مجله علمی پژوهش در حقوق، فقه، فلسفه و الهیات (سال دوم)
شماره۵/ پاییز ۱۳۹۵ / ص۴۹-۳۶

بررسی حقوقی جعل رایانه ای در حقوق کیفری ایران

علیرضا شایق [۱]

[۱] کارشناس ارشد حقوق جزا و جرم شناسی

نام و نشانی ایمیل نویسنده مسئول:
علیرضا شایق

چکیده

در نظام قانونگذاری کیفری ایران یکی از شایع ترین بزه ها، جعل می باشد که با توجه به رشد سریع تکنولوژی رایانه ای و تحول عصر ارتباطات و گسترش ارتباطات شبکه ای و در عین حال سهولت ارتکاب جرایم مرتبط با فناوری های نوین، از شکل سنتی به شکل رایانه ای نیز روی آورده است. اگر چه در جعل سنتی ممکن است با استفاده از رایانه موجبات تحقق این بزه فراهم شود، اما در جعل رایانه ای در واقع جعل داده های رایانه ای و ورود در فضای مجازی اتفاق می افتد. تفاوت عمده ای که بین این دو بزه به ویژه در بحث عنصر مادی آنها و ویژگی های خاص جرایم رایانه ای وجود دارد، ضرورت جرم انگاری جعل رایانه ای را ایجاب نموده است. لذا بدلیل جدید بودن این موضوع لازم بود این جرم مورد واکاوی قرار گیرد که در این پایان نامه با تحلیل و بررسی عناصر متشکله به اهمیت جرم انگاری آن در حقوق ایران پی خواهیم برد که برای پیشگیری از این جرم که جرمی علیه آسایش و امنیت می باشد راهکارهایی در زمینه پیشگیری غیرکیفری که شامل پیشگیری اجتماعی و وضعی می باشد ارائه شده است که امید است با توجه به پیشنهادات مطروحه و محدودیت های اشاره شده، موجبات تقلیل این جرم در جامعه فراهم شده باشد.

واژگان کلیدی: جعل رایانه ای، جرایم رایانه ای، فضای سایبر

مقدمه

یکی از اختراعات بی‌نظیر بشری که زندگی او را در تمامی شئون فردی و اجتماعی با تحولات گسترده‌ای مواجه کرده است، فناوری اطلاعات و رایانه می‌باشد . اصولاً هر پدیده اجتماعی به دلیل فرایند تأثیر و تأثر در جامعه تابع یک سری قوانین و مقررات حقوقی است. رایانه به عنوان یکی از اجزای لاینفک اجتماعی در عصر حاضر از این اصل پیروی می کند. لذا به لحاظ این امر که تعیین عناوین مجرمانه در حیطه مسئولین قانونگذاری می باشد، تخطی کاربران آن در رعایت قوانین منجر به ظهور جرم می گردد. چرا که رایانه از یکسو می تواند ابزار وقوع جرم واقع شود و از سوی دیگر نقش محیط اعمال جرم را ایفا می کند. به دلیل گستردگی حضور رایانه در بسیاری از ابعاد زندگی فردی و اجتماعی، جرائم آن نیز در حوزه های مختلف حقوقی مطرح می گردد. از جمله: حقوق تجارت، حقوق مالکیت، حقوق بین الملل، حقوق فناوری و تکنولوژی ارتباطات.

تفاوت های اساسی بین جرائم رایانه ای رایج در کشورهای در حال توسعه و کشورهای توسعه یافته ناشی از روش استفاده از این ابزار است. در کشورهای توسعه یافته، رایانه از یک وسیله برای سرعت در انجام کار پا را فراتر نهاده و تبدیل به یک دریچه شده است. دریچه ای برای ورود به فضای بی انتها که علاوه بر امور تخصصی، حتی بسیاری از کارهای شخصی مهم در آن فضا صورت می گیرد، بنابراین بعد محیطی رایانه در بروز جرائم در این کشورها بیشتر است. کافی است به آمار جرائم اینترنتی مراجعه کنید تا متوجه بشوید که بیشترین درصد این جرائم در کشورهای توسعه یافته رخ می دهد.

در مقابل در کشورهای در حال توسعه از جمله ایران، بعد ابزاری رایانه در بروز جرائم نمود بیشتری پیدا می کند، مثلاً تکثیر سی دی های غیرمجاز و یا شکستن قفل نرم افزارها و تکثیر آن ها بدون کسب اجازه اولیه از پدیدآورندگان آن نرم افزار. از جمله جرائم مهمی که در پی توسعه و پیشرفت روز افزون روابط اجتماعی، اقتصادی و فرهنگی و ... به وجود آمد و روز به روز پیچیدگی، ظرافت و اهمیت آن بیشتر می شود جعل و در پی آن استفاده از اسناد و نوشتجات مجعول و مزور می باشد که از جرائم مهم و مخل امنیت و آسایش عمومی به شمار می رود. با فراگیر شدن استفاده از رایانه و نرم افزارهای رایانه ای در عرصه مختلف زندگی، حافظه رایانه ها و نرم افزارها جایگزین سند و نوشته سنتی می شود و در سطح گسترده ای برای بیان و اعلام اراده از رایانه استفاده خواهد شد.

بدنبال تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲ و قانون تجارت الکترونیکی مصوب 1382 و قانون جرائم رایانه ای در تاریخ 1388 و جرم انگاری جعل رایانه ای در قوانین مزبور به موجب ماده ۱۳۱ قانون نیروهای مسلح و ماده ۶۸ قانون تجارت الکترونیکی و ماده۶و۷ قانون جرائم رایانه ای به نظر می رسد عنوان جزایی نوظهوری پا به عرصه نظام حقوقی ایران گذاشته است که نیازمند تحلیل و بررسی می باشد.

۱. رکن قانونی جعل رایانه ای

در خصوص بزه جعل رایانه ای نخست باید به این نکته اشاره شود که به دلیل اصل لزوم تفسیر مضیق قوانین کیفری نمی توان با استناد به مواد عام راجع به جعل سنتی ذکر گردیده در قانون مجازات اسلامی، داده ها و اسناد رایانه ای را موضوع این جرم بر شمرد و مرتکب جعل رایانه ای را به مجازات های مذکور در این مواد محکوم کرد. علی ایحال ناگزیر به مراجعه به قوانین جزایی کیفری راجع به جعل رایانه ای در حقوق جزای ایران می باشیم. به لحاظ نوظهور بودن بزه جعل رایانه ای ما فقط با سه قانون کیفری مواجه می باشیم که فی الواقع رکن قانونی بزه جعل رایانه ای را تشکیل می دهد و قانونگذار ایران با جرم انگاری این عنوان جزایی در سه قانون کیفری مبادرت به تعیین ضمانت اجرای کیفری نموده است که صرفاً به بیان مواد قانونی مربوط به جعل رایانه ای در این فصل بسنده می کنیم.

۱. ماده ۶ قانون جرائم رایانه ای مصوب ۸۸/۳/۵ مجلس شورای اسلامی

۲. ماده ۶۸ قانون تجارت الکترونیکی[1] مصوب ۸۲/۱۰/۱۷ که نخستین قانون در ایران در زمینه جرم های مربوط به فناوری اطلاعات و شاخه های خاص آن یعنی جرم های مربوط به تجارت الکترونیکی است

۳. ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح مصوب ۸۲/۱۰/۹ مجلس شورای اسلامی

[1] – روزنامه رسمی، شماره ۱۷۱۶۷، مورخه ۱۳۸۲/۱۱/۱۱

ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح برای اولین بار در ایران « داده های رایانه ای» را به عنوان موضوع جعل مطرح نموده و جعل رایانه ای را جرم انگاری کرد.

۲.رکن مادی

در بحث از عنصر مادی به ترتیب مطالبی را پیرامون رفتار مجرمانه، عمل و صور فعل مرتکب، و تأثیر وسیله و نتیجه در وقوع جرم جعل در هر کدام از سه قانون مربوط به جعل رایانه ای در حقوق جزایی ایران (ماده ۶ قانون جرائم رایانه ای، ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح و ماده ۶۸ قانون تجارت الکترونیکی) بیان می نماییم، به تعبیر دیگر عنصر مادی هر جرمی متشکل می شود از عمل فیزیکی، شرایط و اوضاع و احوال و نتیجه به دست آمده که البته می باید بین عمل فیزیکی و نتیجه به دست آمده ی آن جرم رابطه علیت موجود باشد. در بحث عنصر مادی باید گفت که می توان استنباط نمود که جعل رایانه ای همانند جعل سنتی به دو گونه ارتکاب می یابد: ۱- جعل مادی ۲- جعل معنوی

جعل مادی عبارتست از: تغییر، وارد کردن، محو کردن و متوقف کردن داده هاست که دارای آثار خارجی محسوس و مشهود است به گونه ای که با چشم یا با وسایل دقیق تر آثار خارجی آن قابل تشخیص باشد. جعل معنوی رایانه ای هم بدین ترتیب است که داده ها به صورت چاپ شده ارائه نشود، بلکه به طور مستقیم مثلاً در حین پردازش صورت گیرد.« این نکته در مورد بانک و معاملاتی را که فرایند آن تنها در کامپیوتر صورت می گیرد و نمود خارجی ندارد قابل مشاهده است» (خداقلی، ۱۳۸۳) بیشترین مصادیق این نوع جعل در حقوق سنتی در ماده ۵۳۴ قانون تعزیرات و مجازاتهای بازدارنده ۱۳۷۵ بیان شده است. اگرچه قانونگذار در مقرره های قانونی راجع به جعل رایانه ای در خصوص جعل معنوی هیچگونه اشاره ای ننموده است ولی با استنباط از مواد قانونی راجع به جعل سنتی می توان گفت که ارتکاب جعل معنوی رایانه ای به پنج روش امکان پذیر است:۱- تغییر موضوع یا داده پیام۲- تحریف داده پیام مربوط به یکی از مقامات رسمی ۳- تحریف داده پیام مرتبط به یکی از طرفین ۴- صحیح جلوه دادن امر باطل و یا باطل جلوه دادن امر صحیح ۵- اقرار جلوه دادن چیزی که بدان اقرار نشده است و یا بالعکس.

