سیاست تقنینی جمهوری اسلامی ایران در زمینه جرایم رایانه‌ای

نویسندگان: دکتر سهیل ذوالفقاری (ایران)[1]، علی توانگر (ایران)[2]

دریافت: ۱۳۹۵/۱۱/۰۵ **پذیرش**: ۱۳۹٦/۰٤/۳۰

چکیده

با پیشرفت فناوری و استفاده از رایانه در تمامی امور اقتصادی، نظامی و اجتماعی، جرایم مختلفی می‌تواند در حوزه رایانه حادث شود؛ لذا قانونگذار برای پیشگیری و مبارزه با این جرایم- در سال ۱۳۸۸- اقدام به تصویب قانون جرایم رایانه‌ای در ٥٦ ماده و ۲۵ تبصره نمود که از کامل‌ترین قوانین در زمینه جرایم مربوط به فضای مجازی و رایانه به شمار می‌رود؛ البته در قانون تجارت الکترونیك و قانون جرایم رایانه‌ای جمهوری اسلامی ایران، تعریفی از جریم رایانه‌ای ارائه نشده است که احتمال می‌رود دلیل آن، اختلافات مبنایی میان حقوقدانان از این مفهوم باشد. به طور کلی، آن دسته از جرایمی که با سوء استفاده از یك سامانه رایانه‌ای و برخلاف قانون واقع می‌شود، جرایم رایانه‌ای نام دارند؛ هر چند این دسته از جرایم را می‌توان شامل جرایم سنتی که به واسطه رایانه صورت می‌گیرد- از قبیل کلاهبرداری و سرقت- و نیز جرایم نوظهوری که با تولد رایانه پا به عرصه حیات گذاشته‌اند- مانند جرایم علیه صحت و تمامیت داده‌ها- دانست. در این پژوهش، مصادیق، ارکان قانونی، مادی و روانی و نیز مجازات هر یک از جرایم رایانه‌ای مورد بررسی قرار گرفته است.

واژگان کلیدی: جرایم رایانه‌ای، سیاست تقنینی، مجازات، جمهوری اسلامی ایران

---

۱. دانشجوی دکتری گروه حقوق خصوصی، دانشگاه آزاد اسلامی، اراک، ایران، soheilzolfaghari@yahoo.com

۲. کارشناس ارشد گروه مدیریت آموزشی، دانشگاه آزاد اسلامی، گرمسار، ایران، a.tavan22@yahoo.com

مقدمه

پیشرفت تکنولوژی، علم و دستیابی بشر به فناوری اطلاعات و استفاده از رایانه و پیدایش دنیای مجازی، دارای پیامدهای مثبت و منفی فراوانی برای بشر بوده که از جمله پیامدهای منفی آن، پیدایش جرایم رایانه‌ای است.

در مورد جرایم رایانه‌ای، تعاریف متعددی بیان شده که به برخی از آن‌ها اشاره می‌شود:

- پلیس جنایی فدرال آلمان در تعریفی از جرایم رایانه‌ای، این چنین اعلام داشته است: جرم رایانه‌ای دربرگیرنده همه اوضاع و احوال و کیفیاتی است که در آن، شکل‌های پردازش الکترونیك داده‌ها، وسیله ارتکاب یا هدف یك جرم قرار گرفته و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است. (دزیانی، ۱۳۷۳: ۱۵۸-۱۵۷)
- کمیته اروپایی مسائل جنایی در شورای اروپا در سال ۱۹۸۹ میلادی، گزارشی ارائه داد که در آن، یکی از متخصصان چنین تعریفی ارائه نموده است: هر فعل مثبت غیر قانونی که رایانه، ابزار یا موضوع جرم باشد؛ به عبارت دیگر هر جرمی که ابزار یا هدف آن، تأثیرگذاری بر عملکرد رایانه باشد. (همان)
- پروفسور شیک از حقوقدانان اتریشی بیان می‌دارد: جرم رایانه‌ای به هر عمل مجرمانه‌ای گفته می‌شود که در آن رایانه، وسیله یا هدف ارتکاب جرم باشد. (شیرزاد، ۱۳۸۸: ۳۵)
- در آمریکا جرم رایانه‌ای عبارت است از: هر اقدام غیر قانونی که با یک رایانه یا به کارگیری آن مرتبط باشد؛ هم‌چنین هر اقدامی که به هر ترتیب با رایانه مرتبط بوده و موجب ایجاد خسارت به بزه‌دیده شود و مرتکب از این طریق منافعی را تحصیل کند. (عمیدی، ۱۳۸۷: ۲۰)

- در کانادا جرایم رایانه‌ای این چنین بیان شده است: جرم رایانه‌ای شامل هر فعالیت مجرمانه‌ای است که دربرگیرنده کپی، استفاده، جابجایی، مداخله، دسترسی یا سوء استفاده از سامانه‌های رایانه‌ای، عملکرد رایانه، داده‌ها یا برنامه‌های رایانه است. (شریفی، ۱۳۷۹: ۸۰)

در این میان، در حقوق ایران نه در قانون تجارت الکترونیك و نه در قانون جرایم رایانه‌ای- مصوب سال ۱۳۸۸- هیچ تعریفی از این مفهوم ارائه نشده است. شاید دلیل آن، اختلافات مبنایی است که میان حقوقدانان از تعریف جرایم رایانه‌ای وجود دارد؛ با این وجود و به عنوان نمونه می‌توان این تعریف را ارائه نمود:

آن دسته از جرایمی که با سوء استفاده از یك سیستم رایانه‌ای برخلاف قانون ارتکاب می‌یابد، جرایم رایانه‌ای نام دارد؛ البته این دسته از جرایم را می‌توان شامل جرایم سنتی که به واسطه رایانه صورت می‌گیرد از قبیل کلاهبرداری، سرقت و نیز جرایم نوظهوری مانند جرایم علیه صحت و تمامیت داده‌ها که با تولد رایانه پا به عرصه حیات گذاشته‌اند، دانست. (طارمی، ۱۳۸۶: ۸۸)

همان‌گونه که بیان شد، در حقوق ایران، تعریف جرایم رایانه‌ای به سکوت واگذار شده و در بیشتر موارد- تقریباً- همان تعریف ارائه شده از طرف سازمان همکاری و توسعه اقتصادی را پذیرفته‌اند. (پاکزاد، ۱۳۸۰: ۳۸)

بنابراین، در این تحقیق تلاش می‌شود مصادیق و ارکان تشکیل دهنده جرایم رایانه‌ای که در قانون جرایم رایانه‌ای- مصوب ۱۳۸۸- بیان شده، تبیین می‌شود.

جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

داده[1] در لغت به معنای اطلاعات، مفروضات، دانسته‌ها و سوابق آمده است. (حییم، ۱۳۳۷: ۱۲۵)

1. Data

داده در زبان فارسی ترجمه عبارت لاتین «دیتا» است و در اصطلاح، به هرگونه اطلاعاتی گفته می‌شود که از طریق دستگاه ورودی به درون رایانه وارد می‌شود تا عملیاتی روی آن به اجرا درآید که جمع آن‌ها داده‌ها است.

به عبارت دیگر، به اطلاعات خاصی که وارد رایانه می‌شوند تا پردازشی روی آن‌ها صورت گیرد، داده و به نتیجه‌ای که حاصل پردازش بر روی داده‌های خام باشد، اطلاعات گفته می‌شود. (شیرزاد، ۱۳۸۸: ۸۰-۷۰)

بر اساس بند- الف- ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷:

داده پیام[1] هر نمادی از واقعه، اطلاعات یا مفهومی است که با وسایل الکترونیکی، نوری یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.

بر اساس بند- و- همان قانون، سامانه رایانه‌ای[2]:

هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری- نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده پیام» عمل می‌کند.

بنابراین:

داده عبارت است از مجموعه‌ای از حروف، ارقام و هر گونه علامت، نشان و نماد که به وسیله رایانه مورد پردازش قرار می‌گیرد.

