تحلیل جرم‌شناختی جرایم سایبری

علیرضا مشیراحمدی

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

چکیده

شکل‌گیری 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 روبه‌رشد برای سیاست عمومی بدل شود؛ بنابراین لازم است تا برای درک صحیح و جلوگیری از این جرایم، همه ابعاد لازم در این خصوص موردتوجه قرار گیرد. در این مقاله قصد داریم تا ضمن تبیین مفهوم، خصوصیات و چالش‌های موجود در مواجهه با جرایم سایبری، تدابیر پیش‌گیرانه و مقابله با آن را نیز موردبررسی قرار دهیم.

واژگان کلیدی: جرایم سایبری، محیط سایبر، پیش‌گیری کیفری، پیش‌گیری غیر کیفری

۱- مقدمه

امروزه فضای مجازی تبدیل به دنیای مستقل شده و باید گفت، دنیای مجازی دیگر تنها عنوانی از مَجاز 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 به‌موازات دنیای واقعی، جرایم در دنیای مجازی نیز در حال شکل‌گیری است. بنابراین پیوندی ناگسستنی میان دنیا یا فضای واقعی و مجازی برقرار بوده و هرروز نیز بر این آمیختگی و وابستگی افزوده می‌شود. شاید در وهلهٔ نخست این‌چنین تصور شود که اتفاق و تغییر خاصی به وجود نیامده و فقط وسیله ارتکاب جرم است که دگرگون شده، امّا 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 بشری نتوانستند خود را به‌لحاظ حقوقی با آن هماهنگ کنند. به تعبیری دیگر، سرعت هماهنگی و برنامه‌ریزی به‌منظور مقابله با جرایم حادث‌شده در فضای مجازی با سرعت بسیار پایینی صورت می‌پذیرد. به‌عنوان مثال تحولات ایجادشده در صنعت حمل‌ونقل، عاملی در شکل‌گیری جرایم نوین شد؛ اگرچه ورود و بهره‌گیری از هواپیما سبب تسریع و سهولت در جابه‌جایی مسافران شد، امّا جرایمی را نیز به‌مانند هواپیماربایی به‌دنبال داشت. در چنین حوزه‌هایی بشر توانست با فاصلهٔ زمانی اندکی از حیث شیوه‌های قانونی، پیش‌گیری و مقابله خود را با جرایم هماهنگ کند. درحالی‌که تحولات رخداده در زمینهٔ جرایم سایبری به‌هیچ‌عنوان 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 دومین 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. به‌عنوان‌مثال نمی‌توان تعریفی واحد از سرقت را چه در فضای سایبر و چه در دنیای واقعی به‌کار بست. زیرا اگرچه در جهان واقعی مالی ربوده 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 فریفتن او مصداق 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 بیش‌ازپیش احساس شود. به همین منظور در ادامه نخست به تبیین مفهوم، طبقه‌بندی و

*نویسندهٔ مسؤول

[Downloaded from monadi.isc.org.ir on 2026-11-21]
[DOR: 20.1001.1.24763047.1398.8.1.4.0]

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] امّا آغاز توجه جدی به این‌گونه 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 شبکهٔ جهانی در سال ۱۹۹۰ ، فزونی و رویه روبه‌رشد 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 مصادیق و تشریح این‌چنین اعمالی بیشتر شود. به‌طورکلی باید گفت، به‌منظور تبیین و تعریف این جرایم، نظرات بسیاری ارائه شده، اما با توجه به گستردگی و عدم تعیین دقیق مصادیق، اجماعی در این خصوص حاصل نشده است. قانون‌گذاران کشورهای مختلف، حقوق‌دانان، جرم‌شناسان و اسناد بین‌المللی و منطقه‌ای هر یک به فراخور تهدیدات و نیازها، تعاریف متفاوتی را در این رابطه ارائه کرده‌اند که در ادامه به برخی از آن‌ها اشاره می‌کنیم:

دستهٔ نخستِ تعاریف ارائه‌شده 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. [۳] 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، گفته‌شده که هر جرم و جنایتی که از رایانه و شبکه به‌عنوان 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 فن‌آوری 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 ارائه‌شده را باید سرچشمه‌گرفته از نظرات مراجع و سازمان‌های جهانی و بین‌المللی دانست. جنبه جهانی و فراملی جرایم سایبری موجب شد تا این مراجع درصدد 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 ارائه‌شده از جانب انجمن 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 به‌کاررفته در ارتکاب جرم حائز اهمیت بوده و بنابر تعریف ارائه‌شده از این سازمان، جرایم سایبری ممکن است، دربردارنده فعالیت‌های مجرمانه‌ای باشد که ماهیتی سنتی دارند؛ امّا با استفاده از ابزاری مدرن و نوین ازجمله اینترنت، رایانه و دیگر ابزارهای تشکیل‌دهنده فضای سایبر محقق می‌شود. [۱۲]

مجموعهٔ این تعاریف درواقع، نگرشی دوگانه را نسبت به جرایم سایبری مطرح کرده‌اند، با این توضیح که تمرکز برخی از تعاریف بالا، دربردارندهٔ مفهومی مضیق از این جرایم بوده و بر همین مبنا جرایم سایبری را بزه‌هایی دانسته‌اند که

---

[۱] شرکت بل اقدام به استخدام تعدادی از نوجوانان به‌منظور پاسخ‌گویی و متصل‌کردن تماس‌های تلفنی به مشترکان کرد. این افراد علاوه‌بر توهین و برخورد نامناسب با مشترکان، با ترفندهایی هوشمندانه در صفحه سوئیچ اتصال، 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 دستورالعمل‌های اضافی به برنامه حسابداری شرکت، قیمت کالاها را با ظرافت خاصی تغییر می داد؛ و ارقام حاصله از این راه را به حساب‌های مخصوصی واریز کرده و در فواصل زمانی معین اقدام به برداشت از این حساب‌ها می‌کرد، اما درنهایت چون شیوه‌ای برای متوقف‌سازی این عملکرد پیش‌بینی نشده بود وی با مراجعه به مراجع قضایی، اعتراف به این جرم کرد.