از آنجا که رکن مادی در جعل مادی و جعل معنوی به صورت واحد می باشد و فی الواقع قانونگذار در جعل رایانه ای آنگونه که در جعل کلاسیک بیان شده است دست به تفکیک این دو نوع جعل نزده است و به صورت واحد آن را بیان کرده است ما هم به همین میزان که توضیح دادیم بسنده می کنیم و به صورت کلی عناصر متشکله رکن مادی جعل رایانه ای را بررسی می نماییم.

۱-۲ نحوه و شرایط رفتار مرتکب

در این گفتار طی عناوین جداگانه رفتار مرتکب را در قوانین داخلی و همچنین کنوانسیون جرائم سایبر در مورد جعل رایانه ای بیان می داریم و طی عنوان دیگری شرایط رفتاری مجرمانه جعل رایانه ای را بیان می داریم.

الف : رفتار مرتکب در ماده ۶ قانون جرایم رایانه ای

جرم جعل رایانه ای موضوع ماده ۶ قانون جرائم رایانه ای از فعل مثبت مرتکب تشکیل شده است و این جرم با ترک فعل تحقق پیدا نمی کند. رفتار مرتکب برای این جرم بر مبنای ماده ۶ قانون جرائم رایانه ای عبارتست از: تغییر، ایجاد و وارد کردن متقلبانه داده و تغییر علائم موجود در کارت های حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها: پس این افعال که حصری هستند عبارتند از: ۱- ایجاد کردن ۲- تغییر دادن ۳- وارد کردن که در مورد هر کدام از آنها توضیحاتی را ارائه می نماییم.

۱- ایجاد کردن داده

منظور از آن ایجاد یک داده جدید می باشد که هیچ یک از اجزاء آن از قبل وجود نداشته است. ایجاد یا ساختن یک داده ی جدید فقط از طریق وارد کردن داده ها امکان پذیر است.از طریق تغییر دادن یا حذف یا متوقف کردن داده ها نمی توان داده ای ایجاد کرد که از قبل هیچ یک از اجزاء آن وجود نداشته است. اگر یک کاربر رایانه ای که مشمول خدمت سربازی است، وارد سیستم های رایانه ای اداره نظام وظیفه شود و یک سند الکترونیکی ایجاد کند که منجر به معافیت او از خدمت سربازی شود عمل وی مصداق ایجاد یک داده غیر صحیح جدید از طریق وارد کردن عمدی و بدون حق داده هاست.

مثال دیگری که در خصوص ایجاد کردن داده می توان زد موردی است که با ورود به سیستم رایانه ای یک دانشگاه بزرگ و ایجاد یک پرونده تحصیلی که به صدور مدرک تحصیلی در آن دانشگاه برای فرد منجر شود، روبرو هستیم.

2- تغییر دادن داده ها یا علائم موجود در کارت های حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها

تغییر در داده ها یا علائم فوق الذکر مشتمل به انجام اقداماتی به منظور دگرگون سازی داده ها و علائم مذکور و روند پردازش آنها است. به گونه ای که در نتیجه اقدامات انجام شده، داده پیامی متفاوت از داده پیام اصل و حقیقی ایجاد شود که البته قابل بهره برداری به عنوان داده پیام معتبر باشد.به عبارت دیگر ایجاد تغییر و دگرگونی در ماهیت یا مفاد و شرایط داده پیام باید به گونه ای باشد که داده پیام را از حیّز انتفاع ساقط نکرده و نتیجه عمل، ایجاد داده پیامی قابل مقایسه با داده پیام معتبر بوده و قابل استفاده در مراجع مختلف باشد. «عنصر اصلی جعل، قلب حقیقت است و آن دگرگون کردن و تغییر دادن حقیقت یک امر است.» (ساریخانی، ۱۳۸۴- ۲۱۶) مثل اینکه شخصی با ورود به سیستم رایانه ای بانکی، بدهی خود را که یکصد میلیون ریال است به یک میلیون ریال تغییر دهد و یا با ورود به رایانه شرکت مخابرات مکالمه تلفنی مصرفی خود را کم کند و بر اساس آن تغییر، قبض مصرفی صادر شود. بی شک در این موارد جعل تحقق یافته است. گاهی داده غیر صحیح با دستکاری داده های ذخیره شده ایجاد می شود که از رهگذر تغییر داده امکان پذیر است؛ مانند تغییر نمره یا حذف غیبت ناموجه یا اضافه کردن نظر موافق یکی از مسئولان دانشگاه یا ورود عمدی و غیر مجاز به سیستم رایانه ای آن.

۳- وارد کردن داده ها

منظور از وارد کردن اطلاعات ناصحیح و خلاف حقیقت به رایانه جهت پردازش است، اعم از اینکه با ورود اطلاعات و پردازش نهایی توسط رایانه، تحریف و جعل حقایق در داده پیام، محسوس و رؤیت پذیر باشد یا اینکه بدون هیچ تغییری در ظاهر داده پیام، مفاد و شرایط آن تحریف شده و امر باطلی، صحیح یا صحیحی، باطل جلوه داده شود. عمل مرتکب در هر دو صورت مشمول عنوان مجرمانه جعل خواهد بود.« برای مثال، عمل یک متصدی سیستم در افزودن نام یک کارگر واهی به فهرست پرداخت حقوق شرکت یا شماره حساب خود جهت دریافت مبلغ حقوق را می توان نمونه ای از این رفتار دانست»(مرکز مطالعات راهبردی توسعه قضایی و شورای عالی توسعه قضایی،۱۳۸۳- ۴۲) در مقایسه بین وارد کردن داده ها و ایجاد کردن داده ها باید خاطر نشان ساخت که منظور از ایجاد کردن داده به وجود آوردن و ساختن یک داده جدید می باشد که هیچ یک از اجزاء آن از قبل وجود نداشته است ولی از وارد کردن داده اجزاء آن از قبل وجود داشته است متنهی با وارد کردن داده جدید به اجزاء قبلی بزه جعل رایانه ای را محقق می بخشیم. به تعبیر دیگر همانگونه که در جعل سنتی بین ساختن سند و نوشته و الحاق و الصاق نوشته ای به نوشته دیگر تفکیک قائل می شدیم و ساختن سند مجعول را در یک مقوله و الحاق و الصاق نوشته ای به نوشته دیگر را در مقوله تغییر سند بررسی می کردیم. در جعل رایانه ای نیز بین ایجاد کردن داده ها و وارد کردن داده نیز تفاوت قائل هستیم و اگر بخواهیم هر دو را واحد بدانیم در واقع نقض غرض می باشد و دلیلی ندارد که قانونگذارهر دو فعل را در این ماده قانونی بگنجاند.

همانگونه که گفتیم قانونگذار رفتار مرتکب را در ماده ۶ قانون جرائم رایانه ای منحصر به ایجاد کردن، وارد کردن و تغییر دادن داده ها و علائم، منحصر کرده است و این در حالی است که در این ماده قانونی از موارد «حذف یا متوقف کردن» داده های رایانه ای که به نظر می رسد می بایست در زمره ی رفتار ارتکابی تلقی می گردیده، سکوت کرده است که این از جمله ایرادات وارده به قانونگذار در این ماده قانونی است که شاید بتوان در پاسخ چنین بگوییم که با تفسیر موسع از فعل تغییر و گنجاندن « حذف» یا «متوقف کردن» در فعل تغییر، بر این ایراد قانونگذار پوشش بگذاریم اما به نظر می رسد که تفسیر موسع در قوانین جزایی برخلاف اصول حقوق جزاء می باشد.

