

همایش ملی مطالعات و پژوهش های علمی علوم انسانی

نهاد برگزار کننده همایش: موسسه قانون یار با حمایت معنوی دانشگاه آزاد اسلامی واحد کرمانشاه
سر دبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی شماره مجوز: ۴۸۵۳-۷۸۸۶۴
سال برگزاری همایش: ۱۳۹۷ شماره مقاله: ۸۹۵/۸۹۹ رده بندی کنگره: ب ۵۰۳/۲

مسئولیت کیفری مجرمان در قبال بزه جعل رایانه‌ای

سعید چقا کبودی

چکیده

یکی از مصادیق جرایم رایانه‌ای جرم جعل رایانه‌ای و استفاده از داده جعلی است. در جعل سنتی، ایجاد نوشته یا سند یا تغییر و تحریف در مندرجات سند و همچنین اضافه کردن نوشته یا عکس به نوشته اصلی شرط تحقق جرم جعل سنتی است. دارنده این سند جعلی، اگر با علم و اطلاع نسبت به جعلی بودن، آن را مورد استفاده و استناد قرار دهد، مرتکب جرم استفاده از سند جعلی شده است. جعل رایانه‌ای به عنوان یکی از جرائم رایانه‌ای به لحاظ خصوصیتی که در آن نهفته است و خاص کلیه جرائم رایانه‌ای می‌باشد از حیث مسئولیت و مجازات کیفری اقتضاء دارد که با جرائم سنتی متفاوت باشد و از طرفی از حیث جنبه شکلی و من جمله آیین دادرسی ضرورت دارد تا مورد توجه قانونگذاران قرار گرفته و آیین دادرسی مختص به این جرم را از سیر قانونگذاری بگذرانند. ما در این مقاله سعی داریم مسئولیت کیفری مجرمان در قبال بزه جعل رایانه‌ای را مورد مذاقه و بررسی قرار دهیم.

واژگان کلیدی: جعل رایانه‌ای، جرایم سایبری، اینترنت، مسئولیت کیفری

بخش اول: کلیات

«در فرهنگ فارسی معین مسئولیت به معنای مسئول یا موظف به انجام کاری و مسئول در دو معنا به معنای چیز خواهش شده (مفعولی)، یا کسی که فریضه‌ای به ذمه دارد که اگر به آن عمل نکند، باز خواست شود (فاعلی) تعریف شده است.^۱ مسئولیت به معنای اصطلاحی در حقوق نیز از وجه تسمیه آن دور نیفتاده و به معنای لزوم پاسخگویی اشخاص در قبال اقدامات خود در برابر جامعه و دیگران است و در تعریف مسئولیت گفته‌اند: «مسئولیت عبارتست از وجود تعهد به انجام یا عدم انجام کاری و تحمل آثار و ضمانت اجرایی‌های مقرر در صورت نقض این تعهد.»^۲ در کتب حقوقی تقسیم‌بندیهای مختلفی از مسئولیت نظیر مسئولیت اخلاقی و قانونی (حقوقی) صورت گرفته است. رایج‌ترین این تقسیم‌بندیها، تقسیم مسئولیت به مسئولیت مدنی، کیفری انتظامی است. «حقوقدانان از مسئولیت کیفری به دو وجه مختلف یکی در معنای «اهلیت تحمل تبعات جزایی» و دیگری در معنای «اجبار به تحمل تبعات جزایی» یاد کرده‌اند که اولی معرف جنبه انتزاعی و مجرد و دومی نشانگر جنبه عینی مسئولیت است. جنبه انتزاعی مسئولیت ناظر به وضعیت و صفتی خاص در شخص است که به موجب آن اهلیت و قابلیت این را پیدا می‌کند تا هر زمان رفتار مجرمانه‌ای از او صادر شود تبعات جزایی آنرا متحمل گردد. پس صحیح است که بگوییم شخص واجد اهلیت دارای مسئولیت کیفری است اما از نوع مسئولیت بالقوه؛ یعنی که این تشخیص به خاطر داشتن وضعیت و صفتی خاص اگر فعل مجرمانه‌ای انجام دهد لاجرم تبعات جزایی آنرا هم متحمل خواهد شد. اما

۱ - معین، محمد، فرهنگ فارسی معین، جلد پنجم، انتشارات امیرکبیر، ۱۳۸۱، حرف میم، ذیل واژه مسئولیت.

۲ - سلیمی، صادق، پدیده مجرمانه و مسئولیت کیفری در حقوق بین‌المللی و حقوق کیفری ایران، انتشارات خیام،

چاپ اول، ۱۳۷۶، ص ۱۸.

زمانی که شخص در برابر رفتار مجرمانه‌ای انجام داده است یکجانبه و به قهر مجبور به تحمل تبعات جزایی آن می‌شود. مسئولیت کیفری وجود واقعی و عینی پیدا کرده است. پس این تغییر هم صحیح است که بگوییم شخص مجرم دارای مسئولیت کیفری است، اما این با از نوع مسئولیت بالفعل: یعنی که شخص به خاطر جرمی که مرتکب شده است تبعات جزایی آن را هم به قهر و اجبار تحمل می‌کنند.^۱ عمده این اختلاف از آنجا ناشی می‌شود که عناصر و رکان تعریف اول با تعریف دوم متمایز و در واقع تعریف دوم عناصر بیشتری را در خود جای داده است، به نحوی که سبب می‌شود به این نتیجه برسیم که اولین تعریف از مسئولیت، تعریفی مضیق و دومی تعریفی موسع‌تر از مسئولیت کیفری است؛ در واقع مسئولیت انتزاعی به این مفهوم استوار است که شخص می‌تواند مسئول باشد. حال آنکه مسئولیت واقعی متضمن این است که شخص اکنون مسئول است و باید پاسخگوی رفتار خود باشد. بنابراین با پذیرش مفهوم مسئولیت به معنای واقعی آن باید توجه داشت که ارکان مسئولیت کیفری برحسب جرائم مختلف و رفتار مادی مختلف و اقسام حالات ذهنی مرتکب متغیر می‌گردد؛ برای مثال قانونگذار که برخی موارد عنصر تقصیر را برای مسئولیت لازم می‌داند، اما در برخی موارد دیگر به حالت ذهنی مرتکب توجهی ندارد و در هر صورت به صرف وقوع پدیده مجرمانه وی را مسئول می‌شناسد (مسئولیت مطلق)؛ یا برای مثال ارکان مسئولیت که در آنجا که رفتار مادی مرتکب را فعل (رفتار مثبت) تشکیل می‌دهد با آنجا که رفتار مادی مرتکب بر ترک فعل استوار است، متفاوت می‌شود، بطوری که در مواردی که ترک فعل عنصر مادی جرمی را تشکیل می‌دهد و قانونگذار برای عدم انجام تکلیفی که از مرتکب انجام آن را خواسته وی را مورد سرزنش قرار می‌دهد، علاوه بر ادراک، اختیار و علم به قانون مرتکب، عنصر دیگری به نام

۱- میر سعیدی، منصور، مسئولیت کیفری، جلد یک، تهران، انتشارات میزان، چاپ اول، ۱۳۸۳، ص ۲۳.

توانایی و امکان فیزیکی انجام تکلیف نیز اضافه می‌شود، چه در صورتی که ثابت شود که تارک فعل قدرت و توانایی انجام خواسته‌ی قانونگذار را نداشته یا اینکه بر فرض داشتن چنین توانایی درونی، حوادث خارجی مانع از انجام خواسته قانونگذار شده است وی قانوناً مسئولیتی نخواهد داشت. بنابراین با بررسی نظر حقوقدانان می‌توان دریافت که گاهی مسئولیت کیفری با وجود جمیع شرایط مسئولیت یعنی دارا بودن شرایط عینی، معنوی و حقوقی آن به شخص بار می‌شود که می‌توان این قسم از مسئولیت را مسئولیت حقیقی نامید؛ به عبارت دیگر آنگاه که قانونی رفتار وی را مجرمانه دانسته باشد و شخص به تقصیر (به معنای کل آن) مرتکب آن رفتار شود حقیقتاً مسئول خواهد بود؛ لیکن گاهی بنا به برخی ضروریات اجتماعی قانونگذار تمامی شرایط را برای احراز مسئولیت لازم نمی‌بیند و به عبارتی بنا بر مصالحی چنین مسئولیتی را بر شخص بار می‌کند؛ این چنین مسئولیتی را می‌توان مسئولیت انتسابی نامید. براساس نظریه‌های کنونی، فضای سایبر که جرم جعل رایانه‌ای نیز در آن فضا محقق می‌گردد، به لحاظ ویژگی‌هایی مانند ضعیف بودن عوامل کنترل و نیز مشکلات تعقیب و مجازات مرتکب، ناگزیر از اعمال چنین مسئولیتی در حوزه مدنی و کیفری است. آنها با بهره‌گیری از توان سایر عوامل دست‌اندرکار برقراری نظام در این فضا، در امر پیشگیری یا کنترل اطلاعات و اقدامات غیرقانونی حائز مسئولیت می‌شوند که به این ترتیب، اصل شخصی بودن مسئولیت تخصیص می‌خورد و میان سایر عوامل، علاوه بر مرتکب اصلی، توزیع می‌شود. مسئولیت انتسابی را می‌توان بر اساس معیارهای مختلفی تقسیم کرد؛ براساس اشخاص مسئول به مسئولیت انتسابی اشخاص حقیقی و حقوقی براساس دایره مشمول به مسئولیت انتسابی انتقالی (انتقال مسئولیت شخص مسئول به شخص ثالث) و توزیعی (توزیع مسئولیت بین مرتکب و ثالث) و براساس نحوه انتساب مسئولیت، بر مطلق، مفروض و غیرمستقیم قابل تقسیم است.

