فصلنامه حقوق، مجلهٔ دانشکده حقوق و علوم سیاسی، دوره ۴۲، شمارهٔ ۳، پاییز ۱۳۹۱، صفحات ۱۹۵ - ۱۷۷

جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین المللی آن

محسن رهامی*
دانشیار گروه حقوق جزا و جرم شناسی دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران
سیروس پرویزی
کارشناس ارشد رشته حقوق جزا و جرم‌شناسی دانشگاه تهران
(تاریخ دریافت: ۱۳۸۹/۸/۳ - تاریخ تصویب: ۱۳۹۱/۳/۷)

چکیده:
جاسوسی رایانه‌ای جرمی است که در آن رایانه به منزلهٔ موضوع جرم، جزء رکن مادی این جرم است. این جرم از جرایمی است که ارتکاب آن قبل از پیدایش رایانه امکان‌پذیر نبوده است؛ به همین خاطر اکثر کشورها اخیراً اقدام به تصویب مقرراتی در این باره کرده اند. در حقوق داخلی ایران نیز اقداماتی نظیر دسترسی غیرمجاز به داده‌های محرمانه که افشای آنها باعث لطمه به امنیت کشور و منافع ملی شود؛ با عنوان جاسوسی رایانه‌ای جرم انگاری شده است. مقاله حاضر حول این موضوع بحث و بررسی کرده است که منظور از جاسوسی رایانه‌ای چیست و نیز نقش و اهمیت رایانه در وقوع جاسوسی رایانه‌ای و اعمالی که مشمول جرم جاسوسی رایانه‌ای می‌شود.

واژگان کلیدی:
جرایم رایانه‌ای، جاسوسی رایانه‌ای، داده های محرمانه، دسترسی غیرمجاز، شنود غیرمجاز، تدابیرامنیتی.

* مسئول مقاله فاکس: ٦٦٤٠٩٥٩٥ Email:mrahami@ut.ac.ir
از این نویسنده مقاله زیر نیز در همین مجله منتشر شده است:
«بررسی نظریه‌های راجع به عناصر جرم با نگاهی به اساسنامه دیوان کیفری بین‌المللی»، سال ۱۳۸۹، شماره ۷.

مقدمه

رایانه با طرح مسایل جدید همه علوم از جمله علوم کیفری را تحت تاثیر قرارداده است. زیرا رایانه نه تنها امکان ارتکاب بسیاری از رفتارهای مجرمانه سنتی را تسهیل کرده؛ بلکه امکان ارتکاب رفتارهای مجرمانه جدید را به وجود آورده که قبل از این به هیچ وجه امکانپذیر نبوده است. از جمله این جرایم، جاسوسی رایانه‌ای است که دارای عناصر تشکیل دهنده جرم، متفاوت از جرم جاسوسی سنتی است. جاسوسی رایانه‌ای ازجمله جرایمی است که با پیدایش فناوری اطلاعات وارد عرصه حقوق کیفری شده است واصول و قواعد حاکم بر جاسوسی سنتی رابه چالش کشیده است. در این مقاله سعی می‌شود با بررسی قوانین حقوق داخلی، کنوانسیون های مربوط و حقوق برخی کشورهای خارجی، ارکان و عناصر تشکیل دهنده این جرم و تفاوت های آن با جاسوسی سنتی بررسی شود.

۱- تعریف جاسوسی رایانه ای

۱-۱- تعریف جرایم رایانه ای

از آنجا که همواره از جرم جاسوسی رایانه‌ای به عنوان یکی از زیرمجموعه‌های جرایم رایانه‌ای در متون حقوقی بحث شده؛ معمولاً به تعریف جرم رایانه‌ای اکتفا و تعریفی خاص از جاسوسی رایانه‌ای به عمل نیامده است. در قانون جرایم رایانه‌ای نیز که در ۵ خرداد ۱۳۸۸ به تصویب رسید و به قانون مجازات اسلامی ملحق شد؛ تعریفی از جاسوسی رایانه‌ای نشده و فقط به تعیین اعمال خاص مجرمانه در زیر عنوان جاسوسی رایانه‌ای و تعیین مجازات برای آنها اقدام کرده است.

برای دستیابی به تعریف صحیح از جاسوسی رایانه‌ای باید ابتدا بررسی شود که اصولاً چه نوع جرمی جزء جرایم رایانه‌ای است و جرم رایانه‌ای چه خصوصیتی دارد تا بتوان تعریفی دقیق تر از جاسوسی رایانه‌ای ارائه داد. بنابراین، ابتدا به تعریف جرم رایانه‌ای پرداخته می‌شود.

طبق تعریف ارائه شده از سوی گروهی از کارشناسان که به دعوت سازمان همکاری و توسعه اقتصادی(OECD[1]) در پاریس در ۱۹۸۳ گرد آمده بودند؛ جرم رایانه‌ای را به این صورت تعریف کرده‌اند: «هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار و یا انتقال داده‌ها جرم رایانه‌ای است». پروفسور زیبر اولریش از محققین مطرح در عرصه جرایم رایانه‌ای این تعریف را از این حیث سودمند دانسته است که امکان استفاده از فرضیات مختلف و همهٔ مطالعات جرم‌شناسی، کیفری، اقتصادی پیشگرانه یا حقوقی را فراهم می‌کند (اولریش، ۱۳۸۳: ۱۸).

1-OECD: organization for Economic co-operation and Development.

در ایالات متحده آمریکا تعریفی وسیع از جرم رایانه‌ای شده مبنی بر آنکه «هر اقدام غیرقانونی را که با رایانه یا کاربرد آن مرتبط باشد، جرم رایانه‌ای می‌گویند(عمیدی، ۸۷: ۲۰).

اما طیف گسترده افعال مجرمانه که ذیل جرایم رایانه‌ای وجود دارند و ماهیت متغیر آنها که ناشی از پیشرفت لحظه به لحظهٔ فناوری اطلاعات و شیوه‌های سوءاستفاده از آن است؛ ارائه تعریف جامع و مانع از آن را مشکل و چه بسا غیرممکن می‌سازد؛ تا آنجا که در جدیدترین و جامع‌ترین سند بین‌المللی موجود در این عرصه یعنی کنوانسیون جرایم سایبر ۲۰۰۱ بوداپست تعریفی از این جرایم به عمل نیامده است. سازمان ملل متحد نیز در نشریهٔ بین‌المللی سیاست جنایی خود، بر عدم وجود تعریف مورد توافق به این عرصه تأکید کرده است(باستانی،۱۳۸۳: ۱۷).

جهت دستیابی به تعریف دقیق تر از جرایم رایانه‌ای می‌توان بطور کلی جرایم رایانه‌ای را به دو دسته تقسیم بندی کرد:جرایم رایانه‌ای سنتی و جرایم رایانه‌ای مدرن. جرایم رایانه‌ای سنتی (موضوع ماده ۷۸۰ قانون مجازات اسلامی)، جرایمی هستند که با همان شرایط قانونی و از راه های مرسوم ارتکاب می‌یابند و استفاده از رایانه تغییری در ماهیت این نوع جرایم نمی‌دهد. بنابراین، این گونه جرایم به وسیله رایانه نیز ارتکاب می‌یابند مانند توهین به فردی که از طریق پست الکترونیک انجام شده باشد یا تخریب عمدی تجهیزات رایانه‌ای که قانونگذار ارتکاب بوسیله رایانه را به عنوان جزئی از اجزاء عنصر مادی آنها ذکر نکرده باشد. در واقع از لحاظ قانونی وسیله ارتکاب جرم،جزئی از اجزاء عنصر مادی این جرم نیست و نوع وسیله ارتکاب جرم، تاثیری در تحقق جرائم مزبور ندارد(خرم آبادی،۱۳۹۰: ۳۰).