البته ممکن است داده‌ها در ابتدا برای انسان قابل فهم نباشد؛ اما پس از پردازش به وسیله رایانه، به حالات گوناگون از قبیل صوت، فیلم، متن و... درآمده و بدین وسیله برای انسان مفهوم شوند.

---

1. Data Message
2. Computer System

۱. دسترسی غیر مجاز

دسترسی غیر مجاز عبارت است از رخنه غیر قانونی به سامانه رایانه‌ای حفاظت شده (عالی‌پور، ۱۳۹۰: ۱۵۹) که رکن قانونی این جرم، ماده ۱ قانون جرایم رایانه‌ای است.

دسترسی غیر مجاز در حقوق کیفری سنتی همانند هیچ‌یک از جرایم نیست و از جمله جرایمی است که با پیدایش رایانه به وجود آمده و مادر بیشتر جرایم رایانه‌ای است؛ البته این جرم با هتک حرمت منزل یا ورود با قهر و غلبه به ملک دیگری (موضوع ماده ٦٩٤ قانون مجازات اسلامی) در حقوق کیفری سنتی، همسان است؛ اما تفاوت این است که در جرم موضوع ماده ٦٩٤ قانون مجازات اسلامی، نیازی نیست که منزل یا مسکن بسته یا حفاظت شده باشد و صرف ورود همراه با عنف و تهدید به منزل یا مسکن دیگری برای تحقق جرم، کافی است؛ اما در جرم دسترسی غیر مجاز لازم است که سامانه رایانه‌ای، ویژگی حفاظت‌شدگی را داشته باشد.

این جرم در مقایسه با جرایمی مانند کلاهبرداری رایانه‌ای، اخلال در سامانه و تروریسم سایبری به عنوان یک رفتار مقدماتی به شمار رفته و در اندازه شروع به جرم است که هنوز با نتیجه که در بردارنده زیان به دیگری است فاصله داشته و از این رو، آن را دروازه جرایم رایانه‌ای می‌دانند.

۱-۱- رکن مادی

- **موضوع جرم**

موضوع جرم، دسترسی غیر مجاز به داده یا سامانه‌های رایانه‌ای و مخابراتی است. داده بیشتر درون سامانه یا سامانه قرار دارد و شکستن محرمانگی سامانه، شکستن محرمانگی داده را به دنبال دارد.

سامانه‌های مخابراتی نیز یکی دیگر از موضوع‌های جرم است. داده‌ها و سامانه‌ها می‌توانند هم متعلق به اشخاص حقیقی و حقوقی باشند و هم متعلق به دولت باشند؛ لذا موضوع جرم در این‌جا، داده‌های سری نیست.

- **رفتار مرتکب**

دسترسی و بهره‌مندی از رایانه یا داده دیگری با شرط حفاظت سامانه به وسیله تدابیر امنیتی که دسترسی در معنای خاص آن، هک یا رخنه‌گری است، رفتار مرتکب در این جرم را تشکیل می‌دهد. شیوه‌های دسترسی، گوناگون است و بر تعداد آن افزوده می‌شود. شیوه باید به‌طور فنی و نرم‌افزاری باشد نه این‌که به صورت گفتاری و فریب جهت به دست‌آوردن رمز عبور باشد.

دسترسی، رفتاری است که از سوی مقنن منع شده است و مرتکب با انجام این رفتار، نهی قانونگذار را نادیده می‌گیرد؛ لذا دسترسی به صورت فعل است و نه ترک فعل؛ هم‌چنین، این جرم از جمله جرایم مطلق است و نیازی به نتیجه ندارد؛ یعنی صِرف دسترسی به داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی صرف‌نظر از ایجاد نتیجه، جرم است.

۱-۲- رکن روانی

مرتکب باید در دسترسی به داده یا سامانه عامد باشد؛ خواه این دسترسی از روی کنجکاوی و خواه به قصد ربودن داده یا از بین بردن آن بوده و این تفاوت، تنها می‌تواند در اندازه کیفر مؤثر باشد؛ هم‌چنین مرتکب باید بداند که از دارنده داده یا سامانه برای نقض تدابیر حفاظتی و ورود به سامانه اجازه نداشته است.

اگر مرتکب اجازه داشته یا به غیر مجاز بودن آگاهی نداشته، جرمی رخ نمی‌دهد و اگر در جایی اجازه دسترسی نداشته، ولی سامانه نیز به تدابیر امنیتی مجهز نبوده، باز هم مرتکب جرمی نشده است.

۱-۳- مجازات

طبق ماده ۱ قانون جرایم رایانه‌ای، مجازات این جرم حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات است.

۲. شنود غیر مجاز

شنود غیر مجاز هم‌چون دسترسی غیر مجاز، ناشی از عدم رضایت دارنده واقعی یا قانونی داده یا محتوای در حال انتقال است؛ هم‌چنین شرط غیر قانونی بودن نیز به شرط عدم رضایت اضافه می‌شود.

رکن قانونی این جرم، ماده ۲ قانون جرایم رایانه‌ای است که این جرم، همان تعرض به حریم ارتباطات به وسیله شنود سنتی و ضبط مکالمات تلفنی افراد را بیان می‌کند. (جلالی فراهانی، کنوانسیون جرایم سایبر، ۱۳۸۹: ۲۸)

۲-۱- رکن مادی

- **موضوع جرم**

موضوع جرم در شنود غیر مجاز، محتوا است. برای محتوا، ویژگی در حال انتقال پیش‌بینی شده است؛ یعنی این جرم، تنها داده‌های در حال رفت و آمد را در برمی‌گیرد و نسبت به داده‌های دیگر، شنود همان دسترسی است.

محتوای در حال انتقال باید در یک پیوند خصوصی میان دو یا چند نفر انجام گیرد تا شرط انتقال غیر عمومی مفهوم محرمانگی پیدا کند.

- **رفتار مرتکب**

در این جرم رفتار مرتکب، شنود یا همان دریافت محتواست؛ لذا میان شنود غیر مجاز و دسترسی غیر مجاز به جهت رفتار، تفاوتی وجود ندارد.

تفاوت عمده میان این دو جرم، در نوع داده‌ای است که مرتکب، آن را دریافت می‌کند؛ به این صورت که در دسترسی، دریافت داده‌های ذخیره شده و در شنود، دریافت محتوای در حال انتقال انجام می‌گیرد و هم‌چنین دسترسی، هم نسبت به داده است و هم سامانه؛ ولی شنود تنها نسبت به داده رخ می‌دهد؛ لذا رفتار فیزیکی در این جرم، فعل شنود کردن است و با ترك فعل محقق نمی‌شود.

- **رکن روانی**

رکن روانی جرم شنود غیر مجاز، رفتار عامدانه یعنی خواست شنود محتوا و داده‌های در حال انتقال و علم به غیر مجاز بودن شنود و نیز علم به ویژگی خصوصی بودن انتقال است.

- **مجازات**

مجازات پیش‌بینی شده برای جرم مزبور در ماده ۲ قانون جرایم رایانه‌ای، حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات است.

۳. جاسوسی رایانه‌ای

مقنن در قانون جرایم رایانه‌ای، گام‌های سه‌گانه زیر را برای جرم جاسوسی رایانه‌ای در نظر داشته است:

- دسترسی به سامانه‌های رایانه‌ای و مخابراتی که داده‌های سری در آن‌ها نگهداری می‌شود. (ماده ٤ قانون جرایم رایانه‌ای).
- دسترسی به داده‌های سری یا تحصیل یا شنود آن‌ها. (بند- الف- ماده ۳ همان قانون)
- در دسترس قرار دادن برای کسانی‌که شایستگی آگاهی از محتوای داده‌های سری را ندارند. (بند- ب- ماده ۳ همان قانون) یا در دسترس قرار دادن داده‌های سری یا افشای آن‌ها به دولت یا نهادهای بیگانه یا عاملان آن‌ها. (بند- ج- ماده ۳ همان قانون)

گام اول- دسترسی به سامانه‌های در بردارنده داده‌ها- و نیز گام دوم- دسترسی به خود داده‌های سری- در اصل همان جرم دسترسی غیر مجاز هستند؛ اما در این گام، شنود به دسترسی یا تحصیل نیز افزوده شده است؛ لذا دو جرم دسترسی غیر مجاز و شنود غیر مجاز، مبنا و پایه جاسوسی رایانه‌ای را تشکیل می‌دهند.

