جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آن‌ها

محمد رضوی
عضو هیئت علمی دانشگاه علوم انتظامی

چکیده

تمایل روزافزون به استفاده از فناوری‌های پیشرفته از جمله رایانه و اینترنت، شرایط و بستر مساعدی برای ظهور جرایم سایبری به وجود آورده است. از آنجا که این جرایم در فضای مجازی انجام می‌شوند و مانند سایر جرایم، ملموس نیستند، مراجع قضایی و انتظامی برای پیشگیری از این جرایم و کشف آن‌ها با چالش‌های نوینی مواجه هستند.

کشور ما به هیچ کدام از کنوانسیون‌های بین‌المللی مربوط به جرایم سایبری نپیوسته است و با توجه به خلأ موجود در قوانین داخلی، نیروهای انتظامی برای پیشگیری از این جرایم و کشف آن‌ها، در عمل با مشکلاتی مواجه هستند و این در حالی است که امروزه پلیس با استفاده از فناوری‌های نوینی که در عرصهٔ نرم‌افزارهای تخصصی پلیس به وجود آمده است، می‌تواند در پیشگیری از وقوع جرایم مزبور نقش مؤثری داشته باشد. بنابراین، لایحهٔ قانون مجازات جرایم رایانه‌ای – که مدت‌هاست در دستور کار مجلس شورای اسلامی قرار گرفته – باید هر چه سریع‌تر به تصویب برسد و به مرحلهٔ اجرا گذاشته شود تا پلیس بتواند به عنوان حافظ نظم و امنیت در فضای مجازی، نقش مؤثر خود را ایفا کند. از آنجا که جرایم سایبری ویژگی‌های منحصر به فردی دارند، مأمورانی که به کشف و بررسی این جرایم می‌پردازند، باید آموزش‌های تخصصی وسیع و جامعی را در خصوص رایانه و اینترنت فرابگیرند تا در این زمینه به نتایج مطلوب‌تری دست یابند. با توجه به آنکه دلایل ارتکاب جرم در فضای مجازی، عمدتاً ادلهٔ الکترونیک می‌باشند، ضرورت آموزش‌های تخصصی در خصوص رایانه و اینترنت به مأموران پلیس بیشتر آشکار می‌شود.

کلید واژه‌ها

جرایم سایبری (Cyber Crimes) / جرایم سنتی (Classic Crimes) / شبکهٔ جهانی اطلاع‌رسانی (W.W.W) / فناوری اطلاعات (Information Technology) / پلیس (Police)؛ پیشگیری (Prevention) / کشف (Detection).

مقدمه

چند دهه‌ای است که رایانه و اینترنت، در مناسبات اجتماعی، فرهنگی و اقتصادی، جای خود را یافته؛ به نحوی که در جوامع پیشرفته استفاده از آن به عنوان یک ضرورت مطرح شده است و این امر، جهان را به دهکده‌ای شبیه ساخته و اعضای آن، در هر نقطه‌ای که باشند، به راحتی می‌توانند با یکدیگر ارتباط برقرار کرده بدون صرف زمان طولانی، در جهان اطلاعات سیر نمایند و بر دانش خود افزوده و مهارت‌های خود را افزایش دهند.

میل و اشتیاق به استفاده از رایانه و اینترنت و بهره‌مندی از مزایای آن، یک تمایل جهانی می‌باشد. این تمایل که با سرعت قابل توجهی در حال افزایش است، اگر چه زمینهٔ مشارکت جوامع را در فرآیند اقتصاد داده‌پردازی فراهم می‌سازد، اما در عین حال، شرایط و بستر مساعدی نیز برای ظهور پدیده‌های نوین بزهکاری به وجود آورده است. جرایم ارتکابی در فضای مجازی، یکی از این پدیده‌های نوین تلقی می‌شود (خداقلی، ۱۳۸۳: ۱۸). امروزه در اکثر جوامع، کاربرد فناوری‌های پیشرفته رو به گسترش است. از آنجا که این فناوری‌ها درعرصه‌های مختلفی از جمله تجارت الکترونیک، انجام خدمات بانکی توسط شبکه، فروش محصولات، انجام خدمات مراقبتی و درمانی، آموزش و تحقیقات رواج یافته است، تمایل ویژهٔ افراد مستعد برای بزهکاری، به استفاده از این فناوری، عامل بالقوه‌ای در گسترش جرایم مزبور بوده است.

در حال حاضر، جرایم سایبری، به عنوان یکی از دغدغه‌های بزرگ هزارهٔ سوم میلادی، آیندهٔ اجرای قوانین را در بسیاری از کشورهای جهان به مخاطره انداخته است. کشورهای توسعه یافته، برای مبارزه با این جرایم، پیشقدم شده و قوانینی تدوین کرده‌اند که بسیاری از آن‌ها، از اسناد بین‌المللی سرچشمه می گیرند. این اسناد، راهکارهای مناسبی پیش روی قانون‌گذاران کشورها قرار داده‌اند. در عین حال، از آنجا که بررسی نقش پلیس در پیشگیری از جرایم سایبری و کشف آن‌ها، مستلزم تبیین ماهیت این جرایم، چالش‌های مرتبط با آن و واکنش‌های لازم به منظور تحول و دگرگونی اساسی در کیفیت سیاست‌گذاری هاست، با در نظر گرفتن آنچه بیان شد، در آغاز به تبیین ماهیت جرایم سایبری و چالش‌های مرتبط با آن و نیز تشریح واکنش‌های نوین مطرح شده در فرایند پیشگیری، کشف و تعقیب متهمان این جرایم خواهیم پرداخت و سپس نقش پلیس در پیشگیری از این جرایم و کشف آن‌ها را تبیین خواهیم کرد.

۱. ماهیت جرایم سایبری و چالش‌های مرتبط با آن

پیوند و اتصال شبکهٔ جهانی اینترنت، به روشنی گویای این واقعیت است که ویرانگری و آسیب‌رسانی می‌تواند در یک لحظه، سراسر جهان را فرا گیرد. سوء استفاده از فناوری‌های رایانه‌ای و اینترنتی می‌تواند امنیت ملی، آسایش عمومی و موجودیت یک جامعه را به مخاطره انداخته و تأثیرهای منفی بی‌شماری را بر زندگی افراد اجتماع

تحمیل کند (وایلدینگ[1]، ۱۳۷۹: ۱۱). با کمی دقت در این خصوص می‌توان به این نتیجه دست یافت که اغلب مرتکبان جرایم سایبری را جمعیت جوان تشکیل می‌دهند. (آیکاو[2]، ۱۳۸۳ :۵۵) این مجرمان هم از ظرفیت جنایی بالایی برخوردارند و هم استعداد خوبی برای انطباق اجتماعی از خود نشان می‌دهند (جعفری، ۱۳۸۵ : ۷۰).

اشخاصی که در شرایط عادی زندگی، هیچگونه تصوری از سرقت یا تجاوز به اموال دیگران ندارند، در مواجهه با فرصت‌ها و موقعیت‌های ارزشمندی که رایانه و اینترنت برای آن‌ها مهیا کرده، حتی لحظه‌ای دچار تردید، احساس گناه یا تزلزل در تصمیم‌گیری نخواهند شد. در بیشتر جرایم سایبری، خشونت وجود ندارد، بلکه طمع، غرور یا دیگر ضعف‌های شخصیتی قربانی است که در ارتکاب این جرایم نقش اصلی را بازی می‌کند(خداقلی، ۱۳۸۳ : ٤١). در این بخش ابتدا به بررسی ماهیت جرایم سایبری خواهیم پرداخت، سپس چالش‌های مرتبط با این جرایم و برخی واکنش‌ها را به منظور دفع این چالش‌های مرتبط با این جرایم و برخی واکنش‌ها را که به منظور دفع این چالش‌ها صورت گرفته است، مطرح خواهیم کرد.

الف) ماهیت و اقسام جرایم سایبری

جرم عبارت است از: فعل یا ترک فعلی که برای آن در قانون، مجازات تعیین شده است و جامعه با ابراز مجازات، آن نکوهش می‌نماید (اردبیلی، ۱۳۸۰: ۱۲۰). محیط سایبر، به محیطی مجازی اطلاق شود که اطلاعات در آن رد و بدل می‌گردند (پرویزی، ۱۳۸٤: ٤٦). بنابراین جرایم سایبری در اصطلاح به جرایمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات ارتکاب می‌یابند. امروزه شاهد آن هستیم که تعداد قابل توجهی از جرایم سنتی، همزمان با پیشرفت فناوری اطلاعات و ارتباطات، به شدت متحول شده و در سطح وسیعی صورت می‌گیرند. برای مثال، جرم جاسوسی از جرایم سنتی است که در ارتکاب آن وسیلهٔ خاصی شرط نیست. این جرم با هر وسیله‌ای انجام می‌گیرد و در قالب مقررات موجود، قابل مجازات است (خداقلی، ۱۳۸۳ : ۱۰۲). کلاهبرداری و سرقت نیز از جرایم سنتی تلقی می‌شوند که به علت استفادهٔ روزافرون از رایانه و اینترنت، به سهولت و سرعت خیره‌کننده‌ای ارتکاب می‌یابند (آیکاو، ۱۳۸۳: ٦٤).

