مطالعات فقه و حقوق اسلامی
سال۱۴ ـ شماره ۲۶ ـ بهار ۱۴۰۱
صفحات ۳۲۳- ۳۵۸ (مقاله پژوهشی)

تدابیر پیشگیری از جرائم سایبری با تأکید بر اقدامات پلیسی با رویکردی فقهی

سید جمال موسوی* / محمد روحانی مقدّم** / مریم آقایی بجستانی***

تاریخ دریافت:۱۴۰۰/۰۷/۲۶ تاریخ پذیرش: ۱۴۰۰/۱۰/۱۳

چکیده

جرائم سایبری از جمله جرائمی است که مولود جامعه تکنولوژیک و مدرن می باشد و به همین دلیل، ابهامات زیادی در باب ماهیّت و پیشینه اینگونه جرائم از یک سو، و ویژگی های این جرائم و مرتکبان آنها از سوی دیگر وجود دارد. با عنایت به این ابهامات و نیز تفاوت های موجود بین جرائم سایبری و سایر جرائم، پیشگیری و مقابله با جرائم سایبری اقدامات پلیسی خاصّی را می طلبد. از جمله اقدامات پیشگیرانه در این خصوص می توان به حضور مؤثر پلیس در عرصه سایبری، آموزش همگانی و ارائه آموزش های خاص به افراد و سازمان هایی که در معرض جرم سایبر ی قرار دارند اشاره کرد. مواجهه با جرائم سایبری وپی جویی آنها از سوی پلیس، تخصّص ها و مراحل خاصّی را می طلبد؛ چراکه جرائم سایبر ویژگی هایی دارند که صحنه جرم آنها به گونه ای است که مأموران در صحنه جرم، علاوه بر اقدامات عمومی صحنه جرم باید اقدامات ویژه ای را نیز انجام دهند. بعد از مفهوم شناسی تحقیق و روش شناسی نسبت به رویکرد فقه حکومتی، گزاره ها و قواعد فقهی متعدّدی در اثبات حکم به وجوب ایجاد تمام ابعاد امنیّت در فضای سایبر از سوی حکومت اسلامی از جمله: قاعده التعزیر بما یراه الحاکم، حرمت حفظ کتب ضلال، حدّ محاربه و اخافه عمومی، حرمت تدلیس، نجش و اجحاف در تجارت، حرمت نقض حریم خصوصی و عدم ضمان به سبب دفع مطّلع بر حریم غیر و

* دانشجوی دکتری، گروه حقوق کیفری و جرم شناسی، واحد سمنان، دانشگاه آزاد اسلامی، سمنان، ایران
** دانشیار گروه فقه و مبانی حقوق اسلامی، واحد سمنان، دانشگاه آزاد اسلامی، سمنان، ایران(نویسنده مسئول)
rohani113r@gmail.com
*** دانشیار گروه فقه و مبانی حقوق اسلامی، واحد سمنان، دانشگاه آزاد اسلامی، سمنان، ایران

قاعده نفی سبیل مستند دانسته شدند. در نتیجه وجوب ایجاد امنیّت اعتقادی و مذهبی، امنیّت اخلاقی، امنیّت روانی، امنیّت آبرویی، امنیّت مالی و اقتصادی، امنیّت حریم خصوصی، امنیّت جانی و امنیّت اطّلاعات محرمانه ملّی در فضای سایبر به اثبات رسیده و بر اساس رویکرد فقه حکومتی و تمدّن‌ساز، علاوه بر رفتارهای سلبیِ حکومت، انجام رفتارهای ایجابی نیز ضروری دانسته شده است؛ لذا در این مقاله با روشی توصیفی- تحلیلی، ضمن بر شمردن اقدامات پلیسی در صحنه جرائم الکترونیکی، با عنایت به قانون جرائم رایانه ای به تبیین مهم ترین این جرائم پرداخته شده است.

کلیدواژه: جرائم سایبری، اقدامات پلیسی، تدابیر پیشگیرانه، رویکرد فقه.

مقدّمه

همزمان با گام نهادن بشر بر کره خاکی، حقوق نیز شکل گرفت؛ بدین معنا که زندگی بشری نظمی را می طلبید که گریزی از آن نبود. بدین ترتیب، می‌توان گفت رابطه مستقیمی بین حقوق از یک سو، و جامعه بشری از سوی دیگر وجود دارد که تغییر در یکی، تغییر دردیگری را به دنبال دارد. تغییر وتحولات رندگی بشری حدّی ندارد؛ به این معنا که هیچگاه به پایان نخواهد رسید، بنابراین حقوق و سیر تطوّر آن نیز فرآیندی است که همیشه وجود خواهد داشت.

یکی از دستاوردهای نوین بشر، خلق دنیایی در کناردنیای شناخته شده فیزیکی است. این دنیا که به فضای مجازی موسوم است، برای گذشتگان بی‌مفهوم بود و اگر هم مفهوم داشت، همعرض افسانه‌ها و خیال بافی‌ها قرار می‌گرفت. اما امروزه، این آروز تبدیل به واقعیّت گشته است و سیل عظیم اطلاعات و امور وجود دارند، ولی نه در دنیای فیزیکی؛ بلکه در فضای مجازی. لازم به ذکر است که فضای مجازی به معنای فضای دروغین و غیر واقعی نیست، بلکه به معنای دنیایی متفاوت با دنیای فیزیکی و بیرونی است که هزاران سال است که بشر آن را تجربه کرده است.

این فضای جدید تقریباً تمام ویژگی های دنیای واقعی را دارد. برای اغلب چیزهایی که در دنیای بیرونی وجود دارد، می‌توان ما به ازایی در این فضا یافت؛ از

امور مادی گرفته از قبیل کتاب الکترونیک، نامه الکترونیک و ... تا امور اعتباری و حقوقی از قبیل ازدواج اینترنتی، خرید و فروش اینترنتی، قتل اینترنتی، سرقت اینترنتی و ... .

بدین ترتیب، این سؤال به وجود می‌آید که این فضا و امور ناشی از آن چه ارتباطی به علم حقوق دارند؟ آیا این فضا، ضرورت درانداختن طرحی نو در عالم حقوق را طلب می‌کند یا می‌توان با مبانی سنّتی حقوق، همچنان به تدبیر در این زمینه پرداخت؟ می‌توان به صورتی دقیق تر نیز این سؤال را مطرح کرد: فضای مجازی و توابع آن در چه زمینه هایی از علم حقوق تأثیر دارند و در چه بخش‌هایی ضرورت تغییر در مبانی احساس می‌شود؟ از سوی دیگر، آن چه مهمّ است اقدامات و رویکرد پلیس به اینگونه جرائم است؛ چراکه هم ماهیّت و هم حیطه جرائم سایبری، با جرائم سنّتی متفاوت است و هم نحوه اثبات جرم و کیفیّت مجازات ها.

۱- ماهیّت جرم سایبری و اقسام آن

تاکنون تعاریف گوناگونی از جرم کامپیوتری و جرم مجازی از سوی سازمان های بین المللی، قانونگذاران و مراجع رسمی و غیر رسمی ارائه شده است که وجود تفاوت و گاه تعارض در آنها، بیانگر ابهامات موجود در ماهیّت و تعریف این جرائم می باشد. هنوز یک تعریف کلّی برای جرائم کامپیوتری به دست نیامده و به طور معمول به جای آن، تعاریفی کاربردی ارائه شده است. نکته قابل تأمّل این که این عبارت از دو بخش جرم و سایبر تشکیل شده است:

اندیشمندان حقوق، هر یک به نوبه خود و احیاناً بر اساس گرایش به مکتبی خاص، تعریف ویژه‌ای از جرم ارائه کرده‌اند. برخی جرم را «هر فعل مغایر اخلاق و عدالت» تعریف کرده‌اند. برخی دیگر گفته‌اند جرم، جریحه‌دار کردن آن بخش از حسّ اخلاقی است که احساسات بنیادی نوع خواهانه یعنی شفقت و درست‌کاری را شامل

می‌گردد (اردبیلی، ۱۳۸۵ :۱۱۹) در باب عبارت «سایبر»، تعریف جامع و شاملی که مورد اتفاق باشد – چه در دکترین و چه در رویّه قضایی بین المللی – وجود ندارد. با این وجود، با تحلیل لغوی و اصطلاحی از یک سو، و بررسی دیدگاه های اندیشمندان این حوزه از سوی دیگر می‌توان به تعریف نسبتاً جامعی نزدیک شد.

کلمه محیط سایبر برای اولین بار در سال ۱۹۸۲ در داستان‌های علمی تخیّلی به کار گرفته شد و در سال ۱۹۹۰ جان پری بارلو به هنگام صحبت در یک کنفرانس مجازی آنلاین از این اصطلاح استفاده کرد و آن را بر سرزبان ها انداخت. محیط سایبر، یک مکان فیزیکی و معمولی نیست. سایبر در اصطلاح به مجموعه‌هایی از ارتباطات درونی انسان ها از طریق کامپیوتر و وسایل مخابراتی بدون درنظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم آنلاین، نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرارکنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد. به عبارت دیگر، فضای سایبر، محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود در آن، زنده و مستقیم روی می‌دهد؛ در این محیط، تمام اطلاعات مربوط به روابط افراد، ملّت ها، فرهنگ ها و کشورها به صورت ملموس و فیزیکی (به صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی و به شکل دیجیتالی وجود داشته و برای همه استفاده کنندگان و کاربران قابل استفاده می‌باشد؛ کاربرانی که از طریق کامپیوتر، اجزای آن و شبکه‌های بین المللی به هم مرتبط اند (باستانی، ۱۳۸۳: ۵۶).

جرایم رایانه‌ای اصطلاحاً از سه نسل تشکیل می‌شوند: توضیح آن که دسته نخست جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن، موضوع جرم واقع می‌شود؛ مانند: سرقت و تخریب؛ دسته دوم جرایمی هستند که در آنها رایانه به عنوان ابزار

ارتکاب جرم به کارگرفته می‌شود، مثل کلاهبرداری، جعل و سرقت رایانه‌ای؛ و دسته سوم جرایمی هستند که در دنیای مجازی به وقوع می‌پیوندد اما آثار آنها در دنیای واقعی ظاهر می‌گردد؛ از قبیل نفوذ غیر مجاز، انتشار ویروس و کرم های رایانه‌ای؛ دسته اخیر را می‌توان جرایم سایبر در معنای اخصّ به حساب آورد (پرویزی، ۱۳۸۱: ۳).

بدین ترتیب می‌توان گفت: عبارت جرم سایبر تبدیل به مشترک لفظی شده که برخی را با ابهام در مفهوم این موضوع روبرو ساخته است. آن چه که از بررسی اسناد بین المللی از یک سو، و مکتوبات اندیشمندان حقوقی از سوی دیگر برداشت می‌شود این است که جرم سایبر در سه معنا به کار رفته است:

۱- جرم سایبر در معنای خاصّ: که آخرین نسل (نسل سوم) جرایم رایانه‌ای را تشکیل می دهد.

