بررسی عناصر تشکیل دهنده مادی و معنوی مصادیق جرایم رایانه ای

(تاریخ دریافت۱۳۹۶/۱۲/۲۲ ، تاریخ تصویب ۱۳۹۷/۰۴/۰۸)

مختارفتاحی

دانشجوی دکترای حقوق کیفری و جرم شناسی

چکیده

قانون جرایم رایانه ای مصوب ۱۳۸۸یکی از کامل ترین قوانین در زمینه جرایم مربوط به فضای مجازی و رایانه ای می باشد. در این قانون در فصل اول: جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی، شامل؛ دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه ای، در فصل دوم: جرائم علیه صحت و تمامیت داده ها و سیستم های رایانه ای و مخابراتی، شامل؛ جعل رایانه ای، تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی در فصل سوم سرقت و کلاهبرداری مرتبط با رایانه، در فصل چهارم: جرایم علیه عفت و اخلاق عمومی، در فصل پنجم: هتک حیثیت و نشر اکاذیب و در فصل هفتم سایر جرایم جرم انگاری شده اند.

واژگان کلیدی: جرایم رایانه ای، رایانه، فضای سایبر، داده، مجازات

بخش اول: کلیات

بحث جرایم رایانه‌ای در ایران ابتدا در اوایل دهه ۱۳۸۰ مطرح شد. آن زمان بیشتر حوزه‌هایی را در بر می‌گرفت که به جعل اسناد دولتی و شخصی مربوط می‌شد. چنانکه اولین جرم رایانه‌ای در خرداد ۱۳۷۸ به ثبت رسید که در آن یک دانشجوی کامپیوتر و یک کارگر چاپخانه در کرمان، چک‌های تضمینی را جعل می‌کردند. جعل اسکناس، بلیت شرکت‌های اتوبوسرانی، جعل اسناد دولتی از قبل گواهینامه رانندگی، کارت پایان خدمت، مدرک تحصیلی، اوراق خرید و فروش خودرو و چک‌های مسافرتی از دیگر موارد جرم رایانه‌ای در اوایل دهه ۸۰ به حساب می‌آمد. پیشرفت تکنولوژی و علم و دست یابی بشر به فناوری اطلاعات و استفاده از رایانه و پیدایش دنیای مجازی دارای پیامدهای مثبت و منفی فراوانی برای بشر بوده است. از جمله پیامدهای منفی آن، پیدایش جرایم رایانه ای بوده است. در مورد جرایم رایانه ای تعاریف متعددی ذکر شده است برخی از این تعاریف عباتند از:

پلیس جنایی فدرال آلمان در تعریفی از جرایم رایانه ای این چنین اعلام داشته است: «جرم رایانه ای در برگیرنده همه اوضاع و احوال و کیفیاتی است که در آن شکل های پردازش الکترونیک داده‌ها، وسیله ارتکاب و یا هدف یک جرم قرار گرفته است و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است.»[۱۵۸-۱۵۷: ۹] کمیته اروپایی مسایل جنایی در شورای اروپا : در سال ۱۹۸۹ گزارش کاری بیان کرد که در آن یکی از متخصصان چنین تعریفی ارایه کرده است: «هر فعل مثبت غیر قانونی که رایانه، ابزار یا موضوع جرم باشد. یعنی به عبارت دیگر هر جرمی که ابزار یا هدف آن تاثیر گذاری بر عملکرد رایانه باشد.»[همان]

بند اول: شنود غیرمجاز

شنود غیرمجاز همچون دسترسی غیرمجاز ناشی از عدم رضایت دارنده واقعی یا قانونی داده یا محتوای در حال انتقال می باشد. همچنین شرط غیرقانونی بودن نیز به شرط رضایت اضافه می شود. رکن قانونی این جرم ماده ۲ قانون جرایم رایانه (ماده ۷۳۰ ق.م.ا) می باشد. این جرم در واقع همان تعرض به حریم ارتباطات به وسیله شنود سنتی و ضبط مکالمات تلفنی افراد را بیان می کند.

۱.موضوع جرم:موضوع بزه در شنود غیرمجاز، محتواست. برای محتوا ویژگی در حال انتقال پیش بینی شده است یعنی این بزه تنها داده های در حال رفت و آمد را در بر می گیرد و نسبت به داده های 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.

۲.رفتار مرتکب:در این بزه رفتار مرتکب شنود یا همان دریافت محتواست بنابراین میان شنود غیرمجاز و دسترسی غیرمجاز به جهت رفتار تفاوتی وجود ندارد. تفاوت عمده بین این دو بزه در نوع داده ای است که مرتکب آن را دریافت می دارد. به این صورت که در دسترسی، دریافت داده های ذخیره شده و در شنود دریافت محتوای در حال انتقال انجام می گیرد و همچنین دسترسی هم نسبت به داده است و هم سامانه ولی شنود تنها نسبت به داده رخ می دهد. بنابراین رفتار فیزیکی در این جرم فعل شنود کردن می باشد و این جرم با ترک فعل محقق نمی شود.

۳.رکن روانی:رکن روانی بزه شنود غیرمجاز عمد رفتاری یعنی خواست شنود و علم به محتوا و داده های در حال انتقال و غیر مجاز بودن شنود و ویژگی خصوصی بودن انتقال است.

مجازاتمجازات پیش بینی شده برای بزه مزبور در ماده ۲ ق جرایم رایانه ای (م ۷۳۰ ق.م.ا) حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰/۰۰۰/۰۰۰ ریال) تا چهل میلیون (۴۰/۰۰۰/۰۰۰ ریال) یا هر دو مجازات می باشد.

بند دوم: جاسوسی رایانه ای

قانونگذار در قانون جرایم رایانه ای گام های سه گانه ای را برای جرم سیاسی رایانه ای در نظر داشته است: گام اول، دسترسی به سامانه های رایانه ای و مخابراتی که داده های سری در آن ها نگهداری می شود (م ۴ قانون جرایم رایانه ای). گام دوم، دسترسی به داده های سری یا تحصیل یا شنود آن ها (بند الف م ۳ ق جرایم رایانه ای). گام سوم، در دسترس قرار دادن برای کسانی که شایستگی آگاهی از محتوای داده های سری را ندارند (بند ب م ۳ ق جرایم رایانه ای) و یا در دسترس قرار دادن داده های سری یا افشای آن ها به دولت یا نهادهای بیگانه یا عاملان آن ها (بند ج م ۳ ق جرایم رایانه ای).

