دانشگاه علامه طباطبایی

دانشکده حقوق و علوم سیاسی

پایان نامه جهت دریافت مدرک کارشناسی ارشد حقوق جزا و جرم شناسی

موضوع:

جاسوسی در فضای سایبر

استاد راهنما:

جناب آقای دکتر منصور میرسعیدی

استاد مشاور:

جناب آقای دکتر حسنعلی موذن زادگان

نگارش:

سید محمد عقیلی

تابستان ۱۳۹۰

تقدیم به:

پدرم که حضورش جوانه وجودم را از ناملایمات مصون می دارد...

مادرم که حضورش عشق را معنا و محبت را تفسیر می کند...

برادر و خواهرم که حضورشان امید به فردا ها را به ارمغان می آورد...

با تقدیر و تشکر بیکران از استاد بزرگوار و مهربانم جناب آقای دکتر میر سعیدی به پاس زحمات و همراهی های بیدریغشان...

با سپاس از جناب آقای دکتر موذن زادگان به سبب راهنمایی ها و دلسوزی های ارزنده ایشان...

و با قدردانی از لطف و عنایت جناب آقای دکتر رضوی فرد...

چکیده

به واسطه افزایش پردازش داده ها در مشاغل و ادارات، داده های ارزشمند اقتصادی اداری، حکومتی و خصوصی به طور زیاد در سیستم های داده پردازی و در حامل های داده ها ذخیره می شوند، امروزه شاهد نفوذ یابنده ها (خدشه زننده ها) هستیم که به طور غیرمجاز به سیستم ها دست یابی پیدا می کنند این افراد از توانایی های خاص کامپیوتر آگاهی دارند و به همین دلیل در صدد دستیابی غیرمجاز به آن هستند دلایل و انگیزه های متنوعی می تواند از ارتکاب به چنین اعمالی وجود داشته باشد گاه انگیزه مرتکبین ایجاد چالش در سیستم امنیتی شرکتها است و گاه در صدد استفاده از بانکها داده ها فیلتریزه نشده اند هستند و یکی دیگر از انگیزه های آنها تحصیل اطلاعات اقتصادی و بازرگانی و تسلیم آنها به مراکز دیگر است که اصطلاحاً به آن جرم جاسوسی گویند.حال در رساله پیش رو سعی شده است تا با بررسی جرم جاسوسی در حقوق جزای کلاسیک، نحوه ارتکاب آن نیز در فضای مجازی(سایبری) مورد مداقه قرار گیرد و با توجه به آن، وضعیت قوانین مدون داخلی و نقاط ضعف و قوت آنها در راستای جرم انگاری،پیشگیری، برخورد و رسیدگی به این جرم نوظهور،مطالعه و بررسی شود.

