بررسی خلاءها و ابهامات قانونی در قانون جرائم رایانه‌ای جمهوری اسلامی ایران

تاریخ دریافت:۱۳۹۳/۱۱/۱۶
تاریخ پذیرش: ۱۳۹۳/۱۲/۱۸

چکیده

پیشرفت علم و رشد شتابان فن آوری اطلاعات و ارتباطات(ICT) [۱] بخصوص اینترنت چالش های جدیدی در زندگی بشر ایجاد نموده است. اینترنت سبب ایجاد فضای مجازی در زندگی افراد شده است لذا در کنار تمام مزیت‌ها و محاسنی که ایجاد نموده، خطراتی نیز به دنبال داشته است که از آن جمله می‌توان به وقوع انواع جرائم در سطح وسیعی و گسترده‌ای در جامعه اشاره نمود. وقوع جرائم علیه اموال، اشخاص و امنیت و آسایش عمومی همچنان که در دنیای واقعی رخ می‌دهد در دنیای مجازی نیز به شکل وسیع تر و پیچیده‌تری قابل تحقق است. لذا تدوین قانون جرائم رایانه‌ای توسط مسئولین و متولیان امر پاسخی برای نیاز به وجود آمده در این زمینه بود.

علی ایحال وجود خلاء و ابهام در قانون جرائم رایانه‌ای، عدم تناسب مجازات های تعیین‌شده در قانون با ارتکاب جرم در فضای سایبر، سبب ناامن شدن فضای مجازی و متضرر شدن تعدادی از افراد شده است. لذا شناسایی و برطرف نمودن خلاء های قانونی گام موثری در کارآمدی فضای به وجود آمده در بستر اینترنت و تحقق عدالت کیفری خواهد بود.

واژگان کلیدی: خلاءها و ابهامات قانونی، جرائم رایانه‌ای، فضای مجازی، فن آوری اطلاعات و ارتباطات

مقدمه

۲. Information Connection Technology

امروزه شاهد نفوذ فن آوری اطلاعات و ارتباطات و خصوصاً اینترنت در زندگی روزمره افراد جامعه هستیم. بسیاری از جوامع سعی دارند که مشکلات و موانع خود را با تکیه بر ابزارهای فن آوری اطلاعات و ارتباطات بخصوص اینترنت حل کنند. بنابراین شهر الکترونیکی، شهروند الکترونیکی در بسیاری از کشورهای توسعه‌یافته و در حال توسعه بخصوص کشور عزیزمان ایران در دستور کار دولت‌ها قرارگرفته و امکانات لازم در این زمینه فراهم شده است. دفاتر پیش‌خوان دولت در اقصی نقاط کشور از جمله روستاها از مصادیق دولت الکترونیک می‌باشد.

گرایش ورود افراد جامعه به چنین فضایی باوجود تمامی نکات و جنبه‌های مثبت آن، تبعات منفی فراوانی را نیز به دنبال دارد تا جایی که برخی معتقدند که وجود اینترنت جرم ساز است اما این تصویر نادرستی است. بااینکه اینترنت و استفاده از فضای مجازی لازم و ضروری است اما این بدین معنا نیست که مشکلات زاییده این اجبار بوده بلکه این عامل انسانی است که منشأ بسیاری از معضلات و اعمال مجرمانه در این فضای جدید می‌باشد.(نجار: ۱۳۸۹، ۵) کاربردهای فن‌آوری اطلاعات و ارتباطات از قبیل دولت الکترونیک، تجارت الکترونیک، تحصیل الکترونیک و سلامت الکترونیکی می‌توانند راه را برای جوامع جهت نیل به توسعه و پیشرفت فراهم ساخته و سبب کاهش فقر و بهبود سلامت و شرایط محیطی در کشورها شوند. علی‌رغم تمامی این مزایا، در دسترس بودن فن آوری اطلاعات و ارتباطات و اینترنت، خطراتی را برای جوامع به دنبال دارد که از آن جمله می‌توان به وقوع انواع جرائم رایانه‌ای مانند کلاه‌برداری های اینترنتی، سرقت های اینترنتی، انتشار عکس های خصوصی افراد، جعل های رایانه‌ای و سایر جرائم رایانه‌ای اشاره نمود که در سطح وسیعی از جامعه انجام می‌شود.(گری: ۱۳۸۹، ۱۹-۱۳)

در ایران برای اولین بار در سال ۱۳۸۸ قانون جرائم رایانه‌ای به تصویب رسید. نظر به اینکه جرائم رایانه‌ای سابقه اندکی در ایران داشته و قوانین کمی به این موضوع پرداخته‌اند، بنابراین در این تحقیق قانون جرائم رایانه‌ای در فصل های مختلف مورد بررسی قرارگرفته و با استخراج عناوین مجرمانه، به تحلیل و احصاء نقاط ضعف و خلاءهای موجود در قانون اشاره‌شده و در بخش پایانی نیز پیشنهادها و راهکارها ارائه گردیده است.

مبانی نظری و بیشینه تحقیق

تعریف جرم رایانه‌ای

جرم رایانه‌ای را از دو نظر می‌توان تعریف کرد: در تعریف مضیق، جرم رایانه‌ای اساساً منحصر و محدود به نفوذ غیرمجاز تحریف یا تخریب از طریق کدهای رایانه‌ای، جاسوسی رایانه‌ای، جعل و کلاه‌برداری رایانه‌ای، خرابکاری رایانه‌ای، خواهد بود و شامل آزار و اذیت، سوءاستفاده از پست الکترونیک، سرقت و افترا از طریق

سیستم های رایانه‌ای، نخواهد بود. در تعریف موسع از جرم رایانه‌ای هر فعل یا ترک فعلی که از طریق یا به کمک رایانه و یا از طریق شبکه‌های رایانه‌ای یا از طریق اینترنت انجام می‌شود که توسط قانون ممنوع شده و برای آنها مجازات در نظر گرفته شده است را شامل می‌شود. (بای، قهرمانی،۱۳۸۸: ۳۷)

تاریخچه جرم رایانه‌ای در ایران

در مورد تاریخچه جرم رایانه‌ای در ایران باید گفت: با توجه به اینکه کاربرد رایانه در ایران از ابتدای ورود آن تا دهه ۱۳۷۰ بسیاری محدود بوده است. در نتیجه جرم رایانه‌ای سابقه چندانی در کشور ما ندارد و اگر احیاناً جرمی در این خصوص واقع شده باشد، گزارشی از آن منتشر نشده است. وقوع جرم رایانه‌ای به‌تدریج از دهه۱۳۷۰ در ایران شروع شد. سوءاستفاده از رایانه برای ارتکاب جرائم سنتی، به‌کارگیری ویروس از طریق توزیع حامل‌های داده آلوده به ویروس، سوءاستفاده مالی و تکثیر غیرمجاز نرم‌افزار های رایانه‌ای از جمله جرائم رایانه‌ای هستند که در مقیاس بسیار کم در دهه۱۳۷۰ واقع شده است و با قوانین کیفری مرسوم مورد رسیدگی قرارگرفته اند. داد نامه مورخه۱۳۷۲/۴/۳ شعبه ۶۵ دادگاه کیفری۲ تهران یک نمونه از آنهای است که بیان گر به‌کارگیری قوانین کیفری سنتی در خصوص جرائم رایانه‌ای است. (همان، ۵۷:۱۳۸۸)

ویژگی جرائم رایانه‌ای

جرائم رایانه‌ای اقدامات زیان باری است که از طریق یک رایانه یا شبکه رایانه‌ای به وقوع پیوسته و یا هر اقدام زیان باری است که علیه رایانه یا شبکه‌ای رایانه‌ای ارتکاب می‌یابد. این جرائم ویژگی متمایزی نسبت به سایر جرائم کلاسیک دارند، چرا که ماهیت این‌گونه جرائم به دلیل تکنولوژی پیچیده و بالا خصوصیات منحصر به فردی داشته و باعث می‌شود قوانین مرسوم پاسخ گوی مسایل نباشند. در ذیل به تشریح این ویژگی می‌پردازیم. (بای، پور قهرمانی،۶۱:۱۳۸۸)

در خصوص عنصر مادی جرائم سنتی یا کلاسیک و مرسوم باید گفت: به دلیل بسترهای متفاوت ارتکاب آنها به شکل های متفاوت سناریوی مجرمانه، طبعاً عنصر مادی هر جرم با جرم دیگر تفاوت دارد، ولی در جرائم رایانه‌ای خصوصاً در جرائم نسل اول، شکل عنصر مادی تقریباً یکسان است. به عبارتی، اجزای جرم رایانه‌ای عبارت‌اند از ورود، تغییر، محو، متوقف سازی، دست‌کاری و امثال آن در داده‌ها، برنامه‌ها یا سیستم های رایانه‌ای و شبکه‌های ارتباط راه دور می‌باشند. همین ویژگی باعث بروز تفاوت در جرائم رایانه‌ای نسبت به جرائم کلاسیک است. برای مثال، در جرم کلاه‌برداری رایانه‌ای ورود و یا تغییر داده‌های مالی موجب نقل‌وانتقال وجوه می‌شود، بدون اینکه آن فرد مستقیماً فریب بخورد یا حتی با مجرم مواجه شده باشد.(باستانی،۷۷:۱۳۸۱)

