



*ISLAMIC AZAD UNIVERSITY
CENTRAL Tehran branch
Faculty of Law – Department of
Criminal law group
Law M.A thesis
Criminal law*

Subject:

Obtaining Criminal Argument in Cyberspace

Advisor:

Dr. Abolfateh Khaleghi

Reader:

Dr. Mohammadesmail Afrasiabi

By:

Masoud Ferdosi

Autumn 2013

فهرست مطالب

صفحه	عنوان
۱	چکیده.....
۲	مقدمه.....
<u>فصل اول- مبانی، مفاهیم و پیشینه</u>	
۷	مبحث اول- پدیده جرم رایانه ای.....
۸	گفتار اول- تاریخچه.....
۱۰	گفتار دوم- تعاریف.....
۱۵	مبحث دوم- ویژگیهای جرائم رایانه ای و شبکه بین المللی.....
۱۵	گفتار اول- خصوصیات مرتکبین جرائم رایانه ای و شبکه بین المللی.....
۱۶	گفتار دوم- عدم تخمین دقیق جرائم ارتكابی.....
۱۷	گفتار سوم- حجم صدمات و خسارات.....
۱۹	گفتار چهارم- خصوصیت فراملی و بین المللی جرائم رایانه ای و شبکه بین المللی.....
۲۰	مبحث سوم- ویژگیهای عمومی فضای مجازی.....
۲۰	گفتار اول- گسترده بودن.....
۲۰	گفتار دوم- جهانشمول بودن.....
۲۱	گفتار سوم- پوشیده بودن.....
۲۱	گفتار چهارم- گزینشی بودن اطلاعات.....
۲۲	گفتار پنجم- قابل کنترل نبودن.....
۲۳	مبحث چهارم- قابلیت های رایانه به عنوان بستر تمامی جرائم رایانه ای.....

- گفتار اول- قابلیت تراکم اطلاعات ۲۳
- گفتار دوم- قابلیت دستیابی به سیستم های رایانه ای ۲۳
- گفتار سوم- تکنولوژی رایانه به عنوان بستر ۲۴
- مبحث پنجم- گستره جرائم رایانه ای و شبکه بین المللی ۲۵
- گفتار اول- کلاهبرداری رایانه ای ۲۵
- گفتار دوم- جعل رایانه ای ۲۸
- گفتار سوم- شنود غیر مجاز ۲۹
- گفتار چهارم- هرزه نگاری ۳۰

فصل دوم- کشف و شناسائی ادله دیجیتال

- مبحث اول- راههای شناسائی ادله دیجیتال ۳۳
- گفتار اول- تفتیش و توقیف داده ها و سیستم های رایانه ای ۳۳
- گفتار دوم- شنود داده ها ۳۷
- گفتار سوم- معاینه صحنه جرم ۴۰
- گفتار چهارم- جلب نظر کارشناس ۴۰
- مبحث دوم- مشکلات و ویژگی های ادله دیجیتال ۴۲
- گفتار اول- اهمیت ادله دیجیتال ۴۲
- گفتار دوم- انواع ادله دیجیتال ۴۳
- گفتار سوم- ویژگیهای ادله دیجیتال ۴۷
- گفتار چهارم- مشکلات کشف و شناسایی جرائم رایانه ای ۴۷

فصل سوم- بررسی استناد پذیری ادله دیجیتال و تعیین دادگاه صالح

- مبحث اول- استناد پذیری ادله دیجیتال ۵۶
- گفتار اول- هویت پدید آورنده ادله دیجیتال ۶۰
- گفتار دوم- اصالت و صحت ادله دیجیتال ۶۴
- مبحث دوم- قابل استناد بودن ادله دیجیتال ۷۰
- مبحث سوم- جمع آوری و محافظت از ادله دیجیتال ۷۳
- گفتار اول- شناسایی ۷۳
- گفتار دوم- محافظت، جمع آوری و مستندسازی ادله دیجیتال ۷۴
- گفتار سوم- طبقه بندی ادله دیجیتال ۷۵
- گفتار چهارم- بازسازی ادله دیجیتال ۷۶
- گفتار پنجم- بسته بندی و حمل و نقل ادله ۷۶
- گفتار ششم- تسلیم و ارائه داده های دیجیتال ۷۷
- گفتار هفتم- ضرورت به صورت مدارک بودن ادله دیجیتال ۷۹
- گفتار هشتم- ادله اثبات دعوی در نظام حقوقی ایران در قلمرو جرائم رایانه ای ۸۲
- مبحث چهارم- تعیین صلاحیت دادگاه صالح ۸۷
- گفتار اول- اصول سنتی صلاحیت ها ۸۷
- گفتار دوم- اصول حاکم بر صلاحیت دادگاه کیفری جرائم سایبری ۹۰
- نتیجه گیری ۹۲
- پیشنهادات ۹۵
- ضمائم ۹۷
- فهرست منابع ۱۰۷