امّا جرایم رایانه‌ای مدرن، جرایمی هستند که پس از پیدایش رایانه به وجود آمده‌اند و با پیشرفت رایانه تحوّل پیدا کرده‌اند که به موجب قانون، رایانه به عنوان موضوع و یا ابزار جرم و جزئی از اجزاء تشکیل دهنده عنصر مادی آن را تشکیل می‌دهد. در واقع این‌گونه جرایم که می‌توان از آن به عنوان جرایم رایانه‌ای محض یاد کرد اصولاً بدون تصریح قانونگذار نمی‌توان مرتکب را مسئول شناخت. از این دیدگاه جرم رایانه ای صرفاً شامل آن دسته از اعمال مجرمانه مرتبط با فناوری اطلاعات می‌شود که قبل از پیدایش رایانه و سایر ارکان فناوری اطلاعات، ارتکاب آنها به هیچ وجه امکان پذیر نبوده است.

۱-۲- تعریف جاسوسی رایانه ای

برای ارائه تعریفی کامل از جاسوسی رایانه‌ای ابتدا بهتر است که تعریفی از جاسوس و جاسوسی سنتی به عمل آوریم و سپس تفاوت‌های جاسوسی سنتی را با جاسوسی رایانه‌ای مورد بررسی قرار دهیم. در فرهنگ معین جاسوسی این گونه بیان شده «جاسوسی آن است که اخبار و اطلاعات کسی یا مؤسسه‌ای و یا کشوری را مخفیانه گردآورد و به شخص یا مؤسسه

و یا کشوری دهد»(معین، ۱۳۸٦: ٤۹۹). دکتر جعفر لنگرودی در تعریف جاسوسی می‌نویسد: «در اصطلاح حقوقی عمل کسی که به صورت مخفیانه یا تحت عناوین نادرست به نفع خصم برای تحصیل اطلاعات یا جمع‌آوری اشیایی صورت می‌گیرد، جاسوسی می‌گویند»(جعفری لنگرودی،۱۳۷۲: ۱۸۹).

در تعریفی دیگر«جاسوس به شخصی اطلاق می‌شود که در پوشش متقلبانه یا مخفیانه وبه نفع دشمن در صدد تفحص در باره اسرار یا تحصیل اطلاعات یا اشیاء یا سایر مدارک و اسناد مربوط به استعداد و توانایی های نظامی، اقتصادی و فرهنگی مربوط به یک کشور دشمن باشد»(ولیدی، ۷۱، ج ۳: ۱۱۲). در تعریف های مزبور تحصیل غیرمجاز اطلاعات جهت ارایه به اشخاص فاقد لاحیت از عناصر جاسوسی دانسته شده است.

با توجه به فصل جرایم رایانه‌ای که جرایمی را در بر می‌گیرد که با سوءاستفاده از سامانه رایانه‌ای برخلاف قانون ارتکاب می‌یابند، می‌توان در تعریف جرم مزبور چنین گفت که جاسوسی رایانه‌ای جرمی است که در آن در عمل رایانه به منزلهٔ موضوع جرم جزء رکن مادی اعلام شده است. به عبارت دیگر، درجاسوسی رایانه‌ای داده ها و اطلاعات یا به عبارتی موضوع جرم در مرحله مقدماتی انجام جرم دارای پایه و قالب مادی نیست که قابل لمس باشند و دارای وجودخارجی نبوده و صرفاً در فضای سایبر وجود دارند؛ بدون اینکه بصورت خارجی مثل سی دی(CD) درامده باشند.

با توجه به اینکه جرم جاسوسی سنتی و جاسوسی رایانه‌ای سنتی دارای عنصر مادی یکسان هستند قانونگذار هم در هنگام وضع مادهٔ ۷۸۰ قانون مجازات اسلامی به این موضوع توجه داشته است. در ماده مزبور مقرر شده: «در مواردی که سیستم رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم به‌کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قوانین جزایی مربوط عمل خواهد شد». در واقع، از عبارت قانونگذار می‌توان چنین استنباط کرد که چون اصولاً در جرایمی که رایانه به عنوان وسیله‌ای در جهت ارتکاب به آن جرایم به کار می‌رود با جرایمی که از رایانه استفاده نشده تفاوت ماهوی خاصی وجود ندارد. بنابراین، از نظر آثار و عواقب قانونی هم دارای آثار یکسان بوده و وضع مجازات جداگانه لازم نیست.از جمله قوانینی که به نظر می‌رسد جاسوسی سنتی رایانه‌ای را (که درآن رایانه تنها به عنوان ابزار و وسیله‌ای جهت ارتکاب جرم و برداشت اطلاعات استفاده می‌شود) مورد توجه قرار داده است ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح مصوب ۹ دی ۱۳۸۲ است. در این ماده، قانونگذار مجازات تسلیم اطلاعات طبقه‌بندی شده رایانه‌ای به دشمن یا افرادی که صلاحیّت دسترسی به آن اطلاعات را ندارند را به مجازات جاسوسی سنتی احاله داده است. ماده مزبور مقرر می‌دارد: «هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تاخیر

تاریخ نسبت به تاریخ حقیقی و نظایر آن که بطورغیر مجاز بوسیله نظامیان در سیستم رایانه و نرم افزارهای مربوط صورت گیرد و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه بندی شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به ان اطلاعات را ندارند، افشاء غیرمجاز اطلاعات.... جرم محسوب و حسب مورد مشمول مجازاتهای مندرج در مواد مربوط به این قانون می‌باشند». با توجه به نص صریح فصل جرایم رایانه‌ای قانون مجازات اسلامی، در مواردی که شخصی نظامی از رایانه مانند سایر ابزار به عنوان وسیله ارتکاب جرم جاسوسی استفاده بکند براساس ماده ۷۸۰ قانون فوق الذکر، ماده۱۳۱ قانون مجازات جرایم نیروهای مسلح حاکم خواهد بود و مرتکب مشمول مجازات های مقرره در هر مورد خاص است. اما در صورتی که شخص نظامی از رایانه نه به عنوان وسیله بلکه فراتر از آن و به عنوان موضوع جرم استفاده کند و به اطلاعات موجود در آن بدون اینکه مجوز دسترسی به آنها را داشته باشد دست یابد؛ طبق ماده ۷۳۱ قانون مجازات اسلامی مجازات خواهد شد که در این صورت نیز با توجه به ماده ٧٥٤ قانون مجازات اسلامی از موجبات تشدید مجازات مرتکب خواهد بود. ماده ٧٥٤ مقرر می‌دارد: «در موارد زیر حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد: الف. هر یک از کارمندان و کارکنان اداره ها و سازمان ها... و همچنین نیروهای مسلح و ماموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند...»؛ که یکی از آن موارد تشدید کارمند یا نظامی بودن شخص مرتکب است.