نکته‌ای که در اینجا باید خاطرنشان کرد این است که در حالت کلی عنصر مادی هر جرم عبارت است از فعل، ترک فعل، فعل ناشی از ترک فعل، نگهداری و داشتن چیزی که به‌موجب قانون جرم شناخته شده است. حال آیا تصور جرم رایانه‌ای که عنصر مادی آن به شکل ترک فعل و نگهداری باشد ممکن است یا همه جرائم رایانه‌ای به‌صورت فعل مثبت تحقق می‌یابد؟ (بای، پور قهرمانی،۱۳۸۸:۶۳)

برخی نویسندگان ادعا کرده‌اند که در جرائم رایانه‌ای ترک فعل، داشتن و نگه‌داری تا کنون مصداق عینی نداشته است، بنابراین جرائم رایانه‌ای ، جزو جرائم عمدی است و هرگونه بی‌احتیاطی، بی‌مبالاتی، نداشتن مهارت و ... که جزو مصادیق خطا هستند باید در زمره تخلفات مدنی یا اداری بررسی شوند و نباید جزو موارد کیفری به حساب آیند. (حسینی خواه، ۱۳۷۷:۴۶)

عنصر روانی جرائم رایانه‌ای

عمل مجرم علاوه بر اینکه در قانون ذکر می‌شود و تحقق خارجی می‌یابد، باید توأم با سوءنیت و قصد مجرمانه یا تقصیر جزایی باشد. در جرائم سنتی یا کلاسیک اصل بر عمدی بودن جرائم است، اما در جرائم رایانه‌ای به‌واسطه ماهیت فضای سایبر، درصد جرائم ناشی از بی‌مبالاتی افزایش‌یافته است، به گونه‌ای که به طور یکسان یا حتی فراتر از جرائم عمدی با انواع جرائم ناشی از بی‌مبالاتی آن مواجه می‌شویم. از سویی تبلور این رویکرد در نوع مسئولیت کیفری و افراد دارای مسئولیت کیفری به خوبی قابل‌مشاهده است. تعدادی از افراد مشغول به‌کار در زمینه فن آوری به‌واسطه نوع مسئولیت و فعالیت یا به‌واسطه تدابیری که باید بیندیشند یا به‌واسطه چهارچوب وظایف حرفه‌ای که برای آن تعیین شده است، دارای مسئولیت هستند و این مسئولیت غالباً به خاطر بی‌مبالاتی به وجود می‌آید. (دزیانی،۱۳۸۲:۷۷)

مرتکبین جرائم رایانه‌ای

در برخی جرائم، ارتکاب جرم مستلزم آشنایی با تکنیک یا تکنولوژی خاصی است. در جرائم رایانه‌ای، رایانه هدف و یا وسیله واسطه ارتکاب جرم است، بنابراین مجرم تا حدی از تخصص را دارا می‌باشد. بسته به نوع جرم رایانه‌ای، گاه آشنایی کلی با این تکنولوژی کافی و گاه نیاز به تخصص در سطح بالاست. سطح مهارت معمول در مجرمان رایانه‌ای محور برخی مباحث را تشکیل می‌دهد. برخی عقیده دارند سطح مهارت، شاخصی برای مجرمان رایانه‌ای به شمار نمی‌آید حال آنکه بعضی دیگر بر این باورند مجرمان بالقوه رایانه‌ای افرادی باهوش، باذوق و دارای انگیزه‌اند که آمادگی رویارویی با چالش های تکنولوژی را دارند. (بای، پور قهرمانی،۱۳۸۸:۶۷)

تاریخ نشان داده است که طیف وسیعی از افراد مرتکب جرائم رایانه‌ای شده‌اند دانشجویان، غیرحرفه‌ای‌ها، تروریست ها و اعضای گروهای سازمان‌یافته می‌باشند. سن مجرمان بین ده تا شصت سال است و دامنه مهارت آنها از سطح تازه‌کار تا حرفه‌ای را می‌پوشاند.بنابراین، مجرمان رایانه‌ای غالباً افرادی معمولی هستند و نه ابر تبهکارانی با توانایی و استعدادهای بی‌همتا. (پاکزاد،۴۵:۱۳۷۵)

هر فردی باهر سنی و با داشتن مهارت‌های نه چندان زیاد و باانگیزه چالش های فنی، امکان کسب منافع، اشتهار یا انتقام یا اشاعه باورهای عقیدتی، یک مجرم رایانه‌ای بالقوه محسوب می‌شود. (بای، پور قهرمانی،۶۷:۱۳۸۸)

مطابق مطالعات انجام‌شده بیشترین تهدیدها از طرف کارمندان است و در واقع جرائم رایانه‌ای غالباً با منشأ داخلی به شمار می‌آیند. طبق برآوردی که به عمل‌آمده، نود درصد از جرائم رایانه‌ای به‌وسیله کارمندان بزه دیده انجام گرفته است. (نشریه بین‌المللی سیاست جنایی،۱۲۳:۱۳۷۷)

جرائم رایانه‌ای

جرائم علیه محرمانگی داده‌ها و سامانه‌ها

دسترسی غیرمجاز

دسترسی غیرمجاز، به معنی دستیابی بدون مجوز به محتوای ذخیره‌شده و یا در حال پردازش در یک یا چند سامانه رایانه‌ای، مخابراتی یا شبکه‌ای می‌باشد؛ این محتوا می‌تواند طیف متفاوت و گسترده‌ای از داده‌های رایانه‌ای در قالب فایل‌هایی با پسوندهای مختلف باشد. (الهی منش،سدره نشین، ۱۳:۱۳۹۱)

تحقق جرم دسترسی غیرمجاز در این ماده، به سامانه‌های امن و نیز نقض تدابیر ایمنی مقید شده و سامانه‌های غیر ایمن و نیز دسترسی بدون نقض تدابیر ایمنی، از شمول این ماده بیرون هستند که این یک خلاء قانونی جدی محسوب می‌شود. از طرف دیگر، تا کنون ملاک و معیار مشخصی برای تعیین ایمنی(امنیت) و یا ناامنی برای یک سامانه یا شبکه رایانه‌ای یا مخابراتی ارائه نشده و معمولاً این‌گونه موارد، سلیقه‌ای است؛ به‌طوری که از نگاه عده‌ای با نصب یک نرم‌افزار امنیتی و یا دیوار آتشین سامانه یا شبکه‌ایمن محسوب می‌شود اما از نظر برخی دیگر از متخصصان حرفه‌ای، چنین سامانه‌هایی از امنیت مطلوب برخوردار نیستند و لازم است تجهیزات نرم‌افزاری و سخت‌افزاری خاصی بر روی آنها نصب گردد. (همان، ۱۳۹۱: ۱۴)

معاونت در جرم دسترسی غیرمجاز نیز در صورت وجود شرایط مقرر در ماده ۱۲۶ قانون مجازات اسلامی[1] امکان‌پذیر است و از این منظر تابع شرایط عمومی مجازات ها می‌باشد. (همان، ۱۳۹۱: ۲۲)

[1] ماده ۱۲۶ قانون مجازات اسلامی مقرر می دارد :» اشخاص زیر معاون جرم محسوب می شوند:

برای تحقق جرم دسترسی غیرمجاز، رفتار مرتکب باید به‌صورت فعل مثبت باشد؛ لذا با ترک فعل نمی‌توان وقوع این جرم را محرز دانست. (همان، ۱۳۹۱: ۲۲)

دست‌یابی ممکن است در فضای مجازی و یا در فضای واقعی صورت گیرد. دسترسی در فضای مجازی اقدام به نفوذ در سامانه و مشاهده داده‌ها است اما دسترسی به اطلاعات در فضای واقعی نیز قابل تصور است مانند اینکه مرتکب وارد اتاق کاربر شده و به داده‌های در حال نمایش و قابل‌مشاهده بوده و به آنها دسترسی پیدا کرده باشد. (محمد نسل، ۱۳۹۲: ۲۸)