فهرست مطالب

عنوان **صفحه**

مقدمه

فصل اول : مفاهیم و پیشینه تحقیق ۱

مبحث اول: فضای سایبر ۱

مبحث دوم: جرم سایبری..... ۴

مبحث سوم: تقسیم بندی جرائم سایبری..... ۵

گفتار اول: تقسیم‌بندیهای موجود ۵

گفتار دوم: تقسیم‌بندی براثر فضای سایبر..... ۶

مبحث چهارم: سیر تاریخی استفاده از رایانه ۸

فصل دوم: جاسوسی؛ تحولات و انواع **۱۲**

مبحث اول: تعریف جرم جاسوسی..... ۱۲

مبحث دوم: جاسوسی از منظر قرآن کریم..... ۱۴

مبحث سوم: تحولات تاریخی جاسوسی..... ۱۵

بند اول: دوره باستان و قرون وسطی ۱۵

بند دوم: دوره جدید ۱۶

بند سوم: دوره معاصر ۱۷

مبحث چهارم: انواع جاسوسی..... ۱۸

گفتار اول: جاسوسی نظامی..... ۱۸

گفتار دوم: جاسوسی اقتصادی ۲۱

گفتار سوم: جاسوسی منابع/ محیطی ۲۳

گفتار چهارم: جاسوسی رایانه ای (کامپیوتری) و جاسوسی اینترنتی(درفضای سایبر) ۲۴

بند اول: چالش ها و موانع جرم انگاری ۲۵

بند دوم: اهمیت جرم انگاری ۲۸

فصل سوم: جاسوسی از منظر قوانین موضوعه ۳۱

مبحث اول: جاسوسی از منظر حقوق فرانسه ۳۱

مبحث دوم:جاسوسی از منظر حقوق ایران ۳۳

گفتار اول: جاسوسی در قوانین نیروهای مسلح ۳۴

بند اول: رکن قانونی ۳۶

بند دوم: رکن مادی ۳۷

گفتار دوم: جرم جاسوسی در قانون مجازات اسلامی مصوب ۱۳۷۵ ..... ۳۹

بند اول: رکن قانونی ۴۰

بند دوم: رکن مادی ۴۱

بند سوم: رکن روانی (در دو قانون نیروهای مسلح و مجازات اسلامی) ۴۲

گفتار سوم: جاسوسی در قانون جرائم رایانه ای مصوب ۱۳۸۸ ..... ۴۳

بند اول: ارتکاب اعمال مجرمانه نسبت به داده‌های سری یا حامل‌های داده ۴۵

بند دوم: نقض تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی ۵۱

بند سوم: بی‌احتیاطی و بی‌مبالاتی در حفظ داده‌های سری ۵۳

بند چهارم: انتشار یا در دسترس قرار دادن محتویات آموزش جاسوس ۵۵

فصل چهارم: راه های اثبات و صلاحیت کیفری در جرائم سایبری ۵۸

مبحث اول: راه های اثبات جرائم سایبری ۵۸

گفتار اول: چالشهای تحصیل دلیل ۵۸
بند اول: آسیب پذیری سامانه های رایانه ای در برابر جرایم ۶۰
بند دوم: تراکم اطلاعات و فرایندها ۶۱
بند سوم: قابلیت دستیابی به سامانه و آسیب پذیری ادله الکترونیکی ۶۱
گفتار دوم: اعتبار ادله الکترونیکی ۶۳
بند اول: قاعده بهترین دلیل ۶۳
بند دوم: قاعده ادله سماعی ۶۴
گفتار سوم: راه های رفع موانع و رهیافتهای سامانه های حقوقی گوناگون ۶۵
بند اول: راه های رفع موانع ۶۵
بند دوم: رهیافتها ۷۸
مبحث دوم: صلاحیت کیفری در جرایم سایبری ۸۳
نتیجه گیری و پیشنهاد ۸۷
منابع ۹۵

مقدمه

جرم جاسوسی در فضای سایبر

کاربردی

بیان مسئله:

با ابداع اینترنت در قرن بیستم برقراری ارتباط و مبادله و داد و ستدهای اطلاعاتی و تجاری به نحو معجزه آسایی تسهیل شد.بنابر این کشورها و دولت ها سعی نمودند تا حد امکان اداره امور خود را بر پایه این شبکه استوار سازند.

اما پس از چندی این شبکه خود به مأمنی برای ارتکاب تخلفاتی چون هک کردن سایتهای مختلف و از طریق آن ربایش اطلاعات خصوصی و مالی افراد،کلاهبرداری،جعل و ... تبدیل شد.ویژگی فراملی بودن این جرائم و نیز پیچیدگی،تعارض صلاحیت قضایی و پاک شدن سریع آثار ارتکاب جرم در این شبکه،برخورد و مقابله با این جرائم را بسیار سخت نموده است.لذا کشورهای پیشرفته در راستای مقابله با این پدیده ابتدا اقدام به تعریف جرم رایانه ای نموده و سپس با تصویب قوانین و کنوانسیون های مختلف از جمله کنوانسیون بوداپست اقدام به جرم انگاری موضوعاتی چون جرائم علیه محرمانگی،تمامیت و دسترس پذیری داده ها،جعل،کلاهبرداری،هرزه نگاری کودکان و نقض حق نشر نمودند.اما در این بین آنچه حساس تر به نظر می رسد مسئله مربوط به جاسوسی و دسترس پذیری به اطلاعات محرمانه اشخاص و دولتها در زمینه های مختلف از جمله اقتصادی،صنعتی و از همه مهمتر نظامی می باشد.آنچه مسلم است با توجه وابستگی و پیچیدگی روابط بین دول و ملتها،جنگهای نظامی و مسلحانه جای خود را به جنگهای سایبری و الکترونیک داده اند.

