دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دانشگاه پیام نور مرکز تهران

دانشکده علوم انسانی

گروه حقوق

پایان نامه برای دریافت درجه کارشناسی ارشد

در رشته حقوق جزا و جرم شناسی

عنوان:

مقایسه جرم جاسوسی درمحیط حقیقی ومجازی

استاد راهنما :

آقای دکترمهدی نقوی

استاد مشاور:

آقای دکتر نریمان فاخری

دانشجو:

سیده فهیمه طاهریان

تابستان ۱۳۹۰

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تقدیم به:

روح پدرم که اصلی‌ترین مشوقم به آموختن بود

و

دستان پرمهر مادر مهربانم

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

سپاسگزاری:

سرآغاز کلام سپاسی است ویژه محضر استاد گرانقدر جناب آقای دکتر مهدی نقوی که به عنوان استاد راهنما قبول زحمت نموده و اینجانب را در عین تواضع از گنجینه غنی معلومات خویش بهره مند ساختند.

همچنین از استاد بزرگوار مشاور، جناب آقای دکتر نریمان فاخری نیز کمال تشکر و تقدیر را دارم، بهره مندی از راهنمایی های علمی ایشان نقش مؤثری در تکمیل این پایان نامه داشته است.

و در آخر تقدیر و تشکر خاص خود را به مادر مهربان و خواهر عزیزم تقدیم می دارم که در همه حال یار و یاور و همراه و مشوقم در پایان دادن به این پایان نامه بوده اند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

چکیده

با تصویب قانون جرایم رایانه‌ای (۱۳۸۸)، مفاهیم وجرایم تازه‌ای در حقوق کیفری ایران خلق شد که هریک نیازمند بررسی‌های دقیق وکارشناسانه می‌باشد.دراین میان،جرم جاسوسی اگرچه یکی ازجرایم قدیمی و کلاسیک حقوق جزابه شمار می‌رود، ولی درپرتو پیشرفت‌های فناوری، نحوه ارتکاب آن دستخوش تغییراتی می‌شود که در قانون جرایم رایانه‌ای تحت عنوان جاسوسی رایانه‌ای، جرم انگاری شده است.

هرچند که وقوع جرم جاسوسی به هرطریقی امکان پذیراست بعنوان مثال می توان اطلاعات راازطریق تلفن به شخص حقوقی یا حقیقی دیگر اطلاع داد وازحیث ابزاربکار برده شده تفاوتی دروقوع جرم ندارد.

اما جرم جاسوسی رایانه ای تفاوتهایی دارد که به همین لحاظ ازجلدجرم کلاسیک بیرون آمده وشکل نوینی ازاین جرم راپدیدآورده است.

ازآنجاییکه اکثرکشورها به وضع قوانین خاص درخصوص جرائم رایانه ای پرداخته اند لزوم وضع این قوانین درکشور مانیزبه چشم می خوردبه خصوص اینکه جرم جاسوسی کلاسیک درکشورما بیشتر ناظربه مسائل نظامی وسیاسی وامنیتی است ومسائل بازرگانی واقتصادی درآن نادیده انگاشته شده درحالیکه دراکثر کشورها جرم جاسوسی اقتصادی نیز درنظر گرفته شده است.

جاسوسی سایبری، واقعیتی سیاسی- اجتماعی و فنی- حقوقی است که شناخت آن و یافتن جایگاهش در نظام حقوقی داخلی و بین‌المللی، وابسته به انجام مطالعات میان رشته‌ای است.

علاوه بر جرم انگاری، رویارویی با اعمال جاسوسی سایبری، نیازمند پیشگیری و اتخاذ تدابیر شکلی افتراقی وخاص است.

کلیدواژه: فضای سایبر،جرایم سایبری ،جاسوسی، جاسوسی اینترنتی ، جاسوسی کامپیوتری ، جاسوسی سنتی ، محیط حقیقی ، محیط مجازی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فهرست مطالب

عنوان صفحه

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقدمه

ورودبه اسرارمردم ازجمله اعمالی که موردمذمت ادیان الهی و اخلاق عمومی جوامع بوده،که متأسفانه با گسترش عرصه‌فن‌آوری اطلاعات وارتباطات[1] آفت‌های این پدیده شگرف نیزاز پیچیدگی‌های خود برخوردار است. مگر نه آن است که خواجه‌شیراز فرمود:

آنکسست اهل بشارت که اشارت داند
نکته هاهست بسی محرم اسرارکجاست
حافظ از باد خزان در چمن دهر مرنج
فکر معقول بفرما گل بی‌خار کجاست[2]

روزگاری فضای مجازی تنها منحصر به ذهن انسان بود. انسان از همان ابتدا در ذهن خود تخیلاتی داشت بیرون از مکان و متواری از زمان و در این فضا خود را از همه چیز رها می‌کرد.گاه به ماه می شتافت و گاه خورشید را به خانه اش می‌آورد. گاهی یاور همه مظلومان می‌شد و گاه بر سر خود تاج ثروت و مکنت می‌یافت. گاه خود را اندرون زیبایی‌ها می‌دید و گاه خود را سیراب از چشمه حیات جاودان می‌کرد.گاهی ریسمان محکم برگردن همه مشکلاتش می افکندوگاه قدرت شمارش پیروزی-هایش را از کف می داد؛ ولی همه اینها در فضای ذهنش بود. فضایی تنها که خود آن را مرور می کرد؛ نه می توانست ببیند و نه می‌توانست به دیگران نشان دهد.

فضای سایبر یا فضای مجازی که درگام اول با رادیووتلویزیون مطرح گردیدوسپس رایانه و مخابرات و از همه مهمتر اینترنت پایه‌هایش را بنا نهادند، دست کمی از ذهن آدمی ندارد. ولی این فضا هرچند همچون ذهن درگیر و دار زمان و مکان نیست و نمی توان در آن پا نهاد ولی می‌توان آن را دید و می‌توان به دیگران نیز نشان داد. این فضای خارق العاده تنها چهره دورنمای ذهنی دارد ولی در عمل با زندگی انسان عجین شده و معنای دیگری به آن داده است. دریک کلام با توجه به دارایی‌ها و

---

[1]. Information Technology

[2]. حافظ شیرازی، خواجه شمس الدین محمد، ۱۳۷۰، انتشارات حافظ نوین ، مصحح عبدالرحیم خلخالی، غزلیات ص۵۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ویژگی‌های فضای سایبر باید پذیرفت که جهان جدیدی در برابر جهانی که تا کنون می شناختیم و می شناساندیم، ظهور کرده است. جرم جاسوسی متعلق به این جهان پراز تارنما[1] است.

برای دانستن بستری که در آن جاسوسی اینترنتی شکل می‌گیرد و خیره سرانه رشد می‌یابد، ابتدا باید بسترارتکاب یا همان فضای سایبر و ارزش‌ها و هنجارهایی که در آن حاکم است را شناخت. شاید بتوان گفت که امنیت این فضا در برابر جاسوسی اینترنتی مهمترین ارزش به شمار می‌رود.

با رایانه ای شدن اموروتجهیزمراکز حساس به رایانه واینترنت ، احتمال وقوع جاسوسی به نسبت گذشته افزایش یافته است،بااین تفاوت که درفضای سایبر هرلحظه حجم عظیمی از اطلاعات مبادله می شوند وهرکاربراینترنتی که خلاقیت نفوذ درسیستم داشته باشد، می تواند جاسوسی کند .

جاسوس رایانه ای نه منحصراً از طرف دولت یا شرکتی خاص مأموربه جاسوسی است ونه لزوماً قصد ابتدایی اش نفوذ به سیستم رایانه ای حاوی اطلاعات حساس یا طبقه بندی شده است ، بلکه دربرخی موارد کسب اطلاع درفضای سایبر بدون سوء نیت علیه امنیت ملی وصرفاً دراثر کنجکاوی انجام می شود ، امادرهرحال می تواند عواقب سوئی علیه امنیت ملی داشته باشد.

امنیت ملی ، پیوند محکمی با مرزهای سرزمینی ورابطه دیرینه ای با وضعیت داخلی کشور دارد . اما درفضای سایبر که مرزهای مشخصی برای آن ترسیم نشده ودنیای کوچک است که همه دنیای بزرگ را بهم پیوند می دهد ، نمی توان از اقدامات سنتی برای پاسبانی امنیت ملی درفضای سایبر سود جست ، زیرا به قول جناب رنو، دادستان آمریکایی، درفضای سایبر یک هکر نیازی به گذرنامه ندارد ، زیرا درهیچ معبری بازرسی نمی شود .

ویژگی جهانی وبدون مرز بودن این فضا که مهمترین مشخصه اش نورافکنی درهر تاریک خانه بی خبر واسرارآمیز با توسل به فناوری تبادل اطلاعات است ، امنیت ملی رابا چالشی جدید وجدی مواجه کرده است . اگرچه این فضاراهکارهای نوینی مانند اطلاع رسانی ، رمزنگاری وخبرگیری رابرای تأمین امنیت ملی پیش رو نهاده است ، امادرمقابل تهدیداتی راوارد این حوزه کرده که ماهیتاً با نظایر فیزیکی متفاوت است .

---

[1]. وب سایت یاوب‌گاه (به انگلیسی: SiteWebیاWebsite) مجموعه‌ای از صفحات وب است که دارای یک دامنه اینترنتی یا زیردامنه اینترنتی مشترک‌اند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ارتکاب دوجرم مشهور جاسوسی رایانه ای واقدامات تروریستی سایبری ، اگر درحدی بود که رایانه برای تحقق آنهافقط نقش وسیله را داشت ،هردوراجرم سنتی فرض می کردیم وباقوانین وراهکارهای غیرسایبری موجود به پیشگیری ازآنها می شتافتیم .اما دراین دو جرم ، اولاً موضوع مستقیم، امنیت ملی نیست تا ادعا کنیم همان موضوع سنتی جرایم علیه امنیت است . موضوع جرم درجاسوسی محرمانگی داده وسیستم ها ودراقدامات تروریستی سایبری ،امنیت اطلاعات وشبکه است که به دلیل پیوند امنیت ملی با آنها ، از جاسوسی رایانه ای واقدامات تروریستی سایبری نهایتاً به عنوان جرایم علیه امنیت ملی یادمی کنیم .ثانیاً درهر دو جرم ، وسیله بابستر درهم آمیخته ودرزمانی بسیار کوتاه ودرمکان های متکثر مورد نظر مرتکب تحقق می یابد، کیفیتی که نمی توان درجرایم سنتی سراغ گرفت .

مع الوصف به زودی با دنیای کاملاً رایانه ای واینترنتی مواجه خواهیم شد که اگر برخورد مناسبی باآن نکنیم ، به پدیده ای مخوف وکنترل ناپذیر علیه همه چیز ، اعم از امنیت ملی ، اخلاق ، دین وروابط اجتماعی وخانوادگی تبدیل خواهد شد.

۱.بیان مسأله

در یک تعریف عام، جاسوسی رایانه‌ای یا سایبری عبارت است از « جستجوی غیرمجاز برای آزمودن وضعیت اهداف رایانه‌ای یا ارزیابی سیستم دفاعی رایانه یا رؤیت اطلاعات یا کپی برداری غیر قانونی از داده های فایل است.»[۱] جاسوسی سایبری شامل وارسی غیرمجازجهت کشف پیکربندی کامپیوتر مورد هدف، یا ارزیابی حفاظت‌های سیستمی آن یا مرور و کپی برداری غیرمجاز از فایل های داده‌ای است.

جاسوسی رایانه‌ای اساساً با جاسوسی سنتی تفاوتی ندارد و در هر دو، مرتکب در جستجوی اطلاعات است. حتی انگیزه های ارتکاب این دو گونه از جاسوسی نیز می تواند شبیه هم باشد.[۲] به همین دلیل

---

[۱] . CRS report for congress: **Botnets, Cybercrime, and Cyberterrorism**: Vulnerabilities and Policy issues for Congress, January ۲۰۰۸,P.۱۲

[۲] . برای دیدن برخی ار مهمترین انگیزه های جاسوسی ر.ک میرمحمد صادقی، حسین؛ جرایم علیه امنیت و آسایش عمومی، ص ۷۹ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

می توان گفت که در جاسوسی رایانه ای، رایانه تنها در حد وسیله است و به جهت الکترونیکی شدن اطلاعات و رایانه ای شدن فعالیت های امنیتی، اهمیت یافته است.

جاسوسی در معنای دقیق کلمه، همان تجسس وکنکاش است و عموماً مرحله ای پس ازحمله سایبری را در بر می گیرد. در واقع حمله کننده پس از دسترسی به رایانه، اقدام به جستجوی اطلاعات می نماید. این نوع حمله نیز مقدمه‌ای برای کسب اطلاعات و انجام حمله‌های سایبری مخرب و مختل-کننده است و با انجام آن محرمانگی سیستم و داده‌ها نقض می‌شود.جاسوسی سایبری بسیار خطرناک است؛ زیرا با در نظر گرفتن این که شکاف امنیتی پس از کشف متجاوز قابل اصلاح است، نقاط ضعف نا آشکار امنیتی این امکان را می دهد تا از آنها نه برای یک بار، بلکه برای مدت زمانی طولانی بهره برداری کند.

در عمل قانونگذاران کشورهاواز جمله ایران، جاسوسی را تنها به معنای تجسس و وارسی تلقی نکرده و قبل و بعد از این رفتار را نیز لحاظ کرده‌اند. به سخن دیگر جاسوسی شامل **سه رفتار ورود به مواضع یا مکان حاوی اطلاعات طبقه‌بندی شده، تجسس و تحصیل اطلاعات و در نهایت افشاء یا ارایه اطلاعات است.** به جهت حساسیت اطلاعات طبقه‌بندی شده و ارتباط آنها با امنیت کشور، زمینه جاسوسی که همان ورود به مواضع یا مکان مربوطه است نیز جرم دانسته شده است.[1]

جاسوسی رایانه ای بر خلاف جاسوسی سنتی که جایگاه مبهمی در قانون مجازات اسلامی دارد، با شفافیت در ماده ۳ قانون جرایم رایانه ای(ماده ۷۳۱ قانون مجازات اسلامی) پیش بینی شده است. طبق این ماده«هرکس به طورغیرمجاز نسبت به داده‌های سری درحال انتقال یاذخیره‌شده درسامانه‌های رایانه‌ای یا مخابراتی یاحاملهای داده مرتکب اعمال ذکرشده درقانون شود،به مجازاتهای مقرر محکوم خواهدشد.»