ب : رفتار مرتکب در ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح

جرم جعل رایانه ای موضوع ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح نیز از فعل مثبت مرتکب تشکیل شده و این جرم با ترک فعل تحقق پیدا نمی کند. آنچه که از ظاهر صدر ماده ۱۳۱ قانون مجازات مزبور – که ناظر بر بزه جعل رایانه ای می باشد- بر می آید، اینست که رفتار مرتکب بر مبنای این ماده قانونی عبارتست از: تغییر و حذف اطلاعات و الحاق یا تقدیم با

تأخیر تاریخ نسبت به تاریخ حقیقی به صورت غیر مجاز در سیستم رایانه ای و نرم افزارهای مربوطه می باشد. اما با مداقه در این ماده قانونی و ملاحظه ی عبارت« و نظایر آن» در می یابیم که رفتار مرتکب در این ماده قانونی به صورت تمثیلی می باشد و احصائی نمی باشد. به عبارت دیگر رفتار مرتکب در بزه جعل رایانه ای در قانون مجازات جرائم نیروهای مسلح منحصر به تغییر، حذف،الحاق، تقدیم و تأخیر تاریخ سند نسبت به تاریخ حقیقی نمی باشد و می تواند شامل ایجاد کردن، وارد کردن، متوقف کردن باشد که شرح آن گذشت.

در اینجا در مورد رفتارهای ارتکابی که در این قانون بدان تصریح گردیده است توضیحاتی را ارائه می نماییم:

۱- تغییر دادن اطلاعات

که منظور از آن دگرگون سازی اطلاعات در سیستم های رایانه ای به صورت غیر مجاز می باشد که قابلیت استفاده داشته باشد. از آنجا که در جعل رایانه ای در ماده ۶ قانون جرائم رایانه در بحث رفتار مرتکب به این موضوع پرداخته ایم به همین میزان بسنده می کنیم.

۲- حذف کردن اطلاعات

که در واقع همان محو کردن اطلاعات می باشد و « محو داده پیام عبارت از حذف دائمی اطلاعات است، به گونه ای که قابل بازسازی و بهره برداری مجدد نباشد.»(حسنوی، ۱۳۷۹- ۱۶۵) محو و حذف بخشی از داده پیام و پردازش مجدد آن، به تنهایی یا در کنار سایر داده پیام ها، باید منجر به ایجاد وضعیتی شود که در نتیجه آن ناحقی اثبات یا حقی تضییع گردد. در غیر این صورت، عمل مرتکب ممکن است با عناوین مجرمانه ی دیگری نظیر اتلاف سند، قابل انطباق باشد. از این رو در موردی که شخصی با محو بخشی از داده پیامی که برائت ذمه شخص ثالثی را گواهی می کند، داده پیام ظاهراً معتبری ایجاد می نماید و خود را مجدداً طلبکار نشان می دهد، مرتکب عمل جعل شده است.

۳- الحاق

در این مورد چیزی به داده پیام اضافه می گردد، مثلاً رقمی به عدد اضافه می گردد یا با افزودن حرف « ی» به واژه حسن، این واژه به حسین تبدیل می گردد. به زعم ما الحاق در واقع یکی از مصادیق وارد کردن داده ها می باشد که با الحاق اطلاعات در سیستم رایانه ای، تحریف و جعل حقایق در داده پیام، محسوس و قابل مشاهده می باشد.

۴- تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی

منظور از این بخش آن است که پس از ایجاد داده پیام، تاریخ مندرج در آن را جلو یا عقب بیندازد به نحوی که موجب قلب حقیقت گردد و با توجه به اینکه این موضوع در زمره مصادیق وارد کردن داده ها می باشد که قبلاً راجع به آن بحث نمودیم از ذکر آن خودداری می کنیم.

پ: رفتار مرتکب در ماده ۶۸ قانون تجارت الکترونیک

در جعل رایانه ای موضوع ماده ۶۸ قانون تجارت الکترونیکی نیز رفتار مرتکب با فعل مثبت محقق می شود و با ترک فعل، صورت نمی گیرد. رفتار مرتکب بر مبنای متن ماده مذکور عبارتست از: « ورود، تغییر، محو و توقف داده و مداخله در پردازش داده پیام و سیستم های رایانه ای، و یا استفاده از وسایل کاربردی سیستم های رمز نگاری تولید امضاء - مثل کلید اختصاصی – بدون مجوز امضاء کننده و یا تولید امضاء فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن و نتیجتاً جعل داده پیام های دارای ارزش مالی و اثباتی.»

و در اینجا در مورد رفتارهای ارتکابی که در این ماده قانونی قید شده است به صورت مجزا مطالبی را بیان می داریم:

۱- ورود، تغییر، محو و توقف داده پیام

در خصوص وارد کردن و تغییر دادن و محو کردن داده پیام، سابقاً در مباحث قبلی توضیحات لازم را بیان کرده ایم و از توضیح دوباره آن خودداری می کنیم. اما در خصوص « توقف داده پیام» باید خاطر نشان ساخت که منظور از توقف داده پیام، اختفای تمام یا بخشی از داده ها به گونه ای است که، عمل پردازش را از مسیر عادی خارج و مانع از عملکرد صحیح سیستم ها و پردازش دقیق اطلاعات شود. پردازش چنین اطلاعاتی، منجر به حصول نتایج غیر واقعی شده و داده پیام ایجاد شده از این طریق، هیچگونه انطباقی با واقعیت نخواهد داشت ولی چنانچه به عنوان داده پیام معتبر قابل استفاده باشد، داده پیام مجعول

تلقی می شود. از این رو در مواردی که مرتکب با موقوف سازی بخشی از اجزای داده پیام های تجاری، در خصوص مشخصات کالاها یا خدمات یا مشخصات واحد بازرگانی یا تاجر و مسئول بنگاه تجاری، داده های تفصیلی را از مسیر پردازش خارج و از این طریق، داده پیام ظاهراً معتبری ایجاد می نماید، عمل وی مشمول مجازات مندرج در ماده ۶۸ قانون تجارت الکترونیکی قرار می گیرد. به عبارت دیگر «متوقف کردن بخشی از داده ها به این صورت است که با ورود به یک سیستم رایانه ای، مانع از انتقال بخشی از داده ها هنگام انتقال آن از یک بخش سیستم به بخش دیگر شده، یا مانع از دسترسی به آن بخش از داده ها توسط کاربر مجاز شوند. بنابراین داده ای که به کاربر مجاز می رسد، داده ای ناقص و غیرصحیح خواهد بود. به عنوان مثال، فرد با ورود به سیستم رایانه ای دانشگاه مانع از دسترسی به اطلاعات مربوط به عدم پرداخت شهریه می شود و در نتیجه کاربر مربوط انتخاب واحد وی را مجاز ثبت می کند.» (خرم آبادی، ۱۳۸۴- ۱۴۲)

۲- مداخله در پردازش داده پیام و سیستم رایانه ای

سیستم رایانه ای مجموعه ای از عناصر سخت افزاری است که برای انجام کار خاصی با هم کار می کنند. هرگونه مداخله در عملکرد سیستم سخت افزاری، یا عملیات پردازش داده پیام و سیستم های نرم افزاری رایانه ای، می تواند رایانه را از مسیر پردازش صحیح داده پیام خارج کند و کارکردهای اساسی سیستم سخت افزاری رایانه را مختل کند. این عمل، مداخله در عملکرد سیستم رایانه ای و پردازش داده پیام تلقی می شود« که عبارت ایجاد اختلال به جای مداخله» صحیح تر است.»(جاویدنیا، ۱۳۸۶- ۱۵۲)

مداخله در پردازش داده پیام و سیستم رایانه ای، چنانچه منتهی به ایجاد داده پیام جعلی شود و امکان استفاده از آن به عنوان داده پیام معتبر وجود داشته باشد، عمل مرتکب را در حیطه مشمول ماده ۶۸ قانون تجارت الکترونیکی قرار می دهد.

۳- استفاده از وسایل کاربردی سیستم رمزنگاری تولید امضاء- مثل کلید اختصاص بدون مجوز امضاء کننده

این رفتار ارتکابی، عین عبارت قانون در مقام بیان یکی از مصادیق عنصر مادی جعل رایانه ای است. یکی از روش های تولید امضای الکترونیکی، استفاده از سیستم کاربردی رمزنگاری است. عملیات مربوط به رمزنگاری و متعاقباً رمز گشایی، از طریق یک جفت کلید عمومی و اختصاصی صورت می پذیرد و آنچه محرمانه و استفاده غیر مجاز آن مجرمانه است، کلید اختصاصی است، که یک کد چند رقمی کاملاً انحصاری و قابل مقایسه با اثر انگشتان شخص است که در زمره اطلاعات محرمانه اشخاص قرار دارد و هرگونه استفاده بدون مجوز از آن، جهت تولید امضاء به عنوان عنصر مادی جرم جعل قابل تعقیب است. از این رو چنانچه مرتکب با دستیابی به کلید اختصاصی شخص، امضای وی را ذیل یک سند الکترونیکی، یا داده پیامی که به عنوان گواهی یا سند الکترونیکی قابل بهره برداری است، جعل کند. اقدام وی به عنوان قلب و تحریف حقیقت قابل مجازات است.

منظور از واژه امضاء در این عبارت همان امضاء دیجیتالی است. این رفتار زمانی اتفاق می افتد که دارنده کلید خصوصی کوتاهی کرده و در نتیجه کلید خصوصی اش در اختیار فرد غیر مجاز قرار می گیرد. در این صورت، آن فرد غیر مجاز که با علم به غیر مجاز بودن استفاده از کلید خصوصی طرف، به امضای دیجیتالی اقدام کند مرتکب جعل شده است. باید توجه داشت که این عمل مصداقی از « وارد کردن» است.