لذا در این پایان نامه سعی می شود درابتدا با بیان کلیاتی از جرائم رایانه ای به بررسی جرم جاسوسی سایبری با توجه به مواد ۴،۳و۵ قانون جرائم رایانه ای پرداخته شود.همچنین به دلیل جدید بودن مبحث مذکور و پیوستگی مباحث شکلی با موضوع،اشاره ای نیز به ادله مورد نیاز جهت کشف،تعقیب و رسیدگی به این جرائم خواهیم داشت.

سوالات تحقیق:

۱.تا چه حد عناصر و ارکان جرم جاسوسی رایانه ای مندرج در قانون جرائم رایانه ای مصوب ۱۳۸۸ با عناصر و ارکان جرم جاسوسی سنتی(منعکس در قانون مجازات اسلامی و قانون جرائم نیروهای مسلح)هم پوشانی دارند؟

۲. چرا ادله سنتی اثبات جرم برای اثبات جرم جاسوسی رایانه ای از کارایی لازم برخوردار نیستند و نظام حقوقی نیازمند پیش بینی ادله نوین در این مورد می باشد؟

فرضیه های تحقیق:

۱.ارکان جرم جاسوسی رایانه ای تباین کلی با عناصر و ارکان جرم جاسوسی سنتی دارند.

۲. ماهیت فراملی،تنوع حوزه های صالح به رسیدگی و امکان زوال سریع آثار این جرم در فضای سایبر از مهمترین علل عدم کارایی ادله سنتی و ضرورت پیش بینی ادله نوین اثباتی در این موضوع می باشد.

هدف تحقیق:

مطالعه مباحث مطابق با موازین بین المللی به جهت هماهنگی با جامعه بین الملل در راستای مقابله منسجم با این جرائم.

ضرورت تحقیق:

با توجه به افزایش گستره دولت الکترونیک در کشور این نیاز احساس شد که به بررسی قوانین موضوعه در این رابطه پرداخته شود و با مطالعه نقاط ضعف و قوت این قوانین در راستای روز آمدسازی و هماهنگ سازی آنها با نظامات بین المللی اقدام شود.

کاربرد تحقیق:

نتایج این تحقیق می تواند در اختیار نهادهای علمی،نظامی و تقنینی کشور قرار گیرد تا در راستای اقدامات عملی و کاربردی قدم برداشته شود.

پیشینه تحقیق:

کتابهای مجموعه مقالات حقوق فناوری اطلاعات،اخبار جرایم سایبری و مقالات:

What is cyber crime?
The internet legal dimensions
Defining cyber terrorism

کتاب حقوق فناوری اطلاعات چاپ معاونت حقوقی قوه قضائیه تنها بـه ارائـه مقـالاتی چنـد در زمینه جرائم سایبری در شکل کلی آن پرداخته و به هیچ عنوان اشاره ای بـه مصـادیق مـاهوی ارتکابی در فضای مجازی از جمله موضوع پایان نامه پیش رو ننموده است.

کتاب اخبار جرایم سایبری چاپ معاونت حقوقی قوه قضائیه نیز تنها اقدام به انتشار پرونده های جرایم سایبری و نحه ارتکاب آن نموده و هیچ گونه بررسی ماهوی در این زمنه صـورت نگرفتـه است.

مقالات فوق الذکرهم بیشتر به بیان کلیات و تعاریف موجود در زمینه جرائم رایانـه ای پرداختـه اند.

نوآوریهای تحقیق:

می توان گفت تحقیق پیش رو به عنوان اولین منبعی است که به بررسی ماهوی جرم جاسوسی در فضای سایبر به همراه بررسی و تحلیل مواد مربوط، در قانون جرائم رایانه ای و تطبیق آن بـا جرم جاسوسی کلاسیک مندرج در قوانین جزایی ایران پرداخته است و به طور همزمان مسـائل شکلی پیش روی مجریان قانون را در رسیدگی به این جرایم واکاوی کرده و به ارائه راه حل می پردازد.