در مورد جاسوسی رایانه‌ای که در آن، رایانه در عمل به منزلهٔ موضوع جرم، جزء رکن مادی اعلام شده باشد؛ می‌توان به حمله ویروس جاسوسی استاکس نت به تاسیسات هسته‌ای ایران اشاره کرد. اوایل مرداد ۱۳۸۹ خبری روی خبرگزاری‌ها قرار گرفت که براساس آن ایران، هدف اصلی کرم جاسوسی استاکس‌نت شده است. طبق این خبر رایانه‌های، ایران مورد هجوم شدید ویروس استاکس‌نت قرارگرفته که تلاش می‌کند اطلاعات سامانه‌های کنترل صنعتی را به سرقت برده و آنها را روی اینترنت قرار دهد». مدیرکل صنایع برق، الکترونیک و فناوری اطلاعات وزارت صنایع درباره چگونگی عملکرد این ویروس می‌گوید: با فعال شدن این ویروس، سامانه های خودکار صنعتی، اطلاعات خط تولید را به مرکز اصلی مشخص شده بوسیله ویروس منتقل می‌کنند و این اطلاعات بوسیله طراحان ویروس مورد پردازش قرار می‌گیرند و به این ترتیب، برای ضربه زدن به کشور و جاسوسی از مراکز مهم کشور برنامه‌ریزی می‌شوند. استاکس نت پس از رسیدن به این سامانه‌های رایانه‌ای، شروع به جمع آوری اطلاعات آن اداره‌ای می‌کند که به سامانه آن نفوذ کرده است. حتی اطلاعات ذخیره موجود در سیستم را نیز منتقل می‌کند؛ سپس از طریق اتصال به اینترنت اطلاعات و اسرار به

دست آمده رابه مقصد مشخص شده و مورد نظر ارسال می‌کند» (مرشدی،۱۳۸۹: http://www.jamejamonline.ir/papertext.aspx?newsnum=100888862821).

۲- عنصر قانونی جاسوسی رایانه‌ای

عنصر قانونی جرم جاسوسی رایانه‌ای فصل جرایم رایانه‌ای قانون مجازات اسلامی الحاقی ۵ خرداد۱۳۸۸ است. مادهٔ ۷۳۱ این قانون که در ذیل مبحث سوم با عنوان جاسوسی رایانه‌ای آمده است در سه بند عنصر قانونی و مادی جاسوسی رایانه‌ای را بیان کرده است. ماده مزبور مقرر می‌دارد: «هرکس بطور غیر مجاز نسبت به داده‌های محرمانه در حال انتقال یا ذخیره شده در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

الف. دسترسی به داده‌های مزبور یا تحصیل آنها یا شنود محتوای محرمانه در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست تا شصت میلیون ریال یا هردو مجازات؛

ب. در دسترس قرار دادن داده‌های مزبور برای اشخاص فاقد صلاحیت به حبس از دوتا ده سال؛

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

علاوه بر ماده ۷۳۱، ماده ۷۳۲ هم در مورد نقض تدابیر امنیتی سامانه های رایانه‌ای مقرر داشته: «هر کس که به قصد دسترسی به داده‌های محرمانه، تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی را نقض 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».

علاوه بر مواد۷۳۱ و۷۳۲ الحاقی قانون مجازات اسلامی، قانون تجارت الکترونیک مصوب ۱۷ دی ۱۳۸۲ در مادهٔ ٦٤، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه ها و مؤسسات برای خود و یا افشای آن برای اشخاص در محیط الکترونیک را جرم دانسته و برای آن مجازات حبس از شش ماه تا دو سال و نیم و جزای نقدی معادل پنجاه میلیون ریال پیش بینی کرده است.

۳- عنصر مادی جاسوسی رایانه‌ای

قبل از بررسی عنصر مادی جرم جاسوسی رایانه‌ای، لازم به ذکر است که با توجه به اینکه جرم مزبور به وسیله قانون، عناوین مجرمانه خاص را به عنوان جرم جاسوسی شناخته و با در نظر گرفتن اصل تفسیر مضیق قوانین کیفری، کیفیّت اقدام متهم و مواردی که در مواد الحاقی قانون مجازات اسلامی تصریح شده کاملاً محدودکننده است. بنابراین، اگر متهم غیر از روش

در قانون، طریقی دیگر برای ورود جهت کسب اطلاعات اتخاذ کند، آن اقدامات جزء عناصر تشکیل دهنده این جرم محسوب نخواهد شد. بنابراین، جهت تحقق این جرم باید مرتکب با همان وسایل و روشی که قانون تصریح کرده است مرتکب جرم شده باشد (گارو،۱۹۹۵: ۷۱۲).

فصل جرایم رایانه‌ای قانون مجازات اسلامی الحاقی ۵ خرداد ۱۳۸۸ در ماده ۷۳۱ چهار دسته از رفتار مجرمانه را به عنوان عنصر مادی جرم قرار داده است که در این گفتار به بررسی آنها پرداخته می‌شود.

۳-۱- دسترسی غیرمجاز و در دسترس قرار دادن داده های محرمانه

الف- موضوع جرم

در مادهٔ ۷۳۱ قانون مجازات اسلامی آنچه موضوع جرم و مورد نظر قانونگذار بوده، داده‌های محرمانه است. طبق تبصره ۱ مادهٔ ۷۳۱، منظور از داده‌های محرمانه، داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه زند. بنابراین، در جرایم جاسوسی رایانه‌ای تفاوتی وجود ندارد بین موردی که اسناد یا تصمیمات محرمانه راجع به امور سیاسی یا نظامی یا اقتصادی و غیره باشد؛ بلکه همین که افشای آنها به امنیت ملی ضربه زند کافیاست. شایان ذکر است در تبصره۲ ماده۷۳۱ تهیه آیین‌نامه نحوه تعیین و تشخیص داده‌های محرمانه و نحوه طبقه‌بندی و حفاظت آنها بر عهده وزارت اطلاعات است که باید این مهم را با همکاری وزارتخانه‌های دادگستری کشور، ارتباطات و دفاع و پشتیبانی نیروهای مسلح انجام دهد و به تصویب هیأت وزیران برساند.

علاوه بر این، از آنجا که طبقه‌بندی بعضی از اسناد و مدارک ثابت نمی‌ماند، مثلاً ممکن است سندی در زمان تنظیم دارای طبقه بندی محرمانه و افشای آن مضر به منافع و امنیّت ملی باشد؛ ولی بعد از گذشت مدتی تنزل طبقه پیدا کند و در نتیجه افشای آن مضر به منافع و امنیّت ملی تشخیص داده نشود، باید گفت طبقه‌بندی سند در زمان وقوع جرم ملاک عمل برای محاکم می‌باشد نه در زمان تنظیم سند(اشراقی،۱۳۸۰: ۷۵).

ماده ۲ کنوانسیون جرایم سایبر در مورد جرم انگاری دستیابی غیرمجاز مقرر داشته: «هر یک از کشورهای عضو کنوانسیون می‌توانند اقدام به وضع آن چنان قوانین و مقرراتی کنند که ضرورتا براساس حقوق داخلی خود هرنوع دسترسی عمدی بدون حق به قسمتی از یک سیستم رایانه‌ای را جرم تلقی کند. عضو مورد نظر می‌تواند مقرر دارد که جرم در اثر تعرض به اقدامات امنیتی با قصد دسترسی به داده های رایانه ای یا دیگر مقاصد ناروا یا نسبت به سیستم رایانه ای محقق می‌شود که با سیستم رایانه‌ای دیگر در ارتباط است»(خرم آبادی،۱۳۹۰: ۳۵). در حقوق داخلی ایران نیز دسترسی غیرمجاز در صورتی جرم جاسوسی تلقی شده است که به

داده های محرمانه در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل های داده دسترسی پیدا کند.

قانونگذار مشخص نکرده که آیا انتقال داده های محرمانه از یک قسمت به قسمت دیگرِ یک سیستم رایانه‌ای و هم انتقال داده ها از یک سیستم رایانه‌ای به سیستم دیگر موضوع جرم دستیابی غیرمجاز خواهد بود یا فقط دستیابی به داده های رایانه‌ای در حال انتقال بین دو سیستم رایانه‌ای موضوع جرم دستیابی غیرمجاز خواهد بود. اما به نظر می‌رسد با توجه به اینکه قانونگذار صرف دسترسی به هر نحوی را جرم دانسته است؛ بنابراین در این مورد تفاوتی بین موارد فوق نباشد.