۲- جرم سایبر در معنای عامّ: که شامل هر سه نسل جرایم رایانه‌ای می‌شود و در این معنا مساوی با جرایم رایانه‌ای است.

۳- جرم سایبر در معنای اعمّ: که محدود به جرایم مربوط به رایانه نمی‌شود، بلکه مخابرات، پخش گسترده و تکنولوژی هایی از این دست را نیز که با فضای سایبر در ارتباط اند شامل می‌شود (دزیانی، ۱۳۸۵: ۴۳).

از نظر فقهی باید گفت که جواز جعل تعزیر برای اعمال حرام، حرمت اضرار به دیگران، حرمت ایذاء، حرمت ظلم، حرمت اتلاف مال غیر و نیز جواز جعل تعزیر برای اعمال مفسده آور که ریشه در مبانی فقهی نظیر آیات و روایات دارد از مهم تریم مبانی فقهی جرایم علیه رایانه یا خرابکاری رایانه ای (سابوتاژ) محسوب می شود که به دلیل رعایت اختصار از ذکر تفصیلی آن اجتناب می کنیم (جهت مطالعه ر.ک: بای و قهرمانی پور، ۱۳۸۸: ۱۱۵ به بعد).

۲- ویژگی های جرایم سایبری

با توجه به تاریخ تحوّل جرایم رایانه‌ای و جرایم سایبر، رسیدن به این نتیجه که جرایم اخیر با جرایم سنّتی تفاوت های بنیادینی دارند، کار دشواری نمی باشد. به عبارت دیگر، مقتضای جرایم سایبر که آن را از جرایم سنّتی متمایز می‌کند نه تنها در کمّیت، که در کیفیّت، ماهیّت، نحوه ارتکاب و ... در این جرایم است. بدین ترتیب، پرداختن به ویژگی های جرایم سایبر که نقطه فارق آنها از جرایم سنّتی می باشد، ضروری است.

۲-۱- جهانی و گسترده بودن

از ویژگی های منحصر به فردی که **فضای سایبر** را از دیگر رسانه‌ها ممتاز می‌سازد، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن به آسانی، به جدیدترین اطلاعات دست یابد. مرزهای جغرافیایی تا کنون نتوانسته از گسترش روزافزون **فضای سایبر** جلوگیری کند. از اینرو، هر نوع فیلتر و مرزبندی در برابر آن بسیار دشوار می نماید.

فضای مجازی همچون فضای واقعی، مکان، مسافت، اندازه، و مسیر دارد؛ مکان دارد از این جهت که اطلاعاتی که قرار است ذخیره گردد دررایانه ای ذخیره می گردد و از مکان مشخّصی قابل بازیابی است. مسافت دارد؛ بدین معنی که اطلاعاتی که باید انتقال یابند مسافتی را طی می کنند تا به مقصد برسند؛ اندازه دارد، از این جهت که اطلاعاتی که ذخیره می گردد در فضای معیّنی قابل ذخیره است؛ و مسیر دارد، بدین مفهوم که اطلاعاتی که قرار است منتقل شود از مسیر خاصی عبور می کند تا به مقصد معیّن برسد. با این همه، این مکان ها که از لحاظ مجازی بسیار گسترده اند به لحاظ فیزیکی بسیار کوچک اند؛ از نظر زمانی نیز دریافت و ارسال اطلاعات در واحد اندکی از زمان رخ می دهند؛ بنا براین با وجود این سرعت و گستردگی، کم حجمی فیزیکی چیزی از پهنه ی گسترده مجازی آن نمی کاهد.

بدین ترتیب فضای سایبر را باید یک محیط لایتناهی دانست. اما این فضای لایتناهی دائماً در حال قبض و بسط است؛ این قبض و بسط بدین معناست که ابعاد فضای سایبری هر لحظه می تواند گسترش یا کاهش یابد. به فضای سایبر می توان حامل های داده ای را متّصل نمود که حاوی ریزپردازنده هایی هستند؛ این ریزپردازنده ها دارای پتانسیل نگهداری اطلاعات در ظرفیّت بالایی بوده و با پیشرفت هایی که نحوه طرّاحی ترکیب ذخیره اطلاعات طی سالیان گذشته توسط مهندسین این صنعت داشته است موجب گردیده که این ریزپردازنده ها به لحاظ فیزیکی کوچکتر شوند؛ لکن در عین حال به لحاظ ساختاری توان ذخیره اطلاعات بسیار بالایی را داشته باشند. بر تعداد این ریزپردازنده ها و سخت افزارهای حامل داده می توان هر لحظه افزود و با ارتباط دادن آنها به یکدیگر در قالب شبکه های دیجیتالی گستره مجازی بی نهایتی آفرید. افزایش کاربران در سطح جهان هر ساله نوید بخش این امر است که گستره فضای مجازی روز به روز بیشتر می شود. ناگفته پیداست که کنترل چنین فضایی که هر لحظه در حال گسترش است و هر لحظه نیز می توان هرگونه اطلاعاتی- که در بسیاری موارد غیر قانونی است - را در آن انتشار داد بسیار مشکل و حتی بعضاً غیر ممکن است (فضلی، ۱۳۸۹: ۴۵).

۲-۲- جذابیّت و تنوّع

رسانه ها از فیلم، عکس، متن و یا هر هنردیگری برای جذّاب کردن خویش به کار می‌گیرند و این ابزارها در فضای سایبر قابل دستیابی است؛ به ویژه آنگاه که هیچ نظارت و فیلتری توان محدود کردنش را نداشته باشد. از ویژگی های منحصر به فردی که در تنوّع و جذابیّت **فضای سایبر** تأثیر بسزایی دارد، مشتری محوری محض است. در متون نوشتاری، ارتباطی تنگاتنگ میان خوانندگان و نویسندگان وجود دارد که خواننده به راحتی می تواند نظر خود را با شخص نویسنده در میان بگذارد. از سوی دیگر، امکان نظرسنجی و ارزیابی در این فضا بسیار آسان تر و روزآمد تر است و این

توانایی را به داده پردازان، فروشندگان و عرضه کنندگان محصولات اینترنتی می‌دهد که از آخرین خواسته های مشتریان و مخاطبان خود مطلع گردند (همان).

۲-۳- آزادی اطلاعات و ارتباطات

معنای واقعی آزادی اطلاعات، در **فضای سایبر** محقّق شده است. از اینرو شما هر نوع اطلاعاتی را که بخواهید - اعمّ از فرهنگی، سیاسی و اقتصادی - بدون محدویّت های حاکم بر دیگر رسانه ها، در **فضای سایبر** قابل دسترسی است. آزادی ارتباطی نیز از ویژگی های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حدّ، قابل دستیابی نیست (همان: ۴۶)

۲-۴- وسعت ضرر و خسارات وارده

با استعانت به تکنولوژی رایانه، مرتکبین با کمترین سرمایه و هزینه و با یک کپرایاه شخصی می‌توانند با ورود به شبکه اطلاعاتی و نفوذ در آن، خسارات هنگفتی وارد نمایند. سهولت ارتکاب با حجم زیاد موضوعات مطروحه، سرعت عملکرد رایانه، عدم نیاز به تخصّص خاص یا بالا و ... موجب گردیده تا حجم صدمات و خسارات وارده افزون گشته و گاه به چندین برابر جرایم معمولی برسد (باستانی، ۱۳۸۳: ۲۷).

۲-۵- سرعت

مفهوم متعارف زمان و مکان در دنیای مجازی دچار تحوّل شده است. یکی از عوامل کندی وقوع پدیده برهکارانه در جهان واقعی، بُعد مکانی میان سه ضلع بزهکاری؛ یعنی بزهکار، اهداف بزه و امکان بزه می‌باشد. ساختار فضای مجازی به صورتی است که در آن قرابت مکان میان سه عنصر مذکور لازم نیست. این وضعیّت موجب صرفه جویی بسیاری زیادی از بُعد زمان و هزینه برای بزهکاران می شود و آنان می توانند بدون وجود مانع مکان، دچارجرایم متعددی در سریع‌ترین زمان شوند، هویّتی را سرقت نمایند و یا پولی را از حسابی به حساب دیگر انتقال دهند (باستانی، ۱۳۸۳: ۲۶؛ جوان‌جعفری، ۱۳۸۹: ۱۷۶).

اگر شخصی بخواهد به آخرین مقاله، کتاب و یا خبری که در زمینه تخصّصی، در سطح جهان منتشر شده، دست یابد ساده ترین و سریع ترین راه، استفاده از **فضای سایبر** است.

۲-۶- ناشناختگی

فضای سایبر یک فضای مخفی است؛ مردم در این محیط در پشت رایانه های خود که هویّت آنان را از دیگران مخفی می کند، محیطی امن و مطمئن می یابند تا هر آنچه می خواهند را به معرض اجرا گذارند؛ چراکه نگاه های شماتت بار پلیس و مردم بر آنها نظاره ندارد تا آنان را از ترس دستگیری یا شرم رسوایی از ارتکاب خواسته هایشان باز دارد. نمونه این امر را می توان در مورد انتشار تصاویر مستهجن کودکان در فضای سایبری دید که در عین حالی که وسیله سودآوری برای ارائه کنندگان این تصاویر گشته، برای خواستاران ارضای غرایز جنسی نیز دنیایی آزاد فراهم آورده تا هر لحظه که خواستند بتوانند به راحتی وارد این دنیای خیال گونه شوند و تمایلات غریزی خود را فروبنشانند.

با این حال، منظور از مخفی بودن این فضا آن نیست که نمی توان آن را مشاهده کرد، بلکه مراد این است که این فضا قابلیّت این را دارد که بازیگران و نقش آفرینان آن کاملاً مخفیانه و در کمال ناشناسی و بدون بیم از آن که شناخته شده یا مورد ردّیابی و تعقیب قرار گیرند و اقدامات خود را به معرض اجرا گذارند. مرتکبین جرایم سایبری از قابلیّت اختفا در چنین فضایی بسیار سود می برند و با استفاده از نقابی که امکانات فنّی و ویژگی های تکنولوژیک در راستای امکان جعل و قلب هویّت در اختیار آنان می گذارد و نیز با استفاده از سیستم های رایانه ای عمومی یا رایانه های کارگذار آزاد، امکان ارتکاب بالقوّه طیف وسیعی از جرایم سایبری را می یابند که وقتی این امکان با گستره بی انتهای فضای سایبر در هم می آمیزد موقعیّت خطرناکی را پدیدار می سازد: گستره ای وسیع با مجرمانی بی شمار، پراکنده و ناشناس (Kamal 2005: 23-24)

۲-۷- حجم جرایم و بالا بودن رقم سیاه

از زمره محدودیّت های ارتکاب بزه در دنیای واقعی این است که ارتکاب بزه، تابع نرم یک در برابر یک می باشد؛ یعنی معمولاً برای وقوع بزه و ارتکاب آن علیه یک بزه دیده، حضور یک بزهکار لازم است. در بزه هایی مانند جعل، سرقت، قتل و ...، بزهکار باید برای آن برنامه ریزی نماید و پس از تهیه وسایل و مقدمات لازم، با انجام عنصر مادی جرم و تحقّق نتیجه، آن را تعقیب نماید.