جاسوسی رایانه ای در حقوق کیفری ایران در سه مرحله تحقق می یابد که هر سه مرحله به طور مجزّا جرم تلقی می شود. **مرحله نخست**، دسترسی به داده‌های سری یا تحصیل آنها یا شنود محتوای سری در حال انتقال که با جاسوسی سنتی از حیث ورود به مواضع ممنوعه که اطلاعات در آن واقع شده اند برابری می‌کند. مرحله نخست جاسوسی رایانه ای در واقع همان دسترسی غیرمجاز است و

---

[1]. بتول ، پاکزاد ،۱۳۸۸ ،**تروریسم سایبری** ، پایان نامه دکتری حقوق کیفری وجرم شناسی ، دانشگاه شهید بهشتی ، تهران ، ص ۱۸۲ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

به لحاظ رفتاری با هم تفاوتی ندارند ولی از جهت قصد مرتکب، در دسترسی غیرمجاز مرتکب صرفاً در صدد نقض تدابیر امنیتی و ورود به سیستم است در حالی که در جاسوسی، مرتکب به قصد به دست آوردن اطلاعات به سیستم رایانه ای دیگری رخنه می کند. از این رو ماده ۴ قانون جرایم رایانه ای، با تکرار ماده یک این قانون که درباره دسترسی غیرمجاز است، تنها موضوع جرم را تغییر داده است. در ماده ۴، موضوع جرم، داده های سری است.

مرحله دوم ، در دسترس قراردادن داده‌های سری برای اشخاص فاقد صلاحیت و **مرحله سوم** که مشابه با مرحله دوم بوده ولی متضمن اقدام خطرناک تری است افشایا در دسترس قرار دادن داده‌های سری برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها است. بدیهی است که درجاسوسی، موضوع جرم حالتی کاملاً امنیتی دارد و آنچه که ماده۳ قانون جرایم رایانه ای پیش بینی کرده، جاسوسی سیاسی است زیرا طبق تبصره۱ ماده۳ داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

در کنار این نوع جاسوسی باید ازجاسوسی تجاری، صنعتی و اقتصادی نیز یاد کرد که می تواند مورد توجه تروریست ها قرار بگیرد. از این رو برخی کشورها، جاسوسی صنعتی که متضمن افشای اسرارتجاری و صنعتی است را، مقوله ای امنیتی می‌دانند؛ برای نمونه، قانون جاسوسی اقتصادی ۱۹۹۶ ایالات متحده، ربودن، شروع به ربودن و تبانی برای ربودن اطلاعات را جاسوسی اقتصادی دانسته است.[۱] البته این قانون شرط قصد رساندن منفعت به یک عامل بیگانه را نیز ذکر کرده که این امر جاسوسی صنعتی را به جاسوسی سیاسی نزدیک می کند.

ماده ۵ قانون جرایم رایانه‌ای نیز به تقلیداز قانون مجازات اسلامی(ماده ۵۰۶)، رفتارهای غیرعمدی مأمورین مربوطه که منجر به تخلیه اطلاعاتی می شود را نیزجرم دانسته است. طبق این ماده چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده۳ این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آنها قرار گرفته است براثربی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حاملهای داده یا سامانه‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای

---

[۱]. Ryan,Robin.D; **The criminalization of trade secret theft under the Economic Espionage Act OF ۱۹۹۶: An evaluation of United States v Hsu**, ۴۰ F. SUPP. ۲D ۶۲۳; University of Dayton law review, volume ۲۵, ۱۹۹۹-۲۰۰۰, p. ۲۴۴

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهندشد.

بررسی مقوله جاسوسی سایبری به عنوان شکل نوین از جاسوسی ،نیازجامعه دانشگاهی و نهادهای تصمیم‌گیر است تا از طریق آن با پدیده‌های جدید روز که در دیگر نقاط جهان طرح گردیده آشنا گردند. همین آشنایی نه تنها محققان و دست اندرکاران قانونی، قضایی و اجرایی ما را به قافله تحقیقات جدید، نزدیک می کند؛ بلکه راهی است برای درک میزان خطری که می تواند جاسوسی سایبری برای جامعه اطلاعاتی ایجاد کند و درک راه هایی که از همین الان باید به فکر پیمودن آنها بود.

۲. سؤالات و فرضیات

پیرامون جرم جاسوسی اینترنتی ومقایسه آن با جرم جاسوسی سنتی سؤالات بسیاری مطرح است و اگر این دسته از جرایم از نگاه‌های متفاوت مانند جنبه‌های حقوقی، جرم‌شناسی و سیاسی بررسی گردند، تعداد سؤالات عدیده و متنوع خواهند بود. اما سؤالاتی که در این تحقیق در پی پاسخ به آنها هستیم در رده سؤالات فرضیه بردار هستند تا بتوان در پرتو آنها سخن ازپایان نامه گفت و درنهایت از آنها دفاع کرد یا بر پایه دلایل قانع کننده ای آنها را رد نمود. سؤالات اصلی تحقیق حاضر عبارتند از:

۱-آیا باتوجه به ویژگی‌های فضای سایبر پدیده ای به نام جاسوسی سایبری وجوددارد؟

۲- درحقوق کیفری، جاسوسی سایبری چه ماهیتی دارد؟

۳- در سیاست تقنینی ایران جاسوسی سایبری وسنتی چه جایگاهی دارند؟

۴- آیاسیاست جنایی درررویارویی با جرم جاسوسی نیازمند اتخاذتدابیر کیفری پیشگیرانه خاصی است؟

فرضیه‌های تحقیق به شکل خبری و در قالب پاسخ به سؤالات فوق به شرح زیر است:

۱- هم ازجهت رخ داده‌های عینی وهم ازحیث ضوابط هنجاری و مقرره های پیش بینی شده، جاسوسی سایبری واقعیت وجودی دارد.

۲- جاسوسی سایبری ماهیتاً گونه ای جدا از مصادیق سنتی جاسوسی است.

۳- سیاست تقنینی ایران، از جهت محتوا و ویژگی های انطباقی، جرم جاسوسی سایبری وسنتی را پذیرفته و پیش بینی کرده است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۴- رویارویی با جاسوسی سایبری نیازمند اتخاذ تدابیری افتراقی است.

۳.روش تحقیق

با توجه به ماهیت و گستره ی موضوعی طرح بحث روش تحقیق تحلیلی توصیفی و در مواردی تطبیقی است.

۴. ضرورت تحقیق

ضرورت تحقیق امری است مرتبط با مقتضیات زمانی و مکانی. از حیث مقتضیات زمانی باید گفت ضرورت تحقیق برپایه یکی ازسه زمان گذشته، حال وآینده متجلی می‌شود. از حیث گذشته، ضرورت تحقیق ازنقطه نظرتاریخی دیده می شود تاتجربه والگویی برای آینده باشد؛بررسی تاریخی موضوعات حقوقی معمولاً به صورت تبعی است و در کنار بررسی حال این موضوعات صورت می گیرد مگر اینکه کلاً چهره ی تاریخی به خود بگیرد مانند بررسی محاکم کیفری پیش از دوره مشروطه یا تفحص درباره قوانین کیفری دوره هخامنشیان.

از جهت حال، ضرورت تحقیق به جهت مشکلات، چالش‌ها، نیازها و ابعاد موضوعی است که در جامعه حضور دارد. نسبت به یک موضوع حقوقی عموماً، تحقیق و پژوهش ازنگاه زمان حاضر بررسی می‌شود؛ برای نمونه، تحقیق پیرامون یک جرم یا یک نهاد کیفری یا یک مقوله جرم شناختی از آن جهت ضرورت دارد که مقتضیات کنونی جامعه آن را ایجاب کرده است.

از جهت آینده، ضرورت تحقیق از آن رو به چشم می‌آید که پدیده‌ای نوظهور دغدغه آینده ما شود. این قبیل موضوعات در دنیایی که سراسر بر فناوری و صنعت مبتنی است کاملاً بدیهی می باشد. در واقع حقوق کیفری امروزه نه تنها باید نگران گذشته و حالش باشد، بلکه باید به آینده نیز نگاهی عمیق داشته باشد. ضرورت انجام تحقیق در رابطه با جاسوسی سایبری دست کم در ایران از منظر آینده نگری توجیه می‌شود.

۵. اهداف تحقیق

مهمترین هدف در نگارش این پایان نامه، هشدار درباره شکل گیری و رسوخِ خیره کننده یک پدیده ویرانگر سایبری است. مقابله در برابر تهدید سهمگین جاسوسی در فضای سایبر در جامعه ای که روز به روز رایانه ای و اطلاعاتی می شود، جز با شناسایی درست و کامل آن امکانپذیر نیست. پس

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

هدف هشدار دادن برای پیشگیری از جاسوسی سایبری سبب می‌گردد تا از همین الان دست به تحقیقاتی گسترده در این زمینه زد.

هدف هشداردهی متوجه قانونگذارونهادهای مربوطه است تابابهره‌گیری ازتحقیقات دانشگاهی، مقررات وتدابیر شایسته اتخاذ کند. درکنار این هدف عمده اهداف دیگری نیز انگیزه نگارش این پایان نامه بوده اندکه عبارتنداز: تهیه یک مجموعه تحقیقی جامع و درخورتوجه جهت استفاده پژوهشگران و دانشگاهیان، فراهم کردن زمینه بررسی موضوعات بسیار جدید در حقوق کیفری ایران، بیان نواقص حقوق کیفری در مبارزه با این پدیده.

۶. سابقه تحقیق

تحقیق ونگارش پایان نامه پیرامون جرایم رایانه ای دارای سابقه‌ای بیشتر ازیک دهه است.اگرچه درخصوص جاسوسی سنتی مقالاتی نوشته شده همچنین پایان نامه هایی درخصوص جرایم سایبری به رشته تحریردرآمده است لیکن ازآنجا که درحوزه جرایم سایبردربستردانشگاهی امروزی یکی از موضوعاتی که همواره ناب و بی‌سابقه است موضوعاتی است که در حوزه فناوری اطلاعات و فناوری‌های نوین قرار دارد. در مجموع جاسوسی سایبر به جهت به روزبودن حوزه فناوری جدید و بکر می نماید.

۷. ساختار تحقیق

این تحقیق شامل کلیات ،۳ فصل وهر فصل شامل چندین بخش ودرصورت نیاز بندهای متعدد وقسمت نتیجه گیری می باشد .

درقسمت کلیات به بیان مسأله ، سؤالات وفرضیات ، روش تحقیق ، ضرورت تحقیق ، اهداف تحقیق و سابقه تحقیق پرداخته شده است . فصل اول که شامل ۴ بخش می باشد به تعریف جاسوسی وجرایم سایبری وویژگیها وسابقه تاریخی جرایم سایبری ازجمله جرم جاسوسی پرداخته شده است . درفصل دوم که شامل ۷ بخش می باشد به شناخت جرم جاسوسی سایبری وسنتی ،شیوه جاسوسی ،مراحل جاسوسی ،مصادیق جرم جاسوسی ،ارکان مرتبط به جاسوسی رایانه ای وتطبیق جرم جاسوسی کلاسیک وسایبری پرداخته شده ودرفصل سوم که شامل ۶ بخش می باشد به راه های

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

پیشگیری از جرایم سایبری،مشکلات تعقیب ورسیدگی جرایم رایانه ای ،ادله اثبات دعاوی رایانه ای، صلاحیت قضایی درمحیط مجازی ودرآخر به بررسی سیاست جنایی درایران پرداخته شده است .

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل اول

ویژگیها و تحولات جرایم سایبری و جاسوسی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بخش اول : جاسوسی

۱-۱-۱ تعریف لغوی جاسوسی

ممکن است تصورشود که معناومفهوم جاسوسی به سبب روشن بودن آن، نیازی به بررسی وبیان نداشته باشد لکن باتوجه به معانی مختلفی که این واژه داردبهترین معناعبارت است از: کنجکاوی کردن، بررسی کردن،خبرجستن ازامورمردم، اموری که مردم می خواهند پنهان بماند.[۱]

در مورد لغت جاسوسی در فرهنگ معین اینگونه بیان شده «جاسوس آن که اخبار و اطلاعات کسی یا مؤسسه‌ای و یا کشوری را مخفیانه گردآورد و به شخص یا مؤسسه و یا کشوری دهد.»[۲]

۱-۱-۲تعریف فقهی جاسوسی

اکثرفقهای عظام جاسوسی راتعریف نکرده اندوممکن است این امربه سبب روشن بودن معنای جاسوسی از دیدگاه آنان بوده باشد ، درابواب فقهی نیز بابی رابه این بحث اختصاص نداده اند، بلکه درجاهای مختلف به طورپراکنده وگذرا از جاسوسی سخن به میان آمده است . درکتب فقه برای این منظور غالباً ازتعبیر عین وعیون استفاده شده است .[۳]

۱-۱-۳ تعریف جاسوسی ازنظرحقوق بین الملل

به طورکلی درحقوق بین الملل سعی شده قوانینی که وضع می گردد باعث ایجاد وحدت گردد . مثلاً درموردجاسوسی تعریفی ارائه شود که به لحاظ رعایت حقوق افراد جامعه وضمانت آزادی های فردی ، دولت ها مجازنباشندکه عملی راجاسوسی تلقی نموده ومرتکب راتعقیب نمایند.ماده ۱۲ قطعنامه بروکسل ۱۸۷۴ می گوید :«جاسوس کسی است که به طور مخفیانه وبا وسایل وبهانه های مجهول اطلاعات راجمع آوری یابرای تحصیل اطلاعات درنقاط اشغال شده بوسیله نیروی دشمن باقصداین که آن هارابه طرف مقابل تسلیم نماید ، تجسس می کند.»

---

[۱] .محمدقریب، تبیین الغات لتبیان الآیات **یا فرهنگ لغات قرآن** ، ج۱، ص۲۷۴و۲۷۵

[۲] .معین، محمد، ۱۳۸۶ ،**فرهنگ معین**،یک جلدی فارسی، انتشارات زرین، ص۴۹۹

[۳] .ساریخانی، عادل، ۱۳۷۸، **جاسوسی وخیانت به کشور**،مرکز انتشارات دفتر تبلیغات اسلامی، ص۳۰ ص۳۱

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ماده ۲۹ آیین نامه ضمیمه قرارداد لاهه مورخه ۱۸ اکتبر۱۹۰۷ مقرر می کند : « کسی رانمی توان جاسوس دانست مگر اینکه به طورمخفیانه یابه بهانه های مجهول به نفع یکی ازمتخاصمین درصدد تحصیل اطلاعات یاجمع آوری اشیائی برآید.»[۱]

۱-۱-۴تعریف قانونی جاسوسی

قانون گذارنیز درهیچ یک از نصوص قانونی ، جرم جاسوسی راتعریف نکرده وتنها دربرخی ازمواد قانونی به کلمه جاسوسی وجرایم مرتبط باآن اشاره نموده است .