منظور از داده همان «دیتا» در واژگان فنی مصطلح فنی است. بر اساس تعریف ارائه‌شده در بند «ب» ماده۱ کنوانسیون جرائم رایانه‌ای اتحادیه اروپا، منظور از «داده رایانه‌ای» هر گونه نمایش حقایق، اطلاعات یا مفاهیم به شکلی مناسب که برای پردازش در یک سیستم رایانه‌ای که شامل برنامه‌ای مناسب است و باعث می‌شود که این سیستم عملکرد خود را به مرحله اجرا گذارد، مورد استفاده قرار می‌گیرد. (همان، ۱۳۹۲: ۲۸)

شنود غیرمجاز

عمل مادی مرتکب، شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری است که نوعاً از طریق فعل مثبت مادی صورت می‌گیرد. (محمد نسل، ۱۳۹۲: ۳۶)

در نگاه اول به نظر می‌رسد که عنوان شنود غیرمجاز فقط ناظر بر داده‌های در حال انتقال است و شنود محتوای داده‌های ذخیره‌شده در رایانه و سامانه‌ها باید تحت عنوان دسترسی غیرمجاز مورد تعقیب و مجازات قرار گیرد؛ لیکن قانون‌گذار در تبصره ذیل ماده ۴۶ قانون جرائم رایانه‌ای دسترسی به محتوای ذخیره‌شده غیرعمومی مانند پست الکترونیکی و پیام رایانه‌ای ذخیره‌شده را نیز در حکم شنود غیرمجاز قرار داده است. (همان، ۱۳۹۲: ۳۷)

شنود غیرمجاز را می‌توان «هر گونه دریافت غیر قانونی محتوای در حال انتقال ارتباطات غیرعمومی در بستر فضای تولید و تبادل اطلاعات به طور پنهانی » تعریف نمود. (الهی منش،سدره نشین، ۱۳۹۱:۱۳)

الف- هرکس دیگری را ترغیب، تهدید، تطمیع یا تحریک به ارتکاب جرم کند یا با دسیسه یا فریب یا سوء استفاده از قدرت، موجب وقوع جرم گردد،

ب- هر کس وسایل ارتکاب جرم را بسازد یا تهیه کند یا طریق ارتکاب جرم را به مرتکب ارائه دهد؛

ج- هر کس وقوع جرم را تسهیل کند.

تبصره۱: برای تحقق معاونت در جرم، وحدت قصد و تقدم یا اقتران زمانی بین رفتار معاون و مرتکب جرم شرط است. چنانچه فاعل اصلی جرم، جرم شدیدتر از آنچه مقصود معاون بوده مرتکب شود، معاون به مجازات جرم معاونت در جرم خفیف تر محکوم می شود.»

تا پیش از تصویب قانون جرائم رایانه‌ای، مقررات لازم جهت پوشش این جرم نوین و مستمر در فضای سایبر در کشور وجود نداشت ازاین‌رو تصویب ماده ۲، مفید و موثر بوده و شنود غیرمجاز و سوءاستفاده‌های احتمالی از سامانه‌های رایانه‌ای و مخابراتی در این بستر را با مجازات، محدود می‌کند. (همان، ۱۳۹۱: ۲۴)

شنود غیرمجاز محتوای در حال انتقال، پدیده‌ای خاص است و با «استراق سمع» تفاوت دارد؛ زیرا استراق سمع به‌صورت شنیداری و در بستر مکالمات تلفنی- مخابراتی صورت می‌گیرد؛ اما عمل شنود تنها در خصوص سیگنال‌ها و امواج مطرح می‌باشد. این سیگنال‌ها ممکن است به‌صورت نوری، صوتی و الکترومغناطیسی (رادیویی، مادون‌قرمز، ماورای بنفش) باشد. هر یک از موارد ذکرشده می‌توانند به‌صورت آنالوگ و یا دیجیتال مبادله شوند. (همان، ۱۳۹۱: ۲۵)

وجه تمایز جرم «شنود غیرمجاز» از جرم «دسترسی غیرمجاز» موضوع جرم می‌باشد. موضوع جرم دسترسی غیرمجاز، داده‌های ذخیره‌شده و یا در حال پردازش در سامانه‌های رایانه‌ای یا مخابراتی است که به طور غیرمجاز توسط افراد ناصالح مورد رصد قرار می‌گیرند؛ ولی موضوع جرم شنود غیرمجاز، محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری می‌باشد و هر گونه کیفیت اضافه بر آن، جرم را با توصیف های دیگر همراه کرده و حتی می‌تواند موجب تحقق تعدد جرم باشد. در واقع جرم شنود غیرمجاز، هم جرم مستقل و هم جزئی از عنصر مادی جرائم رایانه‌ای است که در مورد اخیر موجب تشدید مجازات می‌شود. (همان، ۱۳۹۱: ۲۵)

جاسوسی رایانه‌ای

مرتکب جرم می‌تواند هر کسی اعم از نظامی یا غیرنظامی و ایرانی یا خارجی باشد. وجود سمت خاصی نیز برای شخص مرتکب شرط نشده است.

عمل مرتکب انجام حداقل یکی از سه عمل زیر است که هر سه آنها نوعاً از طریق فعل صورت می‌گیرد:

- دسترسی غیرمجاز؛
- تحصیل غیرمجاز؛
- شنود غیرمجاز.

داده‌های موضوع جرم ممکن است در حال انتقال به سامانه یا حامل داده دیگر باشند و یا اینکه از داده‌های ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل های داده باشند و اصلاً در حال انتقال و جابجایی هم نباشند. (محمد نسل، ۱۳۹۲: ۴۱)

داده‌های موضوع جرم دسترسی غیرمجاز باید از نوع سری باشند. البته لازم نیست که چنین لطمه‌ای حتماً فعلیت پیدا کند بلکه همین که نوعاً خطر چنین لطمه‌ای وجود داشته باشد، برای تحقق جرم کافی است. (همان، ۱۳۹۲: ۴۲)

با رایانه‌ای شدن امور و تجهیز مراکز دولتی حساس به رایانه و اینترنت و شبکه‌های داخلی، احتمال وقوع جاسوسی نسبت به گذشته افزایش‌یافته، با این تفاوت که در فضای سایبر هرلحظه حجم عظیمی از داده‌ها و اطلاعات مبادله می‌شود و کاربری که خلاقیت و دانش نفوذ در سامانه یا شبکه داشته باشد می‌تواند جاسوسی کند.(الهی منش، سدره نشین، ۱۳۹۱: ۳۳)

نقض تدابیر امنیتی سامانه‌ها

این جرم انگاری برای حفاظت از سامانه‌های رایانه‌ای و مخابراتی حیاتی و حساس و تأمین امنیت آنها بوده و نوعی جرم بازدارنده تلقی می‌شود تا مقدمات تحقق جرم جاسوسی رایانه‌ای برچیده شود. (الهی منش، سدره نشین، ۳۶:۱۳۹۱)

جرم موضوع این ماده با انجام فعل مثبت مادی تحقق می‌شود، لذا با ترک فعل نمی‌توان وقوع آن را محرز دانست. (همان،۳۶:۱۳۹۱)

این جرم در زمره جرائم عمدی و مقید قرار دارد و برای تحقق و احراز آن به سوءنیت عام و نیز سوءنیت خاص نیاز است؛ لذا خواست نقض تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی با علم به وجود تدابیر مزبور به‌قصد دسترسی به داده‌های سری باید احراز شود. (همان،۳۶:۱۳۹۱)

نحوه دسترسی خود فرد مرتکب به داده‌های موضوع جرم تأثیری در عنوان جرم ندارد لیکن چنانچه بنا به شغل و موقعیت خود و به طور مجاز به داده‌های اصلی(sorce) دسترسی داشته و یا اینکه متصدی سامانه یا کاربر آن بوده و به‌این‌ترتیب با استفاده از وضعیت خود مرتکب جرم شده باشد، در این صورت عمل وی مشمول تشدید مجازات خواهد شد. (محمد نسل، ۱۳۹۲: ۴۷)

نقض تدابیر امنیتی سامانه‌ها

بزه پیش‌بینی‌شده در این ماده حاکی از نوعی بی‌احتیاطی و سهل‌انگاری در مفهوم عام آن است و به نظر می‌رسد ذاتاً از جنس «ترک فعل» باشد لیکن بهتر است آن را اعم از فعل و ترک فعل بدانیم، زیرا این عناوین در جرائم غیرعمدی قابلیت تبدیل به یکدیگر دارند. (الهی منش،سدره نشین، ۳۸:۱۳۹۱)

قانون‌گذار برای مشخص نمودن مرتکب جرم از عنوان «ماموران دولتی» استفاده کرده، عنوانی که کلیه کارمندان و حقوق‌بگیران دولت را در هر طبقه و صنف و هر مقام دربر می‌گیرد. نکته قابل‌توجه این است که

