Culminatin of Law Quarterly
16th Year, No. 1, Spring 2025
http://dx.doi.org/10.22034/thdad.2023.1990495.2385

Legal-Criminological Investigation of Cyber Stalking and Offline Stalking

Seyedeh Saedeh Hosseini[1*], Seyed Hossein Hosseini[2], Zahra Salehabadi[3]

1. PhD in Criminal Law and Criminology, Faculty of Law, Ferdowsi University, Mashhad, Iran.
2. Associate Professor of Criminal Law and Criminology, Faculty of Law, Ferdowsi University, Mashhad, Iran.
3. PhD in Criminal Law and Criminology, Ferdowsi University, Mashhad, Iran.

Article Type:
Original Research

Pages: 3-36

Received: 2023 February 26

Revised: 2023 April 21

Accepted: 2023 July 13

Abstract

The growth and development of cyberspace, while providing an opportunity to enhance the standard of living of human beings, has also provided new tools for engaging in illegal and immoral activities that violate human rights, including the right to security and the right to privacy. Cyber stalking as a repetition and continuation of threatening behavior that causes psychological, emotional, and sometimes physical harm to the victim is one of the most important crimes in the cyberspace, which has many similarities with its traditional type from the point of view of general principles, and the only special feature of cyber stalking is the use of new technology to commit a crime. In fact, committing this crime in the cyber space has made cyber stalking a more anti-social act and the methods of discovering and proving it are more difficult. Therefore, in order to prevent the irreparable effects of this crime, criminal policymakers have always sought to take appropriate and effective measures to prevent the victims of these crimes and in this regard have been inspired by theories of daily activities and lifestyle. The prevailing view of these theories is that the victimization of individuals is not accidental; Rather, individuals often expose themselves to motivated criminals as an attractive target by engaging in deviant behaviors, thereby facilitating their victimization. In this regard, it is necessary to protect the potential victims of these crimes by identifying the risk factors on the one hand and on the other hand by adopting security and support measures and reduce the possibility of their victimization.

Keywords: Cyber stalking, Offline stalking, Cyber space, Cybercrime, Privacy

* Corresponding Author: saede.hoseini@yahoo.com

فصلنامه تعالی حقوق

سال شانزدهم، شماره ۱، بهار ۱۴۰۴

http://dx.doi.org/10.22034/thdad.2023.1990495.2385

بررسی حقوقی- جرم‌شناختی کمین سایبری و سنتی

سیده ساعده حسینی[۱*]، سیدحسین حسینی[۲]، زهرا صالح آبادی[۳]

۱. دانش‌آموخته دکتری حقوق جزا و جرم شناسی، دانشکده حقوق، دانشگاه فردوسی، مشهد، ایران.

۲. دانشیار حقوق جزا و جرم شناسی، دانشکده حقوق، دانشگاه فردوسی، مشهد، ایران.

۳. دانش‌آموخته، دکتری حقوق جزا و جرم شناسی، دانشگاه فردوسی، مشهد، ایران.

نوع مقاله: علمی پژوهشی

صفحات: ۳۶-۳

تاریخ دریافت: ۱۴۰۱/۱۲/۰۷

تاریخ بازنگری: ۱۴۰۲/۰۲/۰۱

تاریخ پذیرش: ۱۴۰۲/۰۴/۲۲

چکیده

رشد و توسعه فناوری اطلاعات و ارتباطات ضمن اینکه فرصتی را برای ارتقاء سطح زندگی بشر ایجاد کرده است؛ ابزارهای نوینی را برای انجام فعالیت‌های غیرقانونی و غیراخلاقی در جهت نقض حقوق بشری افراد از جمله حق امنیت و حق برحریم خصوصی نیز فراهم نموده است. کمین سایبری به عنوان تکرار و تداوم رفتار تهدیدآمیز و آزاردهنده که موجب آسیب روانی، عاطفی و حتی‌گاه آسیب فیزیکی برقربانی می‌گردد؛ یکی از مهم‌ترین جرایم در فضای سایبر است که از منظر اصول عمومی با نوع سنتی خود مشابهت‌های زیادی دارد و تنها ویژگی خاص کمین سایبری استفاده از تکنولوژی جدید برای ارتکاب جرم است. در حقیقت، ارتکاب این جرم در فضای سایبر، موجب شده که کمین سایبری عملی ضداجتماعی‌تر و طرق کشف و اثبات آن مشکل‌تر باشد. به همین جهت، سیاست‌گذاران جنایی به منظور پیشگیری از اثرات جبران ناپذیر این جرم، همواره به دنبال اتخاذ تدابیر مناسب و مؤثر برای پیشگیری از بزه‌دیدگی افراد بوده و در این خصوص از نظریات فعالیت‌های روزانه و شیوه زندگی الهام گرفته‌اند. تفکر حاکم بر این نظریات آن است که بزه‌دیدگی امری تصادفی نیست؛ بلکه غالبا افراد با انجام رفتارهای منحرفانه و خطرناک، خود را به عنوان یک هدف جذاب در معرض مجرمان با انگیزه قرار می‌دهند و از این طریق بزه‌دیدگی خود را تسهیل می‌نمایند. دراین راستا، باید از یک سو با شناسایی عوامل خطر و از سوی دیگر با اتخاذ تدابیر امنیتی و حمایتی، از قربانیان بالقوه این جرایم محافظت نموده و امکان بزه‌دیدگی آنان را کاهش داد.

واژگان کلیدی: کمین سایبری، کمین سنتی، فضای سایبر، پیشگیری، حریم خصوصی

* نویسنده مسئول: saede.hoseini@yahoo.com

درآمد

فضای سایبر به عنوان ره‌آورد قرن حاضر، تغییرات بی‌سابقه‌ای در زندگی روزمره انسان‌ها ایجاد کرده است. این فناوری عالی که در ابتدا برای آرامش و آسایش مردم مورد استفاده قرار می‌گرفت، به تدریج تبدیل به ابزاری برای رسیدن به آرزوهای جنایتکارانه شده و مجرمان به موازات توسعه و گسترش فضای مجازی، فعالیت‌های جنایی خود را به فضای گمنام مجازی منتقل کردند و اینترنت را پناهگاهی ناشناس برای اقدامات خود قرار دادند.

کمین سایبری[1] و کمین سنتی[2] از دسته جرایمی هستند که با انگیزه اعمال کنترل بر قربانی؛ حریم خصوصی، امنیت و آزادی افراد را به عنوان مهم‌ترین حقوق بشری افراد که در اسناد بین‌المللی همواره مورد تاکید قرارگرفته‌اند، مورد تعرض قرار می‌دهند. انجام این عمل در فضای سنتی یا فیزیکی به علت حضور شهروندان، نیروهای انتظامی و امکان شناسایی مجرمان با موانع و محدودیت هایی روبه رو می‌باشد. به همین جهت، حجم جرایم ارتکابی کمتر و احتمال کشف و پیشگیری از تکرار جرایم و در نتیجه کاهش احتمال بزه‌دیگی بیشتر است(Reyns،۹،۲۰۱۰). اما همگام با گسترش فناوری اطلاعات و ارتباطات امروزه فضای سایبر عمده فعالیت‌های روزانه افراد را تحت تاثیر قرار داده و به ابزاری جدید برای دستیابی مجرمان به آرمان‌های جنایتکارانه‌شان تبدیل شده است. در حقیقت، بسیاری از مزایا و ویژگی‌های فضای سایبر از قبیل هزینه پایین، سهولت و سرعت ارتباطات و طبیعت گمنام، فضای مجازی را به پناهگاهی امن برای مجرمین تبدیل کرده و فرصت‌های مجرمانه جدیدی را برای آنها به وجود آورده است که در آن مجرمین با احتمال کمتری از شناسایی، دستگیری و مجازات، افراد بیشتری را مورد هدف قرار داده و نسبت به دنیای فیزیکی خسارات بیشتری را بر پیکر امنیت و آسایش جامعه

---

1. Cyber stalking
2. Offline stalking

وارد می‌کنند(Ashcroft،۱،۲۰۰۱).

جرم کمین سنتی نیز از این تغییر و تحولات فضای مجازی مصون نمانده است و مرتکبین جرایم فوق که اغلب اختلالات شخصیتی دارند، حوزه فعالیت‌های خود را از فضای سنتی به فضای مجازی منتقل کرده و همین امر باعث گسترش حجم جرایم کمین سایبری و در نتیجه افزایش تعداد قربانیان این جرم همزمان با کاهش امکان شناسایی و مجازات مرتکبین شده است(Halder،۱۰۹،۲۰۱۵). این مسئله موضوعات جدیدی را پیش‌روی جرم شناسی و عدالت کیفری قرار داده است. زیرا فضای مجازی طیف گسترده‌ای از فرصت‌ها را برای تعامل افراد فراهم کرده است که در غیر این صورت ممکن است هرگز با آنها روبرو نشوند.

اگر چه در خصوص ماهیت جرایم مذکور در ادبیات انگلیسی تحقیقات زیادی صورت گرفته است؛ اما ادبیات فارسی در این خصوص ضعیف می‌باشد و همین امر موجب شده که این جرایم تا حدودی ناشناخته باقی بمانند و در حقوق ایران نیز مورد جرم‌انگاری مقنن قرار نگیرد. این در حالی‌ست اتخاذ تدابیر پیشگیرانه برای مقابله با جرایم سایبری مستلزم به‌کارگیری راهبردهای مؤثر و جامع در این خصوص می‌باشد که این امر نیز نیازمند قانونگذاری خوب و اجرای موفق قانون می‌باشد. به همین جهت، مطالعه فرآیند ارتکاب جرایم فوق به جهت تشخیص و تفکیک آنها از یکدیگر با توجه به تفاوت‌هایی که از لحاظ آثار اجتماعی برآنها مترتب است؛ حائز اهمیت می‌باشد. این نوشتار برآن است که ابتدا از منظر حقوقی به بررسی ارکان تشکیل دهنده جرایم کمین سایبری و سنتی با یکدیگر بپردازد و سپس با رویکرد جرم‌شناختی نقاط اشتراک و افتراق ارکان تشکیل دهنده این جرایم و اتخاذ تدابیر جهت پیشگیری از جرم کمین سایبری را مورد بررسی قرار دهد.