با توسعهٔ رسانه‌های الکترونیکی، در کنار جرایم سنتی یاد شده، فرصت‌های جدیدی نیز برای بزهکاری فراهم شده است. اموری از قبیل حملهٔ ویروس‌ها، ورود غیر مجاز به وب سایت‌ها و هک‌کردن آن‌ها، سرقت و سوء استفاده از داده‌ها و ایراد خسارت به رایانه‌ها، در زمرهٔ رفتارهای بزهکارانه‌ای تلقی می‌شوند که قابلیت ارتکاب در محیط خارج از رایانه را ندارند. به همین ترتیب، پیشرفت فناوری رایانه، شرایط و بسترهای مناسبی برای سرقت اطلاعات (وایلدینگ، ۱۳۷۹: ۲۹)، تکثیر نرم‌افزارهای غیرمجاز،سوء

1.Wilding Edward 2. Icove Davidj.

استفاده از بازار سهام، تجاوز به حقوق مالکیت معنوی و مهم‌تر از همه، تهاجم فرهنگی را فراهم کرده است (دزیانی، ۱۳۸٤: ۱۹).

از آنجا که درحال حاضر شبکه‌های ارتباطی، پیوندی جهان شمول یافته‌اند، جرایم این حوزه، اغلب دارای وصف بین‌المللی شده‌اند. به علاوه، با پیدایش فناوری‌های جدید در این حوزه، از قبیل رایانه‌های لب‌تاپ، تلفن و مودم‌های سیار، جرایم‌های ارتکابی نیز این قابلیت را خواهند یافت که در هر زمان و مکان، با وصف امحای آثار صحنهٔ ارتکاب جرم و تأثیر بالقوهٔ آن بر تمامیت شبکهٔ اتصال جهانی، تحقق یابند.

با توجه به اینکه جرایم در فضای مجازی، در اشکال مختلفی ارتکاب می‌یابند، لذا سخن گفتن درخصوص شرایط، ارکان و تقسیم‌بندی این جرایم، قدری مشکل به نظر می‌رسد. عدم ارائهٔ آمار دقیق توسط نیروهای انتظامی و مراجع قضایی پیرامون جرایم مزبور، ناتوانی در خصوص ارائهٔ تعریف صریح و روشن از ماهیت این جرایم را دو چندان کرده است. متأسفانه در حال حاضر، اطلاعات دقیق، مشخص و قابل اطمینانی در خصوص میزان و تأثیر جرایم سایبری، نه تنها در کشور، بلکه در سایر نقاط جهان نیز به چشم نمی‌خورد و شمار زیادی از آن‌ها نامکشوف محسوب می‌شوند. مسئلهٔ اخیر یکی از معضلاتی است که متصدیان تحقیق در مرحلهٔ کشف و تعقیب جرایم مزبور با آن مواجه می‌باشند (خداقلی،۱۳۸۳: ۳۵).

عدم اعلام جرایم مزبور تا حدودی به مسئله باز می‌گردد که اعلام آن احتمال تأثیرهای منفی و نامطلوبی را بر حس اعتماد مصرف‌کنندگان و میزان خدمات ارائه شده بگذارد. عدم اطمینان خاطر نسبت به مأموران و مراجع قانونی در برخورد مؤثر با ان گونه جرایم را می‌توان دلیل دیگری در این خصوص دانست. در عین حال، صرف‌نظر از مشکلات مطرح شده درتبیین ماهیت جرایم سایبری، به نظر می‌رسد که می‌توان این جرایم را در چهار دسته یا طبقهٔ کلی جای داد. این دسته‌بندی تا حدی ماهیت جرایم مزبور را نیز روشن می‌کند.

۱- **جرام کلاسیک (سنتی) با توصیف سایبری**: جرایمی در این دسته قرارمی‌گیرند که جرایم سنتی تلقی می‌شوند، اما در حال حاضر، به علت پیشرفت فناوری، با وسایل نوینی انجام می‌شوند. از جملهٔ این جرایم می‌توان به جعل و کلاهبرداری سایبری اشاره کرد (راجی، ۵۸۳۱ : ۹٦) در حال حاضر، در جایی که شبکه‌های رایانه‌ای، ابزار ارتکاب جرایم سنتی نظیر کلاهبرداری و جعل از طریق اینترنت هستند، قاضی مجبور است به علت فقدان یک قانون مدون و مشخص در این رابطه، از قوانین سنتی مانند قوانین جزایی و «قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای» که آیین نامهٔ آن در سال ۹۷۳۱ به تصویب رسید و همچنین مجازات‌هایی که در «قانون تجارت الکترونیکی» مصوب ۲۸۳۱ وجود دارد، استفاده کند (دزیانی، ٤۸۳۱: ۱۲).

۲- **جرایم علیه محرمانه بودن داده‌ها و سیستم‌های رایانه‌ای و مخابراتی**: هر نمادی از موضوع‌ها، مفاهیم یا دستورالعمل‌ها از جمله متن، صوت یا تصویر را که

برای برقراری ارتباط میان سیستم‌های رایانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای به کار گرفته شده و به وسیلهٔ سیستم رایانه‌ای ایجاد می‌گردد، «داده محتوا»[1] گویند. (گاتن[2] ، ۱۳۸۳ :۱۹) از جمله جرایمی که در این دسته جای می‌گیرند، می‌توان به شنود غیر مجاز داده‌های مخابراتی در یک ارتباط خصوصی یا داده‌های سری که واجد ارزش برای امنیت داخلی و خارجی کشور می‌باشند، اشاره کرد.

۳- جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی: تغییر، ایجاد، محو یا متوقف کردن داده‌های رایانه‌ای و مخابراتی به قصد تقلب، غیرقابل استفاده کردن، تخریب یا اختلال در داده‌ها یا امواج الکترومغناطیسی (دزیانی، ٤٨٣١ : ۰۲)، ممانعت از دستیابی اشخاص مجاز به داده‌ها با تغییر رمز ورود و یا رمزنگاری از جمله جرایمی هستند که در این دسته قرار می‌گیرند (وایلدینگ، ۹۷۳۱: ٥٤).

۴- جرایم مرتبط با محتوا : این دسته، جرایمی را تحت شمول خود قرار می‌دهد که در آن‌ها، رایانه به عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می‌شود و صرفاً فناوری اطلاعات،زمینهٔ ارتکاب آن‌ها را فراهم می‌سازد (گنجی، ۱۸۳۱ : ۹۱)، برای مثال، انتشار محتویات مستهجن از قبیل نمایش اندام جنسی زن و مرد یا نمایش آمیزش جنسی انسان، تبلیغ یا تحریک یا تشویق به انحرافات جنسی یا خودکشی از طریق سیستم رایانه‌ای یا مخابراتی، در این دسته قرار می‌گیرند.

امروزه در نقاط مختلف دنیا، اکثر صنایع و شرکت‌های تولیدی و خدماتی، در معرض تهدید و زوال جدی قرار دارند. درصد زیادی از این شرکت‌ها، انواع مختلفی از مزاحمت‌ها یا استفادهٔ غیر مجاز از سیستم‌های رایانه‌ای را تجربه کرده‌اند. در حال حاضر، این مزاحمت‌ها بیشتر به سیستم‌های بانکی و صنایع مالی معطوف گردیده است. نکتهٔ قابل توجه اینکه جرایم سایبری، عمدتاً توسط نیروهای سازمان‌یافته و طراحی و نقشهٔ قبلی و نیز توسط اشخاص رقیب یا اخراج شده از سازمان‌های مزبور صورت می‌گیرد. بررسی‌های انجام شده در سال‌های اخیر، مبین افزایش چشمگیر میزان بزهکاری و گرایش‌های مجرمانه درفضای مجازی است. براساس این بررسی‌ها، تهدیدات ناشی از جرایم سایبری به شکل مهارناپذیری رو به افزایش بوده و زیان‌های مالی فراوانی نیز بر بخش‌های مختلف وارد آورده است (آیکاو، ۱۳۸۳ : ۱۵). از آنجا که در سال‌های آتی، شاهد رشد تصاعدی در کاربرد فناوری اطلاعات، خصوصاً استفاده از اینترنت خواهیم بود، مسلماً چنین تمایل و گرایش خیره‌کننده‌ای، مقارن با افزایش میزان جرایم سایبری می‌باشد. در این مرحلهٔ حساس زمانی، باید با بررسی چالش‌های موجود در این حوزه، واکنش مناسبی بری مبارزه با این بزهکاری نوین ارائه دهیم.

ب) چالش‌های موجود

اگر چه پیشرفت فناوری اطلاعات و ارتباطات، برای ارتکاب بسیاری از جرایم سنتی به کار گرفته می‌شود، اما ماهیت و ویژگی‌های خاص جرایم در محیط سایبر، مراجع

قضایی و انتظامی را با چالش‌های جدیدی مواجه کرده است که در ذیل به برخی از آن‌ها اشاره می‌شود.