گام اول یعنی دسترسی به سامانه های در بردارنده داده ها و نیز گام دوم یعنی دسترسی به خود داده های سری در اصل همان بزه دسترسی غیرمجاز هستند که در گام دوم، شنود به دسترسی یا تحصیل نیز افزوده شده است. بنابراین دو بزه دسترسی غیرمجاز و شنود غیرمجاز مبنا و پایه جاسوسی رایانه ای را تشکیل می دهند.

۱. موضوع جرم:موضوع بزه جاسوسی رایانه ای، داده های سری است. طبق تبصره ۱ ماده ۳ ق جرایم رایانه ای، داده های سری داده هایی است که افشای آن¬ها به امنیت کشور یا منافع ملی لطمه می زند.

۲.رفتار مرتکب:در ماده های ۳ و ۴و ۵ قانون جرایم رایانه ای، پدیده جاسوسی رایانه ای مطرح شده است که بر پایه پنج رفتار جداگانه بنا می شود که هر یک بزه جداگانه به شمار می رود.

اول: نقض تدابیر امنیتی سامانه های رایانه ای و مخابراتی در بر دارنده داده های سری (م ۴ ق. جرایم رایانه ای)

دوم: دسترسی به داده های سری یا تحصیل یا شنود آن ها.

سوم: در دسترس قرار دادن داده های سری برای اشخاص فاقد صلاحیت.

چهارم: افشا یا در دسترس قرار دادن داده های سری برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن ها.

پنجم: در دسترس قرار دادن غیر عمدی داده های سری برای اشخاص فاقد صلاحیت.

در واقع می توان گفت جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشاء و انتقال و استفاده از اسرار است، فرد مرتکب جرم با دستیابی و فاش کردن این اسرار، ضررسیاسی، نظامی، مالی، تجاری می کند. این جرم امنیت ملی را با مخاطره مواجه می کند.

۳. رکن روانی:رفتارهای جاسوسی رایانه ای باید با عمد انجام گیرد مگر آن چه که در ماده ۵ ق. جرایم رایانه ای آماده است یعنی موجب دسترسی شدن که به طور غیر عمد و از روی بی احتیاطی، بی مبالاتی و یا عدم رعایت تدابیر امنیتی رخ می دهد.همچنین مرتکب باید آگاه به

سری بودن داده ها باشد و نیز در بندهای «ب» و «ج» ماده ۳ ق جرایم رایانه ای، مرتکب باید آگاه به غیر صالح بودن فرد یا عامل بیگانه بودن شخص نیز باشد. در نقض تدابیر سامانه ای موضوع ماده ۴ ق جرایم رایانه ای نیز باید مرتکب آگاه به این مسأله باشد که سامانه موردنظر، سامانه ای است که داده های سری در آن نگهداری می شوند. در صورت نا آگاهی بزه دسترسی غیر مجاز موضوع ماده ۱ ق جرایم رایانه ای شکل گرفته است.در انجام رفتارهای جاسوسی نیازی به قصد خاص نیست مگر در نقض تدابیر امنیتی سامانه های رایانه ای یا مخابراتی موضوع ماده ۴ قانون جرایم رایانه ای که مرتکب باید قصد دسترسی به داده های سری موضوع ماده ۳ ق جرایم رایانه ای را داشته باشد.بر اساس مواد ۳ و ۴ و ۵ قانون جرایم رایانه ای مجازات جاسوسی رایانه ای به قرار ذیل می باشد:

ماده (۳) هر کس به طور غیرمجاز نسبت به داده ای سری در حال انتقال یا ذخیره شده در سیستم های رایانه ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود، به مجازات های مقرر محکوم خواهد شد:

الف) دسترسی به داده ای مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست تا شصت میلیون ریال یا هر دو مجازات.

ب) در دسترس قرار دادن داده ای مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

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

تبصره ۱ـ داده ای سری داده ای است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره ۲ـ آیین نامه نحوه تعیین و تشخیص داده ای سری و نحوه طبقه بندی و حفاظت آن ها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت دولت خواهد رسید.

ماده (۴) هرکس به قصد دسترسی به داده ای سری موضوع ماده (۳) این قانون، تدابیر امنیتی سیستم های رایانه ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۵) چنانچه مأموران دولتی که مسؤول حفظ داده ای سری مقرر در ماده (۳) این قانون یا سیستم های مربوط هستند و به آن ها آموزش لازم داده شده است یا داده ها یا سیستم های مذکور در اختیار آن ها قرار گرفته است بر اثر بی احتیاطی، بی مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده ها، حامل های داده یا سیستم های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

ب- جرایم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی

بستر انجام بزه جعل رایانه ای، فضای سایبر است و فضای سایبر فضایی غیر مادی و نا ملموس است که توسط رایانه ها و شبکه های رایانه ای به وجود آمده است و دنیایی مجازی را در کنار دنیای واقعی ما به وجود آورده است. در واقع فضای سایبر همان فضای مجازی بیکرانی است که از طریق اتصال شبکه های رایانه ای به هم به وجود آمده است.

به لحاظ فنی « شبکه رایانه ای در پایه ای ترین سطح خود شامل دو کامپیوتر می باشد که به وسیله کابل به یکدیگر متصل شده اند به گونه ای که بتوانند از داده ها به طور مشترک استفاده نمایند.» [۱۶: ۱۷] این ارتباط در حال حاضر از طریق کابل مسی است، البته ارتباط رایانه ها با یکدیگر ممکن است از طریق کابل خطوط تلفن نباشد و از طریق؛ «فیبر نوری، مایکروویو، اشعه مادون قرمز و ماهواره های ارتباطی نیز می توان برای ارتباط استفاده کرد.» [۱۴: ۴]بنابراین همه رفتارهای پیش بینی شده در این ماده باید از رهگذر کنش های رایانه ای و در بستر رایانه و مخابرات انجام شود.بنابراین اگر کسی داده رایانه ای را چاپ کند یا از روی صفحه نمایشگر رایانه عکس بگیرد و سپس بر روی کاغذ چاپ شده، تغییراتی را ایجاد کند، جعل رایانه ای محقق نیست و ممکن است با وجود تمام شرایط جعل سنتی باشد. همچنین انجام رفتارهای

موضوع جعل رایانه ای، باید به صورت غیر مجاز باشد یعنی یا اجازه نداشته و یا برخلاف قانون و قرارداد بوده است.

