شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

بررسی تاثیر فناوری‌های نوین در ارتکاب جرم

محمدعلی قربانی[۱] / امیررضا محمودی[۲] / سید احمد پیرو نذیری[۳]

* نوع مقاله: پژوهشی / تاریخ دریافت: ۱۴۰۴/۰۱/۱۵ / تاریخ پذیرش: ۱۴۰۴/۰۳/۱۱

کدمقاله: JHVMN-۲۵۰۵-۱۲۹۳

چکیده

فناوری‌های جدید بر تمامی فعالیت‌های اقتصادی، اجتماعی، تأثیر گذاشته است. فضای مجازی شرایطی را ایجاد کرده است که مجرمان می‌توانند در مکان‌هایی غیر از جایی که آثار و نتایج اعمال آنها ظاهر می‌شود و مرتکب جرم شوند. جرایم فناوری اطلاعات به دو دسته تقسیم می‌شوند. گروه اول شامل طیفی از جرایم رایانه‌ای است که می‌توان آنها را تحت قوانین مربوط به جرایم کلاسیک، تحت پیگرد قانونی و مجازات قرار داد. این گروه شامل انواع جرایم است و این جرایم را به بخش‌هایی چون جرایم علیه افراد، اموال، امنیت و آرامش عمومی تقسیم‌بندی می‌کند. گروه دوم شامل دسته‌ای از جرایم رایانه‌ای است که نیازمند قوانین ویژه‌ای هستند. این نوع جرایم نیز قابل طبقه‌بندی به سه گروه می‌باشند. دسته اول جرایمی که قبل از ظهور فناوری اطلاعات امکان ارتکاب آنها وجود نداشت، مانند دسترسی غیرمجاز، دسته دوم جرایم کلاسیک را شامل می‌شود. از سوی دیگر فناوری در پیشگیری از وقوع جرم تأثیر مثبتی دارد و ابزارها و وسایلی مانند دوربین‌های مداربسته، دزدگیرهای رمزدار موجب پیشگیری از وقوع جرم می‌شوند و رسانه‌ها با کارکردهایی مانند آموزش و آموزش آموزه‌های دینی و امنیتی می‌توانند در پیشگیری اجتماعی از وقوع جرم مفید باشند. فناوری‌های مذکور علاوه بر کارکردهای مؤثر و مثبت، دارای کارکردهای منفی از جمله نقض حق حریم خصوصی و تجاوز به حریم خصوصی هستند.

واژگان کلیدی: فناوری‌های نوین، ارتکاب جرم، جرایم رایانه‌ای، اخلال در داده.

[۱]. گروه الهیات و معارف اسلامی، دانشکده علوم انسانی، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. (نویسنده مسئول) Dr.alighorbani@gmail.com

[۲]. گروه حقوق، دانشکده علوم انسانی، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران.amirreza.mahmodi@iau.ir

[۳]. گروه حقوق، دانشکده علوم انسانی، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. Seyedahmad.peyrovnaziri@iau.ir

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

مقدمه

با کمک فناوری اطلاعات، بسیاری از چیزهایی که قبلا غیرممکن بود، ممکن شده است. علاوه بر این فناوری اطلاعات با تأثیر شگفت انگیز خود بر ارتباطات از راه دور و ایجاد بزرگراه‌های اطلاعاتی، به ویژه اینترنت، دسترسی به انواع اطلاعات و خدمات الکترونیکی را صرف نظر از اینکه در کجای جهان هستند، فراهم کرده است. ممکن ساخته است و از این طریق فضای جدیدی به نام فضای مجازی با اثرات واقعی ایجاد کرده است. فناوری با توجه به آثار مثبتی که دارد، این امکان را برای افراد سودجو فراهم کرده است تا با سوء استفاده از ابزارهای جدید و دستیابی به امیال و شهوات مادی خود مرتکب جرم شوند. همچنین با ظهور تکنولوژی در جوامع بشری، علاوه بر جرایم سنتی، زمینه ظهور جرایم جدید نیز فراهم شد. در واقع سیاست مبارزه با جرایم و اساساً پیشگیری از وقوع جرم در رأس اولویت های سیاست گذاری و پژوهشی اکثر دولت ها و جوامع بوده است. بنابراین آنها از این ناحیه سوءاستفاده می‌کنند و اغلب در نقاطی مستقر می‌شوند که آثار و پیامدهای ناشی از اقدامات مجرمانه آن‌ها آشکار نمی‌شود، تا از محدوده دستیابی مقامات اجرایی و قضایی، که در چارچوب مرزهای جغرافیایی کشور خود محدود شده‌اند، دور بمانند. به این ترتیب، فناوری اطلاعات نه تنها امکان بروز رفتارهای ضداجتماعی و مجرمانه را که پیش از این امکان پذیر نبود، ایجاد کرده است، بلکه پتانسیل ارتکاب انواع جرایم متعارف را نیز به صورت غیرمتعارف ایجاد کرده است.

۱- مفاهیم

۱-۱- مفهوم جرم در لغت و اصطلاح

ریشه کلمه جرم با فتح است (جرم) که به معنای قطع است (ابن منظور، ۱۴۱۴، ۹۰). یا به معنای جدا کردن میوه از درخت است و این کلمه به طور استعاره برای به دست آوردن هر امر نامطلوبی به کار رفته است (راغب اصفهانی، ۱۴۱۲، ۱۹۲). گناهکار را از آن جهت مجرم می‌نامند که تعهد خود را می‌شکند، زیرا مجرم کسی است که تمام پیوندهای خود را با خدا قطع می‌کند و این عمل نشان دهنده محرومیت او از خیر و سعادت است. کلمات «اثم» و «مخلص» به یک معنا هستند، زیرا به اعمالی اطلاق می‌شوند که انسان را از پاداش دور می‌کنند. جمع آن‌ها «مخلص» است که به معنای کند کردن (آهسته و دور کردن) است. کلام خدا که می‌فرماید: «الخمر و قمار از گناهان کبیره هستند» به این معنی است که مصرف آنها انسان را از خیر دور می‌کند (راغب اصفهانی، ۱۴۱۲، ۶۳).

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

«مخالفت با اوامر و نواهی کتاب و سنّت، یا ارتکاب عملی است که به تباهی فرد یا جامعه بیانجامد، هر جرم را کیفری است که شارع بدان تصریح کرده و یا اختیار آن را به ولی امر یا قاضی سپرده است.» (گرجی، ۱۳۷۸، ۱، ۵۸). برخی می‌نگارند: جرم عبارت است از ارتکاب عملی که قانون آن را ممنوع و برای آن مجازات تعیین کرده است، یا ترک عملی که قانون برای آن مجازات تعیین کرده است. به عبارت دیگر، فعل یا ترک فعلی که دین، ممنوعیت و مجازات آن را بیان کرده است (عوده، ۲۰۰۹، ۱، ۶۴). این تعریف، منشأ جرم‌انگاری اعمال را دینی می‌داند و از آن نتیجه می‌گیرد که هر عملی که در دین، حرمت و مجازات آن مشخص نشده باشد، جرم محسوب نمی‌شود. طبق تعریف دیگر، جرم مترادف با گناه است و جرم همان معصیت در حق خداست؛ چه انجام کارهای حرام باشد و چه ترک کارهای واجب، و هر جرمی در دین، چه در دنیا و چه در آخرت، مجازات دارد (ابوزهره، ۱۹۹۸، ۲۰). فیض، از علمای معاصر فقه اسلامی، در این زمینه می نویسد: "جرم عبارت است از انجام عملی یا گفتن سخنی که شریعت اسلام آن را حرام دانسته و برای آن عمل مجازات تعیین کرده است. یا ترک عملی یا گفتن سخنی که شریعت اسلام آن را واجب دانسته و برای ترک آن مجازات تعیین کرده است" (فیض، ۱۳۷۹، ۷۱).

