

تحلیل جرم‌شناختی جرایم سایبری

علیرضا مشیراحمدی

دانشجوی دکترا حقوق جزا و جرم‌شناسی دانشگاه فردوسی مشهد، مشهد، ایران
moshir.alireza@yahoo.com

چکیده

شكل‌گیری و توسعه شبکه جهانی اینترنت، نقشی اساسی در ظهور و بروز بزه‌کاران و بزه‌های نوین داشته است. وابستگی روزافزون کشورها به اینترنت و تحولات سریع فناوری‌های جدید نیز بر میزان این آسیب‌پذیری افزوده است. این در حالی است که برخلاف حصول پیشرفت‌های بسیار در عرصه‌های مادی، جوامع بشری از منظر حقوقی و مقابله با جرایم سایبری وضع مطلوبی نداشته و در این زمینه موفق عمل نکرده‌اند. چنین موضوعی سبب شده تا در طول دو دهه گذشته جرایم سایبری به یک چالش بحث‌برانگیز در پژوهش‌های جرم‌شناسان و یک نگرانی رو به رشد برای سیاست عمومی بدل شود؛ بنابراین لازم است تا برای درک صحیح و جلوگیری از این جرایم، همه ابعاد لازم در این خصوص مورد توجه قرار گیرد. در این مقاله قصد داریم تا ضمن تبیین مفهوم، خصوصیات و چالش‌های موجود در مواجهه با جرایم سایبری، تدبیر پیش‌گیرانه و مقابله با آن را نیز مورد بررسی قرار دهیم.

وازگان کلیدی: جرایم سایبری، محیط سایبری، پیش‌گیری کیفری، پیش‌گیری غیر کیفری

۱- مقدمه

امروزه فضای مجازی تبدیل به دنیای مستقل شده و باید گفت، دنیای مجازی دیگر تنها عنوانی از مجاز بودن را با خود یدک می‌کشد. کمتر فعالیتی است که در جهان واقعی در حال رخدادن باشد و نتوان اثری از آن در دنیای مجازی نیافت. تحقق جرایم نیز از این قاعده مستثنی نبوده و اندک جرمی در کره خاکی است که در حال وقوع بوده ولی در فضای مجازی امکان تحقق نداشته باشد؛ پس به موازات دنیای واقعی، جرایم در دنیای مجازی نیز در حال شکل‌گیری است. بنابراین پیوندی ناگسستنی میان دنیا یا فضای واقعی و مجازی برقرار بوده و هر روز نیز بر این آمیختگی و وابستگی افزوده می‌شود. شاید در وهله نخست این چنین تصور شود که اتفاق و تغییر خاصی به وجود نیامده و فقط وسیله ارتکاب جرم است که دگرگون شده، اما این تغییر را باید از دو جهت حائز اهمیت دانست؛ نخستین اهمیت از عدم یا تأخیر هماهنگی ناشی می‌شود، به شکلی که به نسبت سایر تحولات رخداده، جوامع پسری نتوانستند خود را به لحاظ حقوقی با آن هماهنگ کنند. به تعبیری دیگر، سرعت هماهنگی و برنامه‌ریزی به منظور مقابله با جرایم حادث شده در فضای مجازی با سرعت بسیار پایینی صورت می‌پذیرد. به عنوان مثال تحولات ایجاد شده در صنعت حمل و نقل، عاملی در شکل‌گیری جرایم نوین شد؛

اگرچه ورود و بهره‌گیری از هواپیما سبب تسريع و سهولت در حابه‌جایی مسافران شد، اما جرایم را نیز بهمانند هواپیماریایی به دنبال داشت. در چنین حوزه‌هایی بشر توانست با فاصله زمانی اندکی از حیث شیوه‌های قانونی، پیش‌گیری و مقابله خود را با جرایم هماهنگ کند. در حالی که تحولات رخداده در زمینه جرایم سایبری به هیچ عنوان با تحولات حقوقی لازم در این زمینه منطبق نبوده و هرچه زمان می‌گذرد نیز این فاصله بیشتر می‌شود. تفاوت ماهوی در شکل‌گیری جرایم در این حوزه با جرایم دنیای واقعی را باید دو میان اهمیت موجود در این زمینه دانست. عاملی که موجب می‌شود ضرورت تفکیک تعاریف، مبانی و معیارهای جرم و جرم‌انگاری در این دو حوزه از یکدیگر احساس شود. به عنوان مثال نمی‌توان تعريفی واحد از سرقた را چه در فضای سایبر و چه در دنیای واقعی به کار بست. زیرا اگرچه در جهان واقعی مالی ربوه می‌شود، اما در محیط سایبر عملیاتی نسبت به اصل مال صورت نمی‌پذیرد. و یا در کلاهبرداری‌های سایبری، توجه به عنصر فریب فاقد موضوعیت خواهد بود، زیرا در این فضا آماج و هدف انسان نیست تا فریقتن او مصدق پیدا کند. این موضوعات عاملی خواهد بود تا بررسی و توجه به جرایم سایبری حائز اهمیت تلقی شده و نیاز به شناسایی، مقابله و پیش‌گیری از آن نیز بیش از پیش احساس شود. به همین منظور در ادامه نخست به تبیین مفهوم، طبقه‌بندی و

از رایانه و شبکه به عنوان ابزاری برای انجام آن جرم استفاده کند جرم سایبری است. [۵] بر اساس تعریفی دیگر، جرایم سایبری اصطلاحی است که در ارتباط با شرکت در فعالیت‌های غیرقانونی و با استفاده از فناوری رایانه‌ای تحقق می‌یابد. [۶] هم‌چنین عده‌ای برای توصیف این جرایم، از اصطلاحاتی مانند جرایم عصر ارتباطات و جرایم مرتبط با فناوری مدرن بهره جسته‌اند. عده‌ای نیز هر عمل جنایی را که شامل استفاده از ارتباطات، رایانه و شبکه اینترنت باشد، یعنی قابل ارتکاب در محیط مجازی و اینترنت باشد، جرم اینترنتی نامیده‌اند. [۷] و [۸] دسته دوم تعاریف ارائه شده را باید سرچشمه‌گرفته از نظرات مراجع و سازمان‌های جهانی و بین‌المللی دانست. جنبه جهانی و فرامللی جرایم سایبری موجب شد تا این مراجع در صدد ارائه تعریف واحد از این جرایم و به‌تبع آن تلاش برای ایجاد نوعی سیاست جنایی واحد برای کشورها برآیند. در همین راستا سازمان همکاری و توسعه اقتصادی^۳ این جرایم را شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار و انتقال داده‌ها دانست. [۹] بر پایه تعریف ارائه شده از جانب انجمان بین‌المللی جزا^۴ نیز بزه سایبر، جرایمی است که در فضایی غیر فیزیکی بر ضد داده‌های ناشی‌شده از فناوری اطلاعات قابل ارتکاب است. [۱۰] جامعه حقوق‌دانان آمریکا و کانادایی نیز بر این عقیده‌اند که هرگونه فعالیت مجرمانه که حاوی استفاده غیرمجاز، رونوشتبرداری ناروا، جابه‌جایی، سوءاستفاده از دستگاه‌های رایانه‌ای، عملکرد رایانه‌ها یا برنامه‌های رایانه‌ای باشد، جرم سایبری نامیده می‌شود. [۱۱] از نظر سازمان ملل نیز ابزار به کاررفته در ارتکاب جرم حائز اهمیت بوده و بنابر تعریف ارائه شده از این سازمان، جرایم سایبری ممکن است، در بردارنده فعالیت‌های مجرمانه‌ای باشد که ماهیتی سنتی دارند؛ اما با استفاده از ابزاری مدرن و نوین از جمله اینترنت، رایانه و دیگر ابزارهای تشکیل‌دهنده فضای سایبر محقق می‌شود. [۱۲]

مجموعه‌ای این تعاریف درواقع، نگرشی دوگانه را نسبت به جرایم سایبری مطرح کرده‌اند، با این توضیح که تمرکز برخی از تعاریف بالا، در بردارنده مفهومی مضيق از این جرایم بوده و بر همین مبنای جرایم سایبری را بزه‌هایی دانسته‌اند که

از این راه به حساب‌های مخصوصی واریز کرده و در فواصل زمانی معین اقدام به برداشت از این حساب‌ها می‌کرد، اما درنهایت چون شوهای برای متوقف‌سازی این عملکرد پیش‌بینی نشده بود وی با مراجعه به مراجع قضائی، اعتراف به این جرم کرد.

³ O.E.C.D

⁴ AIDP

چالش‌های ناشی از ظهور جرایم سایبری پرداخته می‌شود و سپس چگونگی پیش‌گیری و مقابله با این جرایم مورد بررسی قرار خواهد گرفت.

۲- مفهوم‌شناسی جرایم سایبری

سرآغاز تعیین وقوع نخستین جرم سایبری نامعلوم است، هرچند عده‌ای آن را به سال ۱۸۷۸ و هم‌زمان با اختراع تلفن نسبت داده‌اند.^۱ اما آغاز توجه جدی به این گونه جرایم را باید با ماجرای رویس مرتبط دانست.^۲ [۱] این موضوع توجه حقوق‌دانان و جرم‌شناسان را برای کشف توصیف عنوان مجرمانه در این خصوص به دنبال داشت؛ سپس گسترش و توسعه رایانه‌های شخصی در اوایل دهه ۱۹۸۰، ایجاد شبکه جهانی در سال ۱۹۹۰، فزونی و رویه روبرو شدن ایجاد و استفاده از شبکه‌های اجتماعی در فضای سایبر در سال ۲۰۰۰ فرصتی بی‌سابقه برای ورود اشخاص به اینترنت و به‌تبع آن جرایم مرتبط با این حوزه را فراهم آورد. این عوامل موجب شد تا کوشش‌ها برای تعیین مصاديق و تشریح این چنین اعمالی بیشتر شود. به طور کلی باید گفت، به‌منظور تبیین و تعریف این جرایم، نظرات بسیاری ارائه شده، اما با توجه به گستردگی و عدم تعیین دقیق مصاديق، اجتماعی در این خصوص حاصل نشده است. قانون‌گذاران کشورهای مختلف، حقوق‌دانان، جرم‌شناسان و اسناد بین‌المللی و منطقه‌ای هر یک به فراخور تهدیدات و نیازهای تعاریف متفاوتی را در این رابطه ارائه کرده‌اند که در ادامه به برخی از آن‌ها اشاره می‌کنیم:

دسته نخست تعاریف ارائه شده در این خصوص را باید به حقوق‌دانان، جرم‌شناسان و دیگر فعالان حاضر در این حوزه منتسب دانست. در همین راستا عده‌ای معتقدند هر جرمی که شامل اینترنت و رایانه باشد جرم سایبری بوده، هرچند خیلی نیز وابسته به رایانه نباشد. [۲] در مقابل برخی دیگر این جرایم را دسته‌ای از بزه‌ها دانسته‌اند، که اگرچه در فضای اینترنت و محیط‌های مجازی ظهور می‌یابند، اما متوجه جرایم ارتکابی از طریق رایانه و یا جرایم متمرکز بر رایانه نیز می‌شوند. [۴] نزدیک به همین تعریف، گفته شده که هر جرم و جنایتی که

