مروری بر جرائم رایانه‌ای و تبیین ماهیت تاریخی و تقنینی آن

احمد پورابراهیم[1]

تاریخ دریافت: ۱۴۰۰/۰۸/۱۰ تاریخ پذیرش: ۱۴۰۰/۰۸/۲۲

چکیده

امروزه جرائم رایانه‌ای به مفهوم عام به‌عنوان یک مسئله در سطح عمومی و قانون‌گذاری مطرح بوده و هرروز نیز دامنه آن گسترده‌تر می‌شود. هرچند تمامی جرائم، امنیت کشور و آسایش عمومی را خدشه‌دار می‌سازند، لیکن این خصیصه در برخی از آن‌ها ملموس‌تر است. جرائم رایانه‌ای به‌طور مستقیم با مفاهیم امنیت ملی و آسایش عمومی در ارتباط می‌باشند. بسیاری از اعمال مجرمانه‌ای که در فضای فیزیکی و ملموس قابل تحقق هستند، در فضای مجازی نیز امکان فعالیت دارند. در یک تقسیم‌بندی کلی می‌توان جرائم اطلاعات را ازلحاظ فلسفه قانون‌گذاری، به دو گروه تقسیم کرد. ۱. طیفی از جرائم رایانه‌ای که با قوانین مربوط به جرائم کلاسیک قابل‌تعقیب هستند و نیاز به قانون‌گذاری جدید ندارند و می‌توان آن‌ها را به جرائم علیه اشخاص، اموال، امنیت و آسایش عمومی، اخلاق، عفت عمومی و خانواده دسته‌بندی نمود. ۲. طیفی از جرائم رایانه‌ای که ارتکاب آن‌ها قبل از پیدایش فناوری اطلاعات به‌هیچ‌وجه امکان‌پذیر نبوده است، مانند دستیابی غیرمجاز، شنود غیرمجاز، اخلال در داده و اخلال در سیستم. با توجه به اینکه متأسفانه طی سال‌های اخیر به‌موازات افزایش کاربردی اینترنت شاهد افزایش تصاعدی در میزان جرائم سایبری بوده‌ایم، بنابراین حقوق جزا می‌بایست با ایجاد و تأسیس مفاهیم و نهادهای نوین، تدابیر لازم متناسب با پیشرفت‌های تکنولوژیکی پیش‌بینی نموده و همچنین فرصت‌های پیچیده‌ای که جهت سوءاستفاده از تسهیلات محیط سایبر فراهم آمده را در نظر داشته باشد. در این راستا پژوهش حاضر باهدف تبیین جرائم‌رایانه‌ای از دیدگاه مفهومی و تاریخی به‌مطالعه می‌پردازد.

کلیدواژگان: جرم رایانه‌ای، پیشینه جرائم رایانه‌ای، قوانین ایران.

---

[1] - دکترای حقوق کیفری و جرم شناسی ، استادیار گروه حقوق دانشگاه ازاد اسلامی ، رشت ، ایران

مقدمه

در سال‌های اخیر پیشرفت‌های چشمگیری در حوزه علم و فناوری صورت گرفته است؛ پیشرفت‌های مذکور حائز جنبه‌های خطرناکی نیز می‌باشند که پیدایش انواع جدید جرائم و همچنین بهره‌برداری از فناوری جدید در ارتکاب جرائم سنتی بخشی از آن به شمار می‌رود. فناوری‌های به وجود آمده در عرصه ارتباطات و اطلاعات مفاهیم قانونی موجود را نیز دچار چالش‌هایی نموده است. پیشرفت‌های مذکور با ظهور شبکه‌ها و ابر شاهراه‌های اطلاعاتی ازجمله اینترنت گسترش پیداکرده است که از طریق آن‌ها هر فردی قادر خواهد بود که به‌تمامی اطلاعات الکترونیک، دسترسی داشته باشد. کاربران از طریق اتصال به سرویس‌های اطلاعات و ارتباطات، نوعی فضای عام به نام فضای مجازی را پدید آورده‌اند که متأسفانه این فضا نیز مورد سوءاستفاده مجرمین و اخلال گران قرارگرفته است. در یک تقسیم‌بندی کلی می‌توان جرائم اطلاعات را ازلحاظ فلسفه قانون‌گذاری و قوانین حاکم بر آن‌ها، به دو گروه تقسیم کرد. گروه اول شامل طیفی از جرائم رایانه‌ای است که با قوانین مربوط به جرائم کلاسیک قابل‌تعقیب و مجازات هستند و نیاز به قانون‌گذاری جدید ندارند[۱]. این گروه خود شامل انواع مختلفی از جرائم است و می‌توان آن‌ها را به جرائم علیه اشخاص، اموال، امنیت و آسایش عمومی، اخلاق، عفت عمومی و خانواده دسته‌بندی نمود. گروه دوم شامل طیفی از جرائم رایانه‌ای است که دسته‌ای از آن، جرائم جدیدی هستند که ارتکاب آن‌ها قبل از پیدایش فناوری اطلاعات به‌هیچ‌وجه امکان‌پذیر نبوده است[۲]، مانند دستیابی غیرمجاز، شنود غیرمجاز، اخلال در داده و اخلال در سیستم. با توجه به اینکه میزان استفاده از اینترنت طی سال‌های اخیر به‌طور تصاعدی افزایش پیداکرده است و متأسفانه به‌موازات افزایش کاربردی اینترنت و تجارت الکترونیکی شاهد افزایش خاصی در میزان جرائم سایبری نیز بوده‌ایم. لذا با توجه به این روند و اهمیت موضوع جرائم رایانه‌ای می‌توان گفت دستیابی

[۱] خرم‌آبادی، عبدالصمد، ۱۳۸۴، ص ۵۴.

[۲] خرم‌آبادی، عبدالصمد، ۱۳۸۴، ص ۵۹.

به جزئیات قوانین و مقررات مربوطه در رابطه با جرائم رایانه‌ای از اهمیت و ضرورت این تحقیق به شمار می‌رود که به نظر می‌رسد دراین‌ارتباط مطالعه‌ای منسجم و جامعی انجام نیافته است. در همین راستا پژوهش حاضر درصدد پاسخگویی به سؤالات زیر است: در نظام حقوقی ایران ماهیت و ارکان جرائم رایانه‌ای چیست؟ و نظام کیفری ایران برای مقابله با این جرائم چه تدابیری فراهم نموده است؟ و یا سؤالاتی در خصوص بررسی تداخل قوانین همانند اینکه اگر فرد نظامی در بستر تبادلات الکترونیکی مرتکب جعل شود، شیوه رسیدگی و تعیین مجازات مطابق قانون مجازات جرائم نیروهای مسلح است با قانون تجارت الکترونیکی و یا قانون جرائم رایانه‌ای؟

اهداف تحقیق عبارت‌اند از؛ بررسی ماهیت حقوقی جرائم از طریق سامانه‌های رایانه‌ای و مخابراتی، بررسی پیشینه تاریخی و تقنینی جرائم رایانه‌ای و ارائه پیشنهاد و راهکار برای پیشگیری و مقابله با این جرائم.