۳-۱- رکن مادی

- **موضوع جرم**

موضوع جرم جاسوسی رایانه‌ای، داده‌های سری است. مطابق تبصره ۱ ماده ۳ قانون جرایم رایانه‌ای، داده‌های سری داده‌هایی است که افشای آن‌ها به امنیت یا منافع ملی لطمه می‌زند.

- **رفتار مرتکب**

در مواد ۳، ٤ و ٥ قانون جرایم رایانه‌ای، پدیده جاسوسی رایانه‌ای مطرح شده که بر پایه پنج رفتار جداگانه بنا می‌شود که هریک، جرم جداگانه‌ای به شمار می‌رود:

- نقض تدابیر امنیتی سامانه‌های رایانه‌ای و مخابراتی در بردارنده داده‌های سری.
- دسترسی به داده‌های سری یا تحصیل یا شنود آن‌ها.
- در دسترس قرار دادن داده‌های سری برای اشخاص فاقد صلاحیت.
- افشا یا در دسترس قرار دادن داده‌های سری برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها.
- در دسترس قرار دادن غیر عمدی داده‌های سری برای اشخاص فاقد صلاحیت.

به بیان دیگر، جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشا، انتقال و استفاده از اسرار است؛ لذا فرد مرتکب جرم با دستیابی و فاش کردن این اسرار، ضرر سیاسی، نظامی، مالی، تجاری ایجاد کرده و امنیت ملی را با مخاطره مواجه می‌کند.

- **رکن روانی**

رفتارهای جاسوسی رایانه‌ای باید با عمد انجام گیرد؛ مگر آن‌چه که در ماده ٥ قانون جرایم رایانه‌ای آمده است- یعنی در اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی، موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها شوند که این امر نیز به طور غیر عمد رخ می‌دهد.

هم‌چنین مرتکب باید آگاه به سری بودن داده‌ها باشد و نیز در بندهای- ب و ج- ماده ۳ قانون جرایم رایانه‌ای، مرتکب باید آگاه به غیر صالح بودن یا عامل بیگانه بودن شخص نیز باشد.

در نقض تدابیر سامانه‌ای موضوع ماده ٤ قانون جرایم رایانه‌ای نیز مرتکب باید آگاه به این مسئله باشد که سامانه مورد نظر، سامانه‌ای است که داده‌های سری در آن نگهداری می‌شوند. در صورت ناآگاهی، جرم دسترسی غیر مجاز موضوع ماده ۱ قانون جرایم رایانه‌ای شکل گرفته است.

در انجام رفتارهای جاسوسی، نیازی به قصد خاص نیست؛ مگر در نقض تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی موضوع ماده ٤ قانون جرایم رایانه‌ای که مرتکب باید قصد دسترسی به داده‌های سری موضوع ماده ۳ قانون جرایم رایانه‌ای را داشته باشد.

- **مجازات**

مجازات جاسوسی رایانه‌ای عبارتند از:

مطابق ماده ۳ قانون جرایم رایانه‌ای: هرکس به طور غیر مجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

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 بیست میلیون ریال تا شصت میلیون ریال یا هر دو مجازات؛

در دسترس قرار دادن داده‌ی مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال؛

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

بر اساس ماده ٤ قانون جرایم رایانه‌ای: هرکس به قصد دسترسی به داده‌های سری، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

طبق ماده ٥ قانون جرایم رایانه‌ای: چنان‌چه مأموران دولتی که مسؤل حفظ داده‌های سری یا سامانه‌های مربوط هستند و به آن‌ها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آن‌ها قرار گرفته 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 نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

۱. جعل رایانه‌ای

رکن قانونی جرم جعل رایانه‌ای، ماده ٦ قانون جرایم رایانه‌ای است. بستر انجام این جرم، فضای سایبر است که فضایی غیر مادی و ناملموس است و توسط رایانه‌ها و شبکه‌های رایانه‌ای به‌وجود آمده و دنیایی مجازی در کنار دنیای واقعی به وجود آورده است.

فضای سایبر همان فضای مجازی بی‌کرانی است که از طریق اتصال شبکه‌های رایانه‌ای به هم، به وجود آمده است. (فضلی، ۱۳۸۹: ۱۷)

به لحاظ فنی، شبکه رایانه‌ای در ابتدایی‌ترین سطح خود شامل دو رایانه است که به وسیله کابل به یکدیگر متصل شده‌اند؛ به گونه‌ای که بتوانند از داده‌ها به طور مشترک استفاده نمایند. این ارتباط در حال حاضر از طریق کابل مسی است؛ البته ارتباط رایانه‌ها با یکدیگر ممکن است از طریق کابل خطوط تلفن نباشد، بلکه می‌توان از فیبر نوری، مایکروویو، اشعه مادون قرمز و ماهواره‌های ارتباطی نیز برای ارتباط استفاده کرد.

بنابراین، همه رفتارهای پیش‌بینی شده در این ماده باید از رهگذر کنش‌های رایانه‌ای و در بستر رایانه و مخابرات انجام شود؛ لذا اگر کسی داده رایانه‌ای را چاپ کند یا از روی صفحه نمایشگر رایانه عکس بگیرد و سپس بر روی کاغذ چاپ شده تغییراتی ایجاد کند، جرم جعل رایانه‌ای محقق نیست و ممکن است با وجود تمام شرایط، جعل سنتی باشد. هم‌چنین انجام رفتارهای موضوع جعل رایانه‌ای، باید به‌صورت غیر مجاز باشد؛ یعنی یا اجازه نداشته یا برخلاف قانون و قرارداد باشد.

۱-۱- رکن مادی

- موضوع جرم

موضوع جرم جعل رایانه‌ای، داده، حامل داده یا جای انباشت داده مانند علامت، کارت حافظه و تراشه است. داده‌های موضوع جرم جعل رایانه‌ای باید قابلیت استناد داشته باشند و به همین دلیل نیازی به ایراد ضرر برای تحقق این جرم نیست و اگر زیانی حاصل شود، می‌تواند موجب افزایش مجازات مرتکب شود.

- رفتار مرتکب

در بند- الف- ماده ٦ قانون جرایم رایانه‌ای، دو بخش جداگانه در انجام جرم جعل رایانه‌ای پیش‌بینی شده است:

تغییر یا ایجاد داده‌های قابل استناد که تغییر باید در داده‌های قابل استناد انجام شود و ایجاد نیز باید پدید آوردن داده‌ای باشد که توانایی استنادپذیری داشته باشد.

ایجاد یا وارد کردن متقلبانه داده به آن‌ها.

بند- ب- همان ماده، تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علائم به آن‌ها را به عنوان رفتار مجرمانه برای جرم جعل رایانه‌ای مطرح می‌کند.

در عین حال، به نظر می‌رسد رفتارهای مندرج در بند- ب- تفاوتی با بند- الف- ندارد و نیازی به آوردن بند- ب- نبود؛ اما برای بند- ب- قانونگذار شرط استنادپذیری را بیان نکرده است؛ لذا وارد کردن، تغییر، محو یا موقوف‌سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور و هدف سیاسی و اقتصادی صورت می‌گیرد که همان جعل رایانه‌ای داده‌هاست.

در جعل رایانه‌ای، عمل ارتکابی بر داده‌ها اثر می‌گذارد؛ با این تفاوت که داده، ماهیت اسناد عادی را ندارد.

۱-۲- رکن روانی

عمد مرتکب در پدید آوردن و دگرگونی در داده‌های قابل استناد و سایر رفتارهای مندرج در ماده، رکن روانی این جرم را تشکیل می‌دهد.

۱-۳- مجازات

بر اساس ماده ٦ قانون جرایم رایانه‌ای، کسی‌که مرتکب جرم جعل رایانه‌ای می‌شود، به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم می‌شود.

۲. استفاده از داده‌های مجعول

ماده ۷ قانون جرایم رایانه‌ای، رکن قانونی جرم استفاده از داده‌های مجعول به شمار می‌رود.