^۱ شرکت بل اقدام به استخدام تعدادی از نوجوانان به‌منظور پاسخ‌گویی و متصل کردن تماس‌های تلفنی به مشترکان کرد. این افراد علاوه‌بر توهین و برخورد نامناسب با مشترکان، با ترفندی‌های هوشمندانه در صفحه سوئیچ انصال، به قطع تماس‌های تلفنی و اعمالی این چنینی مبادرت می‌ورزیدند. مهارت و توانایی کافی و ناشناس‌بودن این اشخاص عواملی بودند که موجب بروز این مشکلات شد. [۲]

^۲ رویس حسابدار یک شرکت بود که با افزودن دستور العمل‌های اضافی به برنامه حسابداری شرکت، قیمت کالاها را با خلافت خاصی تغییر می‌داد؛ و ارقام حاصله

تحول سه عصر یا دوره متفاوت است. عصر نخست به زمان ایجاد نخستین دستگاه‌های رایانه‌ای و عمومیت ابتدایی و اولیه استفاده و به کارگیری از آن‌ها باز می‌گردد. در این دوره بر حسن‌ترین فعالیت‌های ناروا و غیرقانونی شامل ایجاد اختلال در عملکرد دستگاه‌های رایانه‌ای و دستگاری داده‌ها بود. دلیل شکل‌گیری چنین اعمالی را باید ناشی از آن دانست که استفاده از اینترنت در آن زمان رواج و شیوع کنونی را نداشته و بدین جهت عمدۀ جرایم ارتكابی در ارتباط با رایانه‌ها بود که محقق می‌شد.^{۱۵} ویژگی اصلی اعمال دوره نخست آن بود که این‌گونه اقدامات غیرمجاز در وسعتی کم تحقیق یافته و مقابله با آن نیز واجد رویکردی امنیتی بود.^۱ محوریت نسل دوم این جرایم را که باید آن را حلقه واسط میان نسل نخست و سوم نامید، مبتنی برداده‌ها و محافظت از آن بود. بر همین مبنای دستگاه‌های رایانه‌ای در صورتی این‌محسوب می‌شند که داده‌های آن‌ها واجد سه عنصر محترمانگی^۲، تمامیت^۳ و دسترس پذیری^۴ بودند. منظور از نخستین مؤلفه حفاظت داده‌ها در برابر دسترسی یا افشا غیرمجاز است. دومین مؤلفه نیز حاکی از حفاظت داده‌ها نسبت به هرگونه آسیب یا تغییر است. در دسترس قراردادشتن داده‌های مجاز که متعاقب حفاظت مطلوب از دستگاه‌ها صورت می‌پذیرد نیز مبنی مؤلفه سوم است؛ بنابراین در این دوران اقداماتی که منجر به افشا یا در دسترس قرارگرفتن داده‌ها شده و یا نقص و تغییر در آن‌ها به وجود می‌آورد، جرم نامیده می‌شد. اگرچه بازه زمانی این دوره از جرایم کوتاه بوده و با فاصله‌اندکی جرایم عصر سوم ظهرور یافت، اما مؤلفه‌های یادشده در این دوره، نقشی مهم و اساسی را در تحولات آینده مربوط به نگرش به جرایم سایبری در پی داشتند.^۵ عصر سوم نیز که از اویل دهه ۹۰ تبلور یافت، باید مرتبط و نشأت‌گرفته از رشد فناوری و توسعه استفاده از شبکه جهانی وب دانست. رشد شتابان استفاده از ابزار دیجیتال و آمیختگی آن با سامانه‌های مخابراتی و اینترنتی عاملی مهم در شکل‌گیری نسل سوم جرایم بود. با این توضیح که در دهه ۹۰ میلادی گسترش فعالیت‌های مرتبط با هک و اخلال در شبکه‌های رایانه‌ای به بحران تبدیل شد. دوره بین سال‌های ۱۹۸۰ و ۲۰۰۱ نیز رشد بالایی در

^۱ چنین رویکردی در فهرست ارائه شده به وسیله سازمان توسعه و همکاری اقتصادی در سال ۱۹۸۶ نیز قابل مشاهده است.

² Confidentiality
^۳ Integrity
^۴ Accessibility

^۵ برای نمونه در بخش اول از فصل دوم کتوانسیون جرایم سایبری که در سال ۲۰۰۱ در بوداپست به تصویب رسیده، با مبنا قرار گرفتن این سه مؤلفه، طی ۵ ماده جرایم دسترس غیرقانونی، شنود غیرقانونی، ایجاد اختلال در سیستم و سوء استفاده از دستگاه‌ها مورد توجه تصویب کنندگان قرار گرفته است.

در بستر فناوری و با روش‌های جدید صورت می‌گیرد، در مقابل مورد توجه قرارگرفتن مفهوم گستردۀ یا توصیفی از این جرایم سبب شده تا طیف گستردۀ از جرایم که گاهی با شیوه‌های به طور کامل نوین و گاهی نیز به شکل سنتی و با استفاده از فناوری جدید ارتکاب می‌یابند، به عنوان جرایم سایبری معرفی شوند.^{۱۶} وجود این دو یا چندگانه‌ای‌ها و عدم وجود اجماع در ارائه تعریفی از جرایم سایبری و بروز اختلاف در تبیین این جرایم، عده‌ای را بر آن داشته که این‌گونه اظهارنظر کنند که ارائه هرگونه تعریفی از رایانه، برنامه و داده بی‌فاایده است؛ زیرا سرعت تغییرات فناورانه به‌زودی هرگونه تعریفی از این قبیل را بی‌استفاده خواهد کرد؛^{۱۷} اماً چنین تفسیری قابلیت دفاع خواهد داشت؛ زیرا نخست این که عدم تعریف این جرایم موجب ناشناختگی آن‌ها شده و ناتوانی دولت‌ها در برنامه‌ریزی، پیش‌گیری، مقابله و تخمین میزان خسارت وارد را به‌دنیال خواهد داشت. دوم این که بزه‌دیدگان نیز به‌دلیل فقدان تعریف، در احراق حق خویش دچار سردرگمی شده و معیاری برای طرح شکایت خویش نخواهند داشت. سوم این که دستگاه قضا نیز در نحوه رسیدگی به این جرایم دچار آشفتگی شده و در اجرای عدالت که از مهم‌ترین آرمان‌های این دستگاه است با چالش مواجه خواهد شد. درنتیجه لازم می‌آید تا تعریفی از این جرایم ارائه شود، هرچند در توصیف و تبیین مصاديق آن همانه‌گی کامل میان مراجع داخلی و بین‌المللی وجود نداشته باشد. به عنوان جمع‌بندی می‌توان گفت که جرایم سایبری فعالیت یا مجموعه اقداماتی است که با بهره‌گیری از امکانات فناورانه که در محیط سایبر و با اهداف غیرقانونی و نامشروع ارتکاب می‌یابد.

۳- انواع جرایم سایبری

اغلب نوع زاویه نگاه به شکل‌گیری جرایم سایبری، عامل اساسی در تعیین طبقه‌بندی‌های موجود است. از همین رو مبانی مختلفی نیز برای تفکیک این جرایم از یکدیگر ارائه شده است. گاهی بررسی سیر تکاملی و تحولات انجام‌گرفته در دوران مختلف، مبنای طبقه‌بندی جرایم سایبری بوده است. گاهی نیز توجه به معیارهایی چون محوریت نقش رایانه، موضوع جرم یا تلفیقی از این موارد، سبب ارائه دسته‌بندی از جرایم سایبری شده است.

۳-۱- معیار سیر تکاملی و ادواری

اگر بر پایه تحولات صورت گرفته در ادوار مختلف به موضوع بنگریم، آنچه را که امروزه جرم سایبری می‌نامیم، حاصل

موضوعاتی عینی و قابل مشاهده بوده و گاه نیز شامل موضوعاتی غیر عینی که در حقیقت همان قابلیت و کارکرد موضوعات سایبری (داده‌ها و سیستم) است، می‌شوند. بر همین مبنای جرایم رایانه‌ای را به دو دسته جرایم سنتی و سایبری محض تقسیم کرده‌اند. دسته نخست دربردارنده جرایمی می‌شود که همانند آن در محیط فیزیکی نیز قابل مشاهده است. به عبارتی دیگر این‌گونه از جرایم همان جرایم سنتی‌اند که در فضای سایبر نیز به وقوع پیوسته و می‌توان این‌گونه جرایم را حاصل مهاجرت از محیط فیزیکی به محیط سایبر دانست.^۳ پس برخی از جرم‌انگاری‌های صورت‌گرفته در فضای سایبر درواقع همان موضوعاتی‌اند که در فضای واقعی، هدف رفتارهای مجرمانه قرار می‌گیرند؛ به عنوان مثال در دنیای واقعی با جرایم اقتصادی، ضد حقوق فردی و یا برخلاف منافع جمعی مواجهیم که شبیه به این جرایم در محیط سایبر نیز تحقق می‌یابد از قبیل کلامبرداری یا جعل رایانه‌ای، جرایم بر ضد امنیت ملی. به این طبقه‌بندی دو ایراد اساسی را می‌توان وارد ساخت. از یکسو بخش عمدۀ جرایمی تحقیق‌بافته در دنیای واقعی قابلیت ارتکاب در فضای سایبر را ندارند و یا بسیاری از جرایم وجود دارند که فقط در فضای سایبر به وقوع می‌پیوندند و نمی‌توان اثری از آن را در محیط واقعی و ملموس یافت. از سویی دیگر اگرچه به نوعی مشابهت در تحقیق برخی جرایم در هر دو فضا قابل مشاهده است، اما باید گفت از نظر ماهیت و کیفیت ارتکاب تفاوت بسیاری در این دو فضا وجود دارد. دسته دیگر شامل جرایمی است که امکان وقوع آن در فضای فیزیکی وجود ندارد. به این معنا که ارتکاب این‌گونه از جرایم مختص محیط سایبر بوده و به‌الازام در این فضا تحقق می‌یابد.^۴ [۱۷]

مقصود از موضوعات سایبر در اینجا سیستم‌ها، شبکه‌ها و اطلاعات و یا هر چیز دیگری است که مرتبط با این موارد باشد. اگرچه این تقسیم‌بندی از نظر ارائه مصادیق خاص و تعداد آن با مشکل رو به رو است، ولی از دیدگاه حقوقی باید آن را بهترین و دقیق‌ترین دسته‌بندی دانست؛ زیرا در اینجا شاهد هم‌پوشانی بین جرایم نوع سنتی و سایبری نبوده و به‌واقع این بزه‌ها هستند که مبین نوع نوین جرایم‌اند.

^۳ جرایمی مانند جعل و کلامبرداری رایانه‌ای، جاسوسی رایانه‌ای، هرزه نگاری اینترنتی، نقش حریم خصوصی ... در این دسته قابل ذکر اند.

^۴ جرایمی از قبیل دسترسی غیر مجاز به اطلاعات یا سامانه‌های رایانه‌ای، حذف یا تخریب غیر مجاز داده‌ها یا حامل‌ها از سامانه‌های رایانه‌ای، پخش برنامه‌های مخرب نظیر ویروس‌ها و کرم‌ها در فضای سایبر و در این دسته قرار می‌گیرند.

حملات رایانه‌ای گزارش شده است. گسترش بهره‌گیری از اینترنت و پوشش خبری گستردۀ حملات ویروسی و سایبری دو عامل اساسی بودند که در این رشد بسیار اثرگذار بودند. به‌طورکلی خصوصیات و ویژگی‌های شکل‌گرفته در این دوره که منشأ اثر در دوران بعدی بود و روزبه‌روز نیز بر قابلیت‌های آن افزوده شد، عاملی در ترویج و گسترش استفاده از این فضا و به‌دلیل آن رشد جرایم سایبری بود.