همچنین قابل‌ذکر است روش پژوهش حاضر توصیفی- تحلیلی است. در این پژوهش برای جمع‌آوری داده‌ها و اطلاعات، از روش کتابخانه‌ای استفاده شد. بدین منظور اطلاعات از کتب و مجلات تخصصی و همچنین سایت‌های تخصصی جمع‌آوری گردید.

۱- تعاریف و مفاهیم

صاحبان اندیشه هرکدام با توجه به حوزه تخصصی خود، تعریفی از جرم و جرائم رایانه‌ای ارائه کرده‌اند؛ بنابراین تعریف خاصی که موردقبول همه آن‌ها باشد وجود ندارد. بااین‌وجود در این مبحث به تعاریف درخور این تحقیق خواهیم پرداخت.

۱-۱- تعریف جرم

جرم در لغت به معنای گناه، جناح و عصیان آمده است. در جرم‌شناسی نه‌تنها فعل یا ترک فعلی را که در قانون برای آن مجازات پیش‌بینی‌شده جرم می‌نامد، بلکه هر عملی را که مضر با وضع اجتماعی بوده، هرچند در قانون جزا پیش‌بینی‌نشده باشد، نیز مورد

بررسی و پژوهش قرار می‌دهند. کنش‌های مثبت یا منفی مخالف نظم اجتماعی افراد در جامعه که به‌موجب قانون برای آن مجازات یا اقدامات تأمینی تعیین‌شده باشد، جرم نام دارد. پس جرم عمل یا ترک عمل قابل مجازات یا اقدامات تأمینی است که قانون آن را مشخص می‌کند[۱]. در قانون مجازات اسلامی مصوب سال ۱۳۷۰، قانون‌گذار ماده ۲ سابق را تغییر داده و نه‌تنها عبارت مستلزم اقدامات تأمینی و تربیتی را لازم به ذکر ندانسته، بلکه عبارت تأکیدی آخر ماده «و هیچ امری را نمی‌توان جرم دانست مگر آنکه به‌موجب قانون برای آن مجازات یا اقدامات تأمینی یا تربیتی تعیین‌شده باشد» را زائد تلقی و ماده ۲ قانون جدیدی را بدین نحو تدوین نمود؛ «هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین‌شده باشد جرم محسوب است.»

۱-۲- تعریف جرائم رایانه‌ای

جرائم رایانه‌ای جرائمی هستند که در آن‌ها رایانه به‌عنوان موضوع و یا ابزار جرم و جزئی از اجزای تشکیل‌دهنده عنصر مادی محسوب می‌شود که در نوشته‌های معاصر علوم جنایی در شاخه‌ای به نام حقوق جنایی فنی یا خاص جای گرفته است. ویژگی‌های غیرملموس بودن و ارتکاب یافتن در محیطی غیر فیزیکی، به‌موازات دشواری فرآیند کشف مکان ارتکاب جرم در این‌گونه جرائم که متأثر از جنبه فرا ملّی آن‌ها است و نیز نظر به گستردگی و پیچیدگی فضای سایبر و فناوری رایانه، عملاً نظام حقوقی و قوانین کشورها (بخصوص حقوق کیفری در ابعاد شکلی و ماهوی) را با مشکلات عدیده‌ای مواجه ساخته و آینده اجرای قوانین را به مخاطره انداخته است[۲].

۲- پیشینه و ماهیت تاریخی جرائم رایانه‌ای

نظر به اینکه بررسی پیدایش سیر تاریخی جرائم رایانه‌ای و نحوه تحول و تکامل شیوه‌های ارتکاب این نوع جرائم کمک شایانی در شناسایی ماهیت و تعریف و طبقه‌بندی آن‌ها خواهد داشت لذا بدواً به بررسی این موضوع می‌پردازیم. بنا بر

۱ - شامبیاتی، ۱۳۸۸، ص ۲۱۴.

۲- پاک‌نهاد، امیر، ۱۳۹۰، ص ۲.

پژوهش‌های مرتبط با زمینه تاریخچه پیدایش جرائم رایانه‌ای، واژه جرم رایانه‌ای برای اولین بار در مطبوعات عمومی و در ادبیات علمی دهه ۱۹۶۰ میلادی ظاهر شد. این بدان معنی نیست که در دهه‌های ۱۹۴۰ و ۱۹۵۰ که در رایانه‌های نسل اول و دوم مورداستفاده قرارگرفته‌اند، جرمی به‌وسیله این رایانه‌ها یا علیه آن‌ها واقع نشده باشد؛ چه‌بسا جرائمی در این مدت در این خصوص ارتکاب یافته باشد، لیکن به دلایل مختلف مانند عدم اطلاع بزهکاران و یا عدم آشنایی مأمورین کشف جرم با رایانه کشف نشده باشد و یا حتی اگر کشف‌شده و مورد رسیدگی هم قرارگرفته باشد به لحاظ جزئی بودن موضوع جرم اعلام‌نشده باشد و یا به لحاظ عدم آشنایی حقوقدانان و سایر دست‌اندرکاران با اصطلاح جرم رایانه‌ای ارتکاب جرمی تحت این عنوان گزارش نشده باشد و شاید به لحاظ قلت تعداد و چشمگیر نبودن، این‌گونه جرائم در دهه‌های ۱۹۴۰ و ۱۹۵۰ موردتوجه قرار نگرفته‌اند. هنگامی‌که پیشینه جرائم سایبر بررسی می‌گردد، بیشتر بر روی جرائم مرتبط با رایانه بحث شده است و جرائم رایانه‌ای- سایبری را در قالب سه نسل موردبررسی قرار می‌دهند. لازم به ذکر است طبقه‌بندی این جرائم در قالب سه نسل، بر اساس نسل‌های تکاملی سیستم‌های رایانه‌ای نمی‌باشد[۱].

۲-۱- نسل اول جرائم رایانه‌ای

این نسل به ابتدای ظهور سیستم‌های رایانه‌ای، به‌ویژه زمانی که برای اولین بار در سطح گسترده‌ای در دسترس عموم قرار گرفتند، مربوط می‌شود. اولین سیستم رایانه‌ای به مفهوم امروزی ENIAC نام داشت که سوئیچ آن در فوریه ۱۹۴۶ چرخانده شد؛ اما حدود سه دهه طول کشید که امکان تولید انبوه این سیستم‌ها در قالب سیستم‌های شخصی و رومیزی فراهم گشت و تعداد بیشتری از مردم توانستند آن‌ها را بخرند و در امور مختلف از آن‌ها استفاده کنند. بدیهی است سوءاستفاده از این سیستم‌ها از این زمان موردتوجه قرار گرفت و تلاش‌هایی جهت مقابله با آن‌ها به عمل آمد. گفتنی است

[۱] - انزالی، ۱۳۷۴، ص ۳۷.

