بررسی قوانین و مواد مرتبط با جرم جاسوسی رایانه‌ای

پیمان رضائی‌ور[1]

چکیده

این مقاله، در صدد بررسی ابعاد مختلف جاسوسی در فضای مجازی و مباحث جرم‌انگاری و حقوقی آن، تبیین وجوه تشابه و افتراق جاسوسی سنتی با جاسوسی سایبری، تبیین شرایط و عناصر جاسوسی در فضای مجازی با رویکرد دستیابی غیرمجاز به اطلاعات و برهم‌زدن امنیت کشور و تبیین رویکرد قوانین موضوعهٔ ایران نسبت به جاسوسی در فضای مجازی است. در این مقاله، جاسوسی رایانه‌ای و ابعاد آن از نظر قانون جرائم رایانه‌ای، و نیز قوانین و مواد مرتبط به جرم جاسوسی رایانه‌ای موردبررسی قرار می‌گیرد. همچنین به چالش‌ها و موانع موجود در مسیر رسیدگی به جرائم رایانه‌ای و به‌طور اخص به جاسوسی رایانه‌ای، تفاوت و شباهت‌ها و رابطهٔ بین مواد گوناگون دربارهٔ جاسوسی در قانون مجازات اسلامی پرداخته می‌شود. درنهایت نیز پیشنهادهایی برای برطرف شدن خلأهای قانونی و مشکلات حقوقی ارائه شده است.

کلمات کلیدی: جاسوسی، جاسوسی رایانه‌ای، قانون جرائم رایانه‌ای، جرم در فضای مجازی.

---

۱. وکیل پایه‌یک دادگستری، دانشجویی دکتری حقوق کیفری و جرم‌شناسی. rezaievar.p@gmail.com

مقدمه

جاسوسی رایانه‌ای از رایج‌ترین اشکال جرم رایانه‌ای است که امنیت داخلی و خارجی کشور را تهدید می‌کند. جاسوسی کلاسیک ناظر به کسب اسرار سیاسی و نظامی و انتقال آن‌ها به کشور بیگانه و جاسوسی رایانه‌ای، علاوه بر انتقال داده‌های سری، ناظر به کسب اسرار تجاری، حرفه‌ای، صنعتی، اقتصادی و انتقال آن به افراد فاقد صلاحیت است که از طریق سیستم‌های رایانه‌ای انجام می‌شود.

هر پدیده اجتماعی به‌طور خاص برای آن‌که وصف مجرمانه بگیرد و قابل‌مجازات باشد باید بر طبق مادهٔ ۲ قانون مجازات اسلامی برای آن مجازات تعیین شده باشد یعنی این‌که هر فعل یا ترک فعلی که به‌موجب قانون برای آن مجازات تعیین شده قابل‌مجازات است و وصف مجرمانه دارد و جرم محسوب می‌شود وگرنه بر طبق اصل قانونی بودن جرم و مجازات نمی‌توان آن پدیده ضداجتماعی را جرم خواند و همین بحث در جاسوسی رایانه‌ای، هم مدنظر است. در مورد این‌که جاسوسی رایانه‌ای عملی خلاف اخلاق و ضداجتماعی و یک ناهنجاری اجتماعی است و باعث می‌شود اعتماد عمومی کم‌رنگ شود شکی نیست، لیکن برای مجازات مرتکبین جاسوسی رایانه‌ای ما نیاز به قانون داریم که این پدیده را جرم‌انگاری کرده باشد که این امر را ما در مواد ۳ و ۴ و ۵ قانون جرائم رایانه‌ای و مادهٔ ۶۴ و ۷۵ قانون تجارت الکترونیکی مشاهده می‌کنیم.

همچنین در قوانین کیفری ایران تعریف صریحی از جرم جاسوسی به عمل نیامده است. این رویکرد در قانون جرائم رایانه‌ای نیز قابل‌مشاهده است زیرا صرفاً مصادیق حصری و احکام آن طی سه مادهٔ (۳، ۴، ۵) در مبحث سوم فصل اول قانون جرائم رایانه‌ای و مواد ۶۴ و ۷۵ قانون تجارت الکترونیک تحت عنوان حمایت از اسرار تجاری بیان شده است با وجود این خلأ در مورد جاسوسی حقوق‌دانان تعاریف متعددی را عرضه کرده‌اند که با در نظر گرفتن این تعاریف می‌توان گفت: «جاسوسی رایانه‌ای یعنی تفحص و تجسس غیرمجاز پیرامون داده‌های سری به‌وسیله رایانه».

اما در مورد تعریف جاسوسی رایانه‌ای از دیدگاه حقوق بین‌الملل می‌توان گفت: شورای اروپا جاسوسی رایانه‌ای را این‌گونه تعریف کرده است: کسب اسرار تجاری یا حرفه‌ای از راه‌های نادرست یا افشا، انتقال و یا استفاده از این اسرار بدون داشتن حق یا هرگونه توجیه قانونی با قصد وارد کردن زیان اقتصادی به فردی که محق در نگه داشتن اسرار است یا تحصیل یک امتیاز اقتصادی غیرقانونی برای خود یا یک شخص ثالث.

البته لازم به ذکر است به این تعریف ایراداتی وارد است؛ اولاً با بیان اسرار تجاری یا حرفه‌ای در آن عملاً این تعریف را از موارد دیگر اسرار ازجمله اسرار امنیتی و اطلاعاتی و فرهنگی خارج کرده که شامل موارد دیگر جاسوسی رایانه‌ای نمی‌شود و با این عنوان به‌طور کامل هماهنگی ندارد و ثانیاً در مورد قصد مرتکب از ارتکاب این جرم که در تعریف فقط منافع اقتصادی مدنظر قرار گرفته که این نیز درست به نظر نمی‌رسد. چراکه ممکن است جاسوسی اهدافی برتر از منافع اقتصادی داشته باشد مثلاً صرفاً اهداف ملی مدنظر باشد. ثالثاً در این تعریف جاسوسی رایانه‌ای تعریف نشده، بلکه صرفاً مصادیق جاسوسی رایانه‌ای آن هم نه به‌صورت کامل بیان شده است.

