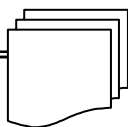


شناخت جرایم رایانه‌ای از منظر اسناد بین‌المللی و قوانین داخلی

علی مراد حیدری^۱ و سمانه لطفی^۲



چکیده: بررسی پیشینه، مفهوم و مصادیق جرایم رایانه‌ای لازمه شناخت دقیق و فهم بهتر این جرایم است. در سیر تحول جرایم رایانه‌ای سه مرحله عمده مشاهده می‌گردد: نسل اول در دهه ۶۰ و ۷۰ رواج یافت که محور جرایم در آن زمان، خود وسیله «رایانه» به عنوان واسطه در عنصر مادی جرم بود؛ نسل دوم در دهه ۸۰ تا اوایل دهه ۹۰ رایج شد. در این دوره به جای این که تأکید بر رایانه باشد، حمایت از «داده» مدنظر قرار گرفت؛ نسل سوم نیز در آستانه هزاره سوم و از اوایل دهه ۹۰ میلادی با گسترش استفاده از «فضای اینترنت» و تحت عنوان جرایم سایبری رواج پیدا کرد.

ارائه تعریف واحد، جامع و مانع از جرایم رایانه‌ای امری است که غالب پژوهشگران بر دشواری آن اذعان نموده و در اسناد بین‌المللی و منطقه‌ای نیز چنین تعریفی مشاهده نمی‌شود به گونه‌ای که در اکثر اسناد مورد اشاره به جای ارائه تعریف جرایم رایانه‌ای، مصادیق آن ذکر شده است. روش ذکر مصادیق جرایم رایانه‌ای به جای ارائه تعریف، در قوانین داخلی ایران نیز بویژه در قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای در پیش گرفته شده است. در این مقاله برای شناخت جرایم رایانه‌ای سه موضوع فوق مورد بررسی قرار گرفته است.

واژگان کلیدی: سایبر، جرم رایانه‌ای، حریم خصوصی، مالکیت فکری



مقدمه

یکی از حوزه‌های چالش برانگیز حال حاضر در بیشتر نظام‌های حقوقی، تصمیم‌گیری راجع به پیشگیری و نحوه مبارزه با جرایمی است که گسترش استفاده از تکنولوژی و فناوری اطلاعات زمینه وقوع آن را فراهم می‌آورد. اهمیت این موضوع از این جهت است که استفاده از رایانه به امری گریزناپذیر در اکثر سازمان‌ها، ادارات، مؤسسات اداری و بنگاه‌های اقتصادی، تجاری و خدماتی داخلی و بین‌المللی تبدیل شده است و این امر فرصت دخالت در امور این مؤسسات از طریق رایانه را بوجود آورده است. به عنوان نمونه تروریست‌های اطلاعاتی فقط با استفاده از یک صفحه کلید و یک موس می‌توانند بصورت غیرمجاز وارد سیستم‌های کامپیوتری امنیتی شوند و با مداخله در سیستم ناوبری هوایی باعث سقوط هواپیما شده یا باعث قطع برق سراسری یا مسموم کردن مواد غذایی شوند. (سلمانی زاده: ۱۳۸۰، ص ۲۰)

اهمیت این موضوع تنها از جهت گسترش استفاده از رایانه نیست، بلکه بیشتر از این جهت است که فن آوری رایانه پیشرفت بسیار سریعی داشته و قابلیت‌های جدید و متنوعی در این عرصه پیدا شده است. امروزه کاربرد رایانه صرفاً ذخیره سازی داده‌ها نیست بلکه به عنوان نمونه مینیاتوری شدن پردازنده‌ها امکان ارتباطات جهانی را فراهم آورده است و با استفاده از ماهواره‌ها و خطوط انتقال داده‌ها می‌توان اطلاعات را به هر نقطه‌ای از زمین ارسال نمود و از طریق شبکه جهانی اینترنت امکان ارتباط مستقیم کاربران در نقاط مختلف کره خاکی فراهم آمده است.

رشد فناوری ارتباطات، به نوبه خود تنوع و پیچیدگی تخلفات و تعدیات مربوط به این قلمرو را موجب گردیده است. اگر در دهه ۶۰ و ۷۰ سرقت اطلاعات از رایانه یا تخریب اطلاعات موجود در رایانه جرمی جدید بشمار می‌آمد، امروزه جرایم ارتكابی در فضای مجازی شبکه اینترنت بخش اعظم جرایم رایانه‌ای را تشکیل می‌دهد.

در کشور ما نیز به موازات پیشرفت فناوری اطلاعات و گسترش استفاده از این فناوری، بیش از پیش نیاز به چارچوب‌های حقوقی جهت برخورد با تعديات و جرایم این قلمرو احساس می‌گردد. در سال‌های اخیر اقداماتی در این راستا صورت گرفته است که مهم‌ترین آنها تصویب قانون جرایم رایانه‌ای در تاریخ ۱۳۸۸/۳/۵ است. انتظار این بود که قانون اخیرالذکر به گونه‌ای تدوین می‌گردید که امکان برخورد جدی با کلیه اشکال بزهکاری رایانه‌ای فراهم می‌آمد، ولیکن به جهت نواقص موجود در این قانون و هم پوشانی آن با بعضی از قوانین دیگر، با متن فعلی امکان برخورد قانونی با بعضی از جرایم رایانه‌ای وجود ندارد.

در این نوشتار امکان بررسی تحلیلی مصادیق جرایم رایانه‌ای وجود ندارد و صرفاً با نگاهی به تاریخچه تحول جرایم رایانه‌ای، تعریف و مصادیق جرم رایانه‌ای در اسناد بین‌المللی و قوانین داخلی، سعی می‌گردد طی سه مبحث معرفی اجمالی از این جرایم ارائه گردد.