سوءاستفاده‌هایی که در این دوره از سیستم‌های رایانه‌ای می‌شد، ازلحاظ نوع و حجم خسارات محدود بود که آن‌هم از قابلیت محدود این سیستم‌ها نشاءت می‌گرفت. در آن زمان، عمده اقدامات غیرمجاز، به ایجاد اختلال در کارکرد این سیستم‌ها و به‌تبع آن دست‌کاری داده‌ها مربوط می‌شد. لذا تدابیری که جهت مقابله با آن‌ها اتخاذ می‌گردید، بیشتر رویکردی امنیتی داشت.

۲-۲- نسل دوم جرائم رایانه‌ای

نکته قابل‌توجهی که می‌توان درباره این نسل از جرائم بیان کرد این است که پیش از آنکه به‌عنوان یک نسل از جرائم با ویژگی‌های خاص موردتوجه قرار گیرد، پل ارتباطی میان نسل اول و سوم بوده است. دلیل بارز آن‌هم عمر بسیار کوتاه این نسل است که به‌سرعت با ظهور نسل سوم منتفی شد. آنچه این نسل از جرائم را از دو نسل دیگر متمایز می‌سازد، توجه به داده‌ها سوای از واسط آن‌هاست. این رویکرد که از اواخر نسل اول زمزمه‌های آن شنیده می‌شد، به دلیل محوریت یافتن داده‌ها اتخاذ گردید. دلیل آن‌هم این بود که در دوران نسل اول، سیستم‌های رایانه‌ای به‌تازگی پا به عرصه گذاشته بودند و عمدتاً به شکل سیستم‌های شخصی یا رومیزی بودند و به همین دلیل به‌تنهایی موردتوجه قرارگرفته بودند؛ اما به‌تدریج با توسعه و ارتقای فناوری رایانه و به‌کارگیری آن در بسیاری از ابزارها و به عبارت بهتر رایانه‌ای شدن امور، به‌تدریج ابزارهای رایانه‌ای جایگاه خود را از دست دادند و محتوای آن‌ها یعنی داده‌ها محوریت یافت. بدیهی است در این مقطع مباحث حقوقی و به‌تبع آن رویکردهای مقابله با جرائم رایانه‌ای نیز تغییر یافت، به‌نحوی‌که تدابیر پیشگیرانه از جرائم رایانه‌ای با محوریت داده‌ها و نه واسطشان تنظیم شدند. حتی این رویکرد در قوانینی که در آن زمان به تصویب می‌رسید نیز قابل‌مشاهده است[۱].

[۱] - دزیانی، ۱۳۷۶، ص ۴.

۲-۳- نسل سوم جرائم رایانه‌ای

نسل سوم جرائم رایانه‌ای از اوایل دهه نود، با جدی شدن حضور شبکه‌های اطلاع‌رسانی رایانه‌ای در عرصه بین‌الملل و به‌ویژه ظهور شبکه جهانی وب که به فعالیت این شبکه‌ها ماهیتی تجاری بخشید، آغاز شد. همچنین از بعد دیگر می‌توان بیان داشت پیشینه تاریخی جرائم کامپیوتری به سال ۱۹۸۵ برمی‌گردد که جرائم کامپیوتری دربرگیرنده جرائمی مانند جاسوسی کامپیوتری سرقت‌های آثار ادبی و سوءاستفاده غیرقانونی از سیستم‌های کامپیوتری بود[۱]. در این راستا بررسی قوانین مربوط به جرائم رایانه‌ای و رویه قضایی کشورهای توسعه‌یافته بیانگر این است که این کشورها در دهه ۱۹۷۰ بدواً نسبت به جرائم رایانه‌ای علیه محرمانگی (جرائم علیه حقوق فردی) عکس‌العمل نشان داده‌اند و بعدازآن شروع به تغییر و اصلاح قوانین مربوط به جرائم اقتصادی و سپس جرائم علیه مالکیت معنوی کرده‌اند. ترتیب عکس‌العمل قانونی کشورها نسبت به انواع جرائم رایانه‌ای ممکن است ناظر بر ترتیب پیدایش این جرائم باشد و ممکن است ناظر به عدم مقاومت بعضی از قوانین نسبت به قوانین دیگر در برابر جرائم رایانه‌ای باشد. در دهه ۱۹۸۰ نظرات علمی و عمومی در مورد جرم رایانه‌ای به‌سرعت تغییر یافت و مشخص شد که جرم رایانه‌ای محدود به جرائم اقتصادی نبوده همه تعرضات نسبت به همه منافعی را شامل می‌شد و مثلاً سوءاستفاده از رایانه بیمارستان یا تخلفات رایانه‌ای نسبت به حقوق خصوصی و فردی که جنبه اقتصادی ندارند و اساساً این موارد را جدا از جرم رایانه‌ای بررسی کرده‌اند. موج وسیعی از سرقت برنامه‌ها سوءاستفاده‌ها از صندوق‌های پرداخت و استفاده از مخابرات موجب شد انعطاف جامعه اطلاعاتی برانگیخته‌شده نیاز برای استراتژی جدید امنیت داده‌پردازی و کنترل جرم احساس شود. در حال حاضر، بیشتر نظرها درزمینه جرائم رایانه‌ای به انتقال غیرقانونی سرمایه‌ها با استفاده از ابزار الکترونیکی، خرابکاری، ویروس‌ها، کرم‌های رایانه‌ای و همچنین جعل اسناد با استفاده از رایانه معطوف است. خطر خرابکاری مخصوصاً در سال ۱۹۸۹ میلادی

[۱] - آل کجباف، ۱۳۷۴، ص ۱۰۳.

آشکار شد؛ زمانی که دادرسی‌های کیفری در جمهوری فدرال آلمان معلوم کرد که خرابکارانی که با استفاده از شبکه‌های اطلاعاتی بین‌المللی به اطلاعاتی در امریکا و انگلستان و دیگر کشورهای خارجی دست‌یافته‌اند و حاصل کار خود را به کشور شوروی سابق فروخته‌اند. تقریباً در همان زمان خطر ویروس‌ها و کرم‌ها هم معلوم شد و زمانی که ویروسی توسط یک دانشجوی آمریکایی ساخته‌شده بود، در طی چند روز نزدیک به ۶۰۰۰ سیستم رایانه‌ای را مختل کرد. بعد شکل‌های جدید بزهکاری درزمینه فنون ارتباط سمعی، بصری و یا قسمت‌های ارتباط ماهواره‌ای، ادامه جرائم اطلاعات را افزایش دادند[۱]. هکرها، به سیستم‌های پست صوتی شرکت‌هایی نفوذ کردند که خدمات معاف از مالیات به مشتریان خود ارائه می‌کردند. بروز جرائم بسیاری با شیوه‌های متفاوت از قبیل شبکه‌های هرمی برای کلاه‌برداری، هکرهای حرفه‌ای که سازمان‌ها و نهادهای خصوصی و دولتی را به ستوه آوردند و نیز تحقق جرائم خلاف اخلاقی چون هرزه‌نگاری و وقایعی ازاین‌دست، منجر به وضع قوانین خاص و مبارزه با جرائم رایانه‌ای و فضای مجازی در کشورها گردید. به‌ویژه افزایش جرائم رایانه‌ای در امریکا ازجمله حمله به پایگاه‌های اینترنتی Amazon,Yahoo، رئیس اف. بی. آی را واداشت تا در فوریه سال ۲۰۰۰ میلادی از کنگره بخواهد ۳۷ میلیون دلار به بودجه ۱۰۰ میلیون دلاری وزارت دادگستری برای مبارزه با جرائم رایانه‌ای بیفزاید و کلینتون در همان ماه درخواست بودجه ۹ میلیون دلاری برای تأسیس مرکز امنیت ملی، مشارکت شرکت‌های اینترنتی و تجارت الکترونیک علیه حمله‌کنندگان به پایگاه‌های کامپیوتری را به کنگره ارائه داد[۲].