این محدودیّت ها به نیروهای اجرای قانون و دستگاه عدالت کیفری کمک می کند که برنامه ها و منابع مالی و انسانی خود را بر روی بزه و بزهکار معیّن متمرکز نمایند، اما مقیاس بزه های ارتکابی در فضای سایبر بسیار وسیع است و به علّت امکانات موجود و فقدان محدودیّت ها، بزهکار از الگوی سریالی و شبکه ای استفاده می کند و لذا قربانی کردن هزاران نفر طیّ اقدامی واحد، فرضی واقعی در فضای سایبر می باشد. این امر باعث می‌شود که حجم و آمار بزه در دنیای مجازی با دنیای واقعی بی اندازه گردد (بای و پورقهرمانی، ۱۳۸۸: ۷۱-۷۲؛ باستانی، ۱۳۸۳: ۲۵-۲۶؛ جاوید نیا، ۱۳۸۷: ۹۹-۱۰۰).

۲-۸- عدم حضور در صحنه جرم

در جرایم سنّتی عمدتاً مجرم چاره‌ای جز حضور در صحنه ارتکاب جرم ندارد. این حضور قبل و همزمان با وقوع جرم ضرورت می یابد. پس از ارتکاب جرم نیز اقداماتی برای مخفی کردن و یا استفاده از آمار و نتایج حاصله از ارتکاب صورت می گیرد. این امر، یافتن سرنخ و تحقیق درباره شناسایی و تعقیب بزهکاران را تسهیل می کند، اما عدم حضور مجرمین در صحنه وقوع جرم، سبب می شود که شیوه های سنّتی کشف بزه، تحقیق و شناسایی بزهکار قابلیّت اجرا نداشته باشد (جوان جعفری، ۱۳۸۹: ۵).

۲-۹- فراملّی بودن

فضای سایبری یک وسیله ارتباطی بین المللی است و حقّ انتخاب و اشتراک افراد را هم در تولید و هم در دسترسی به اطلاعات بسیار افزایش داده و از اینرو مفهوم

آزادی اطلاعات را در سطح جهانی به معنای واقعی کلمه تحقّق بخشیده است. در اقع، اینترنت به گونه ای است که برای استفاده کنندگان و کاربران آن، دو خصوصیّت «انتقال و دریافت اطلاعات» را به طور همزمان داراست؛ لکن این که هرکس می تواند در هر نقطه ای از جهان به این شاهراه اطلاعاتی وارد شود و هرگونه اطلاعاتی که می خواهد بدان وارد کند مشکلاتی جدّی برای این فضا آفریده است؛ حتی یک کاربر نوجوان در یک گوشه دنیا می تواند اطلاعات مجرمانه بسیار خطرناکی را در فضای سایبر توزیع کند و باعث از بین رفتن داده های ارزشمند یا سیستم های رایانه ای بسیاری در سطح بین المللی گردد (بای و پورقهرمانی، ۱۳۸۸: ۷۴-۷۵؛ باستانی، ۱۳۸۳: ۲۸-۲۹؛ جاویدنیا ۱۳۸۷ : ۹۸-۹۹).

۲-۱۰- درونی بودن جرم

در جرایم سنّتی، این امکان وجود دارد که جرایم از ناحیه افرادی که دسترسی به موضوع جرم دارند رخ دهد، مانند سرقتی که مستخدمان منازل مرتکب می‌شوند. از آنجا که این اقدامات مجرمانه، درونی یا از ناحیه افراد مورد اعتماد انجام می‌شود آثار گسترده تری نسبت به اقداماتی که از ناحیه افراد بیگانه انجام می‌شود، دارند. قانونگذار کیفری، این وضعیّت را یک کیفیّت مشدّده تلقّی کرده و مجازات شدیدتری نسبت به آنها اعمال می کند.

این مشکل در جرایم سایبر به صورت حادتری مشاهده می‌شود. یکی از مشکلات جرایم سایبر، درونی بودن بسیاری از این جرایم است. مستخدمان، پیمانکاران، مشاوران و...، عاملان اصلی جرایم علیه یک شرکت یا سازمان هستند که تفکیک آن-ها از خارجی‌ها به سهولت امکان‌پذیر نمی‌باشد.

۲-۱۱- غیر ملموس و پوشیده بودن

جرایم سنّتی مانند سرقت اموال و یا اسناد امنیّتی به علّت عینی بودن، دیر یا زود کشف می‌شوند، اما برخی از جرایم سایبر ممکن است بسیار دیر کشف شده یا هرگز

کشف نشوند. سرقت اطلاعات جاسوسی و یا حتی سرقت ها و تخلّفات جزئی سایبر که به مقدار زیادی رخ می‌دهند، ممکن است هرگز جلب توجه نکرده و کشف نگردند.

فضای سایبر یک فضای مخفی و غیر ملموس است؛ مردم در این محیط در پشت رایانه های خود که هویّت آنان را از دیگران مخفی می کند، محیطی امن و مطمئن می یابند تا هر آنچه می خواهند را به معرض اجرا گذارند؛ چرا که نگاه های شماتت بار پلیس و مردم بر آنها نظاره ندارد تا آنان را از ترس دستگیری یا شرم رسوایی از ارتکاب خواسته هایشان باز دارد.

با این حال، منظور از مخفی بودن این فضا آن نیست که نمی توان آن را مشاهده کرد، بلکه مراد این است که این فضا قابلیّت این را دارد که بازیگران و نقش آفرینان آن کاملاً مخفیانه و در کمال ناشناسی و بدون بیم از آن که شناخته شده یا مورد ردّیابی و تعقیب قرار گیرند اقدامات خود را به معرض اجرا گذارند. مرتکبین جرایم سایبری از قابلیّت اختفا در چنین فضایی بسیار سود می برند و با استفاده از نقابی که امکانات فنّی و ویژگی های تکنولوژیک در راستای امکان جعل و قلب هویّت در اختیار آنان می گذارد و نیز با استفاده از سیستم های رایانه ای عمومی یا رایانه های کارگذار آزاد امکان ارتکاب بالقوّه طیف وسیعی از جرایم سایبری را می یابند که وقتی این امکان با گستره بی انتهای فضای سایبر در هم می آمیزد موقعیّت خطرناکی را پدیدار می سازد: گستره ای وسیع با مجرمانی بی شمار، پراکنده و ناشناس (جاویدنیا، ۱۳۸۷ : ۹۸-۹۹).

۲-۱۲- عدم کنترل اجتماعی

ویژگی دیگر فضای سایبری، قابل کنترل نبودن آن است. محیط سایبر از همان ابتدای پیدایش آن علیرغم نظم فنّی اعجاب آورش، از منظر رفتار کاربران محیطی مبتنی بر آنارشیسم و هرج و مرج بوده است. به موازاتی که این فضا به لحاظ فنّی رشد

داشته، از لحاظ رشد ساختارهای اخلاقی و کنترل کننده که هر محیط برای استقرار نظم به آنها نیازمند است بسیار عقب مانده است. این محیط پلیس ندارد، سازمانی بر آن نظارت نمی کند، مردم اشخاص را در حین ارتکاب جرایم سایبری نمی بینند و هرکس هر آن چه می خواهد انجام می دهد.

بنابراین فضای سایبر، یک فضای سرد و بی روح تکنولوژیک است که آن چه که وجدان جمعی، هنجارهای هدایتگر اجتماعی، اخلاق جمعی و نظایر آن نامیده می شود و در هر جامعه ای مبانی نظم را بنیان می نهد در آن بی معناست. محیط سایبر یک محیط آزاد است و فارغ از هرگونه هنجارهای اجتماعی و سلسله مراتب هرمی نظارتی و فرمانبرداری است؛ قابل کنترل نبودن این محیط ارتباط نزدیکی با خاموش و منفعل بودن آن دارد. چون افراد در این فضا خود را در معرض دیدگان دیگران نمی بینند، هر آن چه را که بخواهند می توانند انجام دهند و قید و بندی برای آنان وجود ندارد.

قواعد مرتبط با جرایم سنّتی یا عموماً ریشه در فرهنگ و اخلاق جامعه داشته و یا بعضاً در طی زمان، بخشی از فرهنگ جامعه شده اند. بنابراین، ارتکاب جرم علاوه بر نقض قوانین رسمی، تعرّض به ارزش ها و نرم های اجتماعی نیز محسوب می‌شود (باستانی، ۱۳۸۳: ۶۲).

شرایط مذکور، در مورد بسیاری از رفتارهای مزاحم در فضای سایبر به گونه‌ای دیگر است و برخی از رفتارهای آسیب رسان هنوزجرم انگاری نشده اند. برخی به علّت فقدان سابقه لازم در فرهنگ جامعه رسوخ نکرده و ارتکاب این رفتارها موجب برانگیختگی افکار عمومی نمی‌شود.

از سوی دیگر، عدم حضور مجرم در صحنه جرم، عدم مشاهده دیگران، پائین بودن احتمال دستگیری و مجازات، از کارآیی مکانیسم فشار و کنترل اجتماعی می-کاهد (جوان جعفری، ۱۳۸۹: ۱۷۶-۱۸۳).

۲-۱۳- تضعیف اعتقادات و فرهنگ های کم حضور و گسترش شبهات فکری

گرچه دستیابی آسان به انواع اطلاعات، از مزایای فضای سایبری است، اما معایبی نیز دارد. از جمله این که طرح و نشر انواع شبهات در آن، موجب تزلزل در باورهای کاربران سست عقیده و کم اطلاع می گردد. فضای سایبر، چاقویی دو لبه است که ما می‌توانیم از آن به سود خود مدد بگیریم؛ اما هجمه و تنوع و گسترش فرهنگ مهاجم غربی، به حدّی است که در شرایط فعلی کوشش های مدافعان فرهنگی مسلمان را بسیار کم اثر می نماید؛ خاصّه این که مدیریّت اصلی اطلاعات نیز در دست غرب و غربیان است (فضلی، ۱۳۸۹: ۴۸).