۲-۱- مفهوم فناوری نوین و اندیشه مجرمانه

فناوری در لغت به معنی تکنولوژی، علم به صنایع و حرفه‌ها و مجموع اصطلاحات فنی و صنعتی می باشد (عمید، ۱۳۸۰، ۴۱۴). در واقع، فناوری را باید ترجمه‌ای از «technology» دانست. این یک تکنیک مشتق شده از علوم مختلف، با ریشه یونانی است که از دو کلمه Techne و Logic تشکیل شده است. Techne به معنای هنر، چیزی است که به دست انسان خلق می‌شود، در حالی که Arche به خلقت الهی اشاره دارد. Logie یا Logic در یونان باستان برای اشاره به دانش و حکمت استفاده می‌شد. بنابراین می‌توانیم بگوییم که فناوری به ترکیبی از هنر، دانش و یادگیری اشاره دارد (محمود زاده، ۱۳۸۹، ۵۷). تعاریف متعددی توسط صاحب‌نظران در مورد مفهوم فناوری و تکنولوژی ارائه شده است که به اختصار به برخی از آن‌ها اشاره می شود: فناوری مجموعه‌ای از فرآیندها، روش‌ها، فنون، ابزارها، تجهیزات، ماشین‌آلات و مهارت‌ها است که به وسیله آن‌ها محصولی تولید یا خدماتی ارائه می‌شود (فتحیان و مولاناپور، ۱۳۹۰، ۱۶). دیگران آن را اینگونه تعریف کرده‌اند: فناوری به کاربرد علم در صنایع با استفاده از رویه‌ها و مطالعات سیستماتیک و جهت‌دار اشاره دارد (حاج فتحعلی‌ها و سید اصفهانی، ۱۳۷۲، ۴۶).

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

اندیشه مجرمانه تفکری است که به طورِ بالقوه قابلیت ظهور در قالب پدیده جنایی را داشته به نحوی که با نشو و نما و گذار از اندیشه به عمل، شخص را در معرض مجازات یا اقدامات تأمینی قرار می‌دهد و به علت فقدان، یا غفلت از سد های اخلاقی و اجتماعی، مرتکب جرم می‌شود. فقدان سد های اخلاقی و اجتماعی موجب پیدایش حالتی می شود که دانشمندان آن را شخصیت کیفری نامیده اند (محسنی، ۱۳۷۵، ۶۰ و ۶۱).

۲- مصادیق جرایم فناوری‌های نوین و ارکان آن‌ها

در این قسمت از پژوهش مصادیق جرایم فناوری های نوین و ارکان آن‌ها مورد بررسی قرار می‌گیرد.

۲-۱- جرایم علیه محرمانگی، دستیابی غیرمجاز به یک سیستم رایانه‌ای

در این به بیان و بررسی مصادیق جرایم علیه محرمانگی و دستیابی‌های غیر مجاز به سیستم‌های رایانه ای اینترنتی می‌پردازیم.

۲-۱-۱-دسترسی بدون مجوز

ماده ۲ پیش نویس قانون جرایم رایانه ای مقرر داشته است: «هر فردی که به صورت عمدی و بدون مجوز، با نقض اقدامات حفاظتی به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی دسترسی پیدا کند، به پرداخت جریمه نقدی از پنج میلیون ریال تا پنجاه میلیون ریال محکوم می‌شود.» ماده ۲ پیش نویس قانون جرایم رایانه‌ای دارای اشکالاتی به شرح زیر است:

اولین اشکال ماده ۲ پیش نویس قانون جرایم رایانه‌ای این است که برخلاف ماده ۲ کنوانسیون جرایم سایبر در مورد دستیابی غیر مجاز به بخشی از یک سیستم رایانه‌ای ساکت است. به همین لحاظ این ماده ممکن است در آینده نیاز به تفسیر داشته باشد مثلا یکی از مصادیق دستیابی غیر مجاز به بخشی از یک سیستم رایانه‌ای موردی است که یک شخص مجاز است که فقط ازیک قسمت از حافظه یک رایانه استفاده کند ولی بدون اذن به قسمت‌های دیگر آن نیز دستیابی پیدا می‌کند آیا عمل این شخص مصداق دستیابی غیر مجاز است؟ به موجب ماده ۲ کنوانسیون جرایم سایبر چنین عملی مصداق دستیابی غیر مجاز است زیرا صراحتا اعلام شده است دستیابی غیر مجاز به قسمتی از یک سیستم رایانه‌ای جرم است اما به لحاظ سکوت ماده ۲ پیش نویس قانون جرایم رایانه‌ای ممکن است باعث شود پاسخ‌های مختلفی در مقام اجرا به این سوال داده شود.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

دستیابی به داده‌های رایانه‌ای عملا زمانی امکان پذیر است که یک شخص ابتدائاً به تمام یا بخشی از یک سیستم دسترسی پیدا کرده باشد معمولاً کشورهایی که دستیابی به تمام یا بخشی از یک سیستم رایانه‌ای را جرم انگاری کرده اند دستیابی به داده ها را که در مرحله بعد از دستیابی به تمام یا قسمتی از سیستم قرار دارد به عنوان کیفیت مشدده در نظر گرفته‌اند به عبارت دیگر باید بین مجرمی که فقط به یک سیستم رایانه‌ای دستیابی پیدا کرده با مجرمی که علاوه بر دستیابی به یک سیستم به داده‌های موجود در آن نیز دست یافته است تفاوت قائل شد. ماده ۲ پیش نویس قانون جرایم رایانه ای از این جهت که تفاوتی بین دو حالت مذکور قائل نشده است دارای اشکال است.

بهتر است به جای استفاده از اصطلاح "دسترسی غیرمجاز" در نام‌گذاری جرم موضوع ماده ۲ پیش‌نویس قانون جرایم رایانه‌ای، از عبارت "دستیابی غیرمجاز" استفاده شود. چرا که کلمه "دستیابی" بر تلاش و قصد مرتکب برای ورود به یک سیستم رایانه‌ای دلالت دارد، در حالی که واژه "دسترسی" چنین مفهومی را منتقل نمی‌کند. اگر به جای اصطلاح بدون مجوز از اصطلاح بدون حق استفاده شود بهتر است زیرا اصطلاح بدون حق جامع تر است و در ضمن شامل مواردی هم می شود که مالک یک رایانه بنا به دلایلی از حق دسترسی به داده های موجود در آن رایانه محروم می شود (تحیری، ۱۳۸۳، ۱۲۰).

۲-۱-۲- شنود و دریافت بدون مجوز

رکن قانونی: شورای اروپا در توصیه نامه شماره۹(۸۹) در مورد جرم انگاری شنود غیر مجاز مقرر داشته: «شنود غیرمجاز از طریق ابزارهای فنی که بر ارتباطات ورودی، خروجی و داخلی یک سیستم یا شبکه رایانه‌ای صورت می‌گیرد، باید به‌عنوان جرم تلقی گردد.» سازمان همکاری اقتصادی و توسعه اعلام کرده است که: «هرگونه دستیابی یا شنود در سیستم رایانه‌ای یا ارتباطی، چنانچه به‌صورت آگاهانه و بدون کسب مجوز از مسئول مربوطه انجام شود، صرف‌نظر از اینکه این عمل با نقض تدابیر امنیتی یا با اهداف ناپسند و زیان‌بار همراه باشد، باید تحت ممنوعیت قرار گرفته و مجازات شود.» ماده ۳ کنوانسیون جرائم سایبری به موضوع جرم‌انگاری شنود غیرقانونی داده‌های رایانه‌ای پرداخته است. بر اساس این ماده، تمامی کشورهای عضو موظف‌اند قوانین و مقرراتی وضع کنند که بر پایه حقوق داخلی کشورشان، شنود عمدی و بدون مجوز داده‌های غیرعمومی در حال انتقال به یک سیستم رایانه‌ای، از یک سیستم رایانه‌ای یا درون آن، و از طریق ابزارهای فنی انجام شده را جرم تلقی کنند. این جرم‌انگاری باید شامل امواج الکترومغناطیسی منتشرشده از یک سیستم رایانه‌ای نیز

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

باشد، به شرط آنکه این امواج برای انتقال داده‌های رایانه‌ای مورد استفاده قرار گیرند. علاوه بر این، کشورهای عضو می‌توانند شنود غیرمجاز را به شکلی جرم‌انگاری کنند که تحقق آن مستلزم قصد سوء بوده و صرفاً از طریق ارتباط میان یک سیستم رایانه‌ای با سیستم رایانه‌ای دیگر صورت گیرد» (دزیانی، ۱۳۷۶، ۱۴۰). با توجه به تعریف ارائه‌شده، پنج شرط برای تحقق شنود وجود دارد که عبارتند از:

۱- شنود باید به‌طور عمدی صورت گیرد.

۲- شنود نباید همراه با مجوز یا حق قانونی باشد.

۳- شنود تنها در ارتباط با داده‌های در حال انتقال قابل تحقق است.

۴- فرایند انتقال داده‌ها باید به‌صورت غیرعمومی صورت گیرد.

۵- شنود باید از طریق ابزارهای فنی انجام شود (پاکزاد، ۱۳۸۸، ۶۹).