۱- بررسی حقوقی کمین سایبری و سنتی

جرم کمین اعم از نوع سایبری یا سنتی آن پدیده‌ای ضداجتماعی می‌باشد که تهدیدی جدی برای آسایش افراد جامعه محسوب می‌شود. کمین سایبری، شکل نوینی ازکمین سنتی است که با استفاده از اینترنت یا سایر وسایل الکترونیکی، راه جدیدی از تعقیب و اذیت و آزار قربانی را برای مجرمین فراهم کرده است و همین استفاده از ابزار و تکنولوژی مدرن موجب تفاوت‌های میان این دو جرم گردیده که امکان اعمال قوانین و مقررات فضای سنتی بر آن را با مشکل مواجه نموده است.

۱-۱- مفهوم کمین سایبری و کمین سنتی

کمین سایبری به عنوان جرم رایانه‌ای فرهنگی که از آن تحت عنوان جرایم محتوا نیز یاد می‌شود، ارزش‌های فردی و اجتماعی افراد را مورد هدف قرار داده و موجب سلب اعتبار، آرامش و دارایی شخص اعم از حقوقی یا حقیقی می‌گردد. جرایم مرتبط با محتوا به جرایمی اطلاق می‌شودکه امکان ارتکاب آنها در محیط غیرمجازی نیز وجود دارد و رایانه و اینترنت صرفا به عنوان یک وسیله، ارتکاب جرم را برای وی در فضای مجازی تسهیل می‌نماید(علیوردی نیا و دیگران، ۱۳۹۱،ص۱۳۳). جرم مذکور، اشاره به رفتاری دارد که در آن مجرم به صورت مداوم با استفاده از اینترنت، ایمیل و دیگر وسایل الکترونیکی شخص و یا یک گروه را مورد اذیت و آزار قرار می‌دهد؛ به‌گونه‌ای که موجب می‌شود شخص متعارف و معقول نسبت به امنیت خود یا دیگر اعضای خانواده احساس ناامنی و ترس را داشته باشد (Fisher, ۹ :۲۰۱۲).

در واقع انجام این عمل در فضای سایبر به جهت خصوصیات و ویژگی‌هایی که بر فضای مجازی حاکم است به صورت‌های گوناگونی شکل می‌گیرد. در این جرم، مرتکب قربانی خود را غالبا از طریق ارسال ایمیل‌های ناخواسته‌ی زشت و ناپسند، آزار و اذیت از طریق چت روم‌های آنلاین، سوء استفاده کلامی آنلاین، سرقت هویت، ردیابی محل یک

شخص بدون اطلاع یا رضایت او، ارسال ویروس‌های الکترونیکی، انتشار فیلم و عکس خصوصی بدون رضایت آنها، افترا، تهمت، انتشار اطلاعات نادرست در خصوص افراد، اذیت و آزار جنسی و غیره مورد هدف قرار می‌دهد(Chandrashekhar,p۹۵:۲۰۱۶).

تحقیقات نشان می‌دهد که مجرمان کمین سایبری برای آزار و تهدید قربانیان از ایمیل بسیار بیشتر از هر وسیله الکترونیکی دیگری استفاده می‌کنند (Petrocelli ۲۰۰۵). زیرا ایمیل به مجرم این اجازه را می‌دهد تا بارها و بارها پیام‌های آزار دهنده، تهدید آمیز، نفرت‌انگیز یا نامفهوم، از جمله عکس، فیلم یا صدا را انتقال دهد. حتی در برخی موارد، مجرمان سایبر از آدرس ایمیل قربانی و سایر اطلاعات شخصی وی برای اشتراک یا خرید کتاب، مجله یا سایر خدمات اینترنتی بدون اطلاع و رضایت قربانی استفاده می کنند(Salimi،۴،۲۰۱۴).

این رفتار تهدیدآمیزکه به صورت مکرر انجام می‌پذیرد، عواقب روانی و اجتماعی جدی برای قربانی در پی خواهد داشت و بسیاری از جنبه‌های شیوه زندگی او را مختل می‌کند که نتیجه چنین رفتارهایی ایجاد استرس عاطفی و روانی برای قربانی و حتی گاه علی رغم عدم وجود تعامل مستقیم میان قربانی و مجرم، موجب صدمه جسمی بر وی نیز می‌باشد(Bocij،۲،۲۰۰۳). نتایج تحقیقات صورت گرفته در خصوص قربانیان این جرم نشان می‌دهد که انجام مکرر این رفتار باعث گرایش قربانیان به خصوص قربانیان نوجوان به خودکشی می‌گردد. زیرا غالبا در این جرم، مجرم اطلاعات قربانی را از طریق چت روم‌ها، کانال‌ها و شبکه‌های مجازی یا اجتماعی به دست می‌آورد و فعالیت‌های آنلاین او را با نصب نرم افزاری بر روی سیستم خود که می‌تواند آنها را از زمان آنلاین شدن قربانی آگاه کند؛ پیگیری کرده و با استفاده از اطلاعات شخصی به دست آمده از قربانیان، آنها را مورد اذیت و آزار قرار می دهند(sissinga ،p۱۹:۲۰۱۳).

به همین علت است که این جرم باعث نقض حقوق اساسی بشر از قبیل حق زندگی، آزادی و امنیت افراد شده و می‌تواند تداخل بسیار جدی با حق حریم خصوصی

آنها داشته باشد.(Vasiu ، p۲۲۹:۲۰۱۳). در فضای مجازی این حق بر حریم خصوصی بیانگر حق فرد در داشتن امنیت و محرمانه بودن کلیه اطلاعات و تعاملات اشخاص است که باید از هرگونه تعرض مصون باشد.(یزدانی زنوز،۱۳۸۸، ص۱۴۰). در ماده ۱۵ کنوانسیون جرایم سایبری نیز به ضرورت و اهمیت حفظ امنیت خصوصی افراد اشاره شده است. اما با این وجود، امکان نقض این حق در فضای سایبر با توجه به ویژگی‌ها و مزایای این محیط بیشتر از محیط فیزیکی می‌باشد. این در حالی ست که حق بر حریم خصوصی افراد از جمله مهم‌ترین جلوه‌های حقوق بشری افراد است که ضامن امنیت افراد در زندگی آنان اعم از محیط مجازی و فیزیکی می‌باشد و تعرض به آن پیامدهای جبران ناپذیری را بر زندگی افراد برجای می‌گذارد. زیرا کمین سایبری می‌تواند به صورت طولانی مدت اثرات روانی جسمی و حتی اقتصادی مخربی به همراه داشته باشد و بستری برای ارتکاب جرایم خشونت‌آمیز را نیز فراهم کند.

در مقابل جرم کمین سایبری، جرم کمین سنتی قرار دارد که شیوه ارتکاب آن نسبت به کمین سایبری متفاوت است. کمین سنتی رفتاری تهدیدآمیز وآزاردهنده می‌باشد که به صورت غیرطبیعی و طولانی مدت با هدف ارعاب وکنترل بر قربانی صورت می‌گیرد و باعث احساس ترس شخص معقول نسبت به امنیت جسمی و روحی خود و نزدیکانش می‌شود(Pittaro),p۱۸۲:۲۰۰۷. درواقع، هدف اصلی مجرم اعمال کنترل بر قربانی از طریق ایجاد ترس در وی می‌باشد. مصادیق این رفتار شامل مواردی از قبیل تماس‌ها و پیام‌های تلفنی تهدیدآمیز مکرر، تعقیب یک فرد در محل کار یا خانه او، ارسال نامه‌های تهدیدآمیز مکرر، خرابکاری اموال اشخاص، مزاحمت با چاقو یا سلاح‌های دیگر و غیره می‌باشد. همچنین این جرم برخلاف نوع سایبری آن نیازمند حضور و برخورد فیزیکی، چشمی، ارتباط کلامی یا گفتاری تهدیدآمیز اعم از ضمنی یا صریح بین مرتکب و قربانی می‌باشد(Paullet,p۲:۲۰۱۳). لذا، این نوع از مزاحمت به علت چهره علنی آن و احتمال حضور شهروندان و نیروی انتظامی نسبت به جرم کمین سایبری که در فضایی از

گمنامی‌ست، کمتر رخ می‌دهد.

به طورکلی جرم کمین اعم از سنتی و سایبری در سه سطح عمده تأثیراتی را برای قربانیان به همراه دارد: تأثیرات مرتبه اول، تأثیرات بر سلامت جسمی و عاطفی فرد (خشونت جسمی، جنسی ،ترس، اضطراب، شرم، ایده خودکشی، افسردگی، اختلالات خواب)می‌باشد. تأثیرات مرتبه دوم تأثیر بر سلامت اجتماعی قربانی (کاهش اعتماد، افزایش بیگانگی، انزوا و فعالیت‌های اجتماعی محدود)است و در نهایت تأثیرات مرتبه سوم تأثیر بر سلامت شناختی قربانیان (باورهای ناسازگار، سرزنش خود، ناسازگاری شخصیت) می‌باشد که در این میان تجربه مداوم این جرم، بیشترین تأثیر را بر سلامت روانی افراد بر جای می‌گذارد (Lynne ،۲۷۳،۲۰۰۸).

۲-۱- ارکان تشکیل دهنده جرم کمین سایبری و کمین سنتی

هر جرمی نیازمند عناصر اختصاصی قانونی، مادی و روانی می‌باشد که آن را از سایر جرایم متمایز می‌کند. جرایم کمین سایبری و کمین سنتی هم از این قاعده مستثنی نبوده و باید برای تحقق این جرایم، هر سه عنصر مذکور وجود داشته باشند. به همین جهت، در این قسمت ابتدا به بررسی مستندات قانونی مربوط به جرم‌انگاری کمین سنتی و سایبری و سپس به بررسی عناصر مادی و روانی جرایم فوق پرداخته می‌شود.