[3] O.E.C.D

[4] AIDP

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

در بستر فناوری و با روش‌های جدید صورت می‌گیرد، در مقابل موردتوجه قرارگرفتن مفهوم گسترده یا توصیفی از این جرایم سبب شده تا طیف گسترده‌ای از جرایم که گاهی با شیوه‌ای به‌طورکامل نوین و گاهی نیز به شکل سنتی و با استفاده از فناوری جدید ارتکاب می‌یابند، به‌عنوان جرایم سایبری معرفی شوند. [۱۳] 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 بی‌فایده است؛ زیرا سرعت تغییرات فناورانه به‌زودی هرگونه تعریفی از این قبیل را بی‌استفاده خواهد کرد؛ [۱۴] امّا چنین تفسیری قابلیت دفاع نخواهد داشت؛ زیرا نخست این‌که عدم تعریف این جرایم موجب ناشناختگی آن‌ها شده و ناتوانی دولت‌ها در برنامه‌ریزی، پیش‌گیری، مقابله و تخمین میزان خسارت وارده را به‌دنبال خواهد داشت. دوم این‌که بزه‌دیدگان نیز به‌دلیل فقدان تعریف، در احقاق حق خویش دچار سردرگمی شده و معیاری برای طرح شکایت خویش نخواهند داشت. سوم این‌که 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 مصادیق آن هماهنگی کامل میان مراجع داخلی و بین‌المللی وجود نداشته باشد. به‌عنوان 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 صورت‌گرفته در ادوار مختلف به موضوع بنگریم، آنچه را که امروزه جرم سایبری می‌نامیم، حاصل تحول سه عصر یا دوره متفاوت است. عصر نخست به زمان ایجاد نخستین دستگاه‌های رایانه‌ای و عمومیت ابتدایی و اولیه استفاده و به‌کارگیری از آن‌ها باز می‌گردد. در این دوره برجسته‌ترین فعالیت‌های ناروا و غیرقانونی شامل ایجاد اختلال در عملکرد دستگاه‌های رایانه‌ای و دست‌کاری 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 عمده جرایم ارتکابی در ارتباط با رایانه‌ها بود که محقق می‌شد. [۱۵] ویژگی اصلی اعمال دوره نخست آن بود که این‌گونه اقدامات غیرمجاز در وسعتی کم تحقق 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 مبنا دستگاه‌های رایانه‌ای در صورتی ایمن محسوب می‌شدند که داده‌های آن‌ها واجد سه عنصر محرمانگی[۲]، تمامیت[۳] و دسترس‌پذیری[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 قرارداشتن داده‌های مجاز که متعاقب حفاظت مطلوب از دستگاه‌ها صورت می‌پذیرد نیز مبین مؤلفه سوم است؛ بنابراین در این دوران اقداماتی که منجر به افشا یا در دسترس قرارگرفتن داده‌ها شده و یا نقص و تغییری در آن‌ها به‌وجود می‌آورد، جرم نامیده می‌شد. اگرچه بازهٔ زمانی این دوره از جرایم کوتاه بوده و با فاصلهٔ اندکی جرایم عصر سوم ظهور 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 اوایل 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
[3] Integrity
[4] Accessibility

[۵] برای نمونه در بخش اول از فصل دوم کنوانسیون جرایم سایبر 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.

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

حملات رایانه‌ای گزارش شده است. گسترش بهره‌گیری از اینترنت و پوشش خبری گسترده 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 به‌دنبال آن رشد جرایم سایبری بود.

۳-۲- 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 تحقق آن رایانه، یا نقش موضوع جرم و یا نقش وسیله جرم را دارد؛ پس هرگاه در دسته‌بندی ارائه‌شدهٔ جرایم از منظر وسیله جرم موردتوجه قرار گیرند، رایانه واجد نقشی فعال فرض شده که بزه به کمک آن تحقق می‌یابد، اما هرگاه از زاویه موضوع جرم به ماجرا نگریسته شود، برای رایانه نقشی منفعل موردتوجه قرارگرفته که موضوع رفتار مجرمانه واقع می‌شود. [۱۶] البته با توجه به آن‌که 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 به‌عنوان نقش کمک‌رسان یا مداخله‌گر یاد کرد.[۱] با توجه به این تفاسیر، ارائه طبقه‌بندی بر پایه نقش رایانه را می‌توان شامل موارد زیر دانست:

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

ب-رایانه به‌عنوان وسیله جرم، به‌مانند جرایمی از قبیل پول‌شویی یا کلاه‌برداری رایانه‌ای

ج- رایانه به‌عنوان مداخله‌گر در ارتکاب جرم، مانند پورنوگرافی[۲]

۳-۳- معیار موضوع جرم

این طبقه‌بندی دربردارنده معیارهایی است که رفتار مجرمانه نسبت به آن محقق می‌شود. جرایم داخل در این دسته، گاه 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 مبنا 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 تعبیری 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؛ به‌عنوان‌مثال 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 کلاه‌برداری یا جعل رایانه‌ای، جرایم بر ضد حریم خصوصی اشخاص و یا جرایم بر ضد امنیت ملی. به این طبقه‌بندی دو ایراد اساسی را می‌توان وارد ساخت. از یک‌سو بخش عمده جرایمی تحقق‌یافته 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 به‌نوعی مشابهت در تحقق برخی جرایم در هر دو فضا قابل‌مشاهده است، امّا 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 به‌الزام 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 روبه‌رو 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.

---

[۱] 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 آن‌که به‌کارگیری و استفاده از رایانه در تحقق برخی از جرایم به‌عنوان وسیله اصلی دخالت داشته و در برخی دیگر از جرایم واجد نقشی فرعی یا اتفاقی است، می‌بایست میان این حالت‌ها تفکیک قائل شد.

[2] Pornographic

[۳] جرایمی مانند جعل و کلاهبرداری رایانه‌ای، جاسوسی رایانه‌ای، هرزه نگاری اینترنتی، نقض حریم خصوصی و... 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 حامل ها از سامانه‌های رایانه‌ای، پخش برنامه‌های مخرب نظیر ویروس‌ها و کرم ها در فضای سایبر و در این دسته قرار می‌گیرند.