البته با توجه به شرایط مندرج در مواد ۱۰ و ۱۵ قانون تجارت الکترونیکی، بار اثبات دلیل، در ادعای جعل امضاء نسبت به چنین داده پیامی، بر عهده دارنده کلید اختصاصی است، که قانوناً به عنوان امضاء کننده مجاز شناخته می شود.چنین کاری از نظر فنی دشوار و تا حد زیادی غیر ممکن است.

۴- تولید امضاء فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی

گاهی ممکن است مرتکب امضائی تولید کند که فاقد سابقه ثبت در «دفاتر اسناد الکترونیکی» یا همان «دفاتر خدمات صدور گواهی الکترونیکی است.»[۲] لازمه تحقق جرم جعل رایانه ای با این رفتار آن است که فردی امضائی الکترونیکی و به نام دیگری ایجاد کند که فاقد سابقه ثبت در دفاتر اسناد الکترونیکی است و از این رهگذر جعل داده های دارای ارزش اثباتی و مالی تحقق پذیرد، در غیر اینصورت، جعل بدین شیوه محقق نمی شود. برای مثال در موارد زیر جعل رایانه ای محقق نمی شود؛ دو

[۲] – براساس مشروح مذاکرات مجلس شورای اسلامی، این دو کلمه معادل اند. مشروح مجلس مذاکرات شورای اسلامی، دوره ششم، جلسه ۳۱۶

نفر شریک تجاری بر مبنای قرارداد خصوصی میان خود، جهت انجام مبادلات تجاری برای خود با استفاده از زیر ساخت کلید عمومی، امضاء دیجیتالی تولید می کنند؛ به نحوی که کلید عمومی هر یک فقط در اختیار دیگری قرار می گیرد و نیازی به ثبت در مراجع گواهی احساس نمی کنند. اسناد الکترونیکی موجود میان آنان از نظر قانون تجارت الکترونیکی معتبر است و در حد اسناد عادی قابلیت استناد دارد بنابراین تولید چنین امضائی هر چند فاقد سابقه ثبت در دفاتر اسناد الکترونیکی باشد جعل نیست.

یک متخصص رایانه که به سفارش یک شخص برای او و به نام او یک امضاء الکترونیکی ایجاد می کند تا در اسناد عادی تجاری طرف به کار برده شود، هر چند از ناحیه دیگری امضائی ایجاد کرده است که فاقد سابقه ثبت در دفاتر اسناد الکترونیکی است، مرتکب جعل رایانه ای نشده است.

۵- عدم انطباق وسایل کاربردی سیستم های رمزنگاری تولید امضاء به نام دارنده در فهرست مزبور

عبارت « عدم انطباق آن وسایل با نام دارنده در فهرست مزبور» عبارت گویایی نیست، زیرا این عبارت بیانگر یک حالت است نه یک فعل. به نظر می رسد که منظور مواردی است که مرتکب از کلید خصوصی ثبت شده به نام یک فرد خاص استفاده کرده و یک امضاء دیجیتالی به نام خود یا شخص ثالثی ایجاد می کند. پس از مراجعه به فهرست مرجع گواهی، مشخص می شود نام فردی که امضاء دیجیتالی پیوست به سند الکترونیکی منتسب به اوست و به عبارتی از کلید خصوصی مربوط به نام او استفاده شده است با دارنده کلید عمومی مرتبط با آن کلید خصوصی مندرج در فهرست مطابقت ندارد. در این مثال، چنانچه به این عدم مطابقت توجه نشود، چون امضاء دیجیتالی با استفاده از آن کلید عمومی قابل رمزگشایی است، دریافت کننده ممکن است دچار خطا شده و امضاء را از ناحیه فردی که در امضاء الکترونیکی کلید خصوصی به او نسبت داده شده است بداند.

۶- اخذ گواهی صحت و اصالت امضای الکترونیکی به طرق مجعول

صدور گواهی صحت و اصالت امضای الکترونیکی، از طریق دفاتر خدمات صدور گواهی الکترونیکی صورت می پذیرد. این تأسیس حقوقی نوین که در نتیجه بهره مندی از فناوری های اطلاعات و ارتباطات ایجاد گردیده، یکی از اساسی ترین پایه های تجارت الکترونیکی به شمار می رود. این دفاتر در بستر مبادلات الکترونیکی و در فضای مجازی جایگزین سازمان های متولی ثبت حقایق مربوط به اشخاص و دفاتر صدور گواهی صحت و اصالت امضاء تلقی می شوند و عملیات مربوط به شناسایی هویت طرف های معاملاتی و گواهی صحت صدور و اصالت امضای اشخاص را به عهده دارند. از این رو تحت عنوان دفاتر اسناد الکترونیکی نیز شناخته می شوند.

این دفاتر وظیفه دار تأمین و تضمین منافع، حقوق اجتماع، امنیت و صحت در روابط حقوقی معاملات الکترونیکی اشخاص هستند.

بنابراین در حالت طبیعی گرفتن گواهی مجعول معنا ندارد اما« صدور گواهی مجعول» در موارد زیرمفروض است.

- متصدیان یک دفتر خدمات الکترونیکی اقدام به صدور گواهی مجعول کنند یک گواهی مجعول توسط جاعل صادر و به دفتر خدمات الکترونیکی خاصی منتسب شود.

- یک نشانی اینترنتی به دروغ به دفتر خدمات الکترونیکی اعلام شود و درخواست کننده، فریب خورده و اقدام به گرفتن گواهی از آن کند. در هر دو صورت یاد شده، « صدور گواهی مجعول» است که وصف مجرمانه دارد و نه گرفتن آن؛ به ویژه آن که افرادی که مبادرت به گرفتن گواهی می کنند، فاقد سوء نیت بوده و خود اغلب بزه دیده هستند.

«اخذ گواهی مجعول» فقط در یک حالت موضوعیت پیدا می کند و آن هم در جایی است که کارمند یک شرکت که مسئول احراز درستی یا نادرستی امضاهای الکترونیکی و گرفتن گواهی های لازم و پیوست کردن آن به سند است، با تبانی با جاعل اصلی اقدام به گرفتن گواهی مجعول و تأیید درستی امضاء سند بر مبنای آن کند. این امر که آیا عمل وی جعل تلقی می شود یا خیر، جای بحث دارد. با توجه به اصل تفسیر محدود قوانین کیفری، جرم دانستن چنین فعلی بر اساس این ماده قابل پذیرش نیست.

در پایان این بحث و بررسی رفتار ارتکابی در ماده ۶۸ قانون تجارت الکترونیکی باید گفت که با توجه به قید عبارت « و نظایر آن» در متن ماده، مصداق های ذکر شده تمثیلی اند، نه حصری البته چهار مورد اخیر از رفتار مجرمانه مرتکب را در

واقع می توان مصداق های تمثیلی از اعمال چهارگانه ورود، تغییر، محو یا توقف داده پیام دانست. زیرا این مصداق ها فقط از رهگذر ورود، تغییر، محو یا توقف داده پیام انجام می شوند و در نتیجه ذکر آن ضروری نبوده است.

۲-۲ وسیله ارتکاب جرم

جرم جعل به صورت کلاسیک جزء آن دسته از جرائمی است که وسیله به خصوصی، شرط در تحقق آن نبوده است و حتی موجب تشدید مجازات نمی گردد، اما با نگاهی به مقرره های قانونی راجع به جعل رایانه ای کاشف به عمل می آید که در جعل رایانه ای برخلاف جعل سنتی، وسیله در تحقق جرم مؤثر می باشد و بدون وجود وسیله مورد نظر امکان تحقق جرم وجود ندارد، چون این جرم در فضای سایبر و مجازی تحقق پیدا می کند لذا هرگونه رفتار ارتکابی در جعل رایانه ای صرفاً از طریق ورود به فضای مجازی و از طریق رایانه امکان پذیر می باشد.

اولین نکته ای که در درک مفهوم جعل رایانه ای باید مد نظر داشت این است که مفهوم رایانه فقط گزینه هایی که ذهن ما به آن معطوف می شود، مانند رایانه رومیزی یا قابل حمل را در بر نمی گیرد، بلکه همانطور که کنوانسیون بین المللی جرائم سایبر(مصوب ۲۰۰۱)[3] به این موضوع صراحتاً اشاره کرده، « سیستم رایانه ای یک دستگاه یا مجموعه ای از دستگاه های متصل به هم یا مرتبط به هم است که به وسیله یک برنامه، داده های دیجیتال را به طور خودکار پردازش می کند.»

قدر متیقن محرز است که حوزه تحت شمول سیستم رایانه ای بسیار گسترده تر از حوزه متصور ماست و همه دستگاه هایی که برنامه ای داشته باشند که داده های دیجیتال را پردازش کند، در بر می گیرد، مانند تلفن های همراه امروزی، سیستم های پی جو، تلفن های ثابت حافظه دار و موارد دیگر.هر چند این واقعیت نیز انکار نمی شود که مثال کامل این تعریف همان رایانه های رومیزی یا قابل حمل است.