۳- جایگاه جرائم رایانه‌ای در قوانین داخلی و بین‌المللی

اصطلاحات جرم رایانه‌ای و جرم مرتبط با رایانه، اولین و قدیمی‌ترین اصطلاحاتی هستند که برای نسل اول جرائم فناوری اطلاعات مورداستفاده قرارگرفته‌اند و علت انتخاب

[۱] - طارمی، ۱۳۸۶، ص ۱۵.

[۲] - گنجی، ۱۳۸۲، ص ۲۵.

عناوین جرم رایانه‌ای و جرم مرتبط با رایانه برای این‌گونه جرائم این بوده که رایانه به‌عنوان هدف و یا به‌وسیله ارتکاب جرم در این‌گونه جرائم محوریت داشته است[۱].

در تعاریف جرم رایانه‌ای چنین آمده است: هر جرمی که قانون‌گذار به‌صراحت رایانه را به‌منزله موضوع یا وسیله جرم جزء رکن ماده آن اعلام کرده باشد یا عملاً رایانه به‌منزله موضوع یا وسیله ارتکاب جرم در آن نقش داشته باشد. این تعریف هم علاوه بر جرائم سده قبل، آن دسته از جرائم سنتی را نیز که با استفاده از رایانه و فناوری اطلاعات ارتکاب یابند را، بدون اینکه تغییری در عنصر مادی آن‌ها صورت گرفته باشد، یا قانون‌گذار رایانه را جزء این عنصر برشمرده باشد، مشمول این عنوان می‌داند مانند توهین به یک فرد که از طریق پست الکترونیکی صورت پذیرفته باشد یا تخریب عمدی تجهیزات رایانه‌ای یا اینکه هر جرمی که قانون‌گذار به‌صراحت رایانه را به‌منزله موضوع یا وسیله جرم جزء رکن مادی آن اعلام کرده باشد، یا عملاً رایانه به‌منزله موضوع یا وسیله ارتکاب یا وسیله ذخیره یا پردازش یا انتقال دلایل جرم در آن نقش داشته باشد. این تعریف هم علاوه بر جرائم ذکرشده در دودسته قبل، جرائمی را نیز که صرفاً دلایل آن‌ها یا اطلاعات مربوطه در رایانه ذخیره‌شده‌اند، با در نظر گرفتن قواعد خاص آیین دادرسی کیفری، جزء جرائم رایانه‌ای دانسته است[۲].

۳-۱- جایگاه جرائم رایانه‌ای در قوانین بین‌المللی

۳-۱-۱- تعریف سازمان ملل متحد از جرم رایانه‌ای

سازمان ملل در نشریه شماره ۴۴ خود (نشریه بین‌المللی سیاست جنایی) با ذکر این نکته که تعریف موردتوافقی در خصوص جرم رایانه‌ای وجود ندارد و شاید نتوان ارائه کرد، جرم رایانه‌ای را شامل فعالیت‌های مجرمانه با ماهیت سنتی مانند سرقت و جعل و یا با ماهیت نوین یعنی راه‌های تازه برای استفاده بیان می‌کند. تصریح به‌جا و به‌موقع

[۱] - خرم‌آبادی، ۱۳۸۳، ص ۷۶.

[۲] - باقری پور، ۱۳۸۹، ص ۱.

سازمان ملل مبنی بر اینکه باید جرم رایانه‌ای گفت نه سوءاستفاده از رایانه؛ از نکات بسیار مهم است.

۳-۱-۲- تعریف سازمان همکاری و توسعه اقتصادی از جرم رایانه‌ای.

متخصصان این سازمان در سال ۱۹۸۳ به‌جای تعریف جرم رایانه‌ای، سوءاستفاده رایانه‌ای را بدین‌صورت تعریف کرده‌اند: سوءاستفاده از کامپیوتر شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش اتوماتیک و انتقال داده‌هاست[۱]. لذا اولین تعریف ارائه‌شده در مورد جرائم رایانه‌ای، تعریف سازمان همیاری اقتصادی و توسعه در مورد سه گروه از جرائم رایانه‌ای است:

- جرائم اقتصادی مربوط به رایانه مانند کلاه‌برداری رایانه‌ای، جاسوسی رایانه‌ای و خرابکاری رایانه‌ای
- جرائم مربوط به رایانه علیه حقوق فردی، خصوصاً علیه حریم خصوصی شهروندان
- جرائم مربوط به رایانه علیه منافع جمعی مثل جرائم علیه امنیت ملی. کنترل جریان فرامرزی داده‌ها، علیه تمامیت رویه‌های رایانه‌ای و شبکه‌های داده‌ای- ارتباطی یا علیه مشروعیت دموکراتیک مصوبات مجلس در مورد رایانه[۲].

۳-۱-۳- تعریف جرم رایانه‌ای از دیدگاه شورای اروپا

شورای اروپا در گزارش توجیهی توصیه‌نامه مصوب سال ۱۹۹۵ اصطلاح جرم فناوری اطلاعات را به‌اصطلاح جرم رایانه‌ای به‌کاربرده است. در بند ۲۸ گزارش مذکور تصریح گردیده تعریف کردن جرم مربوط به رایانه به‌عنوان طبقه ویژه‌ای از جرم بسیار مشکل است. در بندهای ۲۹ و ۳۰ گزارش مذکور علت استفاده از اصطلاح جرم فناوری اطلاعات به‌اصطلاح جرم رایانه‌ای بیان‌شده است و در تفسیر خود از واژه فناوری

[۱] - خداقلی، ۱۳۸۳، ص ۲۹.
[۲] - زبیر، ۱۳۹۰، ص ۱۹.

اطلاعات وسیع‌ترین معنای ممکن را برای این واژه در نظر گرفته است. در این راستا کمیته اروپایی مسائل جنایی در شورای اروپا در سال ۱۹۸۹ گزارش کاری بیان کرد که در آن‌یکی از متخصصان چنین تعریفی ارائه کرده است: هر فعل مثبت غیرقانونی که کامپیوتر، ابزار یا موضوع جرم باشد، یعنی به‌عبارت‌دیگر هر جرمی که ابزار یا هدف آن تأثیرگذاری بر عملکرد کامپیوتر باشد.