رکن مادی جرم شنود غیرمجاز شامل سه بخش اصلی است که عبارت‌اند از: الف- رفتار مجرمانه فرد مرتکب، ب- موضوع جرم، ج- ابزار یا وسیله‌ای که برای ارتکاب جرم به کار گرفته شده است

الف- رفتار فرد مرتکب: رفتار مجرمانه در جرم شنود غیرمجاز شامل اقدام عمدی فرد در گوش دادن، کنترل یا نظارت بر محتوای ارتباطات و یا دستیابی به محتوای داده‌ها است. این رفتار می‌تواند به‌صورت مستقیم از طریق ورود، دسترسی و استفاده از یک سیستم رایانه‌ای انجام شود یا به شکل غیرمستقیم با بهره‌گیری از دستگاه‌های استراق سمع الکترونیکی صورت گیرد. علاوه بر این، شنود ممکن است شامل ضبط داده‌ها نیز باشد.

ب- در خصوص موضوع جرم شنود غیرمجاز، محور اصلی این جرم "داده‌های" رایانه‌ای در حال انتقال غیرعمومی است. برای آن‌که داده‌ها و فرآیند انتقال آن‌ها به‌عنوان موضوع جرم شنود غیرمجاز شناخته شوند، باید از سه ویژگی برخوردار باشند:

۱- داده‌های رایانه‌ای باید در حال انتقال باشند،

۲- فرآیند انتقال داده‌ها باید به‌صورت غیرعمومی صورت گیرد،

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۳- فرد مرتکب نباید حقی برای شنود این داده‌ها داشته باشد (دزیانی، ۱۳۷۶، ۱۴۰).

ج- ابزار ارتکاب جرم: ماده ۳ کنوانسیون جرائم سایبری به طور ویژه به ابزارهای مورد استفاده در ارتکاب جرم شنود غیرمجاز توجه دارد. بر اساس این ماده، یکی از شروط محسوب شدن شنود به عنوان جرم، این است که این عمل با استفاده از ابزارهای فنی انجام شده باشد. گزارش توجیهی مرتبط با کنوانسیون جرائم سایبری به مصادیق ابزارهای فنی پرداخته و آن‌ها را مورد بررسی قرار داده است. بر اساس این گزارش، ابزارهای فنی شامل دستگاه‌هایی هستند که به منظور جمع‌آوری و ضبط داده‌ها طراحی و نصب می‌شوند. همچنین دستگاه‌هایی که برای جمع‌آوری و ضبط ارتباطات بی‌سیم به کار می‌روند نیز در دسته ابزارهای فنی قرار می‌گیرند. علاوه بر این، این مفهوم می‌تواند استفاده از نرم‌افزارها، گذرواژه‌ها و کدها را نیز در بر بگیرد. معیار استفاده از ابزارهای فنی، به عنوان عاملی محدودکننده، برای جلوگیری از گسترش جرم‌انگاری بیش از حد در نظر گرفته شده است (تحیری، ۱۳۸۳، ۱۲۹).

جرم شنود غیرمجاز نیز مشابه جرم دسترسی غیرمجاز به‌عنوان یک جرم مطلق تعریف می‌شود، چراکه صرفاً انجام عمدی و بدون مجوز شنود داده‌های رایانه‌ای، بدون توجه به اینکه به خسارتی منجر شود یا نه، به‌عنوان یک جرم شناخته می‌شود. بنابراین، این جرم نیازی به نتیجه نداشته و تحقق آن وابسته به تأثیر خاص یا پیامدی مشخص نیست؛ نتیجه جرم بخشی از عناصر مادی تشکیل‌دهنده این جرم محسوب نمی‌شود.

رکن معنوی: مطابق با ماده ۳ کنوانسیون جرائم سایبری، جرم شنود غیرمجاز به‌عنوان یک جرم عمدی تعریف شده است. برای تحلیل عنصر معنوی در جرائم عمدی، باید بررسی شود که آیا ارتکاب این جرم مستلزم داشتن علم، سوءنیت عام یا خاص و انگیزه مجرم می‌باشد یا خیر. اجزای تشکیل‌دهنده رکن معنوی جرم شنود غیرمجاز نیز، همانند جرم دسترسی غیرمجاز، وابسته به رویکردی است که قانون‌گذاران ملی اتخاذ می‌کنند. چراکه ماده ۳ این کنوانسیون، به کشورهای عضو امکان داده است تا یکی از دو رویکرد گسترده یا محدود را برای جرم‌انگاری شنود غیرمجاز انتخاب کنند (جعفرپور، ۱۳۸۱، ۴۱).

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۳-۱-۲- جرایم علیه امنیت

ماده ۴ لایحه قانونی جرایم رایانه‌ای بیان می‌کند: هر فردی که به‌صورت عمدی و بدون داشتن مجوز، به داده‌های محرمانه در سیستم‌های رایانه‌ای، مخابراتی یا ابزارهای ذخیره اطلاعات دسترسی یابد، مرتکب جرم می‌شود. یا اطلاعات محرمانه رایانه ای در حال استفاده را رهگیری کند به جزای نقدی از ده میلیون ریال تا یکصد میلیون ریال محکوم خواهد شد. نکات زیر در رابطه با ماده ۴ لایحه قانون جرایم رایانه ای از جمله نکاتی است که در تصویب این طرح می‌تواند مورد توجه قرار گیرد.

ماده ۴ پیش نویس قانون جرایم رایانه ای مانند مواد ۲ و ۳ به جرایم دسترسی و شنود غیرمجاز می پردازد با این تفاوت که موضوع این ماده داده های طبقه بندی شده رایانه‌ای است در حالی که موضوع مواد ۲ و ۳ داده های غیر طبقه بندی شده است. بنابراین با توجه به اینکه جرم موضوع این ماده جرم مستقل محسوب نمی‌شود، نیازی به اختصاص عنوان و موضوع جداگانه برای آن نبود. تهیه کنندگان می‌توانستند مجازات‌های شدیدتری را برای دسترسی غیرمجاز به سیستم‌های رایانه‌ای یا حامل های داده حاوی داده های طبقه بندی شده یا شنود غیرمجاز داده‌های طبقه بندی شده در مواد ۳ و ۲ این پیش نویس تعیین کنند.

ماده ۴ پیش نویس صرفاً به داده‌های محرمانه طبقه بندی شده می‌پردازد و در مورد داده های محرمانه و فوق محرمانه رایانه ای ساکت است. با توجه به اینکه دسترسی و شنود غیرمجاز داده‌های محرمانه رایانه‌ای نیز می‌تواند برای امنیت یک کشور خطرناک باشد، بهتر است در هنگام تصویب این پیش‌نویس، تکلیف دسترسی و رهگیری غیرمجاز داده‌های رایانه‌ای محرمانه مشخص شود.

داده‌های رایانه‌ای مخفی در واقع همان اسناد محرمانه دولتی هستند که به صورت دیجیتال تولید یا به داده‌های رایانه‌ای تبدیل شده‌اند. با توجه به اینکه قانون مجازات انتشار و افشای اسناد سری و دولتی مصوب ۲۹ بهمن ۱۳۵۳ و آیین‌نامه اجرایی آن، تعریف مشخصی از اسناد سری و محرمانه دولتی ارائه داده‌اند، نیازی به تدوین تعریف یا آیین‌نامه‌ای جدید برای این اسناد وجود ندارد. به‌ویژه که تعاریف ارائه‌شده در قانون و آیین‌نامه مذکور بسیار دقیق و کارشناسی شده هستند. همچنین پیش‌نویس تبصره ۱ ماده ۴ به دلیل مغایرت با تعاریف قانون ذکرشده، نیازمند اصلاح یا بازنگری است.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

مجازات تعیین شده برای دسترسی غیرمجاز و رهگیری استاد مخفی رایانه بسیار ملایم است. طبق ماده ۵۰۵ قانون مجازات اسلامی، جمع آوری اطلاعات طبقه بندی شده به قصد برهم زدن امنیت کشور از یک تا پنج سال حبس است.