ب- رفتار مرتکب

رفتار مرتکب عبارت است از فعل مثبت مرتکب جرم دائر بر ورود به تمام یا بخشی از یک سامانه رایانه‌ای. یکی از شرایط تحقق این جرم این است که دستیابی به صورت غیرمجاز انجام گیرد. قانونگذار ایران صرف دسترسی غیرمجاز به داده‌های محرمانه یا تحصیل آنها را در بند الف ماده ۷۳۱ جرم جاسوسی دانسته است. امّا با توجه به امکانات بسیار زیاد رایانه در انجام امور مختلف و عدم محدودیّت زمانی و مکانی و عدم لزوم حضور مرتکب در صحنهٔ جرم، نحوهٔ دسترسی به داده‌های محرمانه هم با انجام رفتارهای خاص، قابل تحقق است. به عبارت دیگر، اگر بخواهیم در جاسوسی رایانه‌ای عملی را دسترسی غیرمجاز بدانیم، لازم نیست مرتکب جرم شخصا دست به ارتکاب اعمال مجرمانه بزند و خودش در صحنهٔ جرم حاضر باشد؛ بلکه می‌تواند با استفاده از فناوری‌های روز و نرم‌افزارهای جاسوسی به راحتی اطلاعات مورد نظر خود را از رایانهٔ ای خاص کسب کند. به عنوان مثال، شخصی می‌تواند با نصب نرم‌افزار جاسوسی روی رایانه مورد نظر با بیشترین دقّت، تمام فعالیّت‌های کاربر رایانه اعم از ایمیل‌های ردوبدل شده، کلیدهای فشرده شده و وب سایت‌های دیده شده و بسیاری کارهای دیگر را ضبط و به دیگری تحویل دهد.

علاوه بر دسترسی غیرمجاز به داده‌های محرمانه، تحصیل این داده‌ها به صورت غیرمجاز نیزجاسوسی تلقی می‌شود. تحصیل در لغت به معنای بدست آوردن آمده است(معین، ۱۳۸٦: ۱۰۳۸). به عبارت دیگر، در مورد جاسوسی رایانه‌ای می‌توان گفت برای صدق عنوان جاسوسی شخص جاسوس به هر طریقی که این اطلاعات را به دست آورده باشد؛ جرم محقق می‌شود اعم از اینکه در قبال آن به طرف مقابل پول یا چیز دیگری داده باشد یا از آن فرد ربوده باشد.

درخصوص در دسترس قرار دادن داده های محرمانه با توجه به صراحت و تأکید این بند بر «در دسترس قراردادن داده‌های مزبور» منطقی به نظر می‌رسد که این داده‌ها اعم از فیلم،

عکس، متن و.... باید به طور مستقیم در اختیار فرد فاقد صلاحیت قرار گیرد. افشای مفاد این داده‌ها که شکل غیرمستقیم در دسترس قراردادن است؛ شامل ماده نمی‌شود و جرم نیست. زیرا اگر قانونگذار نظر در دسترس قراردادن مفاد داده‌ها را جرم می‌دانست مانند ماده۵۰۱ ق.م.ا از واژه‌ای «مفاد» در این ماده استفاده می‌کرد و آنگاه مقرر می داشت: «در دسترس قراردادن داده‌های مذکور یا مفاد آن....» این امر یکی از نقایص بندب ماده۷۳۱ الحاقی ق.م.ا است؛ زیرا با توجه به محرمانه بودن داده‌ها و اهمیت بالای آن عقلاً تفاوتی میان تسلیم خود و مفاد داده‌ها نیست و اطلاع افراد فاقد صلاحیت از خود داده یا مفاد آن به هر حال به امنیت کشور لطمه می‌زند (بوجاری،۸۸: ۲).

البته می‌توان در دسترسی قراردادن مفاد این داده‌ها را طبق ماده۵۰۱ ق.م.ا جرم دانست. به این ترتیب، اگر این داده‌ها در برگیرنده نقشه‌ها، اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور باشد؛ آنگاه در دسترس قرار دادن مفاد آنها به افراد فاقد صلاحیت، جرم محسوب می‌شود. به هر نحو، 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.

نکتهٔ قابل ذکر دیگر در مورد بندهای الف، ب و ج مادهٔ ۷۳۱ این است که **متهم** باید داده‌های محرمانه را در اختیار اشخاصی فاقد صلاحیت یا شخص بیگانه قرار دهد تا مشمول مجازات‌های مقرر قرار گیرد. پس اگر موفق به این امر نشود مشمول حکم جاسوسی رایانه‌ای نخواهد بود. پس می‌توان گفت که جرم جاسوسی رایانه‌ای از جهت دسترسی پیدا کردن یا در دسترس افراد فاقد صلاحیت قرار دادن، جرمی مقیّد به نتیجه است. ولی از جهت هدف و انگیزه شخص از این اقدامات اینکه به نفع دشمن اقدام کند یا علیه منافع ملی و یا هر هدف و انگیزه دیگر، جرم مطلق است و هدف و انگیزه مرتکب هر چه باشد تاثیری در مجازات وی نخواهد داشت. در واقع از جرایم مادی صرف است.

۳-۲- شنود غیرمجاز محتوای محرمانه در حال انتقال

الف- رفتارمرتکب

رفتار مجرمانه مرتکب در جرم شنود غیرمجاز شامل فعل مثبت مرتکب دائر برگوش کردن، کنترل یا نظارت بر محتوای ارتباطات چه به صورت مستقیم یعنی از راه ورود و دسترسی و استفاده از یک سامانه رایانه‌ای، یا به شکل غیر مستقیم یعنی با استفاده از دستگاه های استراق سمع الکترونیک است. علاوه بر این، شنود ممکن است شامل ضبط کردن داده ها نیز بشود؛ مثلاً در یک شیوه، صدای حاصل از چاپگر رایانه(این صدا در اکثر چاپگرهای سوزنی ایجاد

می‌شود) را ضبط کرده و سپس با گوش دادن، نوار ضبط شده کلیدهای فشرده شدهٔ صفحه کلید را آشکار کرده و به محتوای آن پی می‌برند.

ب- موضوع جرم

عمل دیگر که ارتکاب آن را قانونگذار عنصر مادی جرم جاسوسی رایانه‌ای شناخته است؛ شنود غیرمجاز محتوای محرمانه در حال انتقال است. طبق بند الف ماده ۷۳۱، شنود محتوای محرمانه در حال انتقال، جرم بوده و مرتکب به مجازات حبس از یک تا سه سال یا جزای نقدی از بیست تا شصت میلیون ریال یا هردو مجازات محکوم خواهد شد.گزارش توجیهی کنوانسیون جرایم سایبردر خصوص داده های در حال انتقال اشعار داشته: «انتقال داده های رایانه‌ای می‌تواند در داخل یک سیستم رایانه‌ای مستقل صورت بگیرد. مانند جریان داده ها از واحد پردازش مرکزی(CPU) به صفحه نمایش یا چاپگر.همچنین می‌تواند مابین دو سیستم رایانه‌ای متعلق به یک شخص، دو رایانه در ارتباط با همدیگر و یا یک رایانه و یک شخص مثلاً از طریق صفحه کلید صورت گیرد(خرم آبادی،۱۳۹۰: ٤٣).

شنود غیرمجاز در حالی که محتوای داده‌ها محرمانه نباشد به صورت مجزا در ماده۷۳۰ ق.م.ا جرم انگاری شده است. مطابق این ماده، «هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترو مغناطیسی یا نوری را شنود کند...».