۱- **داشتن جنبهٔ بین‌المللی**: ابعاد جرایم ارتکابی در فضای مجازی، نه تنها حاکمیت سرزمینی یک دولت را تحت تأثیر قرار می‌دهد، بلکه تمامی دولت‌های عالم را در بر می‌گیرد، ماهیت جرایم سایبری این‌گونه است که هیچ حد و مرز سرزمینی مشخصی را نمی‌شناسد (پرویزی، ۱۳۸٤ : ۷۷). ابعاد یاد شده، موجب طرح مباحثی از جمله صلاحیت، تعدد و تعارض قوانین کیفری و قابلیت ارتکاب جرایم مذکور علیه قربانیان بی‌شمار می‌گردد. در اینجا مسئله صلاحیت را با ذکر مثالی توضیح خواهیم داد. به عنوان مثال، می‌توان فردی را تصور کرد که در نقطهٔ دور افتاده‌ای از یک کشور آفریقایی، در اتاق کوچک خود نشسته و مدام با نفوذ در سیستم اطلاعات امنیتی وزارت دفاع آلمان، بدون آنکه کمترین اثری از خود بر جای گذارد، به سرقت داده‌های حساس و کلیدی مبادرت می‌ورزد. این درحالی است که خودش هم نمی‌داند اطلاعات یاد شده در کجا قرار دارند. پس از این اطلاعات، احتمال دارد آن‌ها را به چندین کشور دیگر منتقل کند و این کشورها را نیز تحت تأثیر پیامدهای این امر قرار دهد. بر مبنای این واقعیت، چندین کشور در معرض ارتکاب چنین جرمی قرار می‌گیرند و احتمالاً ادعای خود را دایر بر صلاحیت رسیدگی به جرم مزبور، مطرح خواهند ساخت. با توجه به اولویتی که برای عناصر مراحل ارتکاب جرم قایل می‌شویم، کشورهای ذی‌نفع در چنین جرایمی، با اعلام اینکه حادثهٔ مزبور در درون مرزهای آن‌ها اتفاق افتاده است، خود را محق می‌دانند در اجرای اصل صلاحیت سرزمینی، برای تعقیب و مجازات مرتکب جرم اقدام نمایند (گلدوزیان، ۱۳۸۳: ۹۲). این مسئله نوعی تعارض درصلاحیت دادگاه‌های کشورهای مزبور به وجود می‌آورد که این امر از مباحث مهم و اساسی در حوزهٔ جرایم سایبری محسوب می‌شود (الماسی، ۱۳۸۲: ۲۲).

۲- **مشکل تعریف واحد از جرایم سایبری**: با وجود اینکه جرایم سایبری، درحال حاضر، بخش عظیمی از جرایم ارتکابی در کشورهای مختلف را تشکیل می‌دهند، در این خصوص تعریف قانونی واحدی به چشم نمی‌خورد. در حقیقت، از آنجا که این جرایم در اشکال مختلفی ارتکاب می‌یابند، سخن گفتن در خصوص تعریف واحد، شرایط و ارکان این جرایم، قدری مشکل به نظر می‌رسد.

۳- **عدم تخصص کافی مراجع قضایی و انتظامی**: یکی از چالش‌های مهم موجود در این حوزه، نداشتن تخصص کافی مراجعی است که به تعقیب، کشف و رسیدگی ماهوی به این جرایم می‌پردازند. این مسئله باعث می‌شود که تعقیب و کشف این جرایم با مشکل مواجه شده و دادگاه‌ها نیز نتوانند به نحو شایسته به جرایم مزبور رسیدگی کنند.

۴- **تغییر پذیری ماهیت دلایل اثبات جرم**: یکی از مباحث مهم در تمام نظام‌های حقوقی، بحث ادله و نحوهٔ استناد و پذیرش آن برای اثبات یا رد دعاوی است، به

نحوی که می‌توان گفت بدون وجود دلیل، هیچ دعوایی سرانجام ندارد. حال با گسترش حوزهٔ فناوری اطلاعات در تمامی شئون زندگی انسان‌ها، آیا می‌توان گفت اسناد و مدارک ناشی از کارکردهای این فناوری، برای اثبات دعاوی راجع به آن، هیچ جایگاهی ندارد؟ پاسخ منفی است؛ زیرا علاوه برتأثیرپذیری کارکردهای فیزیکی و مادی از دنیای دیجیتال، امروزه بسیاری از امور فقط دراین فضا امکان‌پذیر است و عملاً می‌توان گفت هر سند و مدرکی که راجع به آن‌ها لازم باشد، باید در این فضا و فقط به صورت الکترونیکی جست و جو کرد. نمونهٔ بارز این موضوع، طیف وسیعی از جرایم رایانه‌ای است که وقوع آن‌ها فقط در دنیای دیجیتال امکان‌پذیر است. امروزه اطلاعات مختلفی که در دعاوی حقوقی یا پیگردهای جزایی نقش مهمی ایفا می‌کنند، در یک سیتم رایانه‌ای، ذخیره و بایگانی می‌شوند، در پرونده‌های کاغذی، به همان نسبت که افراد و شرکت‌ها، اتکای خود را بر سیستم‌های رایانه‌ای افزایش داده‌اند، کارآگاهان و مقامات قضایی و وکلا نیز به ارزش ذخایر گرانبهای الکترونیکی پی برده‌اند، ذخایری محفوظ در سیستم‌های رایانه‌ای که به طور گسترده‌ای استناد به آن‌ها برای کشف و به جریان انداختن انواع دعاوی آغاز شده است (گاتن، ۳۸۳۱ : ۱). اما در عین حال، این گونه دلایل نسبت به اسناد و مدارک دیگر آسیب‌پذیرتر هستند؛ زیرا به آسانی می‌توان در آن‌ها دستکاری یا آن را جعل کردو یا آن‌ها را با استفاده از دانش فنی مناسب پنهان کرد. به علاوه، برخی ادلهٔ قانونی که همواره در سایر جرایم از وسایل مهم اثبات تلقی می‌شوند، کارآمد نخواهند بود، برای مثال شهادت شهود، انگشت نگاری با استفاده از .D.N.A در اثبات جرایم سایبری کمک چندانی نخواهند کرد.

۵- **مشکلات خاص مرحلهٔ کشف**: یکی از مسائلی که در خصوص جرایم سایبری اهمیت فراوانی دارد، بالا بودن هزینهٔ کشف آن‌ها است. از سوی دیگر، اختیارات قانونی برای بازرسی و دستیابی به سیستم‌های رایانه‌ای به واسطهٔ غیر قابل لمس بودن داده‌های رایانه‌ای، کافی نیست (دبیرخانه شورای عالی انفورماتیک،۱۳۷٦: ۲۵).

۶- **عدم هماهنگی قوانین کشورهای مختلف**: در خصوص تعقیب متهمان جرایم سایبری و بازجویی از آن‌ها رویه یکسانی در کشورها به چشم نمی‌خورد. افزون بر آن، در خصوص عناصر تشکیل دهندهٔ جرایم سایبری نیز میان حقوق جزای داخلی کشورها با مقررات یکپارچهٔ بین‌المللی، هماهنگی دیده نمی‌شود.

۷- **فقدان همکاری‌های متقابل**: در خصوص پیشگیری، تعقیب و کشف جرایم سایبری، همکاری متقابلی از ناحیهٔ کشورها به چشم نمی‌خورد. همچنین مکانیزم قانونی مشترکی که تشریک مساعی بین‌المللی را تجویز کند، وجود ندارد.

مواردی که در فوق به آن‌ها اشاره، صرفاً بعضی از چالش‌های مطرح شده در این حوزه است که پیش روی مراجع قضایی و انتظامی قرار دارند و در عین حال، بدیهی است که منحصر به موارد مذکور نمی‌باشند. در هر حال، برای رفع این چالش‌ها، تدابیری در سطح بین‌المللی و نیز منطقه‌ای اتخاذ شده است. همچنین برخی کشورها

برای رفع این چالش‌ها، اقدامات مناسبی را انجام داده‌اند.

ج) راهکارهای نوین رفع چالش‌ها

فعالیت‌های انجام گرفته به منظور رفع چالش‌های موجود در خصوص تعقیب و کشف جرایم سایبری و مبارزه با آن‌ها را می‌توان در سه سطح «جهانی، منطقه‌ای و داخلی» بررسی کرد. در حقیقت، علاوه بر آنکه کنوانسیون‌های جهانی در زمینهٔ مبارزهٔ با جرایم سایبری به تصویب کشورها رسیده‌اند، سازمان‌های منطقه‌ای نیز در راستای رسیدن به این هدف، فعالیت‌های چشمگیری انجام داده‌اند. افزون بر آن، در برخی کشوها با تصویب قانون خاص، در رفع چالش‌های یاد شده اقدامات شایسته‌ای صورت گرفته است.

۱- کنوانسیون‌های جهانی

به منظور مبارزه با جرایم سایبری و رفع چالش‌های موجود در این حوزه، برخی کنوانسیون‌های بین‌المللی به تصویب رسیده‌اند که کنوانسیون ۲۰۰۱ بوداپست با عنوان «کنوانسیون جرایم رایانه‌ای» یکی از آن‌هاست. در این کنوانسیون هماهنگ‌سازی بین حقوق کیفری داخلی و مقررات یکپارچهٔ بین‌المللی در خصوص عناصر تشکیل‌دهندهٔ جرایم سایبری به چشم می‌خورد. همچنین به منظور تعقیب متهمان این جرایم و بازجویی از آن‌ها، اختیارات خاصی برای مراجع قضایی و انتظامی مقرر شده است. در زمینهٔ تشریک مساعی بین‌المللی، این کنوانسیون پیشنهاد می‌کند دولت‌های طرف قرارداد به انحای گوناگون، در موارد لازم، به ویژه در امور مربوط به ارائهٔ دلایل جرم و اعلام دقیق محل وقوع آن، به یکدیگر یاری رسانند. همچنین امور دیگری از قبیل اصول کلی مربوط به همکاری بین‌المللی، استرداد مجرمان، همکاری‌های دو جانبه، حل و فصل منازعات، پلیس اینترنتی، تنگناهای قانونی مبارزه با جرایم سایبری، نقش مراکز غیردولتی در مبارزه با جرایم در فضای مجازی، ضمانت اجراها، تدابیر قانونی و ... در زمرهٔ مباحث مهم مطروحه در کنوانسیون مزبور است.