۱. موضوع جرم:موضوع جعل رایانه ای، داده و یا حامل داده و یا جای انباشت داده می باشد مانند علامت، کارت حافظه و تراشه.داده های موضوع جعل رایانه ای باید قابلیت استناد داشته باشند و به همین دلیل است که دیگری نیازی به ایراد ضرر برای تحقق این جرم نیست و اگر زیانی حاصل شود می تواند باعث افزایش کیفر شود.

۲.رفتار مرتکب:در بند الف ماده ۶ ق جرایم رایانه ای دو بخش جداگانه در انجام رفتار جعل رایانه ای پیش بینی شده است : اول، تغییر یا ایجاد داده های قابل استناد که در واقع تغییر باید در داده های قابل استناد انجام شود و ایجاد نیز باید پدید آوردن داده ای باشد که توانایی استناد پذیری داشته باشد. دوم، ایجاد یا وارد کردن متقلبانه داده به آن ها بند ب ماده ۶ ق جرایم رایانه ای، تغییر داده ها یا علایم موجود در کارت های حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها با ایجاد یا وارد کردن متقلبانه داده ها یا علایم به آنها را به عنوان رفتار مجرمانه برای جرم جعل رایانه ای مطرح می کند.البته به نظر می رسد که رفتارهای مندرج در بند ب تفاوتی با بند الف ندارد و نیازی به آوردن بند ب نبود. لیکن برای بند ب، قانونگذار شرط استناد پذیری را بیان نکرده است .بنابراین واردکردن، تغییر، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور و اهداف سیاسی و اقتصادی صورت می گرد جعل رایانه ای جعل داده هاست. در جعل رایانه ای عمل ارتکابی برداده‌ها اثر می گذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.

۳. رکن روانی:عمد مرتکب در پدید آوردن دگرگونی در داده های قابل استناد و سایر رفتارهای مندرج در ماده، رکن روانی این بزه را تشکیل می دهد.

۴. مجازات:کسی که مرتکب جرم جعل رایانه ای می شود بنا به تصریح ماده ۶ ق جرایم رایانه ای به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا یکصد میلیون (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم می شود.

بند سوم : استفاده از داده مجعول

ماده ۷ ق جرایم رایانه ای (ماده ۷۳۵ ق.م.ا) ، رکن قانونی بزه استفاده از داده مجعول به شمار می رود.

۱.رکن مادی: داده، کارت های الکترونیکی و تراشه ها موضوع رفتار مجرمانه در این جرم می باشند.

۲. رفتار مرتکب:استفاده کردن از داده مجعول که باید در فضای سایبر و سامانه های رایانه ای و مخابراتی یا داده برها و کارت های حافظه انجام شود، رفتار مرتکب در بزه استفاده از داده مجعول را تشکیل می دهد.بنابراین اگرکسی در فضای بیرونی و فیزیکی از داده مجعول استفاده کند، این بزه رخ نمی دهد.به عنوان مثال اگر فردی جعل رایانه ای کند ومتن یک قراردادالکترونیکی راتغییر دهد ویا اینکه چنین قرارداد مجعولی را بیابد یا دریافت دارد و سپس آن را چاپ کرده و به نهاد یا کسی ارایه دهد مرتکب جرم استفاده از سند مجعول شده است نه جرم استفاده از داده مجعول، چرا که استفاده کردن در فضای بیرونی انجام شده است.

۳.رکن روانی:آگاهی مرتکب به جعلی بودن ، برجسته ترین عنصر رکن روانی است. همچنین لازم است که مرتکب عمد در استفاده کردن از داده مجعول را نیز داشته باشد.

۴. مجازات:بر ساس ماده ۷ ق جرایم رایانه ای هرکس با علم به مجعول بودن داده ها یا کارت ها یا تراشه ها از آن ها استفاده کند، بنا به تصریح ماده ۶ ق جرایم رایانه ای به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال تا یکصد میلیون (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم می شود.

بند چهارم: خرابکاری رایانه ای

خرابکاری رایانه ای در بردارنده هر رفتاری است که داده را بطور کلی یا جزیی از میان ببرد یا کارکرد داده یا سامانه را به هر نحو بر هم بزند. [۲۱۶: ۱۳] استفاده از عنوان تخریب واخلال درداده ها یاسامانه های رایانه ای ومخابراتی برای مبحث دوم از فصل یکم در بخش نخست قانون جرایم رایانه ای برای این است که چهار عنوان مجرمانه تخریب، اخلال، ممانعت از

دستیابی و تروریسم سایبری را در برگیرد. از آنجایی که ویژگی های تخریبواخلال نزدیک به هم هستند انها را دریک بند بررسی می کنیم.

بخش دوم : تخریب یا اخلال داده

تخریب به معنای از بین بردن تمام یا قسمتی از یک چیز واخلال در معنای ایجاد آشفتگی وناتوانی در کارکرد چیزی است. م ۸ ق جرایم رایانه ای(م ۷۳۶ ق م ا) این جرم راپیش بینی کرده است.

۱.موضوع جرم:موضوع بزه تخریب یا اخلال، «داده» می باشد. این داده باید از آنِ دیگری باشد.خواه مالیت داشته باشد، خواه نداشته باشد و خواه استاندارد پذیر نباشد، خواه شخصی باشد خواه دولتی. اما اگر موضوع بزه، داده های دولتی باشد مطابق بند ج ماده ۲۶ ق جرایم رایانه ای مرتکب با افزایش مجازات مواجه خواهد بود.

۲. رفتار مرتکب:چهار رفتار حذف، تخریب، مختل و غیر قابل پردازش کردن در ماده ۸ ق جرایم رایانه ای پیش بینی شده است که زیر دو رفتار تخریب و اخلال قرار می گیرند. دو رفتار حذف وتخریب نسبت به خود داده و دو رفتار مختل کردن و غیر قابل پردازش نمودن نسبت به کارکرد و توانایی داده رخ می دهد.هر چهار رفتار باید در فضای سایبر رخ دهد این مسأله با به کار بردن عبارت «سامانه های رایانه ای یا مخابراتی یا حامل های داده» در متن ماده روشن می شود ورفتارهای بزهکارانه باید رایانه ای و سایبری باشد. به عنوان مثال اگر کسی به قصد از بین بردن داده دیگری، رایانه اش را از بلندی پرت کند یا آن را بسوزاند یا لوح فشرده را بشکند یا آن را بخراشد یا سنگ، بر روی حامل داده بزند، هیچ یک تخریب یا اخلال رایانه ای نیست بلکه حسب مورد تخریب یا اخلال سنتی است.