چکیده

امروزه پیشرفت های فراوانی در علم تکنولوژی کامپیوتر ایجاد شده است. این پیشرفت ها باعث شده، این علم تقریباً در تمام جنبه های زندگی مردم رخنه کند. جنبه منفی این پیشرفت سوء استفاده از تکنولوژی کامپیوتری است، که این سوء استفاده از تکنولوژی با گسترش اینترنت و ایجاد شبکه های ارتباطی در سطح جهانی موجب بروز جرائم نوظهوری به نام جرائم سایبری شده است.

جرائم سایبری، ساختاری متفاوت از جرائم سنتی و در عین حال زیانبارتر از آنها دارند. این ساختار ویژه موجب شده است تا قانونگذاران کشورهای مختلف اقدام به ایجاد مقررات جدیدی در این زمینه کنند تا بتوانند این گونه جرائم را به اثبات برسانند.

جرائم سایبری باید به وسیله ادله جدیدی به نام ادله الکترونیکی کشف و شناسائی شود، که در نتیجه آن اقدام به اثبات وقوع جرم از ناحیه متهم صورت گیرد، و مجازات مقرر در قانون را نسبت به او اجرا کرد.

واژگان کلیدی: جرائم سایبری، فضای سایبری، ادله الکترونیکی.

مقدمه

«پیدایش رایانه و پس از آن دنیای مجازی اینترنت، همراه خود دستاوردهای مثبت و منفی بسیاری داشته و دارد از جمله پیامدهای منفی آن پیدایش جرائم نوظهور رایانه ای و اینترنتی است.^۱ رایانه و اینترنت نقشی اساسی در میان جوامع بشری برای خود باز کرده است تا آنجا که بدون آن امکان برنامه ریزی، توسعه و بهروری در زمینه هایی چون فرهنگی، اجتماعی، اقتصادی و علمی در جهان آینده امکان پذیر نخواهد بود.»^۲

این پیشرفت علوم و فناوری، آثار خود را در همه زمینه ها و از جمله وسایل و ابزار کشف و اثبات جرائم آشکار ساخته است، به گونه ای که در عصری که آن را، عصر «ادله علمی» می نامند، حتی ادله سنتی مانند شهادت، اقرار، درموردی با کمک ادله جدید سنجیده می شوند، مهمترین ویژگی دوره علمی، کم رنگ شدن مستندات غیر تجربی یا به عبارتی معنوی در نظام عدالت کیفری است.

«این ادله که طیف گسترده ای از اقدامات، آزمایشات و معاینات علمی و فنی را در بر می گیرد، بسیار متنوع و گوناگون هستند به نحوی که ارائه فهرستی کامل و جامع از آنها بسیار مشکل به نظر می رسد. اقداماتی مانند، معاینات علمی و فنی، توقیف، ضبط اسناد و داده ها، رهگیری مکاتبات و ارتباطات، ضبط صدا و تصویر و بسیاری دیگر از اقدامات پس از وقوع جرم به منظور کشف حقیقت و دستیابی به مجرم، انجام می شوند که بسیاری از این کشفیات به عنوان «قرائن و امارت» قضایی در آیین دادرسی کیفری ایران مورد توجه قرار گرفته اند.»^۳

تحصیل دلیل از محوری ترین موضوعات حقوقی و بویژه حقوق کیفری است. آثار تحصیل دلیل دارای جنبه های بسیاری است که در برخی موارد به علت نقص در تحصیل دلیل، ممکن

^۱ COMPUTER & CYBER CRIME

^۲ طارمی، محمدحسن؛ گذری بر جرائم رایانه ای، نشریه ره آورد نور، شماره ۲۱، صص ۱۱۲ الی ۱۳
^۳ تدین، عباس؛ تحصیل دلیل در آیین دادرسی کیفری، پاییز ۱۳۸۸، چاپ اول، تهران، انتشارات میزان، صص ۳۶۵ الی ۳۶۶

است شخص ماه ها و یا سال های متمادی در بازداشت به سر ببرد و پس از آن تبرئه شود. یک اظهار نظر و اطلاع ناصحیح، یک گزارش خلاف واقع، یک نوشته مجعول، شهادت دروغ و یا اظهار نظر کارشناسی بی دقت ممکن است قاضی را به اشتباه بکشاند و موجبات محکومیت بی گناهی را فراهم سازد.