مبحث اول) تاریخچه جرایم رایانه‌ای

اصطلاح جرم رایانه‌ای نخست در مطبوعات عمومی و نوشتگان علمی دهه ۱۹۶۰ مطرح شد. در آن زمان بیشتر پرونده‌ها شامل سوء استفاده‌های ابتدایی از رایانه، خرابکاری رایانه‌ای، جاسوسی رایانه‌ای و استفاده‌های غیر قانونی از سیستم‌های رایانه‌ای بود اما چون بیشتر گزارش‌ها بر مبنای نوشته‌های روزنامه‌ها بود، در مورد واقعی یا خیالی بودن پدیده جرم رایانه‌ای بحث و تردید وجود داشت (زیبر: ۱۳۸۵، ج ۳، ص ۱۵)

از دهه ۱۹۷۰ کشورها ابتدا نسبت به جرم‌های رایانه‌ای علیه محرمانگی (جرایم علیه حقوق فردی) واکنش نشان دادند؛ پس از آن تغییر و اصلاح قوانین ناظر به جرم‌های اقتصادی و سپس برخوردهای ناظر به جرایم علیه مالکیت معنوی آغاز شد. بنابراین، از دهه ۱۹۷۰ به بعد بحث‌های مربوط به سوء استفاده رایانه‌ای نه تنها جرم‌های مربوط به حمایت از داده‌ها، بلکه جرم‌های اقتصادی مرتبط با رایانه را نیز در بر گرفته است که امروزه به

منزله محور و حوزه اصلی جرم رایانه‌ای مورد توجه‌اند. در این زمینه جرم‌های اصلی عبارتند از سوء استفاده رایانه‌ای، خرابکاری رایانه‌ای، اخاذی رایانه‌ای، نفوذ یافتن، جاسوسی، سرقت نرم‌افزار و دیگر شکل‌های سرقت محصولات (همان: ج ۲، ص ۱۳۲)

در دهه ۱۹۸۰ نظرهای علمی و عمومی در مورد جرم‌های رایانه‌ای تغییر یافت و معلوم شد جرم رایانه‌ای به جرم‌های اقتصادی محدود نیست و همه تعرض‌های انجام شده نسبت به منافع را شامل می‌شود. موج گسترده سرقت برنامه‌ها، سوء استفاده از صندوق‌های پرداخت و استفاده از مخابرات موجب شد تا حساسیت جامعه اطلاعاتی پرانگیخته شده و نیاز به راهبرد جدید امنیت داده‌پردازی و کنترل جرم احساس شود.

در حال حاضر بیشتر دیدگاه‌ها در زمینه جرم رایانه‌ای به انتقال غیرقانونی سرمایه‌ها با استفاده از ابزار الکترونیکی، خرابکاری، ویروس‌ها، کرم‌های رایانه‌ای و نیز جعل اسناد با استفاده از رایانه معطوف است (همان: ص ۵)

بطور مختصر، از بدو پیدایش جرایم رایانه‌ای در دهه ۱۹۶۰ میلادی تا کنون سه نسل جرایم رایانه‌ای مشخص شده است:

نسل اول؛ در دهه‌های ۶۰ و ۷۰ میلادی حاکم بود که از آن‌ها به عنوان جرایم رایانه‌ای در معنای خاص یاد می‌کنند. در آن زمان هنوز استفاده از اینترنت رواج نیافته بود و لذا محور جرایم رایانه‌ای، خود «رایانه» بود و رایانه به عنوان واسطه در عنصر مادی جرم مطرح بود. در آن زمان سرقت برنامه‌ها، دسترسی غیرمجاز، جاسوسی کامپیوتری، سابوتاژ کامپیوتری، استفاده غیرمجاز از سیستم‌های رایانه‌ای عمده جرایم رایانه‌ای را تشکیل می‌دادند.

نسل دوم؛ در دهه ۸۰ تا اوایل دهه ۹۰ میلادی و در پی گسترش تکنولوژی مخابراتی و خطوط تلفنی حاکم شد که اعمال خرابکارانه بر ضد خطوط تلفنی، خطوط ارتباطی و داده‌ها افزایش یافت به گونه‌ای که «داده» صرفنظر از این که در رایانه قرار داشته باشد یا در واسطه‌های انتقال،

مورد توجه قرار گرفت و به جای این که تأکید بر رایانه باشد، حمایت از «داده» مدنظر قرار گرفت و جرایم علیه داده‌ها که ترکیب تکنولوژی مخابراتی و تکنولوژی کامپیوتر است مصطلح شد.

نسل سوم؛ در آستانه هزاره سوم و از اوایل دهه ۹۰ میلادی جرایم سایبری رواج پیدا کرد (باستانی: ۱۳۸۳، ص ۴۹) که غالباً در فضای شبکه جهانی اینترنت قابل تحقق است.

در ایران، بین ورود رایانه به کشور تا وقوع جرایم رایانه‌ای حدود ۳۰ سال فاصله وجود دارد. به گفته بعضی محققان، رایانه از ابتدای ۱۳۴۰ - ۲۰ سال بعد از اختراع رایانه - وارد ایران شد. بانک ملی و شرکت نفت نخستین نهادهای استفاده کننده از رایانه در ۱۳۴۱ بودند. دانشگاه تهران در ۱۳۴۳ کار با رایانه را شروع کرد. در ۱۳۴۵ جمعاً ۹ رایانه و در ۱۳۴۹ جمعاً ۷۸ رایانه در ایران بود که اغلب اجاره‌ای بودند. میزان اجاره آنها در ۱۳۴۹، ۷۰۳ هزار دلار، در ۱۳۵۵، ۳۱۵ میلیون دلار و در ۱۳۵۶، ۴/۵ میلیون دلار بود. در ۱۳۵۶ تعداد رایانه‌های نصب شده در ایران به ۶۱۶ دستگاه رسید. (خرم آبادی: ۱۳۸۴، ص ۴۴)

این در حالی است که وقوع جرایم رایانه‌ای در ایران از دهه ۱۳۷۰ شروع شد. دادنامه مورخ ۱۳۷۲/۴/۳ شعبه ۶۵ دادگاه کیفری ۲ تهران در خصوص شکایت یک شرکت نرم‌افزاری رایانه علیه شرکت رایانه‌ای دیگر مبنی بر تکثیر و فروش غیرمجاز نرم‌افزار رایانه‌ای موجب شد دادگاه به استناد بند ۱۱ ماده ۲۳ قانون حمایت از حقوق مؤلفان و مصنفان و هنرمندان ۱۳۴۸ متهم را به تحمل مجازات محکوم و حکم به جلوگیری از ارائه نرم‌افزارهای تکثیر شده صادر نماید و بدین ترتیب با اعمال قوانین کیفری سنتی با جرم رایانه‌ای برخورد شد (همان: ص ۴۷)

مبحث دوم) تعریف جرایم رایانه‌ای

ارائه تعریف دقیق، جامع و مانع از جرایم رایانه‌ای از مشکل‌ترین مباحث در بررسی این جرایم است به گونه‌ای که در شماره ۴۴ نشریه