همچنین به شدّت تحت تأثیر هر نوع عرضه گسترده ای قرار می‌گیرد.گرچه این فضا، گذرگاه فرهنگ های متنوع و گوناگونی است که هر یک درصدد عرضه خویش هستند، اما تنها فرهنگی پیشتاز خواهد بود که حضورپر رنگ تر وگسترده تری داشته باشد و بدین سبب است که در آن فرهنگ غالب، فرهنگی جز فرهنگ قدرتمند، اما منحط غرب نیست؛ چراکه با بکارگیری صحیح از امکانات وسیع و تلاشی وافر، به عرضه گسترده خود پرداخته و یکّه تاز این عرصه گردیده است. به طور متوسط، توسعه وب که یکی از مهم ترین ابزار عرضه فرهنگ است، هر سه ماه یکبار دو برابر می‌شود. اما این رشد روز افزون، به نفع فرهنگ غربی است؛ چراکه پر رنگ ترین حضور از آن ایشان است. طبق آماری، آمریکا و کانادا ۶۳ درصد، اروپا ۲۲/۴ درصد و استرلیا، ژاپن و نیوزلند ۶/۴ درصد از کامپیوترهای متّصل به اینترنت را در اختیار دارند و بقیه کشورهای آسیایی و آفریقایی تنها ۵/۹ درصد از این آمار را به خود اختصاص داده اند. گرچه ممکن است تاکنون این آمار افزایش نیز یافته باشد، ولی حقیقت این است که سلطه غرب و فرهنگ بی بندبار غرب در جای جای فضای سایبر سایه گسترانده است. چنان که حکومت زبان انگلیسی موجب شده

است که کاربران با حضور در فضای سایبر، ضمن این که با زبان انگلیسی حاکم بر آن درگیر هستند، از زبان ملّی خود دور شوند؛ از اینرو، دانستن زبان انگلیسی از لوازم حضور فعال در فضای سایبر شده است. آموزش، پژوهش و ارتباطات نمی‌تواند به حرکت پیش رونده خود ادامه داده و نیازهای جامعه را پاسخ دهد، مگر این که زبان انگلیسی را به کار گیرد و این خود به صورت طبیعی موجب سیطره فرهنگ غرب بر عرصه‌های گوناگون جوامع به ویژه جوامع اسلامی می‌گردد. بدین وسیله، ارزش ها، روش ها و هویّت های مطلوب فرهنگ غربی بر جوامع تزریق شده، فرآیند دگرگونی عناصر فرهنگی سرعت خواهد گرفت (همان).

۲-۱۴- به خطر افتادن حقوق مادی و معنوی مولفین

یکی از نگرانی‌های مؤلّفان آثار علمی، ادبی و یا هنری ارائه آثارشان به صورت دیجیتال است. با توجه به گسترش روزافزون سرقت داده‌های گوناگون و نرم افزارها و دشوار بودن نظارت و حفاظت از داده‌ها، حقوق مادی و معنوی مؤلّفان در فضای سایبر دو چندان به خطر خواهد افتاد؛ چراکه با توجه به قدرتمند شدن انواع ابزارهای قفل شکن و نبود نظارت لازم بر فضای سایبر، مؤلّفانی که بخواهند از منافع مادی و معنوی اثر خویش بهره ببرند، از ارائه اثرشان در غالب داده‌های الکترونیکی خودداری می ورزند (همان).

۳- اقسام جرائم سایبری بر اساس قانون جرایم رایانه ای

این قانون به عنوان مهم‌ترین سند حقوقی در نظام حقوقی کشور در تاریخ ۱۳۸۸/۳/۵ به تصویب مجلس شورای اسلامی رسید (روزنامه جمهوری اسلامی ایران ۱۳۸۸: ۱). جرم انگاری گسترده و کیفرگذاری های تشدیدی و سنگین در این قانون، از بکار گیری سیاست کیفری سختگیرانه‌ای نسبت به جرایم رایانه‌ای حکایت دارد که امروزه در برخی از نظام های حقوقی با عنوان تسامح صفر شناخته می‌شود؛ یعنی عدم چشم پوشی حتی نسبت به کوچک ترین تخلّف ها، زیرا به زعم سیاستگذاران،

گذشت از این تخلّف ها، خود می‌تواند زمینه ساز جرم های مهمّ تری باشد که در نهایت، امنیّت ملّی را به خطر می اندازد (رایجیان اصلی، ۱۳۸۸: ۴۱۰). به) در این قسمت، مطابق سرفصل‌های قانون مذکور با کمی دخل و تصرّف، به جرایم مرتبط با رایانه پرداخته خواهد شد.

۳-۱- جرایم علیه محرمانگی داده‌ها و سامانه‌ها

این دسته از جرایم، اطلاعات و داده‌های رایانه‌ای را مرکز حملات و هدف خود قرار می‌دهند. قانون جرایم رایانه‌ای، جرائم مذکور را تحت سه عنوان ذکر کرده است: دسترسی غیر مجاز به داده‌ها یا سامانه ها، شنود غیر مجاز و جاسوسی رایانه‌ای که ذیلاً به آنها اشاره می‌شود.

الف) دسترسی غیر مجاز به داده‌ها یا سامانه

درباره مقیّد یا مطلق بودن این جرم دو نظر وجود دارد. برخی معتقدند دسترسی غیر مجاز، از جرایم مقیّد است و نتیجه آن، دست یافتن، احاطه و تسلّط بر سیستم دیگری می‌باشد (بای و پورقهرمانی، ۱۳۸۸: ۱۹۶). در مقابل می‌توان گفت که این جرم چیزی جز مجموعه افعال مرکّب نیست، با این توضیح که مرتکب کارهای متنوعی را انجام می‌دهد که از مجموع آنها به عنوان دسترسی یاد می‌شود. به نظر می‌رسد هرکس به طور غیر مجاز، محتوای در حال انتقال ارتباطات غیر عمومی در سیستم های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. به نظر می‌رسد دیدگاه اخیر صحیح‌تر باشد.

ب) شنود غیر مجاز

این جرم در ماده ۲ قانون جرایم رایانه‌ای پیش‌بینی شده است. به موجب این ماده: «هر کس به طور غیر مجاز محتوای در حال انتقال ارتباطات غیر عمومی در سیستم مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال محکوم خواهد شد.»

ج) جاسوسی رایانه‌ای

این جرم در قانون جرایم رایانه‌ای و دیگر قوانین مربوط تعریف نشده است و تنها در مواد ۳، ۴ و ۵ قانون مذکور احصاء شده است که تحت عناوین چوبه داده های سرّی، ارائه غیر مجاز داده های سرّی به افراد فاقد صلاحیّت یا بیگانگان و عوامل آنها و نقض تدابیر امنیّتی برای دسترسی غیر مجاز به داده های سرّی آمده است.

۳-۲- جرایم علیه صحّت و تمامیّت داده‌ها و سامانه‌ها

قانونگذار، در این قسمت سه موضوع را مورد تقنین قرار داده است: جعل رایانه‌ای، تخریب و اخلال داده‌ها یا سامانه های رایانه‌ای و مخابراتی و سرقت و کلاهبرداری رایانه‌ای. ذیلاً به هر یک از این موارد اشاره می گردد.

الف) جعل یارانه ای

مواد ۶ و ۷ قانون جرایم رایانه‌ای، به این موضوع پرداخته است. قانونگذار در این بخش، سه عنوان مجرمانه را ذکر کرده است: جعل داده های قابل استناد، جعل کارت ها و تراشه ها و استفاده از داده ها یا کارت و تراشه جعلی.

ب) تخریب یا اختلال داده یا سامانه متعلّق به دیگری

این بخش تحت سه عنوان تخریب داده ها،[1] تخریب یا مختلّ کردن سامانه، ممانعت از دسترسی اشخاص مجاز به داده یا سامانه مورد بحث واقع شده است.

۳-۳- سرقت و کلاهبرداری مرتبط با رایانه

در این دسته، دو عنوان سرقت داده‌ها و کلاهبرداری مرتبط با رایانه مورد بحث واقع شده است.

۳-۴- جرایم علیه عفّت و اخلاق عمومی

---

۱. ایجاد خسارت در داده ها یکی از اقسام جرایم علیه رایانه محسوب می شود که خود شامل: ایجاد خسارت در داده ها، اختلال در داده ها و غیر قابل استفاده کردن داده ها می گردد (بای، پورقهرمانی، ۱۳۸۸: ۱۲۹به بعد)

این موضوع تحت سه عنوان تولید یا توزیع محتویات خلاف عفّت عمومی، زمینه-سازی دسترسی افراد به محتویات مستهجن و مبتذل و زمینه سازی برای ارتکاب جرایم و مفاسد مورد بحث قرار گرفته است.

۳-۵- هتک حیثیّت و نشر اکاذیب

این مورد، تحت سه عنوان هتک حیثیّت از طریق انتشار محتوای صوتی و تصویری جعلی، انتشار صدا یا تصویر یا اسرار خصوصی دیگران و نشر اکاذیب مورد بحث واقع شده است.

۳-۶- جرایم ارائه دهندگان خدمات

این جرایم تحت چهار عنوان: خودداری از پالایش محتویات مجرمانه، خودداری از منع دسترسی افراد به محتوای مجرمانه، استفاده غیر مجاز از پهنای باند بین‌المللی و جرایم مرتبط با نگهداری، حفاظت و ارائه داده ها مورد بررسی قرار گرفته است.

۳-۷- تسهیل ارتکاب جرایم رایانه‌ای

این بخش که آخرین بخش از تقسیم بندی جرایم رایانه‌ای بر اساس قانون جرایم رایانه‌ای می‌باشد، در سه بخش تحت این عناوین مورد اشاره واقع شده است: تولید یا ارائه داده ها یا ابزارهای مختصّ ارتکاب جرایم رایانه‌ای، فروش یا ارائه داده های مرتبط با نفوذ به داده ها یا سامانه ها و انتشار یا ارائه آموزش نفوذ، شنود، جاسوسی و خرابکاری رایانه‌ای.

۴- وظایف و اقدامات پلیس در جرائم سایبری

۴-۱- وظایف پلیس در جرائم سایبری

همان‌طور که در مباحث قبل به تفصیل گفته شد، جرایم سایبر به عنوان جرایمی که زاییده عصر جدید هستند و ماهیّتی خاص دارند، علاوه بر تفاوت در مجازات ها، نوع قانونگذاری و ...، اقدامات پلیسی خاصّی را نیز می‌طلبند. این مبحث به بررسی اقدامات پلیسی در پی‌جویی جرایم مذکور می‌پردازد.

پلیس فتا، به منظور پیگیری، تحقیق و کشف جرایمی که در فضای مجازی اتفاق می افتد، ایجاد شد. وظایف فتا، ایجاد امنیّت و کاهش مخاطرات برای فعالیت های مختلف در جامعه اطلاعاتی، ممانعت از تعرّض به ارزش ها و هنجارهای جامعه، مراقبت و پایش از فضای تولید و تبادل اطلاعات، با هدف پیشگیری از تبدیل شدن این فضا به بستری برای انجام فعالیت های غیر قانونی می باشد.

امروزه استفاده از **اینترنت** و حضور در دنیای **مجازی**، بخش جدایی ناپذیری از زندگی شده است که نمی توان از آن چشمپوشی کرد. به همین دلیل، این فضا نیازمند سر و سامان و نظم گرفتن است تا از امنیّت برخوردار باشد و حقوق افراد در آن، مورد تعرّض و خدشه توسط سوء استفاده گران قرار نگیرد.

با رواج کلاهبرداری های اینترنتی، سرقت اطلاعات، تجاوز به حریم خصوصی افراد از طریق این فضا و افشای اطلاعات خصوصی مردم، ضرورت نهادی که ناظر بر این دسته از جرایم باشد و بتواند از وقوع آنها پیشگیری نماید، بیش از پیش احساس می شد. از همین رو، نهادی با عنوان **پلیس فتا**، برای امنیّت فضای مجازی و پیگیری جرایم در این فضا درنظر گرفته شد که دارای **وظایف** مشخّصی می باشد.