اینک باتوجه به معنا ومفهوم لغوی جاسوسی وباتوجه به طبع وماهیت عمل مذکور وبا استناد به مواد قانونی درتعریف جاسوسی می توان گفت : « جاسوسی به عمل شخصی گفته می شود که با عناوین غیرواقعی ومتقلبانه ، اقدام به کسب اطلاعات یا نقشه ها یا مدارک واسناد مخفی ومحرمانه مربوط به اسرارنظامی ، اقتصادی ، سیاسی و تسلیم آنها به کشور بیگانه نماید.»[۲]

بخش دوم : فضای سایبر

خلاقیت انسان ، فضای سایبر رابه ما هدیه کرده است ، فضایی که منافع وقابلیت های بسیاری دارد.اما هدایای بزرگ بهای گزافی نیز دارند . پیش از اینکه فضای سایبر به عنوان یک فناوری ظاهر شود، تعدادی ازفلاسفه درارتباط با امکان وجود «حقیقت مجازی»[۳] اظهارنظرکرده بودند.برای نمونه، افلاطون درکتاب جمهوریت خود به تمثیل غار می پردازد ومی گوید « آنچه حقیقت واقعی است دربیرون غار است وماسایه های آن بردیوار غار هستیم . او می گوید ، ما حقیقت مجازی هستیم واین یک فریب است که فکر می کنیم حقیقت واقعی هستیم.» درهرحال فضای سایبرعبارتی است که دردنیای اینترنتی ، رسانه وارتباطات بسیارشنیده می شود به نظر می رسد به کارگیری این اصطلاح دراین زمینه وبرای ارجاع به آن رنگ وبویی صرفاً فنی ومکانیکی داده باشد.ملاحظه دقیق تراین اصطلاح نشان می دهد که این واقعیت وجوه وجنبه های متنوعی از جمله خصلت های روان شناختی

---

[۱] .شامبیاتی، هوشنگ،۱۳۷۷،حقوق کیفری اقتصادی ،جلدسوم،چاپ آینده،ص ۱۰۱

[۲] .ساریخانی، عادل، پیشین ،ص۳۱

[۳].Virtual Reality

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

قابل توجهی دارد.[1] برای روش شدن بستری که جاسوسی مدرن درآن صورت می گیرد نیاز به تعریف سایبرومحیط سایبری داریم.

۱-۲-۱ معمای نامگذاری

جرم رایانه‌ای[2]،جرم سایبری[3]، جرم مجازی[4]، جرم شبکه[5]، جرم اینترنتی[6]، جرم دیجیتال[7]، جرم فناوری بالا[8]، جرم فناوری اطلاعات[9]، جرم الکترونیکی[10]، جرم برخط[11]، به راستی کدامیک ازاین عناوین در بردارنده معنای واقعی جرایم ارتکابی در فضای غیر مادی هستند؟ در نگاشته‌های مختلف حقوقدانان از اصطلاحات مختلفی برای توصیف موضوع جرم فضای غیر فیزیکی استفاده نموده‌اند.

البته در پاره‌ای موارد استدلال‌هایی نیزصورت گرفته که به توجیه عناوین انتخابی پرداخته‌اند. به عنوان مثال در خصوص جرم رایانه‌ای عده ای با این عنوان که چون جرایم این حوزه به وسیله رایانه‌ها ارتکاب می یابند، می بایست از آنها به جرایم رایانه‌ای تعبیر نمود. گروهی دیگر به این استدلال که جرایم این حوزه در شبکه ها اتفاق می افتد از آن به جرایم شبکه‌ای یاد نموده‌اند و برخی نیز با توجه به تعریف ارائه شده در خصوص فضای سایبر از این جرایم به طور عام به جرایم سایبری نام برده‌اند و حتی با توجه به نفوذ شبکه جهانی اینترنت برخی این دسته از جرایم را که با واسطه اینترنت به وقوع می پیوندند، جرایم اینترنتی نامیده‌اند.

با این همه بنابرآنچه که ازآن به فناوری اطلاعات و ارتباطات یاد شده است برخی از جرایم این حوزه به جرایم فناوری اطلاعات و ارتباطات و یا جرایم فناوری بالا یاد نموده‌اند.

---

[1].جلالی فراهانی ، امیر حسین ، ۱۳۸۸a،**حقوق فناوری اطلاعات وارتباطات** (مجموعه مقالات)، تهران، روزنامه رسمی جمهوری اسلامی ایران،ص ۱۲۳

[2].Computer crimes
[3].Cyber crime
[4]. Virtual crimes
[5]. Net crimes
[6]. Internet crimes
[7]. Digital crimes
[8]. High technology crimes
[9]. Information technology crimes
[10]. Electronic crimes
[11]. Online crimes

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تمامی این دیدگاه‌ها در جای خود معقول و پسندیده هستند، به گونه‌ای که می توان از آن استدلال‌ها در جای خودشان بهره جست، حال آنکه تمامی این دیدگاه‌ها یک ایراد واحد دارند و آن اینکه در هیچ یک جامعیت لحاظ نشده است. به دیگر سخن هر یک از ظن خویش این دسته از جرایم را مورد بررسی قرار داده‌اند در حالی که کلیت جرایم ارتکابی در فضای غیر مادی با آنچه که در این تعاریف از آن یاد شده است، جمع نمی شود و نمی توان تمامی این جرایم را زیر هر یک از این عناوین آورد.

با این اوصاف به نظر می رسد که بهترین عنوانی که هم جامعیت و هم مانعیت این دسته از جرایم را در خود ملحوظ داشته است، عنوان جرایم مجازی است. چرا که این عنوان هم جرایم رایانه‌ای صرف را در خود جای می دهد و هم توانایی تحت پوشش قرار دادن جرایم شبکه‌ای و مرتبط با فناوری را نیز در خود دارد. به گونه‌ای که تمامی این جرایم خود به گونه‌ای در فضای مجازی محقق می شوند و از این حیث، می توان آنها را جرایم مجازی دانست.[۱]

۱-۲-۲ تعاریف

تحلیل تاریخی آشکارمی سازدکه اصطلاحات«جرم رایانه‌ای»[۲]،«جرم مرتبط بارایانه»[۳]و«جرم سایبری»[۴] دیگر به سادگی به شکل نوینی ازجرم اشاره ندارند، بلکه پدیدهٔ گوناگون گسترده‌ای را دربر می گیرند که شامل انواع جدیدی از جرم همچنین جرم سنتی ارتکاب یافتهٔ مرتبط با داده ها وسیستم های رایانه‌ای می شوند.

به دلیل وجود این گوناگونی، تحلیل این پدیده مستلزم شناسایی یک مخرج مشترک و ویژگی‌های ماهوی جرایم می باشد. این موضوع نه تنها برای توجیه رفتارهای مجرمانهٔ مشابهی که طیفشان از هرزه نگاری تا تروریسم گسترده است، ضروری به شمار می آید، بلکه به منظور ایجاد چارچوبی برای اعتبارنظریهٔ عمومی این پدیده‌های جدید و همچنین اقداماتی (نظام) حقوقی ملی وسازوکارهای هماهنگی بین المللی، اساسی است.

---

[۱] .زرخ ،احسان ، ۱۳۸۸، پایان نامه کارشناسی ارشد حقوق کیفری وجرم شناسی، مؤسسه آموزش عالی شهیداشرفی اصفهانی ، ص۳۴ به بعد

[۲]. Computer crimes
[۳]. Computer related crimes
[۴]. Cyber crimes

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مخرج مشترک و ویژگی‌های ماهوی تمامی این جرایم را می توان در روابط آنها با سیستم های رایانه‌ای (کما اینکه در عبارات «جرم رایانه‌ای» و «جرم مرتبط با رایانه» صراحتاً آمده) یا شبکه‌های رایانه‌ای (با عبارت «جرم سایبری» مشخص شده) احراز کرد. جنبهٔ ماهوی اصلی این طبقه‌بندی، رابطهٔ میان جرم و داده‌های رایانه‌ای است یا در جایی که محتوا مدنظر است،رابطه میان جرم و اطلاعات رایانه‌ای مطرح می شود.

نتیجهٔ این رابطه (یعنی رابطه با اطلاعات رایانه‌ای)، طرح آشکار این مسأله است که برای دستیابی به یک پاسخ به منظور مواجهه با جرایم نامتجانس مذکور، ابتدا باید سؤال‌های اساسی راجع به انتقال پارادایمی را پاسخ گفت که در جامعهٔ اطلاعات رخ داده‌اند، از جمله انتقال محوری اشیای ملموس به اشیای ناملموس (به ویژه اطلاعات) و تأثیر این انتقال بر نظام‌های قانونی سنتی که از لحاظ نظری موجب توسعهٔ اساسی اشیای ملموس شده است. سایر جنبه‌های ماهوی این ارتباط میان جرم رایانه‌ای و سیستم‌ها و شبکه‌های رایانه‌ای، ماهیت جهانی اینترنت و توان فناوری اطلاعات است که هر دو آنها نسبت به جرایم ارتکابی از طریق اینترنت یا به مدد سیستم‌های رایانه‌ای، بنیادین به شمار می آیند.

به این ترتیب، عبارات «جرم رایانه‌ای» و «جرم سایبری» می توانند پدیده‌های متمایزگوناگونی را در برگیرند، اما پدیده‌هایی که یک مخرج مشترک دارند:

- جرم رایانه‌ای و جرم مرتبط با رایانه تمامی جرایم مرتبط با داده‌های رایانه‌ای را در بر می گیرد.
- جرم سایبری شامل تمامی جرایم رایانه‌ای (یعنی جرایم مرتبط با داده‌های رایانه‌ای) می‌شود که در شبکه‌های رایانه‌ای ارتکاب می یابند، یعنی جرایم مرتبط با فضای جهانی سایبر.

این دو طبقه نه تنها به جرایمی محدود می شوند که ویژگی‌های مشترکشان ذکر شد، بلکه تعریف کاربردی موسعی ارائه می‌دهند که برای مطالعه پدیده شناسی، جرم شناسی، امنیتی و قانونی، از جمله مطالعهٔ جنبه‌های ویژهٔ حقوق ماهوی، حقوق صلاحیت ضروری‌اند. آنها شامل تمامی پدیده‌های فوق می شوند، چه رایانه هدف یا ابزار ارتکاب باشد و چه جرم به ارزش‌های نوین مبتنی بر رایانه تعرض

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

کند.(مانند تمامیت سیستم‌های رایانه‌ای) یا ارزش‌های سنتی با شیوه‌های خاص رایانه‌ای مورد تهاجم قرار گیرند(مانند کلاهبرداری رایانه‌ای).[۱]

۱-۲-۳ تعریف واژه سایبروفضای سایبری

واژه سایبرازلغت یونانی keybermetes به معنای سکانداریا راهنما مشتق شده است ونخستین باراین اصطلاح سایبرنتیک توسط ریاضیدانی به نام نوربورت ونیر[۲] به کاربرده شده است سایبرنتیک علم مطالعه وکنترل مکانیزهادرسامانه های انسانی وماشینیِ ماشین ورایانه ها است.سایبر پیشوندی است برای توصیف یک شخص، یک شیء یک ایده ویایک فضا که مربوط به دنیای رایانه واطلاعات است[۳]. درطی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر به وجودآمده است که به تعدادی ازآنها اشاره می کنیم:مانندفضای سایبر[۴]،فرهنگ سایبر[۵]،شهروندسایبر[۶]،پول سایبر[۷].

درواقع واژه سایبر به همه محیطهایی اشاره دارد که اساس فعالیت آنها برمبنای پردازش است وطبق سامانه صفر ویک کارمی کنند.واژه رایانه ای بگونه ای دقیق وجامع نمی تواند گستردگی این محیط رانشان دهد زیرا بسیاری از ابزارووسایل امروزی با داده هایی کار می کنند که اساساً به آنها رایانه ای اطلاق نمی شود از این روعبارتهایی مانند جرمهای رایانه ای یا جرمهای اینترنتی[۸] نیزنمی توانند بگونه ای دقیق جرمهای ارتکابی مربوط به این حوزه راپوشش دهند،برای نمونه یک سامانه ضبط وپخش صوتی الکترونیکی رایانه نیست ولی بطور کلی درزیر مجموعه جهان سایبر قرارمی گیرد.

درفارسی واژه سایبر رابه مجازومجازی ترجمه کرده اند.این ترجمه گویای دقیق این واژه نیست مجاز دربرابرحقیقت به کارمی رود و درزبان انگلیسی معادل واژهvirtual است.ازسویی دیگرمحیط سایبرمحیطی است حقیقی وواقعی ونه دروغین ومجازی ، درواقع جهان سایبرهرچند به شکل مادی وملموس احساس شدنی نیست.اماهمانگونه که به اطلاعات ناشی از امری نمی توان عنوان مجازی

---

[۱] .جلالی فرهانی، امیرحسین ، پیشین،ص۳۵ و۳۶

[۲]. Norbert Wiener

[۳] .حسنوی، رضا، فرسایی، داریوش ، **فرهنگ تشریحی رایانه** ص۱۵۰و۱۵۱

[۴].Cyber space
[۵].yber culture
[۶].Cyber citizen
[۷].Cyber cash
[۸]. Internet crimes

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

داد به جهان سایبرنیزنمی توان مجازومجازی اطلاق کرد. باوجود این چون درزبان فارسی واژه ای که مترادف با این عبارت باشدیافت نشده است استفاده ازعبارت فضای مجازی[۱] وجرمهای جهان مجازی[۲] روبه گسترش است که رفته رفته جانشین عباراتی چون جرمهای رایانه ای وجرمهای اینترنتی می شود.

فضای سایبردرمعنا به مجموعه هایی از ارتباطات درونی انسانها ازطریق رایانه ووسایل مخابراتی بدون درنظرگرفتن جغرافیای فیزیکی گفته می شود.یک سامانه آنلاین[۳] نمونه ای ازفضای سایبراست که کاربران آن میتوانند ازطریق ایمیل با یکدیگر ارتباط برقرار کنند.برخلاف فضای واقعی درفضای سایبر نیاز به جابه جایی فیزیکی نیست وکلیه اعمال فقط ازطریق فشردن کلیدها یا حرکات ماوس صورت می گیرد . روند کاری یک کاربر رایانه در فضای سایبر دقیقاً نوع یکی شدن یا محوشدن در درون واقعیتی متفاوت یعنی واقعیتی مجازی که ورای قوانین وواقعیتهای ملموس است که کاربررایانه در هنگام کاردرفضای مجازی با آن یکی می شود.