روش تحقیق:

در این تحقیق با روش توصیفی و تحلیلی سعی در توضیح و تشریح وضع موجود و ارائه راهکـار با توجه به مطالب مذکور،شده است.

ساماندهی تحقیق:

این تحقیق در چهار فصل مجزا ابتدائاً به بیان مفاهیم و پیشینه هادر فصل اول و در قالب پنج مبحث می پردازد،در فصل دوم با مفهوم جاسوسی و انواع و تحولات آن در چهار مبحث آشنا می شویم، فصل سوم در دو مبحث جاسوسی در قوانین موضوعه را مورد کنکاش قرار می دهد و در نهایت راههای اثبات و صلاحیت کیفری در جرائم سایبری در فصل چهارم و در دو مبحث مورد بررسی قرار می گیرد.

فصل اول: مفاهیم و پیشینه تحقیق

مبحث اول: فضای سایبر

فضای سایبر عبارتی است که در دنیای اینترنتی رسانه و ارتباطات بسیار شنیده می شود. به نظر می رسد به کارگیری این اصطلاح در این زمینه و برای ارجاع بـه امـور فنـی بـه آن رنگ و بویی صرفا فنی ومکانیکی داده باشد. ملاحظه دقیق تر این اصطلاح نشان مـی دهـد که این واقعیت وجوه و جنبه هـای متنـوعی از جملـه خصـلت هـای روان شـناختی قابـل توجهی دارد در منابع موجود آمده است که واژه سایبر از لغت یونـانی keybermetes بـه معنای سکاندار یا راهنما مشتق شده است و نخستین بار این اصـطلاح سـایبرنتیک توسـط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین در سال ۱۹۴۸ به کار برده شده. سایبرنتیک علم مطالعـه و کنتـرل مکانیزمهـا در سامانه های انسانی و ماشینی ماشین و رایانه ها است. ماننـد سـامانه عصـبی در موجـودات زنده و توسعه سامانهای معادل آنها در وسایل الکترونیکی و مکانیکی است.

سایرنتیک تفاوتها و شباهتهای میان سامانه های زنده و غیرزنده را مقایسه کرده است.[۱]

سایبر پیشوندی است برای توصیف یک شخص یک شی یک ایده و یا یک فضا کـه مربـوط به دنیای رایانه و اطلاعات است. در طی توسعه اینترنت واژه های ترکیبـی بسـیاری از ایـن کلمه سایبر به وجود آمده است که به تعدادی از آنها اشاره می کنیم:

فضای سایبر[۲]، شهروند سایبر[۳]، پول سایبر[۴] فرهنگ سایبر[۵]، راهنمای فضای سایبر[۶]و ... .

---

[۱] - حسنوی، رضا، فرسایی، داریوش- فرهنگ تشریحی رایانه صص ۱۵۰- ۱۵۱.

[2] - Cyber space
[3] - Cyber citizen
[4] - Cyber cash
[5] - Cyber culture
[6] - Cyber coach

بعضی معتقدند واژه فضای سایبر را نخستین بار ویلیام گیبسون[1] نویسنده داستان علمی تخیلی در کتاب neveromancer در سال ۱۹۸۴ به کار برده است. فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسانها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود. یک سامانه آنلاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی در فضای سایبر نیاز به جابجایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می گیرد. این عدم جابجایی فیزیکی، محققان را واداشت که به مطالعه برخی شباهتهای فضای سایبر با حالتهای ناهشیاری بخصوص حالتهای ذهنی که در رویاها ظاهر می شوند بپردازند.

