که پلیس پیشگیری بایستی به آن‌ها مجهز باشد بر اساس واقعیات موجود اظهارنظر کرده‌ایم البته ممکن است وسایل و امکاناتی که در رده‌های فرماندهی و مدیریت مورداستفاده قرار می‌گیرد مجهز و سالم و مرتب باشد از قبیل اتومبیل‌های فرم و نیز ساختمان‌ها، میزها، بی‌سیم‌ها و تلفن مانند آن اما این امکانات در رده‌های پایین سازمان بخصوص کلانتری‌ها و پاسگاه‌ها که عمدتاً به‌عنوان پیشگیری‌کننده از جرائم و بزهکاری محسوب می‌شوند، موجود نیست (گرکی، ۱۳۸۹: ۲۶۵). هم‌چنین لازم به ذکر است با توجه به پیشرفت روزافزون در حوزه اینترنت و تدابیری که مجرمان سایبری به کار می‌برند پلیس نیز باید از امکانات و ابزارهای لازم برای مقابله با جرائم سایبری و پیشگیری از آن برخوردار باشد این در حالی است که پلیس از امکانات لازم برخوردار نیست و این چالش بزرگی در پیشگیری از این جرائم است.

۲،۷. عدم تخصص کافی مراجع قضایی و انتظامی

ازجمله چالش‌ها و خلأهای مهم موجود در این حوزه، نداشتن تخصص کافی مراجعی است که به تعقیب، کشف و رسیدگی ماهوی این جرائم می‌پردازند. عدم آشنایی بازرسان و قضات با رسانه‌های اطلاعاتی و ضعف آن‌ها در برخورد با مسائل فنی جرائم سایبری عاملی است برای تشدید هر چه بیشتر مشکلات موجود. البته با عنایت با ماهیت نوین این جرائم، این مسأله چندان تعجب‌آور نیست. بسیاری از اقدامات و تلاش‌های صورت گرفته در بسیاری از کشورهای فاقد ساختار کیفری مناسب فضای سایبر، برای تعقیب مجرمان متوقف‌شده و شکایات بسیاری در این زمینه رد شده و احکام بسیاری صرفاً در خصوص جنبه‌های حقوقی دعاوی صادرشده است که همه این امور بیانگر عدم تمایل مجریان قانون به‌مواجهه با مشکلات خاص پرونده‌های مطرح‌شده است، این مسأله باعث می‌شود که تعقیب و کشف این جرائم با مشکل مواجه شود و دادگاه‌ها نیز نتوانند به نحو شایسته به جرائم مزبور رسیدگی نمایند (طهماسبی و شاهمرادی، ۱۳۹۷: ۱۰۶).

جرائم سایبری آن‌گونه که از نام آن‌ها برمی‌آید، در فضای سایبری روی می‌دهند و برخلاف جرائم سنتی، به‌جای آنکه شواهد حاصل از آن در بستر مادی، فیزیکی و ملموس باشند، دیجیتالی، شکننده و پیچیده می‌باشند. پیچیدگی آن‌ها ازاین‌جهت است که رمزگشایی از این دلایل به‌مراتب بیش از سایر جرائم به تخصص، آموزش و مهارت نیازمند است. همچنین شکننده‌اند چون تعلل و تساهل مأمورین تحقیق در ضبط، نمونه‌برداری و نگاهداری آن‌ها ممکن است برای همیشه آنان را از شناسایی بزهکار مأیوس سازد (تراب زاده، ۱۳۸۸: ۷). زیرا دلایل دیجیتالی می‌تواند توسط مرتکبان به‌انحاءمختلف به‌سرعت از بین رود. از همین رو است که قانون‌گذار در موارد اضطراری یعنی مواقعی که داده‌ها را خطر آسیب، تغییر، دست‌کاری و از بین رفتن تهدید می‌کند، حفاظت فوری از این شواهد را حتی بدون دستور مقام قضایی مجاز دانسته و برای مستنکف مجازات تعیین نموده است (طهماسبی و شاهمرادی، ۱۳۹۷: ۱۰۷). در این رابطه لازم به ذکر است به‌ویژه در ایران ضابطان از تخصص و دانش کافی در رابطه با جرائم سایبری برخوردار نیستند بلکه به‌نوعی همان پلیس‌های معمولی

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

هستند و ممکن است دوره‌های کوتاه‌مدت در رابطه با جرائم سایبری و فضای سایبری را دیده باشند، لذا عدم تخصص ضابطان قضایی و پلیس فتا نیز یکی از چالش‌ها در رابطه با پیشگیری وضعی از جرائم مذکور است.