پلیس جمهوری اسلامی ایران تلاش می‌کند تا با بهره گیری از آخرین دستاوردهای فنّاوری اطلاعات و ارتباطات سیستم های پیشرفته انتظامی - امنیّتی کشور، امنیّت اجتماعی را بهبود بخشیده و محیط امن و توأم با آسایش را برای کلیه شهروندان فراهم کند (احمدوند و دیگران، ۱۳۸۳: ۲۲). این نهاد یکی از مهمّ ترین و تأثیرگذارترین نهادها در زمینه پیشگیری و کشف جرایم می باشد. در این خصوص، جرایم رایانه‌ای نیز از این امر مستثنی نیست.

اگرچه حقوقدانان به منظور حفظ نظم جامعه و پیشگیری از وقوع جرم، برای قوانین آئین دادرسی کیفری اهمیّت بیشتری قائل اند و پلیس را صرفاً مسئول کشف و تعقیب جرایم می پندارند، اما باید اذعان داشت که پلیس را می‌توان مهمّ ترین عامل

پیشگیری از جرم به شمار آورد؛ زیرا نقش حسّاس آن اقتضا می‌نماید که گام هایی جلوتر از زمان برداشته و از پیش، آمادگی لازم برای مواجهه با ناامنی های احتمالی آینده را احراز کند (رضوی، ۱۳۸۶: ۱۳۴). بدون تردید، سیستم کلان مبارزه با جرم که از سوی پلیس اتّخاذ می‌شود - چه در محیط فیزیکی و چه در فضای مجازی - یکسان است و پلیس در پیشگیری از وقوع جرایم سایبری، همان جایگاه خود را خواهد داشت. در واقع، اقدامات پلیس برای پیشگیری از وقوع این جرایم، چیزی جز مبارزه وضعی و سیاست عامّ این نهاد در مقابله با سایر جرایم نیست؛ اما آن‌چه باعث تفاوت در این حوزه می‌شود، ویژگی های منحصر به فرد جرایم سایبر است که شیوه های اجرایی خاص خود را به منظور تحقّق این سیاست عام طلب می‌کند (آیکو ۱۳۸۳: ۱۵۱).

وظایف پلیس، در برابر فضای سایبری به شرح زیر است:

- ایجاد امنیّت و کاهش مخاطرات برای فعالیت های علمی، اقتصادی، اجتماعی در جامعه اطلاعاتی.
- حفاظت و صیانت از هویّت دینی و ملّی.
- مراقبت و پایش از فضای تولید و تبادل اطلاعات، با هدف پیشگیری از تبدیل شدن این فضا به بستری برای انجام فعالیت های غیر قانونی.
- ممانعت از تعرّض، به ارزش ها و هنجارهای جامعه.

هدف **پلیس** این است که با در دست داشتن تخصّص و تجهیزات لازم، امنیّت این فضا را تأمین کند و اقدام به پیش بینی، جلوگیری و کشف جرایمی که ممکن است در این فضا رخ دهد، نماید. همان طور که ملاحظه می کنید این ارگان، نقش بسیار مهمّی را در حفظ نظم و امنیّت فضای مجازی بر عهده دارد.

در محیط فیزیکی، حضور پلیس در جامعه، عاملی در پیشگیری از جرم محسوب می‌شود. شکل و ترکیب خودروی پلیس و مؤموران ملبّس به لباس پلیس، تهدیدی

برای مجرمان بالقوّه به شمار می‌رود. به بیان دیگر، حضور پلیس در جامعه را می توان نوعی تهدید ضمنی برای مجرمان تلقّی کرد. بدون تردید، حضور فیزیکی پلیس در مواردی که جرایم سایبری با ورود کاربران غیر مجاز به یک سایت رایانه ای صورت می پذیرد، نقش مؤثّری در پیشگیری از این جرایم خواهد داشت (آیکو، ۱۳۸۳: ۱۵۱)، اما سؤال این است که آیا این امر در فضای مجازی و در ارتباط با جرایم رایانه‌ای امکان‌پذیر است؟

۱الف) ایفای نقش فعّال پلیس فتا

به نظر می رسد در چنین فضایی نیز می‌توان حضور داشت و با گشت زنی و مراقبت، مجرمان را تهدید کرد و از این طریق، مانعی بر سر ارتکاب جرایم رایانه‌ای نهاد. بعد از این که یکی از جرایمی که رسیدگی به آن در صلاحیّت **پلیس** هست، رخ بدهد و **پلیس،** آن را شناسایی کند یا شکایتی از بابت آن صورت بگیرد، از جمله شکایت فروشگاه های اینترنتی بابت کلاهبرداری؛ **پلیس،** اقدام به انجام تحقیقات مقدماتی، جمع آوری دلایل جرم و پیدا کردن متّهم می کند. بعد از پیدا شدن متّهم، **پلیس** او را تحویل مقامات قضایی می دهد، زیرا بازجویی در این جرایم، کمتر رخ می دهد و ادعا و اقرار متّهم، ارزش اثباتی ندارد و معمولاً برای اثبات، از مدارک دیجیتالی استفاده می شود. برای تشخیص جرایمی که **پلیس** می تواند به آن رسیدگی کند، می توان به قانون جرایم رایانه ای مراجعه کرد.

در **قانون جرایم رایانه ای،** جرایمی که با استفاده از فنّاوری کامپیوتری و با استفاده از اینترنت رخ می دهند شناسایی شده است، که از میان آنها می توان به جرایمی همچون برداشت غیر مجاز از حساب دیگران، شنود غیر مجاز، جعل رایانه ای، فیشینگ، کلاهبرداری اینترنتی، جاسوسی رایانه ای، نشر اکاذیب در فضای مجازی، انتشار عکس و فیلم خصوصی دیگران، پخش تصاویر مستهجن در فضای مجازی، دسترسی غیر مجاز به گذرواژه های دیگران و مواردی از این دست، اشاره

کرد. علاوه بر این، جرایمی مانند هک کردن تلگرام دیگران نیز در زمره **وظایف پلیس** می باشد.

امروزه، نرم افزارهای قدرتمندی در اختیار پلیس وجود دارد که شبیه سیستم های دزدگیر عمل کرده یا مسئول امنیّتی را از هرگونه تهدید قریب الوقوع به منظور انجام عملیّات مجرمانه در فضای مجازی مطّلع می‌سازد و امکان پیشگیری از این جرایم را به پلیس خواهد داد.

ب) ایجاد آموزش همگانی

یکی دیگر از شیوه های پیشگیری از جرم که سال هاست به طور معمول توسط نیروی انتظامی بکار گرفته می‌شود، آموزش همگانی و همچنین شناسایی و ارائه آموزش های خاصّ به اشخاص و سازمان هایی است که احتمال دارد در معرض جرایم سایبری قرار گیرند. در واقع، بکارگیری این شیوه، به همان اندازه که در پیشگیری از جرایم ارتکابی در محیط فیزیکی مؤثّر است در فضای مجازی نیز تأثیر دارد (رضوی، ۱۳۸۶: ۱۳۴-۱۳۵) و شاید بتوان گفت به دلیل کمتر شناخته شده بودن و ابهام بیشتر در مورد مکانیزم جرایم مذکور نسبت به جرایم سنّتی و در محیط فیزیکی، انجام این عمل از سوی پلیس به عنوان مهمّ ترین نهاد رسمی راهنما در این حوزه، تأثیر پیشگیرانه بیشتری نسبت به انجام همین عمل در مورد جرایم سنّتی دارد.

ج) اهمیّت کشف جرم

نقش دیگر پلیس در مورد جرایم سایبر، نقشی است که این نهاد در مورد کشف این جرایم بازی می‌کند. به موجب ماده ۱۵ قانون آئین دادرسی کیفری، وظیفه کشف جرایم، بر عهده نیروی انتظامی می‌باشد. بدین ترتیب، می توان گفت از دیدگاه پلیس در سیستم کلان مبارزه با جرم، تهدید بالفعل مجرمان، بازدارندگی و ارعاب مجرمان بالقوّه و همچنین تسریع در اجرای مجازات، دارای نقش مهمّ ارزنده‌ای است که برای ایفای این نقش باید به کشف جرایم، اعم از سنّتی و پیشرفته بپردازد (پرویزی ۱۳۸۴:

۸۱). در اینجا نیز علیرغم سیاست های عامّ و مشترک موجود در کشف تمام جرایم، به دلیل وجود تفاوت های ماهوی میان محیط فیزیکی و فضای مجازی یا محیط سایبر، روش های کشف جرایم سایبری نیز متفاوت خواهد بود. برای مثال، صحنه جرایم ارتکابی در محیط فیزیکی، به طور معمول متمرکز بوده و پراکندگی جغرافیایی نخواهند داشت، اما در جرایم سایبری، پراکندگی جغرافیایی صحنه جرم، بسیار زیاد و معمولاً دور از هم و در محدوده مرزی کشورهای مختلف است. ابزارهای بررسی صحنه جرایم سایبری، عمدتاً نرم‌افزارهای تخصّصی می‌باشند که بر اساس استانداردهای بین‌المللیِ تولید شده از سوی مأموران پلیس، مورد استفاده قرار می-گیرند. بنابراین، با ابزارهای بررسی صحنه سایر جرایم تفاوت اساسی دارند. دلایل ارتکاب جرایم سایبری، غالباً ادله الکترونیک هستند که با سرعت قابل ملاحظه‌ای، امکان تغییر و از بین بردن آنها وجود دارد (رضایی ۱۳۸۵: ۳۱). بنابراین، سرعت عمل در شناسایی و جمع‌آوری این دلایل بسیار ضروری خواهد بود (رضوی، ۱۳۸۶: ۱۳۶).

قانون جرایم رایانه‌ای این موضوع را مدّنظر قرارداده است و در فصل سوم خود، تحت عنوان استنادپذیری ادله الکترونیکی، به این نیاز پاسخ گفته است. در ماده ۴۹ این قانون آمده است: «به منظور حفظ صحّت و تمامیّت، اعتبار و انکارناپذیری ادله الکترونیکی جمع‌آوری شده، لازم است مطابق آئین نامه مربوط از آنها نگهداری و مراقبت به عمل آید.»

نکته دیگری که پرداختن به آن ضروری است، نحوه و چگونگی کشف جرایم در حوزه جرایم رایانه‌ای می‌باشد. پلیس به منظور بررسی و کشف جرایم سایبری با مشکلاتی روبرو می گردد که در سایر جرایم وجود ندارد. ادله الکترونیک، ویژگی هایی دارند که آنها را از ادله سنّتی متمایز می سازند. اینگونه دلایل نسبت به اسناد و مدارک دیگر، آسیب پذیرتر هستند؛ زیرا به آسانی می‌توان آنها را دستکاری یا جعل کرد و یا با استفاده از دانش فنّی مناسب آنها را پنهان کرد. ماهیّت خاصّ دلایل

الکترونیک به گونه ای است که پذیرش آنها را در مراجع قضایی با چالش های جدّی مواجه کرده است. به منظور مقابله با این چالش ها، مأموران پلیس باید روش های خاص جمع‌آوری دلایل مذکور را که مرکّب از چهار مرحله: جمع‌آوری مدرک، بررسی، تجزیه و تحلیل و ارائه گزارش می‌باشد، به نحو صحیحی اجرا کند.