آنان از گفته های یکی از رهبران بزرگ ذن به نام چانگ تزو برای تحقیقات خود در زمینه کشف شباهتهای بین فضای سایبر و رویا بهره جسته اند. گفته می شود که چانگ تزو شبی در خواب می بیند که یک پروانه شده است یا اینکه پروانه ای هستم که اکنون خواب می بیند یک مرد شده است روند کاری یک کاربر رایانه در فضای سایبر دقیقا نوعی یکی شدن یا محو شدن در درون واقعیتی متفاوت یعنی واقعیتی مجازی که ورای قوانین و واقعیتهای ملموس است که کاربر رایانه در هنگام کار در فضای مجازی با آن یکی می شود. بنای محیط سایبرا را چند سالی بیشتر نیست که متخصصان فناوری اطلاعات مورد استفاده قرار میدهند و در همین چند سال آنچنان مقبولیتی یافته که اغلب از محیطهای الکترونیکی که با داده کار می کند به عنوان سایبر یاد می شود در واقع واژه سایبر به همه محیطهایی اشاره دارده که اساس فعالیت آنها بر مبنای پردازش است و طبق سامانه صفر و یک کار می کنند. واژه رایانه ای بگونه ای دقیق و جامع نمی تواند گستردگی این محیط را

[1] - William Gibson

نشان دهد زیرا بسیاری از ابزار و وسایل امروزی با داده هایی کار می کنند که اساسا به آنها رایانه ای اطلاق نمی شود از این رو عبارتهایی دقیق جرمهای رایانه ای یا جرمهای اینترنتی نیز نمی توانند بگونه ای دقیق جرمهای ارتکابی مربوط به این حوزه را پوشش دهند. برای نمونه یک سامانه ضبط و پخش صوتی الکترونیکی رایانه نیست ولی بطور کلی در زیر مجموعه جهان سایبر قرار می گیرد.

در فارسی واژه سایبر را در مجاز و مجازی ترجمه کرده اند. این ترجمه گویای دقیق این واژه نیست. مجاز در برابر حقیقت به کار می رود و در زبان انگلیسی معادل واژه است از سویی دیگر محیط سایبر محیطی است حقیقی و واقعی و نه دروغین و مجازی در واقع جهان سایبر هر چند به شکل مادی و ملموس احساس شدنی نیست اما همانگونه که به اطلاعات ناشی از امری نمی توان عنوان مجازی داد به جهان سایبر نیز نمی توان مجاز و مجازی اطلاق کرد با این وجود این چون در زبان فارسی واژه ای که مترادف با این عبارت باشد یافت نشده است استفاده از عبارت فضای مجازی و جرمهای جهان مجازی رو به گسترش است که رفته رفته جانشین عبارتی چون جرمهای رایانه ای و جرمهای اینترنتی می شود.[1]

از محیط سایبر به محیط فناوری اطلاعات it یا محیط اطلاعات و ارتباطات نیز یاد شده است از این رو مشاهده می شود که برای نمونه به جرمهای محیط سایبر جرمهای علیه فناوری اطلاعات نیز گفته می شود.

[1] شیرزاد، کامران، جرائم رایانه ای از منظر حقوقی جزای ایران و بین الملل، انتشارات بهینه فراگیر، تهران، ۱۳۸۸، ص ۱۵

مبحث دوم: تعریف جرم سایبری

اولین مشکل در ارایه تعریف، ماهیت جرم سایبری است. در مورد تعریف و ماهیت جرایم الگوی یکسانی مورد تبعیت قرار نگرفته است. حتی در اروپا کشورها وضع یکسانی ندارند بطور مثال اسپانیا در گزارش ملی خود صریحا بیان می کند که تعریف قضایی از این پدیده نداریم، زیرا قوانین و مقررات کیفری مناسب برای آن نداریم. از سویی چون رهیافت های کشورهایی که به بحث جرایم رایانه ای پرداخته اند متفاوت است شاهد تعاریف گوناگون هستیم.