۲-۱- رکن مادی

- **موضوع جرم**

داده، کارت‌های الکترونیکی و تراشه‌ها، موضوع رفتار مجرمانه در این جرم هستند.

- **رفتار مرتکب**

استفاده از داده‌های مجعول که باید در فضای سایبر، سامانه‌های رایانه‌ای و مخابراتی یا داده‌برها و کارت‌های حافظه انجام شود، رفتار مرتکب در جرم استفاده از داده مجعول را

تشکیل می‌دهد؛ لذا اگر کسی در فضای بیرونی و فیزیکی از داده‌های مجعول استفاده کند، این جرم رخ نمی‌دهد.

به عنوان مثال؛ اگر فردی مرتکب جعل رایانه‌ای شود و متن یک قرارداد الکترونیکی را تغییر دهد یا چنین قراردادی مجعولی را بیابد و سپس آن را چاپ کرده و به نهاد یا کسی ارائه دهد، از آن‌جا که بهره‌برداری از آن در فضای بیرونی انجام شده، مرتکب جرم استفاده از سند مجعول شده است؛ نه جرم استفاده از داده‌های مجعول.

۲-۲- رکن روانی

علم و آگاهی مرتکب به جعلی بودن، برجسته‌ترین عنصر روانی این جرم است؛ هم‌چنین لازم است مرتکب، توان استفاده از داده‌های مجعول عمد نیز داشته باشد.

۲-۳- مجازات

بر اساس ماده ۷ قانون جرایم رایانه‌ای، هرکس با علم به مجعول بودن داده‌ها، کارت‌ها یا تراشه‌ها از آن‌ها استفاده کند، به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم می‌شود.

۳. خرابکاری رایانه‌ای

خرابکاری رایانه‌ای، دربردارنده هر رفتاری است که داده را به طور کلی یا جزئی از میان ببرد یا کارکرد داده یا سامانه را به هر نحو برهم بزند. (عالی‌پور، ۱۳۹۰: ۲۱۶)

استفاده از عنوان تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی برای مبحث دوم از فصل یکم در بخش نخست قانون جرایم رایانه‌ای برای این است که چهار عنوان مجرمانه تخریب، اخلال، ممانعت از دستیابی و تروریسم سایبری را دربرگیرد که با توجه به نزدیکی ویژگی‌های جرایم تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی، در یک بند بررسی می‌شوند.

تخریب به معنای از بین بردن تمام یا قسمتی از یک داده و اخلال در معنای ایجاد آشفتگی و ناتوانی در کارکرد داده است که ماده ۸ قانون جرایم رایانه‌ای، به جرم‌انگاری این اعمال پرداخته است.

۳-۱- رکن مادی

- موضوع جرم

موضوع جرم، تخریب و اخلال در داده‌های متعلق به دیگری است؛ خواه مالیت داشته باشد و خواه نداشته باشد، خواه شخصی باشد و خواه دولتی؛ اما اگر موضوع جرم، داده‌های دولتی باشد، مطابق بند- ج- ماده ۲۶ قانون جرایم رایانه‌ای، مجازات مرتکب، تشدید خواهد شد.

- رفتار مرتکب

چهار رفتار حذف، تخریب، مختل و غیر قابل پردازش کردن، در ماده ۸ قانون جرایم رایانه‌ای پیش‌بینی شده است که ذیل دو عنوان تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی قرار می‌گیرند.

دو رفتار حذف و تخریب نسبت به خود داده و دو رفتار مختل کردن و غیر قابل پردازش نمودن، نسبت به کارکرد و توانایی داده رخ می‌دهد. هر چهار رفتار نیز باید در فضای سایبر رخ دهد که این مسئله با به کاربردن عبارت سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده در متن ماده روشن می‌شود؛ هم‌چنین رفتارهای مجرمانه نیز باید رایانه‌ای و سایبری باشد.

به عنوان مثال؛ اگر کسی به قصد از بین بردن داده‌های دیگری، رایانه‌اش را از بلندی پرت کند یا آن را بسوزاند یا لوح فشرده را بشکند یا آن را بخراشد یا سنگ روی حامل داده بزند، هیچ‌یک تخریب یا اخلال رایانه‌ای نیست؛ بلکه حسب مورد، تخریب یا اخلال سنتی است.

۳-۲- رکن روانی

علم و عمد در انجام رفتارهای مرتکب، رکن روانی جرم را تشکیل می‌دهد؛ هم‌چنین جرم تخریب و اخلال داده‌های رایانه‌ای، باید به طور غیر مجاز انجام گیرند و مرتکب، آگاه به غیر مجاز بودن باشد.

بر این اساس، اگر رفتارهای موضوع ماده مذکور با اجازه دارنده آن باشد، جرمی در کار نخواهد بود و میان شخص حقوقی، حقیقی و دولت تفاوتی نیست.

۳-۳- مجازات

ماده ۸ قانون جرایم رایانه‌ای، برای مرتکب جرم مزبور از شش ماه تا دو سال حبس یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات در نظر گرفته شده است.

٤. اخلال در سامانه‌های رایانه‌ای یا مخابراتی

ماده ۹ قانون جرایم رایانه‌ای، به بیان این جرم پرداخته است.

٤-۱- رکن مادی

- **موضوع جرم**

سامانه ممکن است از آن شخص حقیقی، حقوقی یا نهادها و سازمان‌های دولتی باشد که اخلال در سامانه‌های دولتی، سبب تشدید مجازات می‌گردد.

- **رفتار مرتکب**

در ماده مذکور، دو نوع رفتار پیش‌بینی شده است:

رفتارهای احصایی که شامل از کار انداختن و مختل نمودن می‌شود.

رفتارهای تمثیلی که در صدر ماده آمده که عبارتند از وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب و مانند آن‌ها.

رفتارهای تمثیلی بر روی سامانه‌ها رخ نمی‌دهند؛ بلکه بر روی داده یا موج انجام می‌شوند و سپس به اخلال می‌انجامند. از کار انداختن و مختل نمودن نیز بر روی سامانه‌های رایانه‌ای و مخابراتی انجام می‌شوند.

٤-۲- رکن روانی

مرتکب جرم اخلال در سامانه‌ها، رفتار خویش را باید عامدانه انجام داده و به موضوع جرم آگاهی داشته باشد.

به عبارت دیگر، هم نسبت به این‌که سامانه از آ دیگری یا دولت است و هم نسبت به غیرمجاز بودن عمل خویش، آگاه باشد.

٤-۳- مجازات

برای جرم موضوع ماده ۹ قانون جرایم رایانه‌ای، حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات، مقرر گردیده است.

۵. ممانعت از دسترسی

ممانعت از دسترسی در مفهوم گسترده، شامل هر رفتاری است که مانع دستیابی کاربر یا مشترک مجاز به سامانه‌ها و داده‌ها شود. (عالی‌پور، ۱۳۹۰: ۲٦٦) رکن قانونی این جرم نیز ماده ۱۰ قانون جرایم رایانه‌ای است.

۵-۱- رکن مادی

- موضوع جرم

بر اساس ماده‌ی ۱۰ قانون جرایم رایانه‌ای، موضوع این جرم، داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی است.

- رفتار مرتکب

در ماده مذکور، اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذر واژه‌ها، رمزنگاری داده‌ها که مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی شود، جرم‌انگاری شده است.

۵-۲- رکن روانی

دارنده داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی و هم متصرف قانونی آن‌ها و نیز اشخاصی که قانوناً یا به دستور دادرس، صلاحیت دسترسی به داده‌ها یا سامانه‌ها را دارند،

مجاز به دسترسی است؛ اما اگر ممانعت از دسترسی، به طور غیر مجاز، عامدانه و بر اساس علم و آگاهی مرتکب صورت پذیرد، این جرم محقق می‌گردد.

۵-۳- مجازات

مجازات جرم مقرر در ماده ۱۰ قانون جرایم رایانه‌ای، حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات است.