مسئولیت غیرمستقیم یا ثانوی نیز خود به مسئولیت انتسابی اشتراکی و مسئولیت انتسابی عارضی تقسیم می‌شود. در فضای سایر، با توجه به اینکه تکلیف پیشگیری از اطلاعات و اقدامات غیرقانونی به عهده سایر عوامل است، اقسام مسئولیت انتسابی ثانوی یا غیرمستقیم بیشتر مدنظر است.^۱

بخش دوم: مسئولیت کیفری اشخاص حقوقی در جعل رایانه‌ای

باید توجه داشت که هر چند شخص حقوقی اعتباراً و به حکم قانون می‌تواند حقوق و تکالیفی داشته باشد بطوریکه به وی شخصیتی مستقل و قانونی بخشیده و وجود وی را از اشخاص تشکیل دهنده آن جدا می‌سازد، لیکن از آنجا که این شخص فاقد شعور و اراده و ارکان مسئولیت بالقوه و انتزاعی که شامل ادراک، اختیار، علم به قانون و توانایی است در وی وجود ندارد قانون در واقع همانگونه که به وی اعتباراً حق بخشیده، اعتباراً تکلیف و مسئولیت نیز بخشیده است و این مسئولیت به واسطه همین اعتبار، حقیقی نیست، بلکه به این خاطر که وی را به خاطر اعمال اشخاص تحت تشکیل آن مسئول می‌شناسد غیرحقیقی و اصطلاحاً اعتباری است و نتیجه اینکه مسئولیت شخص حقوقی همواره اعتباری است و شخص حقوقی به این دلیل که همچون افراد حقیقی شرایط مسئول شدن را ندارد هرگز نمی‌تواند مانند آنان مشمول مسئولیت حقیقی قرار گیرد.

قانونگذار در ایران با تصویب قانون جرائم رایانه‌ای و با تخصیص فصل ششم از بخش نخست این قانون به مسئولیت کیفری اشخاص و نهایتاً مسئولیت کیفری اشخاص حقوقی دست به یک نوآوری در نظام حقوقی ایران زد که تاکنون مسبوق به سابقه نبوده است.

۱- آل محمد، فاطمه، همان منبع، ص ۱۰۴.

تا قبل از آن محور اصلی قانونگذاری، اعمال مسئولیت کیفری به اشخاص حقیقی بوده است و لحاظ کردن مسئولیت کیفری اشخاص حقوقی محلی از اعراب نداشته است در ماده ۱۹ و ۲۰ قانون جرائم رایانه‌ای در خصوص مسئولیت کیفری اشخاص حقوقی این چنین بیان گردیده است:

«ماده ۱۹- در موارد زیر، چنانچه جرایم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد شخص حقوقی دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

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

تبصره ۲- مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسئول خواهد بود.

ماده ۲۰ - اشخاص حقوقی موضوع ماده‌ی فوق، با توجه به شرایط و اوضاع و احوال جرم ارتكابی، میزان درآمد و نتایج حاصله از ارتكاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتكابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنان که حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد.

تبصره - مدیر شخصی حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری با نظارت بر شخص حقوقی دیگر نخواهد داشت.

با توجه به نقش اشخاص حقوقی و علی‌الخصوص اشخاص حقوقی حقوق خصوصی در روابط اجتماعی و به خصوص در امور الکترونیکی و رایانه‌ای و با عنایت به اینکه بروز رفتارهای مجرمانه از سوی اشخاص حقوقی، دارای اثرات زیان‌باری می‌باشد، مع‌الوصف برای اولین بار صراحتاً در حقوق کیفری ایران در مواد ۱۹ و ۲۰ قانون جرائم رایانه‌ای، مسئولیت کیفری اشخاص حقوقی مورد شناسایی قرار گرفت.

بدیهی است که قاعده مسئولیت کیفری اشخاص حقوقی از یک طرف از متضرر ماندن شاکی خصوصی و عدم جبران خسارتهای وارده جلوگیری می‌کند و از طرف دیگر مانع تجری متصدیان اشخاص حقوقی در ارتكاب جرم به وسیله اشخاص حقیقی می‌گردد. زیرا

که قبل از تصویب این قانون، به کرات اشخاص حقیقی در پوشش اشخاص حقوقی برای گریز از تعقیب و مجازات مرتکب جرم می‌شدند.

«در بند ج ماده ۱۹، با پیش‌بینی امکان ارتکاب جرم رایانه‌ای توسط کارمند شخص حقوقی با اطلاع مدیر، یکی دیگر از قواعد حقوق جنایی معاصر یعنی مسئولیت کیفری نیابتی به رسمیت شناخته شده است.

البته همانطور که در تبصره ۲ ماده ۱۹ تصریح شده، تحمیل مسئولیت کیفری به اشخاص حقوقی مانع مجازات مرتکب جرم نمی‌شود. توضیح این‌که با توجه به اعتباری بودن شخصیت حقوقی، شبهه مجازات دو نفر در قبال یک جرم مطرح نمی‌گردد و اساساً چنین ایرادی وارد نیست و شخص حقوقی رأساً در قبال اقدامات خود مسئول انگاشته می‌شود.

در ادامه ماده ۲۰، قانونگذار مجازاتهای گوناگونی را برای جرائم رایانه‌ای ارتکاب یافته توسط اشخاص حقوقی پیش‌بینی کرده است که با توجه به ویژگی‌های آنها سازگاری یافته‌اند. البته محوریت اصلی با جزای نقدی است و در کنار آن مجازاتهای تکمیلی دیگری حسب نوع جرائم ارتکاب یافته پیش‌بینی شده است.

یکی از کاستی‌های برجسته قانونی از نظر شکلی، ویرایش پر ایراد آن است که افزون بر آنها، برخی از غلطها جنبه‌ی ماهوی نیز پیدا می‌کند. از جمله اصطلاح شخص خصوصی در تبصره ۲ ماده ۱۹، تعبیر نادرستی از شخص حقوقی است که به ظاهر در اثر اشتباه چاپی به متن قانون راه یافته است.^۱

۱- آل محمد، فاطمه، همان منبع ص ۱۱۰.

از آنجا که مسئولیت کیفری اشخاص حقوقی مشمول کلیه جرایم رایانه‌ای مندرج در قانون جرایم رایانه‌ای می‌گردد و بزه جعل رایانه‌ای نیز یکی از آن جرایم می‌باشد لذا در خصوص بزه جعل رایانه‌ای نیز مسئولیت کیفری اشخاص حقوقی قابل تحقق می‌باشد.

بخش سوم: بررسی توصیفی مجازاتهای موجود در قوانین مربوط به بزه

جعل رایانه‌ای

هنگامی که جرم یعنی رفتاری ضد اجتماعی ارتکاب می‌یابد، حاکمیت عمومی وظیفه دارد با توسل به شیوه‌های مناسب و مؤثر ضمن پیشگیری از وقوع تکرار جرم در آینده لزوم احترام به احکام و دستورهای خود را بار دیگر به شهروندان گوشزد کند. هشدار مقامات به حفظ نظم عمومی و مراعات حقوق جامعه بیانی گوناگونی دارد که صورت مؤکد آن اجرایی مجازات است. لیکن مجازات، سزاوار کسانی است که پیش از آن مقصر و مسئول شناخته شده باشند. بنابراین نخستین گام، بررسی میزان تعهد مرتکب جرم به تبعیت از قانونگذار و پایبندی به اجرای دستورهای او است. واکنش اجتماعی بستگی تام به نتایج این تشخیص دارد. هرگاه مسئولیت او در قبال فعل مجرمانه به اثبات رسید به عقوبت عمل خود گرفتار خواهد شد، ولی اگر بزه‌کار قانوناً مسئول اعمال خود شناخته نشود، هر آینه مجازات او بیهوده خواهد بود.

برخورد یا مبارزه هر جامعه با جرایم موجود امری واضح و بدیهی است. مسأله جرایم رایانه‌ای هم از این قاعده بیرون نمی‌باشد و حتی می‌توان گفت به دلایل چندی مثل تراکم اطلاعات ذخیره شده، آسیب‌پذیری سیستم‌ها و ...، این مبارزه باید دقیق و شدیدتر هم باشد. از جمله این تدابیر برای مقابله با این دسته از جرایم، می‌توان به تدابیر کیفری اشاره نمود. پاسخ کیفری عبارت هستند از واکنش رسمی در برابر هر جرم «حقوق کیفری به

خاطر سامان‌دهی چنین پاسخی که شدیدترین شیوه کنترل محسوب می‌شود- از دیگر نظام‌های کنترل رسمی و غیررسمی متمایز شده است. کیفر با هر نظریه و هدفی توجیه شود جزء جدایی‌ناپذیر نظام کیفری است که باید در هر دعوایی که به اثبات مجرمیت و مسئولیت کیفری مرتکب یا مرتکبان می‌انجامد تعیین و اعمال شود.^۱

همانطور که می‌دانیم اصل فرعی بودن حقوق جزاء اقتضاء می‌کند، مقابله کیفری با تعرضات رایانه‌ای و به عبارت دیگر جرم‌شناختی این عمل و اعمال مجازات به عنوان آخرین راه حل صورت پذیرد و در درجه اول اقدامات غیر کیفری اولویت داشته باشند. گسترش جرایم رایانه‌ای در اغلب کشورها سبب گردید، نارسایی تدابیر غیر کیفری آشکار شود و بر همین اساس برخی از کشورها با استفاده از ابزارهای کیفری به عرصه مبارزه با تعرضات رایانه‌ای گام نهادند.

امروزه دیگر ضرورت به کارگیری تدابیر کیفری در خصوص این تعرضات، برکسی پوشیده نیست در همین راستا انجمن بین‌المللی حقوق جزاء توصیه‌های ذیل را ارائه می‌نماید:

«الف- توسعه فناوری انفورماتیک، منافع و ارزش‌های جدیدی را به وجود آورده است که مستلزم حمایت کیفری است. به ویژه برای حفظ تمامیت سیستم‌های انفورماتیک و داده‌ها و اطلاعاتی که در آن انباشته و نگاهداری می‌شود.

ب- با توجه به این که حقوق جزائی سنتی فاقد مقررات و اصولی در این زمینه می‌باشد، قوانین موجود باید اصلاح شوند و قوانین جدید وضع گردند.

۱- محمودی جانکی، فیروز، «نظام کیفردهی، هدف‌ها و ضرورت‌ها»، کتاب تازه‌های علوم جنایی، تهران، نشر میزان، چاپ اول، ۱۳۸۸ ص ۶۶۷.

ج- در هنگام وضع قوانین و مقررات جدید نیز باید به صراحت، دقت و تعریف جرایم در قالب عناصر عینی تأکید شود.