۲-۲- جرایم علیه سیستم‌های مخابراتی

۱-۲-۲- جعل رایانه‌ای

ماده ۷ کنوانسیون جرائم سایبری بر جرم‌انگاری جعل رایانه‌ای تأکید دارد و کشورهای عضو این کنوانسیون را ملزم می‌کند قوانینی وضع کنند که مطابق با سیستم حقوقی داخلی آنها، هرگونه تغییر، حذف یا توقف عمدی و بدون مجوز داده‌های رایانه‌ای را که منجر به تولید داده‌های نادرست می‌شود، جرم تلقی کنند. این اقدام باید با هدف استفاده یا ارزیابی این داده‌های نادرست به‌جای داده‌های صحیح برای مقاصد قانونی صورت گیرد. لازم به ذکر است که این جرم شامل داده‌هایی می‌شود که چه به صورت مستقیم قابل خواندن و درک باشند و چه نباشند. بر این اساس، ماده ۷ جعل رایانه‌ای را تعریف می‌کند به‌عنوان هرگونه تغییر، حذف یا توقف عمدی و غیرمجاز داده‌های رایانه‌ای که منجر به ایجاد داده‌های نادرست شود، با نیت اینکه این داده‌ها به‌عنوان داده‌های درست برای اهداف قانونی مورد استفاده قرار گیرند یا مورد بررسی قرار گیرند؛ فارغ از اینکه این داده‌ها به‌طور مستقیم قابل خواندن و فهم باشند یا خیر (آزمایش، ۱۳۷۸، ۲۰).

۱. عنصر مادی

الف- رفتار مرتکب جرم جعل رایانه‌ای به‌صورت فعل مثبت انجام می‌گیرد و نمی‌توان آن را با ترک فعل محقق دانست. طبق ماده ۷ کنوانسیون جرایم سایبری، اقداماتی که به ارتکاب جعل منجر می‌شوند، به شکل حصری تعیین شده‌اند. این اقدامات شامل معرفی، تغییر، حذف، و قطع عمدی و غیرموجه داده‌های رایانه‌ای هستند، به طوری که نتیجه آن ایجاد داده‌های نادرست باشد.

ب- موضوع جرم جعل رایانه‌ای مرتبط با داده‌های رایانه‌ای است. داده‌های رایانه‌ای به این صورت تعریف می‌شوند: هر نوع نمایش از حقایق، اطلاعات یا مفاهیم که به شکلی مناسب برای پردازش در یک سیستم رایانه‌ای طراحی شده باشد، از جمله هر برنامه‌ای که قادر است سیستم رایانه‌ای را به انجام عملکرد خاصی وادارد. منظور از پردازش داده‌ها، انجام عملیات مشخص روی داده‌های رایانه‌ای

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

از طریق اجرای یک برنامه در یک سیستم رایانه‌ای است. برنامه رایانه‌ای نیز شامل مجموعه‌ای از دستورالعمل‌هاست که سیستم رایانه‌ای می‌تواند آن‌ها را اجرا کرده و به نتیجه موردنظر برسد.

ماده ۷ کنوانسیون جرائم سایبری بیان می‌کند که بدون توجه به این‌که داده‌ها به صورت مستقیم قابل خواندن و فهمیدن هستند یا نه، کشورهای عضو این کنوانسیون باید جعل آن‌ها را به عنوان جرم در نظر بگیرند. این بخش از ماده ۷ نشان می‌دهد که جرم جعل در لحظه ایجاد یا تغییر داده‌ها با نیت جعل، تحقق می‌یابد. جعل به عنوان مثال، به این بستگی ندارد که آیا داده‌های جعلی چاپ شده‌اند یا قابل مشاهده هستند. گزارش توضیحی مربوط به توصیه شماره ۹(۸۹) شورای اروپا درباره این موضوع بیان می‌کند که حمایت حقوق کیفری از داده‌های الکترونیکی باید به نحوی باشد که حتی زمانی که اطلاعات به صورت چاپی ارائه نمی‌شوند و به صورت مستقیم مثلاً در حالت پردازشی قرار دارند، تحت حمایت قرار گیرند. این امر به‌ویژه در خصوص فعالیت‌های بانکی و معاملات که تمام فرایند آن‌ها تنها در رایانه انجام می‌شود و نمود خارجی محسوسی ندارند، قابل توجه است (دزیانی، ۱۳۷۶، ۱، ۱۳۵).

ج- وسیله ارتکاب جرم: جعل کامپیوتری با استفاده از کامپیوتر انجام می‌شود. با این حال، ماده ۷ کنوانسیون جرایم سایبری، که معیارهای جرم‌انگاری جعل کامپیوتری را تعیین می‌کند، ابزار ارتکاب آن را مشخص نمی‌کند. جعل کامپیوتری می‌تواند با استفاده از امکانات شبکه انجام شود و شامل ارتکاب جرایمی مانند دسترسی و شنود غیرمجاز و همچنین داده‌های ذخیره شده در یک کامپیوتر غیر شبکه‌ای و روی یک حامل داده باشد. در این مورد، جعل نیازی به دسترسی یا شنود غیرمجاز ندارد (دزیانی، ۱۳۷۶، ۱، ۱۳۶).

د- عنصر ضرر در جرم جعل رایانه‌ای به‌عنوان یکی از موضوعات مهم در حقوق جزا محسوب می‌شود. اساتید حقوق جزا هنگام بررسی عناصر تشکیل‌دهنده جرم جعل کلاسیک، معمولاً بر عنصر ضرر تأکید دارند و آن را یکی از ارکان اساسی این جرم تلقی می‌کنند. اما منظور از "ضرر" دقیقاً چیست و آیا این عنصر در تمام موارد به‌عنوان بخش جدایی‌ناپذیر جرم جعل شناخته می‌شود؟

برای پاسخ به این پرسش‌ها، دیدگاه‌های مختلفی از سوی حقوق‌دانان مطرح شده است. برخی عنصر ضرر را ضرورتی برای جرم جعل می‌دانند، زیرا هدف جعل معمولاً تقلب، فریب یا وارد کردن زیان مادی یا معنوی به دیگران است. از سوی دیگر، گروهی معتقدند که صرف تغییر یا تحریف حقیقت، بدون توجه به بروز خسارت، ممکن است برای شکل‌گیری جرم جعل کافی باشد. بنابراین، با تحلیل

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

نظرات گوناگون و مبانی حقوقی مرتبط، می‌توان به برداشت روشنی از جایگاه عنصر ضرر در جرم جعل دست یافت.

در مورد نقش عنصر ضرر در ارتکاب جرم جعل کلاسیک، بیان شده که یکی از عناصر اصلی جرم جعل، امکان ایراد ضرر است. بر این اساس، اگر تغییر یا تحریف حقیقت در یک سند یا نوشته یا هر چیز دیگر توانایی ایجاد ضرر به دیگری را نداشته باشد، عمل انجام‌شده جرم تلقی نمی‌شود (پیمانی، ۱۳۷۵، ۱۱۸). به‌علاوه، در خصوص مبنای لزوم وجود عنصر ضرر در جعل، عده‌ای بر این باورند که منشأ این عنصر در قوانین وجود دارد، اما به طور صریح و مستقیم ذکر نشده است؛ بلکه این مفهوم طی زمان از سوی دکترین حقوقی از قوانین استنباط شده است (آزمایش، ۱۳۷۷، ۱۷).

۲. رکن معنوی جرم

الف- علم مرتکب: طبق ماده ۷ کنوانسیون جرایم سایبری، یکی از شرایط تحقق جرم جعل رایانه‌ای این است که اعمالی که منجر به ایجاد سند نامعتبر می‌شوند، باید بدون اختیار انجام شوند. بنابراین، علم به ماهیت غیرمجاز اعمال ورود، تغییر، حذف و عدم ارائه داده‌ها که منجر به ایجاد داده‌های نادرست می‌شوند، برای تحقق جرم جعل ضروری است.

ب- بر اساس ماده ۷ کنوانسیون جرایم سایبری، جرم جعل رایانه‌ای به عنوان یک جرم عمدی تعریف شده است که تحقق آن نیازمند سوء نیت عمومی مرتکب می‌باشد. سوء نیت عمومی در این زمینه به معنای داشتن قصد انجام اعمالی است که به ایجاد سند جعلی منجر می‌شوند. بنابراین، اگر فرد به صورت ناخواسته بخشی از داده را حذف کرده یا چیزی به آن اضافه کند، عمل او در دسته جعل قرار نمی‌گیرد. علاوه بر این، برای تحقق این جرم، وجود قصد در انجام اعمالی که منتج به جعل می‌شود، شرط اساسی محسوب می‌گردد.