۱-۲- عنصر قانونی

براساس ماده ۲ قانون مجازات اسلامی ۱۳۹۲که بیانگر اصل قانونی بودن جرم و مجازات می‌باشد، زمانی می‌توان شخص را به اتهام ارتکاب جرم محکوم و سپس مجازات کرد که عمل او در قانون جرم‌انگاری و برای آن مجازات تعیین شده باشد. در خصوص جرم کمین سایبری در قانون جرایم رایانه‌ای جرمی با این ماهیت و تحت این عنوان پیش‌بینی نشده است که بتوان بر اساس آن هر شخصی را که به صورت مداوم و مکرر با انجام اعمال

تهدیدآمیز و آزاردهنده قربانیان را هدف قرار داده و باعث مختل شدن زندگی اجتماعی و شخصی آنها می‌شود، مجازات کرد. اگرچه برخی از رفتارهای مجرمانه از قبیل تهمت و هتک حیثیت (ماده۱۶)، انتشار فیلم و عکس خصوصی افراد (ماده۱۷)، ارسال فیلم و عکس مستهجن(ماده۱۴)، در قانون جرایم رایانه‌ای مورد صراحت قانونی قرارگرفته است؛ اما شرایط و اوضاع و احوال پیش‌بینی شده نسبت به این جرایم حاکی از آن است که جرایم مذکور از منظر عنصر مادی (رفتار مجرمانه و نتیجه مجرمانه) با جرم کمین سایبری مطابقت ندارند و لذا نمی‌توان آنها را تحت شمول جرم کمین سایبری قرار داد.

در خصوص رفتار مجرمانه، ضابطه اصلی در جرم کمین سایبری تداوم و تکرار رفتاری است که موجب اختلال در زندگی فردی و اجتماعی قربانی شده که گاها" اثرات جبران ناپذیری همچون خودکشی را نیز به همراه دارد. در حالی که در جرایم پیش بینی شده در قانون جرایم رایانه‌ای، قانون گذار صراحتی در این خصوص ندارد و این جرایم به صرف یکبار انجام رفتار مجرمانه تحقق پیدا می‌کنند. لذا، تکرار رفتار مجرمانه شرط تحقق این جرایم نمی‌باشد.

همچنین نتیجه مجرمانه پیش بینی شده در این جرایم متفاوت ار نتیجه مجرمانه در جرم کمین سایبری می‌باشد. به عنوان مثال، در ماده ۱۶ قانون جرایم رایانه‌ای قانونگذار در مقام بیان شرایط جرم، تحقق جرم مذکور را منوط به این دانسته است که این جرم موجب هتک حیثیت قربانی گردد و برای رسیدن به این نتیجه ارتکاب یکبار رفتار مجرمانه راکافی دانسته است. این در حالی ست در جرم کمین سایبری، نتیجه مجرمانه آسیب جسمی، عاطفی و روانی شخص قربانی و در نهایت مختل شدن زندگی وی می‌باشد تا آنجا که ممکن است قربانی حتی به علت فشار روحی و روانی اقدام به خودکشی نمایند. درواقع انگیزه مجرم از تکرار رفتارها این است که قربانی تحت کنترل وی باشد و به تمام خواسته‌های او تن در دهد.

ضمن اینکه در خصوص برخی رفتارهای مجرمانه از قبیل ارسال مداوم ایمیل‌های

آزار دهنده ناخواسته، تعقیب آنلاین فعالیت‌های قربانیان، ترغیب و تشویق افراد ثالث جهت تهدید و آزار و اذیت قربانی، نیز هیچ صراحت قانونی وجود ندارد. این در حالی ست که امروزه با توجه به گستردگی استفاده از اینترنت و سایر وسایل فناوری اطلاعات و با توجه به ویژگی‌های حاکم بر فضای مجازی، تعداد زیادی از افراد ممکن است قربانی جرم مذکور واقع شده که این امر می‌تواند پیامدهای اجتماعی و روانی مخربی بر زندگی آنها برجای‌گذارد و امنیت و آسایش افراد و جامعه را مختل کند. لذا، در خصوص جرم‌انگاری اعمال مذکور که امروزه بخش مهمی از جرایم فضای سایبر را تشکیل می‌دهند، وضع قوانین جدید و تکمیلی که بتواند با جرم‌انگاری ماهیتی و عام تمام مصادیق احتمالی رفتارهای مجرمانه جرم مذکور را پوشش دهد ضرورتی اجتناب‌ناپذیر می‌باشد.

در خصوص جرم کمین سنتی نیز جرمی با این ماهیت و تحت این عنوان در قانون مجازات اسلامی جرم‌انگاری نشده است. اگرچه برخی از مصادیق رفتارهای مجرمانه از قبیل مزاحمت تلفنی موضوع ماده ۶۴۱ قانون مجازات اسلامی، مزاحمت برای بانوان و اطفال موضوع ماده ۶۱۹ قانون مجازات اسلامی و مزاحمت و تهدید با چاقو موضوع ماده ۶۱۷ قانون مجازات اسلامی مورد تصریح قانونی قرارگرفته‌اند. اما باز هم مطابق ظاهر مواد قانونی، جرایم مذکور فاقد عنصر مادی و روانی مشابه با جرم کمین سنتی می‌باشند. البته در خصوص مزاحمت تلفنی موضوع ماده ۶۴۱ قانون مجازات اسلامی می‌توان بیان داشت که برداشت منطقی از این ماده این است که منظور قانونگذار از مزاحمت تلفنی صرف یکبار تلفن زدن و قطع کردن یا تلفن زدن و سکوت کردن یا تهدید کردن موجب صدق عنوان مزاحمت نمی‌شود؛ بلکه مرتکب باید این رفتار را چندین بار تکرار کرده تا عنوان مزاحمت صدق نماید. اما ظاهر مادی حاکی از آن است که ارتکاب یکبار رفتار برای تحقق جرم کافی می‌باشد. با این وجود جرم موضوع این ماده بر خلاف جرم کمین سنتی جرمی مطلق است که قانون‌گذار تحقق آن را منوط به حصول نتیجه خاصی نکرده است. اگر این مزاحمت با ایجاد هراس در طرف مقابل موجب مگر یا صدمه بدنی به وی شود

مقررات راجع به قتل و صدمات جسمانی اعم از عمدی و غیرعمدی قابل اعمال خواهد بود.

جرم موضوع ماده ۶۱۹ نیز جرم خاصی‌ست که قانون گذار آن را از موارد توهین کیفری محسوب نموده است. در جرم مذکور مرتکب بدون هدف کنترل قربانی و مخدوش کردن زندگی وی، صرفا با رفتار و یاگفتار خود موجب ایجاد مزاحمت و یا هتک حیثیت برای قربانی می‌گردد. این امر در خصوص جرم موضوع ماده ۶۱۷ نیز صادق است. همچنین در خصوص سایر انواع رفتارهای مجرمانه احتمالی مانند تعقیب کردن یک شخص در محل کار یا نزدیک خانه(مراقبت چشمی و بصری افراد)، ارسال نامه‌های تهدید آمیز و هر رفتار احتمالی دیگری که موجب احساس ترس و ناامنی در فرد شود، هیچگونه صراحت قانونی وجود ندارد.

بنابراین، قانون‌گذار در مواد ۶۱۷ ،۶۱۹ و ۶۴۱ قانون مجازات اسلامی و مواد ۱۴، ۱۶ و ۱۷ قانون جرایم رایانه‌ای اشاره‌ای به تداوم رفتار مجرمانه نکرده است؛ اما ماهیت جرایم کمین سایبری و سنتی تکرار و تداوم رفتار را برای ایجاد ترس در قربانی و مختل شدن زندگی او اقتضا می‌کند. زیرا به صرف یک تماس تلفنی ناخواسته و یا ارسال یک فیلم و عکس مستهجن یا تهمت به قربانی نتیجه مجرمانه‌ای که باید از رفتار حاصل گردد، تحقق نمی‌یابد؛ بلکه رفتار باید در طول زمان تداوم داشته باشد تا بتواند باعث فشار روانی و عدم کنترل قربانی بر زندگی‌اش گردد. ضمن اینکه جهت تحقق جرایم کمین سایبری و کمین سنتی شرایطی و خصوصیاتی لازم است که خاص جرایم فوق بوده و وجود آنها برای تحقق این جرایم ضروری می‌باشد. از جمله این خصوصیات می‌توان به وجود تهدید معتبر از سوی مرتکب جرم و ترس انسان متعارف در نتیجه این تهدید اشاره نمود که در قانون مجازات اسلامی به این شروط نیز توجهی نشده است.

کالیفرنیا در سال ۱۹۹۰ اولین قانون در خصوص جرم کمین سنتی را تصویب کرد و پس از آن سایر ایالت‌ها برای پرکردن خلاهای قانونی خود این قانون را تصویب کردند.

مطابق این قوانین هر شخصی که با انگیزه کشتن، زخمی کردن، اذیت و آزار و غیره شخص دیگری را دنبال کند و با انجام این کار موجب گردد که قربانی احساس ترس معقولی در خصوص امنیت جسمی خود و خانواده‌اش داشته باشد یا موجب ناراحتی روانی در وی شود، مجرم تلقی می‌گردد. (Vasiu،ibid،۲۳۰). قانون ما نیز در این خصوص نیز نیازمند قانون‌گذاری ماهیتی برای جرایم مذکور می‌باشد تا بتواند تمام انواع رفتارهای مداوم تهدیدآمیزی که منجر به آسیب‌های عاطفی، روانی و جسمی می‌شوند را تحت شمول قرار دهد.

۲-۲- عنصر مادی

عنصر مادی از ارکان مهم تشکیل دهنده جرم می‌باشد که بدون وجود آن تحقق جرم در خارج امکان پذیر نمی‌باشد. در واقع به صرف قصد مجرمانه نمی‌توان کسی را مجازات کرد؛ بلکه این قصد مجرمانه باید توسط عنصر مادی ظهور و بروز خارجی پیدا نماید تا بتوان فرد را در قبال رفتار ارتکابی مسئول دانست. عنصر مادی متشکل از رفتار مجرمانه، موضوع جرم، اوضاع و احوالی که شرط تحقق جرم است و نتیجه مجرمانه می‌باشد.