۲-۳- معیار نقش رایانه

مشهورترین طبقه‌بندی از جرایم سایبری بر پایه توجه به نقش رایانه انجام‌گرفته است. بر همین اساس بزه‌های سایبری را جرایمی دانسته‌اند که در تحقیق آن رایانه، یا نقش موضوع جرم و یا نقش وسیله جرم را دارد؛ پس هرگاه در دسته‌بندی ارائه شده جرایم از منظر وسیله جرم مورد توجه قرار گیرند، رایانه واحد نقشی فعال فرض شده که بزه به کمک آن تحقق می‌یابد، اما هرگاه از زاویه موضوع جرم به ماجرا تگریسته شود، برای رایانه نقشی منفعل مورد توجه قرار گرفته که موضوع رفتار مجرمانه واقع می‌شود. [۱۶] البته با توجه به آن که در بیان این نوع از طبقه‌بندی، گاهی هم در میزان و نوع مصادیق مجرمانه و هم در کیفیت نقش رایانه، وجود تفاوت مشهود است، غالب جرم‌شناسان و حقوق‌دانان نقش سومی نیز برای رایانه‌ها ملحوظ داشته‌اند که می‌توان از آن به عنوان نقش کمک‌رسان یا مداخله‌گر یاد کرد.^۵ با توجه به این تفاسیر، ارائه طبقه‌بندی بر پایه نقش رایانه را می‌توان شامل موارد زیر دانست:

الف- رایانه به عنوان موضوع یا هدف جرم، در این دسته جرایمی چون اخاذی اطلاعات، سرقت اموال معنوی یا سرقت اطلاعات تجاری جای می‌گیرند.

ب- رایانه به عنوان وسیله جرم، به‌مانند جرایمی از قبیل بول‌شوی یا کلامبرداری رایانه‌ای

ج- رایانه به عنوان مداخله‌گر در ارتکاب جرم، مانند پورنوگرافی^۶

۳-۳- معیار موضوع جرم

این طبقه‌بندی دربردارنده معیارهایی است که رفتار مجرمانه نسبت به آن محقق می‌شود. جرایم داخل در این دسته، گاه

^۵ اگرچه ارائه سومین نقش را می‌توان به نوعی زیر مجموعه‌ای از دسته دوم قرار داد لیکن برخی از حقوق‌دانان بر این عقیده‌اند که با توجه به آن که به‌کارگیری و استفاده از رایانه در تحقیق برخی از جرایم به عنوان وسیله اصلی دخالت داشته و در برخی دیگر از جرایم واحد نقشی فرعی یا اتفاقی است، می‌باشد میان این حالت‌ها تفکیک قائل شد.

⁶ Pornographic

۴-۳- معیار تلفیقی

به آن اختصاص یافته است. جرایمی چون کلاهبرداری، جعل، تخریب، جاسوسی و جرایم مرتبط با مواد مخدر که موصوف به وصف سایبری‌اند در این دسته جای می‌گیرند. در جرایم سایبری علیه محظوا نیز جرایمی از قبیل تحریک به انجام فعالیت‌های غیرقانونی و توهین و اشاعه تفکرات غیرانسانی یا نژادپرستانه جای می‌گیرند. وجه تمایز دسته سوم جرایم را باید توجه به بعد فنی‌شان عنوان کرد. جرایمی چون دست‌یابی غیرمجاز یا استفاده غیرمجاز از داده‌ها در این دسته قرار می‌گیرند. جرایم مخابراتی نیز اگرچه درگذشته به صورت مجزا مورد بحث قرار می‌گرفتند، اما با تلفیق محیط سایبر با حوزه مخابرات جرایم نوبنی شکل گرفت که بخشی از آن مبتنی بر ماهواره و بخشی دیگر فضای سایبر بود؛ درنتیجه پرداختن به آن تحت عنوانی واحد ضروری شد. جرایمی چون شنود غیرمجاز و جرایم مرتبط با ماهواره و موبایل با وصف سایبری در این دسته جای می‌گیرند.^{۱۸]} بر اساس طبقه‌بندی دیگر بزه‌های سایبری را می‌توان مشتمل بر ۱- بزه‌های ضد رازمندی، یکپارچگی و قابلیت دسترسی که شامل بزه‌هایی چون شنود یا دریافت غیرقانونی، دسترسی غیرقانونی و دست‌کاری داده‌ها یا سیستم‌ها می‌شود. ۲- بزه‌های مرتبط با رایانه که شامل کلاهبرداری یا جعل رایانه‌ای می‌شود. ۳- بزه‌های مرتبط با محتوا که دربردارنده بزه‌های مرتبط با هرزه‌نگاری است. و ۴- بزه‌های مرتبط با نقض حق نوشتمن، چاپ و حقوق وابسته به آن است دانست^[۱۶].

۴- چالش‌های جرم‌شناسی حاصل از جرایم سایبری

عمومیت و فراگیری استفاده از اینترنت شکل‌گیری نوع ویژه و نوبنی از جرایم را به دنبال داشته است. اگرچه تحقق برخی از جرایم علاوه بر دنیای واقعی در دنیای مجازی قابل مشاهده است (که البته از نظر شیوه و شرایط ارتکاب، تفاوت میان دو فضا مشهود است)، اما برخی دیگر از جرایم تنها در بستر اینترنت است که ظهور می‌یابند. بنابراین وجه مشترک این جرایم را باید بهره‌گیری از اینترنت و داده‌های^۲ اینترنتی دانست. پس موضوع جرم در این جرایم اینترنت بوده که بزه در آن و یا به وسیله آن محقق می‌شود. به بیانی دیگر شکل‌گیری این جرایم را باید جنبه نهان و توالی ناخواسته

طبقه‌بندی تلفیقی دربردارنده همان دسته‌بندی‌های رایج است. اما با توجه به آن که عده‌ای معتقدند تفکیک دقیق جرایم سایبری از یکدیگر ممکن نیست، لذا لازم است تا عنوانین مشابه در دسته‌های کلی‌تر جای گیرند. به تعبیری دیگر از آنجایی که گاهی امکان دارد معیار یا شیوه ارتکاب برخی از جرایم با یکدیگر همپوشانی یا مشابهت داشته باشد و نتوان آن‌ها را در دسته‌های مشابه جای داد، روى آوردن به چنین معیاری اجتناب‌ناپذیر است. به طور اصولی گزینش چنین شیوه‌ای به وسیله سازمان‌ها، کنوانسیون‌ها و یا در استناد بین‌المللی مورد استفاده قرار می‌گیرد. البته به موازات تلاش‌های مجتمع بین‌المللی؛ حقوق دانان، متخصصان و صاحب‌نظران امر نیز با توجه به مقتضیات پیش‌رو کوشیده‌اند، تقسیم‌بندی‌هایی در این زمینه ارائه دهند. نخستین کوشش‌های متمرکز توسط سازمان‌های بین‌المللی را در تعیین مصاديق بزه‌های سایبری که از مشکلات حقوقی در حوزه جرایم رایانه‌ای ناشی شده بود، باید به اقدامات OECD مرتبط دانست. کمیتی‌ای اختصاصی از این سازمان در یک دوره سه‌ماهه مشغول بررسی کیفری، به منظور مقابله با جرایم همراهی کیفری قوانین کیفری، در تلاش‌ها حاکی از اقتصادی مرتبط با رایانه شد. نتیجه این تلاش‌ها حاکی از جای‌گیری اقدامات مجرمانه در پنج دسته مختلف بود؛ سپس شورای اروپا این میزان را به دوازده مورد رساند که شامل دو فهرست حداقلی و اختیاری می‌شد. سازمان ملل نیز موضوع ویروس‌ها را بر این فهرست افزود که بعدها به وسیله AIDP نقش آن تأکید شد. سازمان‌ها و نهادهای منطقه‌ای و بین‌المللی دیگر از جمله اینترپل و کنوانسیون اروپایی جرایم سایبری نیز تلاش‌های بعدی در تبیین تقسیم‌بندی از این جرایم را به انجام رسانده‌اند. که دسته‌بندی ارائه شده اینترپل بیشتر مبتنی بر اصول پلیسی بوده که فاقد جامعیت و مانعیت کافی است، و دسته‌بندی کنوانسیون اروپایی نیز به صورت حداقلی و جزئی ارائه شده است. به طور کلی دو دسته‌بندی در این خصوص مقبولیت بیشتری یافته‌اند. بر پایه یک تقسیم‌بندی این جرایم را می‌توان شامل ۱- جرایم سنتی با وصف سایبری ۲- جرایم سایبری علیه محظوا ۳- جرایم محض سایبری و ۴- جرایم مخابراتی دانست. در دسته نخست بزه‌هایی جای می‌گیرند که درگذشته نیز وجود داشته‌اند، اما با توجه به تغییرات جزئی یا کلی در عنصر مادی‌شان به عنوان جرایم سایبری از آن تعبیر شده و قوانین مجزا و یا ویژه‌ای نیز

^۱ این جرایم در گذشته فقط شامل هر گونه رفتاری بود که صد ارتباطات تلفنی و مخابراتی ارتکاب می‌یافتد؛ مانند دسترسی غیر مجاز به خطوط تلفن.

^۲ Data

پس ارتکاب جرم در محیط سایبر فاقد یکی از محدودیت‌های موجود در محیط فیزیکی است.

۴-۲-۴- دشواری کنترل جرایم از طرق معمول

در دنیای واقعی راه و شیوه‌هایی برای کنترل جرایم واقعی قابل‌کشف است؛ یعنی امکان توسل به انواع پیش‌گیری‌ها وجود دارد؛ اما در فضای مجازی به دلیل پیچیدگی‌های موجود در جرایم سایبری، حجم بالا، سرعت رشد و عدم شناخت کافی نسبت به این جرایم، کار کنترل راحت نیست. شناسایی الگوی ارتکاب جرم بکی از راههای مقابله با جرایم در دنیای واقعی است، پلیس و ضابطان دادگستری با کشف شیوه‌های شکل‌گیری جرایم با سهولت بیشتری موفق به شناسایی بزهکاران و مجرمان می‌شوند، اما در فضای سایبر با توجه به آن که الگوها به شدت گستردۀ و متعدد بوده و به سرعت نیز تغییر می‌یابند، توسل و دسترسی به چنین ویژگی‌ای میسر نیست. به تعبیری دیگر، در تکرش سنتی به تحقق جرایم، با توجه به شناختی که اغلب بزهده‌ی از بزهکار داشت و یا اشرافی را که ضابطان پلیس نسبت به روش‌های ارتکاب جرم از سوی مجرمان به دست می‌آوردند، امر کشف و شناسایی با سادگی و سهولت بیشتری در ارتباط با جرایم نوین وجود نداشته و بهنوعی چنین قابلیتی در ارتباط با جرایم نوین وجود نداشت و کار جستجو و کنترل دشوارتر می‌شود.