۸. چالش‌های حقوق بشری پیشگیری وضعی از جرائم سایبری

پیشگیری وضعی، درواقع، تغییر سبک زندگی، کار و حضور اجتماعی افراد، تغییر ساعات فعالیت روزانه، صرف‌نظر کردن از برخی علاقه‌ها و آرزوها را می‌طلبد؛ یعنی صرف‌نظر کردن افراد از برخی حقوق و آزادی‌هایشان که تحت تأثیر تدابیر وضعی، محدود و یا حتی از میان می‌روند؛ تدابیری که می‌توانند هرگونه تحرک و یا حتی هر نوع اندیشه‌ای را با تجهیزات قوی نظارتی الکترونیکی و پیشرفته شناسایی و کنترل کنند (نجفی ابرندآبادی، ۱۳۸۸: ۵۸۲). به‌عبارت‌دیگر، پیشگیری وضعی مستلزم اقدامات و تدابیری است که خلوت افراد و زندگی انسان‌ها را تحت‌الشعاع خود قرار می‌دهد. بدین ترتیب، پیشگیری وضعی خطر تجاوز به حریم خصوصی و خلوت افراد را که موردحمایت ماده ۱۲ اعلامیه جهانی حقوق بشر[۴] و ماده ۱۷-۱ میثاق بین‌المللی حقوق مدنی و سیاسی است، به دنبال داشته و ممکن است آثار نامطلوبی برای حقوق و آزادی‌های افراد به بار آورد. اندیشه رعایت حقوق بشر قدمتی به درازای تمدن انسانی دارد؛ اندیشه‌ای که پس از جنگ جهانی دوم به اوج خود رسید؛ حکومت‌ها نیز در تلاش‌اند با منطبق کردن اقدامات خود، از مقررات حقوق بشری تبعیت نمایند. این مسأله در مواردی که حقوق افراد در میان باشد، نمود بیشتری می‌یابد. به شرح آتی محدودیت‌های حقوق بشری اجرای تدابیر پیشگیرانه وضعی بررسی می‌شود (توکلی، ۱۳۹۹: ۳۲).

۱.۸. حریم خصوصی و چالش‌های نظارت

ارتباط تنگاتنگی جرائم سایبری با استفاده از اطلاعات شخصی و محرمانه، حریم خصوصی اشخاص، به‌طور مستقیم و غیرمستقیم، آماج فعالیت‌های غیرقانونی قرار می‌گیرد؛ بنابراین، اتخاذ راهکارهای پیشگیرانه مؤثر و روزآمد در این راستا از مهم‌ترین پیش‌نیازهای توسعه در جامعه اطلاعاتی است. اگرچه فناوری اطلاعات، معمولاً یکی از عمده‌ترین دلایل نقض حریم خصوصی تلقی می‌گردد، راه‌های گوناگونی نیز وجود دارد که از طریق آن‌ها این فناوری، خود قادر به حمایت از محرمانگی و پیشگیری از نقض آن است. امروزه رهنمودها و شیوه‌های محافظت از حریم خصوصی که به روش‌های علمی طراحی‌شده‌اند مورداستفاده قرار می‌گیرند. این امکانات، طیف وسیعی از تمهیدات و راهکارها از روش‌شناسی‌های طراحی‌شده بر مبنای اطلاع‌رسانی اخلاقی تا رمزنگاری به‌منظور محافظت از اطلاعات شخصی در مقابل استفاده غیرمجاز را در برمی‌گیرد (محسنی، ۱۳۹۵: ۹۳).