۳-۲- جایگاه جرائم رایانه‌ای در قوانین داخلی

۳-۲-۱- تاریخچه رایانه در ایران

رایانه از اوایل سال ۱۳۴۰ یعنی در حدود ۲۲ سال پس از اختراع اولین رایانه وارد ایران شد. بانک ملی و شرکت نفت اولین نهادهایی بودند که کار با رایانه را در سال ۱۳۴۱ شروع کردند. دانشگاه تهران در سال ۱۳۴۳ کار با رایانه را شروع کرد. وقوع جرم رایانه‌ای به‌تدریج از دهه ۱۳۷۰ در ایران شروع شد. البته آمار دقیقی در این خصوص در دست نمی‌باشد. سوءاستفاده از رایانه برای ارتکاب جرائم سنتی، به‌کارگیری ویروس از طریق توزیع حامل‌های داده آلوده به ویروس، سوءاستفاده‌های مالی و تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای ازجمله جرائم رایانه‌ای‌اند که در مقیاس بسیار کم در دهه ۱۳۷۰ واقع‌شده و با قوانین کیفری مرسوم مورد رسیدگی قرارگرفته‌اند. دادنامه مورخه ۷۲/۴/۳ شعبه ۶۵ دادگاه کیفری ۲ تهران یکی از نمونه آرایی است که مبین به‌کارگیری قوانین کیفری سنتی در خصوص جرائم رایانه‌ای است. به‌موجب این دادنامه، دادگاه در خصوص شکایت یک شرکت نرم‌افزاری رایانه علیه مسئولین شرکت ایرانی دیگر مبنی بر تکثیر و فروش غیرمجاز نرم‌افزار رایانه‌ای، پس از احراز وقوع بزه به استناد بند ۱۱ ماده ۲۳ قانون حمایت از حقوق مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ متهم را به تحمل مجازات محکوم و حکم به جلوگیری از عرضه نرم‌افزارهایی که به‌طور غیرمجاز تکثیرشده‌اند صادر نموده است[۱]. از نیمه دوم دهه ۱۳۷۰ و بالأخص از ابتدای دهه ۱۳۸۰ که استفاده از

[۱] - خرم‌آبادی، ۱۳۸۴، ص ۲۱.

رایانه‌های شخصی توسط سازمان‌های اداری و مؤسسات خصوصی و افراد حقیقی گسترش‌یافته دسترسی به خدمات متعدد اینترنت امکان‌پذیر شده است. ارتکاب جرائم رایانه‌ای نیز از رشد نسبتاً سریعی برخوردار بوده است. اشاعه فحشا و منکرات و انتشار عکس‌ها و تصاویر و مطالب خلاف عفت عمومی، ایجاد اختلاف بین اقشار جامعه از طریق طرح مسائل قومی و نژادی، انتشار مطالب نژادپرستانه، انتشار اسناد و مسائل محرمانه، اهانت به مقدسات مذهبی و دینی، اهانت و افترا نسبت به مقامات دولتی و اشخاص حقیقی و حقوقی، سرقت ادبی و غیره ازجمله جرائمی هستند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت از طریق وب‌سایت‌ها و وبلاگ‌ها، پست الکترونیک، گروه‌های خبری و سایر سرویس‌های اینترنت به وقوع پیوسته‌اند.

۳-۲-۲- جرم رایانه‌ای در قوانین ایران

در ایران، نه در قانون تجارت الکترونیک و نه در قانون جدید مصوب جرائم رایانه‌ای هیچ تعریفی از این مفهوم ارائه نشده است. شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرائم رایانه‌ای وجود دارد.

۳-۲-۳- مراحل قانون‌گذاری در مورد جرائم رایانه‌ای در ایران

طبق ماده ۲ قانون مجازات اسلامی هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین‌شده باشد، جرم محسوب می‌شود. بنا بر ظاهر ماده فوق اگر شخصی فعلی انجام دهد که ازنظر قانون جرم شناخته شود، مجرم محسوب شده و مستحق مجازات خواهد بود. تأمل در ماده ۲ قانون مجازات اسلامی، دلالت قطعی دارد که هیچ پدیده‌ای را نمی‌توان مجرمانه دانست، مگر به‌موجب قانون؛ بنابراین تا آن هنگام که قانونی در مجلس شورای اسلامی به توصیف جرم رایانه‌ای نپرداخته بود می‌توان چنین گفت که نظام قضایی ایران، جرم رایانه‌ای نداشته است چراکه قاضی نمی‌توانسته مافوق قانون به

جرم انگاری و صدور حکم بپردازد. علاوه بر جرائم علیه اموال و اشخاص بسیاری از جرائم علیه آسایش و امنیت عمومی مانند جعل اسکناس و سایر اوراق بهادار، جعل اسناد رسمی، جاسوسی، تبلیغ علیه نظام، اهانت به مقدسات، تروریسم سایبر (رایانه‌ای) و جرائم علیه عصمت و عفت و اخلاق حسنه مانند تشویق به فساد، سکس سایبر، ایجاد و توزیع و عرضه انواع صور قبیحه و مستهجن (هرزه‌نگاری) و غیره، بسیار آسان‌تر از گذشته و در مقیاس بسیار گسترده‌تر از قبل به‌وسیله رایانه انجام می‌شوند. قانون‌گذار ایرانی نیز برحسب گسترش این تکنولوژی و جرائم مرتبط با آن در ادوار مختلف زمانی واکنش نشان داده است.

۱) قانون‌گذار در سال ۱۳۷۹ در برابر برخی از جرائم رایانه‌ای واکنش نشان داده و با الحاق تبصره ۳ به ماده ۱ قانون مطبوعات مقرر داشت کلیه نشریات الکترونیکی مشمول مواد این قانون است.

۲) دومین واکنش قانونی کشور ما در مقابل جرائم رایانه‌ای از طریق وضع قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای به عمل آمد. این قانون در تاریخ ۷۹/۱۰/۴ به تصویب مجلس شورای اسلامی و سپس به تائید شورای نگهبان رسیده است. ماده ۱۳ قانون مذکور نقض حقوق پدیدآورندگان آن دسته از نرم‌افزارهای رایانه‌ای را که موردحمایت این قانون قرارگرفته‌اند، جرم تلقی و برای آن مجازاتی معادل ۹۱ روز تا شش ماه حبس و جزای نقدی تعیین کرده است. البته اشکالاتی بر این قانون وارد است که در این مقال نمی‌گنجد.

۳) سومین عکس‌العمل قانون‌گذار ایران در مقابل جرائم رایانه‌ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۸۲/۱۰/۹ مجلس شورای اسلامی به عمل آمد. به‌موجب ماده ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای تسلیم و افشاء غیرمجاز اطلاعات و داده‌ها به افرادی که صلاحیت دسترسی به آن را ندارند، سرقت و یا تخریب حامل‌های داده و سوءاستفاده مالی از طریق رایانه توسط نظامیان جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می‌شود.