از محیط سایبربه محیط فناوری اطلاعات (IT)[۴] یا محیط اطلاعات وارتباطات(ICT)[۵] نیز یاد شده است از این رو مشاهده می شود که برای نمونه به جرمهای محیط سایبر، جرمهای علیه فناوری اطلاعات نیز گفته اند.[۶]

۱-۲-۴تعریف جرم سایبری

ارائه تعریف دقیق به نحوه جامع و مانع مشکل به نظر می‌رسد و دلیل آن نیز جدید بودن ابعاد جرایم رایانه‌ای است. از این رو، مراجع قانونگذاری کشورهای مختلف هریک به فراخور نیازها و تهدیدات پیش‌رو، تعریف متفاوتی ازاین جرایم ارائه کرده‌اند. برای مثال در ایالات متحده آمریکا تعریف وسیعی از جرم رایانه‌ای به عمل آمده مبنی بر آنکه «هر اقدام غیرقانونی که با یک رایانه یا به کارگیری آن مرتبط باشد را جرم رایانه‌ای می‌گویند. یا هر اقدامی‌که به هر ترتیب با رایانه مرتبط بوده و موجب

---

۱. cyber space
۲. cyber crime
۳. ارتباط شبکه ای بارایانه دیگرOnline.
۴. Informatin Technology
۵. Information Cimmunication Technology
۶. زندی ، محمد، ۱۳۸۸، **تحقیقات مقدماتی درجرایم سایبری** ، تهران ، انتشارات جنگل ، جاودانه ص۳۹و۴۰

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ایجاد خسارت به بزه دیده شود و مرتکب از این طریق منافعی را تحصیل کند، جرم محسوب می‌شود.»[۱]

در ایران، نه در قانون تجارت الکترونیک و نه در قانون جدید مصوب جرایم رایانه‌ای هیچ تعریفی از این مفهوم ارائه نشده است. شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرایم رایانه‌ای وجود دارد. اما می‌توان به عنوان نمونه تعریف زیر را ارائه کرد:

«آن دسته از جرایمی‌که با سوءاستفاده از یک سیستم رایانه‌ای برخلاف قانون ارتکاب می‌یابد جرایم رایانه‌ای نام دارد. البته این دسته از جرایم را می توان شامل جرایم سنتی که به واسطه رایانه (هرچند با تغییراتی در ماهیت) صورت می گیرد، از قبیل کلاهبرداری و سرقت ؛ و نیز جرایم نوظهوری که با تولدرایانه به دنیا پاگذاشته اند، چون ایجاد اختلال در داده ها، جرایم مجازی[۲] و... دانست.»[۳]

لازم به ذکر است که یکی از ابعاد مهم تعریف جرم محدودیت مکان است اما رایانه به دلیل غلبه بر محدودیت مکان فیزیکی وفضای مجازی و هم به دلیل ویژگی فرامکانی بودن ،ارائه ی تعریف مشخص از جرم رایانه ای را با سختی مواجه کرده است.

با این وصف مهمترین و اولین تعریف ارائه شده در مورد جرایم رایانه ای،تعریف سازمان همیاری اقتصادی و توسعه(OECD) [۴]در مورد سه گروه ازجرایم رایانه ای است:

۱)جرایم اقتصادی مربوط به رایانه (کلاهبرداری رایانه ای،جاسوسی رایانه ای و خرابکاری رایانه ای).

۲)جرایم مربوط به رایانه علیه حقوق فردی،خصوصاً علیه حریم خصوصی شهروندان.

۳)جرایم مربوط به رایانه علیه منافع جمعی مثل جرایم علیه امنیت ملی،علیه کنترل جریان فرامرزی داده ها،علیه تمامیت رویه های رایانه ای و شبکه های داده ای–ارتباطی یا علیه مشروعیت دموکراتیک مصوبات پارلمان درمورد رایانه.[۵]

---

[۱] .عمیدی، مهدی، « مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه وحقوق کیفری ایران »، تهران، دانشگاه آزاد اسلامی‌واحد تهران مرکز، پایان نامه کارشناسی ارشد حقوق جزا وجرم شناسی، ۱۳۸۷

[۲]. Cyber Crime

[۳] .طارمی،محمد حسین، ۱۳۸۷ ،گذری بر جرایم رایانه‌ای ،در هفته نامه پگاه حوزه شماره ۲۳۳

[۴]. Organization Of Economic Co-Operation And Development

[۵] .اولریش ، زیبر ،۱۳۸۳،**جرایم رایانه ای**،ترجمه ی محمد علی نوری و دیگران، تهران،انتشارات گنج دانش

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۱-۲-۵ تعریف جاسوسی سایبری

جاسوسی عبارت است از جمع آوری مخفیانه وغیرقانونی اطلاعات مرتبط با امور سیاسی ، نظامی یک کشور یا اطلاعات متعلق به مردم آن . به این تعریف باید ویژگی « حساس بودن اطلاعات» رانیز اضافه کرد . تعیین مصادیق جاسوسی و مراحل آن ، همواره مناقشه آمیز بوده و قانونگذاران با هدف تضمین امنیت ملی ، بطور شفاف ، ماهیت، اقسام ومراحل آن را تعریف نکرده اند.حتی قانونگذارایران در قانون مجازات اسلامی، عنوان مجرمانه مستقلی به نام جاسوسی پیش بینی نکرده ورفتارهای مجرمانه مشابه رابه آن ارجاع داده است.فارغ ازگسترگی مفهوم ومصادیق جاسوسی ، غالباً قانونگذاران جرم راصرفاً به دو رفتار توأمان جمع آوری اطلاعات وارائه آن به دشمن منحصر ندانسته ودریافته اند که مراحل چندگانه تحقق جاسوسی دلیلی برمستمر دانستن آن نمی شود، به عبارت دیگر ، مراحل سه گانه جاسوسی که عبارتنداز شناسایی وتعیین اطلاعات مورد نیاز ، جمع آوری اطلاعات وبالآخره تحلیل اطلاعات جمع آوری شده که به هدف اصلی جاسوسی ، یعنی ارائه اطلاعات به مسؤولان یک دولت یا شرکت بیگانه جهت اتخاذتصمیم منجر می شود، موجب نشده تا قانونگذاران درجرم انگاری این جرم منتظر حصول نتیجه شوند وبدون توجه به این مراحل ، هررفتار فیزیکی مرتبط با جاسوسی راجرم مستقل تلقی کرده اند.[۱]

ممکن است دو برداشت از معنای جاسوسی رایانه‌ای به ذهن متبادر شود. اوّل ممکن است این برداشت شود که جاسوسی رایانه ای جاسوسی است که به وسیله رایانه انجام می‌شود یعنی جاسوسی رایانه‌ای یکی از انواع جاسوسی کلاسیک است و به بیان دیگر هر گاه جاسوسی کلاسیک به وسیله رایانه‌ای محقق شود آن را جاسوسی رایانه ای میگویند،دوّم ممکن است این برداشت شود جاسوسی رایانه ای جاسوسی است جدای جاسوسی کلاسیک و جرمی است مستقل از آن که در فضای سایبر(مجازی)رایانه صورت می‌گیرد و کاملا ً از جاسوسی کلاسیک مستقل و جدا است که برداشت دوم صحیح‌تر به نظر می‌رسد زیرا جاسوسی به دو دسته کلی جاسوسی رایانه ای و جاسوسی کلاسیک تقسیم می‌شود و جاسوسی کلاسیک به وسیله رایانه هم (برداشت اول از جاسوسی رایانه‌ای)

---

[۱] .حسن بیگی ، ابراهیم ،۱۳۸۴، **حقوق وامنیت درفضای سایبر**، تهران ، مؤسسه فرهنگی مطالعات وتحقیقاتی بین المللی ابرار

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

جزئی از جاسوسی کلاسیک است و یکی از مصادیق و راههای انجام جاسوسی کلاسیک است و با جاسوسی رایانه‌ای مد نظر ما فرق دارد ، جاسوسی رایانه‌ای اینگونه تعریف می‌شود:

« کسب غیرمجاز اطلاعات دارای ارزش اطلاعاتی ازهر طریقی اعم از نفوذ کردن، استراق سمع کردن در محیط رایانه به قصد ضربه زدن به فرد بزه دیده.»

در مورد این تعریف نکاتی را باید بیان کرد: ۱- منظور از اطلاعات اعم است از اطلاعات مالی و غیرمالی و اطلاعات نوشتاری، غیر نوشتاری و سمعی و بصری و به طور کل هر نوع اطلاعاتی.

۲- « دارای ارزش اطلاعاتی» منظور آن اطلاعات دارای ارزش باشد و به اصطلاح اخبار و خبرهای سوخته نباشد چرا که ممکن است فردی به اطلاعاتی غیرمجاز دسترسی یابد که ارزش اطلاعاتی ندارد که از شمول جرم جاسوسی رایانه‌ای خارج می‌شود.

۳- «از هر طریقی» منظور از هر روشی که فرد اطلاعات دارای ارزش اطلاعاتی را در محیط رایانه به قصد ضربه زدن به فرد بزه دیده کسب کند را باید شامل این جرم دانست .

۴- « در محیط رایانه» اعم است از هر محیط رایانه‌ای چه رایانه‌های بزرگ چه رایانه‌های کیفی و چه شبکه‌های رایانه‌ای مدنظر است.[1]

بخش سوم : طبقه بندی وویژگیهای جرایم سایبری

مسأله مهمی که باید بدان پرداخت این است که اصولاً انواع جرایم مجازی کدامند وتحت چه عنوانی یانامی بایدبدان رسیدگی کرد.آیااین جرائم جزءجرائم عمومی (کلاسیک)قرارمی گیرند ویاخیرجرائمی هستند جدیدکه بایدعنوانی خاص برآنها نهاد ویاهردو این موارد راشامل می شود.

اهمیت موضوع زمانی برای مامشخص می شود که بدانیم که تازمانیکه جرمی شناخته نشود ومشخص نشود چه عنوانی دارد وجزء کدام دسته از جرایم است نمی توان مجازاتی برای آن درنظر گرفت.

[1] .حسن بیگی ، ابراهیم ، پیشین.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۱-۳-۱ انواع جرایم سایبری

با رویکردی جامع می‌توان جرایم مجازی را شامل موارد زیر دانست:

۱. جرایم کلاسیک با توصیف مجازی، مانند کلاهبرداری مجازی و جعل مجازی؛

۲. جرایم علیه محتوا، مانند انواع پرنوگرافی و افترا؛

۳. جرایم صرف فناوری اطلاعات، مثل جرایم دستیابی؛

۴. جرایم مخابراتی، مانند شنود جرایم مربوط به تلفن‌های همراه سیستم‌های ماهواره‌ای؛

۵. جرایم با مبنای غیرجزایی، همچون: نقض کپی رایت،جرایم بانکداری الکترونیک وتجارت الکترونیک.

اما جرایم رایانه‌ای، بخشی از جرایم مجازی هستند که در آنها رایانه وسیله، هدف و یا واسطه ارتکاب جرم است و گاهی علیه اموال، گاهی علیه تمامیت معنوی اشخاص و بعضاً علیه نرم‌افزار، داده و سخت‌افزار رایانه وگاهی نیز بر ضدآسایش و امنیت عمومی است. از این منظر، جرایم رایانه‌ای به سه گروه عمده تقسیم می‌شوند:

اوّل، جرایم اقتصادی مرتبط با رایانه، شامل: کلاهبرداری، جاسوسی، جعل، سرقت خدمات، دستیابی غیر مجاز و جرایم شغلی مرسوم از طریق داده‌پردازی.

دوّم، جرایم علیه حقوق شخصی، شامل: افترا، توهین، افشای اسرار و نقض کپی‌رایت.

سوّم، جرایم اجتماعی و ملّی، همچون: جرایم علیه امنیت ملی، کنترل جریان فرامرزی داده‌ها و تمامیت شبکه‌های ارتباطی داده‌ها.[۱]

۱-۳-۲ بیان ویژگی‌های مجرمین مجازی

در رابطه با مجرمین فضای مجازی دیدگاه‌های متفاوت وگاه متعارضی از سوی حقوقدانان کیفری ارائه شده است که درجای خود محل تردید و تأمل هستند. مجموعه این دیدگاه‌ها را می توان در هفت دسته طبقه بندی نمود که در ذیل بدان ها اشاره می شود. هر چند که این دسته بندی ها بنابر آنچه که در ادامه بحث قرار گرفته به طور مطلق قابل پذیرش نیستند.[۲]

---

[۱] . پروگلر، یوسف ، **فصلنامه ره آورد نور**، شماره ۱۱، تابستان ۱۳۸۴، ص ۱۴ تا۱۷

[۲] .زرخ ،احسان، پیشین، ص ۸۵

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

الف) هوشمندی ذهنی مجرمین مجازی

همانند بسیاری از نگرش‌های غلط، این تفکر نیزدرگذشته که مصادیق صحیح آن به مراتب بیش از امروز بوده ، رواج داشته است . در ابتدا افراد معدودی بودند که به رایانه‌های بسیاربزرگ ، گران دسترسی داشتند. کار بارایانه‌های نخستین مستلزم دانش بالای ریاضی بود.پشت این رایانه ها هرگز کاربرانی به مفهوم امروزین قرارنمی گرفتند و تنها کسانی می توانستند ازآنها استفاده کنند که برنامه نویس ماهری بودند. برنامه نویسی هم یک فرآیند مشقت باربود که به صبر و اراده‌ای پولادین نیاز داشت تا در مدت زمانی طولانی کد گذاری‌های مربوطه انجام شود.در آن زمان به سختی می شد راجع به فعالان این حوزه مطلبی در صفحات اجتماعی روزنامه ها پیدا کرد. هنگامی که این افراد پس از آن فعالیت بسیار خسته کننده شب، هنگامی که به دنیای خارج پا می گذاشتند، هیچ حرفی برای گفتن به افراد جامعه نداشتند. تمام زندگی آنها در میان انبوه لامپ‌های خلاء و نسخه‌های چاپی صفر و یک سپری می شد. یعنی چیزهایی که هیچ کس نه می توانست و نه می خواست به آنها توجه کند.

اکنون سیستم‌های رایانه‌ای تقریباً در همه جا یافت می شوند. مهارت‌های مورد نیاز جهت بهره برداری‌های ناشایست از این سیستم‌ها به مراتب نسبت به گذشته از پیچیدگی بسیار کمتری برخوردار شده است. البته اکنون از آن گونه متخصصان اولیه نیز یافت می شود، اما بسیاری از مجرمان مجازی امروزین، به ویژه حقه بازان رایانه‌ای و آنهایی که ارضای تمایلات جنسی خود را در این فضا جستجو می کنند، انسان‌هایی مؤدب و جذاب هستند ومهارت‌های اجتماعی رابه خوبی فرا گرفته‌اند.[1]

ب) برخورداری مجرمین مجازی از بهره هوشی و دانش فنی بسیار بالا

با توجه به توضیحاتی که داده شد،در می یابیم این نگرش نیز تنها در مورد متخصصین سیستم‌های اولیه رایانه‌ای صادق بوده است. امروزه دسترسی به فضای آن لاین[2] به آسانی یک کلیک کردن شده است. با اینکه بعضی جرایم مجازی، نظیر نگارش و نشر ویروس‌های جدید یا تهاجم به شبکه‌های فوق امنیتی همچنان مستلزم دانش فنی بالایی است، اما طیف وسیعی ازجرایم مجازی هستند که

---

[1] .زرخ ،احسان، پیشین، ص ۸۶

[2].Online

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

اشخاص عادی که بهره هوشی متوسط دارند و دانش فنی شان ناچیز است یا حتی از آن برخوردار نیستند نیز می توانند آنها را مرتکب شوند.

حقه بازی‌های مجازی را هر کسی که قادر به ارسال پست الکترونیک باشد یا بتواند از برنامه‌های گپ اینترنتی استفاده کند، می تواند مرتکب شود.سرقت داده نیز غالباً به سادگی یک کپی کردن است. حتی جرایمی که مستلزم تخصص فنی پیچیده هستند را هم هکرهای غیر حرفه‌ای می توانند مرتکب گردند. این افراد فقط از کدی که دیگران در راستای اهداف شوم خود نگارش کرده‌اند استفاده می کنند. صدها وب سایت و گروه خبری به هکرهایی که هیچ گونه دانش فنی در اختیارندارند، ابزارهای از پیش پیکربندی شده یا خود کاری ارائه می دهند که می توانند با استفاده از آنها سیستم‌های رایانه-ای را مورد تعرض قرار دهند.