از خصوصیات مهم و اساسی هر تعریفی این است که باید موضوع موردبحث را به شیوه‌ای آشکار بیان نماید به‌طوری‌که جامع‌ومانع یا منعکس باشد. این امر در مباحث کیفری و جزایی که آثار مهم و گاهی زیان‌بار دارد، بسیار حائز اهمیت است، زیرا با اندک غفلت و مسامحه‌ای در تعریف و شناخت ارکان و عناصر جرم، ممکن است عمل ارتکابی مصداق قانونی شود که با مجازات مقرر در آن قانون تناسبی نداشته باشد. با نگاهی به تعریف بیان‌شده در بالا متوجه می‌شویم اولاً تعریف ارائه‌شده توسط شورای اروپا یک تعریف جامع‌ومانع نیست و ثانیاً در حقوق داخلی هم تعریف کاملی در خصوص جاسوسی رایانه‌ای نداریم و صرفاً احکامی در خصوص فعل جاسوسی بیان شده است؛ بنابراین در اینجا باید این نکته را بیان کنیم که در خصوص عنوان جاسوسی رایانه‌ای تعریفی روشن ارائه نشده و فقط باید به نتیجه‌گیری‌های کلی در این خصوص تکیه کرد.

این مقاله درصدد بررسی موضوع، قوانین و مواد مرتبط با جرم جاسوسی رایانه‌ای است. در مبحث اول، موضوع جرم جاسوسی رایانه‌ای بررسی شده است. بررسی قوانین مرتبط با جاسوسی رایانه‌ای در مبحث دوم ارائه شده است و مبحث سوم نیز مربوط به بررسی مواد مرتبط با جاسوسی رایانه‌ای است.

۱. موضوع جرم جاسوسی رایانه‌ای

جاسوسی رایانه‌ای یکی از رایج‌ترین انواع جرائم رایانه‌ای محسوب می‌شود به علت ارزشمند بودن اطلاعات ذخیره‌شده در مراکز رایانه‌ای این جرم به‌طور ویژه‌ای برای مرتکب سودمند و برای شرکت متضرر از جرم، خطرناک است. در همه کسب‌وکارها هدف اصلی جاسوسی کامپیوتری «برنامه‌های کامپیوتری» است. ارزش این اهداف جدید جرم را می‌توان از این واقعیت دریافت که در سال ۱۹۸۵ فروش برنامه‌های کامپیوتری تقریباً ۵۵ میلیارد دلار برآورد شده است. در بخش تجاری هدف اصلی جاسوسی کامپیوتری به دست آوردن درآمدهای هنگفت از طریق فروش برنامه‌های ضدجاسوسی است.

۱-۱. روش ارتکاب جرم جاسوسی رایانه‌ای

در خصوص روش ارتکاب جرائم رایانه‌ای و جرم جاسوسی کامپیوتری و سرقت نرم‌افزار باید گفت که رایج‌ترین روش برای به دست آوردن داده‌ها کپی کردن فایل‌های داده است. در زمینه برنامه‌هایی که به تعداد انبوه تولید و به فروش می‌رسند کپی کردن برنامه‌ها روش معمول و سریع است که با وجود این در صورت وجود برنامه‌های ویژه کپی کردن، ممکن است بسیار دشوار شود. در خصوص برنامه‌هایی که به تعداد انبوه تولید نمی‌شود کپی کردن عمدتاً به‌وسیله برنامه‌های کمکی یا به‌وسیله برنامه‌های خودساخته (که بعضاً در غالب برنامه‌های اجرایی معمولی جا زده می‌شوند) یا به‌وسیله زیربرنامه‌های اسب تروآ که به برنامه‌های ممتاز اجرایی نفوذکننده صورت می‌گیرد (زیبر، ۱۳۹۰: ۳۵).

ممکن است جاسوسی از طریق ارسال پیام‌های ناخواسته الکترونیکی واقع شود. پیام‌های ناخواسته هم می‌توانند حامل نرم‌افزارهای جاسوسی باشند و هم ممکن است شرایط تخلیه اطلاعاتی دریافت‌کننده پیام ناخواسته را فراهم سازند و ساده‌تر از همه جاسوسی رایانه‌ای ممکن است با فریب یا تحریک متصدی حفظ اطلاعات رایانه‌ای طبقه‌بندی‌شده از طریق بهره‌گیری از مسائل شخصی یا عاطفی صورت گیرد (Morris-Sheridan, 2004, p.16).

۲. بررسی قوانین مرتبط با جاسوسی رایانه‌ای

در باب عنوان جاسوسی رایانه‌ای قوانین متنوعی وجود ندارد فقط در قانون جرائم رایانه‌ای در مادهٔ ۳، ۴ و ۵ به این موضوع پرداخته است اما قانون مجازات اسلامی و قانون جرائم نیروهای مسلح از جنبه پرداختن به موضوع جرم جاسوسی به قانون جرائم رایانه‌ای شباهت‌ها و تمایزهای قابل‌تأملی دارد لذا در اینجا به بررسی این ۳ قانون درباره موضوع فوق می‌پردازیم:

۲-۱. مواد قانون جرائم رایانه‌ای (قانون جرائم رایانه‌ای)

لایحه جرائم رایانه‌ای به شماره چاپ ۱۲۲ که جهت رسیدگی به کمیسیون قضایی و حقوقی مجلس شورای اسلامی به‌عنوان کمیسیون اصلی ارجاع شده بود در جلسه‌ای در تاریخ ۱۳۸۷/۵/۷ با حضور کارشناسان ذی‌ربط مطرح گردید و پس از بحث و تبادل‌نظر کلیات آن عیناً مورد تصویب قرار گرفت. با تصویب این قانون در سال ۸۸ دیگر لازم نیست قضات جرائم ارتکابی را با مواد قانونی قبل تطبیق دهند.

در مادهٔ ۳، ۴ و ۵ لایحه فوق که بعداً قانون گردید به‌عنوان جاسوسی رایانه‌ای پرداخته است.

مادهٔ ۳ قانون جرائم رایانه‌ای «هرکس به‌طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد»:

الف- دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست‌میلیون (۲۰,۰۰۰,۰۰۰ ریال) تا شصت‌میلیون (۶۰,۰۰۰,۰۰۰ ریال) یا هر دو مجازات.

ب- در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دوتا ده سال.

ج- افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها، به حبس از پنج تا پانزده سال.

تبصره ۱: داده‌های سری داده‌هایی است که افشای آن‌ها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره ۲: آیین‌نامهٔ نحوهٔ تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت آن‌ها ظرف ۳ ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت‌وزیران خواهد رسید.