مرحله جمع‌آوری، شامل جستجو برای شناسایی، جمع‌آوری و مستندسازی مدارک الکترونیکی است (پرویزی، ۱۳۸۱: ۱۱۰). برای این که پلیس بتواند داده ها یا سیستم های رایانه‌ای را تفتیش و توقیف نماید، به دستور مقام قضایی نیاز دارد؛ مگر کسی که داده ها یا سیستم های مذکور را در اختیار دارد، رضایت کتبی به منظور تفتیش آن بدهد. در عین حال، در صوت وجود ظنّ منطقی مبنی بر وجود ادله و فوریّت امر، پلیس می‌تواند بدون دستور قضایی، اقدام به تفتیش یا توقیف داده ها نماید. درحقیقت، هنگام بررسی دلایل وقوع جرم، پلیس باید اطمینان یابد که حقوق شخصی افراد را کاملاً رعایت کرده است (آیکو، ۱۳۸۳: ۲۵۹).

فرایند بررسی، مدارک را قابل رؤیت کرده و اصل و مفهوم آن را روشن می نماید. این کار باید به روشی انجام شود که دلایل موردنظر، از هرگونه تغییر، تحریف یا آسیب مصون بماند. در مرحله تجزیه و تحلیل، به ارزشی اثباتی و اهمیّت دلیل پرداخته می شود و در نهایت، در مرحله ارائه گزارش، پلیس باید گزارش مکتوبی که کلیات مربوط به فرایند بررسی اطلاعات مربوطه به دست آمده را دارا باشد، به مقام قضایی ارائه دهد (رضوی، ۱۳۸۶: ۱۳۷-۱۳۸).

آن چه واضح می‌باشد این نکته است که کارآگاهان مبارزه با جرایم، باید دارای خصوصیّات و ویژگی هایی باشند که ممکن است در هر فردی یافت نشود، اما سؤال این است که آیا کارآگاهان مبارزه با جرایم سایبر، باید ویژگی های دیگری غیر از ویژگی های کارآگاهان مبارزه با سایر جرایم را داشته باشند یا خیر؟

به نظر می رسد اقتضای این جرایم آن است که کارآگاهان مبارزه با این جرایم، دارای خصوصیّات خاصی باشند. برای مثال، شناخت علم رایانه، چگونگی عملکرد و اصطلاحات مورد استفاده در آن و نیز آگاهی از مسائل امنیّتی رایانه و شبکه به منظور کشف جرایمی از قبیل هک کردن سایت ها یا تهاجم به شبکه، برای آن دسته از مأموران پلیس که در این حوزه فعالیّت دارند، ضروری است. بنابراین، مأموران کشف جرایم سایبری، به منظور برخورداری از عملکرد مؤثّر در این حوزه ویژه، نیازمند آموزش های وسیع و جامعی هستند. به طور معمول، سازمان های بزرگ پلیس که در آن متخصّصان فنّاوری اطلاعات و علوم رایانه به منظور کشف جرایم سایبری اقدام به تشکیل گروه ویژه می کنند و به نیروهای پلیس، اطلاعات لازم را می‌دهند این نیاز را به راحتی مرتفع می‌سازند؛ اما اگر جرایم مزبور، در جایی ارتکاب یابند که اداره پلیس آن محلّ، فاقد امکانات یاد شده باشد آموزش تخصّصی برای مأموران پلیس آشکارتر می شود. کشف جرایم، فرایندی خلّاق و نیازمند مهارت های خاصّی است که می - توان آنها را آموخت و توسعه داد. اگرچه داشتن استعداد ذاتی برای تبدیل شدن به یک مأمور پلیس زبردست در حوزه جرایم سایبری لازم است، اما این امر کافی نیست و برای توسعه و کامل کردن مهارت ها، آموزش نیز لازم است. آموزش پیشرفته در زمینه جرایم سایبری باید در دسترس کسانی که کشف جرم را عملاً اداره می کنند قرار گیرد. فنّاوری های نوین، مدام در حال ظهور و تحوّل هستند و مأموران پلیس باید در جریان آخرین اطلاعات روز قرار داشته باشند (پرویزی، ۱۳۸۱: ۱۰۲).

۴-۲- اقدامات پلیسی در صحنه جرایم الکترونیک

یکی از مهمّ ترین مراحل در پی جویی جرایم، مرحله ای است که مأموران پلیس، مستقیماً صحنه جرم را بازرسی می کنند. این مرحله از اهمیّت خاصّی برخوردار می- باشد؛ زیرا هر اقدام غیر متخصّصانه، می‌تواند ادله موجود در مورد جرم ارتکابی و مرتکب آن را مخدوش کند (رشادتی، ۱۳۹۱: ۱) بررسی صحنه های جرم الکترونیکی

به لحاظ ماهیّت بسیار شکننده ای که دارند، نیازمند دقت فراوان و داشتن اطلاعات کافی هستند و هر اقدام اشتباهی در این راه، در واقع، قدمی بی بازگشت خواهد بود. بدین ترتیب، یک کارشناس در بررسی صحنه های جرم الکترونیک باید ابتدا دانش لازم در این خصوص را کسب نماید و سپس با استفاده از این دانش به صحنه جرم قدم بگذارد (تراب زاده، ۱۳۸۸: ۱۰۳).

به علاوه، باید به این نکته اشاره کرد که جرایم سایبر، ویژگی هایی دارند که صحنه جرم آنها نیز به گونه ای است که مأموران در صحنه های این جرایم، علاوه بر اقدامات عمومی در صحنه جرم، باید اقدامات ویژه‌ای را نیز انجام دهند. ذیلاً به مهمّ - ترین اقدامات در صحنه جرم الکترونیک پرداخته می‌شود.

به محض ورود به صحنه جرم رایانه‌ای، به هیچ وجه نباید در وضعیّت رایانه کوچک ترین تغییری ایجاد کرد. از وضعیّت اتّصال تجهیزات رایانه‌ای می‌بایست فیلمبرداری کرد یا صورتجلسه تهیه نمود به نحوی که بعد از توقیف، بتوان در صورت نیاز، آنها را به همان صورت متّصل نمود. در صورت نیاز، باید در مورد نصب قبل از جدا سازی، روی آنها برچسب گذاری نمود.

راه های پیشرفته ای وجود دارد که بر مبنای آن، به محض دسترسی فردی غیر از مجرم به داده های رایانه ای اش، بلافاصله داده ها حذف می شوند. مثلاً ممکن است از ناحیه مجرمان، نحوه خاصّی برای روشن شدن یا خاموش شدن آن طرّاحی شده باشد که در صورت عدم رعایت آن، لطمه به سیستم و داده های آن وارد شود؛ بنابراین اگر در زمان ورود به محلی با سیستمی برخورد شد که روشن است، نباید برق را قطع کرد یا به صفحه‌ی کلید دست زد. روز و زمان جاری رایانه و هرآن‌چه روی صفحه‌ی نمایش آن ظاهر می‌شود، می‌بایست صورت‌جلسه شود. پس از این اقدامات، با کمک گرفتن از متخصص نسبت به خاموش کردن سیستم اقدام می‌شود. اگر متخصص در دسترس نبود، کافی اسن پریز از برق کشیده شود.

اگر هنگام ورود به محلّ، سیستم خاموش است نباید روشن شود. البته با اقدامات فنّی خاصّ، جلوگیری از این اتفاقات میسّر است. به عنوان مثال، می‌بایست سیستم را با دیسکت های سیستمِ کاربرِ خنثی، راه‌اندازی کنیم تا برنامه احتمالی تنظیم شده برای حذف اطلاعات در صورت ورود بدون استفاده از مشخّصات کاربر اصلی عمل نکند (آیکو، ۱۳۸۳: ۲۶۰). کوچک ترین اقدام نسنجیده می‌تواند قابلیّت استناد داده را از بین ببرد. به عنوان مثال، اگر در حالی که به محلّ وارده شده ایم سیستم روشن و یک فایل متنی روی صفحه نمایش آن باز باشد و با فشردن یک کلید، تغییری در آن ایجاد شود و هنگام بستن آن فایل، به طور اتوماتیک، تغییر مذکور ذخیره گردد تاریخ و ساعت تغییر این فایل پس از ساعت شروع بازرسی شکل می‌گیرد و بدین ترتیب، مجرم می-تواند با استناد به آخرین تغییر، ادّعا کند که این فایل را ایجاد نکرده یا مطالب مجرمانه را نیفزوده است (قاجارقیونلو، ۱۳۷۴: ۱۲۸).

در بازبینی رایانه و حامل های داده ضرورت دارد از کلیه فایل‌های موجود و تاریخ تغییرات آنها لیست تهیه گردد (گاتن، ۱۳۸۳: ۲۶). به متّهم و افراد مشکوک نباید اجازه داد به سیستم نزدیک شوند یا رایانه را خاموش کنند و چنان چه این افراد اصرار به همکاری داشتند، از آنها خواسته می‌شود مراحل کار خود را بنویسند تا بعداً مشخص شود قصد تخریب داشته اند یا خیر (همان).

در برخی موارد، با تشخیص کارشناس فنّی ضرورت دارد قبل از اجرای حکم ورود به محلّ و بازرسی، برق محلّ و خطوط تلفن قطع شود تا مجرمان فرصت نیابند در فاصله اطلاع از ورود مأموران تا فاصله دستگیری، داده‌هایی را محو یا منتقل نمایند.

تجهیزات رایانه‌ای را می‌بایست پس از توقیف، به صورت فیزیکی یا الکترونیکی قفل کرده و به صورت جداگانه برچسب زده و انتقال داد و در دمای نه خیلی بالا و نه خیلی پایین و دور از رطوبت نگهداری کرد. جلوگیری از شوک و لرزش‌های شدید حین انتقال نیز ضروری می‌باشد (دزیانی، ۱۳۸۵: ۳۷).

دیسک های مغناطیسی (فلاپی‌ها) دکمه‌ای دارند که با عوض کردن وضعیّت آن، داده های موجود در آن قابل حذف یا تغییر نخواهند بود. ضمناً این دیسکت ها می - بایست در شرایط خاصی نگهداری شوند تا اطلاعات به خودیِ خود، حذف نگردد. به عنوان نمونه، نباید آنها را نزدیک آهن ربا، تلفن همراه یا اجسامی که حوزه مغناطیسی ایجاد می‌کنند قرار داد (آیکو، ۱۳۸۳: ۲۶۲). این موضوع درباره دیگر انتقال دهنده ها از قبیل سی دی ها، دی وی دی ها و ... نیز صدق می‌کند.