ج)مجرمین مجازی مردان و معمولاً جوانان کمتر از ۲۰ سال

این نگرش نیز از آنجا ناشی می شود که دانش ریاضی به طور عام فناوری رایانه به طور خاص از همان ابتدا در انحصار مردان بوده است. هر چندآمارهای مجریان قانون نیز حاکی از این است که در تمامی جرایم، مردان بیش از زنان مستعد ارتکاب جرم هستند. با این حال، آمارهای اخیر حاکی از پر شدن این شکاف جنسیتی است. دراواخر دهه نود، ۲۲ درصد دستگیر شدگان را زنان تشکیل می دادند. این در حالی است که ۱۴ درصد جرایم خشن و ۲۹ درصد جرایم علیه اموال را زنان مرتکب شده‌اند.

البته این موضوع از این جهت نیز قابل تأمل است که از آنجا که جرایم را عمدتاً مردان تشکیل داده بودند، این نگرش به وجود آمده است. هر چند باید خاطر نشان کرد که این حوزه، نیز متحول شده است. هم اکنون زنان بسیاری در مناصب مدیریتی و اجرایی قرار گرفته‌اند که مستعد ارتکاب جرایم یقه سفید هستند و آمارهایی نیز حاکی از رشد ارتکاب این جرایم نزد آنان است.[1]

[1].نجفی ابرندآبادی ، علی حسین ، ۱۳۸۵،تقریرات جرم شناسی (امنیت خصوصی) دانشگاه علوم اسلامی رضوی ، سال تحصیلی ۸۲-۸۱

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

به این ترتیب، واقعیت این است که دیگر دانش رایانه در انحصار مردان نیست. آمارهای وزارت بازرگانی آمریکا نشان می دهد که ۲۸/۵ درصد برنامه نویسان را زنان تشکیل می دهند که البته درصد ناچیزی از آنها به دنبال بهره برداری نامشروع از مهارت خود هستند.

هر چند به هرحال ابزار ارتکاب طیف وسیعی از جرایم مجازی در اختیارشان قرار گرفته است بنابراین، این نکته مهم را نباید فراموش کرد که جرایم مجازی توسط هر جنسیت، نژاد و هر گروه سنی قابل ارتکاب است.

ه) پسران جوان دارای رایانه، مجرمین مجازی بالقوه

بی تردید هیچ کس با این واقعیت که اشخاص جوانی که سعی می کنند وب سایت‌ها را تخریب کنند یا به سیستم‌های رایانه‌ای دولتی نفوذ کنند، مجرم محسوب می شوند، مخالفتی ندارد و حتی همگان اذعان دارند که این معضل باید رفع شود. اما این مسأله هرگز به این معنا نیست که طیف عظیم جوانانی که از مهارت‌های رایانه‌ای برخوردارند، همگی از رایانه‌هایشان در راستای مقاصد نامشروع استفاده می کنند. اکثر آنها عمده فعالیت شبکه‌ای شان در پیاده کردن موسیقی یا نرم افزاری خلاصه می شود که از آن برای مصارف شخصی استفاده می کنند. هرچند این اقدام نیز خود می تواند جلوه مجرمانه به خود بگیرد. اما به هر حال، هیچگاه نمی توان چنین رنگ مجرمانه‌ای را به طیف عظیم کاربران شبکه‌ای زد.

و)مجرمین مجازی، مجرمین غیر واقعی

بسیاری از مجرمین مجازی این نگرش را ترویج کرده‌اندتاشایدازاین طریق بتوانند اقدامات خود را توجیه کنند.حتی اشخاصی که در دنیای فیزیکی اقدامات غیر قانونی را مرتکب می شوند، چنین تصویری نسبت به فضای مجازی ندارند و به همین دلیل، بسیار راحت تر دروغ می گویند، تقلب می کنند یا حتی مرتکب اعمال وقیحانه یا نفرت انگیز می شوند.

به همین دلیل، اکنون مطالعات بسیاری در خصوص روان شناسی جنایی مجازی[1] آغاز شده است تا از این طریق بهتر بتوان در خصوص رفتارهایی که در فضای مجازی بروز می یابند اظهار نظر کرد. به

[1].Virtual criminal py choiogy

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

عنوان مثال، مرکز مطالعات ارتباطات میان رایانه‌ای[1]، جلوه دوگانه غیر واقع گرایانه و ناشناس ماندن رفتارهای افراد که هویت متفاوتی به آنها در فضای مجازی بخشیده است را دردستورکار مطالعات خود قرار داده است.

فناوری هایی نظیر گپ آن لاین، سیاه چال‌های چند کاربره[2] و برنامه های واقعیت مجازی باعث شده‌اند برخی کاربران توانایی تفکیک دنیای واقعی از مجازی را از دست بدهند. بسیاری از کاربران اینترنت، به ویژه آنهایی که به تازگی به فضای آن لاین ملحق شده‌اند ، تصور می کنند اشخاص درمقابل آنها در آن سوی مودم در حکم یک برنامه رایانه‌ای هستندو حتی با آنها به مثابه یک بازی رایانه‌ای تعامل برقرار می کنند.

این افراد هویتی که در دنیای واقعی از خود بروز می دهند را در تعاملات آن لاین بکار نمی گیرند. زیرا تصور می کنند در آن سوی خط ارتباطی شبکه مجازی کسی آنها را نمی شناسد. از این رو، به خود اجازه می دهند هر گونه حقه و نیرنگی را در این تعاملات به کار برند. همچنین، از آنجا که این افراد می توانند در فضای آن لاین برای خود هویت دیگری تعریف کنند و حتی برخلاف دنیای فیزیکی به سرعت آن را تغییر دهند و هویت های دیگری با ویژگی‌های کاملاً متقلبانه را برای خود برگزینند، این بستر برای آنها فراهم می شود که به اقدامات متقلبانه آن لاین خود با خیال آسوده تر ادامه دهند.

به این ترتیب، این ایده که هیچ چیز در فضای آن لاین واقعیت ندارد، می تواند مروج یک واقعیت تلخ دیگر نیز باشد که هیچ کس در برابر اقدامات خود مسئول نیست. البته خود بستر فضای مجازی به مجرمین جرأت مضاعفی را اعطا کرده است. زیرا آنها برخلاف دنیای فیزیکی، بی آنکه نتایج شرم آوروتأسف بار جرایم خود را مشاهده کنند یا صدای فغان قربانیان خود را گوش کنند، با خیال راحت

[1].CMC
[2]. MUD (MUVE) Multiuser Virtual Environments

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

به ارتکاب جرایم می پردازند و به واقع می توان گفت تنها چیزی که مشاهده می کنند یک سری اعداد و ارقام و عبارات است که بر روی صفحه نمایشگر شان ظاهر شده است.[1]

ز) عدم استعمال خشونت توسط مجرمین مجازی

با توجه به توضیحاتی که در فوق داده شد، در می یابیم از آنجا که به فضای مجازی بیشتر به عنوان یک فضای مجازی یا حداقل دنیای متمایز و متفاوت از دنیای فیزیکی نگریسته می شود، نتیجه منطقی آن این است که هیچ یک از مصادیق جرایم مجازی از ماهیت خشن برخوردار نباشند. زیرا از فاصله دور ارتکاب می یابند و در نگاه اول این مسئله به ذهن متبادر نمی شود که قابلیت اتصاف به خشونت را داشته باشند.

قبول این واقعیت که بخش عمده‌ای از جرایم مجازی گزارش شده، کلاهبرداری، سرقت و دسترسی غیر مجاز هستند، اما نباید از یاد برد که گزارشات مکرری نیز در خصوص هرزه نگاری کودکان به ثبت رسیده که به طور کلی در زمره جرایم خشن یا بالقوه خشن قرار می گیرد. تعرضات هکرها نیز جرایم خشونت باری هستند که گزارش های بسیاری از خسارات آنها شده است.همچنین تعقیب ایذایی در فضای مجازی نیز یکی دیگر از مصادیق بارز خشونت در فضای مجازی[2] است. یا تروریسم مجازی[3] یکی از نمادهای بارز خشونت مجازی است که به طور جدی فضای مجازی و وابستگان به آن را مورد تهدید قرار می دهد.

ح) بررسی مجرمین مجازی در یک نیم رخ جرم شناسی

ممکن است بتوانیم برای اشخاصی که مرتکب جرایم مجازی خاصی می شوند، نیم رخ مشترکی تهیه کنیم، اما غیر ممکن است تمامی آنها رادریک نیم رخ به تصویرکشیم. درست مانندمتخلفین و مجرمین رانندگی که نه می توان از آنها یک نیم رخ تهیه کرد. یک راننده که به طور اتفاقی سریع رانندگی کرده است، احتمالاً با یک راننده که عادتاً مست است از شخصیت و انگیزه های متفاوتی برخورداراست و

---

[1].زرخ ،احسان، پیشین، ص ۸۹

[2].Cyber Stalking
[3].Cyber Terrorism

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

راننده‌ای که به شدت عصبانی است و از وسیله نقلیه مانند یک سلاح جهت از بین بردن عابران استفاده می کند نیز از شخصیت متفاوتی برخوردار است. به همین ترتیب، یک اوباش اینترنتی ویژگی‌های کاملاً متمایزی با یک تعقیب گر ایذایی مجازی دارد که او نیز به نوبه خود هیچ شباهتی با یک هکر ندارد.

این تمایزات زمانی نمود بیشتری پیدا می کند که ویژگی‌های روان شناختی، جامعه شناختی وانگیزه-های هر یک از مجرمین مجازی رانیز مد نظر قرار دهیم. به این ترتیب، ناگفته پیداست اگر بخواهیم بخشی از توده مجرمین مجازی را به تصویر کشیم، با طیف گسترده‌ای از ویژگی‌ها و خصائص متمایز مواجه خواهیم بود که برای درک دقیق تر آنها نیازمندطبقه بندی مشخص و دقیقی هستیم.[1]

۱-۳-۳ ویژگیهای جرایم سایبری

به دلیل طیف گسترده فعالیت های مجرمانه مرتبط با رایانه ، شناسایی ویژگی های مشترک میان تمامی آنها دشوار است . صرفنظر ازآن ، برخی ویژگی های اشتراکی هستند که از رابطه این اعمال مجرمانه با رایانه ها وشبکه های رایانه ای سربرآورده اند . به عبارت دیگر، ویژگیهای رایانه ها وشبکه های رایانه ای درویژگی های خاص جرم رایانه ای وجرم سایبری انعکاس یافته اند.

فضای سایبر به گونه ای است که یک دنیای مجازی را در کنار دنیای واقعی ما بوجود آورده است.این دنیای جدید به لحاظ ماهیت ناشی از فناوریهایی است که دائماً در حال توسعه و گسترش هستند و ویژگیهای خاص ومتمایز ازدنیای فیزیکی دارد که به همین لحاظ علاوه بر اینکه زندگی بشر وجوامع را متحول ساخته،چالشهاومشکلات جدیدی نیز پدید آورده است. بررسی این چالش‌ها و نیز مزایا و امکانات و در یک کلام دگرگونی منوط به این است که بدانیم فضای سایبر چه ویژگی‌هایی دارد؟ برخی از مهمترین ویژگیهای این دنیای جدید به شرح زیر است:

۱-۳-۳-۱ جهانی و بی مرز بودن

فرامرزی بودن ازویژگیهای مهم وچالش برانگیزاین فضااست. فضای سایبر و اینترنت فارغ از مرزهای جغرافیایی عمل می کند و محدود به چارچوب خطوطی که دولتمردان در طراحی نقشه های سیاسی

[1] .زرخ ،احسان، پیشین، ص ۸۹

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

رسم می کنند نیست.[1]در واقع در فضای سایبر، امکان ترسیم قلمرو حاکمیتی، همانند دنیای فیزیکی وجود ندارد.اینترنت بر پایه استانداردهای جهانی بازو بدون اینکه فرد یا نهاد خاصی مالک آن باشدبناشده است.«هیچ فرد،دولت یامؤسسه تجاری مالک آن نیست»[2] هرکسی می‌تواند از پروتکل‌های شبکه‌ای که اینترنت روی آن قرار گرفته، بدون هیچ محدودیتی اقتباس و استفاده کند. فضای سایبر یک وسیله ارتباطی بین المللی است و حق انتـخاب و اشتراک افراد را، هم در تولید و هم در دسترسی به اطلاعات ، بسیار افزایش داده و از این رو مفهوم آزادی اطلاعات را به معنای واقعی کلمه تحقق بخشیده است. اینترنت، دو خصوصیت«انتقال و دریافت اطلاعات» را به طور همزمان داراست؛ یعنی کاربران اینترنت ضمن اینکه می توانند از اطلاعات موجود در شبکه مذکور استفاده کنند، خود نیزمی توانند خواسته، اندیشه و «اطلاعات» خود را به منظور عرضه آن به سایر کاربران وارد شبکه مذکور نمایند.

اینترنت رسانه ای مبتنی بر تعامل می‌سازد که آن را تبدیل به رسانه ای چند وجهی، آزاد و غیر متمرکزمی‌نماید که نقش قالبی و القایی سایر رسانه ها را نداشته و از تمرکز و تحمیل توسط حکومتها و صاحبان رسانه‌ها آزاد است و به عصر ارتباطات یکسویه نیز پایان بخشیده است.[3]

امکان اینکه هر کس بتواند در هر نقطه ای از جهان به این شاهراه اطلاعاتی وارد شود و هرگونه اطلاعاتی که می خواهد بدان وارد کند مشکلاتی جدی برای این فضا آفریده است؛ حتی یک کاربر

---

[1].فضای سایبری فاقد مرزهای زمینی است، و به همین علت هزینه و سرعت ارسال پیام بر روی اینترنت تقریباً مجزا از مکان فیزیکی است: پیام‌ها می توانند از هر مکان فیزیکی به هر مکان دیگر بدون کاستی، خرابی، یا تأخیری قابل توجه، یا بدون صف‌ها یا موانع فیزیکی که به نحوی افراد و مکان ها را از نظر جغرافیایی از هم جدا می سازد، ارسال شوند. اینترنت امکان انجام معاملات را میان افرادی که نسبت به مکان فیزیکی طرف مقابل بی اطلاع هستند فراهم می کند . مکان بطور مجازی حائز اهمیت است و این فضای مجازی دارای آدرس های اینترنتی است اماهیچ ارتباط ضروری بین آدرس اینترنتی و قلمرو فیزیکی وجود ندارد ومربوط به دستگاه‌های بین پیام‌ها و اطلاعاتی است که مسیریابی می شوند.ر.ک:

David R. Johnson & David G. Post.**Law and Borders - The Rise of Law inCyberspace**,٤٨ STAN. L. REv. ١٣٦٧, ١٩٩٦, http://www.cli.orglX٠٠٢٥_LBFIN.html.