در مقدمهٔ کنوانسیون آمده است: «دولت‌های امضاکنندهٔ این کنوانسیون، با هدف دستیابی به اتحاد فراگیر میان اعضا و با اعتقاد به ضرورت اتخاذ سیاست‌های جنایی عمومی در حمایت جامعه در برابر جرایم سایبری، به تصویب قوانین مناسب و گسترش همکاری‌های بین‌الملل اقدام کرده و با آگاهی از تحولات شگرفی که در اثر همگرایی و تداوم روند جهانی شدن شبکه‌های رایانه‌ای و داده‌های الکترونیکی به منظور ارتکاب جرایم و با احساس نیاز به همکاری بین دولت‌ها و بخش‌های خصوصی در زمینهٔ مبارزه با جرایم سایبری و حمایت از منافع مشروع در توسعهٔ فناوری اطلاعات، در راستای تصویب قوانین یکپارچه و یکسان در این زمینه گام بر می‌دارند» (نشریهٔ بین‌المللی سیاست جنایی در جرایم سایبری، ۱۳۷٦ ، ش ٤٣و٤٤).

سند بین‌المللی دیگری که در این زمینه وجود دارد، قواعدی تحت عنوان «نت اسمارت»[1] است که برای حمایت از کودکان، نوجوانان و جوانانی وضع شده است که کابر اینترنت می‌باشند. در این سند بین‌المللی برای پیشگیری از وقوع جرایم سایبری برضد اشخاص یادشده، توصیه‌هایی مقرر شده است، برای مثال، در سند مزبور چنین آمده است: «هرگز نشانی خانه، شمارهٔ تلفن، اسم مدرسه و... خود را از طریق اینترنت به دیگری ندهید» و یا «هرگز عکس، مشخصات کارت اعتباری یا جزئیات حساب بانکی خود را از طریق اینترنت به دیگری ندهید» (دزیانی، ۱۳۸٤: ۲۱). همچنین اشخاص مزبور از ارائهٔ گذرواژهٔ[2] خود به دیگران و گذاشتن قرار ملاقات از طریق اینترنت با دیگران منع شده‌اند. در هر حال، توصیه‌های مقرر در این سند بین‌المللی، بسیار سودمند است و در مبارزه با جرایم سایبری نقش مهمی ایفا می‌نماید (همان منبع).

با وجود اسناد بین‌المللی یاد شده برای پیشگیری از جرایم سایبری، هنوز در خصوص تحقیقات و بازرسی‌های لازم برای تعقیب جرایم مزبور، در شرایط فعلی با مشکل جدی بازیافت داده‌ها مواجه هستیم. در واقع، مسئلهٔ اساسی این است که آیا مقام تحقیق داده‌های مورد نیاز خود را مستقیماً، بدون مداخله و تجویز یا توافق دولتی که داده‌ها در آنجا قرار داده، به دست آورد. در این خصوص، سازمان ملل متحد اظهار داشته است این تصور که تحقیق داده‌های روی شبکهٔ اینترنت، نقض حریم دیگر دولت‌ها محسوب می‌گردد، تا حدودی صحیح به نظر می‌رسد.

در کنار این اسناد بین‌المللی، سازمان ملل نیز با انتشار متون و نشریات مختلف، در راستای پیشگیری از جرایم سایبری و مبارزه با آن‌ها، اقدامات به‌سزایی را انجام داده که از جملهٔ این نشریات می‌توان به نشریهٔ «سیاست جنایی سازمان ملل در زمینهٔ جرایم سایبری» اشاره کرد. اگر چه مطالب مندرج در این نشریه، جنبهٔ الزام‌آور به خود نمی‌گیرد،اما در هر حال، در راستای اتخاذ سیاست‌های لازم برای زدون این پدیدهٔ نوین بزهکاری، ایده‌های جدیدی به کشورها داده و مساعدت‌های شایسته‌ای به آن‌ها کرده است (نشریهٔ بین‌المللی سیاست جنایی درجرایم سایبری، ۱۳۷٦، ش٤٣و٤٤).

۲- اقدامات سازمان‌های منطقه‌ای

در حال حاضر، سازمان‌های منطقه‌ای و محلی نیز در راستای نیل به هدف مبارزه با جرایم سایبری، از هیچ تلاشی در این زمینه دریغ نمی‌ورزند. شورای اروپا از نهادهایی تلقی می‌شود که در این خصوص نقش فعالی ایفا می‌نماید. این شورا متنی تهیه کرده که در آن لیستی از چالش‌های موجود در حوزهٔ جرایم سایبری و واکنش‌های نوین مطرح شده به منظور رفع این چالش‌ها، به چشم می‌خورد. در متن یاد شده، در کنار ارائهٔ پیشنهادهای ماهوی، در خصوص مسائل شکلی از جمله آیین رسیدگی به جرایم

1. Net Smart 2. Password

سایبری نیز راه‌حل‌هایی ارائه گردیده است.

۳- حقوق داخلی کشورها

در سطح حقوق داخلی، برخی کشورها نیز در این زمینه، فعالیت‌هایی را آغاز کرده‌اند؛ برای مثال، ایالات متحدهٔ آمریکا، برای آموزش قضات، مأموران اف. بی. آی. و سایر علاقه‌مندان، اقدام به ارائهٔ متنی با عنوان «تفتیش و توقیف رایانه‌ها» کرده است. در این متن، پس از بیان مقدمه، مباحثی از جمله تفتیش و توقیف رایانه‌ها بدون نیاز به صدور حکم، تفتیش و توقیف رایانه‌ها به موجب حکم، قانون حریم خصوصی ارتباطات الکترونیک و نظارت الکترونیک در شبکه‌های ارتباطی مورد بحث قرار گرفته است. متن مزبور، برای دانشجویان حقوق، علوم انتظامی، کارآموزان وکالت و نیز کسانی که به صورت حرفه‌ای به جرایم سایبری می‌پردازند یا با پرونده‌های مرتبط با آن سروکار دارند، متن مفید و سودمندی است. در حال حاضر، کشورهای متعددی با تصویب مقررات مربوط به جرایم سایبری، این حوزه از جرایم را قانون‌مند ساخته‌اند؛ از جمله این کشورها می‌توان به فرانسه (جعفری، ۱۳۸۵: ۷۰) و استرالیا اشاره کرد. حتی برخی کشورهای مسلمان آسیایی مانند مالزی نیز به تصویب این‌گونه قوانین پرداخته‌اند.

واکنش‌هایی که در سال‌های اخیر از سوی سازمان‌های بین‌المللی و منطقه‌ای و همچنین کشورها مورد توجه قرار گرفته است، تا حد قابل ملاحظه‌ای از وقوع جرایم سایبری پیشگیری کرده و کشف و تعقیب این‌گونه جرایم را نیز تسهیل نموده است. این در حالی است که متأسفانه نه تنها کنوانسیون‌های یاد شده از سوی کشور ما مورد پذیرش و تصویب قرار نگرفته، بلکه با وصف خلأ قانونی در حقوق داخلی، تاکنون اقدام جدی نیز صورت نگرفته است.

در حال حاضر، هر چند در جایی که رایانه و شبکه‌های رایانه‌ای، ابزار ارتکاب جرایم سنتی نظیر کلاهبرداری و جعل از طریق اینترنت هستند، قضات به علت فقدان یک قانون مدون و مشخص در این رابطه، از قوانین سنتی نظیر قوانین جزایی و همچنین «قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای» (که آیین نامهٔ آن در سال ۱۳۷۹ به تصویب رسید) و جرایم مذکور در «قانون تجارت الکترونیکی» (مصوب ۱۳۸۲) استفاده کنند،اما در جایی که جرم سایبری از مصادیق جرایم سنتی محسوب نمی‌شوند، عمل مجرمانهٔ مزبور به علت فقدان عنصر قانونی، جرم تلقی نمی‌گردد.

در همین راستا، مسئولان امر با درنظر گرفتن واقعیات جامعه و بررسی همه جانبهٔ موضوع، اقدام به تشکیل کمیتهٔ مبارزه با جرایم رایانه‌ای و تدوین لایحهٔ قانون مجازات جرایم رایانه‌ای کردند. تا فضای مجازی را نیز مانند محیط فیزیکی، از نظر جزایی قانون‌مند سازند. در این لایحه، برخی کنوانسیون‌های بین‌المللی یاد شده از جمله کنوانسیون جرایم سایبری ۲۰۰۱ بوداپست و همچنین قوانین کشورهای خارجی از قبیل فرانسه، استرالیا و مالزی مورد توجه قرار گرفته‌اند. البته تا حد امکان سعی شده

است که این مقررات به صورت بومی درآیند. در تدوین لایحهٔ قانون مجازات جرایم رایانه‌ای سعی شده است تا مقررات آن با فقه جزایی اسلام مغایرت نداشته باشد.