مادهٔ ۴ قانون جرایم رایانه ایی: هرکس به قصد دسترسی به داده‌های سری موضوع مادهٔ (۳) این قانون، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده‌میلیون (۱۰,۰۰۰,۰۰۰ ریال) تا چهل‌میلیون (۴۰,۰۰۰,۰۰۰ ریال) یا هردو مجازات محکوم خواهد شد.

مادهٔ ۵ قانون جرائم رایانه‌ای «چنانچه مأموران دولتی که مسئول حفظ داده‌های سری مقرر در مادهٔ (۳) این قانون یا سامانه‌های مربوطه هستند و به آن‌ها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آن‌ها قرارگرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند،

به حبس از یک روز تا دو سال یا جزای نقدی از پنج‌میلیون ۵,۰۰۰,۰۰۰ ریال چهل‌میلیون ۴۰,۰۰۰,۰۰۰ ریال یا هر دو مجازات و انفصال‌ازخدمت از شش ماه تا دو سال محکوم خواهند شد».

۲-۲. مواد قانون مجازات اسلامی(قانون مجازات اسلامی)

مادهٔ ۵۰۱ قانون مجازات اسلامی «هرکس نقشه‌ها یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عالماً و عامداً در اختیار افرادی که صلاحیت دسترسی به آن‌ها را ندارند قرار دهد یا از مفاد آن مطلع کند به‌نحوی‌که متضمن نوعی جاسوسی باشد، نظر به کیفیت و مراتب جرم به یک تا ده سال محکوم می‌شود».

مادهٔ ۵۰۲ قانون مجازات اسلامی «هرکس به نفع یک دولت بیگانه و به ضرر دولت بیگانه دیگر در قلمرو ایران مرتکب یکی از جرائم جاسوسی شود به‌نحوی‌که به امنیت ملی صدمه وارد نماید به یک تا پنج سال حبس محکوم خواهد شد».

مادهٔ ۵۰۳ قانون مجازات اسلامی »هرکس به قصد سرقت یا نقشه‌برداری یا کسب اطلاعات از اسرار سیاسی یا نظامی یا امنیتی به مواضع مربوطه داخل شود و همچنین اشخاصی که بدون اجازه مأمورین یا مقامات ذی‌صلاح در حال نقشه‌برداری یا گرفتن فیلم یا عکس‌برداری از استحکامات نظامی یا اماکن ممنوعه دستگیر شوند به شش ماه تا ۳ سال حبس محکوم می‌شوند».

مادهٔ ۵۰۵ قانون مجازات اسلامی «هرکس با هدف برهم زدن امنیت کشور به هر وسیله اطلاعات طبقه‌بندی‌شده را با پوشش مسئولین نظام یا مأمورین دولت یا به نحو دیگر جمع‌آوری کند چنانچه بخواهد آن را در اختیار دیگران قرار دهد و موفق به انجام آن شود به حبس از دو تا ده سال و در غیر این صورت به حبس از یک تا پنج سال محکوم می‌شود».

مادهٔ ۵۰۶ قانون مجازات اسلامی «چنانچه مأمورین دولتی که مسئول امور حفاظتی و اطلاعاتی طبقه‌بندی‌شده می‌باشند و به آن‌ها آموزش لازم داده شده است در اثر بی‌مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیه اطلاعاتی شوند به یک تا شش ماه حبس محکوم می‌شوند».

۲-۳. مواد قانون مجازات نیروهای مسلح

مادهٔ ۲۴ قانون مجازات نیروهای مسلح «افراد زیر جاسوس محسوب و به مجازات‌های ذیل محکوم می‌شوند:

الف- هر نظامی که اسناد یا اطلاعات یا اشیای دارای ارزش اطلاعاتی را در اختیار دشمن و یا بیگانه قرار دهد و این امر را برای عملیات نظامی یا نسبت به امنیت تأسیسات، استحکامات، پایگاه‌ها، کارخانجات، انبارهای دائمی یا موقتی تسلیحاتی، توقف‌گاه‌های موقت، ساختمان‌های نظامی، کشتی‌ها، هواپیماها یا وسایل نقلیه زمینی نظامی یا امنیت تأسیسات دفاعی کشور مضر باشد به مجازات محارب محکوم خواهد شد.

ب- هر نظامی که اسناد یا اطلاعات برای دشمن یا بیگانگان تحصیل کرده، به هر دلیلی موفق به تسلیم آن نشود به حبس از سه تا پانزده سال محکوم می‌گردد.

ج- هر نظامی که اسرار نظامی، سیاسی، امنیتی، اقتصادی و یا صنعتی مربوط به نیروهای مسلح را به دشمنان داخلی یا خارجی یا بیگانگان یا منابع آن تسلیم و یا آنان را از مفاد آن آگاه سازد به مجازات محارب خواهد شد.

د- هر نظامی که برای به دست آوردن اسناد یا اطلاعات طبقه‌بندی‌شده، به نفع دشمن و یا بیگانه به محل نگهداری اسناد یا اطلاعات داخل شود، چنانچه به‌موجب قوانین دیگر مستوجب مجازات شدیدتری نباشد به حبس از دو تا ده سال محکوم می‌گردد.

تبصره: هر نظامی که عالماً یا عامداً فقط به‌صورت غیرمجاز به محل مذکور وارد شود به حبس از شش ماه تا ۳ سال محکوم می‌گردد.

هـ- هر بیگانه که برای کسب اطلاعات به نفع دشمن به پایگاه‌ها، کارخانجات، انبارهای تسلیحاتی، اردوگاه‌های نظامی، یگان‌های نیروهای مسلح، توقفگاه‌های موقتی نظامی، ساختمان‌های دفاعی نظامی و وسایط نقلیه زمینی، هوایی و دریایی وارد شده یا به محل‌های

نگهداری اسناد یا اطلاعات داخل شود، به اعدام و در غیر این صورت به حبس از یک تا ده سال محکوم می‌گردد.

تبصره ۱: هرکس در جرائم جاسوسی یا نظامیان مشارکت نماید به‌تبع مجرمان اصلی نظامی در دادگاه‌های نظامی محاکمه و به همان مجازاتی که برای نظامیان مقرراست محکوم می‌شود.

تبصره ۲: معاونت در امر جاسوسی و یا مخفی نمودن و پناه دادن به جاسوس جرم محسوب و مرتکب به‌تبع مجرمان اصلی نظامی در دادگاه‌های نظامی محاکمه و در مواردی که مجازات محارب و یا اعدام است به حبس از ۳ سال تا پانزده سال محکوم می‌گردد».