بین‌المللی سیاست جنایی وابسته به سازمان ملل اذعان شده که تعریف مورد توافقی در خصوص جرم رایانه‌ای وجود ندارد و شاید چنین تعریفی را هیچ‌گاه نتوان ارائه کرد. با این وجود، در این نشریه بین‌المللی اشاره شده که جرم رایانه‌ای در برگیرنده فعالیت‌های مجرمانه با ماهیت سنتی مانند سرقت و جعل و یا فعالیت‌های مجرمانه با ماهیت نوین یعنی راه‌های تازه برای سوء استفاده رایانه‌ای است (دزیانی: ۱۳۷۶، ج ۱، ص ۲۱). در توصیه نامه ۹ (۸۹) R شورای اروپا نیز تصریح شده که هر کوششی برای تعریف کردن جرم رایانه‌ای با نوعی نارسایی روبرو می‌شود. (پاکزاد: ۱۳۷۵، ص ۳۴)

انجمن بین‌المللی حقوق کیفری (AIDP) در نشست ۱۹۹۲ در دانشگاه ورتسبورگ آلمان نیز سرانجام نتوانست تعریفی از جرم رایانه‌ای ارائه کند و قرار شد به جای تعریف، فهرست حداقل جرم‌های مقرر در توصیه نامه ۹ (۸۹) R مبنای مشترک قرار گیرد (خرم‌آبادی، همان، ص ۵۶).

حقوق دانان و متخصصان این علم نیز از ارائه تعریف دقیق در مورد جرایم رایانه‌ای اظهار عجز نموده‌اند. پروفیسور ادوارد ام وایز استاد دانشگاه میشیگان در گزارشی که در مورد جرم رایانه‌ای در آمریکا برای AIDP انجمن بین‌المللی حقوق کیفری تهیه کرده اذعان نمود که هیچ تعریف مورد پذیرش همگانی در مورد جرم رایانه‌ای وجود ندارد (همان: ص ۵۷). اما در مورد علت سختی ارائه تعریف کامل از جرم رایانه‌ای نظرات مختلفی ارائه شده است. پروفیسور هنریک کاسپرسن استاد دانشگاه آمستردام، علت فقدان تعریف جامع از جرم رایانه‌ای را این می‌داند که اگر تعریفی با اصطلاحات بسیار کلی به دست داده شود فاقد ارزش توصیفی است و اگر دارای اصطلاحات اختصاصی باشد بسیار مضیق و محدود می‌شود. (جعفرپور: ۱۳۸۵، ج ۴، ص ۳۶) به عقیده بعضی دیگر، تفاوت سطح کاربری و بهره‌برداری از فناوری اطلاعات در کشورهای مختلف، نظرها و دیدگاه‌های مختلفی که مبنای تعریف جرم رایانه‌ای قرار گرفته‌اند و نیز تفاوت در نظام حقوق کیفری کشورهای مختلف، سه عاملی است که

باعث شده اجماع جهانی بر تعریف جرایم رایانه‌ای وجود نداشته باشد و خود تفاوت در تعریف، موجب اختلاف در تعیین مصداق‌های جرم رایانه‌ای شده است. (جورابراهیمیان: ۱۳۸۲ به نقل از خرم آبادی، همان، ص ۵۰)

با وجود این، نهادهای ملی و بین‌المللی متصدی مبارزه با جرایم رایانه‌ای و نیز متخصصان این رشته سعی نموده‌اند تعاریفی از جرم رایانه‌ای ارائه نمایند.

گروه متخصصان جرم رایانه‌ای سازمان همکاری و توسعه اقتصادی (OECD) در گزارش «جرم کامپیوتری - تحلیل سیاست‌های قانونی» در سال ۱۹۸۶ به جای استفاده از اصطلاح جرم رایانه‌ای، اصطلاح "سوء استفاده از رایانه" را بکار برده و اعلام نموده است: «سوء استفاده از کامپیوترها شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار انتقال داده‌هاست.» (پاکزاد: ۱۳۸۴، ص ۸۳)

طبق تعریف وزارت دادگستری آمریکا، جرم رایانه‌ای عبارت است از هر اقدامی غیرقانونی که برای ارتکاب، پی‌جویی یا پیگرد قضایی آن، بهره‌برداری از دانش فناوری رایانه‌ای ضروری است. (پرویزی: ۱۳۸۲، ص ۶)

حقوق‌دانان کانادایی جرم رایانه‌ای را هر نوع فعالیت مجرمانه‌ای می‌دانند که در برگیرنده کپی، استفاده، جابجایی، ملاحظه، دسترسی یا سوء استفاده از سیستم‌های رایانه‌ای، عملکرد رایانه، داده‌ها یا برنامه‌های رایانه‌ای است. (شریفی: ۱۳۸۲، ص ۸۰)

اگوست بگوئیک هم با بکار بردن اصطلاح "سوء استفاده از رایانه" به جای اصطلاح "جرم رایانه‌ای" معتقد است سوء استفاده از کامپیوتر شامل هر واقعه‌ای است که با تکنولوژی کامپیوتر توأم شود و بواسطه آن بزه دیده متحمل خساراتی گردد یا مرتکب به عمد مال یا منفعتی کسب کند. (بگوئیک: ۱۹۹۰، ص ۴۶) از نظر پروفیسور شیک، حقوق دان اتریشی، جرم رایانه‌ای عبارت است از هر عمل مجرمانه‌ای که رایانه وسیله یا راه ارتکاب آن باشد (شریفی: همان).

طبق تعریف دکتر آتسوشی یاماگوجی، حقوق دان ژاپنی، جرم رایانه‌ای عبارت است از جرم‌های دربرگیرنده اعمال همراه با بی‌مبالاتی یا حوادثی که عملکرد یک سیستم رایانه‌ای را مختل کرده یا از آن استفاده غیر قانونی می‌کند. (جعفرپور: ۱۳۷۶، ص ۳۶) کمیته مشورتی جرم رایانه‌ای هلند، در یک تعریف متفاوت اظهار نموده که جرم رایانه‌ای عبارت است از رفتار همراه با قصد مجرمانه که موجب آسیب به منافع خاص ناشی از پردازش خودکار داده‌ها باشد (همان).

بعضی از صاحب نظران کشور ما کوشیده‌اند از حیث دامنه شمول جرم رایانه ای، تعاریف سه گانه از این جرایم ارائه دهند: (خرم آبادی، همان، ص ۷۴)

الف) تعریف مضیق: «هر جرمی که قانون گذار به صراحت رایانه را به منزله موضوع یا وسیله جرم جزء رکن مادی آن اعلام کرده است.»
 ب) تعریف موسع: «هر جرمی که عملاً رایانه به منزله موضوع یا وسیله ارتکاب جرم در آن نقش داشته باشد.»
 ج) تعریف بسیار موسع: «هر جرمی که رایانه به منزله موضوع یا ابزار آن نقش داشته باشد یا دلایل و اطلاعات مربوط به آن در رایانه ذخیره یا پردازش یا منتقل شده باشد.»