۳. رکن روانی:علم و عمد در انجام رفتارهای مرتکب که در قسمت قبل عنوان شد، رکن روانی بزه راتشکیل می دهد همچنین بزه تخریب واخلال داده رایانه ای باید به طور غیرمجاز انجام گیرند و مرتکب آگاه به غیر مجاز بودن باشد بدیهی است که اگر رفتار های موضوع ماده ۸ ق جرایم رایانه ای با اجازه دارنده آن باشد، بزهی در کار نخواهد بود و میان شخص حقوقی و حقیقی و فرد و دولت تفاوتی نمی باشد.بر ساس ماده ۸ ق جرایم رایانه ای برای

مرتکب بزه مزبور حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات در نظر گرفته شده است.

بند اول: اخلال سامانه های رایانه ای یامخابراتی

ماده ۹ قانون جرایم رایانه ای (م ۷۳۷ ق م ا) این بزه رابیان نموده است.

۱- رکن مادی

۱-۱) موضوع جرم

موضوع بزه اخلال در ماده ۹ ق جرایم رایانه ای، سامانه های رایانه ای و مخابراتی است. سامانه ممکن است ازآن شخص حقیقی یا حقوقی خصوصی باشد یا این¬که ممکن است از آن نهادها و سازمان های دولتی باشد. اخلال سامانه دولتی سبب افزایش کیفر می گردد.در ماده ۹ قانون جرایم رایانه ای دو نوع رفتار پیش بینی شده است: اول، رفتارهای احصایی که شامل از کار انداختن و مختل کردن می شود و دوم رفتارهای تمثیلی که در صدر ماده آمده و عبارتند از وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب و مانند آن ها.رفتارهای تمثیلی بر روی سامانه رخ نمی دهند بلکه بر روی داده یاموج انجام می شوند و سپس به اخلال می انجامند. از کار انداختن و مختل کردن بر روی سامانه رایانه ای و مخابراتی انجام می شوند.در اخلال سامانه، مرتکب باید عمد در انجام رفتار را داشته باشد.همچنین او باید به موضوع بزه آگاهی داشته باشد. یعنی هم نسبت به اینکه سامانه از آنِ دیگری است و یا این که از آنِ دولت است و هم نسبت به غیرمجاز بودن آن آگاه باشد.برپایه ماده ۹ ق جرایم رایانه ای(م ۷۳۷ ق م ا) برای بزه مزبور حبس از شش ماه تا دو سال یاجزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات، مقرر گردیده است.

بند دوم: تروریسم سایبری

همان طور که از این عنوان پیداست، مجموعه ای از اقدامات را شامل می شود که افراد خاصی با نیات خاص مرتکب می شوند و به لحاظ خسارات مادی و لطمات جانی که به بار می آورند، از سوی همه کشورها در زمره شدیدترین جرایم قرار گرفته اند. [۱۷۶: ۷] در ایران ماده

۱۱ ق جرایم رایانه ای، بدون نام بردن از اقدام تروریستی یاتروریسم، بزهی راپیش بینی می کند که بسیار نزدیک به تروریسم سایبری است و آن اخلال رایانه ای همراه باقصد است.

۱. موضوع جرم: موضوع تروریسم سایبری، سامانه های رایانه ای و مخابراتی که برای ارایه خدمات ضروری عمومی به کار می روند، می باشند. مواردی که در ماده ۱۱ ق جرایم رایانه ای ذکرشده تمثیلی اند. مواردی مانند خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری که نشان دهنده آن است که خدمات ضروری عمومی به خدماتی گفته می شود که برای رفع نیازهای حیاتی و ضروری شهروندان به کارمی آید.

۲. رفتارمرتکب: رفتارهای موضوع ماده ۱۱ ق جرایم رایانه ای همان رفتارهای پیش بینی شده در ماده های ۸ (حذف یا تخریب یا مختل یا غیر قابل پردازش کردن)، ۹ (از کار انداختن ومختل کردن کارکرد) و ۱۰ (مانع شدن اردسترسی) قانون جرایم رایانه ای است.

۳. رکن روانی:مرتکب باید انجام رفتارهای پیش بینی شده در موارد ۸ و ۹و۱۰ ق جرایم رایانه ای را از روی عمد انجام دهد.همچنین قصد غایی او، به خطر انداختن امنیت ، آسایش وامنیت عمومی باشد و از طرف دیگر باید آگاه باشد که رفتار خود را بر روی سامانه هایی که خدمات ضروری ارایه می دهند، انجام می دهد.بر اساس ماده ۱۱ ق جرایم رایانه ای مرتک این بزه به حبس از سه تا ده سال محکوم خواهد شد.گاه جرایم رایانه ای، رفتارهایی را در بر می گیرد که رایانه در رخ دادن آن ها موضوع بزه است که در دو دسته قبلی یعنی جرایم بر ضد محرمانگی و جرایم بر ضد صحت و تمامیت آن ها را بررسی کردیم. اما گاهی رفتارهایی وجود دارد که رایانه در آن ها وسیله انجام جرم است. در قانون جرایم رایانه ای و در فصل سوم آن دو عنوان سرقت و کلاهبرداری بیان شده و فصل چهارم جرایم علیه عفت و اخلاق عمومی و فصل پنجم با عنوان هتک حیثیت و نشر اکاذیب رفتارهایی را مطرح می کند که در انجام آن ها رایانه، وسیله ارتکاب جرم است.

بند سوم: جرایم مالی رایانه ای

جرایم مالی ناظر به جرایمی است که مرتبط با اموال هستند اعم از این که مال موضوع جرم باشد یا وسیله آن.سرقت رایانه ای درم ۱۲ ق جرایم رایانه ای پیش بینی نشده است. این بزه،

یک بزه رایانه ای محض است چرا که ربودن داده در جایی که عین داده در جای خود باقی است ، مانند جاسوسی و شنود غیر مجاز است که بر ضد محرمانگی داده رخ می دهد ودر جایی که به وسیله برش ، عین داده از سامانه برداشته می شود، همانند تخریب داده است. بنابراین در دسته جرایمی قراردارد که رایانه، هدف یا موضوع بزه است و نباید در کنار کلاهبرداری که درآن رایانه نقش ابزار انجام بزه را دارد آورده شود.