اجرای تدابیر پیشگیرانه وضعی، همانند بسیاری از سایر تدابیر پیشگیرانه، ممکن است محدودیت‌هایی ایجاد کند. ازاین‌رو، هدف پیشگیری، نمی‌تواند کاربرد هر وسیله، فن، اقدام و روش‌های خاص فراقانونی شود (نجفی ابرندآبادی، ۱۳۸۲: ۵۶۷). در بند دوم و سوم اصل ۲۶ رهنمود پیشگیری از جرم سازمان ملل متحد سال ۲۰۰۲ به بهره‌گیری از تدابیر پیشگیری وضعی که به قابلیت و بدنه محیط اجتماعی لطمه وارد نکند و دسترسی آزاد به مکان‌های عمومی را محدود ننماید، تأکید شده است. در ارتباط با بند ۱ لازم به توضیح است که ازنظر فنی و تخصصی، ممکن است با کاربرد تدابیر پیشگیری وضعی در فضای سایبری، شاهد برخی اختلالات همچون کاهش سرعت شبکه، بسته شدن اشتباهی برخی از سایت‌ها و وبلاگ‌ها به جهت پالایه، محدودیت‌های بی‌جهت برای ورود به برخی فضاها، اعمال محدودیت در دسترسی به شبکه‌های بین‌المللی و غیره بود. نتیجه اعمال این شرط رهنمود، بهره‌گیری از رویکردی سنجیده و ملایم‌تر نسبت به ممنوعیت

[۴] احدی نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه و مکاتبات خود مورد مداخله‌های خودسرانه واقع‌شده و شرافت و آبرویش مورد تعرض قرار گیرد.

دانشگاه آزاد اسلامی واحد مراغه

کامل شبکه‌های اجتماعی مجازی، مسئله پالایه و افزایش دقت و هوشمندی سامانه‌های پالایه است. بند ۲ این رهنمود نیز با تفویض تصمیم‌گیری به سازمان‌ها، نهادها یا اشخاصی که صلاحیت قانونی چنین امری را دارند یا بر روند و نحوه اجرا این‌گونه تدابیر نظارت مستقیمی دارند قابل‌اجرا است (محسنی و صوفی زمرد، ۱۳۹۶: ۱۷۳). لذا مباحث حقوق بشری یکی از موانع پیش روی پیشگیری از جرائم سایبری است که از مهم‌ترین آن‌ها می‌توان به آزادی اطلاعات، حریم خصوصی و اصل براعت و... اشاره کرد.

۲،۸. فیلترینگ به‌مثابه ابزار سانسور

باید اذعان داشت پالایش محتوا در ایران، دسترسی آزاد به اطلاعات را با مخاطرات جدی مواجه ساخته است. رصد و فرا تحلیل گزارش‌ها و پژوهش‌های مختلف داخلی و خارجی حکایت از پایمال شدن این شعبه از حق آزادی دارد. قطع‌نظر از محتواهای منافی عفت و مستقیم مجرمانه نظیر تارنماهای اشاعه خشونت، نفرت و خریدوفروش مواد مخدر و برخی موارد این‌چنینی که پالایش فضای مجازی از آن‌ها مورد وفاق نسبی جامعه است، برخی شبکه‌های اجتماعی محبوب نظیر فیس‌بوک و تلگرام و ابزارهای نمایشگر عمومی مانند یوتیوب در ایران مسدود و بدون استفاده از ابزارهای فیلترشکن غیرقابل‌دسترس هستند (سلیمی، ۱۳۹۷: ۸۳). همان‌طوری که قبلاً گفته شد فیلترینگ یا محدود کردن دسترسی یکی از راهکارهای پیشگیری وضعی در پیشگیری از جرائم سایبری است و از طرفی فیلترینگ نیز ضد حقوق بشری به‌مثابه جلوگیری از دسترسی به اطلاعات و به عبارتی سانسور بر فضای مجازی است که این مساله پیشگیری وضعی از جرائم سایبری را با مانع مواجه می‌کند.