ج- سوء نیت خاص: گرچه جرم جعل رایانه‌ای یک جرم مطلق محسوب می‌شود، اما برای تحقق آن علاوه بر علم و سوء نیت عام، وجود سوء نیت خاص نیز ضروری است. سوء نیت خاص در این جرم به معنای قصد کلاهبرداری مرتکب است. طبق ماده ۷ کنوانسیون جرایم رایانه‌ای، «این قصد با هدف استفاده از داده‌های نادرست به همان صورت و برای همان اهداف قانونی که داده‌های صحیح به کار می‌روند، شکل می‌گیرد.» در واقع، این نیت همان قصد متقلبانه تلقی می‌شود. کسانی که بر این باورند که در جرائم مطلق، سوءنیت خاص ضرورتی ندارد، قصد متقلبانه مرتکب جرم جعل را به‌عنوان انگیزه

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

تعریف کرده‌اند. برخی بر این نظرند که یکی از مواردی که در آن سوءنیت خاص با انگیزه تداخل می‌کند، همین بحث جعل است. بر این اساس، اگر تحقق جعل به نتیجه خاصی وابسته نباشد، قصد اضرار به‌جای سوءنیت خاص، به‌عنوان انگیزه تلقی می‌شود؛ چراکه سوءنیت خاص ناظر به نتیجه است و در جرائم مطلق، سوءنیت خاص نه امکان تحقق دارد و نه الزامی است (آزمایش، ۱۳۷۷، ۳۲).

۲-۲-۲- تخریب و ایجاد اختلال در داده‌ها

ماده چهار کنوانسیون جرائم سایبری به موضوع جرم اخلال در داده‌ها اختصاص دارد و مطابق آن مقرر شده است:

تمامی کشورهای عضو کنوانسیون موظف‌اند قوانین و مقرراتی را تنظیم کنند که بر مبنای حقوق داخلی، هرگونه اقدام عمدی و بدون مجوز به آسیب‌رسانی، حذف، خراب‌کردن، تغییر یا متوقف‌ساختن داده‌های رایانه‌ای را جرم تلقی نمایند. هر کشور عضو این کنوانسیون می‌تواند شرطی را برای خود قائل شود که تنها اعمال ذکرشده در بند اول را، در صورتی که منجر به خسارت جدی شود، جرم‌انگاری کند (دزیانی، ۱۳۸۰، ۲، ۳۴).

۱. عنصر مادی

الف- رفتار مرتکب: برای تحقق جرم نقض داده‌ها، فعل مثبت مرتکب لازم است. ترک فعل عنصر مادی نقض داده‌ها نیست. ماده ۴ کنوانسیون جرایم سایبری نمونه‌هایی از رفتار مجرمانه را که می‌تواند منجر به ارتکاب جرم نقض داده‌ها شود، فهرست می‌کند. این نمونه‌ها که جامع نیستند، عبارتند از:

۱- آسیب به داده‌ها

۲- فساد داده‌ها

۳- حذف کردن داده‌ها

۴- تغییر دادن داده‌ها

۵- توقف کردن داده‌ها

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

گزارش توجیهی کنوانسیون جرایم سایبری، اعمال مجرمانه مورد اشاره در بند ۱ ماده ۴ کنوانسیون یادشده به صورت زیر تعریف می‌شوند: آسیب رساندن به داده‌ها و خراب کردن آنها، که شامل هرگونه تغییر منفی در تمامیت یا محتوای اطلاعاتی داده‌ها و برنامه‌ها است. حذف داده‌ها به عنوان تخریبی مشابه با از بین بردن یک شیء فیزیکی و محسوس تعبیر می‌شود، به شکلی که امکان تشخیص و فهم آن‌ها از بین برود. متوقف کردن داده‌ها به هر عملی اطلاق می‌شود که مانع دسترسی افراد دارای مجوز به داده‌ها شده یا جریان اطلاعات را مختل کند. همچنین، تغییر داده‌ها به معنای هر گونه تبدیل و دگرگونی در داده‌ها است.» (پیمانی، ۱۳۷۵، ۱۴۷).

ب- موضوع جرم در دستکاری داده‌ها به مواردی اشاره دارد که داده‌ها، برنامه‌ها یا سیستم‌های رایانه‌ای مشمول دخالت، تغییر، تخریب، آسیب، حذف یا مختل کردن غیرمجاز از سوی مرتکب قرار می‌گیرند. برخلاف تخریب اشیاء مادی که موضوع جرم در آن مربوط به اشیاء متعلق به دیگری است، در جرم دستکاری داده‌ها چنین تعبیری وجود ندارد. بلکه از عبارت «مرتکب حق دسترسی به داده‌ها را ندارد» استفاده می‌شود که معنای وسیع و انعطاف‌پذیری داشته و جنبه‌های مختلفی از دسترسی غیرمجاز را پوشش می‌دهد.

ج- وسیله جرم: داده‌ها از جمله جرایمی هستند که وسیله ارتکاب آنها مورد توجه قانونگذار قرار نگرفته است. بنابراین، هرگونه عمل آسیب‌رسان، تغییر دهنده، نابود کننده، حذف کننده یا متوقف کننده داده‌ها به هر وسیله‌ای، جرم فساد داده‌ها محسوب می‌شود. این جرم ممکن است از طریق انتشار ویروس یا وارد کردن کرم رایانه‌ای، بمب منطقی یا اسب تروا به سیستم رایانه‌ای ارتکاب یابد. گزارش توجیهی کنوانسیون جرایم سایبری در این زمینه بیان داشت: «وارد کردن برنامه‌های مضر مانند ویروس‌ها و اسب‌های تروا به دلیل ایجاد تغییر در داده‌ها، مشمول جرم فساد داده‌ها می‌شود.» (جنیادی، ۱۳۸۳، ۳۵).

د- جرم دستکاری داده‌ها به‌عنوان یک جرم مقید به نتیجه، به‌طور ذاتی با اثری همراه است که از آسیب، تغییر، تحریف یا حذف داده‌ها بر اشخاص مرتبط با این داده‌ها نشأت می‌گیرد. سوال اصلی این است که آیا شخصی که حق دارد باید مستقیماً ضرر یا زیان وارده را ثابت کند، یا اینکه تحقق یکی از عناصر دستکاری برای اثبات کافی است. به نظر می‌رسد در این نوع از جرم، نیازی به اثبات مستقیم و جداگانه وقوع ضرر یا زیان نیست. دلیل این امر آن است که نتیجه جرم (ضرر یا زیان حاصل از دستکاری داده‌ها) با خود عمل مجرمانه در هم تنیده و گره‌خورده است. به بیان ساده‌تر،

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

عمل مجرمانه و نتیجه آن دو عنصر کاملاً مجزا نیستند که نیاز به بررسی و اثبات مستقل داشته باشند. ازاین‌رو، اثبات وقوع عمل دستکاری داده‌ها می‌تواند نشانگر وقوع نتیجه و تحقق جرم باشد و ضرری که مورد نظر است، ذاتاً در خود عمل محقق شده تلقی می‌شود.

۲. رکن معنوی

الف- علم مرتکب به غیرقانونی بودن اعمال مذکور شرط لازم برای تحقق این جرم است. جهل مرتکب به غیرقانونی بودن جعل داده‌ها منجر به عدم انطباق جرم خواهد شد. بنابراین، علم مرتکب به غیرقانونی بودن اعمال منجر به جعل داده‌ها، یکی از ارکان تشکیل‌دهنده جرم جعل داده‌ها را تشکیل می‌دهد.

ب- سوء نیت عام: طبق ماده ۴ کنوانسیون جرایم سایبری، جرم جعل داده‌ها یک جرم عمدی است. بنابراین، ارتکاب آن مستلزم سوء نیت عام مرتکب است. سوء نیت عام در این مورد عبارت است از اینکه اراده و خواست مرتکب به یکی از اعمالی که قصد آسیب رساندن، تغییر، تخریب، محو یا مسدود کردن داده‌ها را دارد، منتسب شود. قصد ارتکاب هر یک از اقدامات یادشده نشان‌دهنده سوء نیت کلی مرتکب است. بنابراین، اگر فرد بدون قصد قبلی، به‌صورت غیرعمدی یا بدون داشتن مجوز، یکی از اعمال مرتبط با جرم جعل داده‌ها را انجام دهد، این اقدام او جرم تلقی نخواهد شد

ج- سوء نیت خاص: اگرچه جرم جعل داده‌ها، جرمی وابسته به نتیجه است، اما از آنجا که نتیجه این جرم در عملی که منجر به جعل داده‌ها می‌شود، منحل شده و عمل مجرمانه و نتیجه جرم دو عنصر جداگانه نیستند، قصد نتیجه در حقیقت بخشی از قصد فعل محسوب شده و در آن مستتر است. از این‌رو، برای اثبات وقوع این جرم، کافی است سوء نیت عام مرتکب به اثبات برسد. در صورت ارتکاب هر یک از اعمال مذکور در ماده ۴ کنوانسیون توسط مرتکب، صرف نظر از انگیزه، جرم جعل داده‌ها محقق می‌شود؛ بنابراین، انگیزه مرتکب هیچ تأثیری در تحقق جرم جعل داده‌ها ندارد.