۳-۳- نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی، به قصد دسترسی به داده‌های محرمانه

الف- رفتارمرتکب

در قانون تعریفی از تدابیر امنیتی که عنصر مادی این جرم را تشکیل می‌دهد، ارائه نشده است. اما در لایحه تقدیمی دولت این اصطلاح تحت عنوان تدبیرهای حفاظتی تعریف شده بودکه طبق آن عبارت است از: «به‌کارگیری روش‌های نرم‌افزاری یا سخت‌افزاری یا ترکیبی از آن دو، متناسب با نوع و اهمیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی به منظور جلوگیری از دسترسی به آنها بدون مجوز مرجع قانونی».

نکته‌ای که باید در اینجا به آن توجه شود این است که قانونگذار سوءنیت خاص نفوذکننده و نقض‌کننده تدابیر امنیتی رایانه‌ها را مورد توجه قرار داده است و کار کسی که با قصدی غیر از دسترسی به داده‌های محرمانه مثلاً از باب کنجکاوی یا نشان دادن مهارت خود اقدام به نقض تدابیر امنیتی سیستم‌ها کند؛ طبق این ماده قابل مجازات نخواهد بود. این امر باعث مشکل شدن اثبات قصد متهم مبنی بر دسترسی به داده‌های محرمانه می‌شود. در این ماده لازم

نیست مرتکب به هدف و قصد خود از نقض سیستم‌های امنیتی رایانه‌ها دست یابد. در واقع، این جرم مقید به نتیجه نبوده بلکه از جمله جرایم مطلق است و همین‌که شخصی سیستم امنیتی رایانه‌ای را به قصد دسترسی به داده‌های محرمانه آن نقض کند مشمول حکم ماده ۷۳۲ می‌شود. حتی اگر در آن رایانه هیچ‌گونه داده‌ی محرمانه وجود نداشته باشد.

ب- موضوع جرم

تأمین امنیت هر سامانه رایانه‌ای و مخابراتی در ابتدا مستلزم تأمین امنیت در محیط فیزیکی سخت‌افزارهاست. کنترل دسترسی و ایجاد پوشش دو روش حفظ و ارتقای امنیت فیزیکی سامانه‌های مزبور در ماده است. کنترل دسترسی مانند آنکه افرادی خاص اجازه ورود به مکان‌هایی را داشته باشند که تجهیزات رایانه‌ای در آن قرار دارد. ایجاد پوشش نیز مانند آنکه فیبرهای نوری و کابل‌های ارتباطی شبکه‌های رایانه‌ای در داخل لوله‌های فلزی محافظ قرار داده شود تا به این صورت فرد نتواند از آنها انشعاب بگیرد؛ یا اینکه رایانه‌ها و سایر سخت افزارها را داخل اتاق مناسب مستقر و در ورودی آن حفاظ مطمئن نصب شود. اما بعد نرم‌افزاری تدابیر رایانه‌ای شامل طیفی وسیع از تدابیر و روش‌هایی است که از دسترسی و تغییرات غیرمجاز در داده‌های رایانه‌ای جلوگیری می‌کند. روش‌هایی مانند تعیین نام کاربرد مجاز و گذرواژه، نصب فایروال(حبیبی،۸۲: ۱۳).

۴- عنصر معنوی جاسوسی رایانه‌ای

قبل از بررسی عنصر روانی رفتارمجرمانه جاسوسی رایانه ای، لازم به ذکر است که قانونگذار در فصل جرایم رایانه‌ای عنصر روانی جاسوسی رایانه‌ای را به صورت دقیق بیان نکرده است. یعنی این که قانونگذار قصد و هدف مرتکب جرم را در دستیابی به داده‌های محرمانه، مورد توجه قرار نداده و قصد مرتکب جرم را در تعیین مجازات مسکوت گذاشته است و به صورت مطلق دسترسی غیرمجاز یا شنود غیرمجاز یا تحصیل غیرمجاز داده‌های محرمانه یا افشاء آنها را جرم و قابل مجازات دانسته و هدف مرتکب را از انجام اینگونه اقدامات به اینکه قصد جاسوسی به نفع دشمن داشته یا جهت ارضاء حس کنجکاوی را در تعیین میزان مجازات او مؤثر ندانسته است.

علاوه بر این، میزان آگاهی مرتکب جرم در مورد موضوع جرم مورد توجه قرار نداده است. مثلاً ممکن است شخصی به تصور اینکه اطلاعات رایانه‌ای جزو داده‌های محرمانه نبوده و جزو داده‌های معمولی است، بخواهد به آنها دسترسی یابد یا آنها را تحصیل کند. امّا بعد از دستگیری شخص معلوم شود که داده‌هایی که او بدست آورده جزء داده‌های محرمانه مرتبط با

منافع ملی و امنیت کشور بوده است. اینجا قانونگذار مشخص نکرده است که تکلیف قضات رسیدگی‌کننده به این پرونده چه خواهد بود. آیا باز مشمول مجازات‌های مقرر در ماده ۷۳۱ خواهد بود چون به هرحال به داده‌های محرمانه دسترسی غیرمجاز پیدا کرده است؛ یا اینکه مشمول مجازات‌های ماده ۷۳۱ نخواهد بود زیرا متهم از ابتدا قصد دسترسی به داده‌های غیر محرمانه را نداشته و اتفاقاً به داده‌های محرمانه دست یافته است. علاوه بر این، اصل تفسیر مضیق و به نفع متهم قوانین جزایی هم ایجاب می‌کند که در موارد شک در تعیین مجازات و نوع جرم، نفع متهم را مدنظر قرار دهیم.

۴-۱- دسترسی غیرمجاز و در دسترس قرار دادن داده های محرمانه

عنصر روانی جرم دسترسی غیرمجاز به داده های محرمانه علاوه بر عمد در دسترسی و تحصیل عبارت است از آگاهی و علم مرتکب به غیر مجاز و بدون مجوز بودن دسترسی یا تحصیل و یا شنود داده های سری ونیز علم به سری بودن داده هایی که شخص به آنها دسترسی و... پیدا کرده است.

امّا در بند ب ماده ۷۳۱ قانون مجازات اسلامی الحاقی ۱۳۸۸/۳/۵ (در دسترس قرار دادن داده‌های مزبور برای اشخاص فاقد صلاحیت) لازم است شخص به این موضوع آگاهی داشته باشد که شخص مقابل که می‌خواهد داده‌های محرمانه را در دسترس او قرار دهد فاقد صلاحیّت دسترسی به این داده‌ها است. در نتیجه، اگر کسی که صلاحیت دسترسی به داده‌های محرمانه را دارد؛ از روی اشتباه یا فریب، فکر کند شخص دیگر نیز صلاحیّت دسترسی به این داده‌ها را دارد و در اختیار او بگذارد و بعدها معلوم شود که شخص مزبور فاقد صلاحیّت بوده، دیگر نمی‌توانیم این شخص واگذارکننده اطلاعات را طبق بند ب مادهٔ ۷۳۱ مجازات کنیم؛ چون در غیر این صورت یکی از اصول مسلم حقوق جزا که همان آگاهی مرتکب از غیرقانونی بودن عمل ارتکابی است نادیده گرفته می شود.