نتیجه‌گیری

جرائم سایبری ازجمله جرائم است که در دهه‌های گذشته با ظهور اینترنت و گسترش استفاده از فناوری اطلاعات پا به عرصه ظهور گذاشته و به دلیل ماهیت خاص و ارتکاب آن در فضای سایبری و با توجه به پیچیدگی‌های مسیر کشف جرم لازم است که از فناوری‌ها و راهکارهای نوین و به عبارتی راهکارهای متفاوت از جرائم سنتی در کشف و تعقیب مجرمان سایبری بکار گرفته شود، به عبارتی باید راهکارهای پیشگیرانه به راهکارهای سرکوبگرانه و تعقیب اولویت داده شود، لذا در این راستا در پژوهش حاضر نقش پیشگیری وضعی در پیشگیری از جرائم سایبری، چالش‌ها و مشکلات پیش روی آن بررسی‌شده است. بر اساس نتایج تحقیق؛ تدابیر محدودکننده یا سلب‌کننده دسترسی که از ورود و ارسال داده‌های غیرمجاز یا غیرقانونی جلوگیری می‌کنند که به‌نوعی موارد را به مجاز و غیرمجاز تقسیم‌بندی و بعد آن اجازه دسترسی می‌دهند و هم‌چنین تدابیر نظارتی که موارد و سوابق مشکوک را موردبررسی قرار می‌دهد ازجمله تدابیر پیشگیری وضعی هستند، تدابیر صدور مجوز از دیگر تدابیر پیشگیری وضعی از جرائم سایبری است که بر اساس معیارهای خاص مانند به استفاده از پسورد و... از ورود و دسترسی مجرمان سایبری جلوگیری می‌کند، ابزارهای ناشناس کننده و رمزگذاری نیز از دستبرد تبهکاران سایبری به داده‌ها و وقوع جرائم سایبری جلوگیری می‌کنند، هرچند امکان سوءاستفاده از این ابزارها در جهت ارتکاب جرائم نیز وجود دارد. اقدامات پیشگیرانه وضعی پلیس در جرائم سایبری مرتبط با فضای مجازی شامل؛ گشت اینترنتی و رصد فضای سایبری برای شناسایی موارد مشکوک و پیشگیری از جرائم احتمالی، آموزش همگانی برای افزایش آگاهی شهروندان از فضای سایبری و جرائم سایبری از طریق رسانه‌های مختلف و راهکارهای نوین از دیگر اقدامات پلیس در این رابطه است، یکی دیگر از اقدامات پلیس در این رابطه شناسایی و کنترل افراد خطرساز است. از اقدامات پیشگیرانه وضعی از جرائم با رویکرد حقوقی و جرم شناختی می‌توان به برهم زدن معادله جرم در فضای سایبری با افزایش خطر ارتکاب جرم که سبب دشواری ارتکاب جرم، افزایش خطر جرم، کاهش منافع، کاهش تحریک‌پذیری و حذف بهانه‌ها می‌شود، افزایش خطرات ملموس ارتکاب جرم از دیگر راهکارهای وضعی پیشگیری از جرائم سایبری

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره سوم | پاییز ۱۴۰۲

است که با افزایش خطر ناشی از ارتکاب جرائم سایبری سبب انصراف از جرائم احتمالی می‌شود، افزایش محافظت‌ها و مراقبت‌ها در فضای سایبری نیز سبب پیشگیری از جرائم سایبری و به عبارتی پایین آوردن احتمال و راه‌های ارتکاب این جرائم می‌شود.