۱. موضوع جرم: موضوع بزه سرقت رایانه ای، داده است. این داده به تعبیر ماده ۱۲ ق جرایم رایانه ای باید متعلق به دیگری باشد.خواه داده های دارای ارزش مالی باشند مثل یک فرمول و خواه نباشند مانند یک مقاله پذیرفته شده و خواه دارنده داده خودش آنها راپدید آورده باشد مانند متن یک کتاب و یا این که آن داده را از دیگری خریداری نموده و یا از طریق قانونی بدست آورده باشد. داده ای که متعلق به دیگری است باید در رایانه او یا جایی که به طور قانونی مکان قرار گرفتن داده¬های آن فرد است، باشد بنابراین اگرکسی نوشته دیگری را که بطور آزاد در اینترنت هست، بارگذاری کند ودریافت دارد، سارق نیست ولی اگرکسی مقاله دیگری را از رایانه وی برباید، حتی اگر متن آن مقاله در اینترنت و به طور آزاد، دسترس پذیر باشد، عمل وی قابل مجازات است.

۲. رفتارمرتکب:رفتارسرقت رایانه ای، همچون سرقت سنتی، ربودن است. آن چه مفهوم ربایش را می سازد، دست اندازی به مال دیگری یا از آن خود کردن بدون خشنودی دارنده آن است. یعنی همین که کسی مال دیگری را بدون رضایت وی بدست آورد رفتارش، ربایش است.ربودن داده هم به معنای دست اندازی به داده دیگری است که یا با رو گرفتن (کپی) است یا با برش (کات). رو گرفت یا کپی باید در فضای سایبر انجام گیرد. اگر کسی به سامانه دیگری که با تدابیر امنیتی محافظت شده، نفوذ کرده و داده یا اطلاعات را یافته و آن ها ر ابر روی کاغذ بنویسد مرتکب بزه دسترسی غیر مجاز شده است نه بزه سرقت رایانه ای. برش داده باید به نحوی صورت گیرد که فرد مرتکب داده را از جایگاه خود برداشته و به جای دیگری چه رایانه و یا وسایل حامل داده بفرستد. اگر مرتکب، داده دیگری را حذف کرده بدون آن که خودش از آن بهره ای ببرد رفتارش مصداق تخریب است. اما اگر در برش، مرتکب مکان

داده را جابجا کند به طوری که عین داده در اختیار دارنده آن نباشد مرتکب سرقت رایانه ای شده است. ربایش رایانه ای که در قانون جرایم رایانه ای مطرح شده است، نسبت به ربایش در فضای بیرونی نگاهی ندارد به عنوان مثال اگر کسی به قصد ربودن اطلاعات دیگری در خیابان، لپ تاپ دیگری را برباید یا به کنار میز رایانه اش رفته و چندین لوح فشرده را بردارد و از آن خود کند، ربایش سایبری انجام نشده است، هرچند که موضوع بزه، داده است این سرقت، از نوع سرقت سنتی می باشد.

۳.رکن روانی:مرتکب باید آگاه باشد که داده از آن دیگری است.مرتکب ربایش رایانه ای باید عمد در رفتار داشته باشد که این عمد خود می تواند به صورت عمد در روگرفت برداری باشد یا عمد در برش داده.مجازات تعیین شده برای بزه سرقت رایانه ای بر پایه ماده ۱۲ ق جرایم رایانه ای، برای روگرفتن یاکپی از داده ها جزای نقدی از یک میلیون(۱/۰۰۰/۰۰۰) ریال تا بیست(۲۰/۰۰۰/۰۰۰) ریال ودر حالت برش داده ها حبس از نود ویک روز تا یک سال یا جزای نقدی از پنج میلیون(۵/۰۰۰/۰۰۰) ریال تابیست میلیون(۲۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات خواهد بود.

بند چهارم: کلاهبرداری رایانه ای

کلاهبرداری یکی از مهم ترین جرایم علیه اموال و مالکیت می باشد که برخی از آن به عنوان بحران قرن بیستم نام برده اند.[۲۸: ۱۸] در حقوق رم جرایم سرقت، خیانت در امانت و کلاهبرداری از یکدیگر تفکیک نشده و «Furtum» شامل هر سه جرم می گردیده است. [۷: ۲] اما با پیشرفت علم و تکنولوژی کلاهبرداران هم برای رسیدن به اهداف خود از این پیشرفت ها استفاده نموده اند و با استفاده از رایانه و فضای سایبر اقدام به کلاهبرداری های رایانه ای نموده اند.

کلاهبرداری رایانه ای همانند کلاهبرداری سنتی جرمی مقید به حصول نتیجه مجرمانه است و باید به واسطه سوء استفاده از رایانه از طریق افعالی نظیر ایجاد، محو، توقف داده و یا اختلال در سیستم رایانه ای، مال یامنفعت یا مزایای مالی عاید مرتکب شود. در حقوق کیفری رایانه ای همانند حقوق کیفری سنتی، سوء استفاده از نرم افزارهای رایانه ای برای تحصیل مال

یامنفعت یا مزایای مالی وجه تمایز بین کلاهبرداری رایانه ای از سایر جرایم مشابه است.ماده ۱۳ قانون جرایم رایانه ای (م ۷۴۱ ق م ا) رکن قانونی این جرم محسوب می شود.

۱. موضوع جرم:موضوع کلاهبرداری رایانه ای وجه یا مال یا منفعت یا خدمات یا امتیازات مالی است. کلاهبرداری رایانه ای به لحاظ موضوع از کلاهبرداری سنتی عام تر است و علاوه بر وجه و مال، منفعت و خدمات و امتیازات مالی را نیز در بر می گیرد.

۲.رفتارمرتکب: با توجه به قید واژه هرکس، مرتکب این بزه همانند کلاهبرداری سنتی هر شخصی می تواند باشد، البته به جز اشخاص حقوقی که بدون تصریح خاص قانونگذار فعلاً در حقوق ایران فاقد مسوولیت کیفری می باشند.[۲۷۷: ۵] کلاهبرداری رایانه ای بزهی مرکب و دو رفتاری است. رفتار اول در ان که به طور تمثیلی در۱۳ ق جرایم رایانه ای به آن اشاره شده است اعمالی چون وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده ها یامختل کردن سامانه می باشند. این رفتارها باید به طور غیر مجاز صورت گیرند و اگر با اجازه انجام شوند، کلاهبرداری رایانه ای رخ نداده، هرچند که به تحصیل مال به طور غیر قانونی بینجامد.رفتاردوم، تحصیل اعم از دریافت واقعی یا مجازی یا منظور کردن اعتبار مالی برای خود می باشد. بستر انجام این بزه، فضای سایبر است. بنابراین رفتارهای فیزیکی و تحصیل باید در فضای سایبر انجام گیرد. اگر فرد از رایانه و فضای سایبر تنها به عنوان وسیله ارتکاب جرم کلاهبرداری استفاده کند مثل این که از طریق تبلیغ ناروا در وبلاگ خود، دیگری را فریفته و خود را دارنده مؤسسه اعزام دانشجو به خارج بشناساند و با دادن شماره حسابی، کاربر یا کاربرانی را بفریبد تا پولی به حسابش بریزد یا در محیط بیرون پول یا مال را دریافت دارد، کلاهبرداری سنتی انجام داده است نه رایانه ای.