٦. تروریسم سایبری

تروریسم سایبری، مجموعه‌ای از اقدامات را شامل می‌شود که افراد خاصی با نیات خاص مرتکب می‌شوند و به لحاظ خسارات مادی و لطمات جانی که به بار می‌آورند، از سوی همه کشورها در زمره شدیدترین جرایم قرار گرفته اند. (جلالی فراهانی، ۱۳۸۹: ۱۷٦)

ماده‌ی ۱۱ قانون جرایم رایانه‌ای بدون نام بردن از اقدام تروریستی یا تروریسم، به جرمی اشاره دارد که بسیار نزدیک به تروریسم سایبری است و آن، اخلال سامانه‌های رایانه‌ای و مخابراتی همراه با قصد خطر انداختن آسایش و امنیت عمومی است.

٦-۱- رکن مادی

- موضوع جرم

موضوع جرم تروریسم سایبری، سامانه‌های رایانه‌ای و مخابراتی است که برای ارائه خدمات ضروری عمومی و رفع نیازهای حیاتی شهروندان است.

موارد مذکور در ماده ۱۱ مانند خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری از باب تمثیل بیان شده‌اند.

- رفتار مرتکب

رفتارهای موضوع ماده مذکور، همان رفتارهای پیش‌بینی شده در مواد ۸ (حذف، تخریب، مختل و غیر قابل پردازش کردن)، ۹ (از کار انداختن و مختل کردن کارکرد) و ۱۰ (مانع شدن از دسترسی) قانون جرایم رایانه‌ای است.

۶-۲- رکن روانی

مرتکب این جرم، باید رفتارهای پیش‌بینی شده در مواد ۸، ۹ و ۱۰ قانون جرایم رایانه‌ای را از روی عمد انجام داده و قصد او، به خطر انداختن آسایش و امنیت عمومی باشد. از سوی دیگر، باید آگاه باشد که رفتار خود را بر روی سامانه‌هایی انجام می‌دهد که خدمات ضروری عمومی ارائه می‌دهند.

۶-۳- مجازات

ماده ۱۱ قانون جرایم رایانه‌ای، مجازات مرتکب این جرم را حبس از سه تا ده سال مقرر نموده است.

جرایم قابل ارتکاب از طریق رایانه

در این بخش از نوشتار، به جرایمی پرداخته می‌شود که رایانه، وسیله ارتکاب جرم است.

در فصل سوم قانون جرایم رایانه‌ای، دو عنوان سرقت و کلاهبرداری، در فصل چهارم، جرایم علیه عفت و اخلاق عمومی و فصل پنجم، هتک حیثیت و نشر اکاذیب مطرح شده است.

۱. جرایم مالی رایانه‌ای

۱-۱- سرقت رایانه‌ای

سرقت رایانه‌ای در ماده ۱۲ قانون جرایم رایانه‌ای پیش‌بینی شده که یک جرم رایانه‌ای محض است؛ چرا که ربودن داده در جایی‌که عین داده در جای خود باقی است، مانند جاسوسی و شنود غیرمجاز که بر ضد محرمانگی داده رخ می‌دهد و در جایی که به وسیله برش، عین داده از سامانه برداشته می‌شود، همانند تخریب داده است؛ لذا در دسته جرایمی قرار دارد که رایانه، هدف یا موضوع جرم است و نباید در کنار کلاهبرداری که رایانه در آن نقش ابزار انجام جرم را دارد، آورده شود.

۱-۱-۱- رکن مادی

- موضوع جرم

موضوع جرم سرقت رایانه‌ای، داده است. این داده به تعبیر ماده ۱۲ قانون جرایم رایانه‌ای باید متعلق به دیگری باشد؛ خواه داده‌ها دارای ارزش مالی باشند مانند یک فرمول و خواه نباشند مانند یک مقاله پذیرفته شده و خواه دارنده داده خودش آن‌ها را پدید آورده باشد مانند متن یک کتاب یا این‌که آن داده را از دیگری خریداری نموده یا از طریق قانونی به دست آورده باشد.

داده‌ای که متعلق به دیگری است، باید در رایانه او یا جایی که به طور قانونی مکان قرار گرفتن داده‌های آن فرد است، باشد. بنابراین اگر کسی نوشته دیگری را که به طور آزاد در اینترنت موجود است، بارگذاری کرده و دریافت دارد، سارق نیست؛ ولی اگر کسی مقاله دیگری را از رایانه وی برباید- حتی اگر متن آن مقاله در اینترنت و به طور آزاد در دسترس باشد- عمل وی قابل مجازات است.

- رفتار مرتکب

در سرقت رایانه‌ای همانند سرقتِ سنتی، ربودن شرط است؛ آن‌چه مفهوم ربایش را می‌سازد، دست‌اندازی به مال دیگری یا از آن خود کردن بدون خشنودی دارنده آن است. همین که کسی مال دیگری را بدون رضایت وی به دست آورد، رفتارش سرقت است.

ربودن داده به معنای دست‌اندازی به داده دیگری است که با روگرفتن- کپی- یا برش- کات- است. روگرفت یا کپی باید در فضای سایبر انجام گیرد؛ اگر کسی به سامانه دیگری که با تدابیر امنیتی نیز محافظت شده، نفوذ کرده و داده یا اطلاعات را یافته و آن‌ها را بر روی کاغذ بنویسد، مرتکب جرم دسترسی غیر مجاز شده است نه سرقت رایانه‌ای؛ برش داده باید به نحوی صورت گیرد که فرد مرتکب، داده را از جایگاه خود برداشته و به جای دیگری اعم از رایانه یا وسایل حامل داده ارسال کند.

اگر مرتکب بدون آن‌که خودش از داده شخص دیگری بهره‌ای ببرد، آن را حذف کند، رفتارش مصداق تخریب است؛ اما اگر در برش، مکان داده جابه‌جا شود به طوری که عین داده در اختیار دارنده آن نباشد، جرم سرقت رایانه‌ای محقق می‌شود.

ربایش رایانه‌ای که در قانون جرایم رایانه‌ای مطرح شده، نسبت به ربایش در فضای بیرونی نگاهی ندارد؛ به عنوان مثال، اگر کسی به قصد ربودن اطلاعات دیگری در خیابان، «تبلت» وی را برباید یا به کنار میز رایانه‌اش رفته و چندین لوح فشرده را بردارد و از آن خود کند؛ هر چند موضوع جرم، داده است، ولی ربایش سایبری انجام نشده؛ بلکه این سرقت از نوع سرقت سنتی است.

۱-۱-۲- رکن روانی

مرتکب باید آگاه باشد که داده از آن دیگری است. مرتکب ربایش رایانه‌ای باید عمد در رفتار خویش داشته باشد که این عمد، می‌تواند به صورت روگرفت یا بُرش داده باشد.

۱-۱-۳- مجازات

مجازات تعیین شده برای جرم سرقت رایانه‌ای، مستفاد از ماده ۱۲ قانون جرایم رایانه‌ای، برای روگرفتن- کپی- از داده‌ها، جزای نقدی از یک میلیون ریال تا بیست میلیون ریال و در حالت برش داده‌ها، حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات خواهد بود.

۱-۲- کلاهبرداری رایانه‌ای

کلاهبرداری، یکی از مهم‌ترین جرایم علیه اموال است که برخی از آن، به عنوان بحران قرن بیستم نام برده‌اند. (میرمحمدصادقی، ۱۳۷۹: ۲۸)

کلاهبرداری رایانه‌ای همانند کلاهبرداری سنتی، جرمی مقید به حصول نتیجه مجرمانه است و باید به واسطه سوء استفاده از رایانه از طریق افعالی نظیر وارد کردن،

تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا اختلال در سامانه رایانه‌ای، وجه، مال، منفعت، خدمات یا امتیازات مالی عاید مرتکب یا دیگری شود.

۱-۲-۱- رکن مادی

- **موضوع جرم**

موضوع جرم کلاهبرداری رایانه‌ای، وجه، مال، منفعت، خدمات و امتیازات مالی است. کلاهبرداری رایانه‌ای به لحاظ موضوع، از کلاهبرداری سنتی عام‌تر است و علاوه بر وجه و مال، منفعت، خدمات و امتیازات مالی را نیز در بر می‌گیرد.