د- قلمروهای حقوقی مشابه حقوق جزاء، نیز باید به منظور اجتناب از تعارض قوانین، تقویت و تجدید شوند.^۱

همچنین ماده ۲۵، رهنمود شورای اروپا در حمایت از داده‌ها، مشعر به این است که: «هر دولت باید برای شخصی که مقررات ملی پذیرفته شده و به موجب این رهنمودها را به کار نمی‌بندد، پیش‌بینی‌هایی برای وضع مجازات‌های بازدارنده به عمل آورد.»^۲ پاسخ کیفری به هر جرم در قوانین کیفری معمولاً گوناگون و از نظر میزان متفاوت است. در اغلب موارد، امکان انتخاب یک یا چند نوع کیفر مختلف به دادرس داده شده است. برای نمونه، در قانون جرایم رایانه‌ای دادرسان معیر شده‌اند که از میان کیفرهای حبس و جزای نقدی، یک یا هر دو نوع را برگزینند. وانگهی، دادرسان باید میزان هر یک از این کیفرها را در محدوده مشخص شده در قانون برای هر مجرم تعیین کنند، با نگاهی به مواد قانون راجع به جعل رایانه‌ای در نظام کیفری ایران ملاحظه می‌کنیم که مجازات در نظر گرفته شده برای جعل رایانه‌ای در ماده ۶ قانون جرایم رایانه‌ای، حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال، هر دو مجازات می‌باشد و مجازات لحاظ گردیده در ماده ۵۸ قانون تجارت الکترونیکی، یک تا سه سال حبس و پنجاه میلیون ریال جزای نقدی بوده است و مجازات تعیین شده در ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح که نظر به مواد ۹۵، ۹۶، ۹۷، ۹۸، ۱۰۳، ۱۰۴ و ۱۰۶ آن قانون می‌باشد با توجه به مجازات لحاظ شده در مواد قانون اخیرالذکر به فراخور احوال، مجازات حبس می‌باشد.

۱- مجله تحقیقات حقوقی دانشگاه شهید بهشتی، شماره‌های ۱۶ و ۱۷، ص ۴۵۶.

۲- آتابوی و آدری هورتن، حمایت از داده‌ها «شورای اروپا» ترجمه: ناهید جعفرپور ص ۲۳.

از نظر سیر تحول تاریخی، ضمانت اجرای کیفری جرم جعل در حقوق ایران، در قوانین قبل از انقلاب عمدتاً حبس بوده است و در مقررات جاری، جزای نقدی نیز در برخی مصادیق به عنوان مجازات اصلی در نظر گرفته شده است.

جزای نقدی در زمره مجازاتهای تعزیری و اصلی و یا تضمینی است و بنا به تعریف عبارت است از الزام محکوم علیه به استناد حکم محکومیت و به پرداختن مبلغی وجه نقد به نفع دولت اصولاً در جرایمی که داعی و انگیزه مرتکب آنها کسب منفعت و سودجویی است مناسبتر چنین است که مرتکب به مجازات فانی تهدید شود و برای مرتکب این جرایم، جزای نقدی پیش‌بینی گردد که در مقایسه با حبس از کارایی بیشتری برخوردار بوده و معایب زندان را نیز ندارد و می‌تواند به عنوان جانشین مطمئن برای مجازات حبس عمل نماید.

همانگونه که دیدیم در قانون جرایم رایانه‌ای و در ماده ۶ آن که برای جعل رایانه‌ای جرم‌انگاری و تعیین مجازات گردیده است، مجازات جزای نقدی در کنار مجازات حبس پیش‌بینی شده است که قاضی مختار است با توجه به شدت جرم ارتكابی در سایر قرائن و احوال متهم را باید به مجازات حبس یا جزای نقدی یا هر دو مجازات محکوم کند. در مواردی که قاضی مختار است بین مجازات حبس یا جزای نقدی یکی را انتخاب کند، در صورت محکوم نمودن متهم به جزای نقدی، این انتخاب قاضی می‌تواند راهکاری برای اعمال سیاست حبس‌زدایی دانست. با این کار، فرد محکوم از معایب مجازات حبس در امان می‌ماند و هزینه‌ای اضافی به دولت تحمیل نشده بلکه مبلغی نیز به صندوق دولت واریز می‌شود.

باید بپذیریم که جزای نقدی در بعضی موارد می‌تواند کیفر مناسبی برای جعل رایانه‌ای باشد. چرا که در جعل رایانه‌ای همانند بعضی از جرایم رایانه‌ای چون کلاهبرداری مرتبط با رایانه و ... انگیزه مادی وجود دارد. بنابراین در آن‌جا که جزای نقدی پاسخ کیفری مناسبی به مجرمیتی «پول‌پرست» و جرایم ارتکاب یافته با انگیزه سودجویی است، می‌تواند در آن دسته از جرایم رایانه‌ای که با انگیزه مادی ارتکاب می‌یابند، مثر ثمر واقع شود.

همچنین از آنجا که در قانون جرایم رایانه‌ای که جعل رایانه‌ای به عنوان یکی از جرایم مندرج در این قانون می‌باشد، قانونگذار برای اشخاص حقوقی هم مسئولیت کیفری قائل شده است، جزای نقدی می‌تواند مجازات مناسبی برای جرایم رایانه‌ای ارتکابی این‌گونه اشخاص محسوب شده و حتی جنبه بازدارندگی داشته باشد.

نکته مثبتی که قانونگذار در تصویب قانون جرایم رایانه‌ای به آن توجه داشته است، پیش‌بینی ماده ۵۳ می‌باشد. در این ماده چنین مقرر شده است: «میزان جزای نقدی در این قانون بر اساس نرخ تورم حسب اعلام بانک مرکزی هر سه سال یک بار به پیشنهاد رئیس قوه قضائیه و تصویب هیأت وزیران قابل تغییر است.» از آنجا که یکی از مجازات‌ها ملحوظ شده برای جعل رایانه‌ای، جزای نقدی می‌باشد لذا حکم مندرج در ماده ۵۳ قانون جرایم رایانه‌ای به جعل رایانه‌ای نیز قابل حصری است. پیش‌بینی این ماده در قانون باعث می‌شود که با توجه به نرخ تورم میزان جزای نقدی این قانون تغییر کرده و این نوع مجازات همواره اثر تسریعی و ارعابی خود را حفظ کند.

در خصوص مجازات حبس لحاظ شده برای بزه جعل رایانه‌ای در قانون جرایم رایانه‌ای باید اذعان نمود که قانونگذار در تصویب این قانون نظر به سیاست سخت‌گیرانه در مبارزه با جعل رایانه‌ای به عنوان یکی از جرایم رایانه‌ای داشته است و بنابراین یکی از مجازات‌ها برای جعل رایانه‌ای مجازات حبس می‌باشد.

در ماده ۲۶ این قانون، در خصوص تشدید مجازات چنین مقرر شده است:

«در موارد زیر، حسب مورد مرتکب به پیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) هر یک از کارمندان و کارکنان اداره و سازمان یا شوراهای و شهرداری‌ها و مؤسسه‌ها و شرکت‌های دولتی و وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به طور کلی اعضاء و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسب انجام وظیفه مرتکب جرم رایانه‌ای شده باشند.

ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد.

ج) داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادهای و مراکز ارائه دهنده خدمات عمومی باشد.

د) جرم به صورت سازمان یافته ارتکاب یافته باشد.

ه) جرم در سطح گسترده‌ای ارتکاب یافته باشد.»

در ماده ۲۷ قانون جرایم رایانه‌ای آمده است: «در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نود و یک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.»

همانگونه که ملاحظه کردیم قانونگذار در قانون جرایم رایانه‌ای با وضع کردن مواردی در خصوص تشدید مجازات و تکرار جرم سعی بر آن داشته است در جرم‌انگاری جعل رایانه‌ای همانند سایر جرائم رایانه‌ای در نظر گرفته در این قانون و تعیین مجازات، از قوانینی راجع به جعل سنتی عقب نمانده و آن را به نحوی کامل نشان دهد اما با این وجود مواد قانون موصوف واحد ایراداتی می‌باشند. که در گفتار بعدی بدان اشاره می‌نماییم. مجازات اصلی جرم جعل رایانه‌ای به موجب ماده ۶۸ قانون تجارت الکترونیکی، ترکیبی از جنس و جزای نقدی اعلام شده است، که توأماً مورد حکم قرار می‌گیرد. مرتکب جرم جعل علاوه بر پرداخت جزای نقدی به مبلغ پنجاه میلیون ریال جزای نقدی ثابت، به یک تا سه سال حبس نیز محکوم می‌گردد. به علاوه دادگاه می‌تواند حسب شدت جرم و خصوصیات مجرم، نسبت به صدور مجازاتهای تتمیمی موضوع ماده ۱۹ قانون مجازات اسلامی، اقدام نماید.

ملاحظه می‌شود که مجازات این جرم، در مقایسه با جعل در مفهوم سنتی، ملایم‌تر تعیین شده است، ولی رویکرد قانونگذار همچنان بر تعیین مجازات سالب آزادی در خصوص جرم استوار است، که نشانگر شدت جرم و اهمیت حمایت از جامعه در برابر ارتکاب چنین جرایمی است. به نظر می‌رسد، قانونگذار امیدوار است تا با بهره‌گیری از ارباب ناشی از اعمال مجازات سالب آزادی، با گسترش روزافزون این پدیده مجرمانه مبارزه نماید.

شروع به این جرم نیز قابل مجازات است و دادگاه می‌تواند، مرتکب را به حداقل مجازات حبس مقرر در ماده ۶۸ قانون تجارت الکترونیکی، محکوم نماید و برای مدت یکسال از وی سلب آزادی نماید.

نهایتاً اینکه مجازات جرم جعل رایانه‌ای در قانون مجازات جرائم نیروهای مسلح صرفاً مجازات حبس می‌باشد و قانونگذار به این یک نوع مجازات بسنده نموده است و از امتیازاتی که در نفی مجازات جزای نقدی که برای جعل رایانه‌ای بر شمردیم محروم مانده است و در نگاه انتقادی در گفتار بعدی به این موضوع اشاره خواهیم نمود. بانگاهی به مواد قانونی راجع به جعل رایانه‌ای در حقوق ایران و مواردی که مطرح نمودیم مشخص گردید که مجازاتهای در نظر گرفته شده منحصر به حبس و جزای نقدی برای این نوع بزه می‌باشد. قابل توجه است که مجازات شلاق و اعدام برای این جرم در نظر قانونگذار نبوده است چرا که این دو مجازات در اینگونه جرایم که جنبه اصلاحی و ارعابی خود را از دست می‌دهند و همچنین تعیین مجازات شلاق و اعدام در جرایم رایانه‌ای برخلاف اصل تناسب جرم و کیفر، می‌باشد. بنابراین قانونگذار این دو مجازات را لحاظ ننموده است.

