فصلنامه بین المللی قانون یار

License Number: 78864 Article Cod:Y6SH24A27458 ISSN-P: 2538-3701

بررسی جرم اخلال در شبکه های رایانه ای و مخابراتی

(تاریخ دریافت ۱۴۰۱/۰۷/۱۵، تاریخ تصویب ۱۴۰۱/۱۲/۱۸)

دکتر حسین یاراحمدی[۱]

غزاله طالبی

چکیده

جرم اخلال در شبکه های رایانه ای و مخابراتی یکی از جرائم نوظهور در عرصه حقوق جزا می باشد. نباید تصور کرد که فعالیت در دنیای مجازی، فاقد اعتبار و پیامدهای حقوقی است، بلکه به همان اندازه و در مواردی حتی بیشتر از نمونه های دنیای فیزیکی، آثار حقوقی به دنبال دارد. بخشی از زندگی اجتماعی، فرهنگی، علمی و اقتصادی انسان های امروزی در اینترنت و به طور کلی در دنیای سایبر و فضای مجازی در جریان است و طبیعی است که دولت ها به فکر تامین امنیت و نیز حفظ حقوق و آزادی های مدنی مردم در دنیا نیز باشند.آگاهی نداشتن جامعه در مورد یکسری جرم ها که به ظاهر ممکن است جرم به شمار نیایند و قابل لمس هم نباشند و به صورت مجازی و غیر قابل ملموس در محیط های مجازی صورت گیرند، سبب شده که موضوع اخلال در فضای مجازی و سامانه های رایانه ای از اهمیت دو چندانی برخوردار باشد. در این راستا برابر قانون هیچ کس حق ندارد به عمد در سیستم‌های رایانه ای اخلال ایجاد کند. یعنی هیچ کس حق ندارد داده هایی را که در سیستم های رایانه ای وجود دارد با صلاحدید خود حذف یا تخریب کند و حتی مختل یا غیر قابل پردازش کردن این داده ها نیز جرم است. در این رابطه و به علت اهمیت بسیار بالای موضوع در مقاله حاضر قصد داریم به بررسی جرم اخلال در شبکه های رایانه ای و مخابراتی بپردازیم.

واژگان کلیدی: فضای مجازی، شبکه رایانه ای، فضای مجازی، جرایم سایبری، مختل کردن سامانه ها، داده رایانه ای

[۱] نویسنده مسئول

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹

بخش اول: کلیات

بند اول: بررسی و شناخت سیستم رایانه ای

سیستم رایانه‌ای[۱]، هر دستگاه یا مجموعه‌ای از دستگاه‌های بهم متصل شده است که یک یا چند تا از آنها مطابق یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهند؛[۲] به عبارت دیگر دستگاهی است که از نرم‌افزار و سخت‌افزاری که برای پردازش خودکار داده‌های دیجیتال طراحی شده تشکیل یافته و ممکن است شامل ورودی، خروجی و امکانات ذخیره‌ساز اطلاعات شود، سیستم رایانه‌ای می‌تواند به صورت مستقل یا متصل به شبکه‌ای از سایر دستگاه‌های مشابه عمل کند. منظور از «خودکار»[۳] این است که انسان دخالت مستقیم ندارد. منظور از «پردازش داده‌ها»[۴] این است که داده‌های سیستم رایانه‌ای با اجرای یک برنامه ی رایانه‌ای عمل کنند. یک «برنامه رایانه‌ای»[۵] مجموعه‌ای از دستورالعمل‌هاست که رایانه می‌تواند آنها را برای نتیجهٔ موردنظر اجرا کند. رایانه می‌تواند برنامه‌های مختلفی اجرا کند. معمولاً سیستم رایانه‌ای از دستگاه‌های مختلفی تشکیل شده است که به پردازشگر یا واحد پردازش مرکزی و وسایل جانبی تفکیک می‌شوند. یک «وسیلهٔ جانبی»[۶] دستگاهی است که کارکردهای خاصی را در برهم‌کنش با واحد پردازشگر انجام می‌دهد، نظیر چاپگر، نمایشگر، خواننده یا نگارشگر لوح فشرده یا سایر وسایل ذخیره‌ساز.

بند دوم: داده

«داده رایانه‌ای»[۷] هرگونه نماد حقایق، اطلاعات یا مفاهیم به شکلی مناسب برای پردازش در یک سیستم رایانه‌ای است که شامل برنامه‌ای می‌شود که برای کارکرد یک سیستم رایانه‌ای

۱- Computer System

۲- کنوانسیون جرایم سایبر و پروتکل الحاقی آن، ترجمه امیرحسین جلالی فراهانی، تهران، انتشارات خرسندی، ۱۳۸۹، ص ۱۹.

۳- Automatic

۴- Processing of Data

۵- Computer Program

۶- Peripheral

۷- Computer Data

مناسب است؛ [۱] تعریف داده رایانه‌ای، از تعریف مؤسسه بین‌المللی استاندارد [۲] از داده‌ها اقتباس شده است. این تعریف حاوی عبارت «مناسب برای پردازش» [۳] است؛ یعنی داده‌ها به شکلی وارد شوند که بتوان آنها را مستقیماً بوسیلهٔ سیستم رایانه‌ای پردازش کرد. برای اینکه احراز شود داده‌های موردنظر این کنوانسیون باید به صورت الکترونیکی یا سایر اشکال قابل پردازش مستقیم باشند، تعبیر «داده رایانه‌ای» بکار رفته است.

بند دوم: اینترنت

اینترنت [۴] سامانه‌ای جهانی از شبکه‌های رایانه‌ای بهم پیوسته‌است که از پروتکل مجموعه پروتکل اینترنت برای ارتباط با یکدیگر استفاده می‌نمایند. به عبارت دیگر اینترنت، شبکه ی شبکه هاست که از میلیون‌ها شبکه خصوصی، عمومی، دانشگاهی، تجاری و دولتی در اندازه‌های محلی و کوچک تا جهانی و بسیار بزرگ تشکیل شده‌است که با آرایه ی وسیعی از فناوریهای الکترونیکی و نوری به هم متصل گشته‌اند. اینترنت در برگیرنده منابع اطلاعاتی و خدمات گسترده ایست که برجسته‌ترین آنها وب جهان‌گستر [۵] و رایانامه می‌باشند. سازمان‌ها، مراکز علمی و تحقیقاتی و موسسات متعدد، نیازمند دستیابی به شبکه اینترنت برای ایجاد یک وب‌گاه، انجام تحقیقات و یا استفاده از سیستم رایانامه [۶]، می‌باشند. بسیاری از رسانه‌های ارتباطی سنتی مانند تلفن و تلویزیون نیز با استفاده از اینترنت تغییر شکل داده اند و یا مجدداً تعریف شده اندو خدماتی جدید همچون صدا روی پروتکل اینترنت و تلویزیون پروتکل اینترنت ظهور کردند.

۸- کنوانسیون جرایم سایبر و پروتکل الحاقی آن، ترجمه امیرحسین جلالی فراهانی، تهران، انتشارات خرسندی، ۱۳۸۹، ص ۲۰.

۹- The International Organization for Standardization (ISO)

۱۰- Suitable for Processing

۱۱- مخفف کلمه ی inter connected network به معنای شبکه های به هم مرتبط می باشد که اختصازاً به آن Internet می گویند.

۱- مخفف کلمه ی World Wide Web یک سامانهی اطلاعاتی از پرونده‌های ابر متنی متصل به هم است که از طریق شبکهی جهانی اینترنت قابل دسترسی هستند.

۲- رایانامه یا Email به پیامی دیجیتالی گفته می‌شود که در شبکه‌ای رایانه‌ای از یک فرستنده به یک یا چند گیرنده فرستاده می‌شود.