[2].هیک، استیون و اف هلپین، ادوارد و هوسکینز، اسکینز، ۱۳۸۶،**حقوق بشر و اینترنت**، ترجمه دکترسید قاسم زمانی ومهناز بهراملو،انتشارات خرسندی، ص۲۰

[3] .فضلی، مهدی،۱۳۸۳a،**مسوولیت کیفری ارایه دهندگان خدمات اینترنتی**، پایان نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه پردیس قم، ص ۷۵ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نوجوان می‌تواند عامل توزیع کنندهٔ اطلاعات مجرمانهٔ بسیار خطرناکی باشد. این نوجوان می‌تواند از یک کشور اطلاعاتی مخرب را وارد فضای سایبر کند که موجب از بین رفتن داده های ارزشمند یا سیستم های رایانه‌ای بسیاری درسطح بین المللی گردد.بی‌شک،این عدم محدودیت به مرزها،حاکمیت دولتها وصلاحیت محلی و بین المللی برای رسیدگی رابه چالش می کشد.[1]

امروزه افراد بیشماری از سراسر جهان به اینترنت دسترسی داشته و درتعامل هستند .از لحاظ مجازی دنیایی در کنار دنیای واقعی بدون هیچ حدو مرزی ایجاد شده است.تعیین عمق کامل و گستره آن مشکل می نماید. در واقع این فضای بیکران اطلاعاتی طی چندین سال اخیر رشد چشمگیری داشته که آمار کاربران[2] وسایت های موجودکه به چندین میلیارد افزایش پیدا کرده است به خوبی گواهی بر این مدعااست.

---

[1] .صدها سال کشورها برای کنترل مرزهای زمینی و آبی خود منابع قابل توجهی را سرمایه گذاری کرده‌اند. کنترل مرزها همواره بخش مهمی از نظارت برافرادو کالاهای تهدید آمیز مثل اسلحه و مواد مخدربوده است. از فضای سایبری می توان برای درهم شکستن این سیستم استفاده کرد و از بازرسی طفره رفت. مرزهای فیزیکی مانعی برای ارتباطات در فضای سایبرایجاد نمی کند .به نحویکه حتی برخی برای مقابله با این مسئله ایجاد "اداره مجازی مهاجرت و گمرک" را پیشنهاد داده اند. سیستمی برای بازرسی داده هایی که در سرتاسر اینترنت جابجا می شوند. انجام این امر مستلزم این است که پروتکل های هدایت کننده ترافیک در سرتاسر اینترنت تغییر یابند.داده ها بصورت بسته ای حرکت می کنند، هر یک از آنها سرپیامی دارد که مشخص کننده آدرس مبدأ ، آدرس مقصد، و حجم بسته است. تا سال ۲۰۰۰ دولت ها قادر نبوده اند تا بسته های داده ای را ردیابی کنند، زیرا اطلاعات سرپیام هیچ راهی را برای تشخیص منشاء بسته ارائه نمی داد. مثلاً نمی توان تشخیص داد که بسته داده از چین است یا این که از پاکستان است. در سال ۲۰۰۰، از واحد مهندسی اینترنت (Internet Engineering Task Force) که مسئول پروتکل ها است، خواسته شد تا آنها را تغییر دهند، و از این راه کشورها توانستند بسته هایی را که به بخش فضای سایبری آنها وارد می شدند کنترل کنند.ر.ک:

William S. Cleveland &Donald X. Sun, Bell Lab; **Internet Traffic Data**, (paper presented at the University of Michigan)،۲۰۰۰,
,http://www.stat.lsa.urnich.edulgrnichaillstat٦oo Foo/traffic.pdf.
.Declan McCullagh,**WiretappingtheNet: Oh, Brother**,Wired News, Oct. ۱۲, ۱۹۹۹,
http://www.wired.comlnews/politics/۰.۱۲۸۳.۳۱۸۵۳.۰۰.html.

[2] .طبق نظرکارشناسان ماهانه ۱۰ درصد به تعداد کاربران اینترنت افزوده می‌شود ولی تعداد دقیق کاربران که روزانه از آن استفاده می کنند مشخص نیست. تعداد کاربران اینترنتی را در سال ۲۰۰۰ کارشناسان ۵۰۰ میلیون نفر اعلام کرده بودند.(مهدی پور – میثم ؛**تاریخ اینترنت** ، ویکی پدیا فارسی http://fa.wikipedia.org/wiki)

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بدین ترتیب فضای سایبر را باید یک محیط لایتناهی دانست اما این فضای لایتناهی دائماً در حال قبض و بسط است؛ این قبض و بسط بدین معناست که ابعاد فضای سایبر هر لحظه می تواند گسترش یا کاهش یابد. به فضای سایبر می‌توان حامل های داده ای را متصل نمود که حاوی ریزپردازنده هایی هستند؛ این ریز پردازنده ها دارای پتانسیل نگهداری اطلاعات در ظرفیت های بالایی بوده بر تعداد این ریزپردازنده ها و سخت افزارهای حامل داده می‌توان هر لحظه افزود و با ارتباط دادن آنها به یکدیگر در قالب شبکه های دیجیتالی گسترهٔ مجازی بی نهایتی آفرید. افزایش تعداد کاربران در سطح جهان باعث افزایش هر چه بیشتر گسترهٔ این فضای مجازی است.

۱-۳-۳-۲ پنهانی و پوشیده بودن

فضای سایبرازجهت خلوت و محرمانگی همچون ذهن آدمی است. در ذهن آدمی تعداد بیشماری از قضایا یا مطلوب هایی نهفته است که اگر عیان شود سبب تحیردیگران یا نقض مکرر قانون یا هنجارها می گردد؛ از این رو آنچه که انسان ها در عمل نشان می دهند یا بیان می دارند چه بسا همان چیزی نباشد که در ذهن آنهاست؛ به همین دلیل هرکس خود را در بند هنجارهای محیطی یا قوانین و مقررات یا ملاحظات شخصی و گروهی می داند، در ذهن خویش این بندها را می‌گسلد و با آزادی کامل می‌اندیشد. فضای سایبر نیز بی‌ارتباط با محیط ذهن نیست. این فضا نیز به اعتبار ارتباط انسان با یک ماشین در محیطی دور از چشم همگان، همان فضای ذهن را یاد آور می شود.

فضای سایبر قابلیت آن را دارد که بازیگران و نقش‌آفرینان آن کاملاً مخفیانه و به طور ناشناس باشند و بدون بیم از آنکه شناخته شده یا مورد ردیابی و تعقیب قرار گیرند اقدامات خود را به معرض اجرا گذارند.« فضای پوشیدهٔ سایبر اجازهٔ تبلور مکنونات درونی انسانها را که در جامعه فرصت ابراز آنها را نیافته اند فراهم می کند و این گفتهٔ اندیشمندانی چون هابز[1]که ذات انسان را شرّ می دانند در چنین فضایی دوباره قوت می‌گیرد،چراکه حس پوشیده بودن ومخفی ماندن اعمال ارتکابی است که اینترنت را دنیایی آزاد جلوه گر می سازد تا در این پهنه، افراد به شکلی افسارگسیخته و فارغ از کنترل های

در سال ۲۰۰۷ آمار کاربران اینترنت در ژوئن ۲۰۰۷ بیش از ۱/۱ میلیارد نفر با رشد حدود ۲۲۵٪ نسبت به سال ۲۰۰۰ بوده است ودر سال ۲۰۰۹ به بیش از۱/۷ میلیارد نفر رسیده است.در سال ۲۰۰۹ این رشد نسبت به سال ۲۰۰۰ حدود ۳۸۰٪ بوده است.حدود ۲۵٪جمعیت جهان کاربر اینترنت هستند.(ر.ک :http://www.internetworldstate.com)

[1].Thomas Hobbes

فیلسوف مشهور انگلیسی (متولد ۱۵۸۸ و متوفی ۱۶۷۹) و نویسنده کتاب مشهور لویاتان درباره هیولای دولت

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

اجتماعی و اخلاقی میدانی برای تاخت و تاز و عقده‌گشایی آنچه بدان دست نیافته اند بیابند؛ نمونه این امر را می‌توان در مورد انتشار تصاویر مستهجن کودکان در فضای سایبر دانست که در عین حالی که وسیله سود آوری برای ارائه کنندگان این تصاویر گشته، برای خواستاران ارضای غرایز جنسی نیز دنیایی آزاد فراهم آورده تا هر لحظه که خواستند بتوانند به راحتی وارد این دنیای خیال گونه شوند و تمایلات غریزی خود را فروبنشانند.»[1]

مجرمین فضای سایبر با استفاده ازقابلیت اختفاء در چنین فضایی امکان ارتکاب بالقوه طیف وسیعی از انواع جرایمی را می یابند که وقتی این امکان با گسترهٔ بی انتهای فضای سایبر در هم می‌آمیزد، موقعیت خطرناکی را پدیدار می‌سازد،گستره ای وسیع با مجرمانی بی شمار، پراکنده و ناشناس.قابلیت مبادله همزمان اطلاعات در حجمی زیاد در این فضا وجود دارد.این ویژگی را سایر وسایل ارتباط جمعی ندارند.همچنین «امکان چند رسانه ای بودن، آن را در حد یک پدیده کاملاً انحصاری از سایر پدیده‌ها جدا می‌سازد.» کاربران امکان گزینش اطلاعات در فضای سایبر را دارند. امکانات جستجو و کنکاش آنان را قادر می سازد که هر اطلاعاتی را که دوست دارند دریافت کنند و بر خلاف سایر رسانه ها که اطلاعات بر مخاطب تحمیل می‌شود و قدرتی در انتخاب اطلاعات وجود ندارد، جریان اطلاعات یکسویه، تک بعدی و تحمیلی نیست.

۱-۳-۳-۳ ناهنجارمند و کنترل ناپذیر بودن

فضای سایبر به جهت افسارگسیختگی و کنترل ناپذیری با دنیای بیرونی قابل مقایسه نیست و باز باید گفت به هر میزان که می توان ذهن انسان ها را دید و آنها را به بند کشید و به زیر یوغ کنترل برد، می تواند درباره فضای سایبر نیز صادق باشد. فضای سایبر به دور از کنترل اجتماعی و نظارت پلیسی است و حتی در بیشتر موارد کنترل گران خانواده مانند والدین نیز توان لگام زدن به سرکشی فضای سایبر را حتی در اندرون خانه خود ندارند. در واقع محیط سایبر از همان ابتدای پیدایش آن، علیرغم نظم فنی اعجاب‌آورش، از منظر رفتار کاربران، محیطی مبتنی بر آنارشیسم و هرج و مرج بوده است.[2] این محیط پلیس ندارد، سازمانی بر آن نظارت نمی‌کند، مردم اشخاص را در حین ارتکاب جرم نمی

---

[1]. فضلی، مهدی، ۱۳۸۳، **تخریب و اختلال در داده ها و سیستم های رایانه ای**، مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات، مرکز مطالعات راهبردی و توسعه قضایی قوه قضائیه، تهران، ۱۷ و ۱۸ خرداد ص ۱۲۷

[2]. Carey, Peter, **Media Law**, Sweet&Maxwell, Second Edition, London, ۱۹۹۹, p ۱۷٦.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بینند و هر کس هر آنچه می خواهد انجام می‌دهد.بنابراین ویژگی دیگر این محیط«عدم امکان یک کنترل مؤثر تکنیکی و حقوقی در شرایط حاضر است.»[۱]

یک علت عمدهٔ این امر، این است که چنین فضایی محیط ملموسی نیست که دائماً تحت دیدگان کنترل و نظارت نهادهای کنترلی و عوامل اجتماعی بازدارنده از تخلف باشد؛ بلکه چنانچه دربالا بیان شد یک محیط خاموش و منفعل است که خلوتگاه مناسبی را برای مرتکبین جرایم سایبر آفریده است.«به عبارت دیگر فضای سایبر دارای یک نظام عرضی است و نه یک نظام طولی و بر خلاف جوامع انسانی، ساختار آن مبتنی بر سیستم سلسله مراتبی بالا به پایین نیست که نهادهای بالادست بر نهادهای پایین دست حاکم و ناظر باشند، بلکه در آن از نظام قدرت و کنترل تمرکز زدایی شده و هر شخص در کنار قرار می‌گیرد و هیچ نهاد بالادستی بر آن حاکمیت ندارد که امر کنترل و ایجاد نظم را در آنجا عهده دار باشد.»[۲]

بنابراین فضای سایبر یک فضای سرد و بی روح تکنولوژیک است که آنچه که وجدان جمعی، هنجارهای هدایتگر اجتماعی، اخلاق جمعی و نظایر آن نامیده می شود و در هر جامعه‌ای مبانی نظم را بنیان می نهد در آن بی معناست. در هر جامعه و محیطی- حتی در محیط‌های حیوانی- برخی نهادهای کنترل اجتماعی به صورت سلسله مراتبی در قالب نظارت و اطاعت فرودست از فرادست ناظر کردار و کارکرد افراد است. اما محیط سایبر یک محیط آزاد است و فارغ از هرگونه هنجارهای اجتماعی و سلسله مراتب هرمی نظارتی و فرمانبرداری است؛ در واقع آن گره‌ها و علقه‌هایی که سبب می‌گردد شخص در درون خود نوعی حس تحت نظارت بودن را احساس کند- اعم از اینکه این حس بیرونی و با نظارت مجری قانون یا مردم و یا درونی و ناشی از هنجارها و قواعدی همچون اخلاق یا ترس ناشی از بی‌آبرویی و امثال آن باشد- وجود ندارد.[۳]

---

[۱]. حسن بیگی، ابراهیم؛ **پیشین** ، ص۳۶

[۲]. Brenner, Susan, **Toward a Criminal Law for Cyberspace: Distributed Security,** University of Dayton School of Law,http://law.bepress.com/expresso/eps /۱۵, p: ۵۵

[۳] .کنترل ناپذیری برحسب رعایت بایسته های این فضا و چهارچوبش است وگرنه کنترل غیر قانونی و سرسختانه فضای سایبر امکانپذیر است ولی چنین کنترلی مبتنی بر عدم رعایت اقتضائات فضای سایبر و حقوق و آزادی‌های فردی است. در حالی که طبق اصل ۲۵ قانون اساسی، بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هر گونه تجسس مگر به حکم قانون ممنوع است؛ طبق ماده ۴۸ قانون جرایم رایانه‌ای مصوب خرداد ۱۳۸۸، شنود محتوای در حال انتقال

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بخش چهارم: سابقه تاریخی جرایم رایانه ای