نوع رابطه استخدامی ایشان مطرح نیست رسمی باشند یا پیمانی، روزمزد باشند یا خرید خدمت، ایرانی باشند یا خارجی. منظور کسی است که با داشتن رابطه استخدامی اعم از دائم یا موقت و با دریافت حقوق، تحت هر عنوانی برای دولت کار می‌کند از این عبارت می‌توان استنباط نمود که این ماده اشخاصی را که مأمور دولت نبوده و اطلاعات قیدشده در ماده را در اختیاردارند شامل نمی‌شود لیکن اگر شخص مرتکب کارمند دولت باشد حتی اگر مسئولیت امور حفاظت از داده‌های سری را بر عهده نداشته باشد مشمول مقررات این ماده خواهد بود. (همان،۱۳۹۱:۳۸)

جرائم علیه صحت و تمامیت داده‌ها و سامانه‌ها

مصادیق و مجازات جعل رایانه‌ای

جعل رایانه‌ای در برخی موارد، مشابه جعل سنتی است، بااین‌وجود لزوم جرم انگاری جعل رایانه‌ای با توجه به عدم کفایت ماده ۵۲۳ قانون مجازات اسلامی احساس می‌شد. مهم‌ترین دلیل این امر را می‌توان در تعریف سند مندرج در قانون مدنی جست و جو نمود؛ زیرا بر اساس قانون مدنی، «سند عبارت است از نوشته ای که در مقام دعوا یا دفاع قابل استناد باشد و منظور از نوشته، نوشتارهای عینی واقعی است.» بدین ترتیب می‌توان گفت که چون تعریف سند و نوشته شامل اسناد الکترونیکی (که داده‌های رایانه‌ای اجزای آن را تشکیل می‌دهند) نمی‌شود لذا، ماده ۵۲۳ قانون مجازات اسلامی نیز شامل جعل رایانه‌ای نیست ازاین‌رو تصویب ماده ۶ اقدامی به‌جا و مناسب می‌باشد. (الهی منش،سدره نشین، ۱۳۹۱:۱۳)

جعل یکی از جرائمی است که در عین خطرناک و ضد اجتماعی بودن، ارتکاب آن از سهولت زیادی برخوردار است و شاید به همین دلیل هم هست که بزه خطرناک و خلاف آسایش عمومی دانسته شده و در تمام قانون‌گذاری‌ها با مجازات نسبتاً شدیدی همراه است چه اگر این جرم جنبه عمومی به خود گرفته و رایج گردد، برای هیچ کس در روابط حقوقی‌اش تأمین و تضمینی وجود نخواهد داشت؛ به همین دلیل جرم جعل در دو وجه سنتی و رایانه‌ای در زمره جرائم «غیرقابل گذشت» قرار دارد. (همان، ۱۳۹۱:۴۴)

بیشتر قوانین جزایی، بدون اینکه تعریف جامعی از جعل رایانه‌ای ارائه دهند و ارکان جرم جعل را دقیقاً تعیین کنند، صرفاً به ذکر و نام بردن روش‌های مختلف جعل و میزان مجازات بسنده کرده‌اند، چرا که ممکن است تعریف، ابزاری جامع‌ومانع نباشد و مصادیقی از این تعریف خارج شود و در نتیجه نظم عمومی با ارتکاب جرائم مشابه به هم بخورد و قانون‌گذار سلاحی برای مقابله با آن نداشته باشد. ازاین‌رو قانون، تعریف جرم را بر عهده رویه قضایی می‌گذارد، چه آنکه رویه قضایی در طول زمان تغییر می‌کند و به‌راحتی می‌تواند خود را با مقتضیات زمان منطبق سازد. (همان، ۱۳۹۱:۴۴)

رایانه‌ها از دو جهت در ارتکاب جرم جعل دخیل هستند:

به‌کارگیری فناوری رایانه‌ای برای دست بردن به اسناد کاغذی که بر مبنای قوانین سنتی (از جمله مواد ۵۲۳ تا ۵۲۴ قانون مجازات اسلامی) قابل مجازات بوده و از بحث ما خارج است.

استفاده از فناوری رایانه‌ای برای دست‌کاری در داده‌ها و اسناد الکترونیکی (دیجیتالی). (همان، ۴۵:۱۳۹۱)

مقنن در بند «الف» سه مصداق زیر را به‌عنوان عمل مجرمانه مرتکب بیان کرده است که با تأمل در آنها روشن می‌شود که هر سه عمل از طریق ارتکاب فعل بوده و با ترک فعل قابل انجام نیستند: (محمد نسل، ۱۳۹۲: ۷۰)

- ایجاد داده‌ها؛
- تغییر داده‌ها؛
- ورود داده‌ها.

جعل رایانه‌ای نیز مانند جعل عادی ممکن است از طریق خلق ابتدایی داده جعلی و یا دست‌کاری و تغییر داده‌های اصیل موجود و تبدیل آن به داده‌های جعلی، صورت گیرد. مقنن در خصوص ایجاد و یا تغییر ابتدایی داده جعلی، متقلبانه بودن عمل را لازم ندانسته و فقط به غیرمجاز بودن عمل اشاره‌کرده است اما در خصوص دست‌کاری داده‌های موجود، متقلبانه بودن عمل مورد تصریح قرارگرفته است. (همان، ۱۳۹۲: ۷۰)

ربایش داده‌های متعلق به دیگری

مجموعه قوانین کیفری کشورها تاکنون به طور عمده، موضوعات مادی و ملموس و قابل‌رؤیت را مورد حمایت قرار داده‌اند، اما در چند دهه گذشته به علت تغییرات فراوان از جمله تبدیل جامعه صنعتی به‌جامعه فرا صنعتی، اطلاعات ارزش بسیاری پیداکرده، به گونه‌ای که داده‌ها و اطلاعات را پس از ماده و انرژی به‌عنوان سومین عامل بنیادی می‌شناسند. امروز داده‌های متعلق به‌کاربران در سامانه‌ها و شبکه‌های رایانه‌ای، دستگاه‌های الکترونیکی، گوشی‌های تلفن همراه، وب سایتها، وبلاگ‌ها و همچنین شبکه‌های اجتماعی مجازی در قالب فایل‌های متنی، صوتی و تصویری ذخیره‌شده‌اند. قانون‌گذار ایران در این ماده، داده‌های متعلق به‌کاربران رایانه و فضای سایبر(به مفهوم عام، شامل تمامی اشخاص حقیقی، حقوقی و دولتی) را مورد حمایت کیفری قرار داده است. (الهی منش،سدره نشین، ۷۳:۱۳۹۱)

با توجه به اینکه حوزه‌های جرائم سرقت و کلاه‌برداری مرتبط با رایانه در بستر محیط سایبر دارای وجوه مشترک بسیاری می‌باشند، به‌راحتی نمی‌توان آنها را از یکدیگر تفکیک نمود. به همین دلیل قانون‌گذار آنها را در ذیل یک فصل از قانون جرائم رایانه‌ای بیان نموده است. (همان، ۷۳:۱۳۹۱)

برخی از استادان پاسخ این پرسش را که آیا موضوع سرقت، شیء است یا مال، به نحوه نگرش حکومت‌ها به اهمیت نظم و امنیت اجتماعی و حدود مالکیت افراد مربوط می‌دانند، با این بیان که اگر نظم، اهمیت بیشتری داشته باشد از هر شیء متعلق به غیر حمایت می‌شود و اگر مال بیشتر اهمیت داشته باشد، دیگر از شیء متعلق به غیر حمایت نمی‌شود، هرچند نظم مخدوش گردد. (همان، ۷۴:۱۳۹۱)

در اصلاح قانون مجازات اسلامی که توسط مرکز تحقیقات فقهی قوه قضاییه تدوین‌شده و به تصویب رییس قوه قضاییه رسیده، سرقت این‌گونه تعریف شده است: «سرقت عبارت است از ربودن شیء متعلق به غیر». با تصویب این ماده است تقریباً این مسئله نیز حل می‌شود، زیرا از دیدگاه دانش مهندسی شیء شامل داده‌ها و اطلاعات رایانه‌ای نیز می‌باشد. (همان، ۷۴:۱۳۹۱)