به منظور افزایش آگاهی مراجع قضایی از جرایم سایبری، قوهٔ قضاییه از سال ۱۳۸۲، با برگزاری کلاس‌های آموزش ضمن خدمت قضات دادگستری استان تهران، دو عنوان درسی آموزشی در برنامه‌های این دوره گنجانده است. این دو عنوان عبارت‌اند از: «جرایم سایبری» (جرایم علیه فناوری اطلاعات) برای قضات کیفری، «دعاوی حقوقی» (حقوق فناوری اطلاعات) برای قضات حقوقی. در دورهٔ جرایم سایبری، کلیاتی در خصوص ادوار زمانی استفاده از رایانه و مسائل جزایی ناشی از آن، تقسیم‌بندی و شرح مختصر انواع جرایم سایبری، ماهیت جرایم سایبری، آیین رسیدگی به این جرایم و صلاحیت سایبری مطرح می‌گردد. در مقابل، در دورهٔ دعاوی حقوقی بیشتر به مباحث حقوقی از جمله قراردادهای انفورماتیک، مسئولیت مدنی در محیط دیجیتال و مالکیت فکری در فضای مجازی پرداخته می‌شود. بدین ترتیب قضات حقوقی و کیفری با مسایل این حوزه آشنا شده و در صورت لزوم می‌توانند به دعاوی مطروحه در این حوزه رسیدگی کنند. علاوه بر آشنایی مراجع قضایی با چالش‌های مرتبط با این‌گونه جرایم در راستای اتخاذ سیاستگذاری صحیح به منظور مقابله با مرتکبان جرایم مزبور، ضرورت دارد مجریان قوانین مربوط به جرایم سایبری نیز از اطلاعات و دانش لازم و کافی برخوردار باشند. به همین منظور در ادامهٔ مطالب به بررسی نقش پلیس در پیشگیری و کشف این جرایم می‌پردازند.

۲- نقش پلیس در پیشگیری و کشف جرایم سایبری

از زمانی که بشر پا به عرصهٔ وجود گذاشت، احساس امنیت همواره از نیازهای اولیه او بوده است.امروزه می‌توان امنیت را بالاترین ارزش دانست و آن را مهم‌ترین کارکرد حکومت‌ها یا نظام‌های سیاسی تلقی کرد (صادقی، ۱۳۸۱ : ۱۹). امنیت اجتماعی یا عمومی[1] ، یکی از انواع امنیت و زیر مجموعه یکی از انواع امنیت ملی هر کشور به شمار می‌آید. سازمان پلیس، یکی از نهادهای مؤثری است که در عصر جدید، به منظور برقراری و حفظ نظم و امنیت و نیز پیشگیری از بروز جرایم در جامعه و نیز پیشگیری از بروز جرایم در جامعه (شاکری، ۱۳۸۱ :۱۵) از سوی نظام سیاسی ایجاد می‌شود و براساس این رسالت، به طور عمده و مستقیم با اجتماع و مردم تعامل دارد.

چنان چه پیش از این اشاره شد، فناوری اطلاعات با سرعت شگفت‌انگیزی، تمامی ارکان حیات بشری از جمله مقولهٔ نظم و امنیت و آرامش عمومی را دستخوش تحولات و دگرگونی‌های اساسی قرارداده است. همزمان با ظهور رایانه و اینترنت و فرآیند جهانی شدن در عصر حاضر، فناوری اطلاعات و ارتباطات امکان ظهور جامعهٔ شبکه‌ای[1]

1. Social Security or Public Safety

را فراهم آورده است که تعاریف جدیدی از هویت‌ها و جوامع انسانی عرضه می‌کند و بافت اصلی آن را، اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد. در نتیجهٔ پیدایش این جامعهٔ شبکه‌ای، مراودات اجتماعی از شکل سنتی خود به صورت جوامع مجازی[2] معاشرت‌های دیجیتالی از طریق متون الکترونیک و سیستم‌های چند رسانه‌ای، تغییر ماهیت داده‌اند که این امر باعث پیدایش نوعی ناامنی اجتماعی و ظهور جرایم و بزهکاری نوین در فضای مجازی شده است (احمدوند، ۱۳۸۳: ۵) و فرایند فاصله رو به رشد این نوع جرایم را می‌توان عامل ایجاد آسیب به امنیت اجتماعی و تحت‌الشعاع قرار دادن امنیت اخلاقی دانست.

در اینجاست که نقش پلیس و اهمیت آن به عنوان نهاد برقرارکنندهٔ نظم و امنیت اجتماعی و مسئول پیشگیری و کشف جرایم در جامعه مطرح می‌شود (آخوندی، ۱۳۸۰ :۵۳).

از آنجا که میان محیط فیزیکی و فضای مجازی، تفاوت‌های بسیاری وجود دارد، باید دید که آیا هنوز هم سیستم‌های پلیسی می‌توانند در چنین فضایی، کارایی داشته باشند و کارآمد باقی بمانند؟ آیا مرتکبان جرایم سایبری واقعاً فرسنگ‌ها از اجرای قانون پیشی گرفته‌اند؟ آیا از زمانی که سازمان‌های پلیس به رایانه دسترسی پیدا کرده‌اند، مبارزه با جرایم سایبری گسترش یافته است؟ یا استفاده ابزار فناوری برتر و دانش فنی، برای مقابله با جرایم سایبری، همیشه ضرورت دارد؟ پلیس تا چه حد مجاز است که مرتکبان این جرایم را تحت پیگرد قرار دهد؟ آیا ورود به حریم خصوصی الکترونیکی اشخاص، نقض حقوق شهروندی آن‌ها به شمار نمی‌رود؟ چگونه می‌توان میان حقوق شهروندی و نیاز مقامات پلیس برای تحقیقات به منظور کشف جرایم سایبری، تعادل برقرار کرد؟ پیش از بررسی پاسخ این پرسش‌ها و نیز سؤال‌های دیگری که در خصوص نقش پلیس در پیشگیری و کشف جرایم سایبری مطرح می‌شود، به مطالعهٔ تطبیقی اقدامات «پلیس بین‌الملل»[3] وپلیس کشورهای خارجی می‌پردازیم. بدیهی است ترتیب مزبور ما را در درک بهتر نقش پلیس در پیشگیری و کشف جرایم سایبری و برداشتن گام‌های مؤثر در همان راستا، مساعدت و یاری خواهد کرد.

الف) نقش پلیس بین‌الملل

سال‌های متمادی است که پلیس بین‌الملل، فعالیت خود را در مبازه با جرایم سایبری آغاز کرده است. این سازمان، با بهره‌گیری از متخصصان و کارشناسان کشورهای عضو، چند گروه کاری را در این زمینه تشکیل داده و رؤسای واحدهای مبارزه با جرایم سایبری کشورهای با تجربهٔ عضو سازمان را گرد هم آورده است (گنجی، ۱۸۳۱ : ۲۰). گروه‌های کاری منطقه‌ای در اروپا، آسیا، آمریکا و آفریقا، زیر نظر کمیتهٔ

1. Network Society
2. Virtual Societis
3. Interpol

راهبردی جرایم فناوری اطلاعات، مستقر در دبیرخانهٔ کل پلیس بین‌الملل فعالیت می‌کنند. گروه کاری اروپایی پلیس بین‌الملل با حضور کارشناسانی از هلند، اسپانیا، بلژیک، آلمان، فرانسه، فنلاند، انگیس، سوئد و ایتالیا در سال ۱۹۹۰ میلادی تشکیل شد و از آن به بعد، سه مرتبه در سال،تشکیل جلسه می‌دهد. از جمله فعالیت‌های گروه کاری می‌توان به تهیهٔ کتاب و سی‌دی راهنمای جرایم رایانه‌ای و پی‌جویی آن‌ها، تشکیل دوره‌های آموزشی برای نیروهای پلیس در طول پنج سال گذشته، سیستم اعلام خطر و پاسخگویی شبانه‌روزی اشاره کرد.

گروه کاری آمریکایی جرایم مرتبط با فناوری اطلاعات پلیس بین‌الملل مرکب از کارشناسان و متخصصان کشورهای کانادا، آرژانتین، جامائیکا، ایالات متحده، کلمبیا و شیلی است که تاکنون چندین دورهٔ آموزشی نیز برای نیروهای پلیس برگزار کرده است.

گروه کاری جنوب اقیانوس آرام و آسیایی پلیس بین‌الملل که در هند تشکیل شده و متخصصانی از کشورهای چین، هنگ کنگ، هند، استرالیا، ژاپن، نپال و سریلانکا عضو آن می‌باشند، فعالیت خود را از نوامبر سال ۲۰۰۰ میلادی آغاز کرده است.

گروه کاری آفریقایی به منظور پیشگیری از جرایم مرتبط با فناوری اطلاعات، مرکب از کارشناسان آفریقای جنوبی، نامیبیا، تانزانیا، زیمبابوه، اوگاندا، بوتسوانا، لسوتو و رواندا در ژوئن سال ۱۹۹۸ میلادی آغاز کرد. این گروه، دومین دورهٔ آموزش نیروهای پلیس را نیز با مساعدت مالی سفارت‌خانه‌های انگلیس و فرانسه برگزار کرده است(پرویزی، ۱۳۸٤: ۸۷).