غالباً در گفتگوهای روزمره از دو واژه ی"وب" و "اینترنت"، به اشتباه، بدون تمایز زیادی استفاده می‌شود، امااین دو واژه معانی متفاوتی دارند. اینترنت یک سامانه ارتباطی جهانی برای داده هاست، زیرساخت‌های نرم‌افزاری و سخت‌افزاری است که رایانه‌ها در سراسر جهان به یک‌دیگر متصل می‌سازد. در مقابل، وب یکی از خدماتی (سرویس) است که بر روی اینترنت ارائه می‌شود و برای ارتباط از شبکه اینترنت بهره می‌جوید. وب مجموعه ای از نوشته های به هم پیوسته است که به کمک ابر پیوندها و آدرس جهانی به یکدیگر پیوند خورده‌اند. وب شامل سرویس های دیگر مانند رایانامه، انتقال فایل، گروه خبری و بازی آنلاین است. البته ناگفته نماند که خدمات و سرویس های یاد شده بر روی شبکه های مستقل و جدا از اینترنت نیز در دسترس هستند.

بند سوم: فضای سایبر

سایبر واژه ای است بر گرفته از لغت «kybernetes» به معنای سکاندار یا راهنما و نخستین کسی که واژه فضای سایبر را به کار برد، ویلیام گیتسون نویسنده داستان های علمی- تخیلی، در کتاب نورومنسر بود. فضای سایبر یا فضای مجازی در تعریف برخی نویسندگان عبارت است از: "مجموعه ای از ارتباطات درونی انسان ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی است." البته شاید بهتر باشد آن را چنین تعریف کنیم: "محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص، خود؛ در آن، زنده و مستقیم روی می‌دهد". قید "واقعی"، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیر واقعی بودن آن است؛ چرا که در این فضا نیز همان ویژگی های تعاملات انسانی در دنیای خارج همچون مسئولیت وجود دارد. ضمن این که فضای سایبر در واقع یک "محیط" است که ارتباطات در آن انجام می‌شود؛ نه صرف مجموعه ای از ارتباطات. از سوی دیگر، این ارتباطات گرچه ممکن است در همه حال بر خط نباشد، ولی زنده و واقعی و مستقیم است. از این رو، تأثیر و تأثر بالایی در این روابط رخ می‌دهد. به عبارت دیگر فضای سایبر عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد.

ارائه دهنده ی خدمات: واژه ارائه‌دهندهٔ خدمات گروه گسترده‌ای از اشخاص را دربرمی‌گیرد که با توجه به ارتباط یا پردازش داده‌ها بر روی سیستم‌های رایانه‌ای، نقش خاصی ایفا می‌کنند. بر اساس بند نخست این تعریف، هر دو گروه نهادهای خصوصی و نهاد عمومی که برای کاربران امکان برقراری ارتباط با یکدیگر را فراهم می‌آورند، مشمول آن می‌شوند. بنابراین، چه کاربران گروه بسته‌ای را تشکیل دهند و چه ارائه‌دهنده خدمات خود را به عموم ارائه دهد و چه به صورت رایگان باشد و چه درازای دریافت هزینه، تفاوتی نمی‌کند. برای مثال، گروه بسته می‌تواند کارمندان یک بنگاه خصوصی باشند که خدمات توسط شبکهٔ شرکت ارائه می‌شود. لازم به ذکر است که امروزه ارائه دهندگان خدمات به صورت شرکت های خصوصی در آمده اند که دولت بر آنها نظارت می کند.

در بند دوم تعریف، این موضوع تبیین شده که واژه «ارائه‌کنندهٔ خدمات» شامل اشخاصی نیز می‌شود که داده‌ها را به جای اشخاص مذکور در بند نخست ذخیره یا به نحو دیگری پردازش می‌کنند. همچنین، این واژه شامل مجموعه‌هایی نیز می‌شود که داده‌ها را به جای کاربران خدمات مندرج در بند نخست ذخیره یا پردازش می‌کنند. برای مثال، بر اساس این تعریف، ارائه‌دهندهٔ خدمات، علاوه بر خدمات میزبانی و انباشت موقت اتصال به شبکه را هم تأمین می‌کند. با این حال، یک ارائه‌دهندهٔ صرف محتوا (مانند شخصی که با یک شرکت میزبان وب جهت میزبانی وب سایتش قرارداد می‌بندد)، اگر خدمات ارتباطی یا پردازش داده‌های مربوط را ارائه نکند، مشمول این تعریف نخواهد شد.

بخش دوم: بررسی و تحلیلی کیفری و مبانی قانونی جرم اخلال در شبکه های رایانه ای

علوم و فنون جدید، گاه خدماتی را به انسان عرضه داشته و گاه زیان هایی را به او بار نموده اند. یکی از این علوم جدید علم برنامه نویسی رایانه هاست که اگر چه توانسته است بسیاری از نیازهای انسان را برآورده نماید لیکن عده ای سودجو یا بزهکار، با تهیه و تولید برنامه های خاصی، به حمله علیه کاربران رایانه ای پرداخته اند. بسیاری از برنامه نویسان رایانه ای در سرتاسر دنیا، ماه ها و سال ها تمام تلاش خود را برای نوشتن برنامه هایی صرف می کنند که تنها حاصلش تخریب، اخلال و سوء استفاده از رایانه هاست. این افراد، برنامه های خود را

همچون روباتی تخریب گر آماده نموده و به طرق مختلف از قبیل شبکه ها و حامل های داده (از قبیل دیسک ها، حافظه های فلش، فلاپی ها) به رایانه های قربانی ارسال کرده و با استفاده از آن ها به تخریب نرم افزاری و سخت افزاری رایانه های قربانیان خود می پردازند. برنامه هایی از قبیل Subv [1] و... که قادرند تمامی اطلاعات قربانی را ضبط و برای هکر ارسال نموده، سیستم عامل ها را از بین برده، دسترسی به اطلاعات توسط کاربر را غیر قابل امکان کرده و حتی به قطعات سخت افزاری رایانه ها نیز آسیب برسانند.

آمار میلیونی ویروس ها و تجارت پر سود آنتی ویروس ها و آنتی تروجان ها و آنتی اسپای ورها و فایروال ها دلیلی است محکم بر این گفته که تخریب گران رایانه ای با اهداف مختلف همواره آماده ی یورش به رایانه های کاربران هستند. این بحث حتی به شکلی جدی است که عنوان « تروریسم رایانه ای » در بسیاری کشور ها هولناک تر و دهشتناک تر از سایر جرایم مرتبط با رایانه است. در بحث تنوع جرایم و اساساً جرم‌انگاری در جوامع مختلف و تحت‌تاثیر مکتب‌های مختلف، مبانی و معیارهای متفاوتی را شاهد هستیم. بسیاری از جرایم نتیجه تغییر اوضاع اقتصادی اجتماعی و صنعتی هستند و معمولا اگر مبانی آنها به نوعی با تمامیت ارزشی در بخش‌های مالی یا جانی یا حتی قسمت‌هایی که سبقه اعتباری یا قراردادی دارد، در ارتباط باشند، این جرم انگاری ها در طول تاریخ ماندنی خواهند بود، اما بعضا با زدایش بسترها و در حقیقت دگرگونی تفکر و سیاست جنایی هر جامعه ممکن است بحث جرم‌انگاری اعمال مربوط منتفی شود و نسبت به آن اعمال به تدریج سیاست جرم‌زدایی در پیش گرفته شود.[2]

در مورد مبنای جرم انگاری اعمال در جامعه ابتدا باید گفت که لزوماً تمامی افعال ضد هنجارهای اجتماعی عنوان جرم را بر خود نمی‌بینند. در توضیح این موضوع باید اضافه کرد که درجه تخریبی این افعال نسبت به جامعه باید به حدی باشد که نظم و آرامش عمومی را به

۱- Subv یا Sub Seven برنامه‌ای است که برای پنهان ماندن در کامپیوتر کاربر و انجام دادن بعضی از کارها و دسترسی داشتن به کامپیوتر کاربر، طراحی شده است. کارهائی که میتواند انجام دهد شامل خاموش کردن کامپیوتر، شروع مجدد کامپیوتر، فعال کردن محافظ صفحهٔ نمایش و نمایش متن بر روی صفحه، مشاهدهٔ فایلهای موجود بر روی دیسک سخت و اجرا کردن دستورات توسط خودش است.

۱- نجات زادگان، سعید، بررسی جرایم رایانه ای در حقوق ایران، پایان نامه مقطع کارشناسی، دانشکده حقوق، علوم سیاسی و زبان های خارجه، دانشگاه آزاد اسلامی واحد مشهد، ۱۳۸۸.