نکته مهمی که باید بدان اشاره نمود، مسئله تفکیک سرقت رایانه‌ای از کلاه‌برداری رایانه‌ای است؛ برای مثال شخصی با ورود به سامانه رایانه‌ای یک بانک، وجوهی را از حساب دیگری به حساب خود انتقال می‌دهد، یا با دست‌کاری نرم افزاری یا سخت‌افزاری دستگاه خودپرداز مبلغی بیش از مقدار حساب خود دریافت می‌کند. چنین مواردی آیا سرقت محسوب می‌شود یا کلاه‌برداری؟ برخی از صاحب‌نظران در تمایز و تفکیک این دو جرم گفته‌اند که کلاه‌برداری در مفهوم عام خود، شامل سرقت رایانه‌ای نیز می‌شود، اما ازآنجاکه سرقت رایانه‌ای ناظر به سرقت داده‌ها و فایل‌هاست، علاوه بر اینکه یک جرم رایانه‌ای محض محسوب می‌شود، موضوع آن نیز صرفاً مال نیست و از همین مجرا، بین کلاه‌برداری رایانه‌ای که منتج به تحصیل مال یا منافع مالی است و سرقت رایانه‌ای که منجر به ربودن داده‌ها و فایل‌های رایانه‌ای است تفاوت حاصل می‌شود. در واقع رایانه در کلاه‌برداری رایانه‌ای «وسیله ارتکاب جرم» و در سرقت رایانه‌ای «موضوع ارتکاب جرم» است. به عقیده نگارندگان قسمت اخیر این توجیه از دیدگاه دانش مهندسی نرم‌افزار رایانه و اصول پذیرفته‌شده حقوق کیفری غیرقابل‌قبول بوده و موجب سردرگمی مخاطبین می‌گردد، زیرا موضوع جرم در سرقت‌های رایانه‌ای «داده‌های متعلق به دیگری» است. درهرصورت به نظر می‌رسد چنانچه قصد مرتکب از سرقت داده‌های رایانه‌ای تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری باشد، برای تعیین تکلیف باید به مقررات و ضوابط مندرج در ماده ۱۳ قانون جرائم رایانه‌ای (م ۷۴۱ ق.م.ا) راجع به کلاه‌برداری رایانه‌ای مراجعه نمود. (همان، ۷۵:۱۳۹۱)

عمل مادی این جرم ربایش داده است. ربایش ممکن است از درون سامانه یا ابزار های حامل داده و یا در حال انتقال از سامانه‌ای به سامانه دیگر صورت گیرد. ربایش داده مستلزم دسترسی به داده‌ها و انتقال آنها از سامانه یا ابزار حامل داده به سامانه یا حامل دیگر است که به‌صورت رونوشت برداشتن یا قیچی کردن داده‌ها و خارج کردن آن از فضای مجازی موجود صورت می‌گیرد. (محمد نسل، ۱۳۹۲: ۱۰۲)

عمل مرتکب باید به طور غیرمجاز صورت گرفته باشد. کلمه ربایش نیز اشاره بر غیرمجاز و عدوانی بودن برداشت داده‌ها دارد. بنابراین درصورتی‌که نفوذ و برداشتن داده‌ها بر اساس مجوز قضایی صورت گرفته باشد ، عمل مرتکب مشمول عنوان سرقت داده‌ها نخواهد بود. (همان، ۱۳۹۲: ۱۰۲)

گاهی ممکن است سرقت داده همراه با سرقت خود سامانه یا ابزارهای حامل داده صورت گیرد که در این صورت سرقت داده‌ها جرمی مستقل از سرقت فیزیکی سامانه یا حامل داده بوده و حکم تعدد جرم در چنین فرضی حاکم خواهد بود. (همان، ۱۳۹۲: ۱۰۲)

در سرقت عادی، تحقق سرقت مستلزم خروج عین مال از دسترسی و تملک مالباخته است، یعنی یک مال نمی‌تواند هم زمان هم در اختیار سارق و هم در اختیار مال باخته باشد اما در سرقت داده‌ها به دلیل ماهیت فضای مجازی و امکان تولید نسخه‌های متعدد یکسان از داده‌ها، می‌تواند در عین حفظ داده اولیه، رونوشت های متعددی از آن تهیه شود بدون این که در موجودیت داده اصلی نقصان یا خللی ایجاد شود. در واقع سرقت داده‌ها می‌تواند به دو صورت برداشت عین داده (با قیچی کردن داده‌ها) یا برداشت رونوشت داده (با کپی کردن داده‌ها) صورت پذیرد. (همان، ۱۳۹۲: ۱۰۲)

داده‌های مورد سرقت باید متعلق به غیر باشند. بنابراین چنان چه داده‌ها، قبل از سرقت به هر نحو ممکن به مالکیت مرتکب درآمده باشد، عنوان سرقت منتفی است. قانون‌گذار در مورد سرقت داده‌های مشترک توسط یکی از صاحبان داده‌ها حکمی را بیان نکرده است و در این مورد باید منتظر رویه قضایی ماند. (همان، ۱۳۹۲: ۱۰۲)

ممکن است شخصی سیستم رایانه‌ای متعلق به خود را به دیگری فروخته و در حین فروش بدون اطلاع و توجه وی داده‌های متعلق به وی در اختیار خریدار قرارگرفته و خریدار آنها را تصرف کند. آیا در چنین فرضی سرقت داده‌ها قابل اطلاق بر مورد خواهد بود یا خیر؟ قانون در این خصوص ساکت است لیکن به دلیل اینکه کل سامانه پس از انجام معامله متعلق به مرتکب بوده و طبعاً داده‌ها نیز به تبع سامانه به تملک خریدار در آمده است، بنابراین اطلاق عنوان سرقت بر عمل مرتکب مناسب به نظر نمی‌رسد و باید به دنبال یافتن عنوان مجرمانه دیگری بود. البته نظر دیگری هم وجود دارد و آن این است که مالکیت داده امری جدا از مالکیت سامانه است و فرد به‌صرف خرید سامانه، مالک داده‌هایی که انتقال آنها مورد نظر متعاملین نبوده است، نخواهد شد و بنابراین داده‌هایی که بدون اطلاع و رضایت فروشنده از اطلاعات موجود در رایانه برداشت‌شده، غیرمجاز بوده و می‌توان تملک آنها را مشمول عنوان سرقت دانست. قول اخیر مناسب تر به نظر می‌رسد. (همان، ۱۳۹۲: ۱۰۳)

کلاهبرداری رایانه‌ای

کلاه‌برداری رایانه‌ای از جهت اسمی و نتیجه حاصل از جرم با کلاه‌برداری کلاسیک شباهت دارد اما تفاوت آنها از جهت فرآیند ارتکاب و عناصر اختصاصی تشکیل‌دهنده جرم، باعث شده کلاه‌برداری رایانه به‌عنوان جرمی مستقل از کلاه‌برداری کلاسیک مطرح شود. خاطرنشان می‌شود هرگونه ارتکاب کلاه‌برداری به‌وسیله رایانه، کلاه‌برداری رایانه‌ای محسوب نمی‌شود. (الهی منش،سدره نشین، ۸۱:۱۳۹۱)

«رایانه» از دو جهت در ارتکاب کلاه‌برداری دخیل است:

الف) استفاده از رایانه برای ارتکاب کلاه‌برداری کلاسیک: بدین‌صورت که مرتکب از طریق رایانه متوسل به وسایل متقلبانه گردیده و دیگری را فریب می‌دهد و مال او را می‌برد. در این صورت چون رایانه صرفاً به‌عنوان وسیله ارتکاب جرم مورد استفاده قرار می‌گیرد و نوع وسیله در تحقق کلاه‌برداری کلاسیک مؤثر نیست، لذا عمل مرتکب با قوانین کیفری مربوط به کلاه‌برداری کلاسیک قابل تعقیب و مجازات بوده و جرم ارتکاب یافته، کلاه‌برداری کلاسیک است که می‌توان آن را «کلاه‌برداری کلاسیک رایانه‌ای» نیز نامید.

ب) استفاده از رایانه برای ارتکاب کلاه‌برداری رایانه‌ای به این صورت که مرتکب بدون فریب قربانی و یا نماینده وی از طریق مداخله‌ای ناروا در داده‌های رایانه‌ای یا عملکرد سامانه‌های رایانه‌ای، مال او را می‌برد، یا از خدمات مالی متعلق به او بهره‌مند می‌شود. این نوع کلاه‌برداری که عنصر مادی آن با کلاه‌برداری کلاسیک متفاوت است و با قوانین کیفری مربوط کلاه‌برداری کلاسیک قابل تعقیب و مجازات نیست، کلاه‌برداری رایانه‌ای نامیده شده است. (همان، ۸۱:۱۳۹۱)

جرائم علیه عفت عمومی

هرزه‌نگاری (پورنوگرافی)

هرزه‌نگاری در مفهوم عام به معنای مطالبی است که عمدتاً به‌قصد تحریک جنسی ارائه می‌شود؛ تصاویری از قبیل اندام تناسلی مرد و زن، جنس مرد و زن و ... که عناوین مستهجن مطرح گردد. در مورد هرزه‌نگاری (پورنوگرافی)، نوشته‌های بسیاری وجود دارد که هیچ یک به تعریف آن نپرداخته و اگر هم تعریف نموده در مورد هرزه‌نگاری کودک بوده است. (الهی منش،سدره نشین ، ۸۹:۱۳۹۱)