اهمیت موضوع تحقیق:

به علت رواج وقوع جرائم رایانه ای، باید به دنبال ادله ای باشیم که این جرائم را با سهولت بیشتری بتوان اثبات کرد و متهم را به مجازات مقرر محکوم گرداند و در اثر این اقدام از وقوع این گونه جرائم حتی الامکان جلوگیری کرد.

روش تحقیق:

در این پایان نامه از روش کتابخانه ای و توصیفی استفاده شده است.

سؤالات و فرضیه های تحقیق

سؤالات تحقیق:

- ۱- ادله دیجیتال چیست؟
- ۲- آیا دلایل الکترونیکی قابلیت استناد پذیری در مراجع قضایی را دارند؟
- ۳- با توجه به ویژگی های فضای مجازی آیا تحقیقات کیفری ناظر به کشف جرائم رایانه ای با مشکلاتی در این زمینه مواجه است؟
- ۴- آیا در تعیین دادگاه صالح در زمینه جرائم سایبری قانون جرائم رایانه ای نوآوری داشته است؟

فرضیه های تحقیق:

- ۱- ادله ای که بر روی یک وسیله الکترونیکی ذخیره یا توسط آن منتقل شود، ادله دیجیتالی است.
- ۲- ادله الکترونیکی قابلیت استناد پذیری در مراجع قضایی را دارند ولی نحوه استناد به آنها با نحوه استناد به ادله سنتی متفاوت است.
- ۳- با توجه به خصوصیات فضای مجازی از قبیل پوشیده بودن، گسترده بودن، تحقیقات کیفری ناظر به کشف و شناسایی جرائم رایانه ای با مشکلات چندی در این زمینه روبه رو است.
- ۴- قانون جرائم رایانه ای با پذیرش محل قرارگیری وسیله مؤثر در ارتکاب جرم نظام قضایی همان محل را صالح به رسیدگی می داند.

پیشینه تحقیق:

در زمینه این پایان نامه تحقیقات فراوانی صورت گرفته است ، ولی به موارد زیر در این پایان نامه بیشتر استناد شده است.

- ۱- عبقری، آدینه؛ جرم کامپیوتری جلوه ای نوین از بزهکاری، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه تهران، ۱۳۷۷
- ۲- پاکزاد، بتول؛ جرائم کامپیوتری، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی، ۱۳۷۵
- ۳- حسن زاده، محمد؛ استنادپذیری ادله دیجیتال در فرآیند کیفری، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق دانشگاه آزاد تهران مرکز، ۱۳۸۵

معرفی ساختار

این پایان نامه شامل سه فصل می باشد. فصل اول از پنج مبحث؛ مبحث اول از دو گفتار، مبحث دوم از چهار گفتار، مبحث سوم از پنج گفتار، مبحث چهارم از سه گفتار و مبحث پنجم از چهار گفتار؛ فصل دوم از دو مبحث؛ مبحث اول از چهار گفتار و مبحث دوم از چهار گفتار؛ فصل سوم از چهار مبحث؛ مبحث اول از دو گفتار؛ مبحث سوم از هشت گفتار و مبحث چهارم از دو گفتار تشکیل شده است.

فصل اول:

مبانی، مفاهیم و پیشینه

مبحث اول : پدیده جرم رایانه ای

«جرایم رایانه ای را می توان در سه رتبه یا نسل دسته بندی نمود:

۱- جرائم نسل اول: تقریباً از سالهای ۱۹۶۰ به بعد در کشورهای پیشرفته با به خطر افتادن حقوق فردی شروع شد. کثرت پدیده سرقت برنامه ها، جاسوسی رایانه ای، سابوتاژ رایانه ای، نفوذ در رایانه دیگران، تحت عنوان جرائم رایانه ای متجلی گردید.

۲- جرائم نسل دوم: همزمان با گسترش سریع تکنولوژی ماهواره در دهه ۹۰، شاهد موج تازه ای از جرائم مرتبط با رایانه بوده ایم. در این دوره زمانی پیشرفتهای زیاد تکنولوژی بویژه تکنولوژی تلفنی و مخابراتی، کامپیوتری و نیز شبکه جهانی اینترنت منجر به اعمال مجرمانه و خرابکارانه علیه خطوط ارتباطی و داده ها در زمینه تکنولوژی شد و بدین ترتیب نسل دوم جرائم رایانه ای تحت عنوان جرایم علیه داده ها که ترکیب تکنولوژی مخابراتی و تکنولوژی رایانه ای می باشد بروز پیدا نمود.