- **رفتار مرتکب**

با توجه به قید واژه «هر کس» همانند کلاهبرداری سنتی، هر شخصی می‌تواند مرتکب این جرم باشد. کلاهبرداری رایانه‌ای، جرمی مرکب است؛ رفتار اول که به طور تمثیلی در ماده ۱۳ قانون جرایم رایانه‌ای به آن اشاره شده، اعمالی چون وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل نمودن سامانه است.

این رفتارها باید به طور غیر مجاز صورت گیرند و اگر با اجازه انجام شوند، کلاهبرداری رایانه‌ای رخ نداده؛ هر چند که به تحصیل مال به طور غیر قانونی منجر شود. رفتار دوم نیز تحصیل اعم از دریافت واقعی، مجازی یا منظور کردن اعتبار مالی برای خود است.

رفتارهای فیزیکی و تحصیل باید در فضای سایبر صورت پذیرد؛ اگر فرد از رایانه و فضای سایبر- تنها- به عنوان وسیله ارتکاب جرم کلاهبرداری استفاده نماید، مانند این‌که از طریق تبلیغ ناروا در وبلاگ خود، دیگری را فریفته و خود را دارنده مؤسسه اعزام دانشجو به خارج معرفی و با دادن شماره حساب، کاربر یا کاربرانی را فریب دهد تا پولی به حسابش واریز یا در محیط بیرون پول یا مال را دریافت دارد، کلاهبرداری سنتی انجام داده است نه رایانه‌ای.

۱-۲-۲- رکن روانی

رکن روانی کلاهبرداری شامل عمد در رفتار و تحصیل مال یا منفعت و آگاهی مرتکب نسبت به تعلق مال، منفعت، خدمات یا امتیازات مالی به دیگری است؛ هم‌چنین مرتکب باید بداند که انجام این رفتار، غیر قانونی بوده است.

۱-۲-۳- مجازات

مجازات تعیین شده برای جرم کلاهبرداری رایانه‌ای، علاوه بر رد مال به صاحب آن، حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات می‌باشد.

۲. جرایم علیه عفت و اخلاق عمومی

۲-۱- هرزه‌نگاری رایانه‌ای

هرزه‌نگاری به مجموعه‌ای از رفتارهای مجرمانه گفته می‌شود که شامل تولید، طراحی، ارائه، انتشار و مورد معامله قرار دادن محتویات شنیداری و دیداری اعم از تصویر، نوشته و صوت است که عفت عمومی را جریحه‌دار می‌سازد. (عالی‌پور، ۱۳۹۰: ۲۹٤) ماده ۱٤ قانون جرایم رایانه‌ای، رکن قانونی جرم مزبور به‌شمار می‌رود.

۲-۱-۱- رکن مادی

- **موضوع جرم**

موضوع جرم هرزه‌نگاری، محتوایی است که به صورت غیر اخلاقی درآمده است. محتویات هرزه به دو دسته مستهجن و مبتذل تقسیم می‌شوند.

مطابق تبصره ۱ ماده ۱٤ قانون جرایم رایانه‌ای، آثار مبتذل به آثاری اطلاق می‌شود که دارای صحنه‌ها و صور قبیحه باشد؛ هم‌چنین بر اساس تبصره ٤ ماده ۱٤ قانون جرایم رایانه‌ای، محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیر واقعی یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد، اندام تناسلی یا آمیزش و عمل جنسی انسان است.

- **رفتار مرتکب**

رفتارهای پیش‌بینی شده در ماده ١٤ قانون جرایم رایانه‌ای به دو گروه تقسیم می‌شوند:

رفتارهایی که بدون قصد خاص، مستحق کیفر هستند؛ این رفتارها عبارتند از انتشار، توزیع یا معامله.

رفتارهایی که به صورت مشروط قابل مجازاتند که شامل تولید، ذخیره و نگهداری می‌شوند. سه رفتار اخیر به خودی خود قابل مجازات نیستند؛ مگر این‌که همراه با قصد تجارت یا افساد، انجام شوند.

همه رفتارهای شش‌گانه باید در محیط سایبر رخ دهند؛ و الا اگر هر یک از این رفتارها در فضای فیزیکی رخ دهد، باید مطابق مقررات کیفری دیگری با آن‌ها برخورد نمود.

٢-١-٢- رکن روانی

برای تحقق جرم مذکور در ماده ١٤ قانون جرایم رایانه‌ای، لازم است که مرتکب در انجام شش رفتار گفته شده عمد داشته باشد و برای سه رفتار تولید، ذخیره و نگهداری، قصد تجارت یا افساد نیز نیاز است؛ هم‌چنین لازم است که مرتکب به رفتار مجرمانه‌ای که نسبت به محتویات مستهجن یا مبتذل انجام می‌دهد، آگاهی داشته باشد.

٢-١-٣- مجازات

بر اساس ماده ١٤ قانون جرایم رایانه‌ای، مرتکب جرم هرزه‌نگاری رایانه‌ای، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

٢-٢- معاونت در هرزه‌نگاری رایانه‌ای

در راستای حمایت از بزه‌دیدگان، بند- الف- ماده ١٥ قانون جرایم رایانه‌ای، معاونت در دسترسی به محتویات هرزه و بند- ب- نیز معاونت در انجام یا آموزش جرم را به عنوان جرمی مستقل، پیش‌بینی نموده است.

۲-۲-۱- رکن مادی

- **موضوع جرم**

بر اساس صدر ماده ۱۵ قانون جرایم رایانه‌ای، موضوع این جرم، سامانه‌های رایانه‌ای، مخابراتی یا حامل‌های داده است.

- **رفتار مرتکب**

بیشتر رفتارهای پیش‌بینی شده در تبصره ماده ۱۵ قانون جرایم رایانه‌ای، همان رفتارهایی است که در ماده ۱۲۶ قانون مجازات اسلامی مصوب ۱۳۹۲ در قالب معاونت در جرم پیش‌بینی شده است. این رفتارها عبارتند از ترغیب، تهدید، تطمیع، تحریک، فریب دادن، تسهیل شیوه دستیابی و آموزش دادن.

تمامی این رفتارها باید از طریق سامانه‌های رایانه‌ای، مخابراتی یا حامل‌های داده در فضای سایبر صورت گیرند. این رفتارها مطلق بوده و نیاز نیست افرادی را که فرد مرتکب، تحریک، ترغیب و... نموده است، به محتویات مستهجن یا مبتذل دست یابند.

۲-۲-۲- رکن روانی

فرد مرتکب باید عمد و قصد خاص دستیابی افراد به محتویات مستهجن یا مبتذل در انجام رفتارهای مذکور را داشته و نیز نسبت به محتوای هرزه و نسبت به کسی که دستیابی محتوای هرزه را آموزش می‌دهد یا رفتارهای دیگر را انجام می‌دهد، آگاه باشد.

علاوه بر این لازم است که مرتکب برای ارتکاب هر یک از جرایم منافی عفت، استعمال مواد مخدر و روان‌گردان، خودکشی، انحرافات جنسی یا اعمال خشونت‌آمیز، رفتارهای مذکور را نسبت به افراد مدنظر خود انجام دهد.

۲-۲-۳- مجازات

به استناد صدر ماده ۱۵ قانون جرایم رایانه‌ای، کیفر پیش‌بینی شده برای جرم معاونت در هرزه‌نگاری رایانه‌ای، حبس از نود و یک روز تا یک سال یا جزای نقدی از

پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات است؛ به نحوی که اگر این اعمال را درخصوص محتویات مبتذل مرتکب شود، موجب جزای نقدی از دو میلیون ریال تا پنج میلیون ریال می‌شود.

۳. جرایم علیه شخصیت معنوی

جرایم علیه شخصیت معنوی به رفتارهایی گفته می‌شود که روان آدمی را هدف می‌گیرند. (عالی‌پور، ۱۳۹۰: ۳۱۲)

جرایم علیه اشخاص در فضای سایبر منصرف از جرایم علیه تمامیت جسمانی شخص است. در فضای سایبر که محل حضور ذهن فرد است، جرایم علیه اشخاص با روان و شخصیت معنوی آنان ارتباط می‌یابد.