نکته دیگر این که پس از توقیف، سیستم رایانه‌ای باید از تاریخ انقضای «باطری پشتیبان» آن اطمینان حاصل کرد، زیرا در صورت تمام شدن این باطری، احتمال این که تنظیمات شخصی که روی خصوصیات کاری سیستم ایجاد شده و نیز زمان و تاریخ آن از دست برود وجود دارد که در این صورت، داده ها قابلیّت استناد خود را از دست می دهند. همچنین در مورد دستگاه هایی مانند شماره‌یاب و پیام‌گیر تلفن که با باطری کار می‌کنند، قبل از جداسازی از برق می‌بایست دقّت کرد که باطری سالم و پر داشته باشند. پس از توقیف نیز می بایست دقّت کرد که باطری آنها در فواصل زمانی مناسب تعویض گردد؛ به این دلیل که اطلاعات دخیره شده بر روی پیام‌گیرها در صورت قطع برق و در صورت نداشتن باطری سالم، پاک می‌شوند (دزیانی، ۱۳۸۵: ۳۸).

آخرین نکته این که بازبینی یک فایل، تنها با همان برنامه‌ای که در قالب آن ایجاد و ذخیره شده است، توصیه می‌شود؛ زیرا گاهی استفاده از سایر برنامه‌ها، موجب تخریب و ناخوانا شدن فایل می‌گردد؛ لذا نوع نرم‌افزاری که فایل در قالب آن است، سیستم عامل رایانه و راحلّ تهیه کپی از آن دقیقاً باید در صورتجلسه قید گردد (قاجارقیونلو، ۱۳۷۴: ۱۲۸).

۵- بررسی ابعاد مختلف امنیّت در فضای سایبر با رویکرد فقه حکومتی

به طور کلّی داشتن امنیّت، یکی از بزرگ ترین مواهب الهی است (قریش: ۴؛ نحل: ۱۲؛ انفال: ۲۶؛ فصّلت: ۴۰؛ انعام: ۸) که سپاسگزاری نسبت به آن، مورد غفلت قرار گرفته و دشوار می نماید (محمدی ری شهری، ۱۳۸۹: ۲۸۰/۱۲) و استقرار آن در جامعه از شاخصه های حکومت مهدوی به شمار می رود (نور: ۵۵). در کلام نورانی امیرالمؤمنین، تأمین امنیّت راه های ارتباطی، از وظایف اصلی حکومت اسلامی یاد شده است (سیّد رضی: ۴۰) که با الغای خصوصیّت عرفی از راه ها و اماکن فیزیکی، می توان فضای ارتباطی و زیستی در محیط سایبر را مشمول کلام امام دانست. البته به دلیل سرعت و سهولت ارتباط در فضای سایبر، ابعاد امنیّت در این فضا مختلف بوده و تأمین آن دارای اهمیّت بسیاری می باشد.

۵-۱- ضرورت ایجاد امنیّت اعتقادی و مذهبی

می توان از احکام فقهی (شیخ انصاری، ۱۴۳۱: ۲۳۸/۱-۲۳۳) حرمت تولید، نگهداری، نسخه برداری، انتشار، اجاره، خرید و فروش کتب حاوی مباحث گمراه کننده (کتب ضلال)، الغای خصوصیّت نموده و می توان حکم به حرمت امور ذکر شده در مورد سایت ها، کانال ها و منابع اینترنتی ضلال داد که وظیفه حاکمیّت در عرصه نشر کتب الکترونیکی و مطالب اینترنتی که گمراه کننده هستند، اعمال فیلترینگ (پالایش) و مرزداری از مرزهای ایدئولوژیک است (اسماعیلی و نصر اللهی، ۱۳۹۵: ۶۲-۷۰).

به همین دلیل، می توان از تنقیح مناط در حکم حرمت ساخت، نگهداری، خرید و فروش صلیب و بت (خمینی، ۱۴۳۵: ۱۶۴/۱و۲۶۹) و یا حرمت قبول ولایت از طرف جائر (همان: ۱۶۷/۲)، حرمت و ممنوعیّت هر آن چه موجب اضلال اعتقادی و رواج آن در جامعه می شود را نتیجه گرفت که این حکم شامل فضای سایبر نیز می گردد.

راهکار ایجاد امنیّت اعتقادی، تنها راهکار سلبی موارد فوق نمی باشد، بلکه با استفاده از فرصت فضای سایبر، با انتشار مباحث استدلالی متقن و فراهم نمودن بستر و محیطی برای مباحثات دینی، تضارب آراء و تولد رأی صواب رخ می دهد (تمیمی آمدی، ۱۴۱۰: ۱۵۸) و ذائقه عموم جامعه، منطقی شده و از اعتماد به مراجع فکری غیر سدید و نا سالم خودداری می کند.

۵-۲- ضرورت ایجاد امنیّت اخلاقی

ادله فقهی حرمت فحشاء، لهو، غنا، استعمال مسکرات و آلات قمار و مانند آن (شیخ انصاری، ۱۴۳۱: ۱۱۶/۱-۱۱۸؛ ۴۱/۲) بدون نیاز به الغای خصوصیّت و یا تنقیح مناط، موضوعات این احکام در فضای سایبر را در بر می گیرد که براساس قاعده «تعزیر» از وظایف حتمی و بدیهی حکومت اسلامی، اعمال فیلترینگ (پالایش) نسبت به انتشار و ترویج محرمات اخلاقی است (اسماعیلی و نصراللهی، ۱۳۹۵: ۶۷-۶۵) و همان طور قرار دادن فضای فیزیکی برای گناه کردن به صورت اجاره یا مجّانی نیز حرام می باشد (شیخ انصاری، ۱۴۳۱: ۱۲۳/۱و۳۸۵؛ ۵۳/۲)، فراهم کردن امکان ارتکاب محرّمات گفته شده و امثال آن در فضای مجازی (سایبری) نیز با الغای خصوصیّت عرفی حرام است، اگر چه در صدق عنوان «اعانه بر اثم» تردید وجود داشته باشد؛ در حالی که دادن اذن به پیام رسان های فحشاء رسان و مانند آن برای حضور در سرزمین مسلمین، در حال حاضر در اختیار دولت و حکومت اسلامی می باشد.

۵-۳- ضرورت ایجاد امنیّت آبرویی آحاد کاربران

ادله فقهی حرمت غیبت، نمیمه (سخن چینی)، تتبع از عثرات (لغزش های) مؤمنین، استهانه (بی اعتنایی و بی حرمتی و خوار کردن مؤمن)، تشبیب (ابراز عشق به زن مؤمن و عفیف و ذکر محاسن او)، شایع کردن گناه سرّی و پنهان افراد (حرّ عاملی، ۱۴۰۹: ۲۷۵/۱۲-۲۷۹و۳۰۶؛ شیخ انصاری، ۱۴۳۱: ۱۷۷/۱؛ ۱۱۱/۲-۱۱۴) شامل ارتکاب این امور در فضای سایبر نیز می شود و در صورتی که تخریب شخصیّت افراد محترم و

تعرض به عِرض و آبروی ایشان در فضای سایبر به صورت خصوصی و یا عمومی انجام شود، با شکایت آن فرد، وظیفه مجازات برعهده دستگاه حاکمیّت است. اما استنباط با رویکرد فقه حکومتی اقتضای آن را دارد که طرّاحی قالب فضای مورد استفاده کاربران به گونه ای باشد که هویّت افراد پنهان نباشد و کسی در پس نقاب های مجازی پنهان نشود. ایجاد این ساختار خود به خود مانع بسیاری از هتّاکی ها می باشد و این نتیجه به دست می آید که اقدام به طرّاحی چنین ساختاری به جهت ایجاد امنیّت آبرویی کاربران بر حکومت واجب است.

۵-۴- ضرورت ایجاد امنیّت مالی و اقتصادی

در این مبحث از چند زاویه می توان بحث نمود. به عنوان نمونه، طرّاحی قالب و نحوه دسترسی به صفحات اینترنتی توسّط حکومت می تواند به صورتی باشد که باعث نگرانی کاربر در استفاده از اینترنت و مصرف بیهوده از ذخیره اینترنتی خریداری شده، گردد. چه از طریق کاهش ناگهانی ذخیره اینترنت کاربر در اثر فریب وی توسّط برخی اپلیکیشن ها و چه از طریق گرانفروشی دولت به مردم و ارائه اینترنت در استفاده های داخلی، اما با اخذ مبالغی متناسب با بهای باند اینترنتی بین الملل؛ در این مورد نیز ایمن نمودن فضای سایبر همانند فضای فیزیکی از وظایف حکومت است، چون جلوگیری از هدر رفتن سرمایه های مردم از وظایف حکومت اسلامی می باشد (شیخ انصاری، ۱۴۳۱: ۱۰۴/۲-۱۰۶) از زاویه دیگر ایجاد بازار تجاری ایمن، از نظر قیمت گذاری اجناس، جلوگیری از تدلیس و غشّ در معرفی کالا ها در تجارت اینترنتی، از وظایف اقتصادی حتمی حکومت اسلامی بوده و تخلّف از قوانین حکومتی مستوجب تعزیر می باشد (نهج البلاغه، نامه ۵۳) تا محیط کسب و کار، امنیّت اقتصادی داشته باشد.

بدین ترتیب، حکومت اسلامی باید بر محیط تجارت سایبری نظارت نموده و در یک رفتار ایجابی، بستری فراهم نماید تا اولاً، قالب صفحات اینترنتی، صرف حدّاقل

هزینه و وقت را بر کاربران تحمیل نماید؛ ثانیاً، محتواهای تجاری در معرفی کالاها و قیمت ها، مورد نظارت و بازرسی باشند؛ وثالثاً، امنیّت رمزهای اینترنتی و حساب های مالی مردم فراهم گردد.

۵-۵- ضرورت ایجاد امنیّت حریم خصوصی و اطلاعات محرمانه کاربران

اسلام، حریم خصوصی را معتبر شمرده و شرط جواز ورود به حریم مسکونی اختصاصی غیر را، به دست آوردن اذن او می داند (نور: -۲۷-۲۸ و ۵۹) و با نهی از تجسّس، تفتیش، استراق سمع و بصر و افشای سرّ، براین حکم به شدّت تأکید نموده است (حسینی و برزویی، ۱۳۹۶: ۱۱۹)؛ همچنین براساس روایات و اجماع فقها، در صورتی که با نگاه کردن به حریم خصوصی افراد و اطلاع پیدا کردن بر اطلاعات او به حریم خصوصی او تجاوز نماید و دفع او جز با آسیب جسمانی و یا قتل او ممکن نباشد، خونش هدر است (نجفی، ۱۴۰۴: ۶۶۰/۴۱) که این مورد در فضای سایبری نیز رخ می دهد و با الغای خصوصیّت عرفی، این حکم شامل حریم خصوصی کاربران نیز می شود (حسینی و برزویی، ۱۳۹۶: ۱۲۶).

بنابراین، فراهم نمودن امکان حفاظت از حریم خصوصی افراد، بر حکومت واجب بوده و عقوبت متجاوزان سایبری و هکرها به حریم خصوصی افراد ضروری است.