۴) چهارمین واکنش قانونی مرتبط با جرائم رایانه‌ای از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ مجلس شورای اسلامی به‌عمل‌آمده است. به‌موجب مواد ۶۶، ۶۷، ۶۸، ۶۹، ۷۴، ۷۵، ۷۶ و ۷۷ این قانون کلاه‌برداری، جعل، دستیابی و افشاء غیرمجاز اسرار تجاری نقض حقوق مربوط به مالکیت معنوی (کپی‌رایت) و ... که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود جرم تلقی و برای آن مجازات تعیین گردیده است.

هریک از چهار قانون فوق‌الذکر در بستر خاص خود قابلیت اعمال دارند. مثلاً قانون مطبوعات صرفاً نسبت به جرائم رایانه‌ای ارتکابی در قالب نشریات الکترونیکی و قانون مجازات نیروهای مسلح صرفاً در مورد بعضی از جرائم رایانه‌ای نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرائم رایانه‌ای ارتکابی در بستر تجارت الکترونیکی قابل‌اجرا هستند. برای مقابله با سایر سوءاستفاده‌های رایانه‌ای مانند سوءاستفاده از رایانه به‌منظور نفوذ به حریم خصوصی افراد، تخریب، سرقت و توقف و تغییر داده‌هایی که فاقد شرایط مقرر در قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای هستند، سوءاستفاده‌های مالی رایانه‌ای خارج از بستر تجارت الکترونیک و سایر سوءاستفاده‌های رایانه‌ای نیاز به یک قانون جرائم رایانه‌ای پیشرفته و جامع‌الاطراف می‌باشد.

۵) و درنهایت قانون جرائم رایانه‌ای که با عنوان لایحه به مجلس شورای اسلامی تقدیم گردیده بود با تصویب در جلسه علنی روز سه‌شنبه مورخ ۱۳۸۸/۳/۵ تصویب و به تائید شورای محترم نگهبان رسید. پنجمین واکنش درست زمانی که بیش از ۱۰ سال از ورود اینترنت به کشور می‌گذشت و جرائم حائز اهمیت در این زمینه رخداده بود پیش‌نویس قانون مجازات جرائم رایانه‌ای توسط کمیته مبارزه با جرائم رایانه‌ای تحت نظارت شورای عالی توسعه قضایی تدوین شد و در خرداد سال ۸۴ در قالب لایحه‌ای به تصویب هیئت‌وزیران رسید. این لایحه در همان سال برای طی مراحل قانونی با امضای رئیس‌جمهور به مجلس شورای اسلامی تقدیم شد اما در هنگام ارائه این لایحه به مجلس قید فوریت در آن ذکر نشد که با توجه به لوایح و طرح‌هایی که با فوریت در

حال پیگیری بودند، بررسی این لایحه مدت‌زمانی طول کشید اما به دلیل آنکه نمودار جرائم رایانه‌ای سیر صعودی به خود گرفته بود، قوه قضائیه اولویت قرار دادن این لایحه را از مجلس خواستار شد که با تصویب نمایندگان مجلس شورای اسلامی، لایحه جرائم رایانه‌ای طبق اصل ۸۵ قانون اساسی در دستور کار کمیسیون حقوقی و قضایی مجلس قرار گرفت. در سال ۱۳۸۸ قانون جرائم رایانه‌ای به تصویب مجلس شورای اسلامی رسید که در نوع خود گام مهمی در عرصه حقوق مربوط به ارتباطات و فن‌آوری جدید محسوب می‌شود و عناصر و مفاهیم جدید را وارد مباحث حقوقی کشور کرده است.

تصویب قانون جرائم رایانه‌ای در تیر ۱۳۸۸ راه جدیدی فراروی امر پیشگیری و مبارزه با جرائم سایبر گشوده و نسبت به مصادیق پدیده‌های مجرمانه سایبر جرم انگاری کرده است، چنانچه در فصل یکم این قانون مصادیق جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی مشتمل بر: دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای تصریح‌شده در فصل دوم، جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی مشتمل بر جعل رایانه‌ای، تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی مورد احصاء قرارگرفته است. در ماده ۶ قانون جرائم رایانه‌ای آمده است هرکس به‌طور غیرمجاز مرتکب اعمال زیر شود جاعل محسوب و یا به‌عبارت‌دیگر اعمال زیر جعل رایانه‌ای به‌حساب می‌آید:

۱) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانه داده به آن‌ها
۲) تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل‌پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا واردکردن متقلبانه داده‌ها یا علائم به آن‌ها.

در فصل سوم، سرقت و کلاه‌برداری مرتبط با رایانه و مصادیق ربایش‌های داده‌های متعلق به غیر مورداشاره قرارگرفته و در ماده ۱۳ صراحتاً مقرر داشته است: هرکس به‌طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم وجه یا مال یا منفعت

یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از ۱۲۰ تا ۱۰۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد. در ادامه فصل چهارم این قانون علیه عفت و اخلاق عمومی از قبیل تولید، ارسال، انتشار و توزیع محتویات مستهجن و مبتذل رایانه‌ای احصا شده است و اشعار می‌دارد: محتویات و آثار مبتذل به آثاری اطلاق می‌شود که دارای صحنه‌ها و صور قبیحه باشد. همچنین در تعریف محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی اطلاق دارد که بیانگر برهنگی کامل زن یا مرد است. فصل پنجم به تبیین مصادیق مجرمانه هتک حیثیت و نشر اکاذیب می‌پردازد. چنانچه در ماده ۱۶ مقرر می‌دارد: هرکس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر و تحریف منتشر کند، به‌نحوی‌که عرفاً موجب هتک حیثیت او شود، یا در ماده ۱۷ و ۱۸ مقرر می‌دارد: «هرکس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی‌که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود...» «هرکس به‌قصد اضرار به غیر یا تشویش اذهان عمومی یا مقام‌های رسمی به‌وسیله سیستم رایانه یا مخابراتی اکاذیبی را منتشر کند و یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به‌عنوان نقل‌قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی اعم از این‌که از طریق یادشده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود.»

و بر این مبنا برای هر یک از اقدام‌های مجرمانه، مجازات متناسبی مدنظر قرار می‌دهد. در فصل ششم به موضوع «مهم مسئولیت کیفری در ارتکاب جرائم سایبر» و شناسایی عنصر فاعلی عملیات مجرمانه پرداخته است و در ماده ۱۹ بیان می‌دارد:

در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:

- هرگاه مدیر شخصی حقوقی مرتکب جرم رایانه‌ای شود.
- هرگاه مدیر شخصی حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد.
- هرگاه یکی از کارمندان شخص حقوقی بااطلاع مدیر یا در اثر نظارت نداشتن وی مرتکب جرم رایانه‌ای شود.
- هرگاه همه یا قسمتی از فعالیت شخصی حقوقی به ارتکاب جرم رایانه‌ای اختصاص‌یافته باشد.

تبصره ۱- منظور از مدیر کسی است که اختیار نمایندگی با تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره ۲- مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود.