۱-۲-۲- رفتار مجرمانه

در جرم کمین سنتی رفتار مجرمانه مرتکب با فعل مثبت تحقق می‌یابد و لذا ترک فعل، حتی اگر با سوءنیت همراه باشد و موجب آسیب روانی، عاطفی و جسمانی قربانی گردد؛ نمی‌تواند عنصر مادی جرم را تشکیل دهد. در جرم مذکور مصادیق رفتار مجرمانه متنوع و گسترده است اما آنچه که در انواع رفتارهای مجرمانه از قبیل ارسال نامه‌ها و پیامهای تهدیدآمیز، تعقیب قربانی، تخریب اموال، شایعه پراکنی در خصوص قربانی و غیره مشترک و حائز اهمیت می‌باشد؛ انجام مکرر و مداوم رفتار تهدیدآمیز و آزار دهنده

علیه شخص دیگر است که موجب مختل شدن زندگی و احساس ترس و ناامنی وی می‌گردد. به عبارت دیگر، مجرم برای نقض قانون باید حداقل بیش از یک بار به گونه‌ای رفتار نماید که باعث ترس قربانی شود.

در جرم کمین سایبری نیز رفتار مجرمانه به شکل فعل مثبت صورت می‌گیرد. در جرم مذکور رفتار مجرمانه، رفتاری مداوم و مکرر شامل دادن، ارسال، انتقال، انتشار مکرر موارد توهین‌آمیز، تعقیب فعالیت‌های قربانی و تحریک دیگران به تهدید قربانی از طریق اینترنت و فناوری اطلاعات می‌باشد(Gregorie،p۲:۲۰۰۱). لذا، وجه تمایز رفتار کمین سایبری نسبت به نوع سنتی آن، انجام رفتارهای مداوم تهدیدآمیز از طریق اینترنت و محیط مجازی می‌باشد.

بنابراین، در جرایم مذکور مرتکب باید درگیر رفتاری شود که حداقل بیش از یک بار رخ داده باشد. لذا، مجازات کردن فرد به صرف انجام یک رفتار، مشروعیت قانونی ندارد. زیرا وقوع رفتارهای مکرر علیه شخص است که باعث ایجاد ترس و مختل شدن زندگی او می‌گردد (Schwartz،p۴۰۹:۲۰۰۹). به همین جهت، شخص باید در مجموعه‌ای از رفتارهای تهدیدآمیز درگیر شود و یک نمونه مداوم از اذیت و آزار در رفتار او وجود داشته باشد تا عنصر مادی جرایم مذکور محقق گردد.

۲-۲-۲- موضوع جرم

یکی از اجزاء مهم عنصر مادی موضوع رفتار مجرمانه می‌باشد که وجود آن برای تمامی جرایم الزامی‌ست و تحقق جرم بدون آن قابل تصور نمی‌باشد. جرایم کمین سایبری و کمین سنتی نیز از این حکم مستثنی نیستند. با توجه به گستردگی مصادیق رفتار مجرمانه در جرایم مذکور، موضوع این جرایم غالبا اهداف جذاب و فاقد نگهبانی هستند که در معرض مجرمین با انگیزه قرار دارند. در واقع، اگرچه تمام افرادی که در فضای مجازی فعالیت می‌کنند ممکن است بزه‌دیده جرم کمین سایبری قرار گیرند؛ اما عموما افرادی که

فعالیت‌های روزمره آنلاین خطرناک دارند (از جمله: ارسال اطلاعات و تصاویر شخصی در شبکه‌های اجتماعی، بازدید از وب‌سایت‌های مستهجن، شرکت در اتاق‌های گفت‌وگوی آزاد و غفلت در نصب نرم‌افزارهای امنیتی و آنتی ویروس‌ها) بیشتر از افرادی که مشارکت کمتری در چنین فعالیت‌ها دارند، قربانی جرائم سایبری می‌شوند(Reyns،۱۱۵۱،۲۰۱۱). در خصوص جرم کمین سنتی نیز با توجه به نظریات فعالیت روزانه و سبک زندگی، افردی که شیوه زندگی بازتری دارند، با افراد بزهکار بیشتر در ارتباط هستند و یا در محیط‌های مجرمانه و خطرناک رفت و آمد می‌کنند، بیشتر از سایر افراد هدف جرم کمین سنتی قرار می‌گیرند (نجفی ابرند آبادی،۱۳۹۱، ص ۱۲۸۰).

۳-۲-۲- شرایط و اوضاع و احوال جرم

جهت تحقق جرم کمین سایبری و کمین سنتی شرایطی و خصوصیاتی لازم است که خاص جرایم فوق بوده و وجود آنها برای وقوع جرایم مذکور ضروری می‌باشد. از جمله این خصوصیات می‌توان به وجود تهدید معتبر از سوی مرتکب جرم و ترس انسان متعارف در نتیجه این تهدید اشاره نمود.

در جرایم فوق، تهدید شفاهی یا کتبی که به صورت صریح و یا ضمنی علیه قربانی صورت می‌گیرد باید معتبر و قطعی باشد. بدین معنی که مرتکب توانایی لازم برای انجام آن تهدید را داشته باشد. اما مهم نیست که مرتکب واقعا قصد عملی کردن تهدید را دارد خیر؟ و همچنین مهم نیست این تهدید در عالم واقع رخ دهد یا خیر؟ بلکه آنچه که مهم است درک قربانی از تهدید صورت گرفته است که باید در حدی باشد که قربانی مطمئن باشد امکان وقوع تهدید وجود دارد و این امر منجر به مختل شدن زندگی اوگردد(Mishler،ibid،۱۲۱).

شرط دانستن "تهدید معتبر" برای تحقق جرم کمین سایبری با چالش مواجه است. زیرا قربانی باید ثابت کند که مرتکب کمین سایبری توانایی آشکار برای انجام رفتار

تهدید آمیز و عملی کردن تهدید را داشته است. این در حالی‌ست که مرتکب جرم و قربانی اغلب مسافت‌ها با هم فاصله دارند و تعامل مستقیم با یکدیگر ندارند و حتی قربانی نسبت به هویت مرتکب جرم و محل اقامت او آگاهی ندارد و به همین جهت برای قربانی غیرممکن است که بتواند تشخیص دهد آیا مرتکب توانایی آشکار برای انجام تهدید را دارد یا خیر. بنابراین، می‌توان بیان کرد که در جرم مذکور صرف رفتار تهدیدآمیزی که قابلیت مختل کردن زندگی قربانی را داشته باشد برای تحقق جرم کافی می‌باشد و نیاز نیست که قربانی ثابت کند که مرتکب توانایی لازم برای عملی کردن تهدید را داشته است.

شرط لازم دیگر برای تحقق این جرم این است که رفتار تهدیدآمیز مرتکب، موجب احساس ترس انسان متعارف نسبت به امنیت خود یا امنیت خانواده یا نزدیکانش شود. بنابراین، ملاک در خصوص مؤثر بودن تهدید و در نتیجه احساس ترس، معیار شخصی نیست؛ بلکه معیار نوعی است. بدین معنی هر انسان متعارفی که در آن شرایط قرارگیرد در اثر تهدید و تداوم رفتار مرتکب نسبت به امنیت جسمی، روانی و عاطفی خود و خانواده‌اش احساس ترس داشته باشد و از استرس روانی رنج ببرد. لذا، اگر هر شخص معقولی این ترس را تجربه کند، شرط لازم برای تحقق جرم مذکور حاصل می‌شود.(Jones,P۳۲:۲۰۰۷).

علاوه بر شرایط فوق، در جرم کمین سایبری وسیله نیز شرط تحقق جرم است. اگرچه جرم مذکور مانند سایر جرایم سایبری با استفاده از فناوری‌ها و وسایل الکترونیکی مدرن صورت می‌گیرد؛ اما سه شکل اصلی و رایج که کمین سایبری از رهگذر آنها غالبا به وقوع می‌پیوندد، عبارت از: پست الکترونیک، اینترنت و کامپیوتر.

پست الکترونیک: یافته‌های تحقیقات نشان دهنده این است که رایج ترین شکل کمین سایبری از طریق ایمیل است که مجرم به عنوان ابزار اصلی برای آزار و اذیت قربانیان خود از آن استفاده می‌کند. ایمیل این امکان را فراهم می‌کند که مجرم بارها و بارها پیامهای تهدیدآمیز و آزار دهنده زشت و ناپسند را ارسال کند یا عکس فیلم و یا صوت دیگری را انتشار و انتقال دهد(Thapa،۴،۲۰۱۱).

اینترنت: در این مورد مرتکب به منظور تهدید کردن و در معرض خطر قرار دادن قربانی از اینترنت استفاده می‌کند. انواع اطلاعاتی که در خصوص افراد در اینترنت قابل دسترس است از قبیل آدرس ایمیل، شماره تلفن، آدرس محل سکونت، حساب بانکی و اطلاعات کارت اعتباری خطر بزه‌دیدگی افراد را افزایش می‌دهد.

کامپیوتر: طریق معمول دیگر، انجام رفتار مجرمانه از طریق کامپیوتر است که فرد به منظور کنترل غیرمجاز کامپیوتر و تعقیب فعالیت‌های روزانه و آنلاین دیگری می‌تواند کامپیوتر خود را از طریق اینترنت به کامپیوتر دیگری متصل نماید و به راحتی به اطلاعات شخصی وی دسترسی و تسلط پیدا کند(Baum ,P۱۸۵:۲۰۰۹). بنابراین، درکمین سایبری استفاده از اینترنت، ایمیل، کامپیوتر و سایر شبکه‌های اجتماعی مانند چت روم‌ها و غیره ضروری می‌باشد.

۴-۲-۲- حصول نتیجه مجرمانه

جرم کمین سایبری و سنتی در زمره جرایم مقید به نتیجه هستند که صرف تداوم رفتار تهدیدآمیز برای تحقق آنها کافی نمی‌باشد؛ بلکه وقوع کامل این جرایم منوط به حصول نتیجه مجرمانه است. در حقیقت، مبنای جرم‌انگاری جرایم مذکور جلوگیری از حصول نتیجه مجرمانه می‌باشد. نتیجه در جرایم مذکور، وضعیتی است که از تداوم این رفتارهای تهدیدآمیز حاصل می‌گردد. این وضعیت شامل آسیب جسمی، عاطفی و روانی شخص قربانی و در نهایت مختل شدن زندگی وی می‌باشد تا آنجاکه ممکن است قربانیان حتی به علت فشار روحی و روانی اقدام به خودکشی نمایند. زیرا ماهیت مکرر رفتار مجرمانه باعث می‌شود که قربانی ثبات روانی خود و در نتیجه قدرت کنترل بر زندگی خود را از دست دهد.