۳- جرائم نسل سوم یا جرائم سایبر: رایانه آنگاه قدرت خود را به معنای واقعی به نمایش گذاشت، که در آستانه هزاره سوم «محیط سایبر»^۱ را به جهانیان عرضه نمود، این فضای مجازی از چنان قدرتی برخوردار است که به جرئت می توان گفت هر آنچه را که انسان بتواند تصور کند می تواند نمونه مجازی آن را در این محیط بیابد و در حوزه های مختلف در جهت مثبت و منفی از آن استفاده کند. امروزه این فضای مجازی بستری بسیار مناسب برای ارتکاب جرائم مختلف به وجود آورده است بدون آنکه مرتکب، اثر خاصی از خود بر جای گذارد. این جرائم تحت عنوان «جرایم سایبر»^۲ معروف شدند که در بر گیرنده تمامی جرائم نسل قبلی البته به شکل کاملاً نوین از لحاظ نحوه ارتکاب که در یک محیط مجازی می باشند»^۳

^۱ cyber space

^۲ cyber Crimes

^۳ گرابلی، محمد باقر؛ بررسی جعل و تخریب و اخلاص رایانه ای، پاییز و زمستان ۱۳۸۹، نشریه آموزه های حقوقی دانشگاه علوم اسلامی رضوی، شماره ۱۴، صص ۱۶۰ الی ۱۶۱

«از لحاظ موضوعی جرائم رایانه ای را می توان در سه گروه تقسیم بندی کرد:

- ۱- جرائم علیه اشخاص؛ مانند، اذیت و آزارهای اینترنتی که می توانند به اشکال جنسی، نژادی، مذهبی و ... رخ دهد، هرزه نگاری کودکان
- ۲- جرائم علیه اموال؛ مانند، خرابکاری های کامپیوتری و تبادل برنامه های خطرناک
- ۳- جرائم علیه دولت ها؛ مانند تروریسم اینترنتی.»^۱

گفتار اول : تاریخچه

«تعیین زمان ارتکاب واقعی اولین جرم رایانه ای کار دشواری است و تاریخچه مشخصی از پیدایش جرم الکترونیکی و کامپیوتری وجود ندارد، ولی به هر حال این دسته از جرائم را باید زائیده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست. بر اساس مطالعات صورت گرفته منشأ پیدایش جرم کامپیوتری و اینترنتی به قضیه رویس برمی گردد؛ او که بعد از بی مهری مسئولان یک شرکت فروش عمده میوه و سبزی، به عنوان حسابدار آنها انتخاب می شود از طریق کامپیوتر اقدام به حسابرسی کرده و با تغییر قیمتها و تنظیم درآمد اجناس، مبلغی را کاهش می داد و به حسابهای مخصوصی واریز می کرد. رویس با ظرافت قیمتها را تغییر می داد، بعد از آن با نام ۱۷ شرکت محل و طرف قرارداد، چکهای جعلی صادر و از آن حساب برداشت می کرده به طوری که کمتر از شش سال بیش از یک میلیون دلار بدست آورده است، اما به علت نداشتن مکانیزم برای توقف این روند، رویس خودش را به محاکم قضایی معرفی می کند و به ۱۰ سال زندان محکوم می شود. بدین ترتیب زمینه پیدایش جرم رایانه ای شکل می گیرد و مبحث جدیدی به نام جرم رایانه ای وارد حوزه حقوق شد.»^۲

^۱ زیبر، اولریش؛ جرائم رایانه ای، ۱۳۹۰، مترجمان؛ محمد علی نوری؛ رضا نخجوانی؛ مصطفی بختیاروند؛ احمد رحیمی مقدم؛ چاپ دوم، تهران، انتشارات گنج دانش، ص ۱۹