ب) نقش پلیس کشورهای خارجی

بسیاری از کشورهای خارجی، سال‌های طولانی است که فناوری اطلاعات را به روش‌های گوناگون به خدمت گرفته و با آثار و تبعات مثبت و منفی آن، پیش از ما آشنا شده‌اند و درصدد تقویت جنبه‌های مثبت و مبارزه با آثار و پیامدهای منفی ناشی از آن، که در قالب جرایم سایبری ظاهر شده، برآمده‌اند. از جملهٔ این کشورها می‌توان به فرانسه، آلمان، ایتالیا، اسپانیا، روسیه، ایالات متحدهٔ آمریکا، انگلیس، چین و ژاپن اشاره کرد؛ برای مثال، در کشورهای فرانسه، از ژانویهٔ ۱۹۷۸ میلادی با تصویب «قانون انفورماتیک و آزادی» که علمای حقوق آن را «منشور بزرگ حقوق بشر در مورد انفورماتیک» خوانده‌اند، فضای مجازی قانون‌مند شد، اما در آن، رایانه به عنوان وسیله‌ای برای آسیب رساندن به اموال، در نظر گرفته نشده بود. به همین منظور مجلس فرانسه با تصویب «قانون پنجم ژانویه ۱۹۸۸ راجع به جرایم رایانه‌ای» که در سال ۱۹۹٤ میلادی در قانون جزای فرانسه ادغام گردید، موجب شد که پلیس متخصص در این حوزه با ایجاد یک واحد مرکزی تخصصی، فعالیت خود را رسماً آغاز کند(جعفری، ۱۳۸۵: ۷۰).

پلیس ملی اسپانیا در سال ۱۹۹۵ میلادی اقدام به تأسیس یک گروه تخصصی پیشگیری و کشف جرایم ناشی از فناوری پیشرفته کرد. این واحد به مبارزه با جرایم مرتبط با رایانه، به ویژه جرایم سازمان یافته در این زمینه، می‌پردازد. گروه مذکور تحت نظارت «واحد مرکزی عملیات»، که بخشی از «ادارهٔ پلیس قضایی گارد شهری» است، قرار دارد و در زمینه‌هایی از جمله امنیت رایانه و مبارزه با جرایم ارتکابی در اینترنت فعالیت می‌کند (پرویزی، ۱۳۸٤ : ۸۹).

ج) نقش پلیس جمهوری اسلامی ایران

پلیس جمهوری اسلامی ایران تلاش می‌کند تا با بهره‌گیری از آخرین دستاوردهای فناوری اطلاعات و ارتباطات سیستم‌های پیشرفتهٔ انتظامی – امنیتی کشور، امنیت اجتماعی را بهبود بخشیده و محیطی امن توأم با آسایش عمومی را برای کلیهٔ شهروندان، در پرتو ارزش‌های اسلامی فراهم کند(احمدوند، ۱۳۸۳: ۲۲).

معاونت آگاهی نیروی انتظامی جمهوری اسلامی ایران، اواخر سال ۱۳۷۸ ش، به انحای گوناگون شروع به جمع‌آوری اطلاعاتی پیرامون جرایم سایبری کرد و در همین راستا، تحقیقی تحت عنوان «شناخت جرایم سایبری» توسط جهاد دانشگاهی دانشگاه علم و صنعت صورت گرفت. همچنین با بهره‌گیری از نظریات کارشناسان و متخصصان شورای عالی انفورماتیک و تشکیل جلسات متعدد با صاحب‌نظران حقوقی و انفورماتیکی، به این نتیجه دست یافت که تشکیل واحدهای مبارزه با جرایم سایبری ضروری است (پرویزی، ٤٨٣١ : ۳۹).

تلاش‌های انجام شده سبب تصویب و ابلاغ تشکیل اداره کل مبارزه با جرایم رایانه‌ای در زیرمجموعهٔ معاونت آگاهی و همچنین تشکیل دایرهٔ مبارزه با جرایم رایانه‌ای در ادارهٔ آگاهی تهران بزرگ شد. بدین‌ترتیب، پلیس متخصص برای پیگیری پرونده‌های جرایم رایانه‌ای، از سال ۱۳۸۱ ش فعالیت خود را با قوت و اقتدار، رسماً آغاز کرد. اگر چه در حال حاضر، پلیس حافظ نظم و امنیت در فضای مجازی است، اما تا زمانی که قانون جرایم رایانه‌ای به تصویب نرسد، نقش چندانی را نمی‌توان از آن انتظار داشت؛ هر چند «قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای»، تا حدودی این مشکل را حل کرده است.

۱ – نقش پلیس در پیشگیری از جرایم سایبری

اگر چه حقوقدانان به منظور حفظ نظم جامعه و پیشگیری از وقوع جرم، برای قوانین آیین دادرسی کیفری اهمیت بیشتری قایل شده‌اند (آخوندی، ۱۳۸۰: ٦٤) و پلیس را صرفاً مسئول کشف و تعقیب جرایم می‌پندارند، اما باید اذغان داشت که پلیس را می‌توان مهم‌ترین عامل پیشگیری از جرم به شمار آورد؛ زیرا نقش حساس آن اقتضا می‌نماید که گام‌هایی جلوتر از زمان برداشته و از پیش، آمادگی‌های لازم برای مواجهه

با ناامنی‌های احتمالی آینده را احراز کند (مظفری، ۱۳۸٤: ۵۸).

بدون تردید، سیستم کلان مبارزه با جرم، که از سوی پلیس اتخاذ 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 مبارزهٔ وضعی و سیاست عام این نهاد در مقابله با سایر جرایم نیست، اما آنچه باعث تفاوت در این حوزه می‌شود، ویژگی‌های منحصر به فرد جرایم سایبری است که شیوه‌های اجرایی خاص خود را به منظور تحقق این سیاست عام طلب می‌کند(آیکاو، ۱۳۸۳: ۱۵۱).

در محیط فیزیکی، حضور پلیس در جامعه عاملی در پیشگیری از جرم محسوب می‌شود. شکل و ترکیب خودروی پلیس و مأموران ملبس به لباس پلیس، تهدید برای مجرمان بالقوه به شمار می‌رود؛ به بیان دیگر، حضور پلیس در جامعه را می‌توان نوعی تهدید ضمنی برای مجرمان تلقی کرد. بدون تردید، حضور فیزیکی پلیس در مواردی که جرایم سایبری با ورود کاربران غیرمجاز به یک سایت رایانه‌ای صورت می‌پذیرد، نقش مؤثری در پیشگیری از این جرایم خواهد داشت (آیکاو، ۱۳۸۳ : ۱٦۹)، اما آیا به هنگامی که جرایم مزبور توسط خطوط ارتباطی و از طریق شبکهٔ اینترنت و بدون نفوذ فیزیکی در سایت رایانه‌ای ارتکاب می‌یابد، می‌توان اقدامات پیشگیرانه را در این فضای مجازی تصور کرد و آن را محقق دانست؟

به نظر می‌رسد در چنین فضایی نیز می‌توان حضور داشت و با گشت‌زنی و مراقبت، مجرمان بالقوه را تهدید کرد. به منظور انجام این امر، ابزارها و روش‌های خاصی مورد نیاز است که آشنایی با آن‌ها برای مأموران گشت شبکه‌های رایانه‌ای واحد مبارزه با جرایم سایبری سازمان‌های پلیس لازم و ضروری است. گشت‌زنی و مراقبت یک مظنون در فضای مجازی کار چندان آسانی نیست و هیچ سازمان پلیسی، هر چند قدرتمند، به تنهایی نمی‌تواند این کار را انجام می‌دهد، بلکه همکاری چند بخشی دولتی و غیردولتی لازمهٔ این اقدام است. در این مرحله از کار وجود تعامل و همکاری مناسب میان شرکت‌های مخابراتی ارائه دهندهٔ خدمات و پلیس، اهمیت ویژهٔ خود را نشان می‌دهد. در راستای لزوم همین تعامل است که مادهٔ ۳۱ پیش‌نویس قانون جرایم رایانه‌ای، اداره کل جرایم رایانه‌ای نیروی انتظامی را مجاز می‌داند در راستای وظایف پیشگیری از جرایم سایبری، به طور مداوم به داده‌های حاصل از تبادل اطلاعات دسترسی داشته و کلیهٔ ارائهٔ‌کنندگان خدمات را مکلف دانسته که در این خصوص با مأموران پلیس همکاری کند.

امروزه نرم‌افزارهای قدرتمندی در اختیار پلیس وجود دارد که شبیه سیستم‌های دزدگیر عمل کرده پلیس یا مسئول امنیتی را از هرگونه تهدید قریب‌الوقوع به منظور انجام عملیات مجرمانه در فضای مجازی مطلع می‌سازد و امکان پیشگیری از این جرایم را به پلیس خواهد داد. به علاوه، این نرم‌افزارها، آن دسته از کاربران مجاز که

با عدم رعایت مقررات مربوط به طبقه‌بندی، قصد دسترسی به اطلاعات غیرمجاز را دارند، شناسایی کرده و مشخصات لازم را در اختیار پلیس خواهد گذاشت. بسیاری از سیستم‌ها، اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد در ورود به سیستم را ثبت می‌کنند (وایدینگ، ۱۳۷۹: ۹۳). همچنین سیستم‌های مزبور امکان شناسایی افراد غیرمجاز که به طور مکرر، رمز عبور نادرست را توسط صفحه کلید تایپ می‌کنند نیز وجود دارد.البته چنان‌چه کاربر غیرمجاز، اطلاعات لازم برای ورود به سیستم را داشته باشد، با نفوذ در رایانه و دستیابی به فایل‌های حاوی رمز عبور، تمهیدات فوق را بی‌ثمر خواهد کرد.

یکی دیگر از شیوه‌های پیشگیری از جرم، که سال‌هاست به طور معمول توسط نیروی‌انتظامی به کار گرفته می‌شود، آموزش همگانی و همچنین شناسایی و ارائهٔ آموزش‌های خاص به اشخاص و سازمان‌هایی است که احتمال دارد در معرض جرایم سایبری قرار گیرند. در واقع، به‌کارگیری این شیوه، به همان اندازه که در پیشگیری از جرایم ارتکابی در محیط فیزیکی مؤثر است، در فضای مجازی نیز از تأثیر قابل توجهی برخوردار خواهد بود.