بخش چهارم: بررسی انتقادی مجازاتهای موجود در قوانین مربوط به بزه جعل رایانه‌ای

الف- بررسی انتقادی مجازات جعل رایانه‌ای در قانون جرایم رایانه‌ای

«فضایی حاکم به قانون جرایم رایانه‌ای، کیفرگذاری‌های تشدید و سنگینی است که حاکی از به کارگیری سیاست کیفری سخت‌گیرانه‌ای نسبت به جرایم رایانه‌ای دارد که امروزه به عنوان «تسامح صفر» در برخی از نظام‌های حقوقی (مانند نظام عدالت جنایی آمریکا) شناخته می‌شود. یعنی عدم چشم‌پوشی حتی نسبت به کوچک‌ترین تخلف‌ها، زیرا

به زعم سیاست‌گذاران، گذشت از این تخلف‌ها خود می‌تواند زمینه‌ساز جرم‌های مهمتری باشد که در نهایت، امنیت ملی را به خطر می‌اندازد.^۱ به همین دلیل قانونگذار در این قانون به کیفرگذاری‌های سنگینی پرداخته است و حتی فصل مستقلی از این قانون را به تشدید کیفر اختصاص داده است. باید گفت از نظر گاه سیاست جنایی، جرم‌انگاری‌ها و کیفرگذاری‌های قانون جرایم رایانه‌ای نشان‌دهنده حمایت از ارزش‌های جدیدی در جامعه ایران است که پدیده‌ای به نام رایانه آن را اقتضا می‌کند. با مقایسه بین جعل رایانه‌ای در قانون جرایم رایانه‌ای و جعل سنتی ملاحظه می‌کنیم که قانونگذار برای مجازات جعل رایانه‌ای آنگونه که در جعل سنتی قائل به تفکیک گردیده است که در موضوع جرم به صورت رسمی قلمداد گردیده و یا به صورت عادی تلقی شده است هیچگونه تفکیکی قائل نشده است و به تعبیر دیگر تفاوتی بین مجازات در جعل رایانه‌ای داده‌های رسمی و داده‌های عادی وجود ندارد که به نظر می‌رسد با توجه به اهمیت موضوع جرم می‌بایست به این نکته توجه می‌گردید. ممکن است در پاسخ بگوییم قانونگذار در ماده ۲۶ این قانون و در مبحث تشدید مجازات به نوعی قائل به تفکیک گردیده است و در مورد داده‌های سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه‌دهنده خدمات عمومی با مجازاتی به بیش از دو سوم حداکثر یک یا دو مجازات در ماده ۶ قانون جرایم رایانه‌ای قائل به تفاوت گردیده است. ولی در پاسخ می‌گوییم که اگر قانونگذار قائل به تعیین مجازات به بیشتر از حداکثر تعیین گردیده در ماده ۶ قانون جرایم رایانه‌ای می‌گردیده پاسخ داده شده صحیح بود ولی حال که قائل به تعیین مجازات کمتر از حداکثر تعیین شده در ماده ۶ قانون جرایم رایانه‌ای گردیده است پاسخ داده شده صحیح نمی‌باشد چه آنکه اختیار قاضی پرونده با موضوع جعل رایانه‌ای در حدی می‌باشد که می‌تواند برای

۱- رابحیان اصلی، مهرداد، «قانون جرایم رایانه‌ای با نوآوری‌ها و کاستی‌ها»، مجله پژوهش‌های حقوقی، شماره ۱۵.

جعل داده‌هایی که متعلق به دولت نباشد مجازاتی تعیین کند که بیشتر از مجازات لحاظ شده برای جعل داده‌هایی باشد که متعلق به دولت و به تعبیری رسمی باشد و این موضوع ما را به تفکیک جعل داده رسمی و جعل داده عادی در مجازات نمی‌رساند. ایراد دیگری که در بحث مجازات در ماده ۶ قانون جرایم رایانه‌ای با آن روبرو هستیم این است که ما گفتیم قانونگذار در تعیین مجازات در قانون جرایم رایانه‌ای به سیاست سخت‌گیرانه، نظر داشته است و طبیعتاً می‌بایست مجازات لحاظ شده در جعل رایانه‌ای سنگین‌تر 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 با ملاحظه برخی از جرم‌انگاریها و کیفرگذارها در جعل سنتی می‌بینیم که مجازاتهای در نظر گرفته که در جعل سنتی از مجازاتها مربوط به جعل رایانه‌ای شدیدتر است و این با سیاست کیفری مربوط به جرایم رایانه‌ای در تضاد می‌باشد.

همانگونه که در بند الف ماده ۲۶ قانون جرائم رایانه‌ای گفته شد، تشدید در صورتی اعمال می‌شود که کارمند، جرم رایانه‌ای را به مناسبت انجام وظیفه مرتکب شده باشد. اما مسأله این است که هیچ یک از جرایم رایانه‌ای را نمی‌توان به واسطه انجام وظایف قانونی مرتکب شد. به نظر می‌رسد منظور واقعی مقنن این باشد که افراد مذکور سوءاستفاده از امکانات و اختیاراتی که برای انجام وظایف قانونی در حیطه کاری خود دارند، مرتکب جرم رایانه‌ای شوند.

«در این ماده از دو اصطلاح جرم سازمان یافته و گسترده استفاده شده است که نسبت به این دو ابهام وجود دارد. چرا که در کشور ما تا کنون قوانین و مقررات شکلی ماهوی

مدونی در رابطه با جرایم سازمان یافته به تصویب نرسیده است.^۱ لذا قضات، حقوقدانان، وکلای دادگستری و ... تفسیرهای متعدد و بعضاً متفاوتی از ارتکاب جرم به صورت سازمان یافته به عمل می‌آورند که این امر عواقب زیانباری را در پی خواهد داشت. «حال باید بررسی نمود منظور از ارتکاب جرم در سطح گسترده چیست؟ هر جرمی که در فضای سایر اتفاق افتد به دلیل گسترده بودن فضای اینترنت در سطح جهان، یک جرم گسترده‌ای می‌باشد. در حال حاضر با وجود فناوریهای نوین و به کارگیری ابزارهای پیشرفته نیز تعیین دامنه، وسعت و گستردگی چنین مواردی امکان‌پذیر نمی‌باشد. جرم سازمان یافته از اصطلاح‌های کلیدی جرم شناختی است و یکی از گونه‌های برجسته جرم‌های بازرگانی یا اقتصادی به شمار می‌رود. ولی، تعبیر مبهم جرم گسترده که تاکنون سابقه‌ای در قانونگذاری‌ها نداشته است، بیشتر که حاکی از شدت جرم ارتكابی است و تمایز مشخص با جرم سازمان یافته ندارد. زیرا جرم سازمان یافته نیز به اعتبار ویژگی «فراملی بودن»، در سطح گسترده‌ای قابل ارتکاب است.»^۲

همانگونه که در ماده ۲۷ قانون جرایم رایانه‌ای و در مبحث تکرار جرم بیان کردیم کیفرهای مقرر در این ماده با واقعیات جهان امروز منطبق و سازگار است و نشان دهنده شتاب زدگی قانونگذار در تصویب این ماده می‌باشد. چرا که در جهان کنونی، افراد قادرند به راحتی از اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی و حتی در صورتی که به حکم دادگاه آنها را از خدمات مذکور محروم نمایند، می‌توانند بسادگی از امکانات بستگان و اطرافیان نزدیک خود بهره ببرند و یا حتی

- حتی در معاهده سال ۲۰۰۰ - پالرمو - که نماینده ایران آن را امضاء نموده است، سیر مراحل قانونی تصویب در^۱

مجلس شورای اسلامی را تا کنون طی ننموده است

- آل‌محمد، فاطمه، پایان‌نامه سیاست جنایی ایران در قبال جرایم رایانه‌ای، دانشکده حقوق و علوم سیاسی دانشگاه^۲

شیراز، فرودین ۱۳۹۰ ص ۲۶.

از خدمات کشورهای دیگر استفاده نمایند. بهتر بود قانونگذار در تعیین مجازات‌های این فصل توجه و دقت بیشتری را مبذول می‌داشت.

ب- بررسی انتقادی مجازات جعل رایانه‌ای در قانون تجارت الکترونیکی

مجازات جعل رایانه‌ای در این قانون برای انواع آن یک تا سه سال حبس و پنجاه میلیون ریال جزای نقدی است. در تبصره ماده نیز برای شروع جرم حداقل مجازات مندرج در ماده ۶۸ یعنی یک سال حبس و پنجاه میلیون ریال جزای نقدی مقرر شده است. با توجه به اهمیت این جرم و تنوع مواد قانونی جعل سستی در قانون مجازات اسلامی که مجازات‌های متنوعی برای اقسام آن در نظر گرفته شده است، شایسته بود که در این مورد نیز حداقل کیفیات مشدده‌ای برای برخی گونه‌های خاص - برای مثال، جعل امضاءهای الکترونیکی مطمئن، جعل امضاءهای الکترونیکی وزیران، شرکت‌های دولتی و امثال آن - در نظر گرفته می‌شد و این امر از جمله ایرادات وارده به این قانون می‌باشد.