در بند ج ماده ۷۳۱ قانون مجازات اسلامی افشاء یا در دسترس قرار دادن داده‌های محرمانه برای دولت، سازمان شرکت یا گروه بیگانه یا عاملان آنها، موجب تشدید مجازات دانسته شده است. امّا متأسفانه در اینجا نیز قانونگذار این موضوع مهم را که آیا مرتکب جرم باید نسبت به بیگانه بودن طرف مقابل یا عامل گروه بیگانه بودن طرف مقابل آگاهی داشته باشد یا نه در جهت تشدید مجازات اشاره‌ای نکرده است. یعنی معلوم نیست که مرتکب جرم به صرف اینکه این داده‌های محرمانه را در اختیار یک طرف بیگانه یا عامل او قرار دهد حتی خودش از بیگانه بودن طرف مقابل آگاهی نداشته باشد و با تصور اینکه طرف مقابل او که اطلاعات را در دسترس او قرار می‌دهد یک عامل داخلی و هم‌وطن است، آیا در این صورت وی مشمول

تشدید مجازات می‌شود یا اینکه حتماً باید با علم و آگاهی نسبت به بیگانه‌بودن طرف اطلاعات را در دسترس او قرار دهد تا مشمول تشدید مجازات قرار گیرد؟ به‌نظر می‌رسد تنها عمل مجرمانه که در این قانون با جاسوسی سنتی مطابقت می‌کند بند ج ماده ۷۳۱ است که در آنیف هدف مرتکب جرم که همان رساندن اطلاعات به بیگانه است (که جزو عناصر جاسوسی سنتی است) در اینجا نیز لحاظ شده است.

۴-۲- شنود غیرمجاز محتوای محرمانه در حال انتقال

عنصر روانی جرم جاسوسی رایانه‌ای از طریق شنود غیرمجاز محتوای محرمانه در حال انتقال علاوه بر عمد شنود؛ عبارت است از آگاهی و علم به غیر مجاز و بدون مجوز بودن شنود داده‌های محرمانه و نیز علم به محرمانه بودن داده‌هایی که شخص به آنها دسترسی و... پیدا کرده است.

۴-۳- نقص تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی، به قصد دسترسی به داده‌های محرمانه

در ماده ۷۳۲ قانونگذار برخلاف موارد قبلی به قصد و سوءنیت خاص مرتکب جرم توجه کرده و آن را در تعیین عمل مجرمانه و مجازات مؤثر دانسته است. ماده۷۳۲ مقرر می‌دارد: «هرکس به قصد دسترسی به داده‌های محرمانه موضوع ماده ۷۳۱ این قانون، تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی را نقض کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد». پس اگر شخصی به قصدی غیر از دسترسی به داده‌های محرمانه که افشاء آنها به امنیت کشور و منافع ملی لطمه می‌زند تدابیر امنیتی رایانه‌ها را نقض کند، مشمول مجازات ماده ۷۳۲ و عنوان جاسوسی رایانه‌ای نخواهد بود.

در این مورد، ابهامی که قبلاً اشاره کردیم پیش می‌آید.اگر شخصی به تصور اینکه داده‌های یک رایانه محرمانه هستند و با هدف دسترسی به آنها اقدام به مختل کردن سیستم‌های امنیتی رایانه‌ای بکند امّا بعد از دسترسی به آنها متوجه شود که این داده‌ها محرمانه نیستند؛ یا اینکه شخصی به قصد دسترسی به داده‌های غیرمحرمانه و به این تصور که اطلاعات رایانه محرمانه نیستند اقدام به مختل کردن سیستم‌های امنیتی رایانه بکند و بعد از دسترسی متوجه شود که این داده‌ها جزء داده‌های محرمانه هستند؛ آیا باز مشمول حکم ماده ۷۳۲ خواهند بود؟ یا چون آنچه که قصد مرتکب بوده انجام نگرفته و آنچه که انجام گرفته خواست مرتکب نبوده، نباید او را مشمول مجازات ماده ۷۳۲ قرار دهیم؟ به نظر می‌رسد در فرض اول که شخص به قصد دسترسی به داده‌های محرمانه اقدام به مختل کردن تدابیر امنیتی رایانه‌ها می‌کند، می‌توانیم

مرتکب را طبق ماده ۷۳۲ مجازات کنیم. زیرا در واقع تحقق جرم او محال تلقی می‌شود و در فرض دوم که قصد مرتکب دسترسی به داده‌های محرمانه نبوده طبق ظاهر ماده ۷۳۲ نمی‌توانیم او را به مجازات مقرر محکوم کنیم؛ زیرا عنصر معنوی جرم در این حالت مفقود بوده و ارکان جرم محقق نشده است.

۵- وضعیت بین‌المللی جاسوسی رایانه‌ای

در این بخش به بررسی اقدامات سازمان‌های بین‌المللی در مورد جرائم رایانه‌ای و جرم جاسوسی رایانه‌ای و همچنین قوانین بعضی از کشورهایی که اقدامات خاص را در این عرصه جرم انگاری کرده‌اند و نیز نحوهٔ تعریف و عناصر مادی... جرم جاسوسی رایانه‌ای در حقوق سایر کشورها می‌پردازیم.نخستین تقسیم‌بندی که از جرایم رایانه‌ای ارائه شد؛ تقسیم‌بندی سازمان همکاری و توسعه اقتصاد(OECD) بود که جرایم رایانه‌ای را به ۵ دسته تقسیم کرد. سازمان مزبور در ۱۹۸۳ به مطالعهٔ امکان اعمال مقررات بین‌المللی و هماهنگی قوانین کیفری به منظور حل مسأله سوءاستفاده رایانه‌ای متعهد شد؛ بدین‌گونه نخستین تقسیم‌بندی جرایم رایانه‌ای بوسیله این نهاد شکل گرفت. در این تقسیم‌بندی، دستیابی یا شنود در یک سیستم رایانه‌ای(جاسوسی رایانه‌ای) که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم انجام بگیرد، جرم تلقی شد. گزارش این نهاد به صورت پیشنهادی در اختیار کشورهای عضو قرار گرفت.

کمیتهٔ منتخب جرایم شورای اروپا در سال ۱۹۸۹پس از بررسی نظریات OECD و نیز بررسی‌های فنی- حقوقی ملی توصیه‌نامهٔ R(89)9 سال ۱۹۸۹ خود[1] عناوینی مجرمانه از جرایم رایانه‌ای را با دو گروه فهرست حداقل(که تصویب آن اجباری بود) و فهرست اختیاری(که تصویب آن بوسیله وزرای دولت‌های اتحادیه اروپا اختیاری بود) به وزراء پیشنهاد داد که در جلسه ای که با حضور آنان در این رابطه برگزار شده بود موردتصویب آنان قرار گرفت (HTTP://www.CONVENTION.COE.INT/TREATY/EN/REPORTS/HTMI/185.HTM)

سازمان ملل‌متحد هم از جملهٔ سازمان‌هایی است که به جرایم رایانه‌ای پرداخته است. در هفتمین کنگره سازمان ملل که در سال ۱۹۸۵ برگزار شد؛ دبیر کل این سازمان مواردی را به عنوان جرایم رایانه‌ای مطرح کرد که طی آن دستیابی غیرمجاز به سیستم‌ها و خدمات رایانه‌ای جرم‌انگاری شده است.

1-Council of Europe, commitment of Ministers; Recommendation NO.R(89),op.cit.

انجمن بین‌المللی حقوق جزا (AIDP[1]) هم در نشست سال ۱۹۹٤ خود کـه در ریـودوژانیرو برگزار شد، دسـتیابی بـه اسـرار بـرخلاف قـانون را جـرم شـناخت؛ ضـمن اینکـه مجـدداً بـر فهرست‌های حداقل(اجباری) و اختیاری شورای اروپا تاکید کرد(امانی، ۱۳۸۳: ۱۵۹).