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

۳-۴- معیار تلفیقی

طبقه‌بندی تلفیقی دربردارنده همان دسته‌بندی‌های رایج است، اما با توجه به آن‌که عده‌ای معتقدند تفکیک دقیق جرایم سایبری از یکدیگر ممکن نیست، لذا لازم است تا عناوین مشابه در دسته‌های کلی‌تر جای گیرند. به تعبیری دیگر ازآنجایی‌که 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، روی‌آوردن به چنین معیاری اجتناب‌ناپذیر است. به‌طوراصولی گزینش چنین شیوه‌ای به‌وسیله سازمان‌ها، کنوانسیون‌ها و یا در اسناد بین‌المللی مورداستفاده قرار می‌گیرد. البته به‌موازات تلاش‌های مجامع بین‌المللی؛ حقوق‌دانان، 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 مصادیق بزه‌های سایبری که از مشکلات حقوقی در حوزه جرایم رایانه‌ای ناشی شده بود، باید به اقدامات OECD مرتبط دانست. کمیته‌ای اختصاصی از این سازمان در یک دوره سه‌ساله مشغول بررسی راه‌کارهای ممکن برای ایجاد هماهنگی بین‌المللی قوانین کیفری، به‌منظور مقابله با جرایم 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 به‌وسیله AIDP بر نقش آن تأکید شد. سازمان‌ها و نهادهای منطقه‌ای و بین‌المللی دیگر ازجمله اینترپل و کنوانسیون اروپایی جرایم سایبری نیز تلاش‌های بعدی در تبیین تقسیم‌بندی از این جرایم را به انجام رسانده‌اند. که دسته‌بندی ارائه‌شده اینترپل بیشتر مبتنی بر اصول پلیسی بوده که فاقد جامعیت و مانعیت کافی است، و دسته‌بندی کنوانسیون اروپایی نیز به‌صورت حداقلی و جزئی ارائه شده است. به‌طورکلی 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 محتوا ۳- جرایم محض سایبری و ۴- جرایم مخابراتی دانست. در دسته نخست بزه‌هایی جای می‌گیرند که درگذشته نیز وجود داشته‌اند، امّا با توجه به تغییرات جزئی یا کلی در عنصر مادی‌شان به‌عنوان جرایم سایبری از آن تعبیر شده و قوانین مجزا و یا ویژه‌ای نیز 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 محتوا 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 به‌صورت مجزا موردبحث قرار می‌گرفتند،[1] اما با تلفیق محیط سایبر با حوزه مخابرات جرایم نوینی 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 نوشتن، 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 نوینی از جرایم را به‌دنبال داشته است. اگرچه تحقق برخی از جرایم علاوه‌بر دنیای واقعی در دنیای مجاری نیز قابل‌مشاهده است (که البته از نظر شیوه و شرایط ارتکاب، تفاوت میان دو فضا مشهود است)، امّا برخی دیگر از جرایم تنها در بستر اینترنت است که ظهور می‌یابند. بنابراین وجه مشترک این جرایم را باید بهره‌گیری از اینترنت و داده‌های[2] اینترنتی دانست. پس موضوع جرم در این جرایم اینترنت بوده که بزه در آن و یا به‌وسیله آن محقق می‌شود. به بیانی دیگر شکل‌گیری این جرایم را باید جنبه نهان و توالی ناخواسته

[1] این جرایم در گذشته فقط شامل هر گونه رفتاری بود که ضد ارتباطات تلفنی و مخابراتی ارتکاب می‌یافت؛ مانند دسترسی غیر مجاز به خطوط تلفن.

[2] Data

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

جهانی‌شدن دانست. با جهانی‌شدن ارتباطات، ترقی و تعالی فناوری، سهولت در امر آمدوشد و حذف مرزهای گمرکی و سیاسی، بزه‌کاران نیز از این مواهب به نفع خویش سود جسته و فرصت‌های نوینی را برای ارتکاب جرایم پیداکرده‌اند. [۱۹] بنابراین اگرچه توقع 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 دست‌یابی 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 به‌سرعت در حال تغییر و تحول بوده و روزانه با طرح و شیوه‌های جدید در حال خلق‌شدن است؛ دوم این که کشف این جرایم از طریق کانال‌های سنتی کشف جرایم مشکل است؛ و سوم این که کنترل این جرایم مستلزم مهارت‌های فنی و تخصصی است که با مهارت و تخصص مرتکبین مطابقت داشته باشد. [۲۱] مهم‌ترین چالش‌های موجود در این حوزه را می‌توان شامل موارد زیر دانست:

۴-۱- سرعت رشد و سهولت ارتکاب جرم

تسریع 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 فعال 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 به‌سرعت به انجام انواع مختلف فعالیت‌ها بپردازند. وقوع جرایم در این حوزه نیز از این قاعده مستثنا 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 به‌سرعت در حال تغییر بوده و این کار برنامه‌ریزی، قانون‌گذاری، پیش‌گیری و مقابله را با مشکل مواجه می‌سازد. علاوه‌براین، 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 جابه‌جایی پول در هر نقطه از دنیا همین یک وسیله کفایت می‌کند. این در حالی است که در دنیای واقعی ارتکاب جرم مستلزم وجود ابزار است، یعنی هر جرمی اقتضای تهیه و به‌کارگیری نوع خاصی از وسایل را دارد. پس ارتکاب جرم در محیط سایبر فاقد یکی از محدودیت‌های موجود در محیط فیزیکی است.

۴-۲- 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 به‌دلیل 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 یکی 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 آن‌که الگوها به‌شدت گسترده و متعدد بوده و به‌سرعت نیز تغییر می‌یابند، توسل و دسترسی به چنین ویژگی‌ای میسر نیست. به تعبیری دیگر، در نگرش سنتی به تحقق جرایم، با توجه به شناختی که اغلب بزه‌دیده 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 به انجام می‌رسید؛ این در حالی است که چنین قابلیتی در ارتباط با جرایم نوین وجود نداشته و به‌نوعی کار جستجو و کنترل دشوارتر می‌شود.

۴-۳- فرامکان و فرازمان‌بودن

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[1] نیز نامیده شده، مؤلفه‌ای در حذف مرزهای جغرافیایی محسوب می‌شود. به بیانی دیگر جهانی‌شدن فرایندی اجتماعی است که در آن محدودیت‌های جغرافیایی بر فرهنگ و دیگر ابعاد زندگی اجتماعی انسان‌ها کاهش‌یافته و موجب نزدیکی اشخاص و فرهنگ‌ها به یکدیگر می‌شود. بنابراین جهانی‌بودن گستره 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. به‌عنوان‌مثال با استفاده از قابلیت‌های چندرسانه‌ای[2] امکان برگزاری جلسات ویدئو کنفرانس در سرتاسر جهان نیز به‌وجود آمده، که دارای ارزش بالایی است. بنابراین با وجود چنین قابلیت‌هایی در محیط سایبر، دیگر تنها

[1] globalization
[2] Multimedia

[Downloaded from monadi.isc.org.ir on 2026-11-21]
[DOR: 20.1001.1.24763047.1398.8.1.4.0]

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 به‌طوراصولی جابه‌جایی، زمان‌بر بوده و عاملی در شناسایی مجرم محسوب می‌شود. یعنی در دنیای واقعی فاصله‌ای باید پیموده شود، از مرز یا 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 به‌منظور تحقق بزه ضروری است؛ همه این موارد به‌عنوان مانعی در ارتکاب جرم قابل‌طرح 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 روبه‌رو نیستند. یعنی زمان در این فضا دارای معنایی متفاوت بوده که با سرعت نور انطباق یافته و حرکت‌ها به‌صورت لحظه‌ای صورت می‌پذیرند. [۲۲] به بیانی دیگر وجود خصوصیات فضای مجازی ازجمله 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 درحالی‌که در فضای واقعی عمل مجرمانه ماهیتی موقتی و زمان‌مند دارد، در فضای مجازی می‌تواند به‌صورتی پایدار و مستمر ادامه پیدا کند؛ [۲۳] درنتیجه وجود دو متغییر فرامکان‌بودن و فرازمان‌بودن موجب شده تا نوع آسیب‌ها و جرایم محیط سایبری بسیار متمایز و متفاوت از محیط فیزیکی باشد.