مادهٔ ۲۶ قانون مجازات نیروهای مسلح: «هر نظامی که اسناد و مدارک، مذاکرات، تصمیمات یا اطلاعات طبقه‌بندی‌شده را در اختیار افرادی که صلاحیت اطلاع نسبت به آن‌ها را ندارند؛ قرار دهد یا به هر نحو آنان را از مفاد آن مطلع سازد به ترتیب ذیل محکوم می‌شود:

الف- هرگاه اسناد، مذاکرات، تصمیمات یا اطلاعات عنوان به‌کلی سری داشته باشد به حبس از سه تا پانزده سال.

ب- هرگاه اسناد، مذاکرات، تصمیمات یا اطلاع عنوان سری داشته باشد، به حبس از دوتا ده سال.

ج- هرگاه اسناد، مذاکرات، تصمیمات یا اطلاعات عنوان خیلی محرمانه داشته باشد به حبس از ۳ ماه تا یک سال.

تبصره ۱: هرگاه اسناد، مذاکرات، تصمیمات یا اطلاعات محرمانه داشته باشد، از طرف فرمانده یا رئیس مربوط تنبیه انضباطی خواهد شد».

مادهٔ ۲۷ قانون مجازات نیروهای مسلح: «هر نظامی که براثر بی‌احتیاطی یا بی‌مبالاتی یا سهل‌انگاری یا عدم رعایت نظامات دولتی موجب افشای اطلاعات و تصمیمات یا فقدان یا از بین

رفتن اسناد و مدارک مذکور در مادۀ ۲۶ قانون شود با توجه به طبقه‌بندی اسناد افشاء شده به ترتیب زیر محکوم می‌شود:

الف- چنانچه اسناد، مذاکرات، اطلاعات یا تصمیمات عنوان سری داشته باشد به حبس از ۶ ماه تا دو سال.

ب- چنانچه اسناد، مذاکرات، اطلاعات یا تصمیمات عنوان سری داشته باشد به حبس از ۳ ماه تا یک سال.

ج- چنانچه اسناد، مذاکرات، اطلاعات یا تصمیمات، عنوان محرمانه داشته باشد به حبس از دو ماه تا شش ماه.

تبصره: هرگاه اسناد و مدارک، مذاکرات، اطلاعات یا تصمیمات عنوان محرمانه داشته باشد از طرف فرمانده یا رئیس مربوط تنبیه انضباطی خواهد شد.

مادۀ ۲۸ قانون مجازات نیروهای مسلح: هر نظامی که پس از آموزش لازم در مورد حفظ اطلاعات طبقه‌بندی‌شده، در اثر بی‌مبالاتی وعدم رعایت اصول حفاظتی، توسط دشمنان و یا بیگانگان تخلیه اطلاعاتی شود، به یک تا شش ماه حبس محکوم می گردد».

۳. بررسی مواد مرتبط با جاسوسی رایانه‌ای

ابتدا به بررسی موارد موجود در مادۀ ۳ می‌پردازیم:

۳-۱. دادۀ رایانه‌ای

هر نمادی از واقعه، اطلاعات یا مفهوم به شکلی مطلوب برای پردازش دریک سیستم رایانه‌ای یا مخابراتی است که باعث می‌شود سیستم‌های ذکرشده کارکرد خود را به مرحله اجرا بگذارند.

داده محتوا: هر نمادی از موضوع‌ها، مفهوم‌ها یا دستورالعمل‌ها نظیر متن یا تصویر چه به‌صورت در جریان یا ذخیره‌شده که به‌منظور برقراری ارتباط میان سیستم‌های رایانه‌ای یا پردازش توسط رایانه.

در تعریفی ساده‌تر می‌توان گفت: داده عبارت است از مجموعه‌ای از حروف، ارقام و نشانه‌ها که به‌وسیله رایانه مورد پردازش قرار می‌گیرند.

ممکن است داده‌ها در وهلهٔ اول اساساً برای انسان قابل‌فهم نباشند اما پس از پردازش به‌وسیله رایانه، به انحاء گوناگون از قبیل صوت، فیلم، متن و...درآمده و بدین‌وسیله برای انسان مفهوم می‌یابد.

عامل‌های داده عبارت‌اند از: مجموعه‌ای گوناگون از وسایل ذخیره‌سازی اطلاعات که قابل‌حمل‌اند و می‌توان به‌سادگی آن‌ها را زا یک رایانه به رایانه دیگر منتقل کرد، مانند دیسک نرم، دیسک سخت، این حامل‌ها هریک ظرفیت‌های متعددی برای ذخیره‌سازی اطلاعات دارند. برای سنجش این ظرفیت معمولاً از اصطلاحاتی مثل مگابایت استفاده می‌شود که هرچه بالاتر باشد اطلاعات بیشتری را می‌توان روی آن ذخیره کرد (سالمی‌فیه، ۱۳۸۶: ۴۲).

۳-۲. بررسی مادهٔ ۳ قانون جرائم رایانه‌ای

۳-۲-۱. بررسی عنصر مادی بند الف مادهٔ ۳ قانون جرائم رایانه‌ای

دربند الف مادهٔ ۳ عمل مجرمانه عبارت‌اند از:

۱- دسترسی به داده‌های سری،

۲- تحصیل داده‌های سری،

۳- شنود محتوای سری در حال انتقال.

برای روشن شدن مفاد این بند توجه به این مطلب لازم است که جاسوسی در معنی وسیع کلمه، دو دسته اقدامات را شامل می‌شود:

دسته اول: اقدامات قانونی که عبارت است از تفحص و تحصیل اطلاعات مزبور و دادن آن به کسانی که باید از آن بهره‌برداری کند. این دسته، ممکن است متضمن قصد جاسوسی یا خیانت نباشد، مثلاً متهم صرفاً ازلحاظ کنجکاوی یا میل به دانستن یا این‌که برحسب غفلت، افراد مملکت

خود را آگاه سازد نه خارجیان را؛ اما دسته دوم همیشه کاشف از وجود اراده خاص برای آگاه کردن عوامل غیرمجاز وغیرصلاحیت‌دار است (گلدوزیان، ۱۳۸۲: ۴۷۶).