طور جدی مختل کند. به عنوان مثال قبح عمل عبور از چراغ قرمز یا برخورد نامناسب کارمند دولت با مراجعان به حدی نیست که قانونگذار برای منع فرد خاطی از چنین اعمال متوسل به مجازات کیفری شود.

مساله بعدی در اعلام جرم توسط مجالس قانونگذاری کشورها توجه به خاستگاه‌های اجتماعی، اقتصادی، مذهبی و فرهنگی در جامعه است. همچنین وجود شرایط اقتصادی خاص در پیدایش برخی جرایم مالی خاص موثر است. در کنار این مسایل، وجود شرایط و مصلحتی در برهه ی زمانی خاص موجب جرم‌انگاری یا حتی جرم زدایی موقت برخی افعال نیز خواهد شد. آنچه در مرحله توافق بر جرم‌انگاری اهمیت دارد، توجه به بازدارندگی و اصلاح مجرمان است. در مواد مربوط به جرم انگاری یک عمل باید تمامی نکات لازم برای بازدارندگی بیشتر افراد از ارتکاب آن جرم پیش‌بینی شود. این مسئله با شدت مجازات و در نظر گرفتن تمامی ابعاد حقوقی در قبال عمل مزبور امکان‌پذیر است. در ضمن نوع مجازات پیشنهادی قانون گذار باید به نحوی باشد که مسئله ی اصلاح مجرمان را بیش از پیش تامین کند. از سوی دیگر در کنار تعیین مجازات باید از تدابیر و اهرم های فرهنگی و اجتماعی متنوع جهت پیشگیری از وقوع جرم استفاده شود.

بند اول: سو استفاده آمیز بودن فضای سایبر

یکی از ویژگی های به واقع متمایز و در عین حال ارزشمند فناوری اطلاعات و ارتباطات الکترونیکی نسبت به دیگر فناوری ها، مانند فناوری هسته ای، زیستی و ریز فناوری[۱]، حداقل در برهه کنونی این است که اکثر افراد با حداقل مهارت فنی می توانند از قابلیت های بسیار متنوع آن استفاده کنند. البته انس گرفتن با این فضا و پیشبرد امور آن برا ی زندگی در دنیای کنونی، به یکی از ضروریات تبدیل شده است و حتی معدود افراد بازمانده از نسل های گذشته که تمایل یا اعتمادی به آن ندارند، معترفند که به آن وابسته هستند. همین کاربر پسند بودن فوق العاده ی این فناوری از یک سو و وابستگی مفرط اکثریت شؤون خر و کلان امروزی از سوی دیگر، از این فناوری گزینه ای منحصر به فرد ساخته است. با این حال، نباید این دسترس

۲- ریز فناوری از فناوری های جدیدی است که از آن به عنوان عامل تغییر در روش تولید مواد یاد می‌شود. این فناوری، مواد را در مقیاس یک میلیونیم متر (یعین مساوی ۱۰۹-) کنترل و تولید می کند.

پذیری فراگیر و بدون تبعیض را به کلی مثبت و سودمند ارزیابی کرد. همواره و همه جا کسانی هستند که تمایل دارند برای تحقق نیات سو خود از قابلیت های شگرف این فضا بهره برداری کنند. به ویژه آنکه عمده فرایند های مشابهی که در این فضا نسبت به دنیای فیزیکی به اجرا در می آید، به هیچ وجه از لحاظ کارایی و بازدهی قابل مقایسه نیستند. از سوی دیگر مقابله با انواع سوء استفاده ها نیز بسیار مشکل است. به هر حال تمامی این مسایل نمی تواند سامان ندادن این فضا و سزا ندادن مرتکبین ناهنجاری ها را توجیه کند. متاسفانه واقعیت حکایت از این دارد که میزان سوء استفاده های گوناگون از فضای سایبر به نحو روزافزونی رو به افزایش است.[۱]

بند دوم: سیاست های کیفری

سیاست کیفری هر کشوری باید به نحوی تعیین شود که نقصی در آن موجود نباشد زیرا نقص در سیاست های جزایی به مجرمین اجازه و همچنین اراده ی ارتکاب جرایم را می دهد که در اصل تجاوز به حقوق خصوصی اشخاص است. آنچه که اصولاً در امر قانونگذاری و تهیه ی قوانین باید مورد توجه قرار گیرد، آگاهی و شناخت لازم از جامعه، محیط، زمینه های گوناگون و عوامل جرم خیز است. از جمله ی این محیط ها فضای سایبر است. طرف دیگر تبیین سیاست جنایی حاکی از آن است که لازم است قبل تهیه و تنظیم قوانینی که مربوط به خطوط اساسی و اصول سیاست کیفری است، از آمار جنایی به عنوان ابزار مطالعه روابط و عوامل اجتماعی به نحو صحیح استفاده نمود.[۲]

بند سوم: رعایت منافع اجتماعی و اجرای عدالت

با احترام به اصل قانونی بودن جرم و مجازات، قواعد و قوانین اجتماعی دارای اعتبار و قدرت بیشتری شده و افراد در گسترش روابط و فعالیت های اقتصادی مجاز و مشروع، تردید به خود راه نخواهند داد. به همین لحاظ مقنن باید برای رفع هر گونه تبعیض و در کمال بی طرفی و واقع بینی و بدون آنکه مجرم را بشناسد و یا بدون آنکه قبل از وضع قانون بداند، کیفرهای

۱- جلالی فراهانی، امیرحسین، در آمدی بر آیین دادرسی کیفری جرایم سایبری، تهران، نشر خرسندی، ۱۳۸۸، ص ۱۷، ۱۶، ۱۵.

۲- شامبیاتی، هوشنگ، حقوق جزای عمومی، جلد اول، تهران، نشر ژوبین، ۱۳۷۶، ص ۲۴۴.

مقرر شده بعداً به چه کسی تحمیل خواهد شد، با متون قانون کلی و عام، اعمال ممنوعه و حداکثر کیفر آنها را معین کند.این روش هم در جهت عدالت و انصاف است و هم موجب تامین حقوق و آزادی های فردی است. از طرف دیگر هدف قانونگذار از اعمال مجازات، تامین آسایش و نظم عمومی در اجتماع است و از این حیث بایستی که حکم مقنن محترم شمرده شود. برای اینکه نظم عمومی بر هم نخورد، باید اعمالی را که مخالف نظم عمومی و مخل آن است معین و مشخص باشد تا افراد از ارتکاب این نوع اعمال که در عین حال مخالف نظم عمومی و نظر قانونگذار است، احتراز جویند.

بند چهارم: رعایت منافع فردی

با قبول اصل قانونی بودن حقوق جزا، افراد قادر به سنجش و ارزیابی رفتار خود بوده و می توانند با اطلاع از جرم و مجازات آن، از ارتکاب عملی بزهکارانه خودداری نمایند.[1]بنابراین قانونگذار باید قبلاً مشخص کرده باشد که عمل ارتکابی جرم است یا خیر؟ تا مرتکب آن قادر به سنجش عملی که در صدد ارتکاب آن است، باشد. چرا که قواعد اخلاقی برای تعیین درجه و اهمیت اعمال ضد اجتماعی کافی نیست، یعنی انسان به خاطر غرایز و امیالی که دارد، به دنبال تامین منافع خویش است و لذا جامعه باید با اعلام قبلی از طریق وضع قوانین صریح و روشن و قابل فهم برای همگان، افراد را قبل از ارتکاب جرم آگاه سازد که فعل یا ترک فعل معین دارای جنبه ضد اجتماعی بوده و جرم تلقی می شود. در این صورت امکان سنجش و مقایسه را خواهند داشت و اتخاذ یک سیاست کیفری و اصولی و منطقی می تواند مانع از افزایش جرم شود.[2]

بند پنجم: فراوانی جرم و بزه دیدگان

در جرایم محیط واقعی معمولاً میزان جرایم و تعداد بزه دیدگان غالباً مشخص است. برای مثال در جرایم محیط واقعی می توان آن را به چند فقره ی قتل، سرقت و کلاهبرداری یا امثال آن محصور نمود؛ در واقع جرایم در محیط واقعی در بسیاری موارد معدود و قابل شمارش اند.