۲ – نقش پلیس در کشف جرایم سایبری

دستیابی به هدف اصلی حقوق کیفری که مبارزه علیه بزهکاری و حفظ نظم و امنیت و آسایش افراد جامعه است، بدون شناسایی و کشف جرم، دستگیری مجرم، صدر حکم و اجرای مجازات ممکن نیست. به موجب بند ۱ ماده ۱۵ قانون آیین دادرسی کیفری، نیروی انتظامی جمهوری اسلامی ایران، در مقام ضابط دادگستری، تحت نظارت و تعلیمات مقام قضایی، در کشف جرم و بازجویی مقدماتی، حفظ آثار و دلایل جرم و جلوگیری از فرار و مخفی شدن متهم، به موجب قانون اقدام می‌کند و چرخ‌های عدالت کیفری را به حرکت در آورده مبارزهٔ عملی با جرم و مجرمان را تحقق می‌بخشد (آخوندی، ۱۳۸۰: ۵۳).

از این دیدگاه پلیس در سیستم کلان مبارزه با جرم، تهدید بالفعل مجرمان، بازدارندگی و ارعاب مجرمان بالقوه و همچنین تسریع در اجرای مجازات، دارای نقش مهم و ارزنده‌ای خواهد بود که برای ایفای این نقش، باید به کشف جرایم، اعم از سنتی و پیشرفته بپردازد (پرویزی، ۱۳۸٤: ۸۱). در اینجا نیز، علی‌رغم سیاست‌های عام و مشترک موجود در کشف تمام جرایم، به دلیل وجود تفاوت‌های ماهوی میان محیط فیزیکی و فضای مجازی، روش‌های کشف جرایم سایبری نیز متفاوت خواهد بود؛ برای مثال صحنهٔ جرایم ارتکابی در محیط فیزیکی، به طور معمول، متمرکز بوده و پراکندگی جغرافیایی نخواهند داشت، اما در جرام سایبری، پراکندگی جغرافیایی صحنهٔ جرم بسیار زیاد و معمولاً دور از هم و در محدودهٔ مرزی کشورهای مختلف است. ابزارهای بررسی صحنهٔ جرایم سایبری، عمدتاً نرم‌افزارهای تخصصی می‌باشند که

براساس استانداردهای بین‌المللی تولید شده از سوی مأموران پلیس مورد استفاده قرار می‌گیرند. بنابراین با ابزارهای بررسی صحنهٔ سایر جرایم تفاوت اساسی دارند. دلایل ارتکاب جرایم سایبری، غالباً ادلهٔ الکترونیک است که با سرعت قابل ملاحظه‌ای، امکان‌تغییر و از بین بردن آن‌ها وجود دارد (رضایی، ۱۳۸۵: ۳۱). بنابراین، سرعت عمل در شناسایی و جمع‌آوری این دلایل، بسیار ضروری خواهد بود(گاتن، ۱۳۸۳: ۳۱).

بدون تردید، در راستای تحقق نقش مؤثر پلیس در کشف جرایم سایبری، استفاده از نیروهای متخصص پلیس در این حوزه و شیوه‌های تحقیق و بررسی توسط این نیروها، از اهمیت فوق‌العاده‌ای برخودار است و ضرورت مطالعهٔ آن در تحقیق مزبور بیش از هر امر دیگری احساس می‌شود.

الف) ویژگی‌های مأموران کشف جرایم سایبری

سیاست‌های کلی نیروی انتظامی جمهوری اسلامی ایران مبتنی بر این اصل است که در راستای تربیت پلیس مقتدر، با در نظر گرفتن معیارهای متنوع، ویژگی‌های مختلفی از جمله: تقوا، قاطعیت، قانون‌مندی، مردمی‌بودن و توانایی‌های علمی و تخصصی را در مأموران خود به وجود آورد (جهانتاب، ۱۳۸٤ :۱۲۵). اما پرسشی که در اینجا باید به آن پاسخ داده شود، این است که آیا همان خصوصیات شخصیتی، مهارت‌ها و آگاهی‌های مأموران پلیس کشف و تعقیب جرایم ارتکابی در محیط فیزیکی، برای مأموران کشف جرایم سایبری نیز کافی است یا مأموران اخیر، نیازمند آموزش‌های خاصی هستند؟

چنانچه واضح است، علاوه بر خصوصیاتی که در میان همهٔ مأموران پلیس مشترک است، مأمور کشف جرایم سایبری باید ویژگی‌های دیگری نیز داشته باشد، برای مثال شناخت علم رایانه، چگونگی عملکرد و اصطلاحات مورد کاربرد در آن و نیز آگاهی از مسائل امنیتی رایانه و شبکه به منظور کشف جرایمی از قبیل هک‌کردن سایت‌ها یا تهاجم به شبکه، برای آن دسته از مأموان پلیس که در این حوزه فعالیت دارند، ضروری است. بنابراین، مأموران کشف جرایم سایبری، به منظور برخورداری از عملکرد مؤثر در این حوزهٔ ویژه، نیازمند آموزش‌های وسیع و جامعی هستند. به طور معمول، سازمان‌های بزرگ پلیس، که در آن متخصصان فناوری اطلاعات و علوم رایانه، به منظور کشف جرایم سایبری، اقدام به تشکیل گروه ویژه‌ای می‌کنند و به نیروهای پلیس اطلاعات لازم را می‌دهند، این نیاز به راحتی مرتفع سازند، اما اگر جرایم مزبور در جایی ارتکاب یابند که ادارهٔ پلیس آن محل فاقد امکانات یاد شده باشد، ضرورت آموزش تخصصی برای مأموران پلیس آشکارتر می‌شود.

کشف جرایم، فرایندی خلاق و نیازمند مهارت‌های خاصی است که می‌توان آن‌ها را آموخت و توسعه داد. اگرچه داشتن استعداد ذاتی برای تبدیل شدن به یک مأمور پلیس زبردست در حوزهٔ جرایم سایبری لازم است، اما این امر کافی نیست و برای توسعه و کامل کردن مهارت‌ها، آموزش نیز لازم است. آموزش پیشرفته در زمینهٔ جرایم

سایبری باید در دسترس کسانی که کشف جرم را عملاً اداره می‌کنند، قرار بگیرد. فناوری‌های نوین مدام در حال ظهور هستند و مأموران پلیس باید در جریان آخرین اطلاعات روز داشته باشند (پرویزی، ۱۳۸٤ : ۱۰۲).

در حال حاضر، علی‌رغم تشکیل دایرهٔ مبارزه با جرایم رایانه‌ای در ادارهٔ آگاهی نیروی انتظامی جمهوری اسلامی ایران، مقامی تحت عنوان «مأمور کشف جرایم سایبری» که وظیفهٔ او منحصراً بررسی جرایم ارتکابی در حوزه باشد، وجود ندارد. شاید یکی از دلایل این امر، فقدان قانون لازم‌الاجرا در خصوص جرایم ارتکابی در فضای مجازی می‌باشد؛ زیرا در صورتی که قانون خاصی در این حوزه تصویب شود، نیروی انتظامی به عنوان ضابط دادگستری، باید تمام تلاش خود را در جهت کشف این جرایم در کشور به کار گیرد.

ب) شیوهٔ کشف جرایم سایبری

پلیس به عنوان ضابط دادگستری، بلافاصله پس از اطلاع از وقوع جرم، باید اقداماتی را که برای حفظ آثار و دلایل جرم و جلوگیری از فرار یا اختفای متهم ضروری است، انجام دهد و مراتب را به مقام قضایی اعلام کند (آخوندی، ۱۳۸۰: ۳۵). از آنجا که دلایل ارتکاب جرم در فضای مجازی، عمدتاً ادلهٔ الکترونیک می‌باشند، پلیس به منظور بررسی و کشف جرایم سایبری با مسائلی مواجه می‌شود که در سایر جرایم مطرح نیست. ادلهٔ دلایل الکترونیک، ویژگی‌هایی دارند که آن‌ها را از دلایل سنتی متمایز می‌سازد. این گونه دلایل نسبت به اسناد و مدارک دیگر، آسیب‌پذیرتر هستند؛ زیرا به آسانی می‌توان آن‌ها را دستکاری یا جعل کرد و یا با استفاده از دانش فنی مناسب پنهان کرد (گاتن، ۱۳۸۳: ۱۰).

ماهیت خاص دلایل الکترونیکی به گونه‌ای است که پذیرش آن‌ها را در مراجع قضایی با چالش‌های ویژه‌ای مواجه کرده است. به منظور مقابله با این چالش‌ها، مأموران پلیس باید روش‌های خاص جمع‌آوری دلایل مذکور را که مرکب از چهار مرحلهٔ جمع‌آوری مدرک، بررسی، تجزیه و تحلیل و ارائهٔ گزارش می‌باشد، به نحو صحیحی اجرا کند.