تعریف مضیق خود دو دسته از جرایم را در برمی‌گیرد:

- جرم رایانه‌ای محض: جرایمی که ارتکاب آن‌ها قبل از پیدایش رایانه و اجزای فناوری اطلاعات امکان پذیر نبوده‌اند مانند دسترسی غیرمجاز.
- جرایم رایانه‌ای سنتی: جرایمی که ارتکاب آن‌ها وسیله رایانه دارای عواقبی بسیار شدید نسبت به ارتکاب سنتی آن است مانند برخی جرایم مرتبط با محتوا نظیر هرزه نگاری و یا تخریب فیزیکی نسبت به کامپیوتر.

تعریف موسع علاوه بر جرایم مضیق، آن دسته از جرایم، سنتی که با استفاده از رایانه و فناوری اطلاعات ارتکاب یابند، بدون این که تغییری در

عنصر مادی آنها صورت گرفته باشد یا مقنن رایانه را جزء این عنصر برشمرده باشد مشمول این عنوان می‌داند مثل توهین به یک فرد از طریق ایمیل یا تخریب عمدی تجهیزات رایانه‌ای.

تعریف بسیار موسع علاوه بر دو دسته قبل، جرایمی که صرفاً دلایل آن‌ها یا اطلاعات مربوطه در رایانه ذخیره شده‌اند، به لحاظ تأمین بهتر اهداف تحقیق و تعقیب جرم با در نظر گرفتن قواعد خاص آیین دادرسی کیفری جزء جرایم رایانه‌ای دانسته است. (همان: ص ۷۵ و ۷۶)

با نگاهی به تعاریفی که ذکر شد می‌توان گفت: "جرم رایانه‌ای شامل هر جرمی است که رایانه به عنوان موضوع یا وسیله ارتکاب جرم بکار رود." با وجود این، به نظر می‌رسد ارائه تعریف از جرم رایانه‌ای نه تنها کاری دشوار است، بلکه ثمره خاصی نیز بر آن مترتب نیست و حتی امکان تفکیک بین جرایم سنتی که از طریق رایانه ارتکاب می‌یابد با جرایم رایانه‌ای نیز بر مبنای تعاریف ارائه شده دشوار می‌گردد. بنابراین روش درست آن است که بدون درگیر شدن در مفهوم جرایم رایانه‌ای، همانند بسیاری از موارد دیگر، قانون‌گذار با در نظر گرفتن نقش مؤثر رایانه به عنوان موضوع یا وسیله ارتکاب جرم، مصادیق جرم رایانه‌ای را تعیین نماید. این روش، نه تنها در اسناد بین‌المللی مربوط به جرایم رایانه‌ای، بلکه در قوانین داخلی بسیاری از کشورها از جمله قانون جرایم رایانه‌ای ایران - با وجود نواقصی که در احصای جرایم وجود دارد - در پیش گرفته شده است.

مبحث سوم) مصادیق جرایم رایانه‌ای

همان‌گونه که گفته شد، در بسیاری از اسناد بین‌المللی و منطقه‌ای و نیز قوانین بیشتر کشورها به جای تعریف جرم رایانه‌ای، مصادیق آن بر شمرده شده است. جهت سهولت مطالعه و نیز امکان مقایسه و بررسی تطبیقی، مصادیق جرایم رایانه‌ای را در دو بخش اسناد بین‌المللی و منطقه‌ای و قوانین داخلی بطور جداگانه مورد بررسی قرار خواهیم داد.

گفتار نخست: مصادیق جرایم رایانه‌ای در اسناد بین‌المللی و منطقه‌ای

سازمان‌های منطقه‌ای و بین‌المللی اقدامات متعددی برای مبارزه با جرایم و سوء استفاده از سیستم‌های رایانه‌ای و امکانات گسترده‌ای که رایانه و فن آوری اطلاعات در اختیار بشر قرار داده در پیش گرفته‌اند. علت حساسیت این نهادها نسبت به جرایم رایانه‌ای آن است که علاوه بر تسهیل وقوع جرایم سنتی با استفاده از رایانه و بویژه فضای مجازی، پیشرفت‌های فنی در این زمینه، موجب بروز و ظهور انواع جدید از جرایمی شده که صرفاً در فضای اینترنت قابل وقوع بوده و تا پیش از پیدایش چنین فضایی امکان تحقق چنین جرایمی اصولاً وجود نداشت. یکی از مهم‌ترین اقدامات بلکه مقدمه سایر تدابیر جهت مبارزه با جرایم رایانه‌ای، شناسایی اقسام و مصادیق جرایم مورد نظر است. مهم‌ترین مصادیق جرایم رایانه‌ای در اسناد منطقه‌ای و بین‌المللی ذیلاً مورد اشاره قرار می‌گیرد:

الف) فهرست سازمان توسعه و همکاری اقتصادی

سازمان توسعه و همکاری اقتصادی (OECD) یکی از اولین نهادهایی است که بطور جدی تعیین جرایم رایانه‌ای را در دستور کار خود قرار داده و در واقع اولین فهرست جرایم رایانه‌ای را ارائه نموده است (پاکزاد: همان، ص ۸۲). یک کمیته اختصاصی از این سازمان در سال‌های ۱۹۸۳ تا ۱۹۸۵ راه کارهای هماهنگی بین‌المللی قوانین کیفری برای مقابله با جرایم اقتصادی مرتبط با رایانه را مورد بررسی قرار داد. این کمیته در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه‌ای و تحلیل سیاست‌های قضایی در مورد اقدامات پیشنهادی به کشورهای عضو برای مبارزه با جرایم رایانه‌ای ارائه نمود که در ضمن این گزارش، فهرستی از رفتارهایی که باید از سوی کشورهای عضو جرم‌انگاری شود را به شرح زیر اعلام نمود:

۱. ورود، تغییر، پاک کردن یا متوقف‌سازی داده‌ها یا برنامه‌های رایانه‌ای که به طور ارادی و به قصد انتقال غیرقانونی وجوه یا هرچیز با ارزش دیگر صورت می‌گیرد؛
۲. ورود، تغییر، پاک کردن یا متوقف‌سازی داده‌ها یا برنامه‌های رایانه‌ای که به شکل عمدی یا به قصد ارتکاب جعل صورت می‌گیرد؛
۳. ورود، تغییر، پاک کردن یا متوقف‌سازی داده‌ها یا برنامه‌های رایانه‌ای یا هرگونه مداخله‌ی دیگر در سیستم‌های رایانه‌ای که به شکل عمدی و به قصد جلوگیری از عملکرد سیستم رایانه‌ای یا ارتباطات صورت می‌گیرد؛
۴. تجاوز به حقوق انحصاری مالکیت برنامه رایانه‌ای محافظت‌شده به قصد بهره‌برداری تجاری از آن برنامه و ارائه آن به بازار؛
۵. دستیابی یا شنود در یک سیستم رایانه‌ای یا ارتباطی به‌طور آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور، اعم از آنکه با تخطی از تدابیر امنیتی صورت گیرد یا با هدف غیرشرافت‌مندانه.