۳-۱- تغییر یا تحریف محتوای دیگری

رکن قانونی این جرم، ماده ١٦ قانون جرایم رایانه‌ای است.

۳-۱-۱- رکن مادی

- **موضوع جرم**

موضوع جرم مذکور در ماده ١٦ قانون جرایم رایانه‌ای، تغییر یا تحریف محتوا، فیلم، صوت یا تصویر دیگری است.

- **رفتار مرتکب**

ماده ١٦ قانون جرایم رایانه‌ای برای رفتار مرتکب، دو حالت را مطرح نموده است:

حالتی که فرد تغییر یا تحریف محتوا را انجام داده و محتوای تغییر یا تحریف یافته را منتشر کند و این یعنی مرتکب جرم مرکبی شده است؛ لذا صِرف تغییر یا تحریف محتوا تا زمانی‌که آن‌ها را انتشار نداده، برای تحقق این جرم کافی نیست.

حالتی که فرد، محتوای تغییر یا تحریف یافته را با علم به تغییر یا تحریف منتشر می‌کند و این یعنی جرمی ساده رخ داده است.

جرم موضوع ماده ۱۶، مقید به نتیجه است؛ هر دو حالت رفتاری یعنی تغییر، تحریف، انتشار و نیز انتشار با علم به تغییر و تحریف- عرفاً- باید موجب هتک حیثیت گردد. ملاک تشخیص هتک حیثیت نیز عرف وابسته به شرایط زمان و مکان است.

۳-۱-۲- رکن روانی

در حالت اول که فرد، محتویات مربوط به دیگری را تغییر یا تحریف داده و سپس آن‌ها را منتشر نموده است، باید در رفتار خویش عامد باشد؛ علاوه بر این، مرتکب باید آگاهی داشته باشد که فیلم، صوت یا تصویر متعلق به دیگری است.

در حالت دوم، فرد باید عمد در انتشار محتوای تغییر یافته داشته و هم‌چنین بداند که فیلم، صوت یا تصویر به دیگری تعلق دارد و آگاه به تغییر یا تحریف محتوا باشد.

۳-۱-۳- مجازات

کیفر پیش‌بینی شده در ماده ۱۶ قانون جرایم رایانه‌ای، حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات است و مطابق تبصره همان ماده، اگر تغییر یا تحریف به صورت مستهجن باشد، حداکثر هر دو مجازات مقرر، کیفر مرتکب خواهد بود.

۳-۲- انتشار اسرار خصوصی و محتویات خانوادگی

ماده ۱۷ قانون جرایم رایانه‌ای به موضوع انتشار اسرار خصوصی و محتویات خانوادگی که جرمی ضد حریم خصوصی اشخاص است، پرداخته است.

بند- الف- ماده ۲ دستورالعمل‌های اروپایی حمایت از داده‌های شخصی مصوب ۱۹۹۲ میلادی، در تعریف داده شخصی اعلام می‌کند:

داده شخصی عبارت است از هر گونه اطلاعات مربوط به یک شخص با هویت مشخص یا قابل شناسایی. شخص قابل شناسایی نیز کسی است که مستقیم یا غیر مستقیم- به ویژه از طریق مراجعه به یک شماره تشخیص هویت یا مراجعه

به چند عامل خاص درباره هویت فیزیکی، روانی، ذهنی، اقتصادی، فرهنگی، اجتماعی یا خانوادگی- قابل شناسایی باشد.

۳-۲-۱- رکن مادی

- **موضوع جرم**

موضوع جرم ماده ۱۷ قانون جرایم رایانه‌ای، صوت، تصویر، فیلم خصوصی و خانوادگی یا اسرار دیگری است که سردسته محتوای خصوصی، خانوادگی و سری را تشکیل می‌دهند.

- **رفتار مرتکب**

دو رفتار انتشار و در دسترس قرار دادن، برای جرم موضوع ماده فوق پیش‌بینی شده است. این دو رفتار باید غیر قانونی و بدون رضایت دارنده صوت، تصویر، فیلم یا اسرار باشد. این جرم، مقید به نتیجه است که عبارت است از ضرر یا هتک حیثیت دارنده و معیار سنجش ضرر یا هتک حیثیت نیز عرف است.

۳-۲-۲- رکن روانی

مرتکب باید رفتارهای پیش‌بینی شده در ماده ۱۷ قانون جرایم رایانه‌ای را عمداً و با اراده آزاد خود انجام داده باشد؛ هم‌چنین آگاه باشد که صوت، تصویر، فیلم خصوصی و خانوادگی یا اسرار، متعلق به دیگری است.

۳-۲-۳- مجازات

مجازات مقرر برای جرم انتشار اسرار خصوصی و محتویات خانوادگی، برابر ماده ۱۷ قانون جرایم رایانه‌ای، حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات است.

۳-۳- نشر اکاذیب

ماده ۱۸ قانون جرایم رایانه‌ای، نشر اکاذیب در فضای سایبر را جرم‌انگاری نموده است.

۳-۳-۱. رکن مادی

- **موضوع جرم**

موضوع جرم، امنیت فردی و همگانی است. امنیت فردی در جایی است که رفتار مرتکب نسبت به اشخاص با قصد اضرار صورت می‌گیرد و در جایی‌که نسبت به مقامات و حتی اشخاص حقوقی با قصد تشویش اذهان عمومی صورت گیرد، امنیت همگانی لطمه می‌بیند.

- **رفتار مرتکب**

در ماده ۱۸ قانون جرایم رایانه‌ای سه رفتار مطرح است:

- نشر اکاذیب در فضای سایبر؛
- در دسترس دیگران قرار دادن محتوای دروغ؛
- نسبت دادن یک امر یا رخداد دروغ و خلاف حقیقت به دیگری.

تفاوت انتشار دروغ با نسبت دادن دروغ به دیگری، در این است که انتشار دروغ به طور کلی نسبت به شخص خاصی نیست؛ اما در نسبت دادن یک شخص حقیقی، حقوقی یا یک مقام شناخته شده مدنظر است.

این جرم، مقید به نتیجه خاصی نیست؛ یعنی با وجود سایر شرایط اعم از این‌که ضرر مادی یا معنوی به دیگری وارد شود یا خیر، جرم محقق می‌شود.

۳-۳-۲- رکن روانی

عمد مرتکب و اراده آزاد وی در تحقق جرم فوق الزامی است و علاوه بر آن، ضروری است رفتارهای سه‌گانه را به قصد اضرار به غیر و تشویش اذهان عمومی یا مقامات رسمی انجام دهد. آگاهی به مقام شخص و آگاهی به خلاف حقیقت بودن اقدام وی نیز جزو دیگری از رکن روانی است.

۳-۳-۳- مجازات

ماده ۱۸ قانون جرایم رایانه‌ای، مجازات حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات را برای جرم نشر اکاذیب تعیین نموده است.

۴. سایر جرایم رایانه‌ای

فصل هفتم از بخش یک قانون جرایم رایانه‌ای با عنوان سایر جرایم، به تشریح جرایم پایه‌ای پرداخته است که به برخی از این دسته جرایم اشاره می‌شود:

٤-١- تولید، انتشار، توزیع، در دسترس قرار دادن یا معامله داده‌ها یا نرم‌افزارها

٤-١-١- رکن مادی

- موضوع جرم

موضوع جرم مدنظر، داده‌ها، ابزارهای الکترونیکی و بدافزار یا نرم‌افزارهای زیان‌آور یعنی نرم‌افزارهایی که برای رفتار غیر قانونی و زیان‌آور، تولید یا پخش می‌شوند، نظیر ویروس رایانه‌ای، کرم‌ها و... است.

- رفتار مرتکب

رفتارهای پیش‌بینی شده در بند- الف- ماده ۲۵ قانون جرایم رایانه‌ای عبارتند از تولید، انتشار، توزیع، در دسترس قرار دادن یا معامله که هریک از این رفتارها به طور جداگانه، جرم محسوب می‌شوند.