۴-۴- مقیاس جرم و فراگیری آن

در جرایم سنتی به‌طورمعمول مقیاس جرم یک در برابر یک است. یعنی تقابلی میان مجرم و قربانی وجود دارد. یک سارق یک سرقت، 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 تحقق هر بزه به‌صورت جداگانه هستند؛ امّا در فضای سایبر چنین مقیاس و محدودیتی وجود نداشته و قربانی‌کردن هزاران یا میلیون‌ها نفر به‌طور همزمان در این محیط امری واقعی و قابل تحقق است؛ درنتیجه در این وضعیت تعداد جرایم بالا رفته و به‌دنبال آن امر پیش‌گیری و مقابله کاهش می‌یابد؛ [۲۴] هم‌چنین تحولات صورت‌پذیرفته در محیط سایبر موجب شده تا نگرش به جرم نیز با دگرگونی مواجه شود؛ یعنی اگرچه درگذشته جرم بیشتر یک پدیده‌ای سرزمینی و در سطح ملی تلقی و تفسیر می‌شد، به‌کارگیری 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 انعکاس‌دهنده تعداد جرایم مکشوفه و یا جرایم واقعی در این حوزه دانست. دلیل عدم اعتنا 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 عمده را می‌توان در این زمینه مطرح ساخت: نخست ناشناختگی و سختی کشف این جرایم. دوم عدم تمایل بزه‌دیدگان به گزارش جرم، به‌خصوص در شرکت‌های بزرگ دولتی یا خصوصی به‌دلیل لطمه‌ای که به اعتبار آن‌ها واردشده و بزه‌دیده واقع‌شدن در این زمینه می‌تواند به‌عنوان نشانه‌ای از ضعف سیستم‌شان مطرح شود. سوم ضعیف‌بودن جنبه اخلاقی ارتکاب جرم در این حوزه که عاملی در کاهش سطح رؤیت‌پذیری و به‌دنبال گزارش‌دهی این جرایم بوده و طبیعتاً عدم بروز حساسیت از جانب افکار عمومی را نیز در پی خواهد داشت [۲۸]. بنابراین ازآنجایی‌که 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 انجام‌گرفته در محیط سایبر بیشتر به دیده سرگرمی، تفنن و تفریح می‌نگرند؛ درنتیجه رنگ اخلاقی جرم در این محیط ضعیف بوده و به همین علت افرادی که در دنیای واقعی تمایلی به ارتکاب جرم ندارند، در فضای سایبر به‌راحتی و سهولت مرتکب جرم می‌شوند.

۴-۶- وسعت و حجم خسارت حادث‌شده

رشد فناوری و دسترسی آسان به آن، بزه‌کاران را قادر ساخته تا با هزینه‌کردی اندک بتوانند خسارات هنگفتی را به بارآورند. به‌طورمعمول هر بزه‌کار با تهیه یک لپ‌تاپ یا تلفن همراه و نفوذ به شبکه‌های اطلاعاتی، سامانه‌های بانکی، سامانهٔ بورس

[۱] انجمن بین‌المللی حقوق جزا بر پایه گزارشی که از کشورهای عضو دریافت کرده‌است گزارش میزان اعلام این جرایم را صرفا ۵٪ اعلام کرده‌است. در همین رابطه سازمان اطلاعات امنیت آمریکا اعلام داشته که بین ۸۵ تا ۹۵ درصد این جرایم حتی کشف نیز نمی‌شوند. [۲۵] ، [۲۶] و [۲۷]

[Downloaded from monadi.isc.org.ir on 2026-11-21]
[DOR: 20.1001.1.24763047.1398.8.1.4.0]

و حتی حریم خصوصی اشخاص، به‌سهولت و بدون مواجهه با محدودیت‌های موجود در فضای فیزیکی، قادر خواهد بود تا ضررهای سنگین و گاهی جبران‌ناپذیری را به‌وجود 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 ازجمله امنیتی، نظامی، هسته‌ای، هواپیمایی، پزشکی و .... در به‌کارگیری از رایانه‌ها و اینترنت هرروز افزایش‌یافته و درنتیجه ایجاد خلل یا خدشه در این سامانه‌ها می‌تواند عواقب جبران‌ناپذیر و شدیدی را به‌همراه داشته باشد؛ درنتیجه سرعت و حجم بروز و تکثیر آسیب‌ها در محیط دیجیتال به‌هیچ‌عنوان قابل قیاس با محیط عینی و ملموس نبوده و ممکن است در اندک زمانی حجم وسیعی از خسارات به‌طور تصاعدی گسترش یابد. [۲۹]

۴-۷- 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. به‌طوراصولی برای جلوگیری ازاین‌گونه از جرایم نیاز به تمرکز بر سه پدیده داریم که عبارت‌اند از ۱-وسایل دیجیتال به‌عنوان ابزاری که برای ارتکاب جرم مورد استفاده قرار می‌گیرد. ۲- بزه‌کاری که منبع جرم است. و ۳- بزه‌دیده بی‌گناه در معرض جرم. پس رویکردی که در امر پیش‌گیری موردتوجه قرار می‌گیرد، باید شامل هر سه راه‌برد باشد.