دسترسی ازنظر لغوی عبارت است از قدرت، توانایی، قدرت دست یافتن به چیزی لذا با توجه به این معنی، فردی که دسترسی غیرمجاز به داده‌های سری پیدا کند، خود رأساً این کار را انجام می‌دهد و تفاوت آن با تحصیل داده‌های سری آن است که تحصیل از طریق یک فرد دیگر می‌تواند انجام شود در فرهنگ فارسی واژه تحصیل یعنی به دست آوردن، کسب کردن، پس اگر تحصیل داده‌های سری منظور باشد، می‌توان آن را از طریق فرضاً یک مسئول دریک اداره دولتی یا یک مرکز نظامی کسب کرد.

۳-۲-۲. بررسی عنصر روانی بند الف مادۀ ۳ قانون جرائم رایانه‌ای

عنصر روانی جرم بند الف علاوه بر عمد در دسترسی، تحصیل و یا شنود محتوای سری عبارت‌اند از آگاهی و علم به غیرمجاز و بدون مجوز بودن دسترسی یا تحصیل و یا شنود داده‌های سری.

پ) بررسی عنصر مادی بند ب مادۀ ۳: با توجه به صراحت و تأکید این بند بر «دسترس قرار دادن داده‌های مذکور» منطقاً به نظر می‌رسد که این داده‌ها اعم از فیلم، عکس، متن و... باید به‌طور مستقیم در اختیار فرد فاقد صلاحیت قرار گیرد. پس اگر مفاد این داده‌ها در اختیار فردی قرار گیرد طبق این ماده جرم نیست زیرا اگر قانون‌گذار نظر در دسترس قرار دادن مفاد داده‌ها را جرم می‌دانست مانند مادۀ ۵۰۱ قانون مجازات اسلامی از واژۀ «مفاد» در این ماده نیز استفاده می‌کرد؛ اما با درنظرگرفتن سری هستند و از اهمیت بالایی برخوردار هستند پس عقلا تفاوتی بین خود داده‌های سری و مفاد آن‌ها وجود ندارد. به‌هرروی بهتر بود قانون‌گذار برای جلوگیری از بروز این دست ابهام‌ها کلمه مفاد را نیز به همان ترتیبی که گفته شد به این بند اضافه می‌کرد (میرمحمدصادقی، ۱۳۸۱: ۸۵).

۳-۲-۳. بررسی عنصر روانی بند ب مادهٔ ۳ قانون جرائم رایانه‌ای

عنصر روانی این جرم عبارت است از: در دسترس قرار دادن داده‌های سری به‌صورت عمدی ازاین‌رو اگر فرد در حالت مستی، بی‌هوشی، خواب، اجبار، اکراه و نظایر این‌ها مرتکب شود مجازات نخواهد شد و جرم محقق نمی‌گردد (میرمحمدصادقی، ۱۳۸۱: ۸۶).

۳-۲-٤. بررسی عنصر مادی بند ج مادهٔ ۳ قانون جرائم رایانه‌ای

به نظر می‌رسد تفاوت (افشا) با «در دسترس قرار دادن» این است که زمانی عمل فرد «افشا» تلقی می‌شود که فرد رأساً داده‌های سری را در اختیار افراد مذکور بگذارد لیکن ماهیت «در دسترس قرار دادن» زمانی جرم است که وی به نحوی از انحاء موجبات دسترسی افراد مذکور را به داده‌های سری فراهم کند، بدون آن‌که داده‌ها به‌طور مستقیم از طرف خود وی به آن‌ها ارائه شود. در خصوص واژه «بیگانه» که معمولاً به خارجیان اطلاق می‌شود، پرواضح است که استعمال آن به‌عنوان صفت دولت، سازمان، شرکت و یا حتی گروه ابهامی ایجاد نمی‌کند و شامل هر دولت، سازمان، شرکت و یا گروهی می‌شود و این تردید ایجاد می‌شود که لزوماً باید یک فرد خارجی و غیرایرانی باشد؟ برای پاسخ به این نکته باید توجه کرد که دولت‌ها برای جاسوسی از یکدیگر به‌صورت کاملاً پنهانی عمل می‌کنند؛ بنابراین اگر دولتی برای به دست آوردن اطلاعات موردنیاز خود دست به استخدام عوامل ایرانی بزند با توجه به فرایند پیچیده جاسوسی و پنهان‌کاری‌های مختص آن به نظر می‌رسد که اگر عامل بیگانه هم یک فرد ایرانی باشد این ماده بر آن صدق می‌کند. ابهام دیگر در واژه «گروه بیگانه» است در ادبیات حقوقی، برای واژه‌های دولت، سازمان و شرکت تعاریف تقریباً مشخص وجود دارد اما منظور از گروه چیست؟ آیا یک گروه جهانگردی را که جهت تفریح به ایران آمده نیز شامل می‌شود؟ یا توجه به حساسیت قانون‌گذار نسبت به حفظ داده‌های سری و این‌که افشای آن‌ها را موجب لطمه به امنیت ملی دانسته است، چنین استنباط می‌شود که به هر صورت هر جا که عنوان گروه بر اجتماع صدق کند اگر داده‌های سری در

دسترس آن‌ها قرار گیرد یا فاش شود، عمل فرد مشمول این بند خواهد بود و لزوماً نیاز نیست که این گروه یک گروه سازمان‌یافته و دارای تشکیلات باشد.

۳-۲-۵. بررسی عنصر روانی بند ج مادهٔ ۳ قانون جرائم رایانه‌ای

عنصر روانی مرتکب این بند علاوه بر عمد در افشا یا در دسترس قرار دادن داده‌های سری، علم و آگاهی نسبت به بیگانه بودن طرف مقابل است (میرمحمدصادقی، ۱۳۸۱: ۸۶).

۳-۲-٦. داده‌های سری

در تبصره ۱ مادهٔ ۳ داده‌های سری تعریف شده است: «داده‌های سری، داده‌هایی است که افشای آن‌ها به امنیت کشور یا منافع ملی لطمه می‌زند.» تفاوت بین داده‌های سری و به‌کلی سری این است که گروه دوم موجب ضرر و زیان جبران‌ناپذیر به امنیت ملی کشور می‌شود. ولی افشای داده‌های اول صرفاً به امنیت کشور ضرر می‌زند و این جای انتقاد است که چرا با وجود این‌که داده‌های به‌کلی سری از داده‌های سری اهمیت بیشتری دارد ولی در این ماده قید شده است؛ اما دلیل پیش‌بینی داده‌های سری بیرون کردن داده‌های محرمانه از تنگنای پشتیبانی کیفری است؛ زیرا گستره داده‌های محرمانه به اندازه‌ای است که می‌توان هر اطلاعاتی را به‌عنوان زیرمجموعه آن قرارداد بنابراین در قانون به داده‌های سری بسنده شده است.