ب) فهرست کمیته وزرای شورای اروپا

کمیته تخصصی کارشناسان جرایم رایانه‌ای شورای اروپا که کارهای تحقیقاتی پیرامون جرایم رایانه‌ای را از سال ۱۹۸۵ آغاز کرده بود، در سال ۱۹۸۹ یک گزارش و یک توصیه نامه به کمیته اروپایی مسائل مربوط به جرم ارائه کرد. کمیته اخیر الذکر نیز پس از بررسی و تایید گزارش و توصیه نامه، آن را به کمیته وزیران شورای اروپا ارسال نمود و پس از تایید آن توسط وزیران، به کشورهای عضو فرستاده شد. در توصیه نامه شماره ۹ (۸۹) R سال ۱۹۸۹ کمیته وزرای شورای اروپا یک فهرست اجباری و یک فهرست اختیاری برای جرم انگاری جرایم رایانه‌ای به کشورها ارائه کرده

است. مصادیق مذکور در این توصیه نامه که بعدها در اسناد سازمان ملل نیز بر آن تاکید شده بدین شرح است:

الف) فهرست حداقل (اجباری):

- ۱- کلاه برداری رایانه‌ای
 - ۲- جعل رایانه‌ای
 - ۳- ایراد خسارت به داده‌ها یا برنامه‌های رایانه‌ای
 - ۴- خرابکاری رایانه‌ای
 - ۵- دستیابی غیرمجاز
 - ۶- شنود غیرمجاز رایانه‌ای
 - ۷- ارائه و ایجاد مجدد و غیر مجاز یک برنامه رایانه‌ای حمایت شده
 - ۸- ارائه و ایجاد مجدد و غیرمجاز یک نیمه‌هادی
- ب) فهرست حداکثر (اختیاری):

- ۱- تغییر داده‌ها یا برنامه‌های رایانه‌ای
 - ۲- جاسوسی رایانه‌ای
 - ۳- استفاده غیرمجاز از رایانه
 - ۴- استفاده غیرمجاز از برنامه رایانه‌ای حمایت شده
- ج) طبقه‌بندی جرایم رایانه‌ای از سوی پلیس بین‌الملل سازمان پلیس بین‌الملل جزایی (اینتراپل) در راهنمای جرایم رایانه‌ای که در سال ۲۰۰۱ از سوی کارگروه اروپایی جرم رایانه‌ای این سازمان منتشر شد، موارد زیر را به عنوان مصادیق جرایم رایانه‌ای ذکر نموده است:

- الف) دستیابی غیرمجاز شامل:
- ۱ - نفوذ غیرمجاز (هک) ۲ - شنود غیرمجاز ۳ - سرقت زمان رایانه.
- ب) تغییر داده‌های رایانه‌ای شامل:
- ۱ - تغییر داده‌ها از طریق انتشار بمب منطقی ۲ - تغییر داده‌ها از طریق انتشار اسب تروا ۳ - تغییر داده‌ها از طریق انتشار ویروس رایانه‌ای ۴ - تغییر داده‌ها از طریق انتشار کرم رایانه‌ای.

ج) کلاه برداری رایانه‌ای شامل:

- ۱ - سوء استفاده از صندوق‌های پرداخت خودکار (AIM) ۲ - جعل رایانه‌ای ۳ - سوء استفاده از ماشین‌های بازی ۴ - دستگیری در مرحله ورودی و خروجی ۵ - سوء استفاده از ابزار پرداخت مستقر در فروشگاه‌ها ۶ - سوء استفاده از تلفن (برای شنود یا استفاده از خدمات مخابرات)

د) تکثیر غیرمجاز شامل:

- ۱ - تکثیر بازی‌های رایانه‌ای ۲ - تکثیر نیمه‌هادی ۳ - تکثیر نرم افزارهای دیگر

ه) خرابکاری رایانه‌ای شامل:

- ۱ - خرابکاری نسبت به سخت افزار ۲ - خرابکاری نسبت به نرم افزار و سایر جرایم رایانه‌ای شامل:

- ۱ - سرقت اسرار تجاری (افشاء، انتقال و استفاده از اسرار تجاری) ۲ - ذخیره سازی و پخش هرزه‌نگاری کودک و نرم افزار غیرقانونی از طریق تابلو اعلانات الکترونیکی. ۳ - سایر محتویات و مطالب قابل تعقیب. (پرویزی: همان، ص ۲۴ - ۳۲)

ج) طبقه بندی کنوانسیون جرایم سایبر

کنوانسیون جرایم سایبر در ۲۳ سپتامبر ۲۰۰۱ در بوداپست مجارستان به امضای کشورهای عضو شورای اروپا، آمریکا، ژاپن، کانادا، و آفریقای جنوبی رسید و در حال حاضر معتبرترین سند بین المللی در زمینه جرایم رایانه‌ای است.

طبق ادعای شورای اروپا، کنوانسیون جرایم سایبر، طرح کنوانسیون سازمان ملل برای سایر کشورها است. اصطلاح جرایم سایبری به جرایمی گفته می‌شود که در فضای مجازی که اینترنت آن را ایجاد می‌کند ارتکاب می‌یابند لذا جرایم سایبری زیرمجموعه‌ای از جرایم اینترنتی و به تبع زیرمجموعه‌ای از جرایم رایانه‌ای است. بطور ویژه، نسل سوم جرایم رایانه‌ای را "جرایم سایبری" نامیده‌اند. البته کنوانسیون جرایم سایبری، جرایم رایانه‌ای را به عنوان یکی از مصادیق جرایم سایبری ذکر کرده که شاید به این علت است که مهم‌ترین جرایم رایانه‌ای جرایم سایبری هستند

و از این جهت جرایم سایبری را معادل جرایم رایانه‌ای تلقی کرده است. انواع جرایم اینترنتی و سایبری مذکور در این کنوانسیون از این قرار است: الف) جرایم علیه محرمانگی، تمامیت و در دسترس بودن داده‌ها و سیستم‌های رایانه‌ای شامل:

- ۱- دسترسی غیر قانونی
- ۲- قطع و شنود غیرقانونی
- ۳- اختلال در داده‌ها
- ۴- اختلال در سیستم
- ۵- سوء استفاده از دستگاه‌ها و وسایل

ب) جرایم مرتبط با رایانه شامل:

- ۱- جعل مرتبط با رایانه
- ۲- کلاهبرداری مرتبط با یارانه

ج) جرایم مرتبط با محتوا شامل:

جرایم مرتبط با هرزه‌نگاری کودکان

د) جرایم مرتبط با تعرض به حق نشر و حقوق مربوطه به آن شامل:

- ۱- جرایم نقض حق مؤلف

۲- جرایم نقض حقوق مرتبط با حق مؤلف. (۴، CYBERCRIME, CONVENTION ON 2001,p)

د) اقسام جرایم رایانه‌ای در قطعنامه مجمع عمومی سازمان ملل

در قطعنامه کنگره دهم سازمان ملل متحد درباره پیشگیری از جرم و اصلاح مجرمین تحت عنوان "جرم‌های مرتبط با رایانه"، سه دسته جرایم رایانه‌ای بدین شرح احصاء شده است:

الف. جرم‌های ارتكابی علیه فناوریها و کاربران آنها

۱. دستیابی غیرمجاز به رایانه یا سیستم‌های رایانه‌ای؛
۲. استفاده غیرمجاز از سیستم‌های رایانه‌ای؛
۳. خواندن، کپی کردن یا کپی گرفتن داده بدون اجازه؛
۴. ایجاد یا تمهید برنامه‌های مهاجم؛
۵. تخریب داده‌ها و سیستم‌های رایانه‌ای مورد استفاده‌ی عموم و خرابکاری رایانه‌ای؛

ب. جرم‌های سنتی ارتكابی با استفاده از رایانه یا فناوریهای ارتباطی

۱. جرمهای مربوط به محتوای مجرمانه؛
 ۲. کودکربایی اینترنتی (به منظور سوءاستفاده جنسی)؛
 ۳. کلاهبرداری؛
 ۴. جاسوسی صنعتی یا تجاری؛
 ۵. جرمهای مربوط به مالکیت فکری؛
 ۶. قاچاق؛
 ۷. پولشویی؛
- ب. استفاده از فناوری برای حمایت از دیگر فعالیتهای مجرمانه. (پاکزاد: همان، ص ۱۲۶)

قوانین داخلی کشورها نیز طبقه بندی‌های خاصی از جرایم رایانه‌ای ارائه کرده‌اند: مثلاً در قانون جرایم کامپیوتری ایالت ویسکونسین آمریکا مصوب ۱۹۸۱ (فصل ۲۹۳) این جرایم شامل جرایم علیه داده‌ها و برنامه‌های کامپیوتری و جرایم علیه کامپیوتر و تجهیزات کامپیوتری است. جرم تغییر، تخریب، اتلاف و کپی کردن داده‌ها از نوع جرایم نخست و جرم تغییر تجهیزات، تخریب و ایراد خسارت و استفاده غیرمجاز از کامپیوتر در زمره جرایم دسته دوم است (زراعت: ۱۳۸۵، ص ۱۶۲). در قوانین داخلی کشور ما نیز بویژه در قانون جرایم رایانه‌ای طبقه بندی خاصی وجود دارد که در گفتار بعدی مورد بررسی قرار خواهد گرفت.

گفتار دوم: مصادیق جرایم رایانه‌ای در قوانین داخلی

هر چند ارتکاب جرایم رایانه‌ای و استفاده از رایانه به عنوان وسیله ارتکاب جرم در ایران تقریباً هم زمان با رواج شبکه‌های رایانه‌ای در اواخر دهه ۱۲۶۰ شمسی شروع شد، ارتکاب این جرایم با شروع دهه ۱۳۸۰ رو به فزونی نهاده است. علت رشد ارتکاب این جرایم، انتشار کتب، جزوه‌ها، سی دی‌های آموزشی و دسترسی آسان تر به اینترنت دانسته شده است (پرویزی: همان، ص ۱۳۶).

به نظر نگارنده، یکی از علل رواج جرایم رایانه‌ای در ایران - همانند سایر کشورها -، را باید در تغییر ذائقه بزه کاری جستجو نمود بدین معنا

که رفته رفته نوع جرایم از ماهیت خشونت آمیز به سمت ماهیت نرم در حال تغییر است و بزه کاران به جای استفاده از قدرت بدنی از قدرت فکری خود برای ارتکاب جرایم استفاده می‌کنند و در این راستا جرایم رایانه‌ای ضمن این که ماهیتی غیرخشونت بار دارند، عمدتاً عواید مالی سرشاری نصیب مجرمین رایانه‌ای می‌نمایند. از این رو بیشتر بزه کاران رایانه‌ای در زمره مجرمین یقه سفید قرار دارند.

در نظام حقوقی ایران، هر چند مبانی فقهی نظیر قاعده حرمت اکل مال به باطل، قاعده لاضرر، حرمت تجسس، امکان برخورد با مصادیق جرایم رایانه‌ای را فراهم می‌آورد (بای: ۱۳۸۸، ص ۲۰۵)، با وجود این، اقدامات تقنینی نیز از سال ۱۳۸۲ با تصویب قانون مجازات نیروهای مسلح شروع شده و با تصویب قانون جرایم رایانه‌ای به اوج خود رسیده است و به موازات آن، نهادهای پلیسی و امنیتی و نیز نهادهای قضایی به این پدیده واکنش نشان داده‌اند. در قوانین داخلی نیز به جای تعریف جرم رایانه‌ای مصادیق آن مورد توجه قرار گرفته است.

الف) قانون مجازات جرایم نیروهای مسلح

اولین متن قانونی که در کشور ما ارتکاب جرایم رایانه‌ای را مورد توجه قرار داد، قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲ / ۱۰ / ۹ بود. ماده ۱۳۱ این قانون مقرر نموده است: "هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تاخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیرمجاز توسط 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 آن اطلاعات را ندارند، افشاء غیرمجاز اطلاعات، سرقت اشیاء دارای ارزش اطلاعاتی مانند سی دی یا دیسکتهای حاوی اطلاعات یا معدوم کردن آنها یا سوء استفاده‌های مالی که نظامیان به وسیله رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازاتهای مندرج در مواد مربوط به این قانون می‌باشند."