نکته مهم اینکه تبصره ۲ ماده ۲۱ این قانون صراحتاً بیان می‌دارد پالایش محتوای مجرمانه موضوع شکایت خصوصی صرفاً با دستور مقام قضایی رسیدگی‌کننده به پرونده انجام خواهد شد و با این تصریح، دستگاه قضایی را متولی اصلی این اقدام معرفی می‌کند.

چنانچه ماده ۲۲ این قانون نیز دادستانی کل کشور را به‌عنوان یک مقام عالی قضایی، مسئول کمیته تعیین مصادیق محتوای مجرمانه معرفی کرده است.

۴- ارتباط قانون جرائم رایانه‌ای با قوانین پیشین

پیش از تصویب قانون جرائم رایانه‌ای، قانون تجارت الکترونیک مصوب ۱۳۸۲ و قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲ به برخی از مصادیق جرم رایانه‌ای اشاره‌کرده بود، ازآنجاکه قانون‌گذار پیش از تصویب قانون جرائم رایانه‌ای، در ماده ۶۸ قانون تجارت الکترونیکی و ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح، برخی از مصادیق جرم از طریق رایانه را جرم انگاری نموده است.

ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح که مقرر می‌دارد: هرگونه تغییر یا حذف اطلاعات؛ الحاق، تقدیم یا تأخیر تاریخ نسبت تاریخ حقیقی و نظایر آن‌که به‌طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم‌افزارهای مربوط صورت گیرد، جرم محسوب و حسب مورد مشمول مجازات مندرج در مواد مربوط به این قانون می‌باشند. ماده ۶۸ قانون تجارت الکترونیکی نیز مقرر داشته است: هرکس در بستر مبادلات الکترونیکی، از طریق ورود تغییر، محو، توقف «داده‌پیام» و مداخله در پردازش داده‌پیام و سیستم‌های رایانه‌ای و یا استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء، مثل کلید اختصاصی، بدون مجوز امضاء کننده و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم انطباق آن وسایل بانام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل داده‌پیام‌های دارای ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری، قضای، مالی و غیره به‌عنوان داده‌پیام‌های معتبر استفاده نماید، جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون محکوم می‌شود. حال این سؤال مطرح است که اگر فرد نظامی در بستر تبادلات الکترونیکی مرتکب جعل شود، شیوه رسیدگی و تعیین مجازات مطابق قانون مجازات جرائم نیروهای مسلح است با قانون تجارت الکترونیکی و یا قانون جرائم رایانه‌ای، ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح نسبت به قانون جرائم رایانه‌ای، خاص تلقی می‌شود و به قوت خود باقی بوده و در مورد نظامیان قابلیت اعمال دارد و قانون اخیر التصویب در مورد جرائم مندرج در ماده موصوف قابل استناد نیست. همچنین با عنایت به ماده ۵۵ قانون جرائم رایانه‌ای که به الحاق آن به قانون مجازات اسلامی تصریح کرده است این موضوع به‌راحتی قابل استنباط است. البته با تأکید بر اینکه محدوده اعمال ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح فقط در حدود جرائم مصرح در آن می‌باشد و همان ادله که در خصوص رابطه قانون مجازات جرائم نیروهای مسلح و قانون جرائم رایانه‌ای ذکر شد[1]، در رابطه قانون تجارت الکترونیکی و

[1] - ترکی، ۱۳۸۹، ص ۱۷۲.

قانون جرائم رایانه‌ای نیز قابل استناد است؛ زیرا قانون تجارت الکترونیکی، قانون خاص و قانون جرائم رایانه‌ای، عام می‌باشد؛ بنابراین چنانچه فردی مرتکب یکی از جرائم رایانه‌ای در بستر معاملات الکترونیکی شود، نخست باید دید چنانچه آن رفتار بر اساس ماده ۶۸ قانون تجارت الکترونیکی با عناوین منطبق بود، به استناد قانون یادشده درباره آن تصمیم‌گیری می‌شود، ولی درصورتی‌که آن رفتار با هیچ‌یک از عناوین مجرمانه آن قانون منطبق نبود، قانون جرائم رایانه‌ای حاکم است[۱]. البته نظر دیگری دراین‌ارتباط بیان‌شده است که طبق آن قانون جرائم رایانه‌ای به‌عنوان بخشی از قانون مجازات اسلامی دانسته شده و طبق ماده ۵۶ آن، قوانین و مقررات مغایر با این قانون ملغی است. در نسخه نخستین این قانون، دو گونه نسخ پیش‌بینی‌شده بود: نسخ کلی که همین متن ماده ۵۶ است و نسخ موردی و مستقیم که به ماده‌های ۶۷ و ۶۸ قانون تجارت الکترونیکی انگشت می‌نهد. این دو ماده به‌نوبت به کلاه‌برداری کامپیوتری و جعل کامپیوتری می‌پردازند که در قانون جرائم رایانه‌ای همین عناوین (با دگرگونی کامپیوتری به رایانه‌ای) تکرار شده‌اند. با برداشتن این دو ماده، اندیشه بر این بود که آوردن نسخ به‌طورکلی، نسخ جزئی و موردی را نیز در بر می‌گیرد، درحالی‌که این اقدام نه‌تنها کارساز نبود بلکه راه را برای ستیز در جهت گزینش یکی از دو قانون باز کرد که در این میان دو راه برای رویارویی قانون جرائم رایانه‌ای و قانون تجارت الکترونیکی هست: راه نخست اینکه ماده ۶۸ با توجه به صدر این ماده و نیز عنوان قانونی که در زیر آن آمده تنها به جعل‌هایی اشاره دارد که در بستر تجارت الکترونیکی اتفاق می‌افتد درحالی‌که جعل موضوع ماده ۶ قانون جرائم رایانه‌ای عام است[۲]. این دیدگاه می‌گوید بهتر این است که ماده ۶۸ را نسخ شده بدانیم زیرا این ماده عملاً درباره همه جعل‌های رایانه‌ای است، افزون بر این تعبیرهای به‌کاررفته در این ماده مانند بستر مبادلات الکترونیکی و جعل کامپیوتری نشان‌دهنده این است که یک ماده کلی بوده و بنابراین با تصویب ماده ۶ قانون جرائم رایانه‌ای نسخ شده است. جدا از این با کشف دیدگاه قانون‌گذار نیز می‌توان

[۱] - ترکی، ۱۳۸۹، ص ۱۷۴.

[۲] - زر کلام، ۱۳۸۸، ص ۱۵.

نسخ صریح ماده‌های ۶۷ و ۶۸ پی برد و آن اینکه نسخ این دو به‌روشنی در متن لایحه بوده و برداشتن آن را در گام‌های پسینی نه به جهت نپذیرفتن آن‌که به جهت بس بودن تعبیر نسخ کلی بوده است.