^۲ تحلیلگران عصر اطلاعات، مرداد ۱۳۸۹، سال چهارم، شماره ۳۵، ص ۳۲

«در ایران، پیشینه پیدایش بزه های رایانه ای، روشن نیست و با اینکه نزدیک به چهل سال از ورود رایانه به ایران می گذرد (آغاز دهه چهل) ولی نمی توان گفت که بزه های رایانه به همین میزان پیشینه دارند. یکی به این دلیل که اندازه آگاهی همگانی با رایانه به اندازه ای نبود که این ابزار در حال رخنه گری در همه جنبه های زندگی انسان ها بود. دوم اینکه بزه بودن هر رفتاری در قبال رایانه وابسته به پیش بینی قانون است و تا زمانی که قانون های کیفری در این زمینه عنوان و کیفری جداگانه پیش بینی نکرده اند یا رفتارهای مرتبط با رایانه مجاز خواهند بود و یا اینکه با عنوان های مجرمانه پیش بینی شده در قانون های کیفری لازم الاجرا قابل پیگرد هستند. به این ترتیب، با اینکه رایانه در آغاز دهه چهل به ایران آمد ولی سخن از بزه های رایانه ای، در پایان این دهه، شنیدنی خواهد بود و این به دلیل تصویب قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان در آذرماه ۱۳۴۸ است که هر چند به روشنی، رایانه را پشتیبانی نکرده اما به طور ضمنی در بند ۱۱ ماده ۲ این قانون زیر عبارت «اثر فنی که جنبه ابداع و ابتکار داشته باشد.» از نوآوری های رایانه ای پشتیبانی کرده است.

پس از انقلاب و بویژه در دهه شصت، اثری از جرم رایانه ای نمی توان دید، بویژه این که در این دوران از جهت فقهی رویکرد حمایت گرایانه از حقوق آفرینش های اندیشه ای وجود نداشت. در دهه ۷۰ نخستین پرونده های مرتبط با رایانه مطرح گردید. «شکایت شرکت نرم افزاری سینا ضد شرکت واژه پرداز مبنی بر تکثیر و فروش غیرمجاز نرم افزارهای تهیه شده شرکت نرم افزاری سینا»، که موجب صدور رأی در تاریخ ۱۳۷۲/۴/۳ در مورد نرم افزارهای کامپیوتری با استناد به قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ شد، را می توان نخستین پرونده طرح شده در ارتباط با بزه های رایانه ای دانست.»^۱

^۱ پاکزاد، بتول؛ بزه های کامپیوتری، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی دانشکده حقوق دانشگاه شهید بهشتی، دی ماه ۱۳۷۵، ص ۳۱

گفتار دوم : تعاریف

۱) تعریف ارائه شده از طرف سازمان های بین المللی در مورد جرائم رایانه ای

«قدم نخست در مورد تعریف جرم رایانه ای، از سوی سازمان همکاری و توسعه اقتصادی (OECD) در سال ۱۹۸۳ برداشته شد. این سازمان اقدام به ارائه تعریفی موسع و مبهم از سوء استفاده از رایانه کرد، که به اشتباه به عنوان جرم رایانه ای مورد استفاده واقع شده است. برابر تعریف سازمان مذکور: سوء استفاده از رایانه شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار و انتقال داده ها است. در این تعریف آشکارا از واژه «سوء استفاده از کامپیوتر» به جای واژه حقوقی «جرم» استفاده شده است و شامل کلیه رفتارهای غیرقانونی، غیرمجاز و غیراخلاقی است که این واژه ها دایره ای وسیعتر از مفهوم جرم دارند. زیرا ممکن است اعمالی صورت پذیرد که از نظر قانون جرم نیست ولی غیراخلاقی و ناپسند باشد.»^۲ به عنوان مثال دوستیهایی که از طریق اینترنت صورت می پذیرد که این عمل از نظر قانون جرم نیست، ولیکن عملی، غیراخلاقی و ناپسندی محسوب می شود.

«پس از اقدامات سازمان همکاری و توسعه اقتصادی، شورای اروپا تلاش هایی را برای تعریف جرم رایانه ای به عمل آورده. شورای اروپا با آنکه دنباله روی از اقدامات سازمان همکاری و توسعه اقتصادی را سر لوحه کار خود قرار داده بود، تعریف ارائه شده از سوی این سازمان را به دلیل ذکر امور غیرمجاز و غیراخلاقی در تعریف جرائم رایانه ای را زیر سؤال برد. این سازمان در فهرست هایی که از انواع جرائم کامپیوتری ارائه کرد، هر یک از اشکال متنوع جرائم کامپیوتری را تعریف کرد، لیکن چون بر این باور بود که هر کوششی برای

^۱ Organization for Economic co-Operation and Development

^۲ باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، ۱۳۹۰، چاپ سوم، تهران، انتشارات بهنامی، ص ۳۰