۳. نتیجه حاصله:کلاهبرداری رایانه ای باید به تحصیل مال یا منفعت یا خدمات مالی یا امتیازات مالی بینجامد. این تحصیل می تواند برای خود مرتکب یا دیگری باشد. دیگری، کسی است که مرتکب تحصیل را برای وی خواسته باشد.

رکن روانی کلاهبرداری شامل عمد رفتاری یعنی عمد در رفتارهای رایانه ای تمثیلی و عمد در تحصیل مال یا منفعت و آگاهی مرتکب نسبت به تعلق مال یا منفعت یا خدمات مالی یا

امتیازات مالی به دیگری است همچنین مرتکب باید بداند که انجام رفتارهای رایانه ای تمثیلی، بدون مجوز بوده است.کیفر تعیین شده برای بزه کلاهبرداری رایانه ای علاوه بر رد مال به صاحب آن، حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون(۲۰/۰۰۰/۰۰۰) ریال تا یکصد میلیون (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات می باشد.

بخش سوم: جرایم علیه عفت و اخلاق عمومی

بند اول : هرزه نگاری

هرزه نگاری به مجموعه ای از رفتارهای مجرمانه گفته می شود که شامل تولید، طراحی ، ارایه، انتشار ومورد معامله قراردادن محتویات شنیداری و دیداری اعم از تصویر، نوشته، صوت می شود که عفت عمومی را جریحه دار می سازد.[۲۹۴: ۱۳] ماده ۱۴ قانون جرایم رایانه ای(م ۷۴۲ ق م ا) رکن قانونی بزه مزبور، به شمارمی رود.

۱.موضوع جرم:موضوع بزه هرزه نگاری، محتوایی است که به صورت غیر اخلاقی درآمده است. محتویات هرزه دو دسته اند: محتویات مستهجن و محتویات مبتذل. مطابق با تبصره ۱ م ۱۴ ق جرایم رایانه ای آثار مبتذل به آثاری اطلاق می شود که دارای صحنه ها و صور قبیحه باشد. همچنین بر پایه تبصره ۴ م ۱۴ ق جرایم رایانه ای محتویات مستهجن به تصویر، صوت یامتن واقعی یا غیر واقعی یا متنی اطلاق می شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

۲.رفتارمرتکب:رفتارهای پیش بینی شده در م۱۴ ق جرایم رایانه ای دو گروهند: نخست رفتارهایی که بدون نیاز به قصد خاص و در هر دو حالت مستحق کیفر هستند این رفتارها عبارتند از انتشار، توزیع یا معامله ودوم رفتارهایی که بصورت مشروط قابل سرزنش و مجازاتند که شامل تولید، ذخیره و نگهداری می باشند. این سه رفتار به خودی خود قابل مجازات نیستند مگر اینکه همراه با قصد تجارت یا افساد، انجام شوند. در واقع انتشار، توزیع و معامله محتوای خلاف عفت عمومی یعنی مبتذل و مستهجن مشمول این قانون می شود.همه رفتارهای شش گانه باید در محیط سایبر رخ دهند وگرنه اگر هریک از این رفتارها در فضای فیزیکی رخ دهند، باید طبق مقررات کیفری دیگری با آنها برخورد نمود.

۳. رکن روانی:برای تحقق بزه مذکور درماده ۱۴ ق جرایم رایانه¬ای لازم است که مرتکب در انجام شش رفتار گفته شده عمد داشته و همچنین برای سه رفتار تولید، ذخیره و نگهداری به عمد غایی که در واقع قصد تجارت یا افساد می باشد، نیز نیاز است. همچنین لازم است که مرتکب به اینکه رفتار مجرمانه را نسبت به محتویات (مستهجن یا مبتذل) انجام می دهد آگاهی داشته باشد.بر اساس ماده ۱۴ ق جرایم رایانه ای مرتکب این بزه به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

بند دوم : معاونت در دسترسی به محتویات هرزه

بند الف م۱۵ ق جرایم رایانه ای در راستای حمایت از بزه دیدگان معاونت در دسترسی به محتویات هرزه را به عنوان جرم مستقلی، پیش بینی کرده است.

۱. رفتارمرتکب:بیشتر رفتارهای پیش بینی شده در ماده ۱۵ ق جرایم رایانه ای همان رفتارهایی اند که در م ۴۳ ق ما در قالب معاونت جرم پیش بینی شده اند.این رفتارها عبارتند از: تحریک، ترغیب، تهدید، تطمیع، فریب دادن، تسهیل شیوه دستیابی و آموزش دادن.تمامی این رفتارها باید از طریق سامانه های رایانه ای یامخابراتی یا حامل های داده یعنی در واقع در فضای سایبر، صورت بگیرند. این رفتارها مطلق بوده ونیازی نیست که افرادی راکه فرد مرتکب تحریک، ترغیب و... نموده است به محتویات مستهجن یا مبتذل دست یابند.

۲. رکن روانی:فرد مرتکب باید در انجام رفتارهای مذکور در قسمت پیش را داشته باشد و همچنین باید در انجام این رفتارهاعمد غایی یا قصد خاص دستیابی افراد به محتویات مستهجن یا مبتذل را نیز داشته باشد از طرف دیگر باید مرتکب هم نسبت به محتوای هرزه و هم نسبت به کسی که دستیابی محتوای هرزه را آموزش می دهد یا رفتارهای دیگر را انجام می دهد، آگاه باشد.بر پایه صدر ماده ۱۵ ق جرایم رایانه ای، کیفر بزه های پیش بینی شده در آن، حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵/۰۰۰/۰۰۰) ریال تا بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات است. اگر این اعمال را در خصوص محتویات مبتذل مرتکب شود، موجب جزای نقدی از دو میلیون (۲/۰۰۰/۰۰۰) ریال تا پنج میلیون (۵/۰۰۰/۰۰۰) ریال است.

بند سوم : دستیابی در انجام یا آموزش بزه

بند ب ماده ۱۵ ق جرایم رایانه ای نیز در واقع معاونت در انجام یا آموزش بزه را به عنوان جرم مستقلی، بزه انگاری نموده است.