۲-۳- عنصر روانی

عنصر روانی از ارکان مهم تشکیل دهنده جرم است که وقوع جرم بدون تحقق آن قابل تصور نیست و فرد را به صرف ارتکاب و اثبات عنصر مادی نمی‌توان مجازات نمود. بلکه علاوه بر عنصر مادی بایستی فرد همزمان عنصر روانی متناسب با آن جرم را نیز داشته باشد. درخصوص جرم کمین سایبری و سنتی این دو جرم مطابق با اصل عمدی بودن جرایم در حقوق کیفری، در زمره جرایم عمدی می‌باشد و مجرم باید عامدانه درگیر در رفتارهای مجرمانه گردد.

اولین جزء در عنصر روانی، علم افراد به قانون است یعنی فرد باید بداند رفتار او در قانون جرم‌انگاری و برای آن مجازات تعیین شده است که در قانون مجازات جمهوری اسلامی ایران، قانون‌گذار به منظور حفظ نظم و مصلحت جامعه اصل را بر آگاهی افراد از حکم قانون دانسته است؛ مگر اینکه تحصیل علم برای وی عادتا غیر ممکن باشد. متاسفانه همانگونه که ذکر شد قانون مجازات اسلامی و قانون جرایم رایانه‌ای در خصوص این جرایم دارای خلا قانونی می‌باشند.

علاوه بر علم به قانون مرتکب باید علم به موضوع جرم و خصوصیات جرم نیز داشته باشد یعنی باید بداند یا باید می‌دانست که رفتارها و تهدیدات او باعث ترس انسان متعارف می‌شود.

درکنار علم و آگاهی، مرتکب باید سوءنیت عام و سوءنیت خاص لازم برای جرایم مذکور را نیز دارا باشد. در این جرایم سوءنیت عام عبارت از قصد تداوم و تکرار رفتارهای تهدیدآمیز می‌باشد. بدین معنی که شخص باید آگاهانه درگیر در تکرار رفتاری شود که باعث گردد قربانی نسبت به امنیت خود احساس ترس داشته باشد و به جهت اینکه دو جرم مذکور در زمره جرایم مقید می‌باشند، باید فرد درکنار سوءنیت عام خواست انجام نتیجه یعنی خواست آزار و اذیت و ارعاب قربانی و در نتیجه آسیب جسمی، روانی و عاطفی به شخص را نیز داشته باشد. بنابراین، باید قصد فعل و قصد نتیجه درکنار عنصر

مادی جرم احراز شود تا بتوان شخص را به ارتکاب جرم مجازات نمود. البته تکرار رفتار تهدیدآمیز را می‌توان دلیلی بر وجود قصد مجرمانه مرتکب دانست.

در پایان، در خصوص شرط بودن یا شرط نبودن انگیزه در جرایم فوق می‌توان بیان کرد که مطابق اصول کلی حقوق کیفری انگیزه اصولا شرط تحقق جرم نمی‌باشد و به طور استثناء در برخی جرایم انگیزه می‌تواند جزء اجزاء تشکیل دهنده جرم تلقی گردد. در جرایم کمین سایبری و سنتی اغلب مجرم دارای شخصیتی ناپایدار و ضد اجتماعی می‌باشد که به دلیل حس کینه توزی، حیله‌گری، غرور، انحراف جنسی، لذت آزار دیگران و غیره دست به ارتکاب جرم می‌زند(لک،۱۳۹۱، ص ۱۰۵). لذا، غالبا مرتکبین جرایم مذکور تحت تأثیر شرایط شخصیتی و اجتماعی خود با اهداف مختلفی از جمله سرگرمی، انتقام‌جویی شخصی، تنفر، حسادت، خشم، بیماری روانی، اذیت و آزار جنسی و غیره اقدام به مزاحمت و آزار دیگران می‌کنند. البته گاهی اوقات این امکان وجود دارد که اذیت و آزار قربانی بدون هدف صورت گیرد و قربانی صرفا به دلیل اینکه در مکان یا زمان نامناسب قرارگرفته است در معرض خطر بزه‌دیدگی قرارگیرد. اگرچه اذیت و آزار یا تهدید به اشکال مختلف و با اهداف مختلفی صورت می‌گیرد؛ اما انگیزه مشترک تمام مرتکبین این جرایم اعمال کنترل بر زندگی قربانی است. در واقع انجام تمام رفتارهای تهدیدآمیز خواه با هدف انتقام شخصی و خواه با هدف سرگرمی، به جهت اعمال کنترل بر قربانی جرم صورت می‌پذیرند.

۲- بررسی جرم‌شناختی کمین سایبری و سنتی

با توجه به اثرات زیان بار و جبران ناپذیری که جرم کمین سایبری بر سلامت جسمی و روانی بزه‌دیدگان بر جای می‌گذارد و نیز با توجه به پایین بودن امکان شناسایی و دستگیری مرتکبین این جرم، اتخاذ تدابیری جهت پیشگیری از وقوع و تکرار آن در جهت حفظ امنیت و آزادی افراد در انجام فعالیت‌های آنلاین ضروری می‌باشد. به همین

علت در این قسمت پس از بررسی و شناسایی وجوه افتراق و تشابه میان این دو جرم به بررسی نظریات مربوط جهت پیشگیری از جرم کمین سایبری پرداخته می‌شود.

۱-۲- مقایسه جرم کمین سایبری و کمین سنتی

جرم کمین سایبری از بسیاری جهات دارای اصول یکسانی با جرم کمین سنتی می‌باشد. اما با این حال، کمین سایبری شکل جدیدی از رفتار مجرمانه است که خصوصیات متمایز و مجزایی نسبت به کمین سنتی دارد. دو جرم مذکور از لحاظ اصول عمومی و کلی از جمله اینکه اکثر قربانیان این جرایم زنان و اکثر مرتکبین آنها مردان هستند و نیز اینکه هر دو در زمره جرایم عمدی می‌باشند که در آن مرتکبین با انگیزه اعمال کنترل بر قربانی، با انجام رفتارهای مداوم تهدیدآمیز و آزاردهنده شخص را مورد هدف قرار می‌دهند؛ با یکدیگر مشابه می‌باشند.

با وجود این شباهت‌ها، دو جرم مذکور وجوه افتراق اساسی با یکدیگر دارند. از جمله این تفاوتها می‌توان به موارد ذیل اشاره نمود:

۱ مجاورت جغرافیایی: در کمین سنتی مجرم و قربانی در حوزه جغرافیایی مشترک یا نزدیک بهم زندگی می‌کنند، در حالی که در کمین سایبری مجرم می‌تواند قربانی خود را در شهر دیگر یا حتی در کشور دیگر مورد اذیت و آزار یا تهدید قرار دهد. به همین علت، مرتکب می‌تواند دائما و بدون ترس از امکان شناسایی و دستگیری عمل خود را تکرار کند و بر عدم توانایی خود فائق شود(Short،۲۴،۲۰۱۵). زیرا در بسیاری از موارد مرتکب توانایی و جرأت برخورد فیزیکی با قربانی را ندارد. اما اینترنت و سایر وسایل الکترونیکی با برداشتن این مانع، راه را برای مرتکب جهت دستیابی به اهداف غیر قانونی خود هموار ساخته است. همچنین عدم مجاورت جغرافیایی و استفاده از فناوری و ارتباطات الکترونیکی این امکان را برای مجرم فراهم کرده که اشخاص ثالث را برای اذیت و آزار و تهدید قربانی تشویق و تحریک نماید. به این صورت که با بدست

آوردن اطلاعات شخصی قربانی و شایعه پراکنی در خصوص وی بر روی شبکه های اجتماعی، دیگران را ترغیب به انجام رفتارهای غیرقانونی و غیر اخلاقی علیه قربانیان نمایند. این در حالی‌ست که در خصوص جرم کمین سنتی به علت لزوم تقابل جسمی، تحریک شخص ثالث جهت آزار و اذیت یا تهدید قربانی برای مجرم آسان نیست. (patel , p۲۱۶:۲۰۱۴).

۲. آشنایی با قربانی: جرم کمین سنتی در روابط بین فردی رخ می دهد. به طورکلی قربانی برای مجرم فردی شناخته شده است. به عنوان مثال قربانی یک فرد مشهور، یا یکی از اقوام یا ساکنین نزدیک وی می‌باشد. اما درکمین سایبری مجرم با توجه به اطلاعات موجود در فضای مجازی به طور تصادفی قربانی را انتخاب می کند و غالبا نیز هیچگونه آشنایی قبلی با وی ندارد.

۳. ناشناس ماندن: درکمین سنتی به علت مجاورت جغرافیایی و تماس فیزیکی میان مجرم و قربانی پنهان کردن هویت برای مجرم دشوار می‌باشد. اما یکی از مزایای بسیار زیادی که مجرمین سایبری نسبت به مجرمین کمین سنتی دارند این است که این متخلفان به طور معمول از سطح بالایی از مهارت و استعداد رایانه‌ای برخوردار هستند. مهارت‌های اساسی که به فرد متبحر اجازه می دهد تا بتواند هویت خود را به راحتی از طریق انواع تاکتیک‌های ارزان و ساده مخفی کند و این ناشناس بودن به مجرمین کمین سایبری این اجازه را می‌دهد تا قربانیان خود را برای مدت طولانی بدون اطلاع قربانی در فضای مجازی دنبال کنند. به همین علت، امکان شناسایی و دستگیری مجرمین این جرم با مشکل روبه‌رو می‌باشد. توضیح اینکه، به دلیل عدم تعامل مستقیم میان قربانی و مجرم و اتخاذ نام‌های مستعار و مختلف، اصولا هویت مجرمان درکمین سایبری ناشناخته است و همین امر اجرای قوانین موجود را با مشکل مواجه می‌کند و این ناشناس ماندن مزیتی بزرگ برای مجرم محسوب می‌شود. زیرا ناتوانی قربانی برای شناسایی منبع آزار و اذیت، باعث می‌شود که مجرم به اقدامات

مجرمانه خود ادامه دهد(Goodno,۲۰۰۷ p۶۷:).