٤-١-٢- رکن روانی

برای تحقق این جرم، عمد در ارتکاب رفتارهای فوق و هم‌چنین علم و آگاهی نسبت به این‌که نرم‌افزار یا هر نوع ابزار الکترونیکی- صرفاً- به منظور ارتکاب جرایم رایانه‌ای به کار می‌رود، ضروری است.

٤-١-٣- مجازات

حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات، کیفر مقرر برای جرم موضوع بند- الف- ماده ۲۵ قانون جرایم رایانه‌ای است.

٤-٢- فروش، انتشار یا در دسترس قرار دادن داده‌های رخنه‌گر

رکن قانونی این جرم، بند- ب- ماده ۲۵ قانون جرایم رایانه‌ای است. این بند بر خلاف بند قبل، به بدافزارها توجهی نداشته؛ بلکه مدنظر قانونگذار، داده‌هایی است که دارای ارزش و کارکرد مثبت بوده؛ لیکن مرتکب، از آن‌ها برای دسترسی غیر مجاز بهره می‌گیرد.

٤-٢-١- رکن مادی

- موضوع جرم

رفتارهای موضوع بند- ب- به جهت بازدارندگی جرم‌انگاری شده‌اند و راهی برای ارتکاب جرم دسترسی غیر مجاز هستند.

داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری، موضوع با واسطه آن‌ها به حساب می‌آیند که این موضوعات، موضوع جرم دسترسی غیر مجاز هستند.

- رفتار مرتکب

سه رفتار فروش، انتشار و در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌کند، موضوع بند- ب- ماده ۲۵ قانون جرایم رایانه‌ای است و نیازی نیست که این سه رفتار، در فضای سایبر انجام گیرد؛ چون همین‌که کسی گذرواژه‌ای را بر روی کاغذی بنویسد و به دیگری بدهد تا از طریق آن امکان دسترسی غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم کند، جرم موضوع این بند تحقق یافته است.

٤-٢-٢- رکن روانی

عمد در ارتکاب سه رفتار فوق و علم به این که گذرواژه یا داده را جهت دسترسی غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او در اختیار دیگران قرار داده، فروخته یا منتشر کرده، از ارکان روانی این جرم به شمار می‌آید.

٤-٢-٣- مجازات

مجازات تعیین شده برای جرم موضوع بند- ب- ماده ۲۵ قانون جرایم رایانه‌ای، همانند مجازات مقرر در بند- الف- ماده مذکور است.

٤-٣- انتشار یا در دسترس قرار دادن محتویات آموزشی جرایم رایانه‌ای

دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای، تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی، جرایمی هستند که بند- ج- ماده ۲۵ قانون جرایم رایانه‌ای، انتشار و در دسترس قرار دادن محتویات آموزشی آن‌ها را جرم‌انگاری نموده است.

٤-٣-١. رکن مادی

- **موضوع جرم**

جرم انتشار یا در دسترس قرار دادن محتویات، جنبه بازدارندگی نسبت به جرایم دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی دارد؛ لذا موضوعات این جرایم به صورت با واسطه، موضوع جرم پخش یا در دسترس قرار دادن محتویات آموزشی به شمار می‌آیند.

- **رفتار مرتکب**

رفتارهای پیش‌بینی شده در بند- ج- انتشار یا در دسترس قرار دادن محتویات آموزشی جرایم رایانه‌ای است که هر یک به طور جداگانه، جرم محسوب می‌شوند.

٤-۳-۲- رکن روانی

عمد در ارتکاب دو رفتار فوق و علم به این‌که محتویات منتشر شده یا در دسترس قرار گرفته، جهت آموزش جرایم دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی هستند، برای تحقق جرم موضوع بند- ج- ماده ۲۵ قانون جرایم رایانه‌ای، ضروری است.

٤-۳-۳- مجازات

مجازات پیش‌بینی شده برای بند- ج- ماده ۲۵ قانون جرایم رایانه‌ای نیز همانند مجازات‌های بند- «الف» و «ب»- این ماده است.

مطابق تبصره این ماده، اگر اعمال یاد شده حرفه مرتکب باشد، وی به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

نتیجه‌گیری

توسعه فناوری اطلاعات و انقلاب الکترونیک- به عنوان پدیده تعیین کننده قرن حاضر- تمام ابعاد زندگی اجتماعی را در بر گرفته است. در حوزه حقوق و جرایم علی‌رغم تلاش‌های صورت گرفته، فضای سایبر هنوز محیطی کنترل نشده، نامنظم و بی‌قانون توصیف می‌گردد که- تقریباً- برای همگان قابل دسترسی است.

جرایم رایانه‌ای، یکی از پدیده‌های نوظهوری است که هر چند برخی از آن، شباهت‌هایی با جرایم سنتی دارد؛ اما تفاوت‌هایی در روش، ماهیت و نوع جرم دارد که از لحاظ جرم‌شناسی، کیفرشناسی و حقوق کیفری، پژوهش‌های جدیدی را می‌طلبد.

جرایم رایانه‌ای به دلیل تأثیرات ناگواری که بر جامعه اطلاعاتی و کاربران دارد، برخورد جدی‌تری را می‌طلبد و نیازمند نظارت دقیق‌تری برای جلوگیری از آسیب‌های امنیتی و فرهنگی است.

در این راستا با عنایت به پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر و تسری استفاده از فناوری و فضای مجازی در میان تمامی اقشار جامعه- به ویژه کودکان و نوجوانان- ضرورت آموزش و فرهنگ‌سازی استفاده از آن، بیش از پیش احساس می شود.

از سوی دیگر، لازم است مقنن با اتخاذ سیاست‌های پیشگیرانه در زمینه جرایم رایانه‌ای، ضمن بررسی تناسب جرم ارتکابی با مجازات قانونی- به ویژه در خصوص جزای نقدی- اقدام لازم به عمل آورد.

فهرست منابع

۱. پاکزاد، بتول (۱۳۸۰). **جرایم رایانه‌ای**. پایان‌نامه کارشناسی ارشد. دانشگاه شهید بهشتی تهران.

۲. جلالی فراهانی، امیرحسین (۱۳۸۹) **کنوانسیون جرایم سایبر و پروتکل الحاقی آن**. تهران: انتشارات خرسندی.

۳. جلالی فراهانی، امیر حسین (۱۳۸۹). **درآمدی بر آیین دادرسی کیفری جرایم سایبری**. تهران، انتشارات خرسندی.

٤. حییم، سلیمان (۱۳۳۷). **فرهنگ کوچک انگلیسی- فارسی**. چاپ۱۵. تهران: انتشارات فرهنگ معاصر.

۵. دزیانی، محمد حسن (۱۳۷۳). **ابعاد جزایی کاربرد کامپیوتر و جرایم کامپیوتری**. خبرنامه انفورماتیك شورای عالی انفورماتیك کشور. شماره۵۸.

٦. شریفی، مرسده (۱۳۷۹). **جرایم رایانه‌ای در حقوق جزای بین‌المللی**. پایان‌نامه کارشناسی ارشد، دانشگاه‌آزاد اسلامی. واحد تهران.

۷. شیرزاد، کامران (۱۳۸۸). **جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و بین‌الملل**. تهران، نشر بهینه فراگیر.

۸. طارمی، محمد حسین (۱۳۸٦). **گذری بر جرایم رایانه‌ای**. ره‌آورد نور. شماره۲۱.

۹. عالی‌پور، حسن (۱۳۹۰). **حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)**. تهران: انتشارات خرسندی.

۱۰. عمیدی، مهدی (۱۳۸۷). **مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران**. پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی. واحد تهران مرکزی.

۱۱. فضلی، مهدی (۱۳۸۹). **مسؤلیت کیفری در فضای سایبر**. تهران: انتشارات خرسندی.

۱۲. **قانون تجارت الکترونیکی**.

۱۳. **قانون مجازات اسلامی**.

۱٤. میرمحمدصادقی، حسین (۱۳۷۹). **حقوق کیفری اختصاصی (۲): جرایم علیه اموال و مالکیت**. چاپ۷. تهران: انتشارات میزان.