۱. رفتار مرتکب:رفتارهایی که دربند ب ماده ۱۵ ق جرایم رایانه ای بازداشته شده اند درواقع در گروه رفتارهایی قرار دارند که معاونت نامیده می شوند این رفتارها عبارتند از: تحریک، ترغیب، تهدید، فریب دادن، تسهیل شیوه ارتکاب یا استعمال یا آموزش دادن.

۲.رکن روانی:عمد رفتاری یعنی اراده آزاد در انجام رفتار یکی از ارکان روانی است. علاوه بر این لازم است که مرتکب برای ارتکاب جرایم منافی عفت یا استعمال مواد مخدر یا روان گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز، رفتارهای مذکور را نسبت افراد مد نظر خود انجام دهد. برای بزه مزبور قانونگذار مجازاتی به صورت حبس از نود و یک روز تا یکسال یا جزای نقدی از پنج میلیون (۵/۰۰۰/۰۰۰) ریال تا بیست میلیون(۲۰/۰۰۰/۰۰۰) ریال یا هردو مجازات ، مقرر نموده است.

بخش چهارم: جرایم علیه شخصیت معنوی

بزه های ضد شخصیت معنوی، به رفتارهایی گفته می¬شود که روان آدمی را هدف می گیرند. بزه های ضد اشخاص در فضای سایبر منصرف از بزه های ضد تمامیت جسم و جان شخص است. در فضای سایبر که محل حضور ذهن فرد است، جرایم علیه اشخاص با روان و شخصیت معنوی آنان ارتباط می یابد.

بند اول : تغییر یا تحریف محتوای دیگری

ماده ۱۶ ق جرایم رایانه ای (م ۷۴۴ ق م ا) رکن قانونی بزه تغییر یا تحریف محتوای دیگری است.

۱.موضوع جرم:موضوع بزه تغییر یا تحریف محتوای دیگری، فیلم یا صوت یا تصویر دیگری است.

۲. رفتار مرتکب:م ۱۶ ق جرایم رایانه ای برای رفتار مرتکب دوحالت را مطرح نموده است. اول؛ حالتی است که فرد تغییر یا تحریف محتوا را انجام داده و آن محتوای تغییر یا تحریف یافته را منتشر می کند. یعنی بزهی مرکب را انجام داده است. بنابراین صرف تغییر یا تحریف

محتوا تا زمانی که آن¬ها را انتشار نداده است، برای تحقق بزه کافی نیست. دوم؛ حالتی است که فرد محتوای تغییر یا تحریف یافته را با علم به تغییر یاتحریف منتشر می¬کند. یعنی بزه ساده رخ داده است.اگر تغییر یا تحریف به صورت مستهجن باشد، بر پایه تبصره م ۱۶ مرتکب به حداکثر هر دو مجازات مقرر در ماده محکوم می شود.بزه موضوع م ۱۶ ، مقید به نتیجه است. هر دو حالت رفتاری یعنی تغییر و تحریف و انتشار و نیز انتشار با علم به تغییر وتحریف، باید عرفاً موجب هتک حیثیت گردد. یعنی هتک حیثیت، نتیجه بزه است. ملاک تشخیص هتک حیثیت عرفِ وابسته به شرایط زمان و مکان می باشد.

۳. رکن روانی:در حالت اول که فرد محتویات مربوط به دیگری را تغییر یا تحریف داده و بعد آنها را منتشر نموده است، مرتکب باید عمد در تغییر و تحریف و همچنین عمد در انتشار داشته باشد. اضافه بر این مرتکب باید آگاهی داشته باشد که فیلم یا صوت یا تصویر، متعلق به دیگری است. در حالت دوم فرد باید عمد در انتشار محتوای تغییر یافته داشته و همچنین بداند که فیلم یا صوت یا تصویر به دیگری تعلق دارد و آگاه به تغییر یا تحریف محتوا باشد.

کیفر پیش بینی شده در م ۱۶ ق جرایم رایانه ای به صورت حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات است و مطابق تبصره ماده اگر تغییر یا تحریف به صورت مستهجن باشد حداکثر هر دو مجازات، کیفری مرتکب خواهد بود.

بند دوم: انتشار اسرار خصوصی و محتویات خانوادگی

م۱۷ ق جرایم رایانه ای (م ۷۴۵ ق م ا) به موضوع انتشار اسرار خصوصی و محتویات خانوادگی که بزهی ضد حریم خصوصی است پرداخته است.این ماده برای حمایت از حریم خصوصی افراد می باشد. بند الف ماده ۲ دستورالعمل های اروپایی حمایت از داده های شخصی مصوب ۱۹۹۲ در تعریف داده شخصی اعلام می کند: «داده شخصی یعنی هرگونه اطلاعات مربوط به یک شخص با هویت مشخص یا قابل شناسایی، شخص قابل شناسایی 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 است.»

بند سوم: فروش یاپخش یا در دسترس گذاری داده های رخنه گر

رکن قانونی این جرم بند ب م ۲۵ ق جرایم رایانه ای است.این بند بر خلاف بند الف، به بد افزارها توجهی نداشته، بلکه مدنظر قانون گذار داده هایی است که دارای ارزش و کارکرد مثبت بوده لیکن مرتکب از آنها برای دسترسی غیرمجاز بهره می گیرد.

۱.موضوع بزه:رفتارهایی که در بند ب آمده اند، موضوع مستقیم ندارند. بلکه موضوع آنها باواسطه است. به عبارت دیگر از آنجایی که این رفتارها به جهت بازدارندگی، بزه دانسته شده اند و راهی برای انجام بزه دسترسی غیر مجاز هستند، داده ها یا سامانه های رایانه ای یامخابراتی متعلق به دیگری موضوع با واسطه آنها به حساب می آیند. در واقع این موضوعات، موضوع بزه دسترسی غیر مجازند.

۲.رفتارمرتکب:رفتارهای موضوع بند ب، سر رفتار فروش، انتشار و در دسترس قرار دادن است و نیازی نیست که این سه رفتار در فضای سایبر انجام گیرد. همین که کسی گذر واژه ای را بر روی کاغذی بنویسد و به دیگری بدهد تا از طریق آن، امکان دسترسی غیر مجاز به داده ها یاسامانه های رایانه ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم کند، بزه موضوع بند ب تحقق یافته است.