۴-۳- فرامکان و فرازمان بودن

امروزه هر شخص با اتصال به اینترنت قادر است ظرف یک دقیقه یا کمتر از آن با شخص یا اشخاص دیگر در هر نقطه از جهان مرتبط شود. این قابلیت که فرامرزی‌بودن یا جهانی‌شدن^۱ نیز نامیده شده، مؤلفه‌ای در حذف مزهای جغرافیایی محسوب می‌شود. به بیانی دیگر جهانی‌شدن فرایندی اجتماعی است که در آن محدودیت‌های جغرافیایی بر فرهنگ و دیگر ابعاد زندگی اجتماعی انسان‌ها کاهش یافته و موجب نزدیکی اشخاص و فرهنگ‌ها به یکدیگر می‌شود. بنابراین جهانی‌بودن گسترده اینترنت، سبب شده قابلیت ارتباط بین نقاط مختلف و حضور چندگانه در این محیط، از حوزه محلی یا منطقه‌ای به حوزه جهانی ارتقا یابد. همچنین روزآمدی و ظهور امکانات نوین نیز بر بهره‌گیری و استفاده از این محیط افزوده است. به عنوان مثال با استفاده از قابلیت‌های چندرسانه‌ای^۲ امکان برگزاری جلسات ویدئو کنفرانس در سرتاسر جهان نیز به وجود آمده، که دارای ارزش بالایی است. بنابراین با وجود چنین قابلیت‌هایی در محیط سایبر، دیگر تنها

جهانی‌شدن دانست. با جهانی‌شدن ارتباطات، ترقی و تعالی فناوری، سهولت در امر آمدوشد و حذف مزهای گمرکی و سیاسی، بزهکاران نیز از این مواهب به نفع خویش سود جسته و فرصت‌های نوینی را برای ارتکاب جرایم پیدا کرده‌اند.^[۱۹] بنابراین اگرچه موقع این بود که پدیده جهانی‌شدن، توسعه را در سطح جهان فزونی بخشد و برخورداری از صلح، امنیت و آزادی فراگیر را تسهیل کند، اما در مقام عمل دست یابی بی‌ضابطه و غیرقابل‌کنترل به منابع اطلاعاتی، مالی و جغرافیایی خود به عاملی در بروز رفتارهای غیرقانونی بدل شد.^[۲۰] با توجه به این تفاسیر باید گفت که امروزه جرایم سایبری به یک چالش برای جرم‌شناسان بدل شده است؛ زیرا که نخست این که به سرعت در حال خلق‌شدن است؛ دوم روزانه با طرح و شیوه‌های جدید در حال مهارت‌های سنتی کشف جرایم مشکل است؛ و سوم این که کنترل این جرایم مستلزم مهارت‌های فنی و تخصصی است که با مهارت و تخصص مرتكبین مطابقت داشته باشد.^[۲۱] مهم‌ترین چالش‌های موجود در این حوزه را می‌توان شامل موارد زیر دانست:

۴-۱- سرعت رشد و سهولت ارتکاب جرم

تسريع و عدم تأخیر در ارسال و دریافت اطلاعات به‌واسطه اینترنت را باید یکی از شگفتی‌های فناوری نوین دانست. رشد بی‌سابقه و ادغام صنایع رایانه‌ای و مخابراتی دسترسی به اینترنت را برای میلیاردها کاربر فعل میسر کرده است. اینترنت بی‌سیم و دستگاه‌های تلفن همراه نیز قابلیت دسترسی آسان‌تری را به فضای سایبری فراهم آورده‌اند. بنابراین مردم اکنون می‌توانند در هر زمان و از هر نقطه‌ای وارد اینترنت شده و به سرعت به انجام انواع مختلف فعالیتها بپردازنند. وقوع جرایم در این حوزه نیز از این قاعده مستثنی نبوده و با سرعت فزاینده در حال رشدند، به‌طوری‌که دگرگونی این جرایم جنبه روزانه و حتی ساعتی به خود گرفته است. شیوه‌های ارتکاب جرم و تولد جرایم نوین پیوسته و به سرعت در حال تغییر بوده و این کار برنامه‌ریزی، قانون‌گذاری، پیش‌گیری و مقابله را با مشکل مواجه می‌سازد. علاوه‌بر این، وقوع جرم در این فضا به‌آسانی و سهولت انجام می‌گیرد. هر آنچه برای تحقق جرم نیاز است تنها یک لپ‌تاپ، تبلت یا موبایل است، حتی برای جایه‌جایی پول در هر نقطه از دنیا همین یک وسیله کفايت می‌کند. این در حالی است که در دنیا واقعی ارتکاب جرم مستلزم وجود ابزار است، یعنی هر جرمی اقتضای تهیه و به کارگیری نوع خاصی از وسائل را دارد.

^۱ globalization

^۲ Multimedia

موجب شده تا نگرش به جرم نیز با دگرگونی مواجه شود؛ یعنی اگرچه در گذشته جرم بیشتر یک پدیده‌ای سرزمینی و در سطح ملی تلقی و تفسیر می‌شد، به کارگیری فناوری‌های مختلف سبب شد تا جرایم جنبه فرا سرزمینی و جهانی پیدا کند.

۴-۵- رقم سیاه بالا

اگرچه آمار مختلفی در ارتباط با میزان بزه سایبری ارائه می‌شود، اما چنین آماری را نمی‌توان انکاس‌دهنده تعداد جرایم مکثوفه یا جرایم واقعی در این حوزه دانست. دلیل عدم اعتماد با این آمار را باید ناشی از یکی از خصوصیات حاکم بر جرایم سایبری که همان وجود رقم سیاه بالاست عنوان کرد.^۱ سه دلیل عمدۀ را می‌توان در این زمینه مطرح ساخت: نخست ناشناختگی و سختی کشف این جرایم. دوم عدم تمايل بزه‌دیدگان به گزارش جرم، به خصوص در شرکت‌های بزرگ دولتی یا خصوصی بهدلیل لطمۀ‌ای که به اعتبار آن‌ها وارد شده و بزه‌دیده واقع شدن در این زمینه می‌تواند به عنوان نشانه‌ای از ضعف سیستم‌شان مطرح شود. سوم ضعیف‌بودن جنبه اخلاقی ارتکاب جرم در این حوزه که عاملی در کاهش سطح رؤیت‌پذیری و به دنبال گزارش‌دهی این جرایم بوده و طبیعتاً عدم بروز حساسیت از جانب افکار عمومی را نیز در پی خواهد داشت [۲۸]. بنابراین از آنجایی که مدنظر قراردادن اخلاقیات، عنصری بنیادی در کنترل جرم در هر جامعه‌ای و عامل اصلی بازدارندگی در این زمینه بوده و بیشتر مردم مرتکب رفتاری که عقیده دارند، غیراخلاقی است نمی‌شوند، اما به اقدامات انجام گرفته در محیط سایبر بیشتر به دیده سرگرمی، تفتن و تفریح می‌نگرند؛ درنتیجه رنگ اخلاقی جرم در این محیط ضعیف بوده و به همین علت افرادی که در دنیای واقعی تمايلی به ارتکاب جرم ندارند، در فضای سایبر به راحتی و سهولت مرتکب جرم می‌شوند.

۴-۶- وسعت و حجم خسارت حادث شده

رشد فناوری و دسترسی آسان به آن، بزه‌کاران را قادر ساخته تا با هزینه‌کردن اندک بتوانند خسارات هنگفتی را به بار آورند. به طور معمول هر بزه‌کار با تهیه یک لپ‌تاپ یا تلفن همراه و نفوذ به شبکه‌های اطلاعاتی، سامانه‌های بانکی، سامانه بورس

^۱ این جمین بین‌المللی حقوق جزا بر پایه گزارشی که از کشورهای عضو دریافت کرده است گزارش می‌یازان اعلام این جرایم را صرفاً ۵٪ اعلام کرده است. در همین رابطه سازمان اطلاعات امنیت آمریکا اعلام داشته که بین ۸۵ تا ۹۵ درصد این جرایم حتی کشف نیز نمی‌شوند. [۲۵] و [۲۶] و [۲۷]

عنوانی از زمان و مکان در این فضا باقی‌مانده است. این در حالی است که محدودیت جغرافیایی و زمانی را باید عاملی اساسی در کنترل جرم دانست. چون به طور اصولی جایه‌جایی، زمان‌بوده و عاملی در شناسایی مجرم محسوب می‌شود. یعنی در دنیای واقعی فاصله‌ای باید پیموده شود، از مزدی در دیواری عبور شود، از محلی به محل دیگر انتقالی صورت گیرد تا بتوان جرمی را مرتکب شد. پس در محیط واقعی نوعی از حضور و تقرب مکانی به منظور تحقیق بزه ضروری است؛ همه این موارد به عنوان مانعی در ارتکاب جرم قابل طرح بوده و امکان دفاع و مقابله را تا حد زیادی فراهم می‌آورد، ولی فقدان اثربخشی این عنصر در فضای مجازی مشهود است و این کار کشف جرایم را مشکل می‌کند. علاوه‌بر بُعد مکانی باید گفت زمان ارتکاب جرم نیز در دنیای واقعی یکی از اهرم‌های کنترل و موانع وقوع جرم است، حال آن‌که مجرمان در فضای مجازی با چنین محدودیتی روبرو نیستند. یعنی زمان در این فضا دارای معنایی متفاوت بوده که با سرعت نور انتلاقی یافته و حرکت‌ها به صورت لحظه‌ای صورت می‌پذیرند. [۲۲] به بیانی دیگر وجود خصوصیات فضای مجازی از جمله حافظه‌ای هم‌افزا و پرقدرت موجب شده تا زمان در این محیط نه به شکل خطی و تعاقبی بلکه به شکلی متراکم، هندسی و موازی ظهور یابد. چنین خصوصیتی به محیط مجازی ویژگی هم‌افزایی متراکم می‌بخشد؛ یعنی در حالی که در فضای واقعی عمل مجرمانه ماهیتی موقتی و زمان‌مند دارد، در فضای مجازی می‌تواند به صورتی پایدار و مستمر ادامه پیدا کند؛ [۲۳] درنتیجه وجود دو متغیر فرامکان‌بودن و فرازمان‌بودن موجب شده تا نوع آسیب‌ها و جرایم محیط سایبری بسیار متمایز و متفاوت از محیط فیزیکی باشد.

۴-۷- مقیاس جرم و فراگیری آن

در جرایم سنتی به طور معمول مقیاس جرم یک در برابر یک است. یعنی تقابلی میان مجرم و قربانی وجود دارد. یک سارق یک سرقた، یک قاتل یک قتل، اغلب این حالت حاکم بوده و تا زمانی که یک جرم تمام نشود، مجرم سراغ جرم دیگر نمی‌رود. به بیانی دیگر بزه‌کاران مجبور به برنامه‌ریزی، تهیه ابزار و مقدمات ضروری و اجرای عنصر مادی برای تحقیق هر بزه به صورت جداگانه هستند؛ اما در فضای سایبر چنین مقیاس و محدودیتی وجود نداشته و قربانی کردن هزاران یا میلیون‌ها نفر به طور همزمان در این محیط امری واقعی و قابل تحقق است؛ درنتیجه در این وضعیت تعداد جرایم بالا رفته و به دنبال آن امر پیش‌گیری و مقابله کاهش می‌باید؛ [۲۴] هم‌چنین تحولات صورت‌پذیرفته در محیط سایبر

- استفاده در سیستم‌های دولتی و اداری دارند را می‌توان شامل موارد زیر دانست:
- خرید و نصب نرم‌افزار محافظه بر اساس ارزش هر یک از موارد؛
 - طبقه‌بندی اطلاعات سیستمی بر اساس میزان اهمیت و درجه محرومگی آن‌ها؛
 - شناسایی نرم‌افزارها، برنامه‌ها و فایل داده‌هایی که نیاز به کنترل و دسترسی ویژه دارند؛
 - نصب نرم‌افزار دارای سازوکار کنترل دسترسی؛
 - به کارگیری عاملی منحصر به فرد، بهمانند فرم‌های شناسایی قابل اثبات، مانند یک کد کاربری یا رمز عبور مخفی برای هر کاربر؛
 - رمزگذاری اطلاعات محروم‌شده در رایانه؛
 - ایجاد روشی برای بازیابی اطلاعات سیستم‌عامل به‌طوری که اگر از بین رفته و یا دچار اختلال شوند، تمامی داده‌های پشتیبانی شده به صورت برونو خط ذخیره شوند. هم‌جنین اطمینان از پشتیبان گیری به‌طور منظم برای کمک به بازیابی اطلاعات؛
 - پیش‌فایل‌های بارگیری شده برای ویروس‌یابی پیش از نصب و عدم بارگیری فایل‌های اجرایی نامأتوس و مشکوک.