الف: تاریخچه جرم جاسوسی

جاسوسی از زمره جرایم قدیمی است که همواره مورد برخوردهای سخت وخشن قرارگرفته است برخی ازنویسندگان قدمت تاریخی این جرم راحداقل به زمان حضرت موسی«علیه اسلام» برمی گردانند.[1] جاسوسی اصولاً به منظور شناسایی دشمن انجام می شود و اخبارمربوط به دشمن که به وسیله جاسوسان حرفه ای جمع آوری می شود،به اطلاعات سری مرسوم است. به بیان دیگر جمع آوری اطلاعات پنهانی با استفاده از ترفند و فریب را جاسوسی گویند.جاسوسی قدیمی ترین شیوه جمع آوری اطلاعات سری است. جاسوسی از همان ابتدای تاریخ ثبت شده بشر، بخشی از امور سیاسی و نظامی بوده اما سیستم مدرن جاسوسی در جریان جنگ جهانی دوم (۱۹۳۹-۱۹۴۵) و دوره پس از آن معروف به جنگ سرد (۱۹۴۵-۱۹۹۱) شکل گرفت. در جریان جنگ جهانی دوم، جاسوسی توسط کشورهایی که مستقیماًبایکدیگردرحال نبرد بودند یعنی بریتانیا، فرانسه، روسیه و ایالات متحده آمریکا از یک طرف و آلمان ژاپن و ایتالیا از طرف دیگر به کار گرفته می شد. در دوره جنگ سرد، جاسوسی توسط دو ابر قدرت یعنی ایالات متحده امریکا واتحاد شوروی استفاده می شد.[2]

ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود. و طبق تبصره این ماده، دسترسی به محتوای ارتباطات غیرعمومی ذخیره‌شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است. طبق قانون و به ویژه قانون آیین دادرسی دادگاه های عمومی و انقلاب شنود تلفنی تنها با مجوز قضایی و آن هم در مواقعی خاص امکانپذیر است. رئیس نیروی انتظامی در پاییز ۱۳۸۸ در قبال پیامدهای رسانه ای و اینترنتی انتخابات ریاست جمهوری خرداد ۱۳۸۸، گفته است که "ایمیل ها و اس ام اس ها از جایی فرستاده می شود که کاملاً در کنترل ما قرار دارد و تصور نکنند که آنتی پروکسی جلویش را می گیرد و این تصور اشتباه را نداشته باشند که کنترل نمی‌شوند" اما در مورد نحوه کنترل مبادله پیام از طریق ایمیل و اس ام اس، نهاد کنترل‌کننده و جنبه‌های حقوقی مورد استفاده در این زمینه توضیحی نداده است. براساس قانون جرایم رایانه ای جمهوری اسلامی، سرویس دهندگان اینترنتی موظف هستند اطلاعات مربوط به کاربران را برای چند ماه نگهداری کنند و این اطلاعات با حکم قضایی می تواند در دسترس نهادهای امنیتی قرار گیرد.به نقل از تارنمای بی بی سی فارسی- ۱۵ ژانویه ۲۰۱۰- ۱۳۸۸/۱۰/۲۵

[1].J.M.Martinand A.T.Romano,MultinationalCrime(London:Saga Publications,۱۹۹۲)P.۳۹,citing .Andrew M .C.Her Majestys Secret Secret Service…(New York: Viking,۱۹۸٦)P.۱

[2]. میرمحمد صادقی، حسین،۱۳۸۱،**جرایم علیه امنیت وآسایش عمومی**، تهران، نشر میزان،ص۷۶

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

پیشینه طولانی جاسوسی سیاسی ونظامی وهمینطور تشدید مجازات یاحتی جرم انگاری مقدمات آن ، هنوز چهره سرزنش آمیز واقعی برای این رفتار ترسیم نکرده است ، زیرا ازمنظر امنیت ملی، جاسوسی به همان میزان که به ضرر یک کشور است ، شاید به نفع کشوردیگری باشد که جاسوسی برای آن صورت گرفته است. کشورها درطول تاریخ ، قبل از مواجهه نظامی همواره باحربه جاسوسی به مصاف هم رفته اند وآن را کلید تأمین امنیت ملی نظام غیرقابل پیش بینی روابط دولت ها دانسته اند . برای مثال ، ایالات متحده با هدف تأمین امنیت ملی وبا تصویب قانون امنیت ملی درسال ۱۹۴۷، سازمان خبرگیری مرکزی (سیا)[۱] رابنیان نهاد که وظیفه اصلی آن جمع آوری وتحلیل اطلاعات وارائه گزارش به دولت آمریکاست . ازاین رو، جاسوسی یا ستون پنجم[۲] که به دلیل مغایرت با امنیت ملی چهره منفی وسرزنش آمیزی دارد، درچهره ای دیگر با تعابیری چون خبرگیری یا کسب اطلاع از کشورهای دیگر برای تأمین امنیت ملی قابل توجیه وحتی ضروری می نماید.

۱-۴-۱جاسوسی درتاریخ اسلام

اززمانی که پیامبراسلام حضرت محمد(ص) ازمکه به مدینه هجرت فرمودند،اولین پایه های حکومت ودولت اسلامی را درآن سامان بنیان نهاد.با تشکیل حکومت اسلامی ، مباحثی از قبیل جاسوسی ، از دوجهت به منظورحفظ نظامات کشور اسلامی ضرورت پیدا نمود:

۱- اطلاع به امور پنهانی وتوطئه های دشمنان اسلام ازمهمترین وسایل حفظ حکومت اسلامی به شمارمی رفت .با اطلاع یافتن از نقشه های دشمنان اسلام،توطئه ها خنثی می شدواین وسیله به عنوان یک ابزارحیاتی برای دفاع از مرزو بوم اسلامی بشمار می رفت دراهمیت تهیه ابزاردفاع از دولت اسلامی همین بس که قرآن کریم مسلمانان رابه آن ترغیب نموده وآماده نمودن وسایل دفاع از کشور را واجب نموده است.[۳]

---

[۱].Central IntelligenceAgency(CIA)

[۲].دراصطلاح عوامل خرابکار وجاسوسان یک کشور دیگریاعوامل گروه مخالف دولت درسازمان دولت را« ستون پنجم» می نامند.این اصطلاح درجنگهای داخلی اسپانیا (۱۹۳۹-۱۹۳۶) پدیدآمدووجه آن نیز این بودکه هنگامی که فرانکو فرمانده سپاه ضدجمهوری با چهارستون به مادرید تاخت درهمان هنگام قراربودکه گروهی به مادرید رخنه کنند وبه مدافعان شهر همزمان با حمله از بیرون حمله برند.این عوامل پنهانی ستون پنجم نامیده می شوند.

[۳].وَاعدّوا لَهُم مَااستطعتُم مِن قوَه ، سوره مبارکه انفال آیه۶۰

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۲- حفظ اسراروامورمحرمانه ازدسترس دشمن درتاریخ اسلام اهمیت ویژه ای داشت، زیرا دشمن با اطلاع از این اسراربه سهولت قادرمی شدکه با کشوراسلامی مبارزه ومقابله نمایدودرصورتی که اسراردراختیاردشمن قرارمی گرفت،وسیله تسلط دشمنان برمرزوبوم اسلامی فراهم می شدواین عمل مستوجب کیفربود.[۱]

۱-۴-۲ جاسوسی ازمنظرقرآن وسنت

جاسوسی درقرآن دو وجه دارد ۱- منع آن و ۲- درمواردی جواز آن .

۱- آیه دوازدهم از سوره شریفه حجرات « یاایَهَا الذَّین َ آمَنوُا اِجتَنِبوُاکَثیراً مِن الظنِّ إنَّ بعضَ الظنِّ إثْم ولَاتجَسَّسوا ولَایغتَب بعضُکُم بَعضا »[۲]

« ای اهل ایمان از بسیاری گمانهای باطل نسبت به هم دوری کنیدکه برخی ازآنها گناه است ونیزهرگز درزندگی دیگران تجسس نکنید وغیبت یکدیگر رامکنید. »

از معنا ومنطوق آیه به خوبی نهی از تجسس فهمیده می شود وبه حکم آن درنظام اسلامی اصل برحرام بودن تفحص وجاسوسی دراموردیگران استفاده می شود.

۲- درمواردی جاسوسی مجاز شناخته شده ونیز درآیات شریفه سوره اسراء خداوند بدین ترتیب بیان می دارد که « فَجاسوُا إخلالَ الدّیار » گروهی رابرشما فرستادیم تادرمیان شمابه جستجو بپردازند که درصدراسلام به آنها نقیب می گفتند که به کسی اطلاق می شد که درپی مراقبت از اوضاع واحوال وفعالیتهای قوم بود .

از لحاظ حدیث ، احادیث متعددی از لسان امامان بزرگوار(ع) وپیامبر اکرم(ص) منقول است هم درباره جواز آن وهم منع آن.[۳]

حضرت علی «علیه اسلام» درنامه خود به مالک اشتر درزمانی که وی رابه عنوان فرماندارمصر انتخاب کردند،اورا از تجسس دراحوال مردم منع وبه پوشانیدن عیوب مردم ودوری جستن از کسانی که عیوب دیگران راآشکارمی سازند ، توصیه فرمودند.[۴]

---

[۱].ساریخانی،عادل،پیشین،ص ۷۴

[۲] .قرآن کریم ، سوره حجرات آیه ۱۲

[۳] .خداقلی،زهرا، ۱۳۸۲ ، جرائم کامپیوتری ، تهران، آریان ، ص ۱۰۵

[۴] .نهج البلاغه ، ترجمه محمد دشتی ، انتشارات مشهور ، ۱۳۸۰ ، نامه۵۳،ص ۵۶۹

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ب : تاریخچه جرایم سایبری

از اواسط دهه ۱۹۷۰، مطالعات تجربی در مورد جرم رایانه ای با استفاده از متدهای تحقیقاتی رشته جرم شناسی انجام شد. در دهه ۱۹۸۰،نظرات علمی و عمومی در مورد جرم رایانه ای به سرعت تغییر یافت ومشخص شد، که جرم رایانه ای محدود به جرایم اقتصادی نبوده، بلکه همه تعرضات نسبت به همه منافع را شامل می شود. مثلاً سوء استفاده ازرایانه بیمارستان یا تخلفات رایانه ای نسبت به حقوق خصوصی و فردی که جنبه اقتصادی ندارند و اساساً این موارد راجدا از جرم رایانه ای بررسی کرده اند. موج وسیعی از سرقت برنامه هاوسوء استفاده ها ازصندوق های پرداخت و استفاده از مخابرات، موجب شد انعطاف جامعه اطلاعاتی برانگیخته شده، نیاز برای استراتژی جدید امنیت داده پردازی و کنترل جرم احساس شود.

در حال حاضر بیشتر نظرها در زمینه جرایم رایانه ای به انتقال غیرقانونی سرمایه ها با استفاده از ابزار الکترونیکی، خرابکاری،ویروس ها، کرم های رایانه ای و همچنین جعل اسناد با استفاده از رایانه معطوف است. خطر خرابکاری، مخصوصاً در سال ۱۹۸۹ و زمانی آشکارشد که دادرسی های کیفری در جمهوری فدرال آلمان معلوم کرد، که خرابکارانی با استفاده از شبکه های اطلاعاتی بین المللی به اطلاعاتی درآمریکا وانگلستان و دیگر کشورهای خارجی دست یافته و حاصل کارخود را به کشور شوروی سابق فروخته اند.تقریبا در همان زمان (۱۹۸۸)خطر ویروس ها وکرم ها هم معلوم شد. زمانی که (Internet - Worm)توسط یک دانشجوی آمریکایی ساخته شده بود، در طی چند روز نزدیک به ۶۰۰۰ سیستم رایانه ای را در اینترنت مختل کرد. بعد شکل های جدید بزهکاری در زمینه تکنیک های ارتباط سمعی – بصری (مثلا درزمینه سیستم مینیتل فرانسه و یا قسمت های ارتباط ماهواره ای) ادامه جرایم اطلاعات را افزایش دادند. اولین جرم رایانه‌ای به طور رسمی در سال ۱۹۶۳ میلادی رخ داد.[۱]

الدون رویس[۲] در این سال به دلیل اختلاف با مسئولان شرکت محل کارش تصمیم به انتقام گرفت و با تغییر در برنامه مربوط به محاسبه صورت هزینه شرکت، درصدی از درآمد حاصله را به حساب‌های خاصی واریز نمود.

---

[۱]. طارمی ، محمد حسین،پیشین ،صفحه ۱۴

[۲].Aldon Roys

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

الدون رویس با ظرافت خاصی قیمت ها را تغییر می داد ، بعد از آن با نام ۱۷ شرکت محل و طرف قرارداد ، چک های جعلی صادر و از آن حساب برداشت می کرده به طوری که در کمتر از ۶ سال بیش از یک میلیون دلار بدست آورده است امابه 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 دادگاه را به تدوین قوانین مدون وا می دارد.

از سال ۱۹۹۴ میلادی به بعد با گسترش فضای مجازی، بحث جرایم مجازی به عنوان صورت تکامل یافته جرایم رایانه‌ای مطرح شد.

اولین قانون راجع به جرایم اینترنتی در سال ۱۹۸۴ در آمریکا به تصویب رسید و در سال های ۱۹۹۴ و ۱۹۹۶ این قانون اصلاح گردید. درحال حاضر ۴۴ کشور دنیا؛ شامل ایالات متحده، انگلیس، کشورهای عضو اتحادیه اروپا، استرالیا و هندوستان، پلیس هایی دارند که به پلیس اینترنتی مشهور هستند و به طور رسمی از طریق کانال های دولتی،جرایم مجازی را پی گیری می کنند.[1]

۱-۴-۳ تاریخچه جرایم سایبری درایران

درایران دیرهنگام ترازکشورهای دیگرموضوع تخلفات وجرایم کامپیوتری نمودپیداکرد. درابتداتخلفات کامپیوتری درایران اکثراً مرتبط با اختلافات ناشی ازعدم ایفای تعهد یا اجرای ناقص آنها بوده است ومرجع رسیدگی به تخلفات بدواً شورای عالی انفورماتیک ایران وسپس محاکم قضائی بودند وقانون مدون مورد استناد ، قانون حمایت از حقوق مؤلفان ومصنفان وهنرمندان مصوب سال ۱۳۴۸ وقانون مجازات اسلامی بود.