۴-۸- پیش‌گیری مبتنی بر نقش ابزار جرم

رایانه و دیگر ابزار دیجیتال را باید به‌عنوان مهم‌ترین عاملی که در معرض تحقق جرایم سایبری قرار دارند، در نظر گرفت. این وسایل پل ارتباطی میان بزه‌دیده و بزه‌کار بوده که دارای کارکردی دوگانه است. با این توضیح که از یک‌سو این ابزار قابلیت نفوذ برای مجرمان را فراهم آورده و از سویی دیگر ابزاری برای بزه‌دیده‌واقع‌شدن قربانی خواهند بود. بنابراین اعمال برخی از تدابیر امنیتی و محافظتی از جانب اشخاص یا سازمان‌های در معرض خطر می‌تواند نقشی اساسی و مهم در عدم بزه‌دیده‌واقع‌شدن آنان ایفا کند. اهم این تدابیر را که گاهی علاوه‌بر سیستم‌های شخصی در سیستم‌های اداری نیز می‌تواند مورداستفاده قرار گیرد و برخی دیگر نیز فقط قابلیت استفاده در سیستم‌های دولتی و اداری دارند را می‌توان شامل موارد زیر دانست:

- خرید و نصب نرم‌افزار محافظ بر اساس ارزش هر یک از موارد؛
- طبقه‌بندی اطلاعات سیستمی بر اساس میزان اهمیت و درجه محرمانگی آن‌ها؛
- شناسایی نرم‌افزارها ، برنامه‌ها و فایل داده‌هایی که نیاز به کنترل و دسترسی ویژه دارند؛
- نصب نرم‌افزار دارای سازوکار کنترل دسترسی؛
- به‌کارگیری عاملی منحصربه‌فرد، به‌مانند فرم‌های شناسایی قابل‌اثبات، مانند یک کد کاربری یا رمز عبور مخفی برای هر کاربر؛
- رمزگذاری اطلاعات محرمانه ذخیره‌شده در رایانه؛
- ایجاد روشی برای بازیابی اطلاعات سیستم‌عامل به‌طوری‌که اگر از بین رفته و یا دچار اختلال شوند، تمامی داده‌های پشتیبانی‌شده به‌صورت برون‌خط ذخیره شوند. هم‌چنین اطمینان از پشتیبان گیری به‌طور منظم برای کمک به بازیابی اطلاعات؛
- پویش فایل‌های بارگیری شده برای ویروس‌یابی پیش از نصب و عدم بارگیری فایل‌های اجرایی نامأنوس و مشکوک.

۴-۹- پیش‌گیری مبتنی بر نقش بزه‌کاران

طیف گسترده‌ای از اشخاص مرتکبان جرایم سایبری را تشکیل می‌دهند که در رده‌های سنی مختلف و با انگیزه‌های متفاوت مرتکب این جرایم می‌شوند. تعیین سن مجرمان سایبری به‌صورت دقیق ممکن نیست، زیرا همین‌که شخص توانایی کار با رایانه را پیدا کرده و کمینه دانش مقدماتی در این زمینه را کسب کرده باشد، قادر خواهد بود تا مرتکب جرم شود. انگیزه یا اهداف چنین بزه‌کارانی نیز در سوق‌یافتن 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 قاچاق 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 به‌خصوصیات

[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 جرایم کلاه‌برداری اینترنتی، سرقت اینترنتی و جاسوسی در این دسته قرار می‌گیرند. انگیزه گروه سوم نیز فقط واردآوردن خسارت و آسیب بر دیگران بوده فارغ از آن‌که در پی کسب منفعت، تفنن و یا اثبات برتری خویش باشند. به‌طوراصولی افراد انتقام‌جو و یا اشخاصی که از مشکلات روانی رنج می‌برند، در این دسته جای می‌گیرند.

[Downloaded from monadi.isc.org.ir on 2026-11-21]
[DOR: 20.1001.1.24763047.1398.8.1.4.0]

مرتکبین و هم‌چنین ویژگی‌های خاص جرایم سایبری، راه‌بردهای 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 دربردارنده دو رویکرد کیفری و غیر کیفری باشد. رویکرد کیفری یا جرم‌انگاری، فرایندی است که به موجب آن قانون‌گذار با درنظرگرفتن ارزش‌ها و هنجارهای 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 به‌عنوان 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].

۴-۹-۱- تدابیر کیفری در مقابله با بزه‌کاران سایبری

جرم‌انگاری به‌عنوان یکی از تدابیر در زمینهٔ 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 به‌صورت 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 کم‌وبیش مؤثری را نیز به همراه داشته است. بنابراین اتخاذ تدابیر کیفری مستلزم آن است که دولت‌ها به تصویب قوانینی جامع و شفاف در زمینهٔ پیش‌گیری از جرایم سایبری پرداخته، به‌گونه‌ای که این قوانین دربردارندهٔ مصادیق مختلف این جرایم باشد؛ یعنی اگر فردی مرتکب جرمی سایبری یا رایانه‌ای شده و جرمش اثبات شد، بتوان آگاهانه وی را منطبق‌بر میزان جرمش محکوم ساخته و برایش حکم صادر کرد. در همین ره‌گذر کشورها سه اقدام یا الگوی مختلف را در راستای تدابیر 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 به‌عنوان قانونی ناپیوسته و مجزا نوشته و تصویب شود، امّا درنهایت منضم به قانون مجازات اسلامی و در در ادامه این قانون جای گرفت. [۳۲]

به‌طوراصولی با توجه به ویژگی‌های خاص جرایم سایبری، ضروری است تا تدابیر پیش‌گیرانه واکنشی در این زمینه، با تدابیر اتخاذشده در محیط واقعی متفاوت باشد؛ یعنی جرم‌انگاری در این محیط باید متمایز از محیط واقعی صورت پذیرد. در همین راستا و به‌منظور اتخاذ تدابیر 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 می‌پردازیم:

الف- جرم‌انگاری بزه‌های سایبری

ازآنجایی‌که تعاریف و بزه‌انگاری‌های موجود با رویکرد سنتی ممکن است در مقام عمل قادر به پوشش‌دادن اقدامات ضداجتماعی که در محیط سایبر رخ می‌دهد، نباشند، لازم است تا نسبت به بازتعریف جرایم در این حوزه اقدام شود. به‌عنوان مثال در جرم جعل یا استفاده از سند مجعول، 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 به‌طورمعمول اقدامات متقلبانه مرتکب، نسبت به سامانه و سیستم اعمال‌شده و نه انسان‌ها، پس یک کنترل مهم که فریب مال‌خورده است، نباید در اینجا جایگاهی داشته باشد. در غالب جرایم روی‌داده در محیط فیزیکی و سایبری وجود چنین تفکیک و تفاوت‌هایی 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. به‌عنوان نمونه یکی از اصلاحات مؤثر در تصویب جرایم سایبری، تصویب این جرایم به‌صورت مطلق است. با این توضیح که با ملحوظ‌داشتن 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 تحقق جرم نقشی نداشته اما در دسته دوم محقق‌شدن نتیجه جزء جدایی‌ناپذیر شکل‌گیری جرم است. به‌طوراصولی جرم‌انگاری به‌صورت مطلق مبین قصد مقنن 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