۱- ژرمی بنتام معتقد بود که هر فردی قبل از ارتکاب عمل مجرمانه، منافع احتمالی حاصل از ارتکاب جرم را با خطرات ناشی از کیفر آن سنجش و مقایسه نموده و با توجه به مرجح بودن یکی بر دیگری، تصمیم گیری نموده و ممکن است مبادرت به ارتکاب عمل یا ترک عمل نماید.

۲- همان، ص ۲۴۳.

البته این امر نیز یک قاعده محسوب نمی شود چرا که در برخی اوقات این جرایم از جهت بزه دیده ای که دارد قابل شمارش نیست و اساساً رقم سیاه بزهکاری که در جرم شناسی از آن گفتگو می شود اشاره به همین موضوع دارد. اما این امر در محیط سایبر امری طبیعی است. برای نمونه آنگاه که شخصی با نوشتن تنها یک برنامه متضمن حملات تخریب و اختلال در شبکه ها و سیستم های رایانه ای سبب می گردد که هزاران رایانه ی کارگذار در سطح جهان از ارائه ی خدمات باز بمانند عملاً مرتکب یک جرم شده است، لکن بزه دیدگانی پراکنده در سطح جهان دارد. چنین فضایی در واقع ارتکاب فعل واحد مجرمانه را که دارای نتایج متعدد است سبب شده است که خود از منظر تعدد جرم قابل تدقیق است. بنابراین در جرایم محیط سایبر، اولاً تعداد بزه دیدگان معمولاً بسیار بالاست و شاید از مرز هزاران و میلیون ها نفر هم فراتر رود، ثانیاً معمولاً نمی توان آمار دقیقی از تعداد بزهدیدگان داشت، چه، جرایم سایبر در شبکه شیوع می یابند و حالت اشاعه ی جرم ارتکابی که در بسیاری موارد به صورت خودکار صورت می گیرد، بسیاری از سیستم های رایانه ای و اطلاعات را درگیر خود می سازد و این امر قابل شمارش نیست. در واقع این طبیعت فضای تکنولوژیک سایبر است که موجد پیدایش جرایمی خودکار شده که مرتکب فقط در قدم اول جرم نقش دارد و نه در استمرار آن؛ به عبارت دیگر در ارتکاب این جرایم مرتکب آغاز گر است، اما شاید هیچ گاه ادامه دهنده نباشد و این امر جرایم مستمری را آفریده است که فاعل آن در استمرارش نقشی ندارد. بنابراین نرخ ارتکاب جرم هم بالاست و در یک لحظه از زمان به میزان بسیار زیادی ممکن است واقع شود. برای نمونه ممکن است بتوان هزاران اطلاعات رایانه ای را در لحظه ای از زمان حذف یا دستکاری نمود. از این رو ارتکاب جرایم جمعی[1] در محیط سایبر یک ویژگی نسبتاً معمول است.[2]

بند ششم: سهولت ارتکاب جرم

۱- جرم جمعی یا Collective Crimes به جرایمی اطلاق می شود که از یک رشته اعمال پی در پی تشکیل شده که مجموع آن اعمال، در مجموع یک عمل شناخته شده و برای آن مجازات تعیین می شود. ضمناً هر یک از این اعمال هم منفرداً جرم بوده و قابل مجازات شناخته می شود.

۲- فضلی، مهدی، مسوولیت کیفری در فضای سایبر، تهران، انتشارات خرسندی، ۱۳۸۸، ص ۷۱.

ارتکاب جرم در محیط کامپیوتری و مجازی کاری بسیار راحت است؛ هر کس با داشتن یک رایانه که امکان اتصال به اینترنت را دارد و اندک آشنایی به سواد رایانه ای می تواند مجرمی بالقوه خطرناک باشد؛ صد البته میزان آشنایی بیشتر به علوم رایانه ای مرتکب جرم را حرفه ای تر می نماید و بر درجات شدت ارتکاب جرم می افزاید. البته بر موارد بالا، محدودیت در ارتکاب جرایم در محیط واقعی به مراتب بیشتر از محدودیت در محیط سایبر است؛ برای مثال در ارتکاب سرقت از یک بانک شاید مدت های زیادی برای برنامه ریزی و طراحی سرقت، از جمله آشنایی مقدماتی با محل، آشنایی و اطلاع کافی از وضعیت موجود بانک، اطلاعات مالی و امنیتی و موشکافی و مداقه در سایر جزئیات لازم باشد. از سوی دیگر محیط واقعی ایجاب می کند که برای شناسایی نشدن توسط نیروی انتظامی و مردم تمام توان برا ی مخفی نگاه داشتن اقدامات و هویت مرتکبین صورت گیرد. لکن در جرایم محیط سایبر این محدودیت ها وجود ندارد، به راحتی می توان با نوشتن برنامه ای ساده به سیستم های محرمانه ی دولتی نفوذ کرد، بدون اینکه مرتکب کوچکترین واهمه ی شناسایی توسط دیگران را داشته باشد.[1]

بخش چهارم: بررسی و تحلیل حقوقی عنصر مادی جرم اخلال در شبکه های رایانه ای

بند اول: رفتار فیزیکی

اینکه گفته می شود هر جرم مستلزم عمل مادی است، نباید چنین تصور کرد که این عمل حتماً بایستی عمل مثبت باشد که از ناحیه ی مجرم سر زده، بلکه جرم ممکن است خودداری از عمل هم باشد بنابراین جرایم از نظر عنصر مادی به جرم فعل و جرم ترک فعل تقسیم می شوند. جرم فعل عملی است که انجام آن توسط قانونگذار منع شده و برای آن مجازات تعیین شده است مثل سرقت، قتل، ضرب و جرح. گاهی جرم فعل مثبت ممکن است سخن یا قول یا بیان باشد مانند اهانت و ناسزا گویی که بر اساس قوانین جزایی کشور جرم محسوب می شود و یا فرضاً اگر کسی در مورد دعوای حقوقی یا جزایی که قسم متوجه ی او شده باشد، سوگند دروغ یاد کند به شش ماه یا دو سال محکوم خواهد شد. در مقابل مواردی وجود دارد که قانونگذار از نظر حفظ نظم عمومی برای افراد تکالیفی معین می کند که عدم انجام آنها جرم شناخته شده

۳- همان، ص ۷۲.

است. در این حالت جرم عبارت است از خودداری از انجام تکالیف محوله که این جرم غالباً از طرف مستخدمین دولتی ارتکاب می یابد ولی گاهی نیز امکان دارد که توسط افراد عادی نیز این جرم واقع شود. بنابراین رفتار مجرمانه ی مرتکب در جرم اخلال در شبکه های رایانه ای و مخابراتی نیز مانند اغلب جرایم، باید به شکل فعل باشد.

بند دوم: وارد کردن

وارد کردن در لغت به معنای داخل کردن، مطلع کردن، ایراد وارد کردن یا اعتراض کردن است. منظور از وارد کردن در این ماده همان معنای حقیقی و متبادر به ذهن یعنی داخل کردن می باشد. مجرم با وارد کردن داده یا امواج نوری یا مغناطیسی باعث می شود شبکه ها و سامانه های رایانه ای یا مخابراتی مربوط به دیگری از کار بیفتد یا در کارکرد آنها اخلال ایجاد شود. وارد کردن از طرق مختلفی امکانپذیر است؛ از قبیل وارد کردن از طریق دیسک های حامل اطلاعات[1] و یا حافظه ای جانبی و.... آنچه که از سیاق ماده بر می آید این است که مهم نیست داده های نادرست و ساختگی وارد شود و یا داده های درست، آنچه که مهم می باشد از کار افتادن یا مختل شدن کارکرد آن شبکه ی رایانه ای یا مخابراتی است. البته لازم به ذکر است که مصادیقی که در این ماده به کار برده شده است غالباً با یکدیگر هم پوشانی دارند؛ به عنوان مثال وارد کردن می تواند با انتقال دادن نیز خلط گردند. به علت اینکه وارد کردن از طریق انتقال دادن صورت می گیرد. هر چند که عمل وارد کردن داده یا امواج الکترومغناطیسی یا نوری می تواند برای ارتکاب جرایم مختلفی از جمله کلاهبرداری رایانه ای و یا سرقت اطلاعات صورت گیرد.