مرحلهٔ جمع‌آوری شامل جست وجو برای شناسایی، جمع‌آوری و مستندسازی مدارک الکترونیکی است(پرویزی، ۱۳۸۵: ۱۱۰). برای اینکه پلیس بتواند داده‌ها یا سیستم‌های رایانه‌ای را تفتیش و توقیف نماید، به دستور مقام قضایی نیاز دارد؛ مگر کسی که داده‌ها یا سیستم‌های مذکور را در اختیار دارد، رضایت کتبی به منظور تفتیش آن بدهد. در عین حال، در صورت وجود ظن منطقی مبنی بر وجود ادله و فوریت امر، پلیس می‌تواند بدون دستور قضایی اقدام به تفتیش یا توقیف داده‌ها نماید. در حقیقت، هنگام بررسی دلایل وقوع جرم، پلیس باید اطمینان یابد که حقوق شخصی افراد را کاملاً رعایت کرده است (آیکاو، ۱۳۸۳: ۲۵۹).

فرایند بررسی، مدارک را قابل رؤیت کرده و اصل و مفهوم آن را مشخص می‌سازد.

این کار باید به طریقی صورت گیرد که دلایل موردنظر، از هرگونه تغییر، تحریف یا آسیب مصون بماند. در مرحلهٔ تجزیه و تحلیل، به ارزشی اثباتی و اهمیت دلیل پرداخته می‌شود و در نهایت در مرحلهٔ ارائهٔ گزارش، پلیس باید گزارش مکتوبی که کلیات مربوط به فرایند بررسی و اطلاعات مربوطهٔ به‌دست آمده را دارا باشد، به مقام قضایی ارائه دهد. دلایل ارائه شده تنها در صورتی قابلیت استناد خواهند داشت که ابزارها و روش‌های استاندارد در مراحل شناسایی، کشف، جمع‌آوری، مستندسازی، تجزیه و تحلیل، حفظ و مراقبت از دلایل الکترونیکی و ارائهٔ آن‌ها به دادگاه، به نحو صحیحی به کار گرفته شده باشد.

نتیجه گیری و پیشنهاد

میل و اشتیاق به استفاده از رایانه و اینترنت و بهره‌مندی از مزایای آن، اگرچه زمینهٔ مشارکت جوامع مختلف در فناوری‌های پیشرفته را فراهم کرده، اما در عین حال، شرایط و بستر مساعدی نیز برای ظهور جرایم سایبری به وجود آورده است. ماهیت و ویژگی‌های خاص جرایم سایبری از جمله داشتن ابعاد جهانی و فراملی، فقدان توافق جهانی پیرامون تعریف قانونی واحد از جرایم سایبری، بالا بودن سرعت ارتکاب این جرایم، فقدان رویه‌های مشخص پیرامون همکاری‌های متقابل و بالا بودن هزینه‌های کشف این جرایم، مراجع قضایی و انتظامی را با چالش‌های جدیدی مواجه کرده است.

به منظور پیشگیری از جرایم سایبری و مبارزه با آن، برخی اسناد بین‌المللی از جمله «کنوانسیون مبارزه با جرایم سایبری ۲۰۰۱ بوداپست» به تصویب رسیده‌اند. به علاوه، سازمان ملل و سازمان‌های منطقه‌ای نیز با انتشار متون و نشریات مختلف، در راستای پیشگیری از جرایم سایبری مبارزه با آن اقدامات خوبی را انجام داده‌اند. در سطح حقوق داخلی نیز برخی کشورها از جمله فرانسه، استرالیا و مالزی، قانون خاصی در این مورد به تصویب رسانده‌اند.

در حال حاضر، کشورما به هیچ کدام از کنوانسیون‌های بین‌المللی تصویب شده در این حوزه نپیوسته است، اما خصوصیت ویژهٔ جرایم ارتکابی در فضای مجازی مبنی برداشتن جنبهٔ فراملی و بین‌المللی، لزوم حکومت قواعدی از این قبیل را بر این دسته از جرایم، بیش از هر چیز دیگری روشن می‌سازد. به علاوه، با توجه به خلاء موجود در قوانین داخلی در حوزهٔ جرایم سایبری، لزوم تدوین و تصویب قانون خاصی در این خصوص احساس می‌شود. بنابراین پیش‌نویس قانون جرایم سایبری باید هرچه سریع‌تر به تصویب رسیده و به مرحلهٔ اجرا گذارده شود.

امروزه پلیس از این توانایی برخوردار است که با استفاده از نرم‌افزارهای قدرتمندی که در اختیار او قرار دارد، با گشت‌زنی و مراقبت در فضای مجازی، در پیشگیری از وقوع جرایم سایبری نقش مؤثری ایفا کند. تعامل و همکاری مناسب میان شرکت‌های

مخابراتی ارائه‌کنندهٔ این‌گونه خدمات و پلیس می‌تواند در فرایند پیشگیری، کمک زیادی داشته باشد. آموزش همگانی و همچنین شناسایی و ارائهٔ آموزش‌های خاص به اشخاص و سازمان‌هایی که احتمال می‌رود در معرض جرایم سایبری قرار گیرند، یکی دیگر از شیوه‌های پیشگیری از این جرایم است.

مأموران پلیس کشف جرایم سایبری، علاوه بر خصوصیاتی که در میان همهٔ مأموران پلیس مشترک است، باید از ویژگی‌های دیگری از جمله شناخت علم رایانه، چگونگی عملکرد آن و آگاهی از مسائل امنیتی رایانه و شبکه، برخوردار باشند و نیازمند آموزش‌های وسیع و جامعی در این خصوص هستند. در حال حاضر، علی‌رغم تشکیل دایرهٔ مبارزه با جرایم رایانه‌ای در ادارهٔ آگاهی، مقامی تحت عنوان «مأمور کشف جرایم سایبری» که وظیفهٔ او منحصراً بررسی جرایم ارتکابی در این حوزه باشد، وجود ندارد. اما با در نظر گرفتن روند روبه‌رشد ارتکاب جرایم سایبری، آموزش تخصص‌های لازم به مأموران ویژهٔ پلیس، به منظور کشف این جرایم، ضروری به نظر می‌رسد.

دلایل ارتکاب جرم در فضای مجازی، عمدتاً الکترونیک هستند. این دلایل در صورتی توان اثباتی دارند که نیروهای پلیس در مرحلهٔ کشف و جمع‌آوری آن‌ها، ابزار و روش‌های خاص ادلهٔ مذکور را که مرکب از چهار مرحلهٔ جمع‌آوری، بررسی، تجزیه و تحلیل و ارائهٔ گزارش به مقام قضایی می‌باشد به نحو صحیحی رعایت بکنند.

کتابنامه

- آخوندی، محمود (۱۳۸۰)، **آیین دادرسی کیفری**؛ چاپ نهم، تهران: وزارت فرهنگ و ارشاد اسلامی، ج ۱.
- آنجلیز، جینا (۱۳۸۳)، **جرایم سایبری**، ترجمه: سعید حافظی و عبدالصمد خرم‌آبادی، چاپ اول، تهران: دبیرخانهٔ شورای عالی اطلاع رسانی.
- آیکاو، دیوید جی (۱۳۸۳)؛ **راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای**؛ ترجمهٔ اکبر استرکی، محمد صادق روزبهانی، تورج ریحانی و راحله الیاسی؛ تهران: معاونت پژوهش دانشگاه علوم انتظامی.
- احمدوند، علی‌محمد و عطایی جعفری، امیر مسعود (۱۳۸۳)؛ نقش و راهبرد فناوری اطلاعات در سیستم پلیس و فضاهای مجازی جرایم در ایران؛ **دوماهنامهٔ توسعهٔ انسانی پلیس**، سال اول، شمارهٔ ۳ ، آذر و دی.
- اردبیلی، محمد علی (۱۳۸۰)؛ **حقوق جزای عمومی**؛ چاپ دوم، تهران: میزان، ج۱ .
- الماسی، نجاد علی (۱۳۸۲) **حقوق بین‌المللی خصوصی**؛ چاپ اول،تهران: میزان.
- پرویزی، رضا (۱۳۸٤)؛ **پی‌جویی جرایم رایانه‌ای**؛ چاپ اول، تهران: جهان جام‌جم.
- جعفری، مجتبی (۱۳۸۵)؛ بزهکاری رایانه‌ای در رویارویی با حقوق جزای فرانسه؛ **نشریهٔ حقوقی گواه**، شمارهٔ ٦ و۷ ، بهار و تابستان.
- جهانتاب، محمد (۱۳۸٤)؛ پلیس مقتدر؛ **فصلنامهٔ دانش انتظامی**؛ سال هفتم، شمارهٔ

۲، تابستان .
- خداقلی، زهرا (۱۳۸۳)؛ **جرایم کامپیوتری**؛ چاپ اول، تهران:آریان.
- دزیانی، محمد حسن (۱۳۸٤)، اخبار جرایم سایبری؛ **خبرنامهٔ انفورماتیک**، سال بیستم، شمارهٔ ۹۸، بهمن.
- دبیرخانهٔ شورای عالی انفورماتیک (۱۳۷٦)، راهنمای سازمان ملل برای پیش‌گیری از جرایم مرتبط با رایانه؛ **نشریهٔ بین‌المللی سیاست جنایی در جرایم سایبری**، ٤۳ و ٤٤ مرداد.
- راجی، سید محمد هادی (۱۳۸۵) ؛ نگاهی به قانون تجارت الکترونیکی؛ **نشریهٔ حقوقی گواه**، شمارهٔ ٦ و۷ ، بهار و تابستان.
- رضایی، روح‌الله (۱۳۸۵)؛ اعتبار اسناد الکترونیک با توجه به قوانین داخلی و بین‌المللی؛ **نشریهٔ حقوقی گواه**، شمارهٔ ٦و۷ بهار و تابستان.