شورای اروپا در تعریف جرم رایانه ای هم به تعریف OFCD نظر داشته هم تعریف متخصصان کمیته مشکلات ناشی از جرم را مدنظر قرار داده است و با دیدی کلی تعریف OFCD را می پذیرد. سو استفاده از رایانه به عنوان هر رفتار غیرقانونی- غیر اخلاقی یا غیر مجاز مربوط به پردازش اتوماتیک و انتقال داده ها است، در این تعریف بیشتر دیدگاه حقوقی دنبال شده است و بسیار کم به مفاهیم اصلی مدنظر در یک مسیر غیرقانونی پردازش داده ها که خود بخشی از معضل جرایم رایانه ای است توجه شده است. نکته دیگر این مورد به کارگیری واژه سو استفاده، بجای استفاده از واژه حقوقی جرم است این امر ناشی از این است که OFCD رویکرد صرف قضایی ندارد و از حیث اخلاقی نیز قضیه را در نظر دارد یکی از متخصصان کمیته یاد شده هر واقعه ای را توام و انجام شده با تکنولوژی رایانه که موجب شده بزه دیده متحمل ضرر خواه بالقوه یا بالفعل شود و مرتکب عامدا توانسته یا خواهد توانست چیزی اعم از امتیاز مالی و غیرمالی کسب کند جرم کامپیوتری می داند.[1]

[1] Ten top computer crime of 2007, Australian institute of criminology

مبحث سوم: تقسیم بندی جرایم سایبری

نخستین تلاشهای گسترده در مورد مشکلات حقوق کیفری در باب جرایم رایانه ای از سوی آغاز شد. از سال ۱۹۸۳ تا ۱۹۸۵ یک کمیته اختصاصی مشغول بررسی راه های ممکن برای هماهنگی بین المللی قوانین کیفری در مبارزه با جرایم اقتصادی مرتبط با رایانه شد. در سپتامبر ۱۹۸۵ این کمیته به کشورهای عضوتوصیه کرد که در مورد اقدامات آگاهانه و بصورت عمدی در زمینه سو استفاده های مرتبط با رایانه محدوده ای را که باید جرم شناخته شود و تحت پوشش قوانین کیفری قرار گیرد مدنظر قرار دهند.[۱]

گفتار اول: تقسیم بندی های موجود

اولین تقسیم بندی از آن تقسیم بندی است که جرایم را به پنج دسته تقسیم کرد شورای اروپا در دو لیست حداقل و اختیاری این میزان را به ۱۲ مورد رساند سازمان ملل بحث ویروس ها را افزود و نیز بر نقش ویروس تاکید کرد متخصصان نیز از جمله زیبر و کاسپرسن و ... تقسیم بندی هایی حسب تئوری های موجود ارایه کردند بعدا اینترپول بر اساس یک تقسیم بندی پلیسی و نه منطبق بر متد حقوق جزا، تقسیم‌بندی جدیدی را ارائه کرد. که البته جامع و مانع نیست. تقسیم‌بندی کنوانسیون اروپایی جرایم سایبری جدیدتر اما بصورت حداقلی و جزئی است. که نمی تواند در بردارنده حتی تعداد قابل توجهی از جرایم سایبری باشد. از این رو و در حال حاضر پروتکل جرایم تروریستی به عنوان مکمل کنوانسیون یاد شده و نیز پیش نویس جرایم حملات علیه سامانه های

[۱] همان، ص ۶۳

اطلاعاتی تصویب و ارایه شده است در قوانین ملی کشورها نیـز تـا حـدی تغییـرات اعمـال شده است.

گفتار دوم: تقسیم بندی بر حسب فضای سایبر

در فضای سایبر بسته به دیدگاه مولفان و تئوری پردازان چهار تا شش دسته جـرایم را مـی توان بر شمرد اینکه تعداد طبقات جرایم چند تا باشد مهم نیست بلکه به کارگیری دقـت و تفکیک طبقات مهم است. در نهایت طبقات و دسته جات زیر را می توان به عنوان طبقـات مادر و عمده جرایم سایبری ذکر کرد.

الف) جرایم کلاسیک با توصیف سایبری: در این دسته جرایمی قرار دارنـد کـه قـبلا وجـود داشته اما به واسطه تغییر در عنصر مادی کلی یا جزیی به توصیف رایانه ای و یا سایبری از آن یاد می شود و قوانین جداگانه ای به آنها اختصـاص یافتـه اسـت برخـی از ایـن جـرایم عبارتند از: کلاهبرداری سایبری رایانه ای جعل سایبری رایانه ای، تخریـب سـایبری رایانـه ای، جاسوسی سایبری/ رایانه ای سابوتاژ سایبری رایانه ای، تطهیر نامشـروع سـایبری مـواد مخدر در سایبر سایبردراگ سایبر تروریسم و ...