[Downloaded from monadi.isc.org.ir on 2026-11-21]
[DOR: 20.1001.1.24763047.1398.8.1.4.0]

وجود دارد، اتخاذ چنین تدبیری در مقابله با این جرایم نیز قابل دفاع است. به همین منظور مقنن ایران نیز در مواد ۷۲۹، ۷۳۰، ۷۳۲ و ۷۳۴ فارغ از توجه به نتیجه احتمالی، اقدامات یادشده در این مواد را به‌صورت 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. به‌طوراصولی پیروی از قواعد تعدد جرم نیز در اینجا فاقد کارایی لازم بوده و نمی‌توان به آن متوسل شد، زیرا در اینجا بحث شمارش فاقد موضوعیت است و باید گفت در برخی از جرایم حتی تعیین تعداد بزه‌دیدگان و بزه‌های تحقق‌یافته 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 به‌هیچ‌عنوان توسل به مجازات غیرانسانی و ناعادلانه نبوده، بلکه آن‌چنان مجازاتی است که به میزان کافی واجد خصیصه بازدارندگی عام و خاص باشد. علاوه بر لزوم سنگینی 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 بکاریا را مورد توجه قرار دهیم که "این شدت کیفر نیست که از جرم پیش‌گیری می‌کند، بلکه حتمی و قطعی‌بودن مجازات است که می‌تواند از جرم‌های آینده جلوگیری کند"، [۳۳] اهمیت تسریع در رسیدگی و مجازات مرتکبین روشن‌تر می‌شود. پس باید گفت اجرای صحیح و مناسب قانون بسیار بااهمیت‌تر 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 سویی 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 حتمیت و قطعیت در اجرای قوانین مرتبط با این حوزه است. درنتیجه یکی از مهم‌ترین و اساسی‌ترین طرق ارسال پیام به خلاف‌کاران، 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 درصورتی‌که بخواهند به چنین جرایمی ادامه دهند، می‌بایست بهای آن را نیز پرداخت کنند. پس اتخاذ تدابیر کیفری سنجیده و اصولی به همراه دقت، سرعت و قطعیت در اجرای آن را باید مکمل یکدیگر و طریقه‌ای اساسی در مقابله و پیش‌گیری از جرایم سایبری دانست.

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

با توجه به آن‌که صرف اتکا به تدابیر کیفری و جرم‌انگاری نمی‌تواند در مقابله با جرایم سایبری مؤثر واقع شود، لازم می‌آید تا تدابیر غیر کیفری نیز در مقابله با این جرایم مدنظر قرار گیرند. در همین راستا نباید از نقش آموزش و آگاهی‌سازی غافل شد. ازآنجایی‌که بسیاری از کاربران و استفاده‌کنندگان اینترنتی به جرایم حادث‌شده در این حوزه، به دیده سرگرمی نگریسته و قبح جرایم محقق‌شده در دنیای 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 اخلاق است؛ زیرا که چنین آموزش‌هایی ممکن است، موجب شود افراد مستعد خلاف‌کارشدن، 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 تدابیر آموزشی در محیط سایبر، درست به‌مانند تمام انواع آموزش‌های دیگر، یک سرمایه‌گذاری بلندمدت به‌خصوص در ارتباط با جوانان بوده که اهتمام به این امر نه‌تنها 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 تدابیر حساس‌سازی و آگاه‌سازی 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].

۴-۹-۳- پیش‌گیری مبتنی بر نقش بزه‌دیده

---

[۱] ماده ۷۲۹ هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد ...

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

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

ماده ۷۳۴ هر کس به‌طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب ... خواهد شد:

الف تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانهٔ 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 واردکردن متقلبانهٔ داده‌ها یا علائم به آنها.

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

بزه‌دیده را باید سومین رکن از ارکان جرایم سایبری دانست که در تحقق این جرایم می‌تواند نقشی بااهمیتی ایفا کند. توجه به تفش این اشخاص در وقوع جرم نخستین‌بار در دانش جرم‌شناسی موردتوجه قرار گرفت. در همین راستا و بر پایه بزه‌دیده‌شناسی علمی یا علت‌شناختی، در مواجهه با جرایم فقط نباید بر نقش مرتکب و بزه‌کار تمرکز کرد، بلکه لازم است تا سهم بزه‌دیده نیز در تحقق بزه موردتوجه قرار گیرد، زیرا جرم در همه حالات نشأت‌گرفته از عوامل شخصی و محیطی مربوط به مرتکب نبوده، بلکه بزه‌دیده نیز ممکن است، در تحقق بزه نقش داشته باشد. [۳۵] بر همین اساس جرم‌شناسان نقش یا کارکردی چندگانه را در ارتباط با بزه‌دیدگان تبیین کرده‌اند[1]؛ درنتیجه با توجه به آن‌که زوج کیفری (بزه‌کار و بزه‌دیده) همیشه به‌صورت سیاه‌وسفید نمایان نمی‌شود، یعنی آن‌که یکی به‌طورکامل گناه‌کار و دیگری بی‌گناه باشد، باید سهم و تأثیر رفتار آنان در وقوع جرم مورد ارزیابی قرارگرفته و بر همین اساس میزان مسئولیت هر یک تعیین شود. توجه به این مسائل عاملی خواهد بود تا بر پایه اطلاعات به‌دست‌آمده 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 مستثنا نبوده و حتی ویژگی جرایم در این فضای عاملی است که توجه به نقش بزه‌دیدگان در این جرایم اهمیتی دوچندان یابد. واقعیت امر نمایان‌گر آن است که در اغلب جرایم محقق‌شده در محیط سایبر، می‌توان اثری از نقش کم‌وبیش 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 مرتبط 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 تحقق جرم نخواهد داشت. (جوان جعفری، ۱۳۸۹: ۱۸۵) یعنی درصورتی‌که حتی مال‌باخته مرتکب سهل‌انگاری شده و مراقبت کافی را به خرج نداده باشد (به‌عنوان مثال درب منزل را باز گذارده باشد) و به همین سبب سرقتی رخ دهد، خدشه‌ای در ماهیت سرقت رخ‌داده به‌وجود نخواهد آمد.[2] اما در محیط سایبر برای آن‌که بتوان امر پیش‌گیری را توسعه بخشیده و به‌نحو مطلوب‌تر به انجام رساند، چنین رویکردی قابلیت دفاع نخواهد داشت. یعنی ضروری است تا در اینجا رویکردی افتراقی را در دستور کار قرارگرفته و تفکیک و تمایزی میان بزه‌دیدگان سهل‌انگار و غیر آن را لحاظ شود. هرچند در نگاه نخست چنین رویکردی می‌تواند به ضرر بزه‌دیده تعبیر 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 قرارگرفته است. همان‌گونه که در ماده ۷۲۹ ق.م.ا یا نخستین ماده از قانون جرایم رایانه‌ای مشخص است، اقدامات صورت‌گرفته درصورتی عنوان مجرمانه خواهد داشت که بزه‌دیده تدابیر امنیتی لازم و موردنیاز را به انجام رسانیده باشد. یعنی در صورت عدم رعایت چنین موضوعی این امکان وجود دارد که قربانی موردحمایت قرار نگیرد. به تعبیری دیگر درصورتی‌که مشخص شود بزه‌دیده نیز در تحقق جرم مرتکب تقصیر یا کوتاهی شده است، علاوه‌بر تقلیل میزان مسئولیت بزه‌کار، حتی امکان زایل‌شدن جرم و عنوان مجرمانه نیز وجود خواهد داشت. بنابراین بر پایه چنین سیاستی مقنن می‌کوشد 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 درصورتی‌که قربانی مرتکب تساهل نشده باشد، مقنن درصدد گسترش چتر حمایتی خویش از وی برمیاید. یعنی می‌کوشد تا به طرقی ازجمله تعریف شروع به جرم یا اقدامات مقدماتی به‌عنوان جرم کامل از شکل‌گیری بزه در همان بدو امر جلوگیری کند. بنابراین در این وضعیت مقنن در پی 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 علاوه‌بر ماده ۷۲۹ به ماده ۷۳۳ نیز اشاره داشت[3]، بر طبق این دو ماده اقداماتی چون صرف دسترسی و یا حتی قصد دسترسی به داده‌ها یا سامانه‌ها که درنهایت در زمره شروع به