تعریف نمودن جرم کامپیوتری با نوعی نارسایی مواجه خواهد شد، خود تعریف مستقلی از جرم کامپیوتری به طور کلی ارائه ننموده.»^۱

۲) تعریف محققان و متخصصان برخی کشورها در مورد جرائم رایانه ای

«دکتر پیراگوف در گزارشی که برای انجمن بین المللی حقوق کیفری در مورد جرائم رایانه ای در کانادا تهیه کرده، گفته است: در بسیاری از موارد جرم رایانه ای به وضوح و به طور قانونی از جرائم موجود همچون سرقت، جعل، کلاهبرداری و ایجاد خسارت کیفری جدا نیست. بسیاری از سوء استفاده های رایانه ای را می توان در قوانین کیفری متداول جای داد. کارمند بانک که وجوه حساب های دیگر را به حساب مخصوص منتقل و آن را برداشت می کند، مرتکب سرقت شده است. رایانه را برای ارتکاب جرم مورد نظرش به کار گرفته است. در حال حاضر مقررات موجود در مورد سرقت و کلاهبرداری باید برای بحث جرائم رایانه ای مربوطه کافی باشند. باید در این گونه موارد توجه داشت که رایانه وسیله مساعدت در ارتکاب جرم است و نه جرم رایانه ای مصطلح.

دکتر مونشلاگر در گزارشی که از جرائم رایانه ای در آلمان برای انجمن بین المللی حقوق جزا تهیه کرده، نوشته است، تاکنون در مورد این اصطلاح تعریفی واحد که مورد پذیرش همگان باشد نیامده و تعریف قضایی ساده ای در این زمینه وجود ندارد. به طور کلی، همه اعمال مجرمانه ای که رایانه، ابزار یا وسیله دست یابی به هدف هایی قرار گرفته است، به نظر در این اصطلاح نمی گنجد. در استفاده از رایانه برای ارتکاب جرم نه می توان این واقعیت را که جرم ارتکاب یافته است، نادیده انگاشت و نه این عمل اثری بر روی طبقه بندی جرم ارتکاب یافته دارد. البته ممکن است اثری بالقوه یا بالفعل در جهت قانون شکنی داشته باشد

^۱ عبقری، آدینه؛ جرم کامپیوتری جلوه ای نوین از بزهکاری، پایان نامه کارشناسی ارشد دانشکده حقوق دانشگاه تهران، ۱۳۷۷، ص ۳۲

وهمین موجب می شود که کشف و تعقیب آن دچار مشکلاتی شود. موجب نظر وزارت دادگستری آمریکا؛ هر گونه عمل ناقض قانون کیفری که مستلزم آشنایی با دانش مربوط به تکنولوژی کامپیوتر جهت ارتکاب عمل، تعقیب و یا رسیدگی به آن باشد، جرم کامپیوتری است.»^۱

«همان طور که ملاحظه می شود هنوز اجماع جهانی و بین المللی برای تعریف جرم کامپیوتری شکل نگرفته و در تعریف آن الگویی یکسان مورد تبعیت قرار نگرفته است. این امر از یک طرف ناشی از سطح غیر یکسان تکنولوژی کامپیوتری و گسترش جرائم کامپیوتری در کشورهای مختلف و از سوی دیگر ناشی از نظرات و دیدگاه های متفاوتی است که مبنای تعاریف جرم کامپیوتری را شکل می دهد.»^۲

«جرم رایانه ای یک جرم کیفری است که با ظهور تکنولوژی کامپیوتر ایجاد شده یا امکان آن به وجود آمده است. یا به عبارت دیگر یک جرم سنتی که با استفاده از کامپیوتر به گونه ای تغییر شکل یافته که مأموران برای رسیدگی به جرم، نیازمند یک فهم ابتدایی از کامپیوتر هستند.»^۳

«در قانون جرائم رایانه ای متأسفانه این موضوع به صراحت تعیین تکلیف نشده است و تعریفی از جرائم رایانه ای به عمل نیآورده است. تنها در ماده ۵۳ آن آمده است: «در مواردی که سیستم رایانه ای یا مخابراتی به عنوان وسیله یا ابزار ارتکاب جرم مورد استفاده قرار گیرد و در این قانون مجازاتی تعیین نشده باشد، مرتکب مطابق مقررات قانون مربوط مجازات خواهد شد.» از این ماده می توان چنین استنباط کرد که کلیه جرائمی که به وسیله رایانه انجام پذیرد، مشمول عنوان جرائم رایانه ای شناخته می شود.»^۴