هر چند ماده ۳۱ انواع مصادیق جرایم رایانه‌ای را از هم تفکیک نکرده

با این حال جرایم مرتبط با رایانه مذکور در این ماده شامل موارد زیر است:

- ۱ - جعل رایانه‌ای
- ۲ - جاسوسی رایانه‌ای
- ۳ - افشای غیر مجاز اطلاعات رایانه‌ای
- ۴ - سرقت حامل‌های اطلاعاتی رایانه‌ای
- ۵ - سوء استفاده مالی از طریق رایانه (ارتشاء، اختلاس، اخاذی و ...)

ب) قانون تجارت الکترونیک

یکی از مهم ترین علل افزایش میزان و تنوع جرایم رایانه ای، گسترش تجارت الکترونیکی و اینترنتی است که به جهت مزایای فوق العاده‌ای که دارد بیش از پیش مورد استفاده اشخاص و شرکت‌های بازرگانی قرار می‌گیرد. تجارت الکترونیکی هر نوع تجارت یا معامله اداری یا تبادل اطلاعاتی است که با استفاده از هر گونه اطلاعات و فناوری ارتباطات به اجرا در می‌آید. (پنلوپ لارنس: ۱۳۸۳، ص ۲۱۱)

در واقع "اقتصاد نوین" مبتنی بر اینترنت، بازرگانی الکترونیکی و تجارت الکترونیکی حاکی از پیشرفت جدیدی در سیر تکامل حیات بشری است، اما در عین حال، این امر خود ابزارهای جدید ارتکاب جرایم اقتصادی را فراهم آورده که در کنار سلاح‌های شیمیایی، باکتریولوژی و اتمی جزء چالش‌های عمده جهانی محسوب می‌گردد. (رادو: ۲۰۰۸، ص ۲۰۱)

برخورد با جرایم تجارت الکترونیکی مستلزم وضع قوانین دقیق در این زمینه است. در ایران نیز پس از مدت‌ها بحث و بررسی، قانون تجارت الکترونیکی برای سروسامان دادن به مبادلات الکترونیکی و بازار خرید و فروش اینترنتی، در تاریخ ۱۳۸۲/۱۰/۱۷ به تصویب مجلس شورای اسلامی رسید. در باب چهارم این قانون تحت عنوان جرایم و مجازات‌ها، طی چهار مبحث جرایم قابل تحقق در بستر مبادلات الکترونیکی شامل موارد

زیر دانسته شده است:

- کلاه برداری کامپیوتری
- جعل کامپیوتری
- نقض حقوق انحصاری در بستر مبادلات الکترونیکی شامل:
 - نقض حقوق مصرف کننده و قواعد تبلیغ؛
 - نقض حمایت از داده پیام‌های شخصی (حمایت از داده).
- نقض حفاظت از داده پیام در بستر مبادلات الکترونیکی شامل:
 - نقض حق مؤلف
 - نقض اسرار تجاری
 - نقض علایم تجاری

ج) قانون جرایم رایانه‌ای

قانون جرایم رایانه‌ای در تاریخ ۱۳۸۸/۳/۵ در ۵۶ ماده و ۲۵ تبصره به تصویب مجلس شورای اسلامی رسید. با توجه به این که کشور ما در سال‌های اخیر شاهد پیشرفت‌های چشمگیری در زمینه دسترسی و استفاده نهادهای دولتی و عمومی و مردم عادی از رایانه و شبکه‌های اینترنتی بوده است، تصویب این قانون گام مهمی در جهت تکامل حقوق ایران و برآورنده نیاز اساسی جامعه ما به شمار می‌آید. قانون مورد بحث دارای اشکالاتی هم چون ابهام در شمول نسبت به بعضی جرایم یا هم پوشانی با بعضی قوانین دیگر است. به عنوان نمونه ماده (۱۴) قانون جرایم رایانه‌ای، ذیل فصل چهارم تحت عنوان «جرایم علیه عفت و اخلاق عمومی» مقرر نموده است: «هر کس به وسیله سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را تولید، ارسال، منتشر، توزیع یا معامله کند یا به قصد ارسال یا انتشار یا تجارت تولید یا ذخیره یا نگهداری کند به حبس از ۹۱ روز تا ۲ سال یا جزای نقدی از ۵ تا ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد.» از سوی دیگر، در ماده ۱۰ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت

غیرمجاز می‌نمایند اصلاحی مصوب ۱۳۷۹، اصلاحی ۱۳۸۷ مقرر شده است: "انتشار آثار مستهجن و مبتذل از طریق ارتباطات الکترونیکی و سایتهای کامپیوتری یا وسیله و تکنیک مشابه دیگر از مصادیق تکثیر و انتشار محسوب و مرتکب حسب مورد به مجازات مقرر در این قانون محکوم می‌شود." بنابراین، در تطبیق حکم بر مورد خارجی انتشار اثر مستهجن ابهام وجود دارد.

بعضی نویسندگان نیز ایرادات دیگری بر این قانون وارد نموده‌اند از جمله این که ادعا شده سیاست سختگیرانه (تساهل صفر) بر فضای قانون مذکور حاکم است (رایجیان اصلی: ۱۳۸۸، ص ۴۱۱). البته در این مقاله مجالی برای بررسی ایرادات قانون مذکور و نقد ایرادات مطرح شده بر آن وجود ندارد و صرفاً نگاهی گذرا به مصادیق مذکور در این قانون خواهیم داشت. در این قانون، جرایم رایانه‌ای به پنج دسته تقسیم شده است:

فصل یکم تحت عنوان "جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی"، شامل سه عنوان مجرمانه "دسترسی غیرمجاز"، "شنود غیرمجاز" و "جاسوسی رایانه‌ای" است.

عنوان فصل دوم از جرایم رایانه‌ای، "جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی" است که شامل دو مبحث "جعل رایانه‌ای"، "تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی" است.

فصل سوم از این جرایم نیز شامل "سرقت و کلاه برداری مرتبط با رایانه" است.

در فصل چهارم، "جرایم علیه عفت و اخلاق عمومی" جرم‌انگاری شده‌اند.

و نهایتاً فصل پنجم نیز "هتک حیثیت و نشر اکاذیب" از طریق سامانه‌های رایانه‌ای یا مخابراتی را جرم‌انگاری نموده است.

از آن جا که قانون جرایم رایانه‌ای اصلی ترین قانون مربوط به جرایم رایانه‌ای است، ایجاب می‌کند حتی الامکان جامع اشکال مهم و پرخطر جرایم رایانه‌ای باشد به گونه‌ای که برای مقابله با بعضی از جرایم رایانه‌ای

باخلاقاً قانونی مواجه نباشیم، در حالی که قانون مذکور جرایمی نظیر ارتشاء، اختلاس، خیانت در امانت، اخاذی، پول شویی رایانه‌ای و مواردی از جرایم علیه مالکیت فکری نظیر نقض اسرار و علائم تجاری و نیز جرایمی نظیر تبلیغ علیه نظام، تحریک به جنگ و کشتار، توهین به مقدسات و... را بطور کامل پوشش نمی‌دهد.