ج- بررسی انتقادی مجازات جعل رایانه‌ای در قانون مجازات جرائم

نیروهای مسلح

ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح شامل چندین جرم رایانه‌ای و ناظر به تعدادی دیگر از مواد قانونی مزبور است، متأسفانه این قانونگذاری در مورد تمام قوانین مربوط به جرائم رایانه‌ای که تاکنون توسط مجلس شورای اسلامی وضع شده‌اند، مشاهده می‌شود. یکی از مسائل بسیار مهم که کمیته منتخب جرائم رایانه‌ای شورای اروپا بر آن توصیه و تأکید نموده است، رعایت اصول قانونگذاری است. کمیته مزبور به کشورهای عضو پیشنهاد کرده است که ۶ اصل اساسی را در هنگام وضع قوانین مربوط به جرائم رایانه‌ای مورد توجه قرار دهند. «بر اساس اصل دقت و صراحت در نحوه بیان قوانین،

مقررات کیفری باید رفتارهای ممنوع را به دقت شرح دهند و از مفاد و شرایط کلی و مبهم پرهیز کنند و بر اساس اصل وضوح اعمال جرم شناخته شده، باید به وضوح توصیف شوند و از به کارگیری بیش از حد روش ارجاع به مواد قانونی دیگر حتی الامکان اجتناب شود.^۱

این نحوه قانونگذاری دارای اشکالات زیادی است. چه اینکه «اصل قانونی بودن جرم و مجازات» به عنوان یکی از اصول حقوقی بسیار مهم که مورد تأکید قانون اساسی جمهوری اسلامی ایران نیز می‌باشد، نه تنها برای مراجع قضایی بلکه برای قانونگذار نیز، تکالیفی را ایجاد می‌کند. اقتضای اصل قانونی بودن جرم و مجازات این است که قانونگذار عناصر قانونی، مادی و معنوی هر جرم را به طور واضح و شفاف و بدون هرگونه ابهام، به طور مجزا بیان کند و از کلی گویی در امور کیفری خصوصاً در مسائل ماهوی کیفری پرهیزد، عمل به این تکلیف توسط قانونگذار باعث می‌شود که شهروندان قانون را بهتر درک کنند و در نتیجه اثر بازدارندگی قانون از ارتکاب جرم افزایش خواهد یافت. قانون کلی و غیر شفاف، مراجع قضایی را وادار به قیاس و عدم رعایت اصل قانونی بودن جرم و مجازات می‌نماید.

متأسفانه قانونگذار در ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح به وظیفه اساسی خود عمل نکرده و خواسته است که با یک ماده کلی تکلیف همه جرائم رایانه‌ای را که توسط کارکنان نیروهای مسلح ارتکاب می‌یابند، مشخص نماید، به هر حال قضات دادرها و دادگاههای نظامی خصوصاً مراجع عالی قضایی که نظارت بر حسن اجرای قانون را برعهده دارند، باید به نحوی ماده مذکور را تفسیر نمایند که از اصل قانونی بودن جرم و مجازات تخطی نشود.

-دزیانی، محمد حسن، جزوه جرائم حمایت از داده‌ها، سازمان مدیریت و برنامه‌ریزی، دبیرخانه شورای عالی^۱
انفورماتیک، ص ۲۰، ۱۳۷۸.

از جمله ایرادات دیگری که در مجازات جعل رایانه‌ای در این قانون وارد است این می‌باشد که قانونگذار فقط به مجازات حبس برای جعل رایانه‌ای بسنده کرده است و از امتیازاتی که در تعیین مجازات جزای نقدی برای جعل رایانه‌ای وجود داشته است بی‌بهره مانده است. زیرا همانگونه که گفتیم چون در جعل رایانه‌ای، انگیزه مادی برای مرتکب وجود داشته است لذا در نظر گرفتن جزای نقدی برای مجازات اینگونه مرتکبین در واقع کیفر مناسب بوده است که این امر از نظر قانونگذار دور مانده است.

بخش پنجم: بررسی صلاحیت کیفری در جعل رایانه‌ای

صلاحیت کیفری عبارت از شایستگی و اختیاری که به موجب قانون برای مراجع جزایی جهت رسیدگی به امور کیفری واگذار شده است. از این مفهوم ساده چنین استنباط می‌شود که کلیه قواعد و مقررات مربوط به صلاحیت آمره هستند و از آنجا که جلوه‌ای از اقتدار حاکمیت را به نمایش می‌گذارند، اعمال آنها در راستای برقراری نظم عمومی است. فلذا هیچ‌گونه تغییری مطابق اراده فردی در آن ایجاد نمی‌شود. در این گفتار صلاحیت کیفری بزه جعل رایانه‌ای را به عنوان یکی از جرائم رایانه‌ای هم در فضای بین‌المللی و هم در محاکم کیفری داخلی بررسی می‌کنیم.

الف- صلاحیت کیفری جعل رایانه‌ای در فضای بین‌المللی

مراد از صلاحیت در این بند، صلاحیت کیفری بین‌المللی به مفهوم عام می‌باشد و عبارت است از «شایستگی دادگاههای ملی یا بین‌المللی در رسیدگی به جرائمی که به علت وجود یک یا چند عنصر خارجی در موضوع صلاحیت یا مرجع صلاحیتدار در حوزه صلاحیت

بین‌المللی قرار می‌گیرد.^۱ «در رسیدگی به جرم جعل رایانه‌ای همانند سایر جرایم رایانه‌ای، قواعد سنتی صلاحیت به طور اساسی دچار چالش شده است.»^۲ تعامل و ادغام این قواعد و قوانین مربوط، ممکن است کاربران اینترنتی را با احتمال مجرم بودن در هر حوزه دارای صلاحیتی که با اینترنت در ارتباط است، روبه‌رو کند. همچنین ماهیت اینترنت امکان ارتباط متقابل میان چند حوزه قضایی را فراهم کرده و رکن‌های یک جرم ممکن است نه تنها در مکان و حوزه‌ای با حضور فیزیکی مجرم شروع شده یا به ثمر رسیده باشند، بلکه این امکان نیز هست که در همه‌ی حوزه‌های دیگر که در اثر عملکرد کاربر به شکل الکترونیکی درگیر شده‌اند، نیز بحث ارتکاب جرم مطرح باشند.

به طور کلی، قانونگذار در چهار حالت، نسبت به فعالیت‌های ارتكابی، صلاحیت کیفری اعمال می‌کند که عبارتند از (۱) محل ارتکاب فعل (۲) تابعیت (۳) حمایت از امنیت و منافع ملی

۴) اجماع جهانی

در ادامه به ترتیب به بررسی آنها می‌پردازیم.

۱- محل ارتکاب جرم

چنانچه تمام یا بخش اساسی از عنصر مادی بزه جعل رایانه‌ای در داخل قلمرو و سرزمین ارتکاب یابد، قانونگذار در راستای اعمال حاکمیت بر قلمرو خود نسبت به آن جرم‌انگاری خواهد کرد. این اصل که به اصل سرزمینی بودن صلاحیت موصوف می‌باشد بیشتر از

-فروغی، فضل‌اله، تقریرات درس حقوق جزای بین‌الملل، کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه^۱

شیراز، ۸۹.

-پاکزاد، بتول، (۱۳۸۸) تروریسم سایبری، رساله دکتری در رشته حقوق کیفری و جرم‌شناسی دانشگاه شهید بهشتی،^۲

ص ۸۴

جانب کشورهای تابع نظام حقوق عرفی مورد توجه قرار گرفته است. برطبق اصل سرزمینی بودن هر دولتی محق است صلاحیت خود را برای تمامی اعمالی که در سرزمین آن دولت ارتکاب می‌یابد اعمال کنند. تفسیر و اجرای این حق، مسایل متنوعی را بدنبال دارد. مسأله مربوط می‌شود به اینکه جرم در کجا ارتکاب یافته است و عوامل فراسرزمینی چگونه باید مدنظر قرار گیرند. «بسیاری از کشورها مکان ارتکاب را بر مبنای دکترین ubiquity (حضور در همه جا) تعیین می‌کنند. طبق این دکترین، جرم اگر چه فقط بخشی از آن در یک مکان ارتکاب یافته باشد، تماماً ارتکاب یافته در آن محل فرض می‌شود، بدین ترتیب طبیعی است چند دولت خود را صالح به رسیدگی بدانند.»^۱

مبنایی ترین و قدیمی ترین قاعده‌ای که برای اعمال قوانین جزایی مورد استناد حاکم کیفری قرار می‌گیرد، صلاحیت سرزمینی است. به عقیده برخی صاحب‌نظران مبنای پذیرش این اصل این است که «حاکمیت سرزمین قدرتمندترین منفعت، مؤثرترین امکانات و راحت‌ترین وضعیت را برای مقابله با جرایمی که در قلمرو سرزمین ارتکاب می‌یابند فراهم می‌کند.»^۲

ولی مسأله مهم اینجا است که با توجه به ماهیت جرم‌های اینترنتی و از جمله جعل رایانه‌ای، محل ارتکاب جرم یا محل حصول نتیجه جرم (در صورت تعدد محل‌های ارتکاب)، آشکار نیست که کدام حوزه صالح به رسیدگی خواهد بود و اگر چند کشور درگیر چنین جرم‌هایی شده باشند، این که کدام کشور صالح به رسیدگی خواهد بود، موضوع بحث است. پس می‌توان اولین چالش در زمینه صلاحیت رسیدگی جرم جعل رایانه‌ای را عدم

^۱، ترجمه دبیرخانه شورای عالی R - شورای اروپا، جرم کامپیوتری (استراسبورگ ۱۹۹۰) توصیه نامه ۸۹/۰۲/۷ (۹)، انفورماتیک سازمان برنامه و بودجه کشور، ۱۳۷۶، ص ۱۵۳.

^۲ - August Ray, International Cyber- Jurisdiction A Comparative Analysis, American Business Law Journal, 2002, P. 530.

لحاظ قابلیت تشخیص محل جغرافیایی یک سیستم رایانه‌ای متصل به شبکه دانست و چالش بعدی زمانی باعث بروز مشکل می‌شود که بین چند کشور تعارض مثبت صلاحیتی حادث گردد.

در کشور ما نیز این اصل پذیرفته شده است در ماده ۳ قانون مجازات اسلامی، مصوب ۱۳۷۰ چنین آمده است: «قوانین جزایی در مورد کلیه کسانی که در قلمرو و حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران مرتکب جرم شوند، اعمال می‌گردد، مگر آنکه به موجب قانون ترتیب دیگری مقرر شده باشد.»

به موجب قانون جرایم رایانه‌ای، فصل یکم از بخش دوم این قانون به صلاحیت جرائم رایانه‌ای و بویژه جعل رایانه‌ای به عنوان یکی از این جرائم اختصاص داده شده است. به موجب بندهای الف و ب ماده ۲۸ قانون آئین دادرسی کیفری ما با صلاحیت سرزمینی روبرو هستیم.