علی هذا به زعم ما اگرچه وسیله در تحقق این جرم شرط می باشد ولی نوع وسیله در ارتکاب این جرم شرط نمی باشد و آنچه که مهم است وسیله ای ملاک می باشد که موجبات ورود به فضای مجازی را برای تحقق جرم فراهم سازد.

«بستر انجام بزه جعل رایانه ای، فضای سایبر است و این نکته را می توان از تعبیر « ... داده ها یا علائم موجود در کارت های حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها ...»که در بند ب ماده ۶ قانون جرائم رایانه ای آمده است برداشت کرد. بنابراین همه رفتارهای پیش بینی شده در این ماده باید از رهگذر کنش های رایانه ای و در بستر رایانه و مخابرات انجام شود. پس اگر کسی داده رایانه ای را چاپ کند یا از روی صفحه نمایشگر رایانه، عکس بگیرد و سپس روی کاغذ چاپ شده، دگرگونی پدید آورد، جعل رایانه ای نخواهد بود و بر حسب مورد و با گرد آمدن بایسته های قانونی، جعل سنتی بنیاد می گیرد.»(عالی پور، ۱۳۹۰- ۲۰۵)

۲-۳ نتیجه حاصل از جرم

در ادامه به این سؤال پاسخ می گوییم که آیا جرم جعل رایانه ای جزء جرایم مطلق است یا مقید؟ آیا حصول نتیجه شرط تحقیق جرم است یا خیر؟

بنابر آنچه تاکنون گذشت و اینکه نتیجه اضرار غیر را شرط تحقق جرم ندانستیم روشن است که جعل رایانه ای همانند جعل سنتی از جرائم مطلق می باشد. نتیجه لازم برای تحقق جرم جعل سنتی ایجاد ضرر است؛ اعم از ضرر بالفعل یا بالقوه، ضرر مادی یا معنوی، ضرر مستقیم یا عدم النفع، ضرر شخصی یا عمومی، ضرر به شخصی که سند مجعول منتسب به اوست یا دیگری. در صورتی که همه مؤلفه های رکن مادی کامل باشد اما ضرری متصور نباشد - برای مثال زنی به لحاظ اینکه همسر وی فرستادن پیام تبریک برای تولد فرزند مشترکشان را فراموش کرده است، با جعل امضای همسر خود چنین پیامی را بفرستد – بزه جعل محقق نشده است. البته این شرط در قانون تصریح نشده و مبنای آن رویه قضایی به نظر حقوقدانان است که اختلاف هایی نیز در این باره وجود دارد. علیهذا با قاطعیت می توان گفت که عنصر ضرر جز نتیجه جرم جعل محسوب نمی شود. چرا که همه اساتید حقوق کیفری معتقدند که منظور از « عنصر ضرر»، ضرر محتمل و بالقوه است نه ضرر بالفعل. به نظر می رسد که « عنصر ضرر» باید به همراه «موضوع» جرم جعل مورد بررسی قرار گیرد، زیرا قابلیت اضرار از خصوصیات موضوع جعل است و داده جعلی باید این قابلیت و خصوصیت را داشته باشد که به صورت بالقوه برای فرد یا جامعه مضر باشد. اگر داده مجعول

[3]- cybercrime convention, http:// conventions.coe.int/treaty/en/reports/html

چنین ویژگی را نداشته باشد، جعل تحقق نمی یابد، جعل فتوکپی یک نوشته کاغذی که تصدیق نشده، جرم جعل نیست زیرا قابلیت اضرار ندارد فتوکپی غیر مصدق ارزشی در مراجع رسمی ندارد و نسخه جعل شده آن هم قابلیت اضرار ندارد. اگر مرتکب قصد اضرار داشته باشد ولی موضوع قابلیت اضرار نداشته باشد، جرم محقق نمی شود. بنابراین قابلیت اضرار یکی از خصوصیات موضوع جرم جعل رایانه ای است.

با توجه به این که ماده ۷ کنوانسیون جرائم سایبر، تحقق جرم جعل را مقید به حصول نتیجه نکرده است، لذا جرم جعل رایانه ای از جرائم مقید به نتیجه محسوب نمی شود. جعل رایانه ای مانند جعل کلاسیک یک جرم مطلق است. کافی است که داده جعل شده قابلیت اضرارداشته باشد، به محض آنکه امکان ایراد ضرر، وجود پیدا کند، بزه جعل تحقق می یابد. در این صورت عمل قابل مجازات است، هرچند که داده جعل شده قبل از اینکه مورد استفاده قرار گیرد تخریب شود.

در ادامه این بحث باید گفت در جرائمی که عنصر مادی آن ها بسیط است، شروع به عملیات اجرائی و در جرائمی که عنصر مادی آن ها مرکب است انجام جزئی از عنصر مادی، شروع به جرم را محقق می گرداند. در جرم کلاهبرداری تا زمانیکه تحقق نتیجه که بردن مال غیر است صورت نگرفته باشد در مرحله شروع به جرم قرار دارد و تحقق نتیجه جرم را تام می نماید. اما در جعل دو حالت متصور است یا اینکه نوشته را می سازد و یا خیر. در چنین جرمی که عنصر مادی آن ساده است شروع به عملیات اجرائی جعل شروع به جرم است و در جعل رایانه نیز همین موضوع صادق است.

قانونگذار برخلاف قانون جرائم رایانه ای و قانون مجازات جرائم نیروهای مسلح در بحث جعل رایانه ای در تبصره ماده ۶۸ قانون تجارت الکترونیکی شروع به این جرم را جرم انگاری کرده است. هرچند از نظر فنی به لحاظ سرعت بالا در عملیات رایانه ای فاصله زمانی بسیار اندکی بین شروع به جرم های رایانه ای و جرم تام وجود دارد، می توان موردی را تصور کرد که اثبات شود فردی کلید خصوصی دیگری را بدون مجوز به دست آورده و در حال تولید امضاء الکترونیکی که با توجه به سرعت رایانه ممکن است چند ثانیه به طول انجامد، قبل از خاتمه عملیات توسط پلیس دستگیر شود.

۴-۲ مرتکب جرم و خصوصیات مرتکب

جرم جعل رایانه ای همانند جعل سنتی ممکن است توسط بیش از یک نفر صورت گیرد. در این حالت طبق قواعد کلی چنانچه جرم ارتکابی مستند به عمل همه آن ها باشد آنان به عنوان شرکای در جرم محسوب شده و مجازاتشان نیز مجازات فاعل مستقل خواهد بود، مانند اینکه دو نفر به طور اشتراکی گذرنامه و یا شناسنامه ای را جعل نمایند.

معاونت نیز در جرائم عمدی با جمع شرایطی قابل تصور است. معاونت در این جرم(مثلاً تهیه وسایل لازم برای مرتکب که نوعی تسهیل وقوع جرم است) هم از نظر تئوری و هم از نظر عملی قابل تصور است. با توجه به جرم انگاری جعل رایانه ای در قانون جرائم رایانه ای و قانون تجارت الکترونیکی و کنوانسیون جرائم سایبر، هر شخصی می تواند مرتکب این جرم شود و خصوصیتی در مرتکب جعل شرط نیست. با این وجود در برخی از مصادیق جرم جعل سنتی چنانچه مرتکب، کارمنددولت باشد (سمت مرتکب) و یا اینکه سند یا نوشته ی جعل شده رسمی یا دولتی باشد (نوع سند) مجازات تشدید شده است، اما شایان ذکر است که در جعل رایانه ای هیچگونه تفاوتی بین اینکه تشدید مجازاتی بر اساس سمت مرتکب صورت گیرد یا اینکه موضوع جرم جعل رایانه ای رسمی یا غیر رسمی باشد صورت نگرفته است و به نظر می رسد این از جمله ایرادات وارده به قوانین مربوط به جعل رایانه ای می باشد. با این وجود جرم انگاری مربوط به جعل رایانه ای در قانون مجازات نیروهای مسلح صرفاً قابل اعمال در مورد اشخاص خاص یعنی نظامی ها می باشد و طبق ماده یک قانون مجازات جرائم نیروهای مسلح مصوب نهم دی ماه ۱۳۸۲ دادگاه های نظامی به جرائم مربوط به وظایف خاص نظامی- انتظامی کلیه افراد زیر که در این قانون به اختصار «نظامی» خوانده می شوند رسیدگی می کنند:

الف- کارکنان ستاد کل نیروهای مسلح جمهوری اسلامی ایران و سازمان های وابسته

ب- کارکنان ارتش جمهوری اسلامی ایران و سازمان های وابسته

ج- کارکنان سپاه پاسداران انقلاب اسلامی ایران و سازمان های وابسته و اعضای بسیج سپاه پاسداران انقلاب اسلامی

د- کاکنان وزارت دفاع و پشتیبانی نیروهای مسلح و سازمان های وابسته

ه- کارکنان مشمول قانون نیروی انتظامی جمهوری اسلامی ایران

و- کارکنان وظیفه از تاریخ شروع خدمت تا پایان آن

ز- محصلان- موضوع قوانین استخدامی نیروهای مسلح، مراکز آموزشی نظامی و انتظامی در داخل و خارج از کشور و نیز مراکز آموزش وزارت دفاع و پشتیبانی نیروهای مسلح.