۴-۹- پیش‌گیری مبتنی بر نقش بزه کاران

طیف گسترده‌ای از اشخاص موتکبان جرایم سایبری را تشکیل می‌دهند که در رده‌های سنی مختلف و با انگیزه‌های متفاوت مرتكب این جرایم می‌شوند. تعیین سن مجرمان سایبری به صورت دقیق ممکن نیست، زیرا همین که شخص توانی کار با رایانه را پیدا کرده و کمینه دانش مقدماتی در این زمینه را کسب کرده باشد، قادر خواهد بود تا مرتكب جرم شود. انگیزه یا اهداف چنین بزه کارانی نیز در سوق یافتن به‌سوی این جرایم بسیار متنوع بوده که می‌تواند از سرگرمی، خودنمایی، اثبات برتری قدرت و انتقام‌جویی شروع شده و تا به کسب منفعت مالی، خرابکاری، جاسوسی، تروریسم و قاجاق ادامه یابد؛ بنابراین از نظر انگیزشی مجرمان سایبری را می‌توان به سه دسته مزاحمان، خلافکاران و خرابکاران تقسیم کرد.^۱ با توجه به این تفاسیر، لازم است تا با توجه به خصوصیات

^۱ مزاحمان بیشتر نوجوانانی‌اند که با انگیزه اثبات قدرت و یا سرگرمی نسبت به دستیابی به اطلاعات موجود در سامانه‌های رایانه‌ای و نفوذ در آن اقدام می‌کنند. خلافکاران که می‌توان آنان را مجرمان به معنای واقعی کلمه نامید، افرادی هستند که با هدف کسب منفعت اقدام به ارتکاب جرم می‌کنند. انجام جرائم کلامبرداری اینترنتی، سرقت اینترنتی و جاسوسی در این دسته قرار می‌گیرند. انگیزه گروه سوم نیز فقط وارد آوردن خسارت و آسیب بر دیگران بوده فائغ از آن که در پی کسب منفعت، تفدن و یا اثبات برتری خویش باشند. به‌طور اصولی افراد انتقام‌جو و یا اشخاصی که از مشکلات روانی رنج می‌برند، در این دسته جای می‌گیرند.

و حتی حریم خصوصی اشخاص، به‌سهوالت و بدون مواجهه با محدودیت‌های موجود در فضای فیزیکی، قادر خواهد بود تا ضررهای سنگین و گاهی جبران‌ناپذیری را به وجود آورد. اهمیت توجه به این چالش زمانی فزونی می‌یابد که این موضوع را مدنظر قرار دهیم که وابستگی امور حیاتی و حساس کشورها در زمینه‌های مختلفی از جمله امنیتی، نظامی، هسته‌ای، هوایپیمایی، پژوهشی و در به کارگیری از رایانه‌ها و اینترنت هر روز افزایش یافته و درنتیجه ایجاد خلل یا خدشه در این سامانه‌ها می‌تواند عواقب جبران‌ناپذیر و شدیدی را به همراه داشته باشد؛ درنتیجه سرعت و حجم بروز و تکثیر آسیب‌ها در محیط دیجیتال به هیچ عنوان قابل قیاس با محیط عینی و ملموس نبوده و ممکن است در اندک زمانی حجم وسیعی از خسارات به‌طور تصاعدی گسترش یابد. [۲۹]

۷-۴- راهبردهای پیش‌گیری از جرایم رایانه‌ای

پیش‌گیری از جرایم سایبری ساده نیست. ویژگی‌های اساسی این جرایم موجب شده تا امر مقابله با آن مستلزم شناسایی و برنامه‌ریزی دقیق و اصولی در این زمینه باشد؛ یعنی لازم است تا با درک چگونگی وقوع این جرایم و همچنین عواملی که در این جرایم دخیل هستند، نسبت به امر پیش‌گیری اقدام شود. به‌طور اصولی برای جلوگیری از این گونه از جرایم نیاز به تمرکز بر سه پدیده داریم که عبارت‌اند از ۱- وسائل دیجیتال به‌عنوان ابزاری که برای ارتکاب جرم مورد استفاده قرار می‌گیرد. ۲- بزه کاری که منبع جرم است. و ۳- بزه‌دیده بی‌گناه در معرض جرم. پس رویکردی که در امر پیش‌گیری موردنویج قرار می‌گیرد، باید شامل هر سه راهبرد باشد.

۸- پیش‌گیری مبتنی بر نقش ابزار جرم

رایانه و دیگر ابزار دیجیتال را باید به‌عنوان مهم‌ترین عاملی که در معرض تحقیق جرایم سایبری قرار دارند، در نظر گرفت. این وسائل پل ارتباطی میان بزه‌دیده و بزه کار بوده که دارای کارکردی دوگانه است. با این توضیح که از یکسو این ابزار قابلیت نفوذ برای مجرمان را فراهم آورده و از سوی دیگر ابزاری برای بزه‌دیده واقع شدن قربانی خواهد بود. بنابراین اعمال برخی از تدبیرهای امنیتی و محافظتی از جانب اشخاص یا سازمان‌های در معرض خطر می‌تواند نقشی اساسی و مهم در عدم بزه‌دیده واقع شدن آنان ایفا کند. اهم این تدبیر را که گاهی علاوه بر سیستم‌های شخصی در سیستم‌های اداری نیز می‌تواند مورد استفاده قرار گیرد و برخی دیگر نیز فقط قابلیت

منضم به قانون مجازات اسلامی و در در ادامه این قانون
جای گرفت.^[۳۲]

به طوراصلی با توجه به ویژگی‌های خاص جرایم سایبری، ضروری است تا تدابیر پیش‌گیرانه واکنشی در این زمینه، با تدبیر اتخاذ شده در محیط واقعی متفاوت باشد؛ یعنی جرم‌انگاری در این محیط باید متمایز از محیط واقعی صورت پذیرد. در همین راستا به منظور اتخاذ تدبیر کیفری مناسب، توجه به دو موضوع ماهیت جرم‌انگاری و میزان مجازات حائز اهمیت است. هر یک از این معیارها مبین اتخاذ و پذیرش رویکرد افتراقی در مقابله با این جرایم است که در ادامه به بررسی آن می‌پردازم:

الف- جرم‌انگاری بزه‌های سایبری

از آنجایی که تعاریف و بزه‌انگاری‌های موجود با رویکرد سنتی ممکن است در مقام عمل قادر به پوشش دادن اقدامات ضداجتماعی که در محیط سایبر رخ می‌دهد، نباشد، لازم است تا نسبت به بازتعریف جرایم در این حوزه اقدام شود. به عنوان مثال در جرم جعل با استفاده از سند مجهول، ساختن سند به آن معنا که در جرایم سنتی وجود دارد، نباید در محیط سایبر نیز مدنظر قرار گیرد، زیرا تا همین میزان که شخص اطلاعات غیرواقعی را وارد کند، قادر خواهد بود تا از امتیازات زیادی بهره‌مند شود. برای مثال مالیات پرداخت‌نشده را پرداخت‌شده قلمداد کند یا شناسنامه‌ای برای خود بسازد. هم‌چنین در جرم کلاهبرداری به طور معمول اقدامات متقابلانه مرتکب، نسبت به سامانه و سیستم اعمال شده و نه انسان‌ها، پس بک نتترل مهم که فریب مال خورده است، نباید در اینجا جایگاهی داشته باشد. در غالب جرایم رویداده در محیط فیزیکی و سایبری وجود چنین تفکیک و تقvaوت‌هایی مشهود بوده و در درنتیجه مشخص می‌شود که تعارف سنتی در همه موارد نمی‌تواند جوابگو باشد و نیاز به اصلاح دارد؛ پس قوانین نوین باید با ویژگی‌های جدید تعریف و تصویب شوند. به عنوان نمونه یکی از اصلاحات مؤثر در تصویب جرایم سایبری، تصویب این جرایم به صورت مطلق است. با این توضیح که با ملاحظه داشتن عنصر نتیجه در تحقق یا عدم تحقق جرم، جرایم به دو دسته مطلق و مقید قابل تقسیم‌اند، که در دسته نخست ظهور نتیجه‌ای خاص در تتحقق جرم نقشی نداشته اما در دسته دوم محقق شدن نتیجه جزء جدایی‌ناپذیر شکل‌گیری جرم است. به طوراصلی جرم‌انگاری به صورت مطلق مبین قصد مقتن در عدم تسامح نسبت به جرم است؛ زیرا گاه حساسیت جرم، گاه آثار و تبعات گستره آن و گاهی نیز شرایط ویژه تحقق بزه موجب می‌شود تا چنین سیاستی در پیش‌گرفته شود. با توجه به آن‌که هر سه این مؤلفه‌ها در جرایم سایبری

مرتكبین و هم‌چنین ویژگی‌های خاص جرایم سایبری را بدهای مختلف و مکمل در مقابله با این جرایم در دستور کار قرار گیرد. به دیگر سخن، کنترل و مبارزه با این جرایم مستلزم اتخاذ سیاست جنایی مؤثر بوده که در بردارنده دو رویکرد کیفری و غیر کیفری باشد. رویکرد کیفری یا جرم‌انگاری، فرایندی است که به موجب آن قانون‌گذار با درنظر گرفتن ارزش‌ها و هنجرهای حاکم بر جامعه، فعل یا ترک فعلی را ممنوع و برای آن ضمانت اجرای کیفری وضع می‌کند. پیش‌گیری از وقوع جرم با تکیه بر مجازات در چارچوب نظام کیفری را می‌توان به عنوان یکی از اهداف این مدل مطرح ساخت. در رویکرد غیر کیفری سعی بر پیش‌گیری از وقوع جرم با اتکا بر شیوه‌ها و ابزارهای غیر قهرآمیز است. این شیوه با هدف شناسایی علل نزدیک به جرم و تلاش در خنثی‌سازی آن می‌کوشد تا میزان ارتکاب جرایم و یا میزان سنگینی آن را کاهش دهد.^[۳۰]