در ماده ۲۸ این قانون چنین پیش‌بینی شده است:

«علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاههای ایران در موارد زیر صالح به رسیدگی خواهند بود.

الف) داده‌های محرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته است به هر نحو در سامانه‌های رایانه‌ای و مخبراتی یا حامل‌های داده‌ی موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب) جرم از طریق تارنماهای (وب سایت‌های) دارای دامنه مرتبه بالایی در کشوری ایران

ارتکاب یافته باشد.»

بند «الف» با مبنا قرار دادن قلمرو حاکمیتی ایران، مستند به قانون مجازات اسلامی محل استقرار سیستمهای رایانه‌ای یا مخابراتی یا حامل‌های داده را مورد توجه قرار داده است و بند «ب» قلمرو حاکمیتی سایبری ایران را ترسیم می‌کند که عبارت است از: دامنه‌ی ir یا آنچه در آینده نزدیک با عنوان ایران عرضه خواهد شد.

۲- تابعیت

در اینجا قانونگذار کیفری به جای تأکید بر قلمرو سرزمینی اعتباری خود که مطابق قوانین بین‌المللی به رسمیت شناخته شده است، اتباعش را هدف قرار می‌دهد. لذا دیگر تفاوتی نمی‌کند که آن فعل سرزنش‌آمیز جرم‌انگاری شده، در کدام نقطه از کره خاکی ارتکاب یافته است. این اصل بیشتر از جانب کشورهای تابع نظام حقوق نوشته مورد توجه قرار گرفته است. این اصل که به صلاحیت شخصی موسوم می‌باشد بر اساس تابعیت مجرم استوار است.

همچنین گاهی اوقات، قانونگذار کیفری تصمیم می‌گیرد در راستای اجرای شایسته عدالت، حوزه صلاحیتی تابعیتی کیفری را به قربانیان جرایم نیز تسری دهد. اما از آنجا که این اقدام چندان با اقبال مواجه نشده است، از آن به صلاحیت تابعیتی منفعل یاد می‌شود که در مقابل صلاحیت تابعیتی فعال که نسبت به مرتکبین جرایم مصداق دارد قرار می‌گیرد. در پایان، قانون مجازات اسلامی کشورمان در ماده ۷ خود راجع به صلاحیت تابعیتی فعال چنین مقرر کرده است: «علاوه بر موارد مذکور در موارد ۵ و ۶ هر ایرانی که در خارج ایران مرتکب جرمی شود و در ایران یافت شود طبق قوانین جزایی جمهوری اسلامی ایران مجازات خواهد شد.»

با نگاهی به مبحث صلاحیت در خصوص جرائم رایانه‌ای و من جمله جعل رایانه‌ای می‌بینیم که این قانون در مسأله صلاحیت شخصی سکوت اختیار کرده است، علیهذا می‌توان از عموماً مبحث صلاحیت در قانون مجازات اسلامی و آنچه که در ماده ۷ این قانون بیان کردیم استفاده کنیم: بدین نحو که هر ایرانی که در خارج از ایران مرتکب جعل رایانه‌ای شود و در ایران یافت شود طبق قوانین جزایی جمهوری اسلامی ایران مجازات خواهد شد.

۳- حمایت از امنیت و منافع ملی

کشورهای تابع نظام حقوق نوشته برای اعمال صلاحیت کیفری خود به قاعده دیگری نیز متوسل می‌شوند و آن در جایی است که یک فعل سرزنش‌آمیز امنیت و منافع ملی کشور را تهدید کند. البته این سخن به این معنا نیست که کشورهای تابع نظام عرفی به آن متوسل نشوند، اما میزان آنکا متفاوت است. به هر حال، این اصل در جایی نظر قانونگذار کیفری را به خود جلب می‌کند که قربانی فعل سرزنش‌آمیز دولت یا حتی خود حاکمیت باشد.

به لحاظ اهمیت این مسأله در قوانین کشورهای دیگر نه محل ارتکاب فعل و نه تابعیت مرتکب مورد توجه قرار گرفته است و در واقع هر کسی در هر جای دنیا چنین اعمالی را مرتکب شود، تحت شمول قوانین جزایی قرار خواهد گرفت. علیهذا اصل صلاحیت واقعی بر اساس حمایت از منافع حیاتی و ملی یک کشور استوار است و طبق این اصل یک کشور می‌تواند در مورد جرایم ارتكابی در خارج از کشور که امنیت ملی را به خطر می‌اندازد صلاحیت خود را اعمال کند.

ماده ۵ قانون مجازات اسلامی مصوب ۱۳۷۰ ناظر به اصل صلاحیت واقعی می‌باشد. در خصوص بزه جعل رایانه‌ای به عنوان یکی از جرایم رایانه‌ای باید خاطر نشان ساخت که بند

«ج» ماده ۲۸ قانون جرایم رایانه‌ای ناظر به صلاحیت واقعی یا حمایتی است. به موجب این بند از جمله مواردی که دادگاه‌های ایران صالح به رسیدگی می‌باشد عبارت از امنیت که «جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای (وبسایت‌های) مورد استفاده تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت و یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد باید تارنماهای (وبسایت‌های) دارای دامنه بالای کد کشوری ایران در سطح گسترده، ارتکاب یافته باشد.»

قید ایرانی در این بند زائد به نظر می‌رسد و اشاره قانونگذار به ایرانیان از باب تأکید بوده است زیرا این بند ناظر به صلاحیت حمایتی می‌باشد و نه صلاحیت شخصی. موارد مشمول حمایت این ماده را می‌توان دو گزینه دانست: ۱- سیستم‌های رایانه‌ای و مخابراتی ۲- وبسایت‌های این موارد باید مورد استفاده یا تحت کنترل مراجع مذکور در این بند باشند.

۴- اجماع جهانی

در نهایت گروهی از افعال هستند که فارغ از هر چیز، در راستای حمایت از جامعه ملل و برای اینکه یک اقدام سرزنش‌آمیز جهانی محسوب می‌شوند، از سوی قانونگذاران کیفری مورد توجه قرار گرفته‌اند. البته این نکته به این معنا نیست که چنین افعالی در قوانین داخلی جرم‌انگاری شوند، بلکه تنها جایی است که می‌توان گفت جرم‌انگاری از حوزه حاکمیت و قلمرو سرزمینی کشورها فراتر رفته و در واقع این مهم را حقوق بین‌المللی به عهده گرفته است. البته پرواضح است که موارد بسیار خاص و در عین حال قابل توجهی را در بر می‌گیرد. تا اجماع جهانی در رابطه با آنها وجود داشته باشد.

به عبارت دیگر «یکی از اصول حاکم بر صلاحیت کیفری در حقوق کیفری بین‌المللی، اصل صلاحیت جهانی است. مفهوم این اصل در واقع توسعه صلاحیت دادگاه‌های داخلی یک کشور برای رسیدگی به جرمی است نه در قلمرو کشور رسیدگی کننده واقع شده است، نه متهم تبعه آن کشور است و نه مجنی علیه یا زیان دیده و نه جرم علیه آن کشور ارتکاب یافته است. به تعبیری جرم از جرائم مهم بین‌المللی است که نگرانی جامعه بین‌المللی را برانگیخته و دولتها می‌توانند بدون هیچ یک از این پیوندها یا عوامل وابسته (مانند محل وقوع جرم، تابعیت و ...) به آن رسیدگی نمایند.»^۱

در این رابطه، ماده ۸ قانون مجازات اسلامی کشورمان چنین اشعار می‌دارد: «در مورد جرایمی که به موجب قانون خاص یا عهود بین‌المللی مرتکب در هر کشوری که به دست آید محاکمه می‌شود اگر در ایران دستگیر شد طبق قوانین جمهوری اسلامی ایران محاکمه و مجازات خواهد شد.»

در بند «د» ماده ۲۸ قانون جرایم رایانه‌ای که ناظر به همه جرائم رایانه‌ای و من جمله جعل رایانه‌ای می‌باشد، صلاحیت جهانی با رویکرد حمایتی از اشخاص زیر ۱۸ سال پذیرفته شده است. به موجب این بند از جمله مواردی که دادگاه‌های ایران صالح به رسیدگی می‌باشند عبارت از اینست که «در جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب یا بزه دیده ایرانی یا غیرایرانی باشد.»

در این بند «در راستای تقویت هر چه بیشتر صلاحیت جهانی کشورمان، هرگونه قید بزهکاری یا بزه دیدگی کودکان و همچنین تابعیت آنها برچیده شده است. به این

۱- فروغی، فضل‌اله، مقاله منشأ و ماهیت حقوقی اصل صلاحیت جهانی، مجله علمی و پژوهشی مطالعات حقوقی^۱
دانشگاه شیراز، دوره اول، شماره سوم، زمستان ۸۸، ص ۲۲.

ترتیب می‌توان ادعا کرد که با توجه به این بند، کشور ما به کلی یکی از پیشگامان حمایت از حقوق کودکان در فضای سایبر تبدیل شده است.^۱

«در حالی که اجرای کامل قواعد سنتی صلاحیت در فضای جدید سایبر امکان‌پذیر نیست، در همین راستا برخی دانشمندان و نویسندگان تئوری‌های جدیدی را از قبیل «تئوری فضای سایبر به عنوان یک فضای آزاد بین‌المللی» که هم عرض با سایر فضای بین‌المللی دیگر از قبیل دریاها، آزاد و ماورای جو و قطب‌ها باشد، «تئوری دادگاه دیجیتالی یا سایبری» که به صورت مجازی به تمام جرائم ارتكابی در فضای مذکور رسیدگی می‌کند و یا تئوری حداقل ارتباط لازم و یا به عبارتی داشتن ارتباط منطقی جرم با یک کشور، با ادعای سازگاری بودن آنها با فضای سایبر، مطرح کرده‌اند که هر کدام از زاویه‌ای دارای ایراد و چالش می‌باشد. بدین توضیح که تئوری اول بیشتر ناظر به وب سایتهاست که فقط حدود یک پنجم از موضوع‌های فضای سایبر را تشکیل می‌دهند و در مورد تئوری دوم باید گفت اولاً تا زمان ایجاد دادگاه مذکور، این تئوری قابلیت اجراء ندارد. ثانیاً یک تئوری آرمان‌گرایانه و ایده‌آلی است و عملاً اجرای آن خیلی سخت است و در صورت تشکیل هم نسبت به جرائم خیلی محدود و معدودی می‌تواند اجراء شود و قدرت پاسخگویی به اکثر جرائم را ندارد. به نظر می‌رسد، با عنایت به مشکل و غیرقابل تشخیص بودن محل وقوع جرم در فضای سایبر بهترین نوع صلاحیت، صلاحیت مبتنی بر ارتباط منطقی میان جرم و یک دولت باشد. در این صورت باید تئوری مذکور را به عنوان اصل در راستای تشخیص صلاحیت مراجع قضایی دانست و سایر تئوری‌ها که در راستای تعیین

۱- امیر حسین جلالی فراهانی، «صلاحیت کیفری سایبری در پرتو قوانین داخلی»، حقوق فناوری اطلاعات و ارتباطات، تهران، انتشارات روزنامه رسمی جمهوری اسلامی ایران، چاپ اول، ۱۳۸۸، ص ۴۰۴.