درواقع، مجهول بودن هویت افراد و عدم امکان شناسایی آنها بر خلاف محیط فیزیکی، زمینه را برای ارتکاب رفتارهای غیر اخلاقی فراهم می‌کند. زیرا علاوه بر اینکه سبب آزادی بیشتر افراد در انجام رفتارهای مجرمانه می‌شود؛ به علت اینکه آثار اعمال و رفتارهای غیر اخلاقی نیز به راحتی در فضای مجازی قابل حذف و مخفی کردن است؛ محرکی برای افزایش فعالیت‌های مجرمانه به علت پایین بودن احتمال دستگیری و شناسایی مرتکبین محسوب می‌شود(پورقهرمانی ۱۳۹۱،ص ۸۰). لذا، یکی از وجوه مهم افتراق میان جرایم سنتی و سایبری خصوصیت‌ها و ویژگی‌های بزه در فضای سایبر است که باعث افزایش و تنوع جرایم سایبری شده است. از جمله این خصوصیت‌ها می‌توان به گمنامی یا مجهول بودن هویت مجرمان، سهولت و سرعت ارتباطات، حجم جرایم ارتکابی و فراملی بودن جرایم اشاره نمود(جوان جعفری، ۱۳۹۰،ص۱۷۹). بنابراین، جرم کمین سایبری جرمی غیراخلاقی ست که به علت خصوصیت گمنام بودن هویت مرتکبین، قربانیان زیادی را بدون ترس از امکان شناسایی در فضای مجازی مورد هدف قرار می‌دهد.

۴. مهم‌ترین وجه تمایز میان دو جرم مذکور شیوه ارتکاب این جرایم می‌باشد. درکمین سایبری مرتکب برای تهدید و آزار شخص از اینترنت استفاده می‌کند و با توجه به امکانات و مزایای گسترده اینترنت می‌تواند در مدت زمان کوتاهی با سهولت به اطلاعات شخصی افراد دسترسی پیدا کند و از این طریق تعداد زیادی از اشخاص را مورد هدف قرار دهد. زیرا اینترنت یک رسانه بدون مرز است که امکان توزیع فوری و ناشناس پیام فرد را فراهم می کند. در این عصر مجازی، وب سایت‌ها، نامه‌های الکترونیکی، اتاق‌های گفتگو، تابلوهای اعلانات الکترونیکی ناشناس، پیام‌رسان‌های فوری و سایر دستگاه‌های ارتباطی این امکان را به مجرمین می‌دهند که به سرعت فعالیت‌های تهدیدآمیز خود علیه بزه‌دیدگان را سامان‌دهی نمایند. در حالی که

در کمین سنتی انجام رفتارهای مکرر علیه قربانی نیازمند مدت زمان طولانی‌تری می‌باشد. به عنوان مثال، یک مجرم کمین سنتی ممکن است قربانی را به طور مکرر آزار دهد، با قربانی تماس تلفنی بگیرد. اما هر تماس تلفنی یک رویداد واحد است که به عمل و زمان مجرم احتیاج دارد. (Chik،۱۳،۲۰۰۸). اما در کمین سایبری مرتکبین این جرم می‌توانند از مزایای سهولت و سرعت ارتباطات سود ببرند و از طریق اینترنت احتمال دسترسی خود را به اطلاعات شخصی افراد افزایش دهند و به راحتی اطلاعات خصوصی در مورد قربانی را با کلیک کردن بر روی یک دکمه به دست آورند. حتی بسیاری از مجرمین حرفه‌ای می‌توانند از برنامه‌هایی استفاده کنند که به طور منظم بدون نیاز به حضور اشخاص در کنار کامپیوتر پیامهای تهدیدآمیز را مکررا برای افراد ارسال نماید که این امر باعث افزایش حجم زیاد جرایم کمین سایبری علیه قربانیان زیادی می‌شود. زیرا مجرم می‌تواند با یک اقدام تعداد زیادی از قربانیان را مورد هدف قرار دهد(Mishler،۱۱۶،۲۰۰۰).

این خصوصیت‌ها و ویژگی‌های جرم کمین سایبری باعث افزایش رقم سیاه بزهکاری این جرم شده است. زیرا تحقیقات پلیس در فضای سایبر به علت پیچیدگی بالای بزهکاری سایبر و همچنین به علت این واقعیت که این جرایم از طریق سیستم‌ها و کانال‌هایی ارتکاب می‌یابند که مانع شناسایی مجرم می‌شوند، پیچیده و سخت است. (Agustina ,p۳۶:۲۰۱۵) انجمن بین‌المللی حقوق در گردهمایی خود درباره جرایم سایبری گزارشی را ارائه نمود که نشان دهنده این واقعیت است که از میان حجم زیاد جرایم ارتکابی در فضای سایبر تنها ۵ درصد از جرایم مذکور به پلیس گزارش می‌شوند و ۹۵ درصد باقیمانده جرایم به علت ناشناخته بودن مرتکبان و فقدان مدارک کافی به اطلاع و آگاهی پلیس نمی‌رسند (باستانی،۱۳۸۳،ص۲۵).

پیمایش بزه‌دیده شناسی که در میان دانشجویان دختر دانشگاه فردوسی مشهد نیز انجام گردید حاکی از بالا بودن رقم سیاه بزهکاری جرم کمین سایبری

می‌باشد. نتایج این تحقیق نشان داد که اغلب دختران، قربانی جرم کمین سایبری واقع شده‌اند که غالبا به علت ناشناخته بودن مرتکب آن را به پلیس گزارش نکرده‌اند.

یکی از آثار بالا بودن رقم سیاه بزهکاری در فضای مجازی کاهش اثر بازدارندگی مجازات‌های احتمالی و در نتیجه افزایش میزان بزه‌دیدگی افراد است. بالا بودن رقم سیاه به معنی کاهش احتمال دستگیری و مجازات است. زیرا بر اساس تئوری انتخاب عقلانی هر چه احتمال دستگیری و اجرای مجازات کاهش یابد، اثر بازدارندگی مجازات‌های قانونی کمتر شده و در نتیجه احتمال ارتکاب جرم افزایش می‌یابد.(جوان جعفری،۱۳۸۹، ص ۱۷۹).

به این ترتیب، ارتکاب این جرم در فضای مجازی نسبت به فضای سنتی، باعث شده که کمین سایبری عملی زیان‌آور و طرق کشف، اثبات و پیشگیری از وقوع و تکرار آن مشکل‌تر باشد. در حقیقت، بسیاری از مزایا و ویژگی‌های فضای سایبر از قبیل هزینه پایین، سهولت و سرعت ارتباطات و طبیعت گمنام، فضای مجازی را به پناهگاهی امن برای مجرمین تبدیل کرده که در آن مجرمین با احتمال کمتری از شناسایی افراد بیشتری را مورد هدف قرار داده و نسبت به دنیای فیزیکی خسارات بیشتری را بر پیکر امنیت و آسایش جامعه وارد می‌کنند (جوان جعفری، پیشین، ص۱۶۹).به همین علت، از جمله راهکارهای مهم و مؤثر جهت مقابله با جرم کمین سایبری پیش‌بینی واتخاذ تدابیر امنیتی و پیشگیرانه می‌باشد که بتوان از رهگذر آنها از قربانیان بالقوه جرم مذکور تا حد امکان حمایت نمود.

۲-۲- رویکرد پیشگیرانه به جرم کمین سایبری

فعالان حوزه پیشگیری از جرم به علت اثرات جبران ناپذیر جرم کمین سایبری بر زندگی اجتماعی و خصوصی افراد، به منظورکشف علت بزه‌دیدگی بزه‌دیدگان این جرم و تدبیر سیاست‌هایی جهت پیشگیری از بزه‌دیدگی مکرر آنها، نظریاتی مطرح نموده‌اند که

از جمله آنها می‌توان به نظریات فعالیت روزانه[1] و سبک زندگی[2] اشاره نمود. تئوری سبک زندگی و فعالیت‌های روزانه هر دو تحت تئوری فرصت جرم مورد بررسی قرار می‌گیرند. تئوری سبک زندگی بر سطح عوامل خطر تمرکز کرده و ادعا می‌کند شیوه خاص زندگی افراد آنها را در معرض خطر بزه‌دیدگی قرار می‌دهد (Halder, ۲۰۱۵; ۱۱۱). لذا، هراندازه فرد شیوه زندگی بازتری داشته باشد، با افراد بزهکار بیشتری در ارتباط باشد و یا در محیط‌های مجرمانه و خطرناک بیشتر رفت و آمد کند، شانس بزه‌دیدگی خود را افزایش می‌دهد (نجفی ابرندآبادی، پیشین، ص ۱۲۸۰).

تئوری فعالیت‌های روزانه در ابتدا توسط کوهن و فلسون[3] برای تبیین تغییرات نرخ جرم و جنایت بعد از جنگ جهانی دوم در ایالات متحده مطرح شد. نتایج حاکی از این بود که تغییر در ساختار اجتماعی مثل ورود زنان به بازارکار و دانشگاه میزان جرایم را افزایش داده است. مطابق این نظر، ویژگی‌هایی از قبیل جنسیت، سن و نژاد موجب تفاوت در شیوه زندگی افراد و در نتیجه میزان بزه‌دیدگی آنها می‌شود. به عنوان مثال، زنان به علت اینکه بیشتر درگیر کارهای خانه هستند، کمتر در معرض مواجه با افراد غریبه قرار می‌گیرند. به همین جهت، کمتر از مردان بزه‌دیده واقع می‌شوند. همچنین مردم در سنین مختلف در شیوه‌های زندگی متفاوتی درگیر می‌شوند و این سبک زندگی متفاوت، افراد را در سنین مختلف در سطح‌های متفاوتی از خطر بزه‌دیدگی قرار می‌دهد. به طور مثال، جوانان بیشتر از سالمندان بزه‌دیده می‌شوند. زیرا سبک زندگی افراد جوان، آنها را در معرض خطر بزه‌دیدگی قرار می‌دهد(Reyns،۳۷،۲۰۱۰). در واقع، این نظریه، فرصت را عامل مهمی برای بزه‌دیدگی افراد دانسته و بیان می‌کند که فرصت زمانی رخ می‌دهد که مجرمان با انگیزه با اهداف مناسب و جذاب در محیط‌های فاقد نگهبان مواجه می‌شوند. بنابراین، نظریه فعالیت روزانه بنیان نظریه سبک زندگی را کامل‌تر می‌کند. این