۳. رکن روانی:عمد رفتاری یعنی عمد در ارتکاب سه رفتار فروش، انتشار و در دسترس قرار دادن و علم به این که گذر واژه یا داده راجهت دسترسی غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی متعلق به دیگری را بدون رضایت او دراختیار دیگزان قرار دادهویا فروخته ویا منتشر کرده، از اجزاء روانی به شمار می آیند.مجازات تعیین شده برای بزه موضوع بند ب م۲۵ ق جرایم رایانه ای، همانند مجازات مقرر برای بزه موضوع بند الف م۲۵ ق جرایم رایانه ای است.

بخش پنجم: پخش یا در دسترس گذاری محتویات آموزنده بزه های ناب رایانه ای

بزه های ناب یا محض رایانه ای، به رفتارهایی گفته می شود که بر ضد رایانه ارتکاب یافته و چون رایانه هدف رفتار بزهکارانه است، همانندی در فضای بیرونی نداشته و پیرو شکل¬گیری رایانه و فضای سایبر بنیاد گرفته اند.دسترسی غیرمجاز، جاسوسی رایانه ای، تخریب واخلال در

داده ها یا سیستم های رایانه ای و مخابراتی، بزه هایی هستند که بند ج م ۲۵ جرایم رایانه ای پخش یا در دسترس گذاری محتویات آموزنده این بزه ها را، جرم انگاری نموده است.

۱. موضوع بزه:در بند ج م ۲۵ ق جرایم رایانه ای نیز ، از جمله موضوعات باواسطه اند.چراکه بزه پخش یا در دسترس قرار دادن محتویات، جنبه بازدارندگی نسبت به بزه های دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه ای و تخریب و اخلال در داده ها یا سیستم های رایانه ای ومخابراتی دارد. بنابراین موضوعات جرایم ذکر شده، به صورت باواسطه موضوع بزه پخش یا در دسترس قرار دادن محتویات آموزنده، به شمار می آیند.

۲.رفتار مرتکب:رفتارهای پیش بینی شده در بند ج، انتشار یا در دسترس قرار دادن است که هریک به طور جداگانه جرم محسوب می شوند.عمد درارتکاب دو رفتار انتشار یا در دسترس قراردادن محتویات آموزنده و علم و آگاهی به این که محتویات منتشر شده یا در دسترس قرار گرفته، جهت آموزش بزه های دسترسی غیر مجاز، شنود غیرمجاز، جاسوسی رایانه ای وتخریب واخلال در داده ها یا سیستم های رایانه ای و مخابراتی، می باشند برای تحقق بزه موضوع بند ج م ۲۵ ق جرایم رایانه ای ضروری است.

نتیجه گیری

با پیشرفت تکنولوژی و استفاده از رایانه در تمام امور اقتصادی، نظامی و اجتماعی جرایم مختلفی می تواند در حوزه رایانه رخ دهد. لذا قانونگذار برای مبارزه و پیشگیری از این جرایم در سال ۱۳۸۸ اقدام به تصویب قانون جرایم رایانه ای در ۵۶ ماده نمود.در حقوق ایران، نه در قانون تجارت الکترونیک و نه در قانون جرایم رایانه‌ای هیچ تعریفی از این مفهوم ارایه نشده است. شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرایم رایانه‌ای وجود دارد. اما می‌توان به عنوان نمونه تعریف زیر را ارایه کرد:

«آن دسته از جرایمی که با سوءاستفاده از یک 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 و سرقت و نیز جرایم نو ظهوری که با تولد رایانه پا به عرصه حیات گذاشته اند دانست، مانند جرایم علیه صحت و تمامیت داده‌ها». در واقع در حقوق ایران تعریف جرایم رایانه ای به سکوت واگذار شده و در بیشتر موارد تقریباً همان تعریف ارایه شده از طرف سازمان همکاری و توسعه اقتصادی را پذیرفته اند.

منابع و ماخذ

۱. انصاری، باقر، حقوق حریم خصوصی، انتشارات سمت، چاپ اول، تهران ۱۳۸۶

۲.پاد، ابراهیم، حقوق کیفری اختصاصی جلد دوم، چاپ اول، تهران، انتشارات رهام، ۱۳۸۲

۳.پاکزاد، بتول، جرایم رایانه، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی، ۱۳۹۵

۴.تننباوم، آندرو اس، شبکه های کامپیوتری، ترجمه عین الله جعفر نژاد قمی، انتشارات علوم رایانه، تهران ۱۳۹۴

۵.جاویدنیا، جواد، جرایم تجارت الکترونیکی، انتشارات خرسندی، چاپ دوم، تهران ۱۳۹۲

۶. جلالی فراهانی، امیرحسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، انتشارات خرسندی، تهران ۱۳۸۹

۷.جلالی فراهانی، امیر حسین، در آمدی بر آیین دادرسی کیفری جرایم سایبری، انتشارات خرسندی، تهران ۱۳۸۹

۸.حییم، سلیمان، فرهنگ کوچک انگلیسی- فارسی، انتشارات فرهنگ معاصر، چاپ پانزدهم، تهران ۱۳۹۲

۹.دزیانی، محمد حسن، ابعاد جزایی کاربرد کامپیوتر و جرایم کامپیوتری، خبرنامه انفورماتیک، شورای عالی انفورماتیک کشور، شماره ۵۸، دی و اسفند ۱۳۹۴

۱۰.شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۷۹

۱۱.شیرزاد، کامران، جرایم رایانه ای از دیدگاه حقوق جزای ایران و بین الملل، نشر بهینه فراگیر ۱۳۹۰

۱۲.عالی پور، حسن، حقوق کیفری فناوری اطلاعات (جرایم رایانه ای)، انتشارات خرسندی، چاپ اول، تهران ۱۳۹۰

۱۳.عمیدی، مهدی، مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز ، ۱۳۹۵

۱۴. فضلی، مهدی، مسوولیت کیفری در فضای سایبر، انتشارات خرسندی، چاپ اول، تهران ۱۳۸۹

۱۵.مایکروسافت، فرهنگ تشریحی واژه ها و اصطلاحات کامپیوتری مایکروسافت، مترجم سعید ظریفی، انتشارات دیباگران، چاپ اول، تهران ۱۳۹۴

۱۶. مایکروسافت، مبانی شبکه، ترجمه امیر اسعد انزالی، جلد اول، انتشارات خجسته، چاپ اول، تهران ۱۳۸۹

۱۷. میرمحمد صادقی، حسین، حقوق کیفری اختصاصی (۲)، جرایم علیه اموال و مالکیت، انتشارات میزان ۱۳۸۲