مکان وقوع جرم مطرح شده‌اند می‌توانند در خدمت این تئوری جهت تعیین حداقل ارتباط لازم و منطقی میان یک مکان و جرم واقع به کار گرفته شوند.^۱

ب- صلاحیت کیفری جعل رایانه‌ای در محاکم کیفری داخلی

آنچه در این قسمت به عنوان بخش پایانی این گفتار خواهد آمد، مقرراتی است که اقدامات شکلی و یا همان آئین دادرسی، ضابطه‌مند می‌سازد و به طور خاص محاکم را مخاطب قرار می‌دهد. در ادامه به ترتیب صلاحیت محلی و ذاتی پرونده‌های جعل رایانه‌ای بررسی خواهند شد.

۱- صلاحیت محلی

به تبعیت از صلاحیت سرزمینی، محل وقوع جرایم ملاک اصلی اعطای صلاحیت به محاکم داخلی است. علاوه بر بند الف ماده ۵۱ قانون آئین دادرسی دادگاههای عمومی و انقلاب در امور کیفری، مصوب ۱۳۷۸، ماده ۵۴ نیز صراحت دارد که متهم در دادگاهی محاکمه می‌شود که جرم در آن حوزه واقع شده است. هر چند محل دستگیری و محل اقامت نیز مورد توجه قانونگذار واقع شده است.

بنابراین برای رسیدگی به جرم جعل رایانه‌ای به عنوان یکی از جرایم سایبر کافی است محل وقوع آن کشف شود. اما این امر به سادگی امکان‌پذیر نیست. از سوی دیگر نباید تحقیق و رسیدگی را منوط به شناسایی دقیق محل ارتکاب جرم کرد. زیرا در بهترین وضعیت دستیابی به مرتکبان جرایم با دشواری‌های بسیاری همراه است، چه رسد به اینکه

-البوعلی، امیر، پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، موضوع صلاحیت مراجع قضایی در رسیدگی^۱ به جرائم ارتكابی در فضای سایبر، شهریور ۸۸ ص ۱۰۲.

محاكم خود در پیشبرد امور مانع تراشی می‌کنند. لذا باید از ظرفیت‌هایی که در قانون فراهم آمده بهره برد.

در این رابطه ماده ۲۹ قانون جرایم رایانه‌ای اشعار می‌دارد: «چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.» علیهذا مفاد این ماده نیز در مورد جعل رایانه‌ای به عنوان یکی از جرایم رایانه‌ای قابل تسری می‌باشد.

۲- صلاحیت ذاتی

در کنار صلاحیت محلی که تمامی دادگاههای عمومی تحت شمول آن قرار می‌گیرند، قانونگذار در موارد خاص برخی محاکم را متمایز ساخته است. گاهی وجه تمیز در مرتبه محاکم بروز می‌یابد. برای مثال در گذشته که دادگاههای کیفری ۱ و ۲ وجود داشتند، این سلسله مراتب رعایت می‌شد. گاهی هم جرائم خاصی احصاء می‌شوند. نمونه بارز آن دادگاههای انقلاب هستند که قانون تشکیل آنها عناوینی را احصاء کرده است. در نهایت شخصیت مرتکبان جرایم نیز وجه تمیز ذاتی محاکم قرار گرفته است. برای مثال می‌توان به نظامیان، ... و مقامات دستگاههای دولتی اشاره کرد.

در رابطه با جرایم سایر، با توجه به اینکه طیف گسترده آنها آحاد جامعه را در بر می‌گیرد، انتظار ارتکاب آنها از سوی این اشخاص نابه‌جا نیست. این مسأله به ویژه با توجه به ویژگی جرأت‌آفرینی فضای سایبر بسیار جدی‌تر تلقی می‌شود.

در خصوص صلاحیت ذاتی محاکم در مورد بزه جعل رایانه‌ای باید خاطر نشان ساخت که گاهی نفی صلاحیت محاکم بر اساس شخصیت مرتکبان تعیین می‌گردد مثلاً موردی که جعل رایانه‌ای توسط شخص روحانی صورت می‌گیرد که دادگاه ویژه روحانیت صالح به رسیدگی می‌باشد و یا مواردی که جعل رایانه‌ای موضوع ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح می‌باشد که مرجع صالح رسیدگی کننده دادگاههای نظامی می‌باشند در سایر موارد مرجع صالح به رسیدگی همان دادگاههای عمومی می‌باشد که مشمول جعل رایانه‌ای موضوع ماده ۶۸ قانون تجارت الکترونیکی و ماده ۶ قانون جرائم رایانه‌ای می‌باشد و به همین اعتبار ماده ۳۰ قانون جرائم رایانه‌ای مقرر داشته است: «قوه قضائیه مکلف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاههای عمومی و انقلاب، نظامی و تجدیدنظر برای رسیدگی به جرایم رایانه‌ای اختصاص دهد.»

در خصوص رویه حاکم در مراجع قضایی ایران، باید خاطر نشان ساخت هم اکنون شعب ویژه‌ای از دادسراها و دادگاههای بدوی و تجدیدنظر در راستای ماده ۳۰ قانون جرائم رایانه‌ای به عنوان شعبه ویژه رسیدگی کننده به جرائم رایانه‌ای تخصیص داده شده است که معمولاً متصدی شعب مذکور از آموزشهای ضمن خدمت قضات که تلفیقی از علم حقوق و رایانه می‌باشد برخوردار می‌گردند. البته در تهران به لحاظ حجم عظیم پرونده‌های مربوط به جرائم رایانه‌ای یک مجتمع قضایی به همین نام، امر رسیدگی به این جرائم را برعهده دارد که متشکل از دادسرا و دادگاه بدوی می‌باشد. ضمناً همانگونه که در بحث کشف جرم بدان اشارت رفت ضابط دستگاه قضایی در رسیدگی به جرائم رایانه‌ای، پلیس فضای تولید و تبادل اطلاعات ناجا معروف به «فتا» می‌باشد که ماهیت آن به صورت عملیاتی و با رویکرد مقابله با جرائم مذکور از طریق پیش‌بینی، پیشگیری و کشف جرم می‌باشد.

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 قلمرو 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 رایانه ای روبرو هستیم؛ یکی جعل سنتی (کلاسیک) و دیگری جعل رایانه ای. به دنبال نوظهور بودن عنوان جزایی جعل رایانه ای و ورود به به نظام حقوقی، ضرورت پرداختن به این جرم و بررسی عناصر مشکله 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 و قبل 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 آنها یکسان هستند ولی تفاوت عمده ای که بین این دو بزه علی الخصوص در بحث عنصر مادی آنها و ویژگی های خاص جرایم 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 عبارت از ساختن یا تغییر دادن آگاهانه داده های رایانه ای یا سایر موارد مذکور در قانون دارای ارزش اثباتی به قصد جازدن آنها به عنوان اصل برای استفاده خود یا دیگری و به ضرر غیر. در بحث جعل و تزویر و همچنین جعل رایانه ای می گوئیم که سند یا حافظه رایانه و نظم اسنادی به عنوان یک ارزش در نظام

حقوقی ما می‌باشد و از ارزش و اعتبار برخوردار است و بر همین اساس رفتارهایی که مخالف با نظم اسنادی هستند، رفتارهایی است که زیان شدید و غیرقابل تحمل را ایجاد می‌کند و نظم اسنادی را مخدوش می‌سازد و همین امر مبنای جرم‌انگاری جعل رایانه‌ای را تشکیل می‌دهد. تمایز جعل رایانه‌ای با جعل سنتی علاوه به اینکه بر این مبنا استوار می‌باشد که جعل رایانه‌ای در فضای سایبر و مجازی تحقق می‌یابد و نه فضای واقعی، می‌توان گفت که از جمله ویژگی‌های جعل رایانه‌ای همانند سایر جرایم اینترنتی، گستردگی، فراوانی، فرامرزی بودن، وقوع سهل و آسان، تنوع، جذابیت و زایدالوصف بودن این جرم می‌باشد. بزه جعل رایانه‌ای همانند سایر عناوین جزایی متشکل از عناصر قانونی، مادی و روانی می‌باشد، عنصر قانونی این بزه در حقوق جزایی ایران منحصر به همان سه مقرر قانونی بود که در فوق به آن اشارت رفت، رفتار مرتکب به عنوان یکی اجزای عنصر مادی این بزه منحصر به وارد کردن، حذف کردن، تغییر دادن و متوقف کردن داده‌های رایانه‌ای می‌باشد و قانونگذار ایران به صورت پراکنده هر کدام از موارد مصرحه را در سه قانون یاد شده آورده است و به جا بود که مقنن آنگونه که در ماده ۷ کنوانسیون جرایم سایبر آمده است هر چهار مورد را به عنوان رفتار مرتکب در قوانین داخلی و یکجا می‌آورد. از جمله شرایط رفتار مجرمانه در جعل رایانه‌ای که تفاوتی با جعل سنتی نداشته است قابلیت اضرار و برخلاف واقع بودن رفتار مجرمانه می‌باشد و در صورت تحقق شرایط فوق بزه جعل رایانه‌ای ارتکاب می‌یابد. یکی دیگر از اجزاء رکن مادی جعل رایانه‌ای، موضوع و متعلق این جرم می‌باشد. موضوع جرم جعل رایانه‌ای عبارتست از داده‌های قابل استناد، داده‌ها و علائم موجود در کارتهای حافظه و داده‌ها و علائم قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی و تراشه‌ها که هر کدام دارای تعریف خاص می‌باشند. به اعداد، حروف و علائم که جهت درک فهم مشترک از انسان‌ها یا رایانه سرچشمه می‌گیرند داده می‌گویند و به