نتیجه‌گیری

با توجه به پیشرفت تکنولوژی و اطلاعات، به‌طور یقین افرادی سودجو و فرصت‌طلب نیز با فراگیری دانش درصدد سوءاستفاده از تکنولوژی می‌باشند که این افراد سودجو، امکاناتی را که توسعه تکنولوژی برای جامعه بشری به ارمغان می‌آورد دستخوش امیال و اغراض خودساخته و باعث ایجاد مشکلاتی برای استفاده‌کنندگان از تکنولوژی گردیده تا جایی که امروزه توجه دولتمردان، حقوقدانان، متخصصین در امر تکنولوژی را به خود معطوف کرده است. جرائم رایانه‌ای امروز از گستردگی زیادی برخوردار است. در رابطه با جرائم رایانه‌ای در حقوق ایران باید گفت، قانون‌گذار در سال ۱۳۷۹ در برابر برخی از جرائم رایانه‌ای واکنش نشان داده و با الحاق تبصره ۳ به ماده‌قانون مطبوعات مقرر داشت کلیه نشریات الکترونیکی مشمول مواد این قانون است. در مرحله بعد دومین واکنش قانونی کشور ما در مقابل جرائم رایانه‌ای در سال ۱۳۷۹ از طریق وضع قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای به عمل آمد و سومین عکس‌العمل قانون‌گذار ایران در مقابل جرائم رایانه‌ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح مصوب مرحله بعد دراین‌ارتباط تصویب قانونی مرتبط با جرائم رایانه‌ای از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ مجلس شورای اسلامی است و درنهایت قانون جرائم رایانه‌ای که به‌عنوان لایحه به مجلس شورای اسلامی تقدیم گردیده بود با تصویب در جلسه علنی روز سه‌شنبه مورخ ۱۳۸۸/۳/۵ تصویب و به تائید شورای محترم نگهبان رسید. قانون‌گذار در قانون جرائم رایانه‌ای گام‌های سه‌گانه‌ای را برای جرم سیاسی رایانه‌ای در نظر داشته است: گام اول، دسترسی به سامانه‌های رایانه‌ای و مخابراتی که داده‌های سری در آن‌ها نگهداری می‌شود برحسب ماده ۴ قانون جرائم رایانه‌ای، گام دوم، دسترسی به داده‌های سری یا تحصیل یا شنود

آن‌ها بر طبق بند الف ماده ۳ قانون جرائم رایانه‌ای، گام سوم، در دسترس قرار دادن برای کسانی که شایستگی آگاهی از محتوای داده‌های سری را ندارند مطابق بند ب ماده ۳ قانون جرائم رایانه‌ای و یا در دسترس قرار دادن داده‌های سری یا افشای آن‌ها به دولت یا نهادهای بیگانه یا عاملان آن‌ها برحسب بند ج ماده ۳ قانون جرائم رایانه‌ای می‌باشد. با توجه به اینکه فناوری‌های اطلاعاتی و ارتباطی فضای جدیدی را برای متخلفین جامعه فراهم کرده است و با روند فزاینده ظهور، گسترش و دسترسی ارزان‌قیمت شهروندان به فناوری‌های اطلاعاتی، همچنان شاهد رشد آمار جرائم رایانه‌ای و پیچیده‌تر شدن روش‌های ارتکاب جرم خواهیم بود. بی‌توجهی به این مهم در آینده‌ای نزدیک، فعالیت‌های علمی، صنعتی و اقتصادی جامعه را دچار صدمات جبران‌ناپذیر نموده و امنیت اجتماعی کشور را دستخوش تهدید جدی خواهد کرد. لذا بر سیاست‌گذاران و مدیران جوامع است که با ایمن کردن رایانه‌های اداری و حتی رایانه‌های شخصی با ابزار و نرم‌افزارهای ضد جاسوسی، برای این مشکل جدید راهکارهای قانونی و اجرایی تدارک ببینند. دولت‌ها ضمن ایجاد بستر قانونی، اجرایی و قضایی برای رسیدگی به امر جرائم رایانه‌ای، موظف به ایجاد اطمینان از گردش اطلاعات مناسب بین سازمان‌های دولتی سیاست‌گذار، مجریان قانون و بخش خصوصی هستند. هم‌چنین آماده نمودن بستر فرهنگی جامعه باید به‌گونه‌ای هدایت شود که هر کاربری بداند چگونه از رایانه و اینترنت استفاده کند تا اطلاعات ذی‌قیمت او حفظ شود.

فهرست منابع

۱) انزالی، امیر اسعد، کامپیوترهای امروزی، مجتمع فنی تهران، چاپ اول، تهران، ۱۳۷۴.

۲) آل‌کجباف، حسین، بررسی جرائم کامپیوتری (بزهکاری مدرن)، دوماهنامه انفورماتیک، شماره ۶۰، ۱۳۷۴.

۳) باقری پور، سید محمد، آشنایی با جرائم رایانه‌ای، به نقل از سایت مدی رایانه، ۱۳۸۹.

۴) پاک‌نهاد، امیر، بررسی قانون جرائم رایانه‌ای از دیدگاه موازین حقوق کیفری فناوری اطلاعات، فصلنامه علمی کارآگاه، سال پنجم، شماره ۱۷، ۱۳۹۰.

۵) ترکی، غلام عباس، نگرش علمی و کاربردی به قانون جرائم رایانه‌ای، ماهنامه دادرسی، سال سیزدهم، شماره ۸۰، ۱۳۸۹.

۶) خداقلی، زهرا، جرائم کامپیوتری، انتشارات آریان، چاپ اول، تهران، ۱۳۸۳.

۷) خرم‌آبادی، عبدالصمد، تاریخچه و تعریف و طبقه‌بندی جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، انتشارات سلسبیل، تهران، ۱۳۸۴.

۸) دزیانی، محمدحسن، جرائم کامپیوتری، دبیرخانه شورای عالی انفورماتیک، جلد اول، تهران، ۱۳۷۶.

۹) زبیر، اولریش، جرائم رایانه‌ای، ترجمه محمدعلی نوری و دیگران، انتشارات گنج دانش، چاپ دوم، تهران، ۱۳۹۰.

۱۰) زر کلام، ستار، قانون تجارت الکترونیکی در بوته نقد، ماهنامه آموزشی دادگستری کل استان خوزستان، شماره ۳۶، ۱۳۸۸.

۱۱) شامبیاتی، هوشنگ، حقوق جزای عمومی، مجمع علمی و فرهنگی مجد، چاپ ۱۳، تهران، ۱۳۸۸.

۱۲) شیرزاد، کامران، جرائم رایانه‌ای از دیدگاه حقوق جزای ایران و بین‌الملل، نشر بهینه فراگیر، چاپ اول، تهران، ۱۳۸۸.

۱۳) طارمی، محمدحسین، گذری بر جرائم رایانه‌ای، فصلنامه ره‌آورد نور، شماره ۳۸، ۱۳۸۶.

۱۴) گنجی، علیرضا، امنیت شبکه: چالش‌ها و راهکارها، نشریه علوم اطلاع‌رسانی، شماره ۱ و ۲، ۱۳۸۲.

۱۵) هیئت مؤلفان و ویراستاران انتشارات مایکروسافت، ترجمه فرهاد قلیزاده نوری، فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، کانون نشر علوم، چاپ اول، تهران، ۱۳۸۴.