۳-۲- جرایم مرتبط با محتوا

چهار ماده از پیش نویس قانون جرایم رایانه ای از ماده ۹ تا ۱۳ به جرایم مرتبط با محتوا اختصاص یافته است. ماده ۹ در مورد جرایم مرتبط با هرزه نگاری بزرگسالان و ماده ۱۰ در مورد جرایم مرتبط با هرزه نگاری کودکان و تشویق آنها به ارتکاب جرم از طریق سیستم های رایانه ای اختصاص دارد

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

ماده ۱۱ در مورد نشر اکاذیب و ماده ۱۲ در مورد اهانت از طریق تغییر یا تحریف فیلم یا صوت افراد است.

۱-۳-۲- جرایم مرتبط با هرزه نگاری

مواد ۹ و ۱۰ لایحه قانون جرایم رایانه‌ای مقرر می‌دارد: «ماده ۹ هر فردی که اقدام به ارائه یا انتشار محتوای مستهجن از طریق سامانه‌های رایانه‌ای یا مخابراتی کند، یا این محتوا را موضوع هر نوع معامله قرار دهد و یا آن را با هدف انتشار یا تجارت تولید نماید، به مجازات تعیین‌شده در ماده ۶۴۰ قانون مجازات اسلامی مصوب سال ۱۳۷۵ محکوم خواهد شد. ماده ۱۰ هر کس با استفاده از حامل‌های داده رایانه‌ای یا مخابراتی مرتکب هر یک از اعمال زیر شود، به شرح زیر مجازات خواهد شد:

هر فردی که محتوای خلاف اخلاق را به افراد زیر ۱۸ سال ارائه دهد، یا اقدام به تولید، انتشار، ارائه یا معامله چنین محتوایی برای افراد زیر ۱۸ سال کند، همچنین اگر این محتوا را تهیه، نگهداری یا ذخیره نماید، به شدیدترین مجازات تعیین‌شده در ماده ۶۴۰ قانون مجازات اسلامی سال ۱۳۷۵ محکوم خواهد شد.

هر کسی افراد زیر ۱۸ سال را به دریافت محتوای مستهجن یا ارتکاب جرایم تحریک، تشویق، تهدید، اغوا یا فریب دهد و از طریق دریافت یا ارتکاب اعمال مذکور، آن‌ها را تسهیل یا آموزش دهد، به مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی محکوم خواهد شد. ج- هر کس محتوای مستهجن غیرواقعی مانند انیمیشن، نقاشی یا طراحی را ارائه، منتشر، تهیه، تولید، ذخیره یا نگه‌داری کند، به حداقل مجازات مقرر در ماده ۶۴۰ قانون مجازات اسلامی مصوب ۱۳۷۵ محکوم خواهد شد...»

۲-۳-۲- اهانت از طریق تحریف و تغییر فیلم یا صوت اشخاص

بر اساس ماده ۱۲ پیش‌نویس قانون جرایم رایانه‌ای، هر فردی که از طریق سامانه‌های رایانه‌ای یا مخابراتی اقدام به تغییر یا تحریف فیلم یا صدای شخصی نموده و آن را منتشر کند یا با اطلاع از تغییر یا تحریف، به انتشار آن بپردازد، به گونه‌ای که موجب هتک حرمت یا زیان رساندن به فرد دیگر شود، مطابق با مجازات تعیین‌شده در ماده ۶۴۰ قانون مجازات اسلامی مصوب سال ۱۳۷۵ مجازات خواهد شد. همچنین در تبصره این ماده تاکید شده است که اگر این عمل از جمله موارد تعرض به

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

نوامیس افراد باشد، مرتکب به حداکثر مجازات مقرر در هر سه بند از ماده ۶۴۰ قانون مجازات اسلامی مصوب ۱۳۷۵ محکوم خواهد شد.»

نکات ذیل در ارتباط با ماده ۱۲ پیش نویس قانون جرایم رایانه ای قابل توجه می‌باشد:

به نظر می‌رسد که کلمه ضرر در ماده مذکور زائد است. چه اینکه وارد آوردن ضرر به دیگری از طریق تحریف و تغییر فیلم با صدای آنها اگر توأم با هتک حرمت نباشد یا مصداق هرزه نگاری نباشد، یک امر حقوقی است که با ضمانت اجرای مدنی قابل جبران است. اگر تغییر و تحریف فیلم و صوت اشخاص صرفاً از مصادیق اهانت باشد اصولاً باید مرتکب به مجازات مقرر برای توهین به افراد ماده ۶۰۸ قانون مجازات اسلامی محکوم شود نه مجازات ماده ۱۴۰ قانون مجازات اسلامی که مربوط به هرزه نگاری. بنظر می‌رسد که اگر به جای اصطلاح منتشر سازد اصطلاح عرضه نماید در متن ماده ۱۲ پیش نویس قانون جرایم رایانه آورده شود بهتر است چرا که هتک حرمت با یک مرتبه عرضه کردن محتویات موضوع ماده ۱۰ تحقق می‌یابد.

منظور از عبارت تعرض به نوامیس مردم در متن تبصره ماده ۱۲ پیش نویس قانون جرایم رایانه مشخص نیست. تعرض به معنی دست درازی کردن است و نوامیس یک اصطلاح کلی است که می‌تواند مورد تفاسیر متعدد واقع شود.

۴-۲- جرایم رایانه ای مرتبط با اقدامات دارای ماهیت نژاد پرستانه

ماده ۲ پروتکل الحاقی کنوانسیون جرائم سایبری، محتوای نژادپرستانه و ضد بیگانه را به این صورت تعریف کرده است: «هر گونه متن نوشته‌شده، تصویر یا هر شکل دیگری از بیان عقاید و نظرات که به نحوی نفرت، تبعیض یا خشونت علیه فرد یا گروهی را بر اساس نژاد، رنگ پوست، تبار، یا منشاء ملی و قومی آنها، و همچنین مذهب‌شان در صورتی که مذهب نقش پوششی برای دیگر عوامل ذکر شده در این تعریف داشته باشد، حمایت، ترویج یا تحریک کند»طبق تعریف فراداده با محتوای نژادپرستانه و بیگانه ستیزانه، دارای سه ویژگی به شرح زیر است: برخلاف پورنوگرافی کودکان که فقط شامل داده های رایانه ای، تصاویر و ویدیوها می شود، محتوای نژادپرستانه و بیگانه ستیزانه شامل انواع داده های رایانه ای از جمله متن، صدا، تصویر و ویدیو می شود (عالی پور، ۱۳۸۳، ۱۰۵).

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۱-۴-۲- جرم پخش مطالب نژاد پرستانه از طریق سیستم‌های رایانه ای و فناوری‌های نوین

ماده ۳ پروتکل الحاقی کنوانسیون جرایم سایبری، در مورد جرم‌انگاری انتشار محتوای نژادپرستانه و بیگانه‌ستیزانه از طریق سیستم‌های رایانه‌ای، بیان می‌کند:

۱- هر کشور عضو موظف است براساس قوانین داخلی خود، مقررات و قوانین لازم را وضع کرده و اقدامات عمدی و غیرمجاز ذکر شده را به عنوان جرم تعریف کند.

انتشار یا ارائه عمومی مطالب نژادپرستانه و مروج بیگانه‌هراسی از طریق سامانه‌های رایانه‌ای

۲- هر کشور عضو می‌تواند، در مواردی که محتوای مذکور در بند ۱ ماده ۲ پروتکل، بدون همراهی با خشونت یا نفرت، تبعیض را تحریک یا تشویق کند، از اعمال مسئولیت کیفری برای اعمال مذکور در بند ۱ این ماده خودداری کند، مشروط بر اینکه سایر راه‌های جبران مؤثر در دسترس باشد.

۳- در مواردی که اصول آزادی بیان در نظام حقوقی داخلی هر یک از طرفین، راهکارهای بند ۲ این ماده را مغایر با قوانین خود بداند، می‌توانند بند ۱ را در شرایطی که شامل تحریک به تبعیض، خشونت، یا نفرت نباشد، اعمال کنند. این امر صرف نظر از بند ۲ است، و تنها در صورتی مجاز است که اصول آزادی بیان در آن نظام حقوقی، چنین اقدامی را قابل قبول بداند خودداری کند.» (جعفرپور، ۱۳۸۱، ۴۹).