^۱ پاکزاد، بتول؛ منبع پیشین، ص ۳۵

^۲ برومند، باستانی؛ منبع پیشین، صص ۲۹ و ۳۱

^۳ بررسی جرائم کامپیوتری، اردیبهشت ۱۳۸۲، نشریه قضاوت، شماره ۱۳، ص ۴

^۴ بررسی جرائم کامپیوتری، اردیبهشت ۱۳۸۲، نشریه قضاوت، شماره ۱۳، ص ۴

به طور کلی می توان جرائم رایانه ای را چنین تعریف کرد:

آن دسته از جرائمی که با سوء استفاده از سیستم رایانه ای بر خلاف قانون ارتکاب یابد، را جرائم رایانه ای گویند. البته این دسته از جرائم را می توان شامل جرائم سنتی که به واسطه رایانه صورت می گیرد از قبیل کلاهبرداری، سرقت، جعل، و ... و همچنین جرائم نوظهوری که با تولد رایانه ایجاد شده اند مانند ایجاد اختلال در داده ها و جرائم مجازی نیز دانست.

۳) تعریف شبکه بین المللی (اینترنت)

شبکه بین المللی یا اینترنت، نام مجموعه ای از منابع اطلاعاتی جهانی است، که به هر نوع رایانه ای امکان می دهد تا در خدمات آن سهیم شود و مستقیماً ارتباط برقرار کند، به گونه ای که این رایانه ها جزئی از یک دستگاه رایانه ای عظیم جهانی به شمار می روند.^۱

«این شبکه که از گسترده ترین شبکه های جهانی است، علاوه بر رایانه های مستقل و شبکه های کوچک محلی، بیشتر شبکه های جهانی را نیز در دل خود جای داده و امکان تبادل اطلاعات را بین آنها فراهم نموده است. لذا اینترنت را «مادر شبکه ها» می نامند.»^۲

۴) تعریف فضای مجازی (فضای سایبری)

«سایبر نتیک ریشه سایبر می باشد که از کلمه یونانی «کایبرنت» است، که به معنای «هنر حکومت کردن است». «سایبر» در فرهنگ لغت به معنای «کامپیوتر» و «شبکه ای کامپیوتری» است و عموماً تحت عنوان فضای سایبر استفاده می شود.» (رضا سردی)^۱

^۱ جاوید نیا، جواد؛ جرایم تجارت الکترونیکی، ۱۳۸۷، چاپ دوم، تهران، انتشارات خرسندی، ص ۱۲۶
^۲ اسحاقی، محمد؛ بزهداری پیشرفته، جرائم رایانه ای و اینترنتی (قسمت اول)، بهار ۱۳۷۹، نشریه دانش انتظامی، شماره ۵، ص ۲۶.

فضای سایبر «محیطی است مجازی و غیرملموس موجود در فضای شبکه های بین المللی (این شبکه ها از طریق شاهراههای اطلاعاتی مثل اینترنت بهم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگها، ملتها، کشورها و بطور کلی هر آنچه در کره خاکی بصورت فیزیکی و ملموس وجود دارد (بصورت نوشته، تصویر، صوت، اسناد) در یک فضای مجازی به شکل دیجیتال وجود داشته و قابل استفاده و در دسترس استفاده کنندگان و کاربران می باشند و از طریق کامپیوتر، اجزاء آن و شبکه های بین المللی بهم مرتبط می باشد.»^۲

۵) تعریف اصطلاحی ادله دیجیتال

دلیل الکترونیکی عبارت است از: «داده پیام، سخت افزار و نرم افزاری است که اصحاب دعوی برای اثبات یا دفاع از دعوی به آن استناد می نمایند.»^۳

«ادله الکترونیکی به رایانه ختم نمی شود و همه اطلاعات قابل کسب از دستگاه های الکترونیکی از جمله: تلفن همراه، دور نگار، پیام گیر تلفن، پیام های صوتی، پیام های الکترونیکی و غیره را نیز شامل می شود.» (محمد حسنی)^۴

^۱ <http://aftana.ir>

^۲ باستانی، برومند؛ منبع پیشین، ص ۶۵

^۳ عبد الهی، محبوبه؛ دلیل الکترونیکی در نظام ادله اثبات دعوا، ۱۳۹۱، چاپ اول، تهران، انتشارات خرسندی، ص ۲۳

^۴ <http://mohassani-persianblog.ir>

مبحث دوم: ویژگی های جرائم رایانه ای و شبکه بین المللی

جرائم رایانه ای ویژگی های متمایزی از سایر جرائم کلاسیک دارند؛ چرا که ماهیت این گونه جرائم به دلیل تکنولوژی پیچیده و بالا خصوصیات منحصر به فردی داشته که در زیر به این خصوصیات پرداخته می شود.