بند سوم: انتقال دادن

انتقال دادن در لغت به معنای منتقل ساختن، جابجا کردن و نقل کردن است. انتقال دادن از طرق مختلفی امکان پذیر است. گاه از طریق حامل های داده مثل CD و یا حافظه های جانبی انجام می شود و لی شایع ترین آن انتقال از طریق شبکه های اینترنتی می باشد. به هر جهت انتقال دادن در جرم اخلال باید به نحوی باشد که سیستم رایانه ای را از کار بیندازد و یا کارکرد مختل نماید.

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹

۱- Compact Disk (CD)

بند چهارم: پخش

پخش به معنای پراکنده کردن، پاشیدن، متفرق کردن و توزیع کردن است. پخش کردن از طرق مختلفی باعث ایجاد اختلال می گردد. پخش کردن در اعلوم رایانه به معنای منتشر کردن است. مهم ترین شیوه ارتکاب آن را می توان پخش کردن داده ها و اطلاعاتی دانست که حامل ویروس هستند. ویروس‌ها گاه ممکن است اطلاعات رایانه را به طور کامل پاک کنند یا آن ها را تغییر بدهند، اطلاعات موجود در رایانه را سرقت کنند، برنامه‌هایی را ناخواسته به اجرا درآورند یا حتی، رایانه را به طور کامل از کار بیندازند.

بند پنجم: حذف کردن

حذف کردن به معنای پاک کردن، انداختن و ساقط کردن است. در علوم رایانه ای حذف کردن به معنای برداشتن داده‌ها از یک واسط داده می باشد. حذف داده‌ها معادل از بین بردن یک شیء مادی است. این عمل آنها را از بین می‌برد تا قابل فهم نباشند. حذف کردن در اصل باید به منظور ممانعت از دسترسی آزاد صورت گیرد، ولی مختل کردن نیز ممکن است با حذف امواج الکترومغناطیسی و نوری رخ دهد.[1] باید توجه داشت که لازم نیست که کلیه ی داده های رایانه ای یا امواج الکترومغناطیسی یا نوری حذف شود یا از بین برود، بلکه حتی اگر بخشی از آن هم صدمه ببیند به نحوی که موجب اخلال شود، جرم محقق شده است.

بند ششم: متوقف کردن

متوقف کردن به معنای بدرنگ وا داشتن، در محلی ایستانیدن و تعطیل کردن است.

متوقف کردن داده‌های رایانه‌ای به معنای هر فعلی است که از دسترس‌پذیری داده‌ها برای شخصی که به رایانه یا حامل داده‌ای که داده‌ها بر روی آن ذخیره شده و به آنها دسترسی دارد، جلوگیری می کند یا پایان می‌بخشد. البته لازم نیست که ایجاد کردن وقفه به صورت طولانی ادامه داشته باشد، همین که در لحظه ای از زمان فرد نتواند به سیستم رایانه ای خود دسترسی پیدا کند و به نوعی در سیستم وی اخلال ایجاد شود جرم تام اخلال در شبکه های رایانه ای و مخابراتی محقق شده است.

۲- فضلی، مهدی، تخریب و اخلال در داده ها و سیستم های رایانه ای، مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات، مرکز مطالعات راهبردی و توسعه ی قضایی قوه ی قضائیه، تهران، ۱۷ و ۱۸ خرداد ۱۳۸۳، ص۱۲۷.

بند هفتم: تخریب

تخریب به معنای ویران کردن و خراب کردن است. «تخریب» به اعمالی اطلاق می شود که بطور خاص به تغییر منفی تمامیت یا محتوای اطلاعات داده‌ها و برنامه‌ها اشاره دارند. تخریب رایانه‌ای یا در مفهوم عام‌تر، خرابکاری رایانه‌ای، عنوان عامی است که هم تخریب را در بر می گیرد و هم اخلال را. هر چند این عنوان در قانون جرایم رایانه‌ای به کار نرفته، ولی جایگاه روشنی در عرف دارد و همین عنوان را می توان برای همه گونه‌های رفتاری که عرف، فاعل آن را خرابکار می‌نامد، به کار برد. خرابکاری رایانه‌ای دربردارنده هر رفتاری است که داده را به طور کلی یا جزئی از میان ببرد یا کارکرد داده یا سامانه را به هر نحو بر هم بزند. به نظر می رسد که بهره‌گیری از عنوان خرابکاری برای درک جایگاه خود تخریب بهتر است.

بخش پنجم: معاونت در جرم اخلال در شبکه های رایانه ای و مخابراتی

تمام کسانی که در اعمال جرم اصالتاً و مستقیماً مداخله داشته اند مباشران و شرکای جرم به شمار می آیند. در مقابل کسانی که فقط به مباشر و شرکای جرم در تدارک و یا ارتکاب جرم کمک رسانیده و نقشی تبعی و فرعی داشته اند معاونان جرم محسوب می شوند، در این صورت عمل ارتکابی آنان را معاونت می نامند. به عبارت دیگر می توان گفت: معاون جرم[1] کسی است که دراعمال تشکیل دهنده ی جرم دخالتی نداشته و فقط مصدر اعمال مقدماتی جرم است که به ارتکاب از طرف شخص دیگری می انجامد. معاونت در جرم یعنی تحریک، ترغیب، تهدید، تطمیع یا با دسیسه یا فریب یا سو استفاده از قدرت، موجب وقوع جرم گردد و همین طور هر کسی که وقوع جرم را تسهیل کند یا وسایل ارتکاب جرم را بسازد یا تهیه کند یا طریق ارتکاب جرم را ارایه دهد معاون جرم محسوب می شود. این اعمال باید هم زمان با عمل مباشر یا قبل از آن انجام گیرد.[2] بنابراین کسی که پس از وقوع جرم، مباشر یا وسایل

۱- Abetting

۲- باید توجه داشت طبق قانون مجازات اسلامی اشخاص زیر معاون جرم محسوب میشوند:

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

ب- هرکس وسایل ارتکاب جرم را بسازد یا تهیه کند یا طریق ارتکاب جرم را به مرتکب ارائه دهد.

پ- هرکس وقوع جرم را تسهیل کند.

ارتکاب جرم را پنهان کرده و بدین طریق مانع کشف حقیقت از سوی ماموران کشف جرم می شود، معاون جرم محسوب نمی شود. تحقق معاونت همچون مشارکت و به طور کلی هر جرم دیگری مشروط به اجتماع عناصر سه گانه ی قانونی، مادی و روانی است. این عناصر کم و بیش با عناصر تشکیل دهنده ی جرم اصلی قرینه و متصل هستند. ولی این امر به این معنی نیست که سرنوشت معاون جرم و مباشر جرم اصلی به یکدیگر پیوند خورده است. در ذیل به بررسی عناصر تشکیل دهنده ی جرم معاونت در اخلال در شبکه های رایانه ای و مخابراتی می پردازیم.

عنصر قانونی: معاونت در این جرم هنگامی تحقق می یابد که موجب وقوع جرم اخلال گردد. شرط دیگری که باید افزود این است که مباشر جرم باید تمام مراحل تهیه ی مقدمات را پشت سر گذاشته و دست کم جرم را شروع کرده باشد؛ به همین دلیل چنانچه اعمال مباشر اصلی در حد مقدمه ی جرم بوده و یا پس از شروع به میل و اراده ی او متوقف بماند به شرط آنکه این مقدار عمل خود جرم نباشد فعل معاونت نیز محقق نخواهد شد.[1] از سوی دیگر جرم شناختن فعل معاون منوط به اجرای کامل آن است. یعنی شروع به معاونت جرم نیست؛ مگر آنکه فعل معاون فی نفسه جرم باشد که در این صورت فعل مذکور نه به عنوان معاونت، بلکه به عنوان جرم مستقل که شروع به آن جرم است قابل مجازات خواهد بود.