۱-۹-۴- تدبیر کیفری در مقابله با بزه‌کاران سایبری
جرائم‌انگاری به عنوان یکی از تدبیر در زمینه پیش‌گیری از جرایم سایبری قابل طرح است. اغلب کشورها می‌کوشند تا با تصویب قوانین و مقرراتی خاص، خسارات و آسیب‌های ناشی شده از جرایم سایبری را به کمینه رسانند. کشور کانادا را باید نخستین کشوری نامید که در قانون فدرال خود و به سال ۱۹۸۳ به صورت مشخص به جرایم رایانه‌ای اشاره داشته و قوانینی را در این زمینه به تصویب رساند.^[۳۱] سپس این روند در سایر کشورها نیز دنبال شد که نتایج کم و بیش مؤثری را نیز به همراه داشته است. بنابراین اتخاذ تدبیر کیفری مستلزم آن است که دولت‌ها به تصویب قوانینی جامع و شفاف در زمینه پیش‌گیری از جرایم سایبری پرداخته، به گونه‌ای که این قوانین در بردازندۀ مصاديق مختلف این جرایم باشد؛ یعنی اگر فردی مرتکب جرمی سایبری یا رایانه‌ای شده و جرمش اثبات شد، بتوان آگاهانه وی را منطبق بر میزان جرم‌ش محاکوم ساخته و برایش حکم صادر کرد. در همین ره‌گذر کشورها سه اقدام یا الگوی مختلف را در راستای تدبیر کیفری در دستور کار خویش قرار داده‌اند. برخی نسبت به اصلاح قوانین پیشین خود اقدام کرده‌اند. برخی دیگر به اختصاص فصل مجزا و جداگانه‌ای درخصوص جرایم سایبری در قوانین موجود اهتمام ورزیده و درنهایت دسته‌ای دیگر به تصویب قوانین خاص در این زمینه پرداخته‌اند. قانون جرایم رایانه‌ای ایران نیز که با تبعیت از الگوی کنوانسیون بوداپست درخصوص بزه‌های سایبری به تصویب رسیده است، اگرچه درابتدا بنا بود به عنوان قانونی ناپیوسته و مجزا نوشته و تصویب شود، اما درنهایت

حتمیت و قطعیت در اجرای قوانین مرتبط با این حوزه است. درنتیجه یکی از مهمترین و اساسی‌ترین طرق ارسال پیام به خلاف کاران، بزه‌کاران و بهطورکلی مجرمان بالفعل و بالقوه آن است که در صورت ارتکاب بزه با اعمال و اجرای محکومیت جدی و قطعی روبه‌رو خواهند شد و درصورتی که بخواهند به چنین جرایمی ادامه دهند، می‌بایست بهای آن را نیز پرداخت کنند. پس اتخاذ تدبیر کیفری سنجیده و اصولی به همراه دقیق، سرعت و قطعیت در اجرای آن را باید مکمل یکدیگر و طریقه‌ای اساسی در مقابله و پیش‌گیری از جرایم سایبری دانست.

۴-۲-۹-۴- تدبیر غیر کیفری در مقابله با بزه‌کاران سایبری

با توجه به آن که صرف اتکا به تدبیر کیفری و جرم‌انگاری نمی‌تواند در مقابله با جرایم سایبری مؤثر واقع شود، لازم می‌آید تا تدبیر غیر کیفری نیز در مقابله با این جرایم مدنظر قرار گیرند. در همین راستا نباید از نقش آموزش و آگاهی‌سازی غافل شد. از آنجایی که بسیاری از کاربران و استفاده‌کنندگان اینترنتی به جرایم حداثت‌شده در این حوزه، به دیده سرگرمی نگریسته و قبیح جرایم محقق شده در دنیا واقعی را نسبت به این جرایم جاری نمی‌سازند، بیشتر به سوی چنین جرایمی سوق پیدا می‌کنند؛ بنابراین یکی از راه‌کارهای مهم در این زمینه، تغییر چنین نگرشی و نمایاندن واقعیت به افراد، با بهره‌گیری از آموزش‌های اخلاقی است؛ زیرا که چنین آموزش‌هایی ممکن است، موجب شود افراد مستعد خلاف کارشدن، در مورد اقدام خود تردید کرده و درنهایت از اقدام به آن منصرف شوند. البته باید این موضوع را نیز در نظر داشت که راهبردها و تدبیر آموزشی در محیط سایبری، درست بهمانند تمام انواع آموزش‌های دیگر، یک سرمایه‌گذاری بلندمدت بهخصوص در ارتباط با جوانان بوده که اهتمام به این امر نه تنها می‌تواند در شکل‌گیری شخصیت و دوری‌جستن آنان از بزه و بزه‌کاری تأثیرگذار باشد، بلکه در هدایت اقدامات آن‌ها در سراسر امور زندگی نیز اثرگذار است. درنتیجه بهره‌گیری مناسب از تدبیر حساس‌سازی و آگاهی‌سازی اشخاص، که سبب تقویت فرهنگ قانون‌مداری و اجتناب از ارتکاب بزه می‌شود، می‌تواند ضمن پیش‌گیری از جرایم سایبری، از بار دستگاه عدالت کیفری در مقابله با این جرایم نیز بکاهد [۳۴].

۴-۳-۹-۴- پیش‌گیری مبتنی بر نقش بزه‌دیده

وجود دارد، اتخاذ چنین تدبیری در مقابله با این جرایم نیز قابل دفاع است. به همین منظور مقدم ایران نیز در مواد ۷۲۹، ۷۳۰، ۷۳۲ و ۷۳۴ فارغ از توجه به نتیجه احتمالی، اقدامات یادشده در این مواد را به صورت مطلق جرم‌انگاری کرده است.^۱

ب- مجازات جرایم سایبری

اگر این‌گونه فرض شود که اعمال مجازات در مقابله با جرایم سایبری مؤثر است، توجه به شدت و حتمیت اجرای آن نیز در کنترل و پیش‌گیری از این جرایم واجد اهمیت خواهد بود. به طور اصولی پیروی از قواعد تعدد جرم نیز در اینجا فاقد کارایی لازم بوده و نمی‌توان به آن متولّ شد، زیرا در اینجا بحث شمارش فاقد موضوعیت است و باید گفت در برخی از جرایم حتی تعیین تعداد بزه‌دیدگان و بزه‌های تحقیق‌بافتی نیز امری غیرممکن است؛ پس لازم است در گزینش نوع و میزان مجازات انتخابی دقت کافی به خرج داده شود. البته مقصود از شدت مجازات در اینجا به هیچ عنوان توصل به مجازات غیرانسانی و ناعادلانه نبوده، بلکه آن چنان مجازاتی است که به میزان کافی واجد خصیصه بازدارندگی عام و خاص باشد. علاوه بر لزوم سنتی و شدت میزان مجازات جرایم سایبری نسبت به مجازات جرایم سنتی، سرعت و قطعیت نیز در اجرای آن از اهمیت بالایی برخوردار است. اگر این گفته بکاری را مورد توجه قرار دهیم که "این شدت کیفر نیست که از جرم پیش‌گیری می‌کند، بلکه حتمی و قطعی بودن مجازات است که می‌تواند از جرم‌های آینده جلوگیری کند" [۳۳] اهمیت تسريع در رسیدگی و مجازات مرتكبین روشان‌تر می‌شود. پس باید گفت اجرای صحیح و مناسب قانون بسیار بالهمیت‌تر از تصویب قوانین خوب است؛ زیرا این اجرای اصولی و درست قوانین است که این باور و اطمینان را از یکسو در آحاد مردم و از سوی دیگر در بزه‌کاران بالقوه ایجاد خواهد کرد که در صورت ارتکاب جرم، اعمال مجازات نسبت به آنان حتمی است. به دیگر سخن ما نمی‌توانیم با جرایم مبارزه کنیم اگر فقط قوانین در کتاب‌ها آمده باشد و قادر به اجرای آن نباشیم؛ بنابراین یکی از راه‌کارهای کاهش جرایم سایبری را باید

^۱ ماده ۷۲۹ هر کس به طور غیرمجاز به داده‌ها با سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدبیر امنیتی حفاظت شده است دسترسی باید ...

ماده ۷۳۰: هر کس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند ...

ماده ۷۳۲: هر کس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدبیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند ...

ماده ۷۳۴ هر کس به طور غیرمجاز مرتكب اعمال زیر شود، جاگول محسوب ... خواهد شد:

الف تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن مقلوبانه داده به آنها، ب تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن مقلوبانه داده‌ها یا علائم به آنها.

جعفری، ۱۳۸۹: ۱۸۵) یعنی در صورتی که حتی مال باخته مرتکب سهل‌انگاری شده و مراقبت کافی را به خرج نداده باشد (به عنوان مثال درب منزل را باز گذارده باشد) و به همین سبب سرقته رخ دهد، خدش‌های در ماهیت سرقت رخداده به وجود نخواهد آمد.^۲ اما در محیط سایبری برای آن که بتوان امر پیش‌گیری را توسعه بخشیده و به نحو مطلوب‌تر به انجام رساند، چنین رویکردی قابلیت دفاع نخواهد داشت. یعنی ضروری است تا در اینجا رویکردی افتراقی را در دستور کار قرار گرفته و تفکیک و تمایزی میان بزه‌دیدگان سهل‌انگار و غیر آن را لاحظ شود. هرچند در نگاه نخست چنین رویکردی می‌تواند به ضرر بزه‌دیده تعییر شود، اما با توجه به مخاطرات حاصل از این جرایم، اتخاذ چنین سیاستی اجتناب‌ناپذیر است. پذیرش چنین وضعیتی در قانون جرایم رایانه‌ای ایران نیز مدنظر مقنن قرار گرفته است. همان‌گونه که در ماده ۷۲۹ ق.م.ا. یا نخستین ماده از قانون جرایم رایانه‌ای مشخص است، اقدامات صورت گرفته در صورتی عنوان مجرمانه خواهد داشت که بزه‌دیده تدبیر امنیتی لازم و موردنیاز را به انجام رسانیده باشد. یعنی در صورت عدم رعایت چنین موضوعی این امکان وجود دارد که قربانی مورد حمایت قرار نگیرد. به تعییری دیگر در صورتی که مشخص شود بزه‌دیده نیز در تحقیق جرم مرتکب تقصیر یا کوتاهی شده است، علاوه بر تقلیل میزان مسئولیت بزه‌کار، حتی امکان زایل شدن جرم و عنوان مجرمانه نیز وجود خواهد داشت. بنابراین بر پایه چنین سیاستی مقنن می‌کشد تا با تعمیم‌بخشی امر پیش‌گیری به‌سوی جامعه یا اشخاص، ضمن آگاهسازی آنان نسبت به خطرات موجود، آن‌ها را نیز در بخشی از امر حفاظت و صیانت دخیل کند.

از سویی دیگر در صورتی که قربانی مرتکب تساهل نشده باشد، مقنن در صدد گسترش چتر حمایتی خویش از وی بر می‌آید. یعنی می‌کوشد تا به طرقی از جمله تعریف شروع به جرم یا اقدامات مقدماتی به عنوان جرم کامل از شکل‌گیری بزه در همان بدو امر جلوگیری کند. بنابراین در این وضعیت مقنن در بی آن است که این پیام را به بزه‌کاران مخابره کند که حتی اگر مرتکب اقدامات ابتدایی نیز شوند، مجازات آنان به‌مانند جرم مستقل لحاظ خواهد شد. در همین راستا می‌توان علاوه بر ماده ۷۲۹ به ماده ۷۳۳ نیز اشاره داشت^۳، بر طبق این دو ماده اقداماتی چون صرف دسترسی و یا حتی قصد دسترسی به داده‌ها یا سامانه‌ها که درنهایت در زمرة شروع به

^۲ هر چند ممکن است در احراز نوع سرقت یعنی حدی یا تعزیری بدون تفاوت وجود داشته باشد لیکن در تحقیق اصل جرم تفاوتی در اینجا وجود نخواهد داشت.

^۳ ماده ۷۳۳ هر کس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدبیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، ...