گفتار اول: خصوصیات مرتکبین جرائم رایانه ای و شبکه بین المللی

«مرتکبین جرائم کامپیوتری اکثراً از طبقات روشنفکر و تحصیل کرده می باشند. ارتکاب این جرائم از آنجایی که منعکس کننده معایب سیستم ها و نحوه نفوذپذیری به شبکه و سیستم های کامپیوتری است، لذا اتخاذ تدابیر پیشگیرانه امنیتی مفید است.

جرائم خطرناک و جدی که موجب خسارات مالی هنگفت می گردد از سوی مرتکبینی که دارای تخصص فنی یا تحصیلات دانشگاهی هستند وقوع می یابند که این دسته از مجرمین را باید جدی گرفت. در یکسری از جرائم کامپیوتری انگیزه اصلی کسب منفعت مالی است ولیکن انگیزه های دیگری چون انتقام جویی شغلی، سرگرمی، اثبات برتری قدرت، خود نمایی، علل روانی و ... وجود دارد. لذا یکی از وجوه تمایز مرتکبین جرائم کامپیوتری از یکدیگر نوع انگیزه آنان می باشد. بر این اساس سه گروه از مجرمین از یکدیگر شناخته شده اند، مزاحمان کامپیوتری، خلافکاران و خرابکاران.

انگیزه گروه اول صرفاً دستیابی به سیستم های کامپیوتری و اطلاعات موجود در آن می باشد و اکثراً نوجوانانی هستند که برای تفریح و سرگرمی و ارضای حس برتری جوئی دست به این اقدامات می زنند.

انگیزه گروه دوم یعنی خلافکارها کسب منفعت مالی است و عمدتاً در دو مقوله جاسوسی و کلاهبرداری فعالیت دارند، که روز به روز بر تعداد این افراد در جهان افزوده می شود.

انگیزه گروه سوم تنها صدمه زدن و ایراد خسارت به دیگران است، که نه به قصد کسب منفعت و نه سرگرمی و تفریح می باشد، بلکه افرادی هستند که دارای اختلالات روانی بوده و یا قصد انتقام جوئی دارند. آنچه در مورد مرتکبین جرائم رایانه ای حائز اهمیت می باشد آن است که این دسته از مجرمین در اذهان عمومی جایگاه چندان نامطلوبی ندارند و به نظر می رسد که نسبت به مجرمان دیگر در اجتماع از مقبولیت بیشتری برخوردارند چه بسا به عنوان یک قهرمان و یا بزرگترین بزهکار کامپیوتری سال در تمام دنیا مشهور شده و نامشان زیانزد عام می شود. جالب اینکه بعضی از مجرمان رایانه ای اقدام به تشکیل انجمن یا گروه نموده اند که به عنوان نمونه به انجمن خدشه زندگان می توان اشاره کرد.^۱

گفتار دوم: عدم تخمین دقیق جرائم ارتكابی

«با افزایش به کارگیری کامپیوتر در تمامی عرصه های زندگی و همچنین سهولت استفاده از آن و گسترش شبکه جهانی (اینترنت) امروزه جرائم کامپیوتری می تواند به وسیله هر کسی در هر نقطه ای از دنیا به وقوع بپیوندد و با آنکه تحقیقات به عمل آمده نشان از روند روبه رشد جرائم کامپیوتری دارند، ولیکن تعداد آمارهای موجود نمی تواند ما را به نتیجه گیری مطلوب رهنمون سازد. به علت وجود رقم سیاه بسیار بالای آن و چه بسا این آمار منعکس کننده تعداد جرائم مکشوفه اند و نه تعداد جرائم واقعی.

ملموس نبودن جرائم کامپیوتری مبتنی بر چند عامل می باشد. اول آنکه تکنولوژی پیشرفته یعنی ظرفیت حافظه فشرده کامپیوتر و سرعت بالای عملیات، موجب کشف دشوار جرائم کامپیوتری است. دوم آنکه به دلیل عدم وجود سابقه و شناخت در خصوص جرائم کامپیوتری بزه دیدگان و مأمورین اجرای قانون پس از مدتی متوجه وقوع جرم می شوند و دسته آخر آنکه

^۱ باستانی، برومند؛ منبع پیشین، صص ۳۳ الی ۳۴