تدابیر فنی در پیشگیری وضعی از جرائم سایبری نیز نقش اساسی دارند، ازجمله این تدابیر حفاظت فیزیکی است که به‌کارگیری قفل‌ها، نگهبان‌ها، علائم و ابزارهای مشابه برای کنترل دسترسی به رایانه و تجهیزات مربوط به آن از جرائم سایبری پیشگیری می‌نمایید، از دیگر تدابیر فنی می‌توان به؛ کنترل فنی، کنترل مدیریتی، توسعه محافظت‌ها، فیلترینگ اشاره کرد. از سایر تدابیر و اقدامات حقوقی و جرم شناختی در پیشگیری وضعی از جرائم سایبری می‌توان به تدابیر و اقدامات مبتنی بر خانواده، راهبردهای کاهنده آثار نامطلوب، تبیین و نهادینه‌سازی فرهنگ استفاده صحیح از فضای سایبر، افزایش میزان تلاش برای ارتکاب جرم، تغییر مسیر بزهکاران، کاهش عوامل محرک، انگیزه زدایی اشاره کرد. تدابیر آموزشی و آگاهی سازی نیز در پیشگیری وضعی از جرائم سایبری نقش اساسی دارند، با اعلان جرم بودن یک عمل در فضای سایبری و اطلاع‌رسانی نسبت به آن و اعلام میزان مجازات اعمال ارتکابی می‌توان تا حد زیادی از ارتکاب جرائم دنیای سایبر، پیشگیری نمود؛ که در این راستا می‌توان از امکانات ارتباطی مختلف، رسانه‌ها و... استفاده کرد. همان‌طور که قبلاً اشاره شد تدابیر مختلف پیشگیری وضعی در پیشگیری و جلوگیری از ارتکاب جرائم احتمالی سایبری نقش اساسی دارند، ولی این به معنای انکار چالش‌ها، خلأها و آسیب‌های تدابیر پیشگیری وضعی نیست لذا باید با شناسایی و آسیب‌شناسی موانع و چالش‌های پیشگیری وضعی در حد امکان در رفع و مرتفع کردن آن‌ها تلاش کرد. یکی از چالش‌های اساسی در رابطه با ماهیت فضای سایبری است چراکه علاوه بر اینکه با کثرت محتواهای مجرمانه در فضاهای عمومی سایبر مواجه هستیم، فراملی بودن جرائم سایبری از دیگر چالش‌های اساسی پیش روی پیشگیری وضعی از جرائم سایبری است. علاوه بر ساختار خاص فضای سایبر، وجود برخی ابزارها و امکانات خاص نیز پیشگیری از جرم را با دشواری مواجه ساخته است. کمبود تجهیزات و امکانات پلیس، عدم تخصص کافی مراجع قضایی و انتظامی و... از دیگر چالش‌ها در این حوزه است. برخی از موانع و چالش‌ها مرتبط با خود تدابیر پیشگیری وضعی به دلیل؛ موقتی بودن پیشگیری وضعی، مقابله محافظه‌کارانه با جرم، فرصت مدار بودن، عدم شمول همه آماج‌ها، جابه‌جایی جرم، عدم شفافیت برخی عبارات قانونی، افزایش احتمال بزه دیدگی و رقم سیاه جرائم سایبری، زمان‌بر بودن و ایراد اقتصادی تدابیر پیشگیری وضعی است.

پیشنهاد

آنچه در کشور ما در زمینه پیشگیری از جرم و بزه‌کاری محسوس است، عدم وجود یک‌نهاد ویژه و مردمی منسجم و مسئول در قلمرو مشارکت مردمی است که توانایی سازمان دادن به این مشارکت و هماهنگی با نهادهای دولتی و تحقیق و تفحص در این زمینه را داشته باشد. امروزه وقوع جرائم و نحوه ارتکاب آن توسط مرتکبین، شکل جدیدی به خود گرفته‌اند که همین امر سبب شده که بررسی‌های دقیق و کارشناسانه‌ای صورت گیرد تا همسو با وقوع این جرائم پیشگیری‌های صحیح و منطقی صورت گیرد؛ بنابراین به‌عنوان یک راه‌حل اساسی برای این موضوع پیشنهاد می‌گردد اقدام به تأسیس نهادی تحت عنوان (سازمان ملی پیشگیری از وقوع جرائم سایبری) گردد؛ که هیئت‌رئیسه آن از جرم‌شناسان، روان‌شناسان و جامعه‌شناسان انتخاب شوند و هر سه قوه (مقننه، قضائیه، مجریه) عضو هیئت‌رئیسه باشند، به‌طوری‌که این نهاد جهت جلوگیری از هرگونه تعارض به‌صورت اشتراکی به‌وسیله نمایندگان دولت و مردم اداره گردد.

دانشگاه آزاد اسلامی واحد مراغه

منابع

- ابراهیمی، شهرام. (۱۳۹۱). جرم‌شناسی پیشگیری، چاپ دوم، تهران: انتشارات میزان.

– اسلامی، ابراهیم. (۱۳۹۵). «جایگاه حمایت از بزه دیدگان جرائم سایبری در مقررات کیفری حقوق داخلی و حقوق بین‌الملل»، پژوهشنامه حقوق اسلامی، دوره ۱، شماره ۴۳.