نتیجه:

جرایم رایانه‌ای سه مرحله مختلف را پشت سر گذاشته است: نسل اول در دهه ۶۰ و ۷۰ پیدا شد که در آن دوره محور جرایم، خود «رایانه» به عنوان واسط در عنصر مادی جرم مطرح بود. نسل دوم در دهه ۸۰ تا اوایل دهه ۹۰ رایج بود. در این دوره به جای این که تأکید بر رایانه باشد، حمایت از «داده» مدنظر قرار گرفت. نسل سوم در آستانه هزاره سوم و از اوایل دهه ۹۰ میلادی جرایم سایبری رواج پیدا کرد.

ارائه تعریف واحد، جامع و مانع از جرایم رایانه‌ای امری است که غالب پژوهشگران بر دشواری آن اذعان نموده و در اسناد بین‌المللی و منطقه‌ای نیز چنین تعریفی مشاهده نمی‌شود. هر چند تعریف جرم رایانه‌ای به "جرمی که در آن رایانه به عنوان موضوع یا وسیله ارتکاب جرم دخالت دارد" جامع‌ترین تعریفی است که می‌توان ارائه نمود، با وجود این، به نظر نگارنده احصاء دقیق مصادیق جرایم رایانه‌ای بهتر از ارائه تعریف است. از این روی، روش ذکر مصادیق جرایم رایانه‌ای به جای ارائه تعریف، نه تنها در اکثر اسناد بین‌المللی و منطقه‌ای، بلکه در قوانین داخلی ایران نیز بویژه قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای در پیش گرفته است.

آخرین طبقه‌بندی جرایم رایانه‌ای را در قانون جرایم رایانه‌ای می‌توان دید. در این قانون، مصادیق جرایم رایانه‌ای تحت عناوین کلی "جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی"، "جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی"، "سرقت و کلاه برداری مرتبط با رایانه"، "جرایم علیه عفت و اخلاق عمومی" و نهایتاً "هتک حیثیت و نشر اکاذیب" از طریق سامانه‌های رایانه‌ای یا

مخابراتی ذکر شده است. با وجود این، قانون مذکور جرایمی نظیر ارتشاء، اختلاس، خیانت در امانت، اخاذی، پول شویی رایانه‌ای و مواردی از جرایم علیه مالکیت فکری نظیر نقض اسرار و علائم تجاری و نیز جرایمی نظیر تبلیغ علیه نظام، تحریک به جنگ و کشتار، توهین به مقدسات و... را بطور کامل پوشش نمی‌دهد.

منابع

۱. باستانی، برومند، (۱۳۸۳)، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران، بهنامی، چاپ اول
۲. بای، حسینعلی و پورقهرمانی، بابک، (۱۳۸۸)، بررسی فقهی حقوقی جرایم رایانه‌ای، قم، پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول
۳. پاکزاد، بتول، (۱۳۸۴)، اقدام‌های سازمان‌های بین‌المللی و منطقه‌ای در خصوص جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، قوه قضائیه، معاونت حقوقی و توسعه قضایی، سلسبیل
۴. پاکزاد، بتول، (۱۳۷۵)، جرایم کامپیوتری، پایان‌نامه کارشناسی ارشد دانشکده حقوق دانشگاه شهید بهشتی
۵. پرویزی، رضا، (۱۳۸۲)، جزوه جرایم کامپیوتری، مرکز مطالعات توسعه قضایی
۶. پرویزی، رضا، (۱۳۸۴)، جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، قوه قضائیه، معاونت حقوقی و توسعه قضایی، سلسبیل
۷. پنلوپ، لارنس، (۱۳۸۳)، کاربرد اینترنت در حقوق، ترجمه سید قاسم زمانی و مهناز بهراملو، تهران، نشر میزان، چاپ اول
۸. جعفرپور، ناهید، (۱۳۸۵)، جرم کامپیوتری و دیگر جرایم علیه تکنولوژی اطلاعات در ژاپن، جزوه جرایم کامپیوتری، ج ۴، شورای عالی انفورماتیک
۹. جورابراهیمیان، نجات‌ا...، (۱۳۸۲)، جزوه جرایم رایانه‌ای در حقوق فرانسه، کمیته مبارزه با جرایم رایانه‌ای مرکز مطالعات توسعه قضایی
۱۰. خرم‌آبادی، عبدالصمد، (۱۳۸۴)، تاریخچه، تعریف و طبقه‌بندی جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، قوه قضائیه، معاونت حقوقی و توسعه قضایی، سلسبیل

۱۱. دزیانی، محمد حسن، (۱۳۷۶)، نشریه بین المللی سیاست جنایی سازمان ملل، شماره‌های ۳۳ و ۳۴، جزوه جرایم کامپیوتری، ج ۱، شورای عالی انفورماتیک
۱۲. رایجیان اصلی، مهرداد (۱۳۸۸)، قانون جرایم رایانه‌ای نوآوری‌ها و کاستی‌ها، مجله پژوهش‌های حقوقی، سال هشتم، شماره ۱۵، تابستان ۸۸
۱۳. زراعت، عباس، (۱۳۸۵)، حقوق جزای اختصاصی تطبیقی - ۲، جرایم علیه اموال و مالکیت، تهران، ققنوس
۱۴. زیبر، اولریش، (۱۳۸۵)، پیدایش بین‌المللی حقوق کیفری اطلاعات، ترجمه محمد حسن دزیانی، جزوه جرایم کامپیوتری، ج ۲ و ۳
۱۵. سلمانی زاده، محمود، (۱۳۸۰)، جنگ اطلاعات و امنیت، خبرنامه انفورماتیک، شماره ۸۰، آذر و دی
۱۶. شریفی، مرسله، (۱۳۸۲)، جرایم کامپیوتری در حقوق جزای بین‌الملل، پایان نامه کارشناسی ارشد دانشگاه آزاد اسلامی تهران
17. Chris reed and John angel, 2007. Computer Law, Oxford University Press, Sixth edition first published
18. August Beguaic, 1990. Computer related Crime, Published by: Council of Europe, Strasbourg
19. Convention on Cyber Crime, Budapest, 23.XI.2001: <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc>
20. Ioan Radu, Computer Crime - A Threat to the Informational Society, Economic Studies Academy of Bucharest, 2008