[1] دسته‌بندی‌هایی مختلف از بزه‌دیده در علم بزه دیده‌شناسی ارائه شده است. گاه بر مبنای تقصیر بزه‌دیدگان به بزه‌دیده مقصر و غیر مقصر تقسیم شده‌اند. گاهی نیز سخن از بزه‌دیگان به‌طورکامل بی‌گناه، ناآگاه، به‌اندازهٔ بزه‌کار مقصر و بیش از بزه‌کار مقصر به میان آمده است. در پاره‌ای دیگر از موارد بزه‌دیدگان به بزه‌کار، بزه‌دیده، بزه‌دیده بالقوه و بزه‌دیده مکرر تقسیم شده‌اند. اهمان|

[2] هر چند ممکن است در احراز نوع سرقت یعنی حدی یا تعزیری بودن تفاوت وجود داشته باشد لیکن در تحقق اصل جرم تفاوتی در اینجا وجود نخواهد داشت.

[3] ماده ۷۳۳: هرکس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، ....

[Downloaded from monadi.isc.org.ir on 2026-11-21]
[DOR: 20.1001.1.24763047.1398.8.1.4.0]

جرم و اعمال مقدماتی قرار می‌گیرند، به‌عنوان 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، امّا چنین رویه‌ای در محیط سایبر دنبال نشده و باید گفت در برخی از جرایم محقق‌شده 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 به‌دلیل 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 تحقق آن جلوگیری کرد. البته باید توجه داشت که پذیرش و به‌کارگیری چنین رویکردهایی بسیار ظریف و خطرناک است، زیرا که در تقابل با اصول شناخته‌شده 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 مقنن در مواجهه با بزه‌دیدگان سایبری و با مدنظر قراردادن میزان رعایت تدابیر حفاظتی از جانب آنان، دو رویکرد مختلف را در دستور کار خویش قرار داده است؛ بنابراین ازآنجایی‌که هر شخصی در طول مدت زندگی‌اش ممکن است، در معرض بزه قرارگرفته و به‌نوعی بزه‌دیده بالقوه محسوب می‌شود، لازم است تا با به‌کارگیری تدابیری از وقوع چنین موضوعی جلوگیری کند. در محیط سایبری نیز اگرچه راه‌بردهای مختلفی قابل شمارش و بازگوکردن است، امّا توجه به دو رویکرد آگاهی‌بخشی و خنثی‌سازی از اهمیت بالاتری برخوردار است.

الف- آگاهی‌بخشی

اغلب عدم آگاهی و شناخت بزه‌دیدگان 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 محقق‌شده در این فضا می‌تواند مخاطره‌آمیزتر نیز باشد، زیرا به‌طوراصولی بسیاری از افراد به‌دلیل 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، تدابیر آموزشی عمومی و اختصاصی به‌صورت مداوم و هماهنگ تعریف و اجرا شود. [۳۶] در حوزه آموزش‌های عمومی، تدابیری از قبیل شناساندن مفهوم و انواع چالش‌های موجود، راه‌کارهای احتمالی مقابله و پیش‌گیری از آن و هم‌چنین ایجاد آگاهی نسبت به ارتقای کدهای رفتاری را می‌توان در دستور کار قرار داد. به‌طوراصولی با توجه به آن‌که جرایم سایبری به‌صورت سازمان‌یافته 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. به‌عنوان‌مثال 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 وارده برقرار است. یعنی با افزایش آگاهی فرد میزان بزه‌دیده واقع‌شدن وی کاهش و با عدم دانش یا کمبود میزان آن، احتمال قربانی‌شدن افزایش پیدا می‌کند.