– امیریان فارسانی، امین، مالمیر، محمود، اشرافی، محمود و حیدری، مسعود. (۱۳۹۶). «کارکردهای نظری و عملی پلیس فتا در پیشگیری از جرائم سایبری و موانع حاکم بر آن». تحقیقات حقوقی بین‌المللی، دوره ۱۰، شماره ۳۵.

– بابایی، محمدعلی و نجیبیان، علی. (۱۳۹۰). «چالش‌های پیشگیری وضعی از جرم»، مجله حقوقی دادگستری، دوره ۷، شماره ۷۵.

– بیات، بهرام، شرافتی، جعفر و عبدی، نرگس. (۱۳۸۷). «پیشگیری از جرم با تکیه بر رویکرد اجتماع‌محور»، چاپ اول، تهران: انتشارات معاونت اجتماعی ناجا.

– توکلی، فخرالدین و مرتضوی، سید مرتضی. (۱۳۹۹). «تعیین عوامل تأثیرگذار در کشف جرائم سایبری با رویکرد دلفی فازی». فصل‌نامه کارآگاه، دوره ۱۳، شماره ۵۰.

– حیدری نژاد، نصر اله. (۱۳۹۷). «پیشگیری وضعی در جرائم سایبری از منظر حقوق کیفری ایران و جهان». فصل‌نامه قانون یار، دوره ۲، شماره ۶.

– داوری، بهاره. (۱۴۰۰)، «راهکارهای پیشگیری وضعی از جرائم سایبری علیه خانواده متأثر از اینستاگرام»، پایان‌نامه جهت دریافت درجه کارشناسی ارشد، دانشگاه شهید اشرفی اصفهانی.

– دهخدا، علی‌اکبر. (۱۳۷۷)، لغت‌نامه دهخدا، چاپ دوم، جلد ۲، تهران، انتشارات دانشگاه تهران.

– سلیمی، احسان. (۱۳۹۷)، آسیب‌شناسی پیشگیری از جرائم سایبری در ایران، رساله جهت دریافت درجه دکترا، دانشگاه قم.

– عالی پور، حسن. (۱۳۹۰). امنیت سایبری در چشم‌انداز ۱۴۰۴، مجموعه مقالات همایش دفاع سایبری

– فهیمی، مهدی. (۱۳۸۰). «جرائم رایانه‌ای و روش‌های مقابله و پیشگیری از آن»، فصل‌نامه دیدگاه‌های حقوقی، دوره ۱۰، شماره ۲۴.

– کوهساری، ابوالفضل. (۱۳۹۹). جرائم سایبری در حقوق ایران و شیوه‌های پیشگیری از آن با تأکید بر رویه قضایی، پایان‌نامه جهت دریافت درجه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد شاهرود.

– گرکی، مارکو. (۱۳۸۹). جرائم سایبری راهنمایی برای کشورهای درحال‌توسعه، ترجمه: مرتضی اکبری، چاپ اول، تهران، انتشارات پلیس فضای تولید و تبادل اطلاعات ناجا (فتا).

– گیدنز، آنتونی. (۱۳۷۸). جامعه‌شناسی، منوچهر صبوری کاشانی، چاپ ۲، تهران: انتشارات نی.

– محسنی، فرید و صوفی زمرد، محسن. (۱۳۹۶). پلیس و چالش‌های اجرایی تأمین امنیت سایبری، فصل‌نامه پژوهش‌های دانش انتظامی، دوره ۴، شماره ۲۰.

– معین، محمد. (۱۳۸۶). فرهنگ معین (یک‌جلدی)، جلد ۳، تهران: انتشارات زرین.

– نجفی ابرندآبادی، علی حسین. (۱۳۹۶). علوم جنایی (مجموعه مقالات در تجلیل از استاد آشوری)، چاپ هفتم، تهران: انتشارات سمت.

– نجفی ابرندآبادی، علی حسین. (۱۳۹۵). درآمدی بر سیاست جنایی مدیریتی خطر مدار، کیفرشناسی نو جرم‌شناسی نو، چاپ اول، تهران: انتشارات تازه‌های علوم جنایی.