ح- کسانی که به طور موقت در خدمت نیروهای مسلح جمهوری اسلامی ایران هستند و طبق قوانین استخدامی نیروهای مسلح در مدت مزبور از اعضاء نیروهای مسلح محسوب می شوند.

علی هذا با توجه به شرح فوق ملاحظه می گردد که جعل رایانه ای در قانون مجازات جرائم نیروهای مسلح صرفاً در مورد افراد نظامی مصداق پیدا می کند و به موجب ماده ۶۸ قانون تجارت الکترونیکی، جعل رایانه ای فقط در مورد اشخاصی تحقق می یابد که در بستر مبادلات الکترونیکی مبادرت به جعل رایانه ای نموده اند و به نوعی قانون مزبور به صورت خاص تلقی می گردد و فقط جعل رایانه ای موضوع ماده ۶ قانون جرائم رایانه ای به صورت عام بوده است و مشمول «هر کسی» می گردد که نسبت به این جرم اقدام نموده است.

۳.رکن معنوی

رکن معنوی یا روانی هر جرم به فعل و انفعال ذهنی مرتکب مربوط است. جرم جعل رایانه ای از جرائم عمدی است و مرتکب عالماً عامداً بر خلاف حکم قانون رفتار می نماید. میزان تأثیر علم مرتکب جعل رایانه ای به حکم یا به موضوع در تحقق این جرم تا چه حد است؟ آیا علم مرتکب به حکم قانون و یا موضوع جعل، شرط در تحقق جرم است؟ مطابق اصول و قواعد کلی، جهل به حکم و عدم اطلاع مرتکب به اینکه جعل جرم است و یا اینکه این عمل خاص داخل در عنوان جعل می باشد مسموع نیست، اما علم مرتکب به اینکه عمل ارتکابی احتمالاً موجد و یا موجب اضرار غیر خواهد شد، لازم است. برای تشخیص این امر، قاضی احتیاجی به مطالعه نفسانیت مرتکب ندارد و همین که عرفاً وقوع ضرر محتمل باشد کفایت می نماید. لذا اگر عرف، اضرار را محتمل نداند و یا اینکه احتمال را به درجه ای نداند که احتراز از این ارتکاب آن ضروری باشد، علم و اطلاع مرتکب محرز نمی باشد.

سوء نیت عام در ارتکاب عمل در تمامی جرائم عمدی لازم است. بنابراین مرتکب جعل رایانه ای الزاماً باید در انجام فعل مجرمانه قاصد و عامد باشد و چنانچه مرتکب، اراده انجام عمل را نداشته باشد عنصر روانی لازم برای جرم جعل وجود ندارد. سوء نیت خاص مرتکب در اضرار شرط نمی باشد و همین که شخص عالم است به اینکه موضوع جرم جعل رایانه ای، بالقوه و یا بالفعل قابلیت اضرار غیر را دارد، کفایت می کند و عمد او در اضرار و خواست نتیجه لازم نیست زیرا در این جرم، تحقق نتیجه شرط در تحقق جرم نمی باشد. به عبارت دیگر مرتکب اولاً باید با علم و آگاهی کامل و عمداً مبادرت به قلب حقیقت و تحریف حقایق نماید و ثانیاً باید آگاه باشد که اعمال وی اضرار آمیز بوده و تولیدات مجرمانه ی وی، قابلیت اضرار به غیر را دارد و ممکن است، به منافع کل جامعه یا افراد تشکیل دهنده آن لطمه وارد نماید.

از این رو در مواردی که مرتکب، با اعتقاد به اینکه حق ورود اطلاعات یا تغییر مندرجات داده پیام را دارد و یا مجاز به مداخله در سیستم یا پردازش داده پیام است، اقداماتی را انجام و در نتیجه آن، داده پیامی خلاف حقیقت ایجاد کند، که اتفاقاً قابلیت استفاده به عنوان داده پیام معتبر را هم داراست، عمل مرتکب، مشمول عنوان مجرمانه جعل قرار نمی گیرد. مثل موردی که کاربر مجاز ، که حق ورود به سیستم پردازش اطلاعات را دارد، با اعتقاد به اینکه حق تغییر مندرجات داده پیام را دارد، بخشی از داده پیام را حذف و محو می کند و آنرا مجدداً مورد پردازش قرار می دهد و در نتیجه داده پیام کاملاً معتبری برخلاف حقیقت ایجاد می کند، در چنین موردی، ایجاد کننده داده پیام، به واسطه عدم آگاهی از اینکه مرتکب قلب و تحریف واقعیت شده است، بزهکار تلقی نمی گردد.همچنین در مواردی که مرتکب، با علم به اینکه عمل وی قلب و تحریف حقیقت است، در داده پیام های شخصی متعلق به خود، تغییراتی ایجاد و با ورود برخی اطلاعات، یا حذف و محو بخشی از آن، داده پیام جدیدی را به ضرر خود ایجاد می نماید.

نتیجتاً اینکه جرم جعل رایانه ای همانند سایر جرائم مطلق، نیازی به سوء نیت خاص ندارد و قصد متقلبانه مرتکب جرم جعل، انگیزه می باشد. آقای دکتر آزمایش در این خصوص گفته است: « یکی از مصادیقی که گفته می شود سوء نیت خاص با انگیزه تداخل پیدا می کند همین مورد جعل است. اگر جعل مقید به نتیجه نباشد قصد اضرار، انگیزه است نه سوء نیت

خاص. چون سوء نیت خاص به نتیجه تعلق می گیرد. در جرائم مطلق سوء نیت خاص نه امکان وجود دارد و نه لازم است.»(آزمایش،۱۳۷۵- ۳۲)

البته نظر مخالف در این زمینه وجود دارد و گفته اند« با توجه به اینکه در تعریف انگیزه گفته شده است، انگیزه به معنی داعی، محرک و هدف غائی و نهایی مرتکب است.» به فرض که تحقق جعل نیاز به قصد اضرار را (قصد تقلب) داشته باشد، به نظر می رسد که چنین قصدی سوء نیت خاص است نه انگیزه. اگر چنین قصدی را انگیزه بدانیم، باید بپذیریم که مثلاً هر کسی برای بدست آوردن پول جهت کمک به شخص ثالث، سند متعلق به دیگری را جعل کند، چون هدف غایی او اضرار به غیر نیست، پس مجرم نیست. اما رویه قضایی کسی را که به طور متقلبانه سندی را جعل کرده باشد، حتی اگر هدف غایی او کمک به شخص ثالث باشد، مجرم می داند. بنابراین باید تعریف دیگری برای انگیزه ارائه دهیم و یا اینکه بپذیریم که قصد اضرار(قصد تقلب) سوء نیت خاص است.(خرم آبادی،۱۳۸۴)

تفاوتی که بین جعل رایانه ای موضوع ماده ۶۸ قانون تجارت الکترونیکی با جعل رایانه ای موضوع ماده ۶ قانون جرائم رایانه ای و ماده ۱۳۱ قانون مجازات جرائم نیرو های مسلح وجود دارد اینست که در جعل رایانه ای موضوع ماده ۶۸ قانون تجارت الکترونیکی عبارتی قید گردیده است که بالصراحه دلالت بر تأثیر انگیزه در تحقق بزه جعل رایانه ای می نماید، بدین توضیح که به موجب ماده ۶۸ قانون تجارت الکترونیکی جعل داده پیام های دارای ارزش مالی و اثباتی در صورتی جرم محسوب می شود که مرتکب قصد داشته باشد با ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان داده پیام های معتبر از آن ها استفاده نماید. مفهوم مخالف این ماده این است که اگر مرتکب چنین قصدی نداشته باشد، جاعل محسوب نمی شود. چنین قصد متقلبانه ای انگیزه نامیده می شود. همانگونه که گفتیم چون جعل رایانه ای جرم مطلق می باشد لذا سوء نیت خاص در آن جایگاهی ندارد و آنچه تحت عنوان «قصد متقلبانه» در آن مورد نیاز می باشد، انگیزه نام دارد و نه سوء نیت خاص.

تفاوتی که از جهت رکن معنوی جرم جعل رایانه ای بین ماده ۶۸ قانون تجارت الکترونیکی و ماده ۷ کنوانسیون جرائم سایبر وجود دارد، این است که به موجب ماده ۶۸ قانون تجارت الکترونیکی یکی از شرایط جعل رایانه ای این است که ایجاد کننده داده های رایانه ای غیر مجعول باید قصد داشته باشد که شخصاً داده های غیر معتبر را به عنوان داده معتبر مورد استفاده قرار دهد تا جاعل محسوب شود. اما به موجب ماده ۷ کنوانسیون مذکور صرف قصد ایجاد کننده داده های غیر صحیح مبنی بر مورد استفاده قرار گرفتن این داده ها به عنوان داده صحیح برای جاعل تلقی شدن وی کافی است. لازم نیست که مرتکب قصد داشته باشد که شخصاً از داده های غیر صحیح به عنوان داده صحیح در اهداف قانونی استفاده کند. به نظر می رسد که عدم توجه قانونگذار به نحوه تدوین و تنظیم عبارات قانونی باعث چنین اشتباهی شده است. به هر حال با توجه به صراحت قانون تا زمانی که این قانون تصحیح نشود، دادرسان مکلفند از آن تبعیت نماید.