در حال حاضر، اینترنت به‌واسطه داشتن سه ویژگی «قابلیت دسترسی آسان کاربران به آن»، «داشتن توان مالی در پرداخت بهای آن» و «ناشناس ماندن مصرف کنندگان آن» مهم‌ترین منبع اشاعه هرزه‌نگاری است. (همان، ۸۹:۱۳۹۱)

ماده ۱۴(م ۷۴۲ ق.م.ا) در جهت دفاع از عفت و اخلاق جامعه برای حمایت از اخلاق فردی و جمعی، تدوین‌شده و جرم موضوع آن در زمره جرم‌های گذشت ناپذیر است. (همان، ۸۹:۱۳۹۱)

این ماده در کشورهای به‌اصطلاح پیشرفته از حیث اینکه در آن کشورها نسبت به بزرگ‌سالان آزادی جنسی برقرار است، پیشینه قانون‌گذاری ندارد. مقررات این ماده فراتر از مقررات این کشورها و کنوانسیون بوداپست و منطبق بر فرهنگ ایرانی اسلامی انگاشته شده است. (همان، ۸۹:۱۳۹۱)

هتک حیثیت و نشر اکاذیب

هتک حیثیت از طریق تحریف نگاری هویت یا هرزه‌نگاری شخصیت

از لحاظ دسته‌بندی کیفری، مواد ۱۶ و ۱۷ قانون جرائم رایانه‌ای (مواد ۷۴۴و ۷۴۵ ق.م.ا) در زمره جرائم علیه شخصیت معنوی اشخاص قرار دارند. (الهی منش،سدره نشین، ۱۰۲:۱۳۹۱)

جرم احصا شده در ماده ۱۶ (م ۷۴۴ ق.م.ا) عبارت است از «هتک حیثیت از طریق تحریف نگاری هویت و هرزه‌نگاری شخصیت» که به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی و در بستر فضای سایبر ارتکاب می‌یابد. (همان، ۱۰۲:۱۳۹۱)

به نظر می‌رسد هتک حیثیت (حرمت) در این ماده، ناظر به قذف، توهین و یا افترا نیست و اگر تغییر یا تحریف، متضمن نوعی قذف، توهین یا افترا باشد، بر اساس قانون مجازات اسلامی قابل مجازات می‌باشد. به عبارت بهتر، در این ماده، واژه هتک حیثیت بیشتر متکی بر مفهومی عرفی از آبروریزی، کسر شأن و اعتبار و شکستن حرمت دیگران است. (همان، ۱۰۲:۱۳۹۱)

عمل مادی جرم، می‌تواند ارتکاب حداقل یکی از اعمال زیر باشد: (محمد نسل، ۱۳۹۲: ۱۳۶)

- تغییر و انتشار؛
- تحریف و انتشار؛
- انتشار محصولات تغییر یا تحریف‌شده توسط دیگران.

لازم است که فیلم یا تصویر یا صوت منتشرشده در فضای مجازی، جعلی باشد. بنابراین چنانچه کسی فیلم یا تصویر یا عکس غیر جعلی از کسی را منتشر کند بر اساس ماده ۱۶ قابل مجازات نخواهد بود و باید به دنبال بررسی تطبیق عمل مرتکب با عناوین مجرمانه دیگری مانند حفظ اسرار و مسائل خصوصی (موضوع ماده ۱۷ قانون جرائم رایانه‌ای) باشیم. (همان، ۱۳۹۲: ۱۳۶)

نشر اکاذیب

این جرم از یک نظر می‌توان جزو جرائم علیه امنیت داخلی کشور یا جرائم علیه آسایش عمومی محسوب کرد، زیرا در آن مطالبی بی‌اساس با علم به‌دروغ بودن آنها، بین مردم پخش می‌شود و بدین‌وسیله، امنیت و آسایش عمومی مختل می‌گردد. (الهی منش،سدره نشین، ۱۱۱:۱۳۹۱)

امروزه محیط‌های سایبری اعم از رایانه‌ای یا مخابراتی، بسترهای ذاتی و مناسبی برای نشر اکاذیب فراهم آورده‌اند. (همان، ۱۱۲:۱۳۹۱)

«این ماده با برخی تغییرات اندک، تکرار ماده ۶۹۸ قانون مجازات اسلامی می‌باشد و به دو دلیل عمده زیر با برخی تغییرات در فضای سایبرآورده شده است:

الف) وسیله ارتکاب جرم در ماده ۶۹۸ ق.م.ا حصری است و سامانه رایانه‌ای و مخابراتی را شامل نمی‌شود و حتی حقوق‌دانان با اختلاف آرا، تلویزیون و رادیو را با توجه به تفسیر منطقی به‌سختی در قلمروی این ماده وارد می‌کنند. همچنین، ضرورت داشت که تکلیف نشر اکاذیب در فضای سایبر نیز مشخص شود.

ب) نشر اکاذیب، جرمی است که در فضای سایبر بسیار متداول می‌باشد و در این مورد، وسیله ارتکاب جرم، بسیار مناسب تر و راحت تر در خدمت تحقق فعل فیزیکی جرم است. (همان، ۱۱۲:۱۳۹۱)

با توجه به متن این ماده، می‌توان موضوع جرم نشر اکاذیب را اخبار دروغ وقایع خلاف واقع دانست که مرتکب جرم، آنها را به‌وسیله سامانه رایانه‌ای یا مخابراتی منتشر نموده یا در دسترس دیگران قرار داده و یا آنها را به طور صریح یا تلویحی (ضمنی) به شخص حقیقی یا حقوقی نسبت می‌دهد. (همان، ۱۱۳:۱۳۹۱)

عمل مادی جرم، می‌تواند به یکی از سه صورت زیر بروز پیدا کند: (محمد نسل، ۱۳۹۲: ۱۴۶)

- انتشار؛
- در دسترس قرار دادن؛
- نسبت دادن.

لازم است که مطالب منتشرشده یا قرار داده‌شده در دسترس دیگران یا اعمال نسبت داده‌شده به دیگران، کذب باشد. بنابراین چنانچه مطالب مذکور کذب نبوده و صحت آنها ثابت شود، مرتکب بر اساس ماده ۱۸ قابل تعقیب و مجازات نخواهد بود مگر اینکه عمل وی مشمول عنوان افشای اسرای خصوصی باشد که در آن صورت بر اساس ماده ۱۷ قانون جرائم رایانه‌ای مجازات خواهد شد. (همان، ۱۳۹۲: ۱۴۶)

برای تحقق این جرم لازم است که اعمال اجرایی جرم با استفاده از سامانه‌های رایانه‌ای یا مخابراتی صورت گرفته باشد. (همان، ۱۳۹۲: ۱۴۶)

آماج جرم می‌توانند اشخاص حقیقی یا حقوقی باشند. (همان، ۱۳۹۲: ۱۴۶)

برای تحقق این جرم لازم نیست که ضرر مادی یا معنوی به بزه دیده واقع شده باشد بلکه صرف ارتکاب عمل توسط مرتکب یا مرتکبین کفایت می‌کند و در این خصوص شاکی خصوصی نیاز به ارائه مدرک برای اثبات ورود ضرر مادی یا معنوی به خود ندارد. (همان، ۱۳۹۲: ۱۴۶)

به نظر می‌رسد که ناشر و یا ارائه‌کننده اکاذیب یا نسبت دهند اعمال خلاف واقع لازم نیست که شخصاً آنها را تولید هم کرده باشد بلکه اقدام به نشر یا ارائه با علم به کذب بودن مطالب برای تحقق جرم کفایت

می‌کند. این امر به خوبی از عبارت قانون‌گذار (رأساً یا به‌عنوان نقل‌قول) قابل‌برگشت است. (همان، ۱۳۹۲: ۱۴۷)

نتیجه‌گیری و پیشنهادهای تحقیق

در قانون جرائم رایانه‌ای مصوب ۱۳۸۸/۳/۵ هیچ‌گونه تعریفی از جرائم رایانه‌ای صورت نگرفته و فقط جرائم و مجازاتها در این قانون ذکرشده است. با توجه به اهمیتی که مشخص بودن تعریف دقیق از جرائم رایانه‌ای دارد فقدان این تعریف می‌تواند یکی از نواقص و خلاءهای قانونی جرائم رایانه‌ای باشد. لذا پیشنهاد می‌گردد با توجه به گسترش فن آوری اطلاعات و دسترسی زیاد افراد به این فن آوری و همچنین تنوع جرائم و آسیب هایی که افراد جامعه ممکن است در صورت بروز چنین جرائمی متحمل شوند، تعریف موسعی از جرائم رایانه‌ای صورت گیرد که تا هر گونه فعل و یا ترک فعل که سبب بروز ضرر و زیان مادی و معنوی به افراد در بستر فن آوری اطلاعات و از طریق رایانه صورت گیرد را به‌عنوان جرم رایانه‌ای در نظر گرفته و جرم انگاری نمود.