۵-۶- ضرورت ایجاد امنیّت اطلاعات محرمانه ملّی

استناد به قاعده «نفی سبیل و سلطه کفّار بر مؤمنین» (موسوی بجنوردی، ۱۴۳۰: ۱۹۳/۱)، لزوم حفظ عزّت و اقتدار مؤمنین در برابر دشمنان و لزوم تجهیز تمام نیروها در مقابل بیگانگان (منافقون: ۸؛ انفال: ۶۰) وجوب حفظ اطلاعات اقتصادی، سیاسی، اجتماعی و ... از دستبرد بیگانگان و ممانعت از جاسوسی و شکست اطلاعاتی در فتنه های منافقان (توبه: ۴۷) که حتی منجرّ به تخریب مسجد ضرار شد (توبه: ۱۰۷؛ سبحانی، ۱۳۸۶: ۸۸۲) ضرورت مقابله حکومت اسلامی با اشراف اطلاعاتی و انجام عملیات داده کاری (data mining) بیگانگان نسبت به مسلمین را اثبات می کند که

ایجاد نمودن اینترنت ملّی و حفاظت تامّ از اطلاعات مردم و حکومت، از راهکارهای ایجابی پیش روی حکومت اسلامی می باشد (کهوند، ۱۳۹۵: ۳۰-۲۳).

نتیجه‌گیری

از مجموع مطالب پیش گفته نتایج ذیل بدست می آید:

۱- فنّاوری اطلاعات و دنیای الکترونیک، به عنوان تحوّلی عظیم در قرن اخیر، تمام ابعاد زندگی بشری را تحت الشعاع قرار داده است. جرایم سایبر به عنوان محصول این فضا، یکی از انواع جرایم نوظهور در عرصه حقوق کیفری می باشد که برخلاف بسیاری از امور نوین - که همچنان قابل تبیین و تدبیر براساس مبانی سنّتی هستند - علیرغم تلاش‌های صورت گرفته، فضای سایبر، هنوز محیطی کنترل نشده، نامنظّم و بی‌قانون توصیف می‌گردد که تقریباً برای همگان قابل دسترسی است.

۲- به نظر می‌رسد مردم برای بسیاری از اعمال در فضای سایبر، قبحی قائل نیستند و حتی بعضاً به ارتکاب آنها مباهات می‌کنند! نمونه بارز این موضوع،، هک کردن سایت ها توسط جوانانی است که به انگیزه هایی از قبیل سرگرمی، نشان دادن خود و ... دست به این کار می‌زنند و از انجام آن هیچگونه شرمی ندارند. یکی از مهمّ ترین معضلات این موضوع، همین عدم تخصّص و عدم آشنایی افراد در برخورد با این جرایم در مراحل مختلف می باشد. بدین ترتیب، با این که در نظام حقوق ایران، تدابیر بسیار ارزنده‌ای در این موضوع اندیشیده شده است، نیاز به دوره های آموزشی فراگیر و منظّم تری احساس می‌شود.

۳- نکته دیگر، بازاندیشی در مبانی سنّتی حقوق جزا و احیاناً تغییر برخی مسائل در برخی حوزه های خاص می‌باشد. به عنوان مثال، استفاده از مفهوم مسئولیّت نیابتی در بعد کیفری است. کسی که حقّ و توانایی کنترل اعمال تجاوزکارانه دیگران را دارد و بخصوص کسی که از آن اعمال سود می‌برد، باید به لحاظ حقوقی و بعضاً کیفری،

مسؤول تلقّی شود. این امر می‌تواند شامل سازندگان، طرّاحان سیستم های رایانه‌ای، ارائه کنندگان خدمات اینترنتی و نقاط اتّصال اینترنتی گردد. این موضوع نیز به شکلی کمرنگ در بند ج ماده ۱۹ قانون جرایم رایانه ای مبنی بر پیش بینی امکان ارتکاب جرم رایانه‌ای توسط کارمند شخص حقوقی با اطلاع مدیر، دیده می شود.

۴- یکی دیگر از اعمالی که می‌تواند در پیشگیری از جرایم سایبر مثمر ثمر باشد، آگاهی بخشی به مصرف‌کنندگان و مجریان برای استفاده امن از فضای سایبر در زمینه راه های مقابله با جرایم سایبر و ایجاد یک سیستم هشدار برای دادن اطلاعات اورژانسی به مصرف کنندگان می باشد.

۵- وجوب ایجاد امنیّت اعتقادی و مذهبی، امنیّت اخلاقی، امنیّت روانی، امنیّت آبرویی، امنیّت مالی و اقتصادی، امنیّت حریم خصوصی و امنیّت اطلاعات محرمانه ملّی، در فضای سایبر به اثبات رسیده و براساس رویکرد فقه حکومتی، علاوه بر رفتارهای سیاسی حکومت، انجام رفتارهای ایجابی نیز ضروری است.

فارغ از اقدامات پیشگیرانه، پس از ارتکاب جرم نیز اقدامات پلیسی، در مهمّ ترین درجه اهمیت قرار دارد. این اقدامات که چیزی فراتر از اقدامات پلیسی در صحنه جرایم سنّتی است، باید به مأموران پلیس و دیگر ضابطین مرتبط با جرایم رایانه‌ای آموزش داده شود تا در مواجهه با این جرم، به بهترین شکل ممکن برخورد قضائی و کیفری صورت گیرد.

منابع

- **قرآن کریم**.

- آیکو، دیویدجی (۱۳۸۳) ، **راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای**، ترجمه: اکبراسترکی و محمدصادق روز بهانی و تورج ریحانی و راحله الیاسی، تهران: معاونت پژوهش دانشگاه علوم انتظامی.

- احمدوند، علی محمد؛ عطایی جعفری، امیر مسعود (۱۳۸۳)، «**نقش و راهبرد فنّاوردی اطلاعات در سیستم پلیس و فضاهای مجازی جرایم در ایران**»، دو ماهنامه توسعه علوم انسانی، ۳، ۵-۲۸.

- اردبیلی، محمدعلی (۱۳۸۵)، **حقوق جزای عمومی**، ج۱، تهران: میزان.

- اسماعیلی، محسن؛ نصراللهی، محمدصادق (۱۳۹۵)، «**پالایش فضای مجازی، حکم و مسائل آن از دیدگاه فقهی**»، مجله پژوهشی دین و ارتباطات، ۴۹، ۵۳-۸۰.

- انصاری(شیخ)، مرتضی بن محمدامین (۱۴۳۱ق)، **کتاب المکاسب**، ج۱و۲، قم: مجمع الفکر الاسلامی.

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

- بای، حسینعلی؛ پورقهرمانی، بابک (۱۳۸۸)، **بررسی فقهی حقوقی جرایم رایانه‌ای**، قم: پژهشگاه علوم و فرهنگ اسلامی.

- پرویزی، رضا (۱۳۸۱)، **ابرار اقتصادی**، ۱ و ۲ و ۸ و ۸۱/۷/۲۳، جرایم کامپیوتری و اینترنتی.

- تراب زاده، حسین (۱۳۸۸)، **بررسی صحنه‌های جرم الکترونیکی**، ۶، ۱۱۰-۱۴۰.

- تمیمی آمدی، عبدالواحد (۱۴۱۰ق)، **غررالحکم و درر الکلم**، قم، دارالکتب الاسلامی.

- جاویدنیا، جواد (۱۳۸۷)، **جرایم تجارت الکترونیکی**، تهران: خرسندی.

- جوان جعفری، عبدالرضا (۱۳۸۹)، **جرایم سایبر و رویکرد افتراقی حقوق کیفری**، مجله دانش و توسعه، ۳۴، ۱۷۱-۱۹۵.

- حرّ عاملی، محمد بن حسن (۱۴۰۹ق)، **تفصیل وسائل الشیعه الی تحصیل مسائل الشریعه**، ج۱۲و۲۵، قم: آل البیت.

- حسینی، مهدی؛ برزویی، محمدرضا (۱۳۹۶)، **مبانی و مؤلفه های فقهی حمایت از حریم خصوصی افراد در فضای مجازی**، مجله پژوهشی مطالعات حقوق بشر اسلامی، ۱۳، ۱۱۵-۱۳۷.

- خمینی(امام)، سید روح الله (۱۴۳۵ق)، **المکاسب المحرّمه**، ج۱و۲، تهران: مؤسسه تنظیم و نشر آثار امام خمینی(ره).

- دزیانی، محمدحسن (۱۳۸۵)، **مقدمه‌ای بر سیاست جنایی ایران در باب جرایم سایبری**، ماهنامه قضاوت، ۳۸، ۴۲-۴۸.

- رایجیان اصلی، مهرداد (۱۳۸۸)، **قانون جرایم رایانه‌ای: نوآوری ها و کاستی ها**، مجله پژوهش‌های حقوقی، ۱۵، ۴۰۹-۴۱۸.

- رشادتی، جعفر (۱۳۹۱)، **عوامل مخدوش کننده صحنه جرم**، ماهنامه دادرسی، ۹۶، ۳-۷.

- رضایی، روح الله (۱۳۸۵)، **اعتبار اسناد الکترونیک با توجه به قوانین داخلی و بین المللی**، نشریه حقوقی گواه، ۶ و ۷، ۳۰-۴۰.

- رضوی، محمد (۱۳۸۶)، **جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها**، مجله دانش انتظامی، ۳۲، ۱۲۰-۱۴۰.

- سبحانی تبریزی، جعفر (۱۳۸۶)، **فروغ ابدیّت**، قم: بوستان کتاب.

- فضلی، مهدی (۱۳۸۹)، **مسئولیت کیفری در فضای سایبر**، تهران: خرسندی.

- قاجارقیونلو، سیامک (۱۳۷۴)، **مطالعه تطبیقی ادله اثبات در محیط‌های دیجیتال و ادله کامپیوتری با توجه به حقوق ایران**، تهران، سازمان برنامه و بودجه، شورای عالی انفورماتیک کشور.

- کهوند، محمد (۱۳۹۵)، **آسیب شناسی شبکه اجتماعی تلگرام، مرکز مطالعات راهبردی فضای مجازی**، تهران: دانشکده علوم اجتماعی و فرهنگی دانشگاه جامع امام حسین(ع).

- گاتن، آلن‌ام (۱۳۸۳)، **ادله الکترونیکی**، ترجمه: مصیّب رمضانی، تهران: دبیرخانه شورای عالی اطلاع رسانی.

- محمدی ری شهری، محمد (۱۳۸۹)، **میزان الحکمه**، ج۱۲، قم: دار الحدیث.

- موسوی بجنوردی، سید حسن (۱۴۳۰ق)، **القواعد الفقهیّه**، ج۱، قم: دلیل ما.

- نجفی(صاحب جواهر)، محمدحسن (۱۴۰۴ق)، **جواهرالکلام فی شرح شرائع الاسلام**، ج۲۱و۴۰و۴۱، چ۳، بیروت: دار القلم.