ب- خنثی‌سازی

باید توجه داشت صرف کسب آگاهی نسبت به چالش‌ها و آسیب‌های موجود، به‌طور کامل نمی‌تواند در عدم بزه‌دیده‌گی شخص در محیط سایبر مفید واقع‌شده و لذا لازم می‌آید تا کاربران از ابزار و روش‌های امنیتی نیز به‌منظور دفع خطر بهره‌گیری کنند. مقصود از امنیت، تلاش و تدابیری است که می‌تواند در حراست از به‌خطرافتادن 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 زمینهٔ حفاظت از آسیب‌دیدگی جرایم سایبری به‌حساب آورد. به‌طورکلی سه نوع تدبیر امنیتی در حوزه جرایم سایبری می‌تواند موردتوجه قرار گیرد. نخست تدابیر حفاظتی فیزیکی که دربردارندهٔ فرایندی است برای جلوگیری از دست‌یابی غیرمجاز به سامانه‌های رایانه‌ای، به‌مانند نگهداری سامانه‌ها در محیطی امن، محدودکردن دسترسی افراد به سامانه‌ها و جلوگیری از آثار وارده بر سامانه‌ها در اثر مشکلات الکتریکی یا سخت‌افزاری است. به تعبیری دیگر این راه‌بردها درصددند تا ابزار ورود به محیط سایبر را از خطرات احتمالی محافظت کنند. دوم تدابیر نرم‌افزاری، که شامل کنترل دسترسی و دست‌یابی‌ها (پالایه)[1]، کنترل مراحل ورودی و خروجی‌ها، رمزنگاری‌ها، استفاده از دیواره آتشین،[2] استفاده از پروکسی‌ها[3] و نصب و به‌روزرسانی آنتی‌ویروس می‌شود[4]. با توجه به خصایص جرایم فضای سایبری که مبتنی بر موضوعات ناملموس و غیر فیزیکی است، بهره‌گیری از این

[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

[Downloaded from monadi.isc.org.ir on 2026-11-21]
[DOR: 20.1001.1.24763047.1398.8.1.4.0]

تدابیر بسیار حائز اهمیت است. سوم تدابیر سازمانی، که چنین تدابیری به‌طوراصولی در ارتباط با شرکت‌ها و سازمان‌ها موضوعیت یافته و جنبه شخصی ندارند. اقداماتی از قبیل انتخاب کارکنان متخصص و آموزش‌دیده، بازرسی 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 نشان‌دهندهٔ آن است که این جرایم از این محیط‌ها فراتر رفته و در بسیاری از زمینه‌ها به وقوع می‌پیوندند. بنابراین به‌موازات استفاده مشروع و افزایش بهره‌وری مفید از فضای سایبر، شکل‌گیری جرایم نوین و استفاده‌های غیرقانونی نیز در این محیط رشد و فزونی 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 علومی 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 مؤلفهٔ 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 مؤلفهٔ 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، مبین 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 شود؛ درنتیجه هر دو این تدابیر در جلوگیری و مقابله با جرایم سایبری مکمل هم محسوب می‌شوند.

هرزنامه‌هاستفیلترینگ با پالایه نیز با هدف محدودکردن و کنترل دسترسی به شبکه یا برخی از خدمات به کار گرفته می‌شود.

استفاده از پروکسی‌ها نیز به دوطریق 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 مانعی در نفوذ هکرها محسوب می‌شود. دوم جلوگیری از اتصال مستقیم کاربر به اینترنت و متصل کردن وی از طریق پروکسی که سبب افزایش امنیت می‌شود.

۶- مراجع

[۱] حسن بیگی، ا. حقوق و امنیت در فضای سایبر، چاپ اول. تهران: انتشارات موسسه فرهنگی مطالعات و تحقیقات بین الملل ابرار معاصر. (۱۳۸۴)

[۲] دی آنجلیز، ج، جرایم سایبر، (ترجمه حافظی سعید و خرم آبادی عبدالصمد)، چاپ اول، تهران: انتشارات دبیرخانه شورای عالی اطلاع رسانی. (۱۳۸۳)

[3] k Jaishankar, Cyber Criminology. London, crc press (Taylor & Francis Group). (2011).

[4] S. Furnell, Cyber crime: Vandalizing the information society. London: Addison Wesley. (2002).

[5] R -Moore, Cybercrime; investigating high-technology computer crime, Publisher: Anderson Publishing Co. (2005).

[6] y Jewkes, Crime Online, First edition, Willan Publishing, 2007.

[7] l. j. Seigel, The core Criminology, usa, Wadsworth, Cengage Learning, 2011.

[۸]عالی‌پور، ح.، حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)، چاپ دوم، تهران: خرسندی. (۱۳۹۳).

[۹]برومند باستانی، ب. جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ دوم، تهران: بهنامی. (۱۳۸۶).

[10] B, Seigel, Crime Prevention, Oxford Of Criminology, Great Britain, 2001.

[۱۱] بابا غیبی ازغندی، ع. ر. الگویی نوین برای پیشگیری از جرایم فضای سایبر، فصل‌نامه مطالعات پیشگیری از جرم، (۱۳۹۱)، شماره ۲۶، ۱۴۴-۱۸۸.

[13] 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 درپیشگیری ازجرایم سایبری وتأمین امنیت در فضای مجازی(پلیس فتا)، فصلنامه پژوهش های انتظام اجتماعی،(۱۳۹۱)، شماره ۱: ۱۰۴- ۱۲۴.

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

[۱۶] عالی‌پور، ح.، حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)، چاپ دوم، تهران: خرسندی. (۱۳۹۳).

[17] 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] طاهری، 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.

[21] l. j. Seigel, The core Criminology, usa, Wadsworth, Cengage Learning, 2011.

[22] s. m. Zancheti, Value, built heritage and syberspace, museum, vol.54 (3), pp.19-28, 2002.

[۲۳] شکرخواه، ی. 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 کامپیوتری 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).

[۳۰] اسرای، م و مشیراحمدی، ع. ر. نقش پلیس در حفظ حریم خصوصی فضای سایبر، مقاله ارائه‌شده در نخستین همایش ملی سبک زندگی، نظم و امنیت، (۱۳۹۴). زنجان.

[۳۱] فریبرزی، ا. سیر تحول قوانین مرتبط با جرایم رایانه‌ای در ایران و جهان. فصلنامه تخصصی فقه و تاریخ تمدن، (۱۳۹۰)، سال هفتم، شماره ۲۷، ۱۸۵-۱۵۷.

[۳۲] عالی‌پور، ح.، حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)، چاپ دوم، تهران: خرسندی. (۱۳۹۳).

[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]-بهره مند، ح. کوره پز، ح. م و سلیمی، ا. راهبردهای وضعی پیشگیری از جرایم سایبری، آموزه های 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 رایانه ای از رهیافت نظری تا رهیافت جهانی در پرتو رهنمود پیشگیری از جرم سازمان ملل. فصلنامه مطالعات راهبردی جهانی‌شدن، (۱۳۹۳)، سال پنجم شماره ۱۳ (۱۶ پیاپی)، ۲۱۶-۱۸۹.

[۳۸] برومند باستانی، ب. جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ دوم، تهران: بهنامی. (۱۳۸۶).



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

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

[Downloaded from monadi.isc.org.ir on 2026-11-21]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]

[DOR: 20.1001.1.24763047.1398.8.1.4.0]
[Downloaded from monadi.isc.org.ir on 2026-11-21]