نهایتاً اینکه رکن معنوی جعل رایانه ای دارای سه جزء به شرح زیر است:

۱. علم مرتکب به بدون حق بودن اعمالی که منجر به ایجاد یک داده پیام غیر صحیح می شوند.

۲. سوء نیت عام یعنی مرتکب عمداً و با خواست خود و با اراده آزاد یکی از اعمالی را که منجر به ایجاد یک داده پیام که کذب می شود انجام داده باشد.

۳. انگیزه، یعنی مرتکب قصد تقلب داشته باشد.

۴. نتیجه گیری

عصر حاضر را به حق، عصر فن آوری اطلاعات نامیده اند. رایانه یکی از ساخته های بسیار مهم و منحصر به فرد بشری است که همه ابعاد زندگی اجتماعی را دگرگون ساخته و آثار گسترده و شگرفی بر جای گذاشته است. فن آوری اطلاعات در قلمروی حقوق کیفری تحولات چشم گیری ایجاد کرده است. امروزه رایانه و فضای سایبر (مجازی) امکان بیش از پیش رفتارهای ضد اجتماعی را به وجود آورده است. از جمله این رفتارها که نشأت گرفته از رایانه و فضای سایبر می باشد، «جعل رایانه ای» است.

در نظام تقنینی ایران با دو نوع بزه جعل روبرو هستیم؛ یکی جعل سنتی و دیگری جعل رایانه ای. به دنبال نوظهور بودن عنوان جزایی جعل رایانه ای و ورود به نظام حقوقی، ضرورت پرداختن به این جرم و بررسی عناصر متشکله آن ایجاد می گردد.

بزه جعل رایانه ای در حقوق کیفری ایران در قوانین مجازات جرائم نیروهای مسلح (ماده ۱۳۱)، تجارت الکترونیکی (ماده ۶۸) و قانون جرائم رایانه ای (ماده ۶) آمده است وقبل از وضع قوانین مذکور هر آنچه از سیر قانونگذاری ایران در مورد جعل بیان گردیده است ناظر به بزه جعل سنتی بوده است. در ظاهر ممکن است این شائبه ایجاد گردد که بین جعل رایانه ای و جعل سنتی تفاوتی وجود ندارد و در ماهیت، آن ها یکسان هستند ولی تفاوت عمده ای که بین این دو بزه علی الخصوص در بحث عنصر مادی آن ها و ویژگی های خاص جرائم رایانه ای و من جمله جعل رایانه ای می باشد، ضرورت جرم انگاری بزه جعل رایانه ای را در نظام تقنینی ایران ایجاب نموده است. جعل رایانه ای عبارتست از ساختن یا تغییر دادن آگاهانه داده های رایانه ای یا سایر موارد مذکور در قانون که دارای ارزش اثباتی و به قصد جا زدن آن ها به عنوان اصل برای استفاده خود یا دیگری و به ضرر غیر. در بحث جعل و تزویر و همچنین جعل رایانه ای می گوییم که سند یا حافظه رایانه و نظم اسنادی به عنوان یک ارزش در نظام حقوقی ما می باشد و از ارزش و اعتبار برخوردار است و بر همین اساس رفتارهایی که مخالف با نظام اسنادی هستند، رفتارهایی است که زیان شدید و غیر قابل تحمل را ایجاد می کند و نظم اسنادی را مخدوش می سازد و همین امر مبنای جرم انگاری جعل رایانه ای را تشکیل می دهد. تمایز جعل رایانه ای با جعل سنتی علاوه بر اینکه بر این مبنا استوار می باشد که جعل رایانه ای در فضای سایبر و مجازی تحقق می یابد و نه فضای واقعی، می توان گفت که از جمله ویژگی های جعل رایانه ای همانند سایر جرائم اینترنتی، گستردگی، فراوانی، فرامرزی بودن، وقوع سهل و آسان، تنوع، جذابیت و زاید الوصف بودن این جرم می باشد. بزه جعل رایانه ای همانند سایر عناوین جزایی متشکل از عناصر قانونی، مادی و روانی می باشد، عنصر قانونی این بزه در حقوق جزایی ایران منحصر به همان سه مقرره قانونی بود که در فوق به آن اشارت رفت، رفتار مرتکب به عنوان یکی از اجزای عنصر مادی این بزه منحصر به وارد کردن، حذف کردن، تغییر دادن و متوقف کردن داده های رایانه ای می باشد و قانونگذار ایران به صورت پراکنده هر کدام از موارد مصرحه را در سه قانون یاد شده آورده است و به جا بود همانطور که در ماده ۷ کنوانسیون جرائم سایبر آمده است هر چهار مورد را به عنوان رفتار مرتکب در قوانین داخلی و یکجا می آورد. از جمله شرایط رفتار مجرمانه در جعل رایانه ای که تفاوتی با جعل سنتی نداشته است قابلیت اضرار و بر خلاف واقع بودن رفتار مجرمانه می باشد و در صورت تحقق شرایط بزه جعل رایانه ای ارتکاب می یابد. یکی دیگر از اجزای رکن مادی جعل رایانه ای، موضوع و متعلق این جرم می باشد.

موضوع جرم جعل رایانه ای عبارتست از داده های قابل استناد، داده ها و علائم موجود در کارت های حافظه و داده ها و علائم قابل پردازش در سامانه های رایانه ای یا مخابراتی و تراشه ها که هرکدام دارای تعریف خاص می باشند. به اعداد، حروف و علائم که جهت درک فهم مشترک از انسان ها یا رایانه سرچشمه می گیرند داده می گویند و به طور کلی می توان گفت که موضوع جعل رایانه ای همان داده ها و برنامه های رایانه ای می باشد که موارد تصریح شده در فوق بدان منتهی می گردد. اما شرط مؤثر و لازم در موضوع جعل رایانه ای اینست که داده ها و برنامه های رایانه ای باید قابلیت استناد و مؤثر در اثبات و نفی امر باشد؛ به عبارت دیگر دارای ارزش قضایی باشد وگرنه اگر داده ها ارزش قضایی نداشته باشد جعل واقع نمی شود. در جعل رایانه ای بر خلاف جعل سنتی، وسیله در تحقق جرم مؤثر می باشد و بدون وجود وسیله مورد نظر امکان تحقق جرم وجود ندارد. با این وجود اگرچه وسیله در تحقق این جرم شرط می باشد ولی نوع وسیله در ارتکاب این جرم شرط نمی باشد و آنچه اهمیت دارد وسیله است که موجبات ورود به فضای مجازی را برای تحقق جرم فراهم سازد. جعل رایانه ای مانند جعل کلاسیک یک جرم مطلق است و کافی است که داده مجعول قابلیت اضرار داشته باشد، به محض آنکه امکان ایراد ضرر وجود پیدا کند، بزه جعل تحقق می یابد. در رابطه با خصوصیت مرتکب جعل رایانه ای به عنوان یکی از اجزاء عنصر مادی باید گفت که جعل رایانه ای در قانون مجازات جرائم نیروهای مسلح صرفاً در مورد افراد نظامی مصداق پیدا می کند و در قانون تجارت الکترونیکی در مورد اشخاصی تحقق می یابد که در بستر مبادلات الکترونیکی مبادرت به جعل رایانه ای نموده اند و به نوعی قانون مزبور به صورت خاص تلقی می گردد و فقط جعل رایانه ای موضوع قانون جرائم رایانه ای به صورت عام بوده است و مشمول هر کسی