طور کلی می‌توان گفت که موضوع جعل رایانه‌ای همان داده‌ها و برنامه‌های رایانه‌ای می‌باشد که موارد تصریح شده در فوق بدان منتهی می‌گردد. اما شرط مؤثر و لازم در موضوع جعل رایانه‌ای اینست که داده‌ها و برنامه‌های رایانه‌ای باید قابلیت استناد و مؤثر در اثبات و نفی امر باشد؛ به عبارت دیگر دارای ارزش قضایی باشد و گرنه اگر داده‌ها ارزش قضایی نداشته باشد جعل واقع نمی‌شود. در جعل رایانه‌ای برخلاف جعل سنتی، وسیله در تحقق جرم مؤثر می‌باشد و بدون وجود وسیله مورد نظر امکان تحقق جرم وجود ندارد. با این وجود اگر چه وسیله در تحقق این جرم شرط می‌باشد ولی نوع وسیله در ارتکاب این جرم شرط نمی‌باشد و آنچه که مهم است وسیله‌ای ملاک می‌باشد که موجبات ورود به فضای مجازی را برای تحقق جرم فراهم سازد. جعل رایانه‌ای 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 می‌یابد. در رابطه با خصوصیت مرتکب جعل رایانه‌ای به عنوان یکی از اجزاء عنصر مادی باید گفت که جعل رایانه‌ای در قانون مجازات جزایم نیروهای مسلح صرفاً در مورد افراد نظامی مصداق پیدا می‌کند و در قانون تجارت الکترونیکی در مورد اشخاصی تحقق می‌یابد که در بستر مبادلات الکترونیکی مبادرت به جعل رایانه‌ای نموده‌اند و به نوعی قانون مزبور به صورت خاص تلقی می‌گردد و فقط جعل رایانه‌ای موضوع قانون جرایم رایانه‌ای به صورت عام بوده است و مشمول هر کسی می‌گردد که نسبت به این جرم اقدام نموده است. در جرم جعل رایانه‌ای علاوه بر اینکه عمل مرتکب و سوءنیت عام به عنوان اجزای رکن معنوی این جرم را تشکیل می‌دهند، انگیزه یعنی قصد تقلب به عنوان یکی از اجزای رکن روانی این جرم می‌باشد زیرا جرم جعل رایانه‌ای همانند سایر جرائم مطلق نیازی به سوءنیت خاص ندارد و قصد متقلبانه مرتکب جرم جعل، انگیزه می‌باشد. با توجه به نقش اشخاص حقوقی و

علی‌الخصوص اشخاص حقوقی حقوق خصوصی در روابط اجتماعی و به خصوص در امور الکترونیکی و رایانه‌ای و با عنایت به اینکه بروز رفتارهای مجرمانه از سوی اشخاص حقوقی، دارای اثرات زیان باری می‌باشد، مع‌الوصف برای اولین بار صراحتاً در حقوق کیفری ایران در مواد ۱۹ و ۲۰ قانون جرائم رایانه‌ای، مسئولیت کیفری اشخاص حقوقی مورد شناسایی قرار گرفت، که مشمول کلیه جرائم رایانه‌ای و از جمله جعل رایانه‌ای می‌گردد. با مقایسه بین جعل رایانه‌ای در قانون جرایم رایانه‌ای و جعل سنتی ملاحظه می‌کنیم که قانونگذار برای مجازات جعل رایانه‌ای آنگونه که در جعل سنتی قائل به تفکیک گردیده است هیچگونه تفکیکی قائل نشده است و به تعبیر دیگر تفاوتی بین مجازات در جعل رایانه‌ای داده‌های رسمی و داده‌های عادی وجود ندارد که به نظر می‌رسد با توجه به اهمیت موضوع جرم می‌بایست به این نکته توجه می‌گردید. قانونگذار در تعیین مجازات در قانون جرایم رایانه‌ای به سیاست سخت‌گیرانه نظر داشته است و طبیعتاً می‌بایست مجازات لحاظ شده در جعل رایانه‌ای سنگین‌تر 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 می‌بینیم که مجازات‌های در نظر گرفته برای جعل سنتی از مجازات‌های مربوط به جعل رایانه‌ای شدیدتر است و این با سیاست کیفری مربوط به جرایم رایانه‌ای در تضاد می‌باشد.

منابع و مآخذ

الف- کتابها

- ۱- آریا، ناصر، فرهنگ اصطلاحات رایانه و شبکه رایانه مرکز تحقیقات تخصصی حسابداری و حسابرسی، تهران، ۱۳۷۲.
- ۲- اصلانی، حمیدرضا، حقوق فن آوری اطلاعات، چاپ اول، نشر میزان، تهران، ۱۳۸۴.
- ۳- آشوری، محمد، آئین دادرسی کیفری، ج ۱، چاپ یازدهم، تهران، انتشارات سمت.
- ۴- آنابوی و آدری هورتن، حمایت از داده‌ها، «شورای اروپا» ترجمه ناهید جعفرپور.
- ۵- باستانی، برومند، جرائم رایانه‌ای و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ اول ۱۳۸۳، انتشارات بهنامی.
- ۶- بای، حسنعلی و پورقهرمانی، بابک، بررسی فقهی حقوق جرائم رایانه‌ای، چاپ اول قم، پژوهشگاه علوم و فرهنگ اسلامی.
- ۷- پیمانی، ضیاءالدین، جرائم علیه امنیت و آسایش عمومی، نشر میزان، چاپ دوم، ۱۳۷۵.
- ۸- جلالی فراهانی، امیرحسین، صلاحیت کیفری سایبری در پرتوی قوانین داخلی، حقوق فن آوری اطلاعات و ارتباطات، تهران، انتشارات روزنامه رسمی جمهوری اسلامی ایران، چاپ اول، ۱۳۸۸.
- ۹- حسنوی، رضا، فرهنگ تشریحی میکروسافت، ۲۰۰۰، (ترجمه)، چاپ اول، ۱۳۷۹، انتشارات دانشیار، تهران.
- ۱۰- خداقلی، زهرا، جرائم رایانه‌ای، چاپ اول، انتشارات آریان، تهران، ۱۳۸۳.

۱۱- دزیانی، محمدحسین، آئین دادرسی کیفری جرائم رایانه‌ای، زمینه توصیه نامه شماره R(۹۵) ناظر بر مشکلات آئین دادرسی کیفری مربوط به فن آوری اطلاعات برنامه انفورماتیک شماره ۸۱

۱۲- دزیانی، محمدحسن، ادله اثبات دعوی در حقوق کیفری ایران شماره ۶۵.

۱۳- ساریخانی، عادل، جرائم علیه امنیت و آسایش عمومی چاپ اول، دانشگاه قم، ۱۳۸۴.

۱۴- سالاری، مهدی، حقوق جزای اختصاصی جعل و تزویر، نشر میزان، چاپ اول، تابستان ۸۶.

ب- مقاله ها

۱- توماس، لی، من، ترجمه محمد حسین زمانی، مقاله داده چیست؟، یا داده‌ها چه هستند؟، فصلنامه کتابداری و اطلاع رسانی، نشریه شماره ۴ جلد ۵.

۲- جاویدنیا، جواد، مقاله نقد و بررسی جرم مندرج، در قانون تجارت الکترونیکی، مجله حقوقی دادگستری، شماره ۵۹، تابستان ۸۶.

۳- خرم آبادی، عبدالصمد، تاریخچه و تعریف و طبقه‌بندی جرایم رایانه‌ای، مجموعه مقالات همایش و بررسی ابعاد حقوق فن آوری اطلاعات.

۴- دزیانی، محمد حسن، نشریه بین‌المللی سیاست جنایی - سازمان ملل، شماره ۴۳ و ۴۴ خیرنامه شورای عالی انفورماتیک کشور.

۵- دزیانی، محمد حسن، ابعاد جزایی رایانه و جرایم رایانه‌ای و خبرنامه انفورماتیک شماره ۵۸، شورای عالی انفورماتیک کشور.

۶-دزیانی، محمدحسن، مقدمه Cyber law (آلمان) خبرنامه انفورماتیک شورایعالی انفورماتیک کشور، ش ۷۱، مرداد ۷۸.

۷-رایجیان اصلی، مهرداد، مقاله قانون جرایم رایانه‌ای، نوآوریها و کاستی‌ها، تابستان ۸۶.

ج-پایان نامه ها

۱-البوعلی، امیر، صلاحیت مراجع قضایی در رسیدگی به جرایم ارتكابی در فضای سایبر، پایان‌نامه کارشناسی ارشد رشته حقوق جزا و جرم‌شناسی، دانشگاه شیراز، شهریور ۸۸.

۲-آل محمد، فاطمه، پایان‌نامه سیاست جنایی ایران در قبال جرایم رایانه‌ای، دانشگاه حقوق و علوم سیاسی دانشگاه شیراز، فروردین ۱۳۹۰.

۳-پاکزاد، بتول، تروریسم سایبری، رساله دکترای رشته حقوق کیفری و جرم‌شناسی، دانشگاه شهید بهشتی، سال ۱۳۸۸.

۴-خرم‌آبادی، عبدالصمد، جرایم فن‌آوری اطلاعات، رساله دکترای حقوق جزا و جرم‌شناسی دانشگاه تهران، ۱۳۸۴.

۵-داوودی بیرق، حسین، ادله اثبات دعاوی حقوق در فضای سایبر و مجازی، پایان‌نامه کارشناسی ارشد

د-منابع لاتین

1-Arkian, sos Prevention and Prosecution of Computer and hiytechnologycrim. 1989.

2-August Ray, international Cyber-Jurisdiction A comparative Analysis, American Busness law journal, 2002.

3-Cybercrime Convention, <http://Conventions>

[.coe.int/Treaty/en/Repats/HTML](http://coe.int/Treaty/en/Repats/HTML).

4-Rolph o, Bloemers. Electronic and digital signatures. Available at www.stol.com.

5-Ulrich sieber. The international Hand bookon , Computer Crime.