ب) جرایم سایبری/ رایانه ای علیه محتوا: این دسته جرایم نیـز گـاهی قـبلا وجـود داشـته است مثل توهین و ترویج ایدئولوژی های غیر انسانی و نژادپرستانه، تحریک به فعالیت های غیر قانونی.

ج) جرایم صرف (محض) سایبری /رایانه ای: این دسته جرایم صرفا بهد فنی دارند اگر چه صوری از آن قبلا در جریام کلاسیک قابل ملاحظه است. این دسته بطور عمده شامل جرایم دستیابی غیر مجاز، استفاده غیر مجاز و و... است.[1]

د) جرایم مخابراتی: جرایم مخابراتی قبلا جداگانه بحث می شدند، زیرا مبتنی بر ماهواره و نیز بخشی از جرایم در فضای سایبر است. این جرایم عبارتند از: جرایم مخابراتی با توصیف سایبری، جرایم مرتبط با ماهواره، جرایم موبایل و شنود.

ه) سایر جرایم: در این دسته سایر جرایم جای می گیرند که عبارتند از رشته ها یا دکترین هایی که بدوا و فی حد ذاته جزو رشته های مدنی، تجاری، عمومی حقوق سایبر قرار دارندف اما از ضمانت اجرایی جزایی برخوردار شده اند. این جرایم عبارتند از: جرایم مالکیت فکری مشتمل بر –جرایم کپی رایت، جرایم حق اختراع و... جرایم تجارت الکترونیک، جرایم بانکداری الکترونیک و پرداخت های الکترونیک و...، جرایم علیه حمایت از داده و...

باید به خاطر داشت این جرایم محدود و منحصر نیستند. از سویی در عرصه فناوری اطلاعات برخی مسایل حقوقی که در زیر گروه نانو[2] رایانه قرار می گیرند، در آینده به تقسیم بندی های موجود افزوده خواهد شد.

[1] زندی، محمدرضا، تحقیقات مقدماتی در جرائم سایبری، انتشارات جنگل، تهران، ۱۳۸۸، ص ۴۵

[2] - فناوری نانو عبارت است از هر دستکاری مواد در مقیاس اتمی یا مولکولی و به خصوص ساخت قطعات و لوازم میکروسکوپی مانند روبات های میکروسکوپی، نانوتکنولوژی، توسعه فناوری و تحقیقات در سطوح اتمی، مولکولی و در مقیاس ۱ تا ۱۰۰ نانومتر، خلق و استفاده از ساختارها و ابزار و سامانه هایی که به خاطر اندازه کوچک یا حد میانه آنها خواص و عملکرد نوینی دارند. یک نانومتر یک هزارم میکرون است. اگر بخواهیم احساس فیزیکی نسبت به آن داشته باشیم می توان گفت یک نانومتر ۸۰۰۰۰ قطعه موی انسان می باشد.