می گردد که نسبت به این جرم اقدام نموده است. در جرم جعل رایانه ای علاوه بر اینکه عمل مرتکب و سوء نیت عام به عنوان اجزای رکن معنوی این جرم را تشکیل می دهند، انگیزه یعنی قصد تقلب به عنوان یکی از اجزای رکن روانی این جرم می باشد زیرا جرم جعل رایانه ای همانند سایر جرائم مطلق نیازی به سوء نیت خاص ندارد و قصد متقلبانه مرتکب جرم جعل، انگیزه می باشد. با توجه به نقش اشخاص حقوقی و علی الخصوص اشخاص حقوقی حقوق خصوصی در روابط اجتماعی و به خصوص در امور الکترونیکی و رایانه ای و با عنایت به اینکه بروز رفتارهای مجرمانه از سوی اشخاص حقوقی، دارای اثرات زیان باری می باشد، مع الوصف برای اولین بار صراحتاً در حقوق کیفری ایران در مواد ۱۹ و ۲۰ قانون جرائم رایانه ای، مسئولیت کیفری اشخاص حقوقی مورد شناسایی قرار گرفت، که مشمول کلیه جرائم رایانه ای و از جمله جعل رایانه ای می گردد. با مقایسه بین جعل رایانه ای در قانون جرائم رایانه ای و جعل سنتی ملاحظه می کنیم که قانونگذار برای مجازات جعل رایانه ای آنگونه که در جعل سنتی قائل به تفکیک گردیده است هیچگونه تفکیکی قائل نشده است و به تعبیر دیگر تفاوتی بین مجازات در جعل رایانه ای داده های رسمی و داده های عادی وجود ندارد که به نظر می رسد با توجه به اهمیت موضوع جرم می بایست به این نکته توجه می گردید. قانونگذار در تعیین مجازات در قانون جرائم رایانه ای به سیاست سخت گیرانه نظر داشته است و طبیعتاً می بایست مجازات لحاظ شده در جعل رایانه ای سنگین تر از مجازات تعیین شده برای جعل سنتی باشد و این امر به خاطر این است که با توجه به فضای سایبر و در دسترس بودن رایانه برای ارتکاب این جرم، تشدید این نوع مجازات امری پسندیده است ولی در مواردی می بینیم که مجازات های در نظر گرفته برای جعل سنتی از مجازات های مربوط به جعل رایانه ای شدیدتر است و این با سیاست کیفری مربوط به جرائم رایانه ای در تضاد می باشد. قانونگذار در قانون مجازات جرائم نیروهای مسلح فقط به مجازات حبس برای جعل رایانه ای بسنده کرده است و از امتیازاتی که در تعیین مجازات جزای نقدی برای جعل رایانه ای وجود داشته است بی بهره مانده است. چه آنکه در اغلب موارد در جعل رایانه ای برای مرتکب انگیزه مادی وجود داشته است و مجازات جزای نقدی کیفر مناسبی برای این جرم می باشد که این امر از نظر قانونگذار دور مانده است. به همراه تصویب مقررات ماهوی در زمینه جعل رایانه ای در کشور ما ضروری است تا بسان سایر کشورها به مسأله تعقیب و مقامات تعقیب و مقامات قضایی در رأس امور مربوط به این جرائم قرار گیرند.

حال باتوجه به نتایج مطروحه پیشنهادات زیر مطرح میگردد :

۱. به دستگاه قضایی پیشنهاد می گردد تا با عنایت به سیر تحول جرائم از سنتی به سمت رایانه ای که جعل نیز یکی از مصادیق آن می باشد در جهت ارتقای علمی قضات، ضابطین دادگستری در این خصوص تلاش نماید و با لحاظ نمودن شعب ویژه و امکانات کافی در این زمینه اقدام نماید. اقداماتی که هم می تواند جنبه پیشگیرانه داشته باشد و هم در جهت تعقیب، تحقیق و رسیدگی و اعمال مجازات آن استفاده نماید.

۲. قانون در مواردی که شخص یا اشخاصی بدون علم و اطلاع به مجعول بودن داده ها، کارتها یا تراشه ها از آنها استفاده نمایند و باعث ایجاد خسارت مالی و ... گردند تکلیفی مشخص نکرده و ساکت است لذا پیشنهاد می گردد تا این خلا در قانون جرایم رایانه ای مرتفع گردد.

۳. پیش از هر چیز لازم است مخاطبین این تدابیر به خوبی شناسایی گردند. مطالعه در زمینه شناخت شخصیت جنایی مجرمین جعل رایانه ای و انگیزه‌های مجرمانه آنها و همچنین آشنایی با بزهدیدگان این جرایم، یکی از اقدامات اساسی و زیربنایی جهت اجرای این تدابیر محسوب می‌شود.

۴. شناخت بستر فضای سایبر و کارکردهای مثبت و منفی ابزارهایی که می‌توان در آنها به کار برد، می‌تواند به ما در اتخاذ تدابیر پیشگیرانه مناسب وضعی از جعل رایانه ای کمک نماید. بدیهی است در این میان مطالعه‌ای بنیادی – کاربردی از نحوه فعالیت شبکه‌های اطلاع‌رسانی رایانه‌ای با رویکرد پیشگیری در اولویت قرار خواهد داشت.

منابع و مراجع

[۱] آزمایش، ع،۱۳۷۵و۱۳۷۵، تقریرات درس حقوق جزای اختصاصی دانشگاه تهران
[۲] آشوری، م،۱۳۸۹، آیین دادرسی کیفری، جلد ۱، چاپ یازدهم، انتشارات سمت، تهران
[۳] اصلانی،ح ،۱۳۸۹، حقوق فناوری اطلاعات، چاپ دوم، نشر میزان، تهران
[۴] البوعلی،ا،۱۳۹۲، صلاحیت محاکم در جرایم سایبری، چاپ اول، نشر جنگل، تهران
[۵] بای، ح و پورقهرمانی، ب،۱۳۸۸، بررسی فقهی حقوقی جرایم رایانه ای، چاپ اول،پژوهشگاه علوم و فرهنگ اسلامی، تهران
[۶] بررسی ابعادحقوقی فناوری اطلاعات، مرکز مطالعات راهبردی و توسعه قضایی، خرداد ۱۳۸۳، صفحه ۳۶
[۷] پاکزاد، ب،۱۳۸۸، تروریسم سایبری، رساله دکتری حقوق کیفری و جرم شناسی، دانشگاه شهیدبهشتی
[۸] پیمانی،ض،۱۳۷۵، حقوق کیفری اختصاصی(جرایم علیه امنیت و آسایش عمومی)، چاپ دوم، نشر میزان، تهران
[۹] جاویدنیا، ج،۱۳۸۶، مقاله نقد و بررسی جرم مندرج در قانون تجارت الکترونیکی، مجله حقوقی دادگستری، شماره ۵۹، صفحه ۱۴۲
[۱۰]جلالی فراهانی،ا، ۱۳۸۸ ، صلاحیت کیفری سایبری در پرتو قوانین داخلی، چاپ اول، انتشارات روزنامه رسمی جمهوری اسلامی ایران، تهران
[۱۱]جلالی فراهانی، ا،۱۳۸۹، کنوانسیون جرایم سایبر و پروتکل الحاقی، چاپ اول، انتشارات خرسندی، تهران
[۱۲]حسنوی،ر، ۱۳۷۹، فرهنگ تشریحی مایکروسافت ۲۰۰۰، چاپ اول، انتشارات دانشیار، تهران
[۱۳]خداقلی، ز، ۱۳۸۳، جرایم رایانه ای، چاپ اول، انتشارات آریان، تهران
[۱۴]خرم آبادی، ع،۱۳۸۴، جرایم فناوری اطلاعات، رساله دکترای حقوق جزا و جرم شناسی، دانشگاه تهران
[۱۵]دزیانی، م،۱۳۷۸، جزوه حمایت از داده ها، سازمان مدیریت و برنامه ریزی، دبیرخانه شورای عالی انفورماتیک
[۱۶]رایجیان اصلی، م،۱۳۸۶، مقاله قانون جرایم رایانه ای، نوآوری ها و کاستی ها ، مجله پژوهش های حقوقی، شماره ۱۵،
[۱۷]سالاری، م، ۱۳۸۶، حقوق جزای اختصاصی جعل و تزویر، چاپ اول، میزان، تهران
[۱۸]سعادت، م، ۱۳۸۴، مبانی رایانه، چاپ پنجم، انتشارات تجمع آموزشی و فنی، تهران
[۱۹]سلیمی،ص،۱۳۷۶، پدیده مجرمانه و مسئولیت کیفری در حقوق بین المللی و حقوق کیفری ایران، چاپ اول، انتشارات خیام، تهران
[۲۰]شیرزاد، ک،۱۳۸۸، جرایم رایانه ای از دیدگاه حقوق جزای ایران و بین الملل، چاپ اول، نشر بهینه فراگیر، تهران
[۲۱]عالی پور، ح، ۱۳۹۰، حقوق کیفری فناوری اطلاعات، چاپ اول، انتشارات خرسندی،تهران
[۲۲]فروغی، ف ، ۱۳۸۸، منشا و ماهیت حقوقی اصل صلاحیت جهانی، مجله علمی پژوهشی مطالعات حقوقی، شماره سوم، صفحه ۲۲
[۲۳]قوه قضاییه، مرکز مطالعات راهبردی توسعه قضایی و شورای عالی توسعه قضایی، کمیته مبارزه جرایم رایانه ای، لایحه قانون مجازات جرایم رایانه ای و گزارش توجیهی،۱۳۸۳، تهران
[۲۴]گلدوزیان، ا،۱۳۷۸، حقوق جزای اختصاصی، چاپ ششم، انتشارات جهاد دانشگاهی(ماجد)، تهران
[۲۵]معاونت اجتماعی و اطلاع رسانی قوه قضاییه، ۱۳۸۱، گزارش ماه، شماره سوم، صفحه ۲
[۲۶]معاونت آموزش و تحقیقات قوه قضاییه، ۱۳۸۹، قواعد حقوق تجارت الکترونیکی، چاپ اول، تهران
[۲۷]معین، م،۱۳۷۵، فرهنگ فارسی، امیرکبیر، تهران
[۲۸]میرسعیدی، م،۱۳۸۳، مسئولیت کیفری، جلد یک، چاپ اول، میزان، تهران
[۲۹]میرمحمدصادقی، ح،۱۳۸۶، حقوق کیفری اختصاصی (جرایم علیه امنیت و آسایش عمومی)، چاپ هشتم، میزان، تهران