1. Routione Activity Theory
2. Lifestyle
3. Cohen and Felson

نظریه بیشتر با اوضاع و احوال و شرایط مادی جرم در ارتباط است و در راستای پاسخ به این سوال است که چه عواملی تمایل افراد به ارتکاب جرم را مساعد می‌کند؟ در این راستا، کوهن بیان می‌کند که بزهکاری نتیجه تضعیف کنترل اجتماعی است. یعنی افراد در برخی از فعالیت‌ها و مشاغل احتیاط لازم را به کار نمی‌برند و از خود در مقابل جرم محافظت نمی‌کنند. (نجفی ابرندآبادی، پیشین، ص ۱۲۸۰)

مطابق این نظریات، بزه‌دیدگان کمین سایبری با انجام رفتارهای منحرفانه و پر خطر، خود را به عنوان یک هدف جذاب در معرض مجرمان با انگیزه قرار می‌دهند و از این طریق بزه‌دیدگی خود را تسهیل می‌نمایند. به عنوان مثال در پژوهشی که میان دانشجویان کالج در یک دانشگاه بزرگ شهر میدوست صورت گرفت کاربرد این دو نظریه برای درک بهتر عوامل خطر موثر بر بزه‌دیدگی کمین سایبری مورد توجه قرارگرفت. جامعه آماری در این پژوهش ۱۰۰۰۰ دانشجو ۱۸ تا ۲۴ ساله دوره کارشناسی بودند. از جمله رفتارهایی که به عنوان عوامل خطر در این پژوهش مورد پرسش قرارگرفتند، عبارتند از: اجازه دسترسی افراد غریبه به اطلاعات شخصی،تعداد مخاطبان شبکه‌های اجتماعی، میزان به‌روزرسانی نرم‌افزارهای مختلف و میزان حضور افراد در محیط‌های آنلاین. در نهایت یافته‌های این تحقیق نیز نشان داد کسانی که درگیر فعالیت‌های منحرفانه آنلاین هستند به عنوان یک هدف جذاب بیشتر در معرض مجرمان با انگیزه قرار می‌گیرند و همین امر خطر بزه‌دیدگی آنها را افزایش می‌دهد (Reyns, ibid; ۶۶).

در تحقیقی دیگر که میان دانشجویان دانشگاه ماساچوست انجام شد. خصوصیات بزه‌دیدگان کمین سایبری از منظر سه عنصر فعالیت روزانه جهت شناسایی عواملی که احتمال بزه‌دیدگی افراد را افزایش می‌دهد، مورد بررسی قرارگرفت. در همین راستا، برای سنجش متغیر قرارگرفتن افراد در معرض مجرمین آنلاین،سوالاتی از این قبیل طراحی شد: «از نام واقعی خود در فضای مجازی استفاده نمی کنم» ، «تمایل دارم هویت خود را در اینترنت پنهان کنم» و از پاسخ دهندگان خواسته شد بین گزینه کاملا موافقم

تاکاملا مخالفم نظریات خود را بیان کنند. برای سنجش جذابیت هدف مواردی از قبیل اینکه: «تصاویر و اطلاعات شخصی خود را به اشتراک می‌گذارم» مورد بررسی قرارگرفت و در نهایت برای سنجش عنصر فقدان نگهبان متغیرهایی از قبیل: «برنامه های ضد ویروس را نصب و به روز رسانی کردم» بررسی گردید. نتایج نشان داد افرادی که در فضای مجازی هویت واقعی خود از قبیل سن، جنس، تلفن، مکان و غیره را پنهان نمی‌کنند، افرادی که اطلاعات و تصاویر شخصی خود را در فضای مجازی منتشر می‌نمایند، افرادی که به غریبه ها اجازه دسترسی به اطلاعات خود را می‌دهند و افرادی که از برنامه های امنیتی مثل آنتی ویروس استفاده نمی‌کنند به عنوان هدفی جذاب برای مجرمین خطرناک تلقی می‌شوند و بیشتر در معرض خطر بزه‌دیدگی هستند. (Phillips،۸،۲۰۱۵).

همچنین در پژوهشی مشابه که در میان زنان یک دانشگاه انجام شد محققان متغیر وابسته را بزه‌دیدگی کمین سایبری قرار دادند و تاثیر سه عنصر فعالیت روزانه را به شرح ذیل بر میزان بزه‌دیدگی سنجیدند:

قرارگرفتن در معرض مجرم با انگیزه: با متغیرهایی از قبیل زمان روزانه صرف شده در فضای مجازی، تعداد شبکه‌های اجتماعی آنلاین متعلق به پاسخ‌دهنده و غیره مورد بررسی قرارگرفت. ۲. جذابیت هدف: با متغیرهایی از قبیل اجازه به افراد غریبه برای دسترسی به اطلاعات شخصی خود، انتشار فیلم و عکس خصوصی و غیره سنجیده شد و در نهایت ۳ . نگهبانان آنلاین: با متغیرهایی از قبیل اینکه آیا فرد شبکه اجتماعی و یا وبلاگ خود را برای دسترسی محدود کرده است یا خیر، آیا پاسخ دهنده از یک ردیاب آنلاین برای مشاهده کسانی که از شبکه اجتماعی یا وبلاگ آنها بازدید کرده‌اند استفاده می‌کند یا خیر، مورد ارزیابی قرارگرفت. نتایج نشان داد افرادی که به طور منظم اطلاعات شخصی و تصاویر خود را آشکار می‌کنند و از یک نرم افزار امنیتی جهت محافظت از اطلاعات خود استفاده نمی‌کنند، آسیب‌پذیری بیشتری برای بزه‌دیدگی دارند؛ زیرا، مجرمان به سهولت به اطلاعات آنها دسترسی دارند (Reyns،۵،۲۰۱۸).

بدین ترتیب، نظریات مذکور با بحث پیشگیری وضعی در ارتباط می‌باشند. پیشگیری وضعی نیز مانند نظریه فعالیت روزانه بر بزه‌دیدگان جرم تمرکز می‌کند و در پی آن است که راهکارها و تدابیری را اعمال کند تا فرد بزه‌دیدگی خود را تسهیل نکند. به همین علت، در پیشگیری وضعی با مصون کردن اهداف، بزهکاران را از ارتکاب جرم منصرف می‌کنیم و این انصراف از ارتکاب جرم موجب پیشگیری از بزه‌دیدگی افراد می‌شود. در حقیقت، هدف پیشگیری وضعی کاهش فرصت‌های ارتکاب جرم است. زیرا جرایم به دلیل وجود فرصت‌های جنایی رخ می دهند. به عنوان مثال اگر چه قرار دادن اشیاء جلوی مغازه ممکن است باعث افزایش دید و در نتیجه فروش آنها شود، اما سرقت آنها را راحت‌تر می‌کند؛ در حالی که قرار دادن آنها در پشت یک پیشخوان این فرصت را از بین می‌برد. همچنین یافته‌های این پیشگیری حاکی از آن است که غالبا افراد پس از سنجش هزینه‌ها و منافع ناشی از جرم، مرتکب جرم می‌شوند. در این راستا، اگر مجرمین دریابند که منافع ناشی از جرم بیشتر از هزینه‌ها هستند، به احتمال زیاد مرتکب جرم می‌شوند. اما اگر بدانند هزینه‌های ارتکاب جرم بیش از منافع آن است؛ از ارتکاب جرم منصرف می‌شوند. لذا، این پیشگیری بر آن است که با افزایش تلاش، افزایش خطرات و کاهش پاداش فرصت‌های جنایی و در نتیجه جرم را کاهش دهد.

بنابراین، از آنجا که فعالیت‌های آنلاین افراد و قرارگرفتن در معرض موقعیت‌های خطرناک از اهمیت ویژه‌ای در ایجاد فرصت‌های جرم کمین سایبری برخوردار است؛ هرچه فرد کمتر در معرض مجرمین سایبری قرارگیرد، فرصت کمتری برای وقوع این جرم وجود دارد. نتایج تحقیقات صورت‌گرفته در این خصوص این جرم نشان می‌دهد که غالبا بزدیدگان این جرم با افشای اطلاعات شخصی، خود را در معرض مجرمین با انگیزه قرار می‌دهند. به همین دلیل است که بسیاری از تکنیک‌های پیشنهادی بر تدابیری متمرکز هستند که میزان قرارگرفتن بزه‌دیدگان در معرض مجرمین را کاهش دهد. به عنوان مثال، یکی از تدابیر مناسب در این خصوص ناشناخته ماندن افراد در اینترنت است که از رهگذر

اقداماتی مانند استفاده از نام مستعار، پنهان کردن جنسیت، سن، مکان، حفظ اطلاعات شخصی و محدود کردن دسترسی به آنها و استفاده از ایمیل متفاوت برای ثبت نام در شبکه‌های اجتماعی حاصل می‌شود. این تدابیر موجب سخت شدن اهداف و در نتیجه افزایش تلاش برای مجرمین بالقوه می‌گردد.

افزایش خطر نیز با اقداماتی از قبیل گسترش نگهبان و استفاده از مدیریت مکان حاصل می‌گردد. به عنوان مثال، مدیران مکان، توانایی بدست آوردن آدرس ایمیل را دشوارتر می‌کنند و می توانند ارائه آدرس ایمیل را منوط به تأیید هویت افراد نمایند که این نیز راهی برای تلاش بیشتر برای مجرمین بالقوه است. گسترش نگهبان نیز با سهولت در خصوص گزارش رفتارهای نادرست دیگران محقق می‌شود. بسیاری از تاکتیک‌های ذکر شده در کاهش پاداش نیز تأثیر دارند. کاهش پاداش مستلزم پنهان کردن اهداف(محدود کردن دسترسی به صفحه شبکه اجتماعی فقط برای دوستان) و از بین بردن اهداف(مسدود کردن پیام‌های ناشناس) می‌باشد.