بزه‌دیده را باید سومین رکن از ارکان جرایم سایبری دانست که در تحقیق این جرایم می‌تواند نقشی بالهمیتی ایفا کند. توجه به تفتش این اشخاص در وقوع جرم نخستین بار در دانش جرم‌شناسی مورد توجه قرار گرفت. در همین راستا و بر پایه بزه‌دیده‌شناسی علمی یا علم‌شناسی، در مواجهه با جرایم فقط نباید بر نقش مرتکب و بزه‌کار تمرکز کرد، بلکه لازم است تا سهم بزه‌دیده نیز در تحقیق بزه مورد توجه قرار گیرد، زیرا جرم در همه حالات نشأت‌گرفته از عوامل شخصی و محیطی مربوط به مرتکب نبوده، بلکه بزه‌دیده نیز ممکن است، در تحقیق بزه نقش داشته باشد. [۲۵] بر همین اساس جرم‌شناسان نقش یا کارکردی چندگانه را در ارتباط با بزه‌دیدگان تبیین کرده‌اند^۴؛ درنتیجه با توجه به آن که زوج کفیری (بزه‌کار و بزه‌دیده) همیشه به صورت سیاوه‌سفید نمایان نمی‌شود، یعنی آن که یکی به‌طور کامل گناه‌کار و دیگری بی‌گناه باشد، باید سهم و تأثیر رفتار آنان در وقوع جرم مورد ارزیابی قرار گرفته و بر همین اساس میزان مستولیت هر یک تعیین شود. توجه به این مسائل عاملی خواهد بود تا بر پایه اطلاعات به دست‌آمده از مطالعات بزه‌دیده‌شناسی، این امکان فراهم شود تا امر برنامه‌ریزی و پیش‌گیری از بزه‌دیدگی به‌نحوی اصولی و مناسب‌تر انجام پذیرد. بزه‌دیدگی در فضای مجازی نیز از این قاعده مستثنی نبوده و حتی ویژگی جرایم در این فضای عاملی است که توجه به نقش بزه‌دیدگان در این جرایم اهمیتی دوچندان یابد. واقعیت امر نمایان گر آن است که در غالب جرایم محقق شده در محیط سایبر، می‌توان اثری از نقش کم‌ویش پررنگ قربانی یافت. پس در ادامه ابتدا به تبیین نقش بزه‌دیده در جرایم سایبری که لزوم پذیرش رویکردی افتراقی را در این زمینه می‌طلبد پرداخته و سپس به بررسی راهبردهای پیش‌گیری مرتب با بزه‌دیدگی در این فضا می‌پردازیم.

۴-۹-۴- عدم حمایت از بزه‌دیدگان سهل‌انگار، تقویت حمایت از بزه‌دیده بی‌گناه

بر پایه حقوق جزای سنتی تفاوت و تمایزی میان بزه‌دیدگان سهل‌انگار و غیر سهل‌انگار در محیط واقعی وجود ندارد. برای مثال در جرم سرقت، رعایت یا عدم رعایت راهبردهای پیش‌گیری وضعی از سوی مال‌باخته در نگهداری و حفاظت از مال خود، تأثیری در تحقیق جرم نخواهد داشت. (جوان

^۱ دسته‌بندی‌هایی مختلف از بزه‌دیده در علم بزه‌دیده‌شناسی ارائه شده است. گاهی بر مبنای تقصیر بزه‌دیدگان به بزه‌دیده مقصّر و غیر مقصّر تقسیم شده‌اند. گاهی نیز سخن از بزه‌دیدگان به‌طور کامل بی‌گناه، ناگاه، بماندۀ بزه‌کار مقصّر و پیش از بزه‌کار مقصّر به میان آمده است. در برآهای دیگر از موارد بزه‌دیدگان به بزه‌کار، بزه‌دیده، بزه‌دیده بالقوه و بزه‌دیده مکرر تقسیم شده‌اند. اهمان ا

کدهای رفتاری را می‌توان در دستور کار قرار داد. به طور اصولی با توجه به آن که جرایم سایبری به صورت سازمان یافته و با طراحی و نقشه قبلی انجام می‌گیرد، دادن آموزش به اشخاص یا مؤسسات در معرض خطر برای مقابله با این جرایم بسیار سودمند است. [۳۷] در سطوح اختصاصی نیز می‌توان با طبقه‌بندی اشخاص در معرض خطر به گروه‌های مختلف، نسبت به ارائه آموزش تخصصی به آنان اقدام کرد. به عنوان مثال برگزاری دوره‌های آموزشی ویژه کودکان و نوجوانان در این دسته قرار می‌گیرد. بنابراین باید گفت رابطه‌ای اساسی میان آگاهی و اطلاع از تهدیدات موجود و میزان خسارت احتمالی واردہ برقرار است. یعنی با افزایش آگاهی فرد میزان بزمدیده واقع شدن وی کاهش و با عدم دانش یا کمبود میزان آن، احتمال قربانی شدن افزایش پیدا می‌کند.

ب- خنثی‌سازی

باید توجه داشت صرف کسب آگاهی نسبت به چالش‌ها و آسیب‌های موجود، به طور کامل نمی‌تواند در عدم بزمدیده‌گی شخص در محیط سایبر مفید واقع شده ولذا لازم می‌آید تا کاربران از ابزار و روش‌های امنیتی نیز به منظور دفع خطر بهره‌گیری کنند. مقصود از امنیت، تلاش و تدبیری است که می‌تواند در حراست از به خطر افتادن کاربران یا سامانه‌ها در محیط سایبر نقش اساسی ایفا کنند؛ پس استفاده از ابزار سخت‌افزاری و نرم‌افزاری امنیتی را باید مکمل دریافت و افزایش دانش در زمینه حفاظت از آسیب‌دیدگی جرایم سایبری به حساب آورد. به طور کلی سه نوع تدبیر امنیتی در حوزه جرایم سایبری می‌تواند موردنظر قرار گیرد. نخست تدبیر حفاظتی فیزیکی که در بردارنده فرایندی است برای جلوگیری از دستیابی غیرمجاز به سامانه‌های رایانه‌ای، به‌مانند نگهداری سامانه‌ها در محیطی امن، محدود کردن دسترسی افراد به سامانه‌ها و جلوگیری از آثار واردہ بر سامانه‌ها در اثر مشکلات الکتریکی یا سخت‌افزاری است. به تعبیری دیگر این رابردها در صددند تا ابزار ورود به محیط سایبر را از خطرات احتمالی محافظت کنند. دوم تدبیر نرم‌افزاری، که شامل کنترل دسترسی و دستیابی‌ها (پالایه)^۱، کنترل مراحل ورودی و خروجی‌ها، رمزگاری‌ها، استفاده از دیواره آتشین،^۲ استفاده از پروکسی‌ها^۳ و نصب و بهروزرسانی آنتی‌ویروس می‌شود.^۴ با توجه به خصایص جرایم فضای سایبری که مبتنی بر موضوعات ناملموس و غیر فیزیکی است، بهره‌گیری از این

جرائم و اعمال مقدماتی قرار می‌گیرند، به عنوان بزههای تام جرم‌انگاری شده‌اند؛ بنابراین اگرچه در نظام کیفری سنتی اعمال مقدماتی جرم به حساب نیامده و شروع به جرم نیز با توجه به جمعبودن شرایطی، مجازاتی اخف از جرم تام دارد، اما چنین رویه‌ای در محیط سایبر دنبال نشده و باید گفت در برخی از جرایم محقق شده در این فضا، تفاوتی در میزان مجازات میان اعمال مقدماتی، شروع به جرم و جرم تام وجود نخواهد داشت. در توجیه این رویکرد باید گفت به دلیل حجم وسیع، آثار گستره و دشواری در مستندسازی و اثبات جرایم سایبری، تا آنجایی که ممکن است، باید پیش از وقوع جرم به مبارزه با آن پرداخته و از تحقیق آن جلوگیری کرد. البته باید توجه داشت که پذیرش و به کارگیری چنین رویکردهایی بسیار ظریف و خطرناک است، زیرا که در تقابل با اصول شناخته شده حاکم بر حقوق جزا بوده و به همین دلیل در طرح و گزینش آن باید احتیاط کرد. با توجه به این تفاسیر مشخص می‌شود که مفون در مواجهه با بزمدیدگان سایبری و با مدنظر قراردادن میزان رعایت تدابیر حفاظتی از جانب آنان، دو رویکرد مختلف را در دستور کار خویش قرار داده است؛ بنابراین از آنجایی که هر شخصی در طول مدت زندگی اش ممکن است، در معرض بزمدیدگر فته و به نوعی بزمدیده بالقوه محسوب می‌شود، لازم است تا با به کارگیری تدابیری از وقوع چنین موضوعی جلوگیری کند. در محیط سایبری نیز اگرچه راهبردهای مختلفی قابل شمارش و بازگوکردن است، اما توجه به دو رویکرد آگاهی‌بخشی و خنثی‌سازی از اهمیت بالاتری برخوردار است.

الف- آگاهی‌بخشی

اغلب عدم آگاهی و شناخت بزمدیدگان بالقوه از تهدیدات پیش‌رو، بر میزان آسیب‌پذیری‌شان افزوده و آنان را در معرض خطر قرار می‌دهد. چنین موضوعی در حیطه‌های نوینی چون محیط سایبر و جرایم محقق شده در این فضا می‌تواند مخاطره‌آمیزتر نیز باشد. زیرا به طور اصولی بسیاری از افراد به دلیل ناآگاهی‌های مرتبط با این محیط، گمان می‌برند که در این فضا همه‌چیز جلوه‌ای غیرواقعی داشته و در صورت مواجهه با تهدیدها نیز چیزی را از دست نداده و به همین سبب زمینه آسیبرسانی به خویش را فراهم می‌آورند. بنابراین ضروری است تا برای ازبین‌بردن این معضل و افزایش اطلاعات کاربران در خصوص تهدیدات پیش‌رو، تدبیر آموزشی عمومی و اختصاصی به صورت مداوم و هماهنگ تعریف و اجرا شود. [۳۶]

در حوزه آموزش‌های عمومی، تدبیری از قبیل شناساندن مفهوم و انواع چالش‌های موجود، راه‌کارهای احتمالی مقابله و پیش‌گیری از آن و همچنین ایجاد آگاهی نسبت به ارتقای

¹ Filtering

² Fire wall

³ Proxy

⁴ دیواره آتشین ترکیبی از سخت‌افزار و نرم‌افزار بوده که سامانه را به دو یا چند قسمت تقسیم کرده و مؤثرترین شیوه برای مقابله و کاهش

شود؛ درنتیجه هر دو این تدابیر در جلوگیری و مقابله با جرایم سایبری مکمل هم محسوب می‌شوند.