عنصر مادی: تحقق معاونت در جرم اخلال، مستلزم این است که شخص معاون به صور مختلف مندرج در قانون، مرتکب اصلی را مساعدت و یاری کند و به نحوی وقوع جرم را توسط مرتکب ممکن سازد. قانون مجازات اسلامی با احصاء اعمال معاونت و توصیف نحوه ی ارتکاب هر یک برای اعمال مذکور استقلال تام شناخته است، چندان که می توان فعل معاونت را از افعال دیگر نظیر مباشرت و مشارکت کاملاً تمیز داد. البته گاه عملی را که فرد مرتکب می شود هر چند به نوعی در قالب معاونت قرار می گیرد ولی به طور مستقل و جداگانه ای

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

۱- در این مورد دیوانعالی کشور چنین اظهار نظر کرده است که: «... به طور کلی معاون وقتی مستوجب مجازات است که فاعل اصلی مرتکب جرمی شود و یا شروع به اجرای آن نماید» (حکم شماره ی ۳۵۹۸-۱۳۱۹/۱۰/۳۰).

جرم انگاری شده است. مثل بند ج ماده ی ۷۵۳ که بیان می دارد « انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی. » در اینجا مرتکب به نوعی طریق ارتکاب جرم را به دیگری نشان می دهد.

افعال معاونت به هر شکل ارتکاب یابد زمانی جرم محسوب می شود که جامع خصوصیات سه گانه ی زیر باشد:

اولاً- تحقق عمل مثبت مادی.همانطور که پیشتر بیان گردید تحقق معاونت در جرم اخلال در شبکه های رایانه ای و مخابراتی مستلزم انجام یک عمل مثبت مادی است و ترک فعل نمی تواند عنصر مادی جرم معاونت قرار گیرد. بنابراین هرگاه کسی که مطلع از وقوع جرم است، مرتکب آن را معرفی نکند یا عملِ جرم را با اطلاع از ارتکاب آن افشا ننماید، یا بعد از وقوف به جریان ارتکاب، از ارتکاب آن ممانعت به عمل نیاورد معاون جرم محسوب نمی شود. حتی ممکن است مجرم، کسی را که از وقوع جرم مطلع شده یا از جریان آن باخبر شده است را با وسایلی ساکت[1] نگه دارد و یا رضایت او را در مقابل دریافت وجهی تحصیل کند و مانع از افشا جرم یا عقیم ماندن آن شود، معذالک نمی توان شخص مطلع را به صرف سکوت معاون جرم نامید.

ثانیاً- تحقق فعل مجرمانه در خارج. بدین معنا که لازم است فعل مجرمانه در خارج تحقق پیدا کند تا معاونت در جرم تحقق یابد. بنابراین اگر شخص معاون، پس از شروع به معاونت، به دلیل عوامل خارجی که اراده ی او در آن دخالت ندارد، از عمل خود منصرف شود و معاونت واقع نشود، صرف شروع به معاونت قابل مجازا نیست. هر چند که معاونت در شروع به جرم قابل مجازات است.

ثالثاً- وجود وحدت قصد. در ارتکاب جرم معاونت می بایستی بین عامل اصلی و معاون جرم در مورد طبع و ماهیت عمل اصلی، وحدت قصد وجود داشته باشد. پس لازم است معاون جرم آشنایی با چگونگی عمل و کیفیت مجرمانه ی آن داشته باشد و با تهیه ی مقدمات، همکاری

۱- در این مورد دیوانعالی کشور چنین اظهار نظر کرده است که: « سکوت و عدم اقدام به ارتکاب جرم را نمی توان معاونت تلقی کرد.... » (حکم شماره ی ۲۵۰۴-۱۳۱۷/۱۱/۱۶).

در فعل ارتکابی را اراده نموده و خواستار حصول نتیجه ی مجرمانـه از طـرف مباشـر جـرم نیـز باشد.

رابعاً- تقدم یا اقتران زمانی. یعنی لازم است که عمل معاون قبل یا مقارن با انجام فعلِ مجرمانـه باشد و در صورتی که اقدام معاون بعد از وقوع جرم توسط مرتکـب اصـلی صـورت گیـرد، از مصادیق معاون در جرم تلقی نمی شود بلکه می تواند جرم مستقل و خاصی باشد.

بخش ششم: بررسی عنصر معنوی جرم اخلال در شبکه های رایانه ای

بند اول: اراده ی ارتکاب فعل و علم وعمد

اراده در لغت عبارت است از خواستن، طلب کردن، قصد، آهنگ و عزم[1] و از نظر حقوقی سه اصطلاح « اصل آزادی اراده »، « اصل استقلال اراده » و « اصـل حاکمیـت اراده » بکـار گرفتـه شده است که آن عبارت است از تأثیر اراده ی افراد در روابط اشـخاص در زنـدگی قضـایی[2]. بنابراین اراده ارتکاب جرم عبارت است از خواستن انجام عمل مجرمانـه[3]. اراده جریـانی اسـت که معلول فعالیت غریزه ای از غرایز انسان می باشد که بیـانگر یـک کیفیـت روانـی اسـت کـه تحت نفوذ جنبه ی عقلانی شخصیت، فرد را برای رسیدن به هدف خاصـی بـه انجـام یـا تـرک فعلی مصمم می کند. این کیفیت های روانی همگی روشنگر اراده ی آدمی است و هر انسـانی می تواند با الهام از وجدان خـویش نقـش آن را در جریـان فعالیـت هـای روزانـه درک کنـد.[4] بنابراین می توان گفت که سـاده تـرین و عملـی تـرین راه ممکـن بـرای درک ماهیـت اراده و جریان تشکیل آن مراجعه به حاکمیت وجدان است، چرا که وجدان آدمـی محـل تشـکیل هـر گونه کیفیت روانی است و ناظر بر جنبـه هـای بـدنی، عـاطفی، اجتمـاعی و عقلانـی شخصـیت آدمی است. باید توجه داشت که در کلیه جرایم اعـم از عمـدی و غیـر عمـدی اراده ارتکـاب جرم وجود دارد و قانون‌گذار فقط انجام عمل ارادی را مجازات مـی‌کنـد. در جـرم اخـلال در

۱- عمید، حسن، فرهنگ فارسی عمید، انتشارات امیر کبیر، تهران، ۱۳۵۵، ص ۱۰۰.

۲- جعفری لنگرودی، محمد جعفر، ترمینولوژی حقوق، تهران، انتشارات ابن سینا، ص ۴۲.

۳- ولیدی، محمدصالح؛ بایسته‌های حقوق جزای عمومی، تهران، جنگل، ۱۳۸۸، ص ۲۵۳.

۴- محمصانی، صبحی، فلسفه ی قانونگذاری در اسلام، ترجمه ی اسماعیل گلسـتانی، ص ۲۷۲. بـه نقـل از: شـامبیاتی، هوشنگ، حقوق جزای عمومی، جلد اول، تهران، نشر ژوبین، ۱۳۷۶، ص ۴۰۲ و ۴۰۳.

شبکه های رایانه ای و مخابراتی همین که فرد انجام و ارتکاب این جرم را بخواهد، این قسم از رکن روانی محقق شده است.

در صورت فقدان ارادهٔ ارتکاب فعل، تحقق جرم منتفی است[1]. از طرف دیگر اراده ی ارتکاب فعل نیز باید با قصد مجرمانه یا خطای جزایی توأم باشد وگرنه به علت فقدان عنصر روانی عمل ارتکابی جرم تلقی نمی شود.