در ماده۱ قانون جرائم رایانه‌ای، جرم دسترسی غیرمجاز در صورتی تحقق می یابد که، دسترسی غیرمجاز به سامانه‌های امن صورت گیرد و همچنین برای حصول این جرم می بایست، نقض تدابیر ایمنی ایجاد شود و در عوض، سامانه‌های غیر ایمن و نیز دسترسی بدون نقض تدابیر ایمنی، از شمول این ماده خارج هستند که این یک خلاء قانونی جدی محسوب می‌شود. از طرف دیگر، تا کنون ملاک و معیار مشخصی برای تعیین ایمنی(امنیت) و یا ناامنی برای یک سامانه یا شبکه رایانه‌ای یا مخابراتی ارائه نشده و معمولاً این‌گونه موارد، سلیقه‌ای است؛ به‌طوری که از نگاه عده‌ای با نصب یک نرم‌افزار امنیتی و یا دیوار آتشین سامانه یا شبکه‌ایمن محسوب می‌شود اما از نظر برخی دیگر از متخصصان حرفه‌ای، چنین سامانه‌هایی از امنیت مطلوب برخوردار نیستند و لازم است تجهیزات نرم‌افزاری و سخت‌افزاری خاصی بر روی آنها نصب گردد.

میزان مجازات ها باید به نسبت حساسیت داده‌ها و اطلاعاتی که مورد دسترسی غیرمجاز قرار می گرفت، تعیین می گردید. می دانیم که داده‌ها و اطلاعات می‌توانند از عادی تا فوق سری باشند؛ لذا باید به همین میزان و با رعایت تناسب، مجازات ها مورد تشدید و یا تخفیف قرار می گرفت.

شروع به جرائم دسترسی غیرمجاز، شنود غیرمجاز، جعل رایانه‌ای، استفاده از داده‌ها، کارتها یا تراشه‌های مجعول، حذف، تخریب، یا اخلال در داده‌ها، ربایش داده‌های متعلق به دیگری، هرزه‌نگاری (پورنوگرافی)، معاونت در هرزه‌نگاری، هتک حیثیت از طریق تحریف نگاری هویت، انتشار یا در دسترس قرار دادن محتویات خصوصی یا اسرار دیگری؛ در قانون جرم انگاری نشده است و این موضوع در هاله از ابهام قرار دارد. برای قابل

مجازات دانستن شروع به جرم باید قصد ارتکاب وجود داشته باشد؛ به گونه ای که با برداشتن گام های اساسی به حصول نتیجه مجرمانه نزدیک شده باشد. از دیدگاه دانش مهندسی نرم‌افزار رایانه و اصول بنیادین حقوق کیفری، امکان تحقق شروع به جرم در جرائم ذکرشده وجود دارد. با توجه به اینکه، شروع به جرم باید در قانون تصریح شده باشد؛ لذا در حال حاضر، شروع به جرم جرائم فوق، واجد عنوان مجرمانه نیست که این یکی از نقاط ضعف قانون به شمار می رود.

جرم جاسوسی رایانه‌ای موضوع این ماده در زمره جرائم عمدی می‌باشد و مرتکب یا مرتکبان باید جرم را آگاهانه انجام داده سوءنیت (عالماً و عامداً) ارتکاب فعل یا افعال مجرمانه ذکرشده در ماده قانونی مربوطه که در واقع سوءنیت عام این‌گونه جرائم می‌باشد و نیز قصد حصول نتیجه مجرمانه ذکرشده در بندهای سه‌گانه یا سوءنیت خاص را دارا باشند یا بتوان آنان را مورد تعقیب کیفری قرار داده و شایسته مجازات دانست. اما تنها در بند «الف» است که حصول نتیجه مجرمانه خاصی برای تحقق این جرائم شرط نشده است (یعنی نیازی به وجود سوءنیت خاص ندارد) که این امر ممکن است موجب تضییع حقوق افرادی شود که ناخواسته به محتوای مورد تصریح در قانون دست یافته‌اند.

مقنن در ماده ۵ عبارتی آورده است که قدری ابهام‌زاست. قانون‌گذار به دو دسته از مأموران دولتی اشاره‌کرده است. دسته نخست مأمورانی هستند که مأمور حفاظت از داده‌ها و سامانه‌های سری هستند(مانند مسئولان شبکه‌ها و بایگان‌ها) و دسته دوم کسانی هستند که داده‌ها و سامانه‌ها در اختیار آنها قرارگرفته است (مانند کاربران مجاز و پیک‌ها و اقدام کننده‌ها) طرز انشای ماده ۵ به نوعی است که در مورد اینکه آیا این قبیل مأموران نیز باید قبلاً آموزش های لازم را دیده باشند یا خیر، ساکت است. به نظر نگارند با توجه به وحدت مناط موجود در این دو دسته، لزوم طی آموزش حفاظتی قبل از ارتکاب سهل‌انگاری منجر به تعقیب کیفری، در مورد آنان نیز ضرورت دارد هر چند که قانون‌گذار صراحتاً متعرض آن نشده است داده‌ها و سامانه‌های موضوع سهل‌انگاری باید از نوع سری باشند. البته اینکه چرا قانون‌گذار فقط به داده‌های سری اشاره‌کرده و داده‌های محرمانه و خیلی محرمانه و حتی به‌کلی سری را ذکر نکرده است، جای بحث و تأمل دارد. البته در مورد داده‌های به‌کلی سری ممکن است چنین استدلال شود که جایی که سهل‌انگاری در حفاظت از داده‌های سری جرم شناخته شده به نحو اولی سهل‌انگاری در حفاظت از داده به‌کلی سری نیز باید جرم باشد اما در مورد داده‌های محرمانه و خیلی محرمانه چه باید گفت؟ آیا سهل‌انگاری در حفاظت از آنها فاقد وصف مجرمانه است؟ به نظر می‌رسد که این امر مور غفلت واقع شده است و گر نه سیاست جنایی کشورمان همواره مصمم به جرم انگاری سهل‌انگاری در نگهداری هر گونه اسناد طبقه بندی شده بوده است و غیرمعقول به نظر می‌رسد که از جرم انگاری سهل‌انگاری در حفاظت از این دسته از داده‌ها در فضای مجازی صرف‌نظر کرده باشد.

با توجه به حرکت جامعه ایران به سمت تحقق «شهر الکترونیک» و تاکید برنامه پنجم توسعه و سند چشم‌انداز بیست‌ساله کشور بر این امر در آینده‌ای نه چندان دور، اکثریت قریب به‌اتفاق اسناد دولتی و غیردولتی، رسمی و غیررسمی که به‌صورت کاغذی می‌باشند، جای خود را به اسناد الکترونیکی (دیجیتالی) خواهند داد. در این فرآیند در بستر فضای سایبر و سامانه‌های رایانه‌ای و مخابراتی طیف گسترده‌ای از اسناد با ارزش‌های متفاوتی تولید و پردازش می‌شوند که حمایت‌های قانونی(حقوقی و کیفری) خاص خود را می‌طلبد. به نظر می‌رسد که قانون‌گذار با تصویب ماده ۶ قانون جرائم رایانه‌ای (م ۷۳۴ ق.م.ا) اسناد الکترونیکی (دیجیتالی را به رسمیت شناخته، لذا ضروری است که مفهوم سند در قانون مدنی اصلاح شود تا این اسناد نیز اثر قانونی برابر با اسناد دیگر (مرسوم) را دارا گردند.

قانون در مواردی که شخص یا اشخاصی بدون علم و اطلاع به مجعول بودن داده‌ها، کارت‌ها یا تراشه‌ها از آنها استفاده نمایند و باعث ایجاد خسارت مالی و ... گردند، تکلیفی را مشخص ننموده و ساکت است.

موضوع جرم منحصر به استفاده از داده‌ها یا کارت‌ها یا تراشه‌های حاوی داده‌های جعلی است. به نظر نگارنده بهتر بود مقنن به‌جای نام بردن کارت و تراشه از عبارت ابزارهای حامل یا پردازشگر داده استفاده می‌کرد تا در صورت اختراع ابزار و تجهیزات جدید در آینده، آنها را نیز شامل شود.

در برخی شرایط، افرادی برای کسب منافع به نفع خود یا دیگری ممانعت از اجرای عدالت و یا اضرار به دیگری، اقدام به حذف، تخریب، مختل و غیرقابل پردازش کردن داده‌های متعلق به خود در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده‌ها می‌نمایند که در ماده ۸ ق.ج.ر به این امر اشاره‌ای نشده است.