نمونه‌هایی از داده‌های به‌کلی سری:

۱- طرح‌های راهبردی که در آن اداره و هدایت جنگ معلوم باشد.

۲- آمار و اطلاعات مربوط به مقادیر ذخایر تسلیحات، مهمات و تجهیزات راهبردی.

۳- اطلاعات مربوط به پیشرفت‌ها و توانایی عملیاتی سازمان اطلاعاتی کشور (آئین‌نامه حفاظت از اسناد و مدارک طبقه‌بندی‌شده نیروهای مسلح، سال ۷۵)

همچنین موارد ذیل نیز می‌تواند مصداق اطلاعات و داده‌های سری باشد:

۱- آمار و استعداد هریک از نیروهای سه‌گانه ارتش، پنج‌گانه سپاه، وزارت دفاع و نیروی انتظامی.

۲- اطلاعات مربوط به طرح‌های حفاظت از محموله‌های راهبردی.

۳- نیازمندی‌های ضروری نیروهای مسلح به اقلام راهبردی و حساس و دفاعی.

۴- طرح‌های تحقیقاتی راهبردی (آئین‌نامه حفاظت از اسناد و مدارک طبقه‌بندی‌شده نیروهای مسلح، سال ۷۵)

۳-۳. نقض تدابیر امنیتی سامانه‌های رایانه‌ای (موضوع مادهٔ ٤ قانون جرائم رایانه‌ای)

۳-۳-۱. بررسی عنصر مادهٔ ٤ قانون جرائم رایانه‌ای

در این قانون تعریفی از تدابیر امنیتی که شاکله عنصر مادی این جرم را تشکیل می‌دهد ارائه نشده است؛ اما در لایحهٔ تقدیمی دولت این اصطلاح تحت عنوان تدابیر حفاظتی مورد تعریف قرارگرفته است. درواقع این تدابیر حفاظتی متناسب با نوع و اهمیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی به‌منظور جلوگیری از دسترسی به آن‌ها بدون مجوز مرجع قانونی.

۳-۳-۲. بررسی عنصر روانی مادهٔ ٤ قانون جرائم رایانه‌ای

عنصر روانی این جرم علاوه بر عمد در نقض تدابیر امنیتی سامانه‌های رایانه‌ای مخابراتی، شامل مسئولیت خاص «دسترسی به داده‌های سری» نیز می‌شود؛ بنابراین اگر کسی صرفاً تدابیر امنیتی رایانه‌ای یا مخابراتی را نقض کند و قصد و سوءنیت خاص دسترسی به داده‌های سری را نداشته باشد شامل این ماده نیست. همچنین موفقیت در دسترسی به داده‌های مذکور ملاک نیست و از این بابت جرم مقید نیست.

۳-٤. بی‌احتیاطی و بی‌مبالاتی در حفظ داده‌های سری (موضوع مادۀ ۵)

جاسوسی اصولاً جرم عمدی تلقی می‌شود به این نحو که مرتکب با سوءنیت اطلاعات طبقه‌بندی‌شده را در اختیار بیگانگان و عوامل غیرمجاز قرار می‌دهد، اما عنایت به این‌که جرم جاسوسی از اهمیت بالا و ویژه‌ای برخوردار است. لذا قانون‌گذار را وادار به جرم‌انگاری برای این‌گونه سهل‌انگاری‌ها و بی‌مبالاتی‌ها نموده است (میرمحمدصادقی، ۱۳۸۶: ۱۰۱).

۳-٤-۱. بررسی عنصر مادۀ ۵ قانون جرائم رایانه‌ای

برای تحقق جرم موضوع این ماده وجود پاره‌ای شرایط عمومی که در خصوص مادۀ ۵۰۶ قانون مجازات اسلامی نیز وجود دارد، ضروری است. اولاً: ارتکاب این جرم به‌وسیله مأموران دولتی که دارای رابطه استخدامی اعم از رسمی، پیمانی، روزمزد، خرید خدمت و... باشد پیش‌بینی شده است. ثانیاً: مأموران باید مسئول حفظ داده‌های سری و سامانه‌های مذکور باشند، به‌عبارت‌دیگر شغل دولتی آن‌ها با داده‌های سری مرتبط باشد. ثالثاً: آموزش لازم در خصوص حفظ داده‌های سری و سامانه‌های مزبور به این مأموران داده شده باشد. چنانچه فرد این آموزش‌ها را طی نکرده باشد عمل وی مشمول این ماده نیست.

۳-٤-۲. بررسی عنصر روانی مادۀ ۵ قانون جرائم رایانه‌ای

عنصر روانی این جرم خطایی جزایی (بی‌احتیاطی، بی‌مبالاتی، عدم رعایت تدابیر امنیتی) است، البته در این ماده «عدم رعایت تدابیر امنیتی» جایگزین «عدم رعایت نظامات دولتی» شده است. بی‌احتیاطی یعنی فرد عملی انجام بدهد که نباید انجام می‌داد. بی‌مبالاتی یعنی فرد عملی که باید انجام می‌داد انجام ندهد. عدم رعایت تدابیر امنیتی یعنی فرد یک هشدار امنیتی، توصیه و یا دستورالعمل اداری را که باید رعایت می‌کرد رعایت نکرده است.

نتیجه‌گیری

در بررسی جاسوسی رایانه‌ای در مجموع به نکاتی دست یافتیم؛ اول این‌که در خصوص جاسوسی رایانه‌ای تعریف روشنی در دست نداریم و به‌جاست که متخصصین کامپیوتر و حقوق‌دانان به‌اتفاق، تعریفی جامع‌ومانع ارائه دهند که بتواند راهگشای مشکلات جرم‌انگاری باشد. دوم این‌که با تمام تلاش‌های کشورها به‌ویژه ایران در خصوص جرم مذکور در زمینه جرم‌انگاری و برخورد قانونی باز هم نقایص بسیاری در قوانین تصویب‌شده موجود است. علی‌الخصوص اشاره به سازمان‌های بین‌المللی در این مورد بسیار به‌جاست. به‌طور مثال سازمان همکاری و توسعهٔ اقتصادی، عنوان جاسوسی رایانه‌ای را به‌طور صریح در جرائم احصاشده نیاورده است و شورای اروپا در فهرست حداقل خود توجهی خاص به این رفتار مجرمانه حائز اهمیت لحاظ نکرده است همچنین سازمان ملل رفتار مشابهی در این زمینه از خود ارائه داده است. بنابراین شایسته است سازمان‌های بین‌المللی با بررسی مجدد و دقیق‌تری در خصوص جرائم رایانه‌ای، جاسوسی رایانه‌ای را موردتوجه خاص قرار داده و توجه سایر کشورها در حوزه بین‌الملل را به این بزه جلب کنند تا عکس‌العمل آن‌ها سدی باشد محکم برای جلوگیری از گسترش روزافزون این تهدید نوین در جامعهٔ جهانی.