مبحث چهارم: سیر تاریخی استفاده از رایانه

الف-دهه های ۵۰ و ۶۰: اگرچه در سال ۱۳۴۵ از رایانه ایی استفاده می شد که با لامپ خلا کار می کرد اما برای بررسی بهتر به دهه های ۱۹۵۰ و ۱۹۶۰ بر می گردیم. در این دو دهه به تدریج استفاده از رایانه رایج شد، امور حسابداری مربوط به توزیع کالا از جمله کالای کشاورزی و نگهداری حسابها به شکل مدرن و ساده از خصایص این دو دهه است. در سال ۱۹۶۳ (۴۶ سال قبل) در اولین جرم رایانه ای فارغ از اینکه آیا واقعا اولین جرم بوده یا خیر یا به عبارت بهتر اولین جرم کشف شده رویس برنامه نویس یک شرکت توزیع کالای کشاورزی بود وی با درست کردن تعدادی حساب موهوم در برنامه و نیز ایجاد کشاورزی بود وی با درست کردن تعدادی حساب موهوم در برنامه و نیز ایجاد دستورالعملی مبنی بر واریز مبلغی وجه از هر حساب به این حسابهای موهوم توانست مبلغ زیادی به دست آورد. نامبرده هر چند یک بار با کشیدن چک وجه حسابهای مذکور را برداشت می کرد و به علت اینکه تکنیک های برنامه نویسی پیشرفته نبود رویس نمی توانست جلوی برنامه را بگیرد بنابراین خود را به مراجع قضایی معرفی کرد و به عنوان کلاهبردار به ۱۰ سال زندان محکوم شد. کشف این جرم توجه طبقات مختلف را به خود جلب کرد افکار عمومی روزنامه نگاران اصحاب مطبوعات، جرم شناسان و حقوقدانان هر کدام به نحوی با آن مواجه شدند. این پدیده جدید با قالب های کلاهبرداری قابل تطبیق نبود از این رو به تدریج روشن شد حقوق جزا در حال روبرو شدن با یک چالش جدی است که اکثر شاخه های حقوق جزا را تحت الشعاع قرار داده است.[1]

[1] - زیبر، اولریش، جرائم رایانه ای ترجمه محمدعلی نوری و رضا نخجوانی، انتشارات گنج دانش، چاپ اول، ص ۵۰، ۱۳۸۳

ب - دهه ۷۰: در این دهه برنامه نویسی پیشرفت داشت کارهای مالی بـه شـکل سـاده بـه واسطه رایانه ای بزرگ انجام می شد، حتی در کشور ما سازمان سنجش از این شـیوه بهـره مند شد و به تـدریج بحـث تبـادل الکترونیکـی داده یـا مطـرح شـد کـه بعـدا بـه تجـارت الکترونیک تغییر یافـت. در ایـن دهـه عـلاوه بـر کلاهبـرداری رایانـه ای جعـل رایانـه ای، جاسوسی و به جمع جرایم نوظهور پیوستند تا حقوق جزا را به طرف یک رشـته جدیـد بـه نام حقوق کیفری اطلاعاتی سوق دهند. دو اصطلاح در دهه ۷۰ استفاده شد.

ج- دهه ۸۰: اصطلاح اول حقوق رایانه و اصـطلاح دوم حقـوق تکنولـوژی اطلاعـات جـرایم رایانه ای و جرایم مربوط یا علیه تکنولوژی اطلاعات از اواخر این دهه با بحـث نـرم افـزار و پرداختهای الکترونیکی به شکل ساده اداره امور بیمارستانی، امور اداری ومالی مطـرح بـود. اینترنت یا به قول سلف آرپانت در حال تغییر و تحول و گسترش بود.

در این دوره برای اولین بار لیستی پنجگانه از جرایم رایانه ای ارایه کرد که به نظر بعضی از اساتید در آن اصل قانونی بودن لحاظ نشده بود. در این دهه به واسطه طـرح مسـاله شـبکه ها، پایگاه داده تا حدی اینترنت، تعداد جرایم و نیز مسایلی مربوط به حق تالیف نـرم افـزار، حریم خصوصی، مالکیت اطلاعات و ... مورد بحث قرار گرفت. در این دهـه بـه دو اصـطلاح قبلی اصطلاحات جرایم اینترنتی و جرایم شبکه ای افزوده شد.

د - دهه ۹۰: در این دهه استفاده از تکنولـوژی اطلاعـات در زمینـه بانکـداری امـور اداری، مالی بصورت پیشرفته امور تولید و صنعت تحقیقات مراکز علمی از جملـه دانشـگاه هـا بـه شدت افزایش یافت. خلق اصطلاح سایبر که امروز محور بسـیاری از بحـث هاسـت در ایـن دهه خصوصا از سال ۱۹۹۴ به بعد بود البته قبل سایبرنتیک مطرح بود اما فضـای سـایبر و به دنبال آن حقوق سایبر و جرایم سایبری از این دهه شروع شد.