امّا در نهایـت اتحادیـهٔ اروپـا بـه همـراه چنـد کـشور دیگـر در سـال ۲۰۰۱ در بوداپـست کنوانسیون جرایم سایبری شورای اروپا[2] را تصویب کرد. این کنوانسیون جرایم رایانـه‌ای را بـه چهار دسته طبقه‌بندی می‌کند و برغم اینکه در این کنوانسیون برخلاف فـصل جـرایم رایانـه‌ای قانون مجازات اسلامی(مصوب۱۳۸۸/۳/۵) از عبارت جاسوسی رایانه‌ای استفاده نمـی‌کنـد؛ امّـا عنوان اول از بخش اول فصل دوم کنوانسیون به جرائم علیه محرمانگی؛ تمامیّت و دسترسی بـه داده‌ها و سیستم‌های رایانه‌ای اختصاص داده شده است. در ماده ۲ در مورد دسترسی غیرمجـاز و در مادهٔ ۳ کنوانسیون در مورد شنود غیرقانونی اطلاعات.... مقرراتی را آورده اسـت. در ذیـل عنوان جرائم علیه محرمانه بودن داده‌ها ۵ ماده بطور مفصل جرائم این حوزه را برمی‌شمارند که عبارت است از: دسترسی غیرمجاز؛ شنود غیرقانونی؛ ایجاد اختلال در سیستم و سوءاسـتفاده از دستگاه.

فصل جرائم رایانه‌ای قانون مجازات اسلامی از لحاظ عناصر مادی و معنوی شباهت بـسیار به کنوانسیون جرائم سایبری شورای اروپا دارد. اما تفاوت عمده این دو در ایـن اسـت کـه در مقررات جرایم رایانه‌ای ایران فقط داده‌های محرمانه که افشاء آنها به امنیت کشور یا منافع ملّی لطمه وارد کند، مورد حمایت واقع شده‌اند. به عبارت دیگـر، در حقـوق داخلـی مـا دسترسـی غیرمجاز یا شنود غیرمجاز داده‌های غیر محرمانه که افشای آنها به امنیـت و منـافع ملـی ضـربه نمی‌زند؛ طبق فصل جرایم رایانه‌ای مورد نظر به عنوان جاسوسـی رایانـه ای قابلیـت تعقیـب و مجازات ندارد و می‌توان بر اساس سایر قوانین عمومی جزایی کشور مورد تعقیب قرار داد. امّـا در کنوانسیون جرایم سایبری همهٔ گونه اطلاعات اعـم از دولتـی، غیردولتـی، امنیّتـی، تجـاری، فرهنگی مورد حمایت قرار گرفته است.

طبق آخرین آمار، تعداد امضاءکنندگان کنوانسیون بوداپست به ۵۰ کشور رسـیده اسـت کـه ۳۹ کشور از ٤۷ کشور عضو شورای اروپا به عـلاوه آمریکـا، ژاپـن، کانـادا، افریقـای جنـوبی، مکزیک، فیلیپین، شیلی، کاستاریکا، جمهوری دومینیکن را شامی می شوند (امانی، ۱۳۸۳: ۱۵۹).

در جرایم علیه محرمانه بودن داده‌ها و اطلاعات رایانه‌ای در حقوق بعضی از کشورها مثـل دانمارک و فرانسه و سوئد و آمریکا، هلند، نـروژ صـرف دسـتیابی غیرمجـاز بـه داده‌هـا جـرم شناخته شده است. امّا برخی کشورها مثل کانادا و آلمان و نروژ دستیابی غیرمجاز به داده‌هـایی

1-Association International de DroitPenal
2-Convention ofCyberCrime

که بوسیله سیستم‌های امنیتی محافظت می‌شوند یا داده‌های ملی رایانه‌ای جرم‌انگاری شده‌اند(پیراکوف،۱۹۸٦: ۱۰۳).

از جمله کشورهایی که در مورد جرایم رایانه‌ای و جاسوسی رایانه‌ای به جرم انگاری اختصاصی پرداخته‌اند؛ می‌توان کشور بلژیک را نام برد. کشور مزبور مطابق قانون مصوب ۲۸ نوامبر ۲۰۰۰ و بر اساس مادهٔ ۵۵۰ مکرر و۵۵۰ ثالث تحت عنوان اثرات تقابلی محرمانه بودن، یکپارچگی و قابل دسترس بودن سیستم‌های رایانه‌ای جرایم علیه محرمان بودن رایانه‌ها را جرم‌انگاری کرده است. بند ۱ ماده ۵۵۰ مکرر مزبور مقرر داشته «کسی که بداند اجازه دسترسی به یک سیستم رایانه‌ای را ندارد ولی خلاف آن را انجام دهد به ۳ ماه تا یکسال زندان و جزای نقدی ۲٦ فرانک تا ۲۵ هزار فرانک یا یکی از این دو مجازات محکوم می‌شود در صورتی که مورد بند یک به منظور سوء استفاده باشد در آنصورت جزای عمل ٦ماه تا۲ سال زندان خواهد بود».

در انگلستان هم در سال ۱۹۹۰ قانون میسوس(Misus act) رایانه‌ای تصویب شده است که مطابق آن در جهت حفاظت از رایانه‌ها، هرگونه تغییر در انجام عملکرد رایانه‌ها و دسترسی غیر مجاز جرم دانسته شده است. در این کشور، قوانینی جدید نیز مشتمل بر جرم انگاری استراق سمع و دستیابی غیر مجاز به داده پردازی و سیستم های ارتباطات وضع شده است. این قوانین موارد متنوع را در بر می‌گیرد؛ از مقررات ناظر بر جرم شناختن صرف دستیابی به سیستم های داده پردازی گرفته تا مجازات دستیابی در مواردی که داده های دستیابی شده به وسیله تدابیر امنیتی مورد حمایت قرار گرفته‌اند.

در مقام مقایسه می‌توان گفت فصل جرایم رایانه‌ای قانون مجازات اسلامی در مورد جرایم جاسوسی از سه جهت با قوانین سایر کشورها و کنوانسیون ۲۰۰۱ بوداپست تفاوت دارد:

۱. از جهت اطلاق عنوان جاسوسی

در حقوق سایر کشورها برخلاف حقوق داخلی با عناوینی دیگر از جمله جرایم علیه محرمانه بودن داده ها نامگذاری شده است.

۲. از جهت محدود شدن دامنهٔ جرم

در حقوق سایر کشورها و کنوانسیون‌ها، دامنه جرم علیه محرمانه بودن همه داده‌ها اعم از محرمانه و محرمانه و غیرمحرمانه مورد حمایت قرار گرفته است اما در حقوق ایران فقط داده هایی که افشای آنها باعث لطمه به امنیت یا منافع ملی شود جرم انگاری شده است.

۳. از جهت کیفیت و چگونگی دسترسی

در حقوق داخلی صرف دسترسی غیرمجاز به داده های محرمانه جرم‌انگاری شده است. اما در برخی دیگر از کشورها مانند کانادا، آلمان و نروژ دستیابی در صورتی جرم محسوب

می‌شود که در هنگام دستیابی غیرمجاز، داده های رایانه‌ای مورد تجاوز قرار گیرند (کاسپرسن،۱۳۷٦: ۲۵).

نتیجه

جرم جاسوسی رایانه‌ای از جملهٔ جرایمی است که در آن، رایانه به منزلهٔ موضوع جرم بوده و تحقق رکن مادی این جرم منوط است به دخالت در سیستم رایانه‌ای که در آن داده‌های محرمانه ذخیره شده‌اند یا داده های محرمانه در حال پردازش یا در حال انتقال هستند. تا سال ۱۳۸۸ قانونی در مورد جاسوسی رایانه‌ای در ایران نداشت؛ امِا در این سال مجلس شورای اسلامی با تصویب قانون جرایم رایانه‌ای و الحاق آن به قانون مجازات اسلامی اقدام به جرم‌انگاری دسترسی غیرمجاز به داده‌های محرمانه یا تحصیل آنها ... به عنوان جاسوسی رایانه‌ای کرد.