بهتر بود قانون‌گذار در تبصره‌ای، سرقت داده‌های دولتی (یا حاکمیتی) و یا سرقت داده‌های سامانه‌هایی که برای ارائه‌ی خدمات ضروری عمومی به‌کار می روند و یا سرقت‌هایی را که به‌قصد به خطر انداختن امنیت و آسایش عمومی انجام می‌پذیرد، به‌عنوان عامل تشدید مجازات معرفی می‌نمود تا جنبه بازدارندگی کیفری ماده ۱۲ق.ج.ر افزون گردد.

از مفهوم معکوس در ابتدای ماده ۱۲ ق.ج.ر این‌گونه استنباط می‌شود که هرکس به طور مجاز داده‌های متعلق به دیگری را برباید، مرتکب جرمی نشده است. اما این مفهوم صحیح نیست زیرا ربودن (سرقت) مجاز در عالم واقع مصداق خارجی ندارد لذا به نظر می‌رسد ذکر عبارت «غیرمجاز» در صدر ماده اضافی بوده و بهتر است قانون‌گذار در اصلاحات بعدی آن را حذف نماید.

به نظر می‌رسد اگر قانون‌گذار در متن این ماده به «برنامه‌های رایانه‌ای» متعلق به دیگری و نیز عبارت «به هر طریق» اشاره می‌نمود؛ از طرفی به ماده مذکور جامعیت بیشتری می‌بخشید و از طرف دیگر، راه را بر هر گونه سوءتعبیر از مفهوم داده‌ها می‌بست. یعنی متن ماده ۱۲ ق.ج.ر را بدین‌صورت بیان می‌کرد. «هرکس

به هر طریقی داده‌ها یا برنامه‌های متعلق به دیگری را برباید ... » امید است در اصلاحات آتی قانون این امر مورد عنایت قانون‌گذار قرار گیرد.

با توجه به جنبه بین‌المللی کلاه‌برداری رایانه‌ای، بهتر بود قانون‌گذار در جرم انگاری آن از تجربیات دیگر کشورها و سازمان های بین‌المللی استفاده می‌کرد. مسئله‌ای که در رابطه با میزان مجازات مقررشده در ماده۱۳ ق.ج.ر به چشم می‌خورد این است که قانون تشدید، مجازات کلاه‌برداری ساده را حبس از ۱ تا ۷ سال و پرداخت جزای نقدی معادل مال اخذشده توسط کلاه بردار و مجازات کلاه‌برداری مجدد را حبس از ۱ تا ۱۰ سال و کلاه‌برداری با تشکیل یا رهبری شبکه چند نفری را حبس از ۱۵ سال تا ابد و پرداخت مالی که کلاه بردار به‌دست آورده و نیز انفصال ابد از خدمات دولتی تعیین کرده است، اما در ماده ۱۳ قانون جرائم رایانه‌ای میزان مجازات، علاوه بر رد مال به صاحب آن، حبس از ۱ تا ۵ سال یا جزای نقدی از بیست میلیون تا یک صد میلیون ریال ذکرشده است حال آنکه با توجه به گسترده بودن مخاطبان جرائم رایانه‌ای در سراسر جهان و امکانات این شبکه که ضمن مخفی ماندن هویت مرتکبان و بدون هیچ گون رد پای فیزیکی وسعت ضرر و زیان وارده و تعداد مال‌باختگان و بزه دیدگان بسیار بیشتر از کلاه‌برداری رایانه‌ای سنتی یا کلاه‌برداری سنتی صرف است این میزان مجازات با اصول قانون منصفانه سازگار نیست.

یکی از نقاط ضعف ماده ۱۴ق.ج.ر این است که هیچ رویکرد افتراقی از رهگذر کیفر گذاری تشدیدی در مقایسه با بزرگ‌سالان به دلیل کودکی بزه دیده اتخاذ نکرده است. همچنین برخلاف بند «ج» ماده۲ پروتکل الحاقی به کنوانسیون حقوق کودک راجع به فروش، فحشا و هرزه‌نگاری کودکان، فعالیت‌های آشکار جنسی باهر وسیله، مشمول تعریف محتویات مستهجن قرار نگرفته و فقط به عمل جنسی انسان اشاره‌شده است.

اقدام قانون‌گذار در جرم انگاری هتک حیثیت از طریق تحریف نگاری هویت یا هرزه‌نگاری شخصیت، قابل‌تحسین می‌باشد؛ اما بهتر بود مواردی را که تحریف نگاری هویت نسبت به مقام رهبری، رؤسای قوای سه‌گانه، مراجع تقلید و... به اعتبار مقام آنها صورت می‌گیرد را از جمله کیفیات مشدد مجازات در نظر می‌گرفت.

منابع:

۱. آیکاو، دیوید جی، و همکاران(۱۳۸۳)، ترجمه اکبراسترکی و همکاران، راه‌کارهای پیش‌گیری و مقابله با جرائم رایانه‌ای ، تهران: دانشگاه علوم انتظامی،.

۲. آقا بابایی، اسماعیل(۱۳۸۹)، مسائل فقهی حقوقی شرکت های هرمی، انتشارت پژوهشگاه علوم و فرهنگ اسلامی،

۳. اردبیلی، محمدعلی(۱۳۷۹)، حقوق جزای عمومی، چاپ اول، تهران: نشر میزان.

۴. اصغری، جمشید و سادات فقیه، صدیق (۱۳۸۷). بررسی علمی حقوقی بازاریابی شبکه‌ای،تهران: انتشارت مجد،

۵. الهی منش، محمدرضا و سدره نشین ابوالفضل(۱۳۹۱)، محشای قانون جرائم رایانه‌ای، انتشارات مجد، سال

۶. انصاری، مرتضی(۱۳۷۶)، «جرم رایانه‌ای و حقوق اطلاعاتی کیفری» ترجمه محمد دزیانی، شورای عالی انفورماتیک.

۷. بای، حسینعلی و پور قهرمانی(۱۳۸۸)، بابک، بررسی فقهی حقوقی جرائم رایانه‌ای،چاپ اول، پژوهشگاه علوم و فرهنگ اسلامی.

۸.بابا زاده، قاسم(۱۳۹۱)، «پیرامون کنوانسیون اروپایی جرائم رایانه‌ای»، خبرنامه انفورماتیک، شماره ۸۱ .

۹. باستانی، برومند(۱۳۸۳)، جرائم رایانه‌ای و اینترنتی جلوه‌ای نوین از بزه کاری، چاپ اول، انتشارات بهنامی،

۱۰. پاکزاد، بتول(۱۳۷۵)، جرائم رایانه‌ای(پایان‌نامه کارشناسی ارشد)، دانشگاه شهید بهشتی،

۱۱. پاکزاد، بتول (۱۳۷۵)«اقدامات سازمان های بین‌المللی و منطقه ای در خصوص جرائم رایانه‌ای»،

۱۲. پرویزی، رضا(۱۳۸۵)، «جرائم رایانه‌ای تهدیدی علیه فن آوری اطلاعات»، مجله عصر ارتباطات، شماره۱۶.

۱۳. نور بها، رضا(۱۳۹۱)، زمینه حقوق جزای عمومی، انشارات گنج دانش،چاپ۳۳،.

۱۴. محمد نسل، غلامرضا(۱۳۹۲)، حقوق جزای اختصاصی جرائم رایانه‌ای در ایران، نشر میزان، سال.

۱.Christion Schwarzengger, computer crimeicy Brspaced, ۲۰۰۲

۲.computer related crime, prefaced by:auguat be quaic puliched by:council op Europe stras Strasbourg.۱۹۹۰

۳. Intrenational Revew of Criminal Policy, nos ۴۳ and ۴۴

۴.Jari raman, Computer crime,۲۰۰۱.

۵. Richad W.Aldrich, Cyberterrorism and computer crimes,۲۰۰۰

The Survey gaps and ambiguities in the law of computer crime Islamic Republic of Iran

ABSTRACT

Progress of science and the rapid growth of information technology and communications (ICT), especially the Internet, has created the new challenges in life. Internet creates a virtual space in people's lives. Therefore, in addition to all the advantages and benefits that create risks have been followed

Including the occurrence of crime in a community wide level cited

Crime against property, and personal safety and general welfare as they occur in the real world to the virtual world is larger and more complex shapes can be realized.

However, there is a legal vacuum in Computer Crime, punishment disproportionate to the crime defined in the law of cyber space, cyberspace has become unsafe due to the loss of some a number of people have been hurt. So effectively identify and address the legal gaps in the current state of the Internet and creating an effective step would be criminal justice.

Keywords: Computer crimes, cyber spaces, information technology and communications, regulatory gaps and ambiguities