ارتکاب عمل نیز، به خودی خود دلیل وجود عنصر معنوی یا روانی نیست و باید تقصیر مرتکب در انجام عمل احراز شود. آنچه تقصیر در معنای عام نامیده می‌شود یا بر پایه عمد یا مبتنی بر خطاست؛ عمد عنصر روانی آن دسته از جرایمی است که اصطلاحا جرایم عمدی نام دارند و خطای جزایی عنصر روانی جرایم خطایی. همانطور که می داتیم در پیوند با علم، مرتکب نه تنها باید علم موضوعی داشته و بداند که شبکه یا سامانه از آنِ دیگری است، باید بداند که از برای نقض تدابیر حفاظتی و درون شدن به سامانه ی وی اجازه نداشته است. باید گفت که نگرفتن اجازه و نقض تدابیر امنیتی از هم جدا هستند و برای نمونه اگر کسی از دارنده سامانه اجازه دسترسی داشته ولی به جهت دسترسی نداشتن به وی و به دنبال آن آگاهی نداشتن از گذرواژه، تدابیر امنیتی سامانه اش را نقض کند، جرمی انجام نداده است. برای تحقق عمد دو شرط مهم لازم می باشد؛ بدین معنا که اراده ی ارتکاب با قصد مجرمانه تقارن و تطابق زمانی داشته باشند، بدین ترتیب به علت آنی بودن این جرم، با توجه به اینکه جرم مستمر به فعل یا ترک فعلی اطلاق می شود که در زمان ادامه دارد و به عبارت دیگر جرم با عناصر خود به طور دایم تجدید حیات می یابد، و این شرایط در این جرم موجود نیست، متهم باید در همان لحظه ی ارتکاب عمل تخریب و ایجاد اختلال از عنصر روانی لازم برخوردار باشد والا اگر مثلاً شبکه و یا سیستم رایانه ی دیگری را به تصور اینکه متعلق به خودش است از کار بیندازد ولی پس از اطلاع از این مسئله بدان راضی باشد وی را نمی توان به ارتکاب جرم تخریب و ایجاد اختلال محکوم نمود. شرط تقارن زمانی، هر چند صراحتاً در قانون نیامده، لیکن از این اصل مسلم ناشی می شود که به هر حال جرم باید در یک لحظه از زمان تحقق یابد و جرم نیز چیزی بیش از مجموع عناصر مادی و روانی نیست؛ اثبات مطابقت این دو با

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹

۱- گلدوزیان، ایرج؛ بایسته‌های حقوق جزای عمومی، تهران، میزان، ۱۳۸۴، چاپ دوازدهم، ص۱۷۸.

مرجع قضایی است. بنابراین این دو عنصر باید در یک لحظه به طور همزمان وجود خارجی پیدا کنند.

بند دوم: قصد مجرمانه

سوء نیت: قصد مجرمانه[1] غالباً مترادف با سوء نیت است و در معنای عام همان عمد در ارتکاب جرم می باشد.زمانی سوء نیت تحقق پیدا می کند که مرتکب جرم خواستار نتیجه ی عمل و نتایج حاصله از عمل مجرمانه باشد و تا این ارکان تحقق نیابد، سوء نیت وجود نخواهد داشت. سوء نیت خود به سوء نیت عام[2] و سوء نیت خاص[3] تقسیم می شود که در زیر به بررسی آن پردازیم.

سوء نیت عام: منظور از سوء نیت عام اراده ی خودآگاه فرد در ارتکاب عمل مجرمانه می باشد؛ به سوءنیت عام در اصطلاح عمد در خواستن فعل نیز گفته می شود. به عبارت دیگر همان اراده و اختیار و خواست مرتکب جرم است.[4] به طوری که ایجاد اختلال در شبکه ها و سامانه های رایانه ای و مخابراتی دیگری، بدون اراده و خواست مرتکب، به دلیل فقدان سوء نیت فاقد جنبه کیفری بوده و تنها موجب مسئولیت مدنی می گردد. معمولاً سوء نیت عام با به کار بردن الفاظی چون عالماً و عامداً، عمداً و یا به طور غیر مجاز (اصطلاح بکار برده شده در قانون جرایم رایانه ای) در متن قانون شناخته می شود. در این جا عمد و اراده در انجام فعل فیزیکی و مادی را می توان سوء نیت عام این جرم دانست؛ به عبارت دیگر مرتکب باید با علم به اینکه شبکه یا سامانه ی رایانه ای و مخابراتی متعلق به دیگری است در ایجاد اختلال و یا از کار انداختن آن عمد در فعل داشته باشد. باید افزود که اعمالی که در نتیجه ی بی مبالاتی بی احتیاطی و عدم رعایت نظامات دولتی ارتکاب می یابد در دایره ی مصادیق این جرم قرار نمی گیرند. بنابراین اگر کسی که مسئول فرستادن اطلاعاتِ روزانه ای از طریق رایانامه برای افرادی خاص می باشد و در اثر بی مبالاتی مطلبی را که حاوی ویروس می باشد، بدون حصول

۱- درجات قصد که در کد کیفری نمونه ایالات متحده آمده تقسیم قصد به عمد، علم، بی احتیاطی و بی مبالاتی است که حداقل درجه از مسئولیت، بی مبالاتی است که بر مبنای ترک فعل می باشد.

۲- General intent; Basic intent

۳- Specific intent

۴- شامبیاتی، هوشنگ، حقوق جزای عمومی، جلد اول، تهران، نشر ژوبین، ۱۳۷۶، ص ۴۱۱.

اطمینان از اینکه آن مطلب بدون ویروس است، برای دیگری بفرستد و در نتیجه آن کارکرد رایانه ی دیگری را مختل کند به علت فقدان سوء نیت مرتکب جرمی نشده است؛ البته شاید بتوان از باب مسئولیت مدنی و جبران ضرر و زیان فرد را مسئول دانست.

سوء نیت خاص: سوءنیت عام برای آنکه جرم عمدی تحقق یابد همیشه لازم است اما کافی نیست. گاه قانونگذار وجود جرم را منوط به داشتن قصد مشخص و صریحی کرده است که فاعل برای تحقق آن کوشیده است؛ بدین معنا که علاوه بر قصد ارتکاب عمل مجرمانه باید قصد دیگری هم که از طرف قانون برای تحقق جرم ضروری شناخته شده، مصداق پیدا کند. در این جا است که بحث از سوء نیت خاص و به عبارت دیگر عمد در خواستن نتیجه مطرح می شود.

سوء نیت خاص اراده ی آگاه مرتکب نسبت به مال موضوع جرم یا شخص متضرر از جرم است. در جرم اخلال در شبکه یا سامانه های رایانه ای و مخابراتی علاوه بر عمد و قصد در انجام فعل مجرمانه ارتکابی (در ایجاد اختلال) نتیجه ی مجرمانه نیز که در واقع احراز قصد ایجاد اختلال و ایراد ضرر و خسارت به دیگری بوده ضروری است.

به بیان دیگر در این جرم مرتکب باید قصد از کار انداختن یا ایجاد اختلال در کارکرد سیستم های رایانه ای یا مخابراتی بطور غیر مجاز داشته باشد. بنابراین اگر کسی عملی انجام دهد که منجر به از کار افتادن یا اختلال در شبکه نگردد، با توجه به رویه ی قضایی معمول در حقوق جزا و همچنین اصول اولیه ی جزایی، این جرم محقق نخواهد شد. چه بسا این اعمال تحت عناوین دیگری از جمله جرایم علیه محرمانگی داده ها و سیستم های رایانه ای قابل پیگرد باشند. فرد مرتکب از حذف کردن یا وارد کردن یا انتقال دادن یا پخش کردن و یا متوقف کردن داده ها یا امواج الکترومغناطیسی یا نوری می تواند در پی اهداف مختلف دیگری باشد؛ از قبیل تخریب داده، اخلال در شبکه یا سامانه ی دیگری، از کار انداختن شبکه، جاسوسی و یا حتی انتقام جویی و تسویه حساب شخصی. حال از میان همه ی این اهداف وجود و اثبات قصد خاص اخلال در شبکه یا سامانه ی دیگری یا از کارانداختن آن برای تحقق جرمِ اخلال در شبکه های رایانه ای و مخابراتی ضروری می باشد. باید اضافه کنیم که منظور از قصد اخلال، قصد اخلالِ جزئی یا کلی سامانه ی دیگری نمی باشد، بلکه صرف ایجاد اختلال مد

نظر قانونگذار می باشد و کمیت آن بی تأثیر است. به عنوان مثال شخصی که با حذف داده ای هر چند کم اهمیت و با حجم کم موجب اخلال ناچیزی در شبکه ی رایانه ای یا مخابراتی دیگری می شود، فاعل این جرم محسوب می شود و قابل مجازات است.