در عرصهٔ بین‌المللی هم قبل از حقوق ایران، سازمان‌های بین‌المللی و کشورهای مختلف اقدام به جرم‌انگاری جرایم علیه محرمانه بودن رایانه‌ها کرده‌اند؛ امّا نه با عنوان جاسوسی رایانه‌ای. از جمله کنوانسیون جرایم سایر شورای اروپا مصوب ۲۰۰۱ بوداپست و مصوبه انجمن بین‌المللی کیفری که در ۱۹۹٤ ریودوژانیرو برگزار شد. بعضی از کشورها هم مانند انگلیس، بلژیک و آلمان جرایم علیه اطلاعات اقتصادی، سیاسی... رایانه‌ها را با عناوینی مثل دسترسی غیرمجاز و جرائم علیه محرمانه بودن داده‌ها جرم‌انگاری کرده‌اند.

از آنجا که همه کشورها در معرض تهدیدات نفوذ به اطلاعات محرمانه رایانه‌ها قرار دارند و پردازش فرامرزی داده‌ها به جرائم رایانه‌ای، خصوصیت بین‌المللی داده و آنها را به پدیدهٔ فراملی تبدیل کرده بسیاری از تدابیر امنیتی باید در سطح بین‌المللی به صورت یکسان درآمده و پیشگیری از نفوذ به رایانه و جاسوسی به داخل مرزهای یک کشور خاص محدود نشود.

از خلاهای موجود در فصل جرایم رایانه‌ای مصوب خرداد ۱۳۸۸ الحاقی به قانون مجازات اسلامی می‌توان به عدم طبقه بندی داده های محرمانه ازجمله بکلی محرمانه، محرمانه... و عدم تاثیر میزان حساسیت و اهمیت های خاص هر طبقه از داده ها در میزان مسئولیت متهم اشاره کرد که باید این نقیصه ها برطرف شود و در نتیجه میزان مجازات کسی که به عنوان مثال با استفاده از ویروس «استاکس‌نت» داده های محرمانه تاسیسات هسته‌ای کشوری را فاش می‌کند نسبت به کسی که داده‌های محرمانه با اهمیت نه چندان زیاد را فاش می‌کند تفاوت وجود داشته باشد.

ایراد دیگر که فصل جرایم رایانه‌ای به نظر می‌رسد دارد، عدم حمایت این قانون از اطلاعات و حریم شخصی افراد جامعه است. با توجه به وظیفه ای که حقوق جزا در قبال

صیانت از حریم اشخاص دارد باید در این مورد نیز اصلاحاتی جهت حمایت از اطلاعات شخصی و سایت شخصی افراد صورت بگیرد. همان طور که در سایر کشورها از جمله انگلیس، استرالیا و امریکا قوانین خاص علیه تجاوزات به حقوق فردی به تصویب رسیده است.

منابع و مأخذ

الف- فارسی

۱. امانی، تقی.(۱۳۸۳)، **قوانین و مقررات حقوق مالکیت فکری و ملی و بین‌المللی تهران**، چاپ اول، تهران: بهنامی.

۲. اشراقی، ارسالان.(۱۳۸۰)، **جاسوسی به نفع اجانب در حقوق کیفری ایران**، چاپ اول،تهران: تخت‌جمشید.

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

٤. بوجاری، الیاس.(۱۳۸۹)، **بررسی ابعاد جاسوسی رایانه‌ای باتوجه به قانون جرایم رایانه‌ای**، نشریه پیام قانون.

۵. جاویدنیا، جواد.(۱۳۸۷)، **جرایم تجارت الکترونیک**. چاپ اول،تهران: خرسندی.

٦. دزیانی، محمد حسن.(۱۳۸۳)، **مقدمه‌ای بر کشف علمی جرایم سایبری**. خبرنامهٔ تخصصی انفورماتیک،(نشریهٔ دبیرخانهٔ شورای عالی انفورماتیک کشور) سال نوزدهم، شمارهٔ ۹۳، تهران.

۷. جعفری لنگرودی، محمّد جعفر.(۱۳۷۲)، **ترمینولوژی حقوق**. تهران: گنج دانش.

۸خرم آبادی، عبدالصمد.(۱۳۹۰)، **جزوه درس جرائم رایانه ای و اینترنتی**. ویژه کاراموزان قضایی.

۹. دیوید جی، آیکاو.(۱۳۸۳)، **راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای**. مترجم اکبر استرکی و همکاران، تهران: دانشگاه علوم انتظامی.

۱۰. سالاری شهر بابکی، مهدی.(۱۳۸٦)، **کلاهبرداری**. چاپ اول، تهران: بنیاد حقوقی میزان.

۱۱. عمیدی، مهدی.(۱۳۸۸)، **مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه وحقوق کیفری ایران**. تهران:دانشگاه آزاد اسلامی واحد تهران مرکز، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی.

۱۲. گارو،رنه.(۱۹۹۵)، **مطالعهٔ نظری و عملی در حقوق جزا**. ترجمه ضیاء الدین نقابت، جلد ۳،تهران:انتشارات بی‌تا.

۱۳. زیبر، اولریش.(۱۳۸۳)، **جرایم رایانه‌ای**. ترجمهٔ محمد علی نوری و همکاران، چاپ اول، تهران:گنج دانش.

۱٤.زیبر اولریش،کاسپرسن ریک، واندربرژه گی،اشتورمان کیس.(۱۳۷٦)، **جنبه های قضایی امنیت و جرم کامپیوتری**. ترجمه محمد حسن دریانی، جزوه جرایم کامپیوتری،جلد دوم،دبیرخانه شورای عالی انفورماتیک.

۱۵. زراعت، عباس.(۱۳۸۰)، **شرح قانون مجازات اسلامی، بخش تعزیرات**. چاپ دوم، تهران:ققنوس.

۱٦. گلدوزیان، ایرج.(۱۳۸٤)، **محشای قانون مجازات اسلامی**. چاپ ششم،تهران: مجد.

۱۷. معین، محمد. ۱۳۸٦، **فرهنگ معین**. چاپ دوم، تهران:انتشارات زرین.

۱۸. میرمحمدصادقی،حسین.(۱۳۸۳)، **جرایم علیه امنیت واسایش عمومی**.چاپ چهارم،تهران:میزان.

۱۹. ولیدی، محمد صالح.(۱۳۷۱)، **حقوق جزای اختصاصی**. تهران:انتشارات غروب.

ب- خارجی

1-COMPUTER-RELATED CRIME: ANALYSIS OF LEGAL POLICY ,OECD.PARIS, 1986.HTTP://WWW.OECD.ORG/DOCUMENT/19/02340-2649—34255-1815059-1-1-1,00-HT.

2-**CONVENTION OF CYBER CRIME, BUDAPEST**, 23XI.2001, HTTP:// CONVENTION.COE .INT/TREATY/EN/TREATYS/HTMI1.

3-**RECOMENDATION(89)9 ON COMPUTERRELATED CRIME AND FINAL EPORT OF THE EUROPEAN COMMITTEE ON CRIME PROBLEMS,**

STRASBOURG,1990,CONCIL OF UROPE HTTP://CONVENTION.COE.INT/ TREATY/EN/REPORTS/HTMI/185/.HT**.**
4- Pirakof, 1986،**collation with computerize crime by punitive provision**, London sweet.