با گذشت زمان باتوجه به استفاده فراگیر از سیستمهاوتجهیزات رایانه ای درکشور وبه تبع آن شیوع جرایم وتخلفات کامپیوتری ضرورت تدوین قانون جدیدبه چشم می خورد که سرانجام مجلس شورای اسلامی دردیماه ۱۳۷۹شمسی « قانون حمایت ازپدیدآورندگان نرم افزارهای رایانه ای »[2] را که پیش نویس آن توسط دبیرخانه شورای عالی انفورماتیک درسال ۱۳۷۴ شمسی تدوین شده بود ،

---

[1].ضیابری ، سید ایمان ، جرایم و مجرمان اینترنتی را بهتر بشناسیم.

http/www..magiran.com/mpview.asp

[2].قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه ای مصوب۱۳۷۹/۱۰/۴ ، روزنامه رسمی شماره ۱۶۲۸۱ مورخ ۱۳۷۹/۱۰/۲۵

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تصویب نمود. درسال ۱۳۸۱ طرح قانون تجارت الکترونیک تهیه ودردستورکارکمیسیون محترم صنایع مجلس شورای اسلامی قرارگرفت که نهایتاً متن آن درسال ۱۳۸۲ به تصویب نهائی رسید ، از جمله نوآوری های مهم درقانون فوق الذکر می توان به جرم انگاری جعل ، کلاهبرداری کامپیوتری ، حمایت کیفری ازحقوق مصرف کننده،حمایت ازداده وکپی رایت اشاره نمود.شورای عالی توسعه قضائی وابسته به قوه قضائیه ازسال ۱۳۸۱ اقدام به تهیه پیش نویس قانون دررابطه باجرایم کامپیوتری وشبکه ای نمود که اقدامات این شورا درتدوین قوانین مرتبط باجرایم تکنولوژی ارتباطات وکامپیوتر دردوبخش قوانین ماهوی وشکلی تهیه ودراواخرسال ۱۳۸۳ به هیأت محترم دولت ارسال واز آنجا دراوایل سال ۱۳۸۴ به مجلس محترم شورای اسلامی به جهت بررسی وتصویب تقدیم گردید که درمجلس درجلسه علنی روز سه شنبه مورخ پنجم خرداد هزاروسیصد هشتاد وهشت به تصویب ودرتاریخ ۸۸/۳/۲۰ به تأیید شورای نگهبان رسید.[۱]

۱-۴-۴ اولین جرم اینترنتی درایران

وقوع اولین جرم اینترنتی درایران مشخص نیست اما برخی گزارشهای غیر رسمی حاکی ازاین است که اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی کامپیوتر در کرمان اقدام به جعل چک های تضمینی مسافرتی کردند و چون تفاوت و تمایزی چندان بین جرم کامپیوتری و جرم اینترنتی وجود ندارد، عمل آن ها به عنوان جرم اینترنتی محسوب می شود.

بعد از این بود که گروههای هکر موسوم به گروه مش قاسم و ... ،جرم های دیگری را مرتکب می شدند، مواردی چون جعل اسکناس ، اسناد و بلیط های شرکت های اتوبوسرانی ، جعل اسناد دولتی از قبیل گواهینامه ، کارت پایان خدمت ، مدرک تحصیلی و جعل چک های مسافرتی و عادی ، بخشی از این جرایم اینترنتی هستند.[۲]

---

[۱].باستانی ، برومند ، ۱۳۸۳،**جرائم کامپیوتری واینترنتی جلوه ای نوین از بزهکاری**، تهران بهنامی ،ص۱۹

[۲].http://www.agahisara.ir/cms/archives/۱۶۳۰۶۲

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۱-۴-۵ آمار جرایم رایانه ای درایران

در سال ۸۵ حدود ۷۹ پرونده در مورد جرایم رایانه‌ای به سیستم آگاهی کشور وارد شد که این آمار در سال ۸۶ به ۹۸ پرونده، در سال ۸۷ به ۱۳۱ پرونده و در شش ماه اول سال ۱۳۸۸ به ۱۷۳ پرونده رسید. که نشان‌دهنده سیر صعودی تعداد پرونده‌های این حوزه است. البته بسیاری از جرایم به دلایل مختلفی به مرحله تشکیل پرونده نمی‌رسند. با این حال نسبت به رشد کاربرد رایانه در زندگی و امور جامعه در ایران افزایش جرایم رایانه‌ای کم بوده است.

آمار رشد اینترنت با جرائم رایانه‌ای

سال	کاربران	درصد رشد کاربران	جرائم رایانه	درصد رشد جرائم
۱۳۸۴	۸،۸۰۰،۰۰۰ نفر		۵۳ پرونده	
۱۳۸۵	۱۲،۰۰۰،۰۰۰ نفر	۱۳۶درصد	۷۹ پرونده	۱۴۹درصد
۱۳۸۶	۱۲،۶۰۰،۰۰۰ نفر	۱۰۵درصد	۹۸ پرونده	۱۲۴درصد
۱۳۸۷	۲۱،۰۰۰،۰۰۰ نفر	۱۶۷درصد	۱۲۸پرونده	۱۳۱درصد
۱۳۸۸	۲۵،۶۰۰،۰۰۰ نفر	۱۲۲درصد	۲۲۲ پرونده	۱۷۳درصد

دربحث از آمارجنایی، یکی از موارد مهم انواع رقم بزهکاری است. آنچه به مأمورین گزارش می شود وموارد‌ی که درمراجع پلیس قضایی رسیدگی می شود،رقم واقعی بزهکاری نیست.زیرااقلام بزهکاری شامل رقم ظاهری ، قانونی وسیاه می شود.آنچه دست نیافتنی است،رقم سیاه[۱] جرایم است وهیچ گاه نمی توان به این رقم دست یافت، اما می توان ارزیابی وتخمین ها رابه این مورد نزدیک کرد. دربرخی جرایم رویه سکوت عمدی مقامات موجب مکتوم ماندن آن پدیده می شود.[۲]

[۱]. Dark Number

[۲]. ضمانت اجرایی قانون جرایم رایانه‌ای چیست؟ آفتاب، ۸ آذر ۱۳۸۸از ویکی‌پدیا، دانشنامهٔ آزاد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل دوم:

شناخت جرم جاسوسی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

با توسعه فضای مجازی در میان عامه مردم و از سویی گسترش منابع موجود در این فضا، ضرورت بحث در خصوص جرایم سازمان یافته اجتناب ناپذیر می نماید. این نکته که آیا اصولاً جرم سازمان یافته در فضای مجازی وجود دارد یا خیر؟ و یا اینکه صرفاً جرایم مجازی به گونه‌ای سازمان یافته ارتکاب می یابند؟ از سؤالات مبتلا بهی هستند که می بایست بدان‌ها پاسخ داد. با این تفاسیر و با توجه به بحث گسترده پیرامون جرم مجازی، در این قسمت تنها به بیان کلیاتی در خصوص جرم سازمان یافته می پردازیم.

بخش اول : جرم سازمان یافته

اصطلاح جرم سازمان یافته در ابتدا در متون جرم شناسی مطرح شد. این اصطلاح نخستین بار توسط ساترلند در کتاب مشهور "اصول جرم شناسی" مطرح شد.[1]

۲-۱-۱ تعاریف جرم سازمان یافته

در خصوص جرایم سازمان یافته تعاریف بسیاری ارائه شده است که در ذیل به برخی از مهم ترین آنها که با موضوع مورد بحث ما نیز ارتباط دارند، اشاره می کنیم:

«جرم سازمان یافته، اقدام مجرمانه مستمری است که برای کسب سود و منفعت از طریق انجام فعالیت‌های غیر قانونی مورد نیاز مردم انجام می شود.»

ماده ۲ کنواسیون سازمان ملل متحد علیه جرایم سازمان یافته و فراملی مصوب سال ۲۰۰۰ مشهور به کنوانسیون پالرمو، بیان می دارد که: جرایم سازمان یافته به جرایم شدید یا جرایم خاص پیش بینی

[1].نجفی ابرند آبادی ، علی حسین ،۱۳۸۵، **مباحثی در علوم جنایی** ، دانشگاه علوم اسلامی رضوی ، سال تحصیلی ۸۲ ص۸۵۰

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

شده در کنوانسیون[1] اطلاق می شود که توسط گروهی متشکل از سه نفر یا بیش تر و با هدف تحصیل مستقیم منفعت مالی یا مادی برای مدتی ارتکاب می یابد.[2]

تعریف دیگر که بر پایه تقسیم بندی وظایف و اعمال است جرم سازمان یافته را اینگونه تعریف می کند: فعالیت‌های غیر قانونی و هماهنگ گروهی منسجم از اشخاص است که با تبانی با هم و برای تحصیل منافع مادی و قدرت، به ارتکاب مستمر (عمل) مجرمانه شدید می پردازند و برای رسیدن به هدف از هر نوع ابزار مجرمانه(ای) نیز استفاده می کنند.[3]

۲-۱-۲ویژگی‌های جرم سازمان یافته

از تعاریف پیش گفته خصایص ده گانه‌ای در خصوص جرم سازمان یافته به دست می‌آید:

۱)ساخت گروهی دارند؛

۲) قدرت مرکزی دارند؛

۳) استقرار و تداوم دارند؛

۴) وجود قواعد و مقررات ضمنی و الزام آور برای اعضاء؛

۵) وجود بزهکاران حرفه‌ای؛

۶) روشمند بودن عملیات یا نظام مند بودن آنها؛

۷) پاسخ دادن به تقاضای خدمات یا اموال نامشروع؛

۸) انحصاری گری؛ یعنی تلاش برای انحصاری کردن کارهای خود؛

۹) توسل به خشونت و نیرنگ؛

۱۰) تقسیم وظایف.

---

[1].این جرایم عبارت اند ازعضویت در گروه مجرمانه سازمان یافته، تطهیر درآمدهای به دست آمده ازجرم، فساد اداری و کارشکنی در اعمال عدالت نسبت به جرایم سازمان یافته

[2].زرخ ، احسان ، پیشین ،ص۵۰

[3].شمس ناتری ، محمدابراهیم ، ۱۳۸۰ **بررسی سیاست کیفری ایران درقبال جرایم سازمان یافته با رویکرد به حقوق جزای بین المللی** ، رساله دکتری ، تهران، دانشگاه تربیت مدرس ،ص ۱۳ به بعد .

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

با این تفاسیر و با توجه به تعاریف فوق که مهم ترین تعاریف ارائه شده در این خصوص هستند، به نظر می‌رسد ، که هیچ یک تعریف جامع ومانعی محسوب نمی‌شوند و هر یک به جهتی دچار ایرادات اساسی هستند.[۱] جرم سازمان یافته دچار تغییراتی شده است که از جمله آنها از دست دادن برخی از خصیصه های پیش گفته چون استقرار و تداوم، توسل به خشونت و ... است. علاوه بر این، در حال حاضر در میان جرم شناسان معاصر بحث از جرم سازمان یافته دولتی و شبه دولتی[۲] مطرح شده، که البته در منابع جرم شناسی ما به آنها اشاره نشده است.[۳]

با این تفاسیر اهمیت این مسئله که چگونه می بایست با جرم سازمان یافته سایبر برخورد نمود و اصولاً می توان قائل به تحقق چنین جرمی بود یا خیر و آیا امکان انطباق نظریات موجود در خصوص جرم سازمان یافته در جهان واقعی در فضای سایبر وجود دارد؟

علاوه بر این آیا جرم سازمان یافته سایبری وجود خارجی دارد و یا اینکه تنها با گونه‌هایی از جرایم سایبری سازمان یافته مواجه‌ایم؟ اینها سؤالاتی است که در این نوشتار در صدد پاسخگویی به آنها هستیم و چینش مطالب نیز بر همین اساس است.

۲-۱-۳ جرم سازمان یافته مجازی

درابتدای بحث پیرامون جرم سازمان یافته مجازی این سؤال مطرح می‌شود که آیا جرم مجازی ماهیتی مستقل از سایر جرایم دارد یا اینکه همان جرایم سنتی با شیوه‌ای مدرن است؟

در این موضوع استدلال های متفاوتی با این نگرش ارائه شده است که: هر گونه بحث درباره جرم سایبر با مراجعه به مسائل پیچیده جرم شناسی و خصوصاً این سؤال که آیا منظور از آن (جرم

---

[۱].زرخ ، احسان ، پیشین ،ص۵۱

[۲]. (Quasi) Governmental Organized crimes

[۳].برای مطالعه بیشتر در این مورد می توانید به این منابع رجوع کنید:

Bartl Oniej Kaminski, Econmic Transitioninrussia and The New States Of Eurasia, M.E.Sharpe publisher,۱۹۹۶.

James B.jacobs,mobsters,unions, and feds, new York university press,۲۰۰۶.

Joseph albini,state and governmental organized crime:threats to interntional security,international law and administration of justice,the interdisciplinary roots and branches of criminology,۵۷th annual meeting,the American society of criminology,۲۰۰۵.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مجازی) ضرورت شکل جدیدی از جرم است یا مربوط به مباحث نظری جرم شناسی است، شروع می‌شود.[۱]

در همین راستا استدلال شده است که: "جرم سایبر به صورت ساده، همان شراب کهنه است که در بطری های جدید ریخته‌اند." در واقع گرابوسکی[۲] با این دیدگاه فضای سایبر را وسیله‌ای نوین برای ارتکاب جرایم قدیمی می‌داند و قائل به وجود جرایم جدید که به عبارتی مجازی محض[۳] باشند، نیست؛ چرا که وی به فضای سایبر به عنوان وسیله‌ای در جهت ارتکاب جرایم سنتی و موجود می نگرد و به این موضوع که فضای سایبر محلی برای شکل گیری جرایم خاص خود باشد، نیست.

در تکمیل این دیدگاه ها ادعا شده است که: "جرم سایبر در حال گسترش است و این بدان معنا نیست که بگوئیم در واقع جرایم جدید به وجود آمده‌اند بلکه بهتر است بگوئیم شیوه‌های جدیدی برای ارتکاب جرایم موجود به دست آمده و البته شیوه‌های بهتری نیز برای پی بردن به آنها ایجاد شده است.[۴]

در واقع، این دسته از نویسندگان که البته جزو برجسته ترین نویسندگان حقوق کیفری سایبر نیز هستند، برای جرم سایبر ماهیتی مستقل از جرایم موجود در فضای مادی، متصور نیستند؛ چرا که اندیشه ایشان بر این اساس استوار است که نمی توان قائل به تحقق جرمی خارج از جهان واقعی بود و تمامی جرایم به نحوی با فضای مادی در ارتباط‌اند و آثارآنها در این محیط نمود ملموس می یابد، از اینرو به فضای سایبر به عنوان متحول کننده جرایم مادی می نگرند تا شکل دهنده نسل جدیدی از جرایم؛ البته دیدگاه‌های آنان مبتنی بر ترسی است که از پذیرش استقلال فضای سایبر در میان بشر امروز یافت می شود، چرا که نا آگاهی از ابعاد گسترده این فضاکه آن را چون سیاه چاله ای تاریک می نماید ، سبب پرهیز حقوقدانان ازپذیرش این فضا وبالتبع جرایم ارتکابی درآن شده است و تا آنجا که ممکن است سعی در انطباق آن با فضایی دارند که در آن زندگی می کنند واز این رو در تمامی

---

۱. Majid Yar.(۲۰۰۵),The novelty of cybercrim: An assessment in Light of routine activity theory European Journal of Criminology.
۲. Grabosky,Peter(۲۰۰۰),Computer Crime:A Criminological Overview, p.۱۹
۳. Pure cyber crimes
۴. Nisbett,C(۲۰۰۲) .New directions in cyber crime .White Paper,QineticQ

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

موارد با نگاه مادی و ملموس به جرایم می نگرند و سعی برآن دارند تا این جرایم را به تبع برخی از آثار مادی آنها، از حالت مجازی و فرامادی خارج و با معیارهای مادی منطبق نمایند.[1]

این دیدگاه‌ها که در خصوص کلیت جرم سایبر و به تبع آن جرم سازمان یافته مجازی وجود دارند، در واقع نشأت گرفته از برداشت‌های متفاوت حقوقدانان ازماهیت جرایم مجازی است که به مهم ترین علل آن اشاره شد، هر چند