قانون‌گذار کشورمان هم بی‌توجه به تمامی نقایص پیش‌گفته در قانون جرائم رایانه‌ای، اصلاحیهٔ جدیدی در این خصوص ارائه نداده است. در ضمن قانون‌گذار محترم در خصوص جاسوسی رایانه‌ای اقتصادی جرم‌انگاری صریحی نکرده و به قانون تجارت الکترونیکی بسنده کرده است. پس لازم است که مسئولین با توجهی ویژه به قانون جرائم رایانه‌ای درصدد رفع اشکالات موجود برآیند به‌طور مثال:

۱. در خصوص مجازات نقدی گفته‌شده در پاره‌ای از مواد برای جاسوسی رایانه‌ای، نظر به اهمیت بالای این جرم تبدیل مجازات نقدی به مجازات مناسب دیگر سبب تناسب جرم و مجازات می‌شود و این با اصل مهم تناسب جرم و مجازات سازگاری خواهد داشت.

۲. در مادهٔ ۳ قانون جرائم رایانه‌ای شاهد اصلاحاتی بودیم که تعریفی از آن‌ها در قانون ذکر نشده بود مثلاً واژگان «تدابیر حفاظتی»، «بیگانه»، «افشاء اطلاعات» و... بنابراین ارائه تعریف صریح در خصوص این واژگان مسلماً گره‌گشای بسیاری از ابهامات خواهد بود.

۳. در فصل هشتم از قانون جرائم رایانه‌ای شاهد بحث تشدید مجازات هستیم؛ اما این قانون در خصوص تشدید مجازات برای تکرار جرم با در نظر گرفتن مجازات خفیف‌تر در مادهٔ ۲۷ نه‌تنها از اهمیت این بحث می‌کاهد بلکه عقل سلیم هم مجازاتی سخت‌تر را برای تکرار جرم جاسوسی رایانه‌ای مناسب می‌داند درنتیجه رفع این اشکال از دید نگارنده می‌تواند یکی از نکات حائز اهمیت در بحث رفع نقص قانون جرائم رایانه‌ای باشد.

۴. همان‌طور که در بحث همکاری در ارتکاب جرم گفتیم قانون‌گذار در قانون جرائم رایانه‌ای در خصوص مجازات شریک ساکت بوده و برای معاونت در جرم هم فقط در مادهٔ ۲۵ به‌طور ضمنی اشاراتی کرده است پس شایسته است نظر به اهمیت جرم به‌صورت صریح در خصوص معاون و شریک در این بزه صحبت کرده و رفتار مجرمانه آن‌ها را جرم‌انگاری نماید.

۵. قانون‌گذار در بخش دوم از قانون جرائم رایانه‌ای به‌صورت آشکار دادگاه‌های صالح به رسیدگی در این جرم را معرفی نکرده است و در مادهٔ ۲۸ به‌صورت کلی به دادگاه‌های ایران و در مادهٔ ۳۰ به دادگاه‌های عمومی و اختصاصی اشاره کرده است، خاصه آن‌که برای رسیدگی به رفتار مجرمانه جاسوسی رایانه‌ای اقتصادی در قانون تجارت الکترونیکی هیچ دادگاه خاصی را مدنظر قرار نداده است، حتی اشاره‌ای ضمنی هم مورد دادگاه صالح به رسیدگی در این مورد نکرده است، بنابراین رفع این نقص مسلماً ازجمله نکاتی است که باید هرچه سریع‌تر به آن توجه شود.

در ادامه با توجه به تبصره مادهٔ ۳۰ قانون جرائم رایانه‌ای که قوه قضائیه را مکلف کرده تا قضاتی را که با امور رایانه آشنایی دارند برای رسیدگی به این جرائم انتخاب کند و عنایت به این

مطلب که پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر ضرورت آموزش‌های بیش‌ازپیش را مشخص می‌سازد و برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرائم رایانه‌ای به‌خصوص جاسوسی رایانه‌ای، این آموزش‌ها باید در مقاطع مختلف زمانی تکرار و روزآمد شوند، بنابراین:

۱. ازآنجاکه پلیس به‌عنوان ضابط دادگستری وظیفه کشف جرائم را به عهده دارد، در کنار آموزش قضات و سایر مقامات قضایی، آموزش پلیس نیز باید در سرفصل برنامه‌ریزی‌ها قرار گیرد.
۲. آموزش عمومی در سطح کارمندان دولت و نظامیان برای جلوگیری از بی‌احتیاطی، بی‌مبالاتی این افراد در خصوص داده‌های سری.

در حال حاضر دولتمردان کشورمان برای جلوگیری از جاسوسی رایانه‌ای، داده‌های سری، تمهیدات خاصی را در نظر گرفته‌اند. ازجمله این روش‌ها و طرح‌های مناسب برای برخورد و مبارزه با حملات برنامه‌ریزی‌شده هکری و سایبری گروه‌های جاسوسی کشورهای بیگانه، استفاده از شبکه اینترنت ملی و سیستم‌عامل طراحی‌شده توسط مهندسان مبتکر کشورمان خواهد بود، زیرا با توجه به امکان سوءاستفاده کشورهای سازنده سیستم‌های عامل موجود نظیر ویندوز[1] و مکینتاش[2] از اطلاعات شخصی کاربران و محرمانهٔ رایانه‌های دولتی، این روش‌ها احتمالاً تا حد زیادی کارآمد خواهد بود و در آینده‌ای نزدیک از این برنامه‌ها در جهت دفاع و حفاظت از امنیت ملی بهره‌برداری خواهد شد؛ اما نظر به این‌که هنوز زمینه استفاده از این تمهیدات ویژه فراهم نشده است، جهت پیشگیری هرچه بیشتر از وقوع جاسوسی رایانه‌ای ارائه راهکارهای زیر را ضروری می‌دانم:

۱. عدم ذخیره‌سازی داده‌های سری و اطلاعات طبقه‌بندی‌شده در شبکه‌های رایانه‌ای به‌خصوص شبکه جهانی اینترنت (تا حد ممکن).