عنصر مادی:

الف- رفتار مجرمانه در جرم انتشار محتوای نژادپرستانه، عنصر اساسی و رکن مادی جرم محسوب می‌شود. این جرم تنها با انجام فعل مشخصی محقق می‌شود و عدم انجام آن، مجازات‌پذیر نیست. انواع رفتارهای مجرمانه‌ای که می‌توانند در این جرم دخیل باشند شامل اقدامات و اعمال آگاهانه‌ای هستند که منجر به انتشار محتوا یا اظهاراتی با مضمون نژادپرستانه می‌گردند. بنابراین، عنصر اصلی در این جرم، انجام یک رفتار فعالانه توسط مرتکب است. تلاش برای انتشار محتوای نژادپرستانه و ضدبیگانه‌پرستانه به عموم از طریق سیستم‌های کامپیوتری بدون مجوز. تلاش برای در دسترس قرار دادن محتوای نژادپرستانه و ضدبیگانه‌پرستانه به عموم از طریق سیستم‌های کامپیوتری بدون مجوز. در واقع، انتشار چنین محتوایی به دیگران نوعی توزیع غیرفعال را تشکیل می‌دهد: در توزیع فعال،

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

توزیع‌کننده مشتری را مخاطب قرار می‌دهد، در حالی که در توزیع غیرفعال (عرضه)، مشتری توزیع‌کننده را مخاطب قرار می‌دهد.

ب- هدف از این جرم، مقابله با انتشار محتوای نژادپرستانه و بیگانه‌ستیزانه است. طبق پروتکل الحاقی کنوانسیون، جرائم سایبری شامل محتوایی است که بر اساس نژاد، رنگ پوست، نسب، یا ریشه ملی و قومی، نفرت، تبعیض یا خشونت را ترویج می‌کند. این محتوا همچنین شامل مواردی است که بر اساس مذهب، به عنوان عاملی برای تبعیض، نفرت یا خشونت علیه افراد یا گروه‌هایی با عقاید و نظرات متفاوت، تحریک و تشویق می‌شود.»

ج- وسیله جرم: جرم نژادپرستی و بیگانه‌ستیزی در فضای مجازی، به استفاده از سیستم‌های رایانه‌ای برای انتشار محتوا بستگی دارد. طبق ماده ۳ پروتکل الحاقی کنوانسیون جرایم سایبری، این نوع محتوا باید از طریق رایانه منتشر شود تا جرم محسوب شود. به این معنی که اگر محتوای نژادپرستانه به صورت آنلاین تولید شود، اما به اشتراک گذاشته نشود یا به صورت فیزیکی بر روی حامل‌های داده توزیع گردد، مشمول این ماده نخواهد بود.

۲-۴-۲- جرم تهدید با نیت نژاد پرستانه از طریق فناوری‌های نوین

جرم نژادپرستی و بیگانه‌ستیزی در فضای مجازی، به استفاده از سیستم‌های رایانه‌ای برای انتشار محتوا بستگی دارد. طبق ماده ۴ پروتکل الحاقی کنوانسیون جرایم سایبری، این نوع محتوا باید از طریق رایانه منتشر شود تا جرم محسوب شود. به این معنی که اگر محتوای نژادپرستانه به صورت آنلاین تولید شود، اما به اشتراک گذاشته نشود یا به صورت فیزیکی بر روی حامل‌های داده توزیع گردد، مشمول این ماده نخواهد بود.

عنصرمادی: جرم تهدیدهای نژادپرستانه و بیگانه‌هراسانه، شامل سه عنصر اساسی است: رفتار مجرمانه، هدف جرم و وسیله‌ای که جرم با آن انجام می‌شود.

الف- رفتار مرتکب: در این جرم، مرتکب با انجام فعل مجرمانه، تهدیدی ناعادلانه و عمدی علیه افراد یا گروهی خاص به دلیل نژاد، نسب، رنگ، ملیت، قومیت، یا مذهب آنها مطرح می‌کند. این تهدید باید جدی و سنگین باشد، به طوری که ترس از وقوع جرمی مهم را در قربانیان ایجاد کند. طبق پروتکل الحاقی کنوانسیون جرایم سایبری، این جرم شامل ترساندن اشخاص به نحوی است که

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

قربانیان احساس خطر جدی برای زندگی، تمامیت جسمانی، امنیت شخصی، یا خسارت به اموال خود یا بستگانشان را تجربه کنند. تعیین مصادیق دقیق این جرم بر عهده کشورهای مختلف است تا در قوانین خود مشخص نمایند (آزمایش، ۱۳۷۸، ۶۷).

ب- موضوع جرم: در برخی موارد، افراد با هویت‌های مشخص، به واسطه ویژگی‌های خاص خود، هدف جرم قرار می‌گیرند. ماده ۴ بیان می‌کند که قربانی جرم لزوماً به یک فرد خاص محدود نمی‌شود. به عنوان مثال، اگر فردی اعضای یک گروه قومی را تهدید به قتل کند، تمام افراد آن گروه، قربانیان بالقوه محسوب می‌شوند. در این شرایط، استدلال متهم مبنی بر تهدید نکردن یک فرد خاص، قابل قبول نخواهد بود. این بدان معناست که قربانی جرم می‌تواند شامل افرادی با ویژگی‌های مشترک باشد و محدود به یک نام خاص نیست.

ج- وسیله ارتکاب جرم: طبق ماده ۴ پروتکل الحاقی کنوانسیون جرایم سایبری، وسیله ارتکاب جرم یکی از عناصر مادی جرم رایانه‌ای تهدیدات نژادپرستانه و بیگانه‌ستیزانه را تشکیل می‌دهد. این ماده مقرر می‌دارد که تهدید باید از طریق سیستم رایانه‌ای انجام شود. تا جرم موضوع این ماده تحقق پیدا کند. عبارت از طریق یک سیستم رایانه ای دلالت بر این دارد که تهدید باید از طریق ارتباطات الکترونیکی صورت گرفته باشد تا جرم موضوع این ماده تحقق پیدا کند. چنین عملی ممکن است مشمول قوانین کلاسیک شود.

۳-۴-۲- جرم اهانت با نیت نژاد پرستانه از طریق فناوری‌های نوین

بر اساس ماده ۵ پروتکل الحاقی به کنوانسیون جرائم سایبری، «کشورهای عضو ملزم به جرم‌انگاری رفتارهایی هستند که به قصد توهین نژادپرستانه و ضد بیگانه انجام می‌شود. این ماده بیان می‌کند که هر کشور باید قوانینی وضع کند که اهانت علنی از طریق سیستم‌های رایانه‌ای را جرم بداند، به خصوص اگر این توهین‌ها بر اساس نژاد، رنگ پوست، نسب، قومیت، ملیت، یا مذهب افراد یا گروه‌های خاصی باشد. این ماده همچنین به کشورهای عضو اجازه می‌دهد تا شرایط تشدید جرم را تعیین کنند، به این صورت که اگر توهین منجر به نفرت، تحقیر، یا تمسخر شود، مجازات‌های سنگین‌تری اعمال خواهد شد. همچنین، کشورها می‌توانند با استفاده از حق شرط، از اجرای کامل یا جزئی این ماده خودداری کنند.» (آزمایش، ۱۳۷۸، ۵۶).

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

رکن مادی و معنوی: این جرم با ترک فعل محقق نمی‌شود. رفتار مجرمانه مرتکب در این جرم شامل توهین عمدی و بدون حق به صورت علنی به یک شخص یا گروهی از اشخاص از طریق سیستم رایانه‌ای صرفاً به این دلیل است که آنها یا واقعاً به یک گروه تعلق دارند یا تصور می‌شود که به گروهی تعلق دارند که با ویژگی قومی یا نژادی خاصی از دیگران متمایز می‌شود (روحانی، ۱۳۸۰، ۳۸).

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

نتیجه‌گیری

جرایم مرتبط با فناوری اطلاعات، تحت قوانین موجود، قابل پیگرد و مجازات هستند. این جرایم متنوع بوده و می‌توان آنها را به چند دسته تقسیم‌بندی کرد: جرایم علیه افراد، اموال، امنیت عمومی، اخلاقیات و خانواده. سازمان‌های بین‌المللی بر اهمیت قانونگذاری ویژه برای این جرایم تأکید دارند. این جرایم را می‌توان به سه گروه کلی تقسیم کرد. گروه اول، جرایمی هستند که با ظهور فناوری اطلاعات، امکان وقوع آنها فراهم شده است. دسته دوم، جرایمی با ماهیتی متفاوت از جرایم سنتی، که نیازمند قوانین خاص خود هستند. و در نهایت، جرایم سنتی که با استفاده از فناوری اطلاعات، خطرات و پیامدهای جدی‌تری به همراه دارند و نیازمند توجه ویژه قانونگذاران است. جرایم مرتبط با امنیت سایبری، شامل مواردی مانند دسترسی غیرمجاز، شنود، دستکاری داده‌ها و سیستم‌ها، و سوءاستفاده از دستگاه‌های رایانه‌ای است. این جرایم، محرمانگی، تمامیت و دسترس‌پذیری داده‌ها و سیستم‌ها را به خطر می‌اندازد. در نتیجه با هیچ یک از قوانین مربوط به جرایم کلاسیک قابل مجازات نیستند و چون ارتکاب آنها محرمانگی و تمامیت داده‌ها و سیستم‌های رایانه‌ای را به مخاطره انداخته است سازمانهای جهانی و منطقه ای بالاتفاق از کشورهای عضو خواسته‌اند نسبت به جرم انگاری آنها اقدام نمایند تعریف و عناصر اختصاصی جرائم مذکور در این تحقیق مورد بررسی قرار گرفته‌اند.