بند سوم: انگیزه یا داعی

انگیزه[1] یا داعی به معنای احساس یا نفعی که فاعل را به ارتکاب جرم سوق می دهد[2]. انگیزه به عنوان یکی از عناصر تشکیل دهنده ی جرم محسوب نشده است لکن در تعیین مجازات، خصوصاً در مواردی که میزان مجازات دارای حداقل و حداکثر است می تواند مؤثر واقع شود. تفاوت بین انگیزه با قصد و عمد چنین مشخص می شود که قصد و عمد نتیجه ی بلافاصله و بلاواسطه ی عمل است ولی انگیزه هدف مع الواسطه از ارتکاب جرم می باشد. به عنوان مثال در جرم اخلال در شبکه های رایانه ای یا مخابراتی قصد فرد ایجاد اختلال یا از کاراندازی شبکه ی رایانه ای یا مخابراتی دیگری است، چه بسا که همین فرد انگیزه های متفاوتی از جمله تسویه حساب شخصی یا شوخی کردن و یا... را در سر بپروراند. عموماً انگیزه ی ارتکاب جرم تأثیری بر مسئولیت کیفری مرتکب ندارد. البته قاضی می تواند بعد از محکوم کردن متهم به ارتکاب جرم، برای تعیین مجازات متناسب، انگیزه ی مرتکب را مد نظر قرار دهد.

نتیجه گیری

در جمع بندی و نتیجه گیری مقاله حاضر باید گفت جرم اخلال در شبکه های رایانه ای و مخابراتی از جمله جرایم علیه سامانه های رایانه ای و مخابراتی می باشد. بسیاری از جرایم نتیجه ی تغییر اوضاع اقتصادی، اجتماعی، صنعتی و تکنولوژی ها هستند. جرم اخلال همانطور که گفته شد نتیجه ی پیشرفت تکنولوژی می باشد که مبانی و دلایل متعددی از جمله سوء استفاده آمیز بودن فضای سایبر، سیاست های کیفری، رعایت منافع اجتماعی و اجرای عدالت، فراوانی جرم و بزه دیدگان و سهولت ارتکاب جرم ضرورت قانونگذاری در این زمینه را برای

۱- Motive

۲- همان، ص ۲۴۰.

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹

قانونگذار جمهوری اسلامی ایران فراهم نمود. اخلال در شبکه های رایانه ای و مخابراتی از زمره جرایم مطلق، که در آنها حصول نتیجه ی خاص برای تحقق جرم ضروری نیست نمی باشد، بلکه از زمره ی جرایم مقید است، که شرط تحقق آنها حصول نتیجه ی خاص می باشد. نتیجه ای که، بنا به تصریح قانون، حصول آن برای تحقق جرم اخلال لازم می باشدایجاد اخلال در سامانه های رایانه ای و مخابراتی و یا از کار انداختن این سامانه ها می باشد. در اخلال سامانه، مرتکب باید عمد در انجام رفتار را داشته باشد. همچنین او باید به موضوع بزه آگاهی داشته باشد. یعنی هم نسبت به اینکه سامانه از آنِ دیگری است و یا این که از آنِ دولت است و هم نسبت به غیرمجاز بودن آن آگاه باشد. در جرم اخلال در شبکه یا سامانه های رایانه ای و مخابراتی علاوه بر عمد و قصد در انجام فعل مجرمانه ارتکابی (در ایجاد اختلال) نتیجه ی مجرمانه نیز که در واقع احراز قصد ایجاد اختلال و ایراد ضرر و خسارت به دیگری بوده ضروری است. علاوه بر لزوم وجود عنصر مادی و عنصر روانی برای تحقق جرم، شرط لازم دیگر آن است که این دو عنصر با هم تقارن زمانی داشته باشند، بدین ترتیب به علت آنی بودن این جرم، با توجه به اینکه جرم مستمر به فعل یا ترک فعلی اطلاق می شود که در زمان ادامه دارد و به عبارت دیگر جرم با عناصر خود به طور دایم تجدید حیات می یابد، و این شرایط در این جرم موجود نیست. سوء نیت خاص اراده ی آگاه مرتکب نسبت به مال موضوع جرم یا شخص متضرر از جرم است.

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹

منابع و مآخذ

الف) منابع فارسی

- اردبیلی، م ع، ۱۳۸۴، حقوق جزای عمومی، جلد دوم، تهران: نشر میزان، چاپ چهارم.
- افراسیابی، م ا، ۱۳۷۷، حقوق جزای عمومی، جلد دوم، تهران: انتشارات فردوسی، چاپ سوم.
- پرویزی، ر، ۱۳۸۱، جرایم کامپیوتری و اینترنتی، تهران: نشر ابرار اقتصادی چاپ اول.
- جعفری لنگرودی، م ج، ۱۳۸۰، ترمینولوژی حقوق، تهران: انتشارات ابن سینا، چاپ یازدهم.
- جعفری لنگرودی، م ج، ۱۳۸۲، فرهنگ حقوقی، تهران: انتشارات گنج دانش، چاپ سیزدهم.
- جلالی فراهانی، ا ح، ۱۳۸۸، در آمدی بر آیین دادرسی کیفری جرایم سایبری، تهران: نشر خرسندی، چاپ اول.
- حسن بیگی، ا، ۱۳۸۴، حقوق و امنیت در فضای سایبر، تهران: انتشارات مؤسسه ی فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر، چاپ دوم.
- خداقلی، ز، ۱۳۸۴، جرایم کامپیوتری، تهران: انتشارات آریان، چاپ اول.
- فضلی، مهدی، مسوولیت کیفری در فضای سایبر، تهران، انتشارات خرسندی، ۱۳۸۸
- کی‌نیا، م، ۱۳۷۴، روان‌شناسی جنائی، تهران: انتشارات رشد، چاپ چهارم.
- ولیدی، م، ۱۳۶۶، مسوولیت کیفری، تهران: انتشارات امیرکبیر، چاپ اول.
- ولیدی، م، ۱۳۸۸، بایسته‌های حقوق جزای عمومی، تهران: انتشارت جنگل، چاپ پنجم.

ب) مقالات

- بوستانچی، م، ۱۳۹۰، پیشگیری از جرایم رایانه ای، دانشگاه علوم و تحقیقات یزد.
- ترکی، غ ع، ۱۳۸۸، ماهیت جرایم رایانه ای، ماهنامه دادرسی، سال سیزدهم، شماره۷۷.

- جلالی فراهانی، ا م، ۱۳۸۴، پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، فصلنامه فقه وحقوق، سال دوم.
- خانزاده، ح، ۱۳۸۸، بررسی و تحلیل قانون جرائم رایانه ای، دانشگاه حقوق و علو سیاسی، دانشگاه تهران.
- زرخ، ا، ۱۳۸۹، جرایم مخابراتی، مجله ی حقوقی دادگستری، شماره ی ۶۹.
- فضلی، م، ۱۳۸۳، تخریب و اخلال در داده ها و سیستم های رایانه ای، مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات، مرکز مطالعات راهبردی و توسعه ی قضایی قوه ی قضائیه، تهران.

ج) پایان نامه

- خرم آبادی، ع، ۱۳۸۳، جرایم فناوری اطلاعات، پایان نامه مقطع دکتری، دانشکده حقوق و علوم سیاسی، دانشگاه تهران.
- دیندار، م، ۱۳۸۹، مسئولیت کیفری اشخاص حقوقی در قانون جرایم رایانه ای، پایان نامه ی مقطع کارشناسی، دانشکده ی حقوق و علوم سیاسی، دانشگاه علامه طباطبایی.
- شمس ناتری، م ا، ۱۳۸۰، بررسی سیاست کیفری ایران درقبال جرائم سازمان یافته، رساله ی دکتری، دانشگاه تربیت مدرس، دانشگاه تهران.
- هوشیار، محمدرضا، ۱۳۹۲، بررسی حقوقی جرم اخلال در شبکه های رایانه ای و مخابراتی، پایان نامه کارشناسی ارشد رشته حقوق(M.A)، دانشگاه آزاد اسلامی واحد علوم وتحقیقات هرمزگان
- عبقری، آ، ۱۳۷۷، جرم کامپیوتری جلوه ای نوین از بزهکاری، پایان نامه ی کارشناسی ارشد، دانشگاه حقوق، دانشگاه تهران.

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