---

1. Windows
2. Macintash

۲. مسدود کردن درگاه‌های رایانه‌های حساس در ادارات به‌عنوان راهکاری سریع و کم‌هزینه درعین‌حال مؤثر: در این روش تمامی درگاه‌های سیستم‌های رایانه‌ای از قبیل درایوهای سی دی[۱] و دی وی دی[۲]، پورت‌های یو اس بی[۳] و... از طریق سرور (شبکه) بسته شده، به‌این‌ترتیب کاربر رایانه نمی‌تواند هیچ داده و اطلاعاتی را وارد رایانه کرده و یا از آن خارج کند. در این حالت کاربر تنها به داده‌های مجاز که از سوی مسئولان و به‌منظور انجام‌وظیفه روی سیستم او قرار داده شده، دسترسی خواهد داشت.

۳. فرهنگ‌سازی: بستر فرهنگی جامعه باید به‌گونه‌ای هدایت شود که هر کاربری بداند چگونه از رایانه و اینترنت استفاده کند تا اطلاعات ذی‌قیمت او حفظ شود. همچنین با توجه به گستردگی فضای مجازی اینترنت، آموزش جنبه‌های مختلف آن ازجمله کاربردها، آفت‌ها و سایر خطرها ضروری است. توجه به برخی نکات ساده مثل فاش نکردن گذرواژه‌های رایانه‌ای از الزامات است.

۴. تدابیر محدودکننده یا سلب‌کنندهٔ دسترسی: این دسته از تدابیر در زمره مهم‌ترین تدابیر پیشگیرانه وضعی از جرائم سایبر قرار دارند. در این روش با نصب برنامه‌های خاص روی رایانه‌های شخصی، سیستم‌های ارائه‌دهنده خدمات شبکه‌ای از ورود یا ارسال برخی داده‌های غیرمجاز یا غیرقانونی جلوگیری می‌کنند این برنامه‌ها معمولاً در سه قالب دیوارهای آتشین[۴]، فیلترها[۵] و پراکسی‌ها[۶] هستند. این برنامه‌ها فهرستی از موضوعات مجاز یا غیرمجاز دارند و از ورودی‌ها و خروجی‌های غیرمجاز جلوگیری می‌کنند.

۵. استفاده از تدابیر نظارتی: این اقدامات از دو بعد فنی و انسانی تشکیل شده است. در حالت فنی برنامه‌هایی روی سیستم نصب می‌شود و تمامی فعالیت‌های شبکه‌ای اشخاص، حتی

---

1. CD
2. DVD
3. USB
4. Fire wall
5. filtering
6. proxy

ضرباتی که بر روی صفحه‌کلیدشان زده‌اند یا نقاطی را که به‌وسیله موشواره (موس) روی آن کلیک کرده‌اند، ضبط می‌کنند و سپس مأمور موردنظر (بعد انسانی) می‌تواند با بررسی سوابق، موارد غیرقانونی را پیشگیری و گزارش کند.

۶. نصب تدابیر صدور مجوز: در این روش از ورود اشخاص ناشناس یا فاقد اعتبار به یک سیستم رایانه‌ای یا سایت جلوگیری می‌شود. نمونه ساده این اقدام به‌کارگیری گذرواژه است که از دیرباز متداول بوده است. به‌این‌ترتیب تنها کسانی حق بهره‌برداری از یک سیستم یا سایت را خواهند داشت که پس از طی مراحل شناسایی و کسب اعتبار گذرواژه مربوطه را دریافت کنند.

۷. استفاده از ابزارهای رمزکننده: برنامه‌هایی هستند که به‌منظور انتقال ایمن محتوای ارتباطات رایانه‌ای استفاده می‌شوند. در این روش بر اساس کدهای خاص، متن اصلی به «رمزنوشته»[1] تبدیل می‌شود و گیرنده در مقصد به‌وسیلهٔ کلیدی که در اختیار دارد، آن را «رمزگشایی»[2] می‌کند. مزیت این روش در این است که با توجه به برنامه‌های متعددی که در فضای سایبر برای شنود و دستیابی به ارتباطات افراد وجود دارد بهره‌گیری از برنامه‌های رمزنگاری می‌تواند خطر این‌گونه تعرض‌ها را کاهش دهد.

1. ciphertext
2. Decryption

منابع و مآخذ

الف- فارسی

۱. دینداری، مرتضی (۱۳۸۹)، *مسئولیت کیفری اشخاص حقوقی در جرائم رایانه‌ای*، دانشگاه علامه طباطبایی، دانشکده حقوق، بهار.

۲. زندی، محمدرضا (۱۳۸۹)، *تحقیقات مقدماتی در جرائم سایبری*، انتشارات جنگل.

۳. زیبر، اولریش (۱۳۹۰)، *جرائم رایانه‌ای*، ترجمه محمدعلی نوری، گنج دانش.

۴. سالمی‌فیه، کیوان (۱۳۸۶)، *مبانی فن‌آوری و اطلاعات*، انتشارات انستیتو ایزایران.

۵. گلدوزیان، ایرج، (۱۳۸۲)، *محشای قانون مجازات اسلامی*، انتشارات مجد.

۶. معین، محمد (۱۳۷۶)، *فرهنگ فارسی*، انتشارات امیرکبیر، دورهٔ ۶جلدی.

۷. میرمحمدصادقی، حسین (۱۳۸۱)، *جرائم علیه امنیت و آسایش عمومی*، نشر میزان.

ب- لاتین

1. Morris. Sheridan. *the future of net crime now.* part1. thetas and challenges. home office online report. 2004. p.16.

ج- قوانین

۱. قانون مجازات اسلامی کتاب تعزیرات مصوب ۱۳۷۵.

۲. قانون جرائم رایانه‌ای مصوب ۱۳۸۸.

۳. آئین‌نامه حفاظت از اسناد و مدارک طبقه‌بندی‌شده نیروهای مسلح، مصوب ۱۳۷۵.