۶- مراجع

- [۱] حسن بیگی، ا. حقوق و امنیت در فضای سایبر، چاپ اول. تهران: انتشارات موسسه فرهنگی مطالعات و تحقیقات بین الملل ایران معاصر. (۱۳۸۴)
- [۲] دی آنجلیز، ج، جرایم سایبر، (ترجمه حافظی سعید و خرم آبادی عبدالصمد)، چاپ اول، تهران: انتشارات دبیرخانه سورای عالی اطلاع رسانی. (۱۳۸۳)
- [۳] k Jaishankar, Cyber Criminology. London, crc press (Taylor & Francis Group). (2011).
- [۴] S. Furnell, Cyber crime: Vandalizing the information society. London: Addison Wesley. (2002).
- [۵] R -Moore, Cybercrime; investigating high-technology computer crime, Publisher: Anderson Publishing Co. (2005).
- [۶] y Jekkes, Crime Online, First edition, Willan Publishing, 2007.
- [۷] l. j. Seigel, The core Criminology, usa, Wadsworth, Cengage Learning, 2011.
- [۸] [علی‌پور، ح، حقوق کیفری فناوری اطلاعات (جرائم رایانه‌ای)، چاپ دوم، تهران: خرسندي. (۱۳۹۳)]
- [۹] [برومند باستانی، ب. جرایم کامپیوتري و اینترنتي جلوه‌ای نوین از بزهکاري، چاپ دوم، تهران: بهنامي. (۱۳۸۶)]
- [۱۰] B, Seigel, Crime Prevention, Oxford Of Criminology, Great Britain, 2001.
- [۱۱] بابا غبی ازغدی، ع. ر. الگویی نوین برای پیشگیری از جرایم فضای سایبر، فصل‌نامه مطالعات پیشگیری از جرم، ۱۴۴-۱۴۳، شماره ۲۶. (۱۳۹۱)
- [۱۲] G. Crowe, Crime & Prevention,shell, Great Britain, 2007.
- [۱۳] قاجارقیونلو، س. مقدمه حقوق سایبر، چاپ اول، تهران: میزان. (۱۳۹۱)
- [۱۴] زندی، م. ر. تحقیقات مقدماتی در جرایم سایبری، چاپ اول، تهران: جنگل جاودانه. (۱۳۸۹)
- [۱۵] مسعودیان، م. نقش پلیس در پیشگیری از جرایم سایبری و تأمین امنیت در فضای مجازی(پلیس فتا)، فصل‌نامه پژوهش‌های انتظام اجتماعی، (۱۳۹۱)، شماره ۱: ۱۰۴-۱۲۴

تدابیر بسیار حائز اهمیت است. سوم تدابیر سازمانی، که چنین تدابیری بهطوراصلی در ارتباط با شرکت‌ها و سازمان‌ها موضوعیت یافته و جنبه شخصی ندارند. اقداماتی از قبیل انتخاب کارکنان متخصص و آموزش‌دهنده، بازرگانی داده‌پردازی‌ها بهصورت ادواری و تفکیک وظایف و عملکردها در این دسته جای می‌گیرند. [۳۸]

۵- نتیجه‌گیری

تا چند دهه گذشته جرایم سایبری تنها محدود به محیط‌های اقتصادی بود، اما تجربیات نشان‌دهنده آن است که این جرایم از این محیط‌ها فراتر رفته و در بسیاری از زمینه‌ها به وقوع می‌پیوندد. بنابراین بهموازات استفاده مشروع و افزایش بهره‌وری مفید از فضای سایبر، شکل‌گیری جرایم نوین و استفاده‌های غیرقانونی نیز در این محیط رشد و فروزی داشته‌اند. بنابراین ضروری است تا ضمن آشنایی با ویژگی‌ها و خصوصیات این جرایم، سیاست جنایی مناسب و کارآمد نیز بهمنظور پیش‌گیری و مقابله با آن اتخاذ شود. دانش جرم‌شناسی یکی از علمی است که می‌تواند در این زمینه کارگشا باشد. در همین راستا و بر پایه اصول کلی و اساسی حاکم بر این دانش، توجه به دو مؤلفه عناصر دخیل در جرایم سایبر و اتخاذ تدابیر مناسب در این حوزه حائز اهمیت است. در ابتدا و بر پایه مؤلفه نخست، لازم می‌آید تا با تمرکز بر سه عنصر بزه‌کار، بزه‌دیده و وسیله ارتکاب بهعنوان سه ضلع دخیل بر وقوع جرم، چالش‌ها، موانع و خصایص هر یک از این عناصر مورد شناسایی قرار گیرند؛ سپس با اتکا بر این موارد و بر اساس مؤلفه دوم ضروری است تا سیاستی دقیق و مناسب طراحی و اجرا شود. بههمین منظور و در مواجهه با جرایم سایبری دو نوع تدبیر کیفری و غیر کیفری می‌تواند مورد توجه قرار گیرد. جرمانگاری‌ها و تعیین ضمانت اجرای کیفری مرتبط با آن، می‌بین تدبیر کیفری بوده که سرعت و قطعیت در اجرای آن‌ها می‌تواند در پیش‌گیری و مقابله با این جرایم نقشی مهم داشته باشد. بر اساس تدابیر غیر کیفری نیز مواردی مانند آموزش‌ها در دو سطح عمومی و تخصصی، آگاهسازی و خنثی‌سازی می‌تواند در جلوگیری از این جرایم مؤثر واقع

هرزنامه‌هاستفیلتینگ با پایه نیز با هدف محدودکردن و کنترل دسترسی به شبکه یا برخی از خدمات به کار گرفته می‌شود. استفاده از پروتکسی‌ها نیز به دو طریق در بالا بردن امنیت اینترنت به کاربران یاری می‌رساند. نخست از میان بردن آی پی (IP) که موجب مخفی ماندن کاربر در اینترنت شده و مانع در نفوذ هکرها محسوب می‌شود. دوم جلوگیری از اتصال مستقیم کاربر به اینترنت و متصل کردن وی از طریق پروتکسی که سبب افزایش امنیت می‌شود.

- [۳۰] اسرای، م و مشیراحمدی، ع. ر. نقش پلیس در حفظ حریم خصوصی فضای سایبر، مقاله ارائه شده در نخستین همایش ملی سبک زندگی، نظم و امنیت، (۱۳۹۴). زنجان.
- [۳۱] فربیزی، ا. سیر تحول قوانین مرتبط با جرایم رایانه‌ای در ایران و جهان. *فصلنامه تخصصی فقه و تاریخ تمدن*, ۱۵۷-۱۸۵، سال هفتم، شماره ۲۷، (۱۳۹۰).
- [۳۲] عالیپور، ح. حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)، چاپ دوم، تهران: خرسندي. (۱۳۹۲).
- [۳۳] دادبان، ح و آقایی، س. بازدارندگی و نقش آن در پیشگیری از جرم *فصلنامه حقوق دانشکده حقوق و علوم سیاسی*, (۱۳۸۷)، دوره ۳۹ شماره ۳، ۱۴۸-۱۲۵.
- [۳۴] بهره‌مند، ح. کوره پز، ح. م و سلیمی، ا. راهبردهای وضعی پیشگیری از جرایم سایبری، آموزه‌های حقوق کیفری، (۱۳۹۳)، شماره ۷، ۱۷۶-۱۴۷.
- [۳۵] صادق نژاد نایینی، م. جرم شناسی (بزه دیده شناسی علت شناختی). *تقریرات درس دکتر نجفی ابرندآبادی*. (۱۳۸۷).
- [۳۶] جلالی فراهانی، ا. ح و منفرد، م. حمایت قانونی از آسیب دیدگان سایبری، *فصلنامه مجلس و راهبرد*, (۱۳۹۲)، سال بیستم، شماره ۷۳، ۱۵۶-۲۰۰.
- [۳۷] رایجیان اصلی، م؛ سلیمی، ا و نوریان، ع. ر. پیشگیری از جرایم رایانه‌ای از رهیافت نظری تا رهیافت جهانی در پرتو رهنمود پیشگیری از جرم سازمان ملل. *فصلنامه مطالعات راهبردی جهانی* شدن، (۱۳۹۳)، سال پنجم شماره ۱۳ (۱۶ پیاپی)، ۲۱۶-۱۸۹.
- [۳۸] برومند باستانی، ب. جرایم کامپیوتروی و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ دوم، تهران: بهنامی. (۱۳۸۶).
- علیرضا مشیراحمدی هم‌اکنون دانشجوی مقاطع دکترای دانشگاه فردوسی مشهد است. مقاطع کارشناسی ارشد را در سال ۹۶ در دانشگاه فردوسی و مقاطع کارشناسی را در دانشگاه پیام نور مشهد به پایان رسانده است. زمینهٔ پژوهشی مورد علاقهٔ ایشان، جرایم سایبری، قصور و تخلفات پژوهشی و فلسفه حقوق است.**
- [۱۶] عالیپور، ح. حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)، چاپ دوم، تهران: خرسندي. (۱۳۹۳).
- [۱۷] y. jewkes, Crime Online, First edition, Willan Publishing, 2007.
- [۱۸] زندی، م. ر. تحقیقات مقدماتی در جرایم سایبری، چاپ اول، تهران: جنگل جاودانه. (۱۳۸۹).
- [۱۹] ظاهری، س و شیخ الاسلامی، ع. جرم شناسی (جهانی‌شدن جرم). *تقریرات درس دکتر نجفی ابرندآبادی*. (۱۳۹۱).
- [۲۰] بابایی، م. ع. ، جهانی‌شدن جرم: ضرورتی پیش رو مطالعات و تحقیقات جرم‌شناسی، آموزه‌های حقوق کیفری، (۱۳۹۰). دوره جدید شماره ۱، ۱۳۶-۱۱۵.
- [۲۱] l. j. Seigel, *The core Criminology*, usa, Wadsworth, Cengage Learning, 2011.
- [۲۲] s. m. Zanchetti, *Value, built heritage and cyberspace*, museum, vol.54 (3), pp.19-28, 2002.
- [۲۳] شکرخواه، ا. فضای مجازی؛ ملاحظات اخلاقی، حقوقی و اجتماعی، چاپ اول تهران: مؤسسه انتشارات دانشگاه تهران. (۱۳۹۰).
- [۲۴] جوان جعفری، ع. ر. جرایم سایبری و رویکرد افتراقی حقوق کیفری، *مجله دانش و توسعه*, (۱۳۸۹)، شماره ۳۴، ۱۹۳-۱۷۰.
- [۲۵] برومند باستانی، ب. جرایم کامپیوتروی و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ دوم، تهران: بهنامی. (۱۳۸۶).
- [۲۶] جوان جعفری، ع. ر. جرایم سایبری و رویکرد افتراقی حقوق کیفری، *مجله دانش و توسعه*, (۱۳۸۹)، شماره ۳۴، ۱۹۳-۱۷۰.
- [۲۷] حاجی‌ده‌آبادی، ا و سلیمی، ا. اصول جرم انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرائم رایانه‌ای). *فصلنامه مجلس و راهبرد*, (۱۳۹۳)، ۲۱ (۸۰)، ۶۱-۸۸.
- [۲۸] ابراهیمی، ش و صادق نژاد نایینی، م. تحلیل جرم شناختی جرایم اقتصادی، پژوهش حقوق کیفری، (۱۳۹۳)، سال دوم، شماره پنجم، ۱۴۷-۱۷۴.
- [۲۹] عاملی، س. ر. در زمان مجازی (مجموعه مقالات)، تهران: بعثت. (۱۳۸۸).



علیرضا مشیراحمدی هم‌اکنون دانشجوی مقاطع دکترای دانشگاه فردوسی مشهد است. مقاطع کارشناسی ارشد را در سال ۹۶ در دانشگاه فردوسی و مقاطع کارشناسی را در دانشگاه پیام نور مشهد به پایان رسانده است. زمینهٔ پژوهشی مورد علاقهٔ ایشان، جرایم سایبری، قصور و تخلفات پژوهشی و فلسفه حقوق است.

اطلاعات
تکامل
توپید
فنای
اینستی
علتی رویی
فصل نام