طی این تحقیق پیشنهادات زیر را ارائه می‌گردد:

استفاده از وسایل امنیتی علی الخصوص دستبند الکترونیکی که نیاز به رضایت مجرم دارد، متضمن هزینه‌های سنگینی است، از همین رو دولت و متصدیان دستگاه قضا باید تدابیری از جمله استفاده رایگان برای عموم اتخاذ نمایند تا افراد فقیر و کسانی که تمکن مالی مناسبی ندارند، از این دستگاه‌ها استفاده کرده و از محیط نامناسب زندان رهایی یابند.

استفاده گسترده از رسانه‌های دیجیتالی مثل اینترنت و شبکه‌های اجتماعی سبب شده است تا تحت تاثیر شدید آن‌ها قرار بگیرند، لذا لازم است دولت و خصوصا خانواده‌ها در راستای کاهش این مسائل کوشا باشند. از اقدامات مثمرثمری که می‌شود در این زمینه صورت پذیرد فرهنگ سازی هشدار خطرات و عوارض آن‌ها و آموزش استفاده صحیح از این رسانه‌ها می‌باشد و تحت نظارت قرار دادن آن‌ها و همراهی آن‌ها زمانی که از این رسانه ها استفاده می‌کنند، است.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

منابع

۱- ابن منظورابوالفضل، محمد بن مکرم، (۱۴۱۴)، لسان العرب، تحقیق: احمد فارس صاحب الجوائب، بیروت، دار الفکر للطباعه للنشر و التوزیع.

۲- ابوزهره، محمد، (۱۹۹۸)، الجریمه والعقوبه فی الفقه الاسلامی، قاهره: دار الفکر العربی.

۳- امینیان، امیر، (۱۳۹۲)، بررسی رابطه بین فناوری اطلاعات و توانمندسازی کارکنان با توجه به نقش میانجی فرهنگ سازمانی، پایان نامه کارشناسی ارشد، دانشکده علوم انسانی دانشگاه آزاد شاهرود.

۴- آزمایش، سیدعلی، (۱۳۷۷)، تقریرات درس حقوق جزای اختصاصی کارشناسی ارشد، دانشکده حقوق و علوم سیاسی دانشگاه تهران.

۵- آزمایش، سیدعلی، (۱۳۷۸)، تقریرات درس حقوق کیفری بین المللی مقطع کارشناسی ارشد دانشکده حقوق و علوم سیاسی دانشگاه تهران.

۶- پاکزاد، بتول، (۱۳۸۸)، تروریسم سایبری، پایان نامه دکتری، دانشگاه شهید بهشتی.

۷- پیمانی، ضیاء الدین، (۱۳۷۵)، جرائم علیه امنیت و آسایش عمومی نشر میزان، تهران، نشر دادگستر.

۸- تحیری، فرزاد، (۱۳۸۳)، دسترسی غیرمجاز جلوه‌ای ازجرائم رایانه‌ای محض، مجموعه مقالات همایش ابعاد حقوقی فناوری اطلاعات خرداد.

۹- جعفرپور، ناهید، (۱۳۸۱)، گزارش توجیهی توصیه نامه شماره (۹۵) R شورای اروپا ناظر به مشکلات آیین دادرسی کیفری مربوط به فناوری اطلاعات خبرنامه انفورماتیک، نشریه دبیرخانه شورای عالی انفورماتیک کشور، شماره ۸۱.

۱۰- جینادی، آنجلیز، (۱۳۸۳)، جرائم سایبر، ترجمه عبدالصمد خرم آبادی و سعید حافظی انتشارت شورای عالی اطلاع رسانی، تهران.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۱۱- حاج فتحعلی‌ها، عباس و سید اصفهانی، مهدی، (۱۳۷۲)، توسعه تکنولوژی (بررسی مفاهیم و فرآیند تصمیم گیری‌ها)، تهران، انتشارات دانشگاه علامه طباطبایی.

۱۲- دزیانی، محمدحسن، (۱۳۸۱)، گزارش جرایم رایانه‌ای: مقررات حقوقی لازم، سازمان ملی، شورای عالی علوم رایانه‌ای.

۱۳- دزیانی، محمدحسن، (۱۹۹۷)، جرم رایانه‌ای: بررسی دستاوردهای شورای اروپا، ترجمه شده در کتاب راهنمای جرم رایانه‌ای، جلد ۱، دبیرخانه شورای عالی انفورماتیک.

۱۴- راغب اصفهانی، حسین بن محمد، (۱۴۱۲)، مفردات ألفاظ القرآن، لبنان، دار العلم ـ الدار الشامیه.

۱۵- روحانی، محمدخیام، (۱۳۸۰)، جرائم کامپیوتری خبرنامه انفورماتیک، دبیرخانه شورای عالی انفورماتیک، ش۷۷ فروردین.

۱۶- عالی پور، حسن، (۱۳۸۳)، جرائم مرتبط با محتوا مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات.

۱۷- عمید، حسن، (۱۳۸۰)، فرهنگ فارسی عمید، تهران، انتشارات امیرکبیر.

۱۸- فتحیان، محمد و مولاناپور، رامین، (۱۳۹۰)، تجارت الکترونیکی، انتشارات آتی نگر.

۱۹- فیض، علی‌رضا، (۱۳۷۹)، تطبیق و مقارنه در حقوق جزای عمومی اسلام، تهران، سازمان چاپ و انتشارات وزارت فرهنگ و ارشاد اسلامی.

۲۰- گرجی، ابوالقاسم، (۱۳۷۸)، مقالات حقوقی، تهران، مؤسسه انتشارات و چاپ دانشگاه تهران.

۲۱- محسنی، مرتضی، (۱۳۷۵)، دوره حقوق جزای عمومی پدیده جنایی، گنج دانش تهران.

۲۲- محمود زاده، ابراهیم، (۱۳۸۹)، مدیریت بر آینده با تکنولوژی فردا، انتشارات انستیتوایزایران.

ISSN: ۲۷۸۳-۱۳۲۹
شماره مجوز انتشار: ۸۷۰۱۹

An Analysis of the Impact of Emerging Technologies on the Commission of Crime

Mohammad Ali Ghorbani[1]/ Seyed Ahmad Peyrovnaziri[2] / Amirreza Mahmoudi[3]

Article Number: JHVMN-۲۵۰۵-۱۲۹۳

Abstract

New technologies have influenced all economic and social activities. Cyberspace has created conditions where offenders can commit crimes in locations other than where the effects and consequences of their actions appear. Information technology crimes are divided into two categories. The first group includes a range of computer-related offenses that can be prosecuted and punished under existing classical criminal laws. This group encompasses various crimes, which can be classified into categories such as crimes against individuals, property, public security, and public order. The second group comprises a set of cybercrimes that require special legislation. These types of crimes can also be classified into three categories: the first includes offenses that could not have been committed before the advent of information technology, such as unauthorized access; the second includes classical crimes.

On the other hand, technology also has a positive impact on crime prevention. Tools such as CCTV cameras and coded alarm systems help deter criminal activity, while the media, through functions like education and the dissemination of religious and security teachings, can play a role in the social prevention of crime. Despite these positive and effective functions, the mentioned technologies also have negative aspects, including the violation of the right to privacy and the intrusion into individuals' private lives.

Keywords: New technologies, crime commission, cybercrime, data disruption.

[1] Assistant Professor, Department of Islamic Theology and Teachings, La.C., Islamic Azad University, Lahijan, Iran. (Corresponding Author) Dr.alighorbani@gmail.com
[2] Master of Criminal Law and Criminology, Department of Law, La.C., Islamic Azad University, Lahijan, Iran. Seyedahmad.peyrovnaziri@iau.ir
[3] Assistant Professor, Department of Law, La.C., Islamic Azad University, Lahijan, Iran . amirreza.mahmodi@iau.ir