در تهران تحقیقی میان کارشناسان رشته‌های تحصیلی کامپیوتر، فناوری اطلاعات، علوم کامپیوتر و مخابرات به منظور شناسایی میزان تأثیر راهبردهای پیشگیری وضعی در جهت پیشگیری از آسیب‌های فضای مجازی صورت گرفته است. نتایج حاکی از آن است که افزایش خطرات، تلاش جهت ارتکاب جرم و کاهش منافع ناشی از ارتکاب جرم در فضای مجازی، تأثیر بسزایی در پیشگیری از آسیب‌های فضای مجازی دارد. مطابق یافته‌های این تحقیق، رمزگذاری روی فایل‌ها، پوشه‌ها و رایانه، استفاده از اینترنت با دریافت شناسه کاربری و رمز، نصب ویروس یاب و به روز نگه داشتن آن روی یارانه، از جمله اقداماتی‌ست که به کارگیری آنها احتمال بزهدیدگی افراد را کاهش می‌دهد(شاه محمدی، ۱۳۹۵،ص ۱۳۱).

بر این اساس، با توجه به نظریات مذکور در تبیین بزه‌دیدگی کمین سایبری، غالبا شخصی بزه‌دیده می‌شود که هدفی در دسترس و جذاب برای مجرم باشد و یک سرپرست

توانا که مانع وقوع جرم باشد را دارا نباشد. تحقیقات انجام شده در خصوص بزه‌دیدگان این جرم نیز نشان داد که بزه‌دیدگان کمین سایبری با انجام رفتارهای پرخطر نقش عمده‌ای در تسهیل وقوع جرم دارند. به همین جهت برای پیشگیری از این امر آنها باید تدابیر امنیتی لازم را در فعالیت‌های فضای مجازی خود تمهید نمایند تا کمتر در معرض خطر مجرمان با انگیزه قرار گیرند.

برآمد

رشد و توسعه فناوری اطلاعات و ارتباطات اشکال جدید و پیچیده‌ای از جرایم را به وجود آورده است که با نوع سنتی آن‌ها تمایزاتی دارد. جرم کمین سنتی یکی از جرایم علیه اشخاص است که با افعال مداوم و مکرر تهدیدآمیز به منظور اعمال کنترل بر قربانی صورت گرفته و موجب احساس ناامنی فرد قربانی می‌گردد که امروزه تحولات کنونی در فضای اینترنت وقوع آن را در فضای سایبر نیز امکان پذیر نموده است. کمین سایبری نسبت به کمین سنتی یک مشکل اجتماعی واقعی و جدی‌تر تلقی می‌شود که به سرعت افزایش پیدا کرده است و می‌تواند اثرات مخربی را برای قربانیان به همراه داشته باشد. در حقیقت، علی رغم وجود اشتراکاتی که میان جرم کمین سایبری و کمین سنتی در ویژگی رفتار مجرمانه، شرط بودن تهدید معتبر، ترس شخص معقول و عمدی بودن جرم وجود دارد؛ تفاوت‌های موجود در فرایند ارتکاب این جرم، امکان دستگیری و شناسایی مرتکبان جرم کمین سایبری را با مشکل مواجه کرده است.

در این راستا، کاربران باید با اتخاذ تدابیر امنیتی اطلاعات و داده‌های شخصی خود را محرمانه نگه دارند و از انجام رفتارهای پرخطری که آنها را در معرض مجرمین با انگیزه قرار می‌دهد، اجتناب نمایند. مسلم است برای پیشگیری از این جرم، تدوین قانونی جامع و اجرای آن نقش بسزایی دارد. قانون‌گذار بایستی در راستای کاهش حجم جرایم کمین سایبری و کاهش احتمال بزه‌دیدگی مکرر افراد به وضع قانون‌گذاری جدید در خصوص جرم کمین سایبری و همچنین جرم کمین سنتی بپردازد تا از این رهگذر در جهت حفظ مهم‌ترین جلوه‌های حقوق بشری افراد گام بردارد و تا حد امکان امنیت و آسایش جامعه و بالتبع آن آسایش افراد را ارتقا و بهبود بخشد.

ضمن اینکه، آموزش و آگاه‌سازی مردم در این خصوص نیز یکی از برنامه‌ها و اهداف اصلی تدابیر پیشگیرانه است. اتخاذ برنامه‌های آموزشی برای کاربران فضای مجازی در خصوص به کارگیری صحیح تدابیر امنیتی و حمایتی، می‌تواند فرصت‌های

ارتکاب این جرایم را سخت و محدود نموده و از بزه‌دیدگی قربانیان بالقوه پیش‌گیری نماید. به عبارت دیگر، یکی از اهداف برنامه‌های آموزشی افزایش آگاهی افراد در خصوص عوامل خطر موجود در فضای سایبری و سنتی و آگاهی آنها نسبت به نحوه اتخاذ تدابیر حمایتی برای مقابله و خنثی سازی با عوامل خطر است. در حقیقت، مجرمین افرادی حسابگر هستند که قبل از وقوع جرم هزینه‌ها و منافع ناشی از جرم را مورد محاسبه قرار می‌دهند. اگر منافع جرم بیش از هزینه‌های جرم باشد؛ مرتکب رفتار مجرمانه می‌شوند؛ اما اگر هزینه‌های ناشی از جرم بیش از منافع آن باشد از ارتکاب جرم منصرف می‌شوند. در این راستا، می‌توان با اتخاذ تدابیر پیشگیرانه وضعی از قبیل سخت کردن آماج جرم و سخت کردن شیوه‌های ارتکاب جرم همراه با افزایش امکان شناسایی و دستگیری مجرمین، بزهکاران بالقوه را از ارتکاب جرم منصرف نمود.

منابع

الف) فارسی

۱.کتب

باستانی، برومند، (۱۳۸۳)، ***جرائم کامپیوتری و اینترنتی جلوه نوینی از بزهکاری***، چاپ اول، انتشارات پیام

۲. مقالات

پورقهرمانی، بابک، (۱۳۹۱)، "اخلاق رایانه ای اصول و قواعد آن از منظر اسلام و مقررات بین‌المللی و داخلی"، ***فصلنامه علمی پژوهشی فقه و مبانی حقوق اسلامی***، سال چهارم

جوان جعفری، عبدالرضا،(۱۳۸۹)، "جرایم سایبری و رویکرد افتراقی حقوق کیفری"، ***مجله دانش و توسعه***،سال هفدهم

شاه محمدی، غلامرضا،(۱۳۹۵)، راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی"***فصلنامه مطالعات راهبردی ناجا***، سال اول

علیوردی نیا، اکبر؛ ملک دار، اعظم، (۱۳۹۱)، "***جرایم رایانه ای: نوع شناسی و تبیین نظری از دیدگاه جرم شناسی***"،گزیده مقالات همایش پیشگیری از آسیب های اجتماعی، سازمان بهزیستی کشور، تهران

لک، بهزاد، (۱۳۹۱)،"شناسایی و پیشگیری ازکمین سایبری در فضای مجازی"، ***کارآگاه***، سال پنجم،

یزدانی زنوز، هرمز، (۱۳۸۸)،"***حریم خصوصی در فضای سایبر***"، مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات، معاونت حقوقی و توسعه قضایی قوه قضاییه، چاپ اول

نجفی ابرندآبادی، علی حسین،(۱۳۹۱)،"***تقریرات جرم‌شناسی***"، ویراست هفتم

ب) انگلیسی

Chandrashekhar .A .M. 2016 ,.***Cyber stalking and Cyberbullying :Ef-***

fects and prevention measure

Vasiu .Ioana .2013 .***Cyber stalking Nature and Response Recommendations***

Fisher.Bonnie S .2012 .***Protection Against Pursuit :A Conceptual and Empirical Comparison of Cyber stalking and Stalking Victimization among a National Sample***

Sissinga .Shandre kim .2013. ***criminological exploration of cyber stalking in South Africa***

Baum. Katrina.2009.,***Stalking Victimization in the United State***s

Paullet. Karenl. 2013.***cyberstalking :an exploratory study of law enforcementin allegheny county ,***pennsylvania

Patel .Rutu Mohin .2104. ***Preventive Majors for Protection against Cyber Stalking***

Goodno .Naomi Harlin .2007.***Cyber stalking ,a New Crime :Evaluating the Effectiveness of Current State and Federal laws***

Gregorie. Trudy M .2001.***Cyber stalking :Dangers on the Information Superhighway***

Schwartz. Kate E .2009. .***Criminal Liability for Internet Culprits :The Need for Updated State Laws Covering the Full Spectrum of Cyber Victimization***

Jones .Richard . 2007 .***Regulating Cyberstalking***

Pittaro .Michael L.2007 .***Cyber stalking :An Analysis of Online Harassment and Intimidation2007***

Agustina .Jose R .2105، ***Understanding Cyber Victimization :Digital Architectures and the Disinhibition Effect***

Halder ،Debarati .2015.***Cyber Stalking Victimisation of Women :Evaluating the Effectiveness of Current Law in India from Restorative Justice and Therapeutic Jurisprudential Perspectives***

Bocij،Paul .2003 ، ***Victims of cyberstalking :An exploratory study of harassment perpetrated via the Internet***

Ashcroft ،John،2001 .***Report to Congress on Stalking and Domestic***

Violence

Lynne .Roberts،2008 ،***Jurisdictional and definitional concerns with computer-mediated interpersonal crimes :An Analysis on Cyber Stalking***

Short،Emma،2015 .***The Impact of Cyberstalking***

Reyns ،Bradford W،2011. ***Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization***

Thapa،Anju،2011 .***Cyber stalking :crime and challenge at the Cyber space***

Reyns ، Bradford،2010 .***Being Pursued Online :Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective***

Petrocelli ,J .(2005) .***Cyber stalking .Law and order***.

Salimi،Ehsan.2014، ***The Criminology of Cyber Stalking :Investigating the Crime ,Offenders and Victims of Cyber Stalking***

Mishler،Joanna،2000،***Cyberstalking :Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if It Does***

Phillips،Elizabeth،2015،***Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending***

Chik،Warren،2008،***Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking***

Reyns،Bradford،2010،***A situational crime prevention approach to cyberstalking victimization :Preventive tactics for Internet users and online place managers***

Reyns،Bradford ،2018،***Explaining Cyberstalking Victimization Against College Women Using a Multitheoretical Approach: Self-Control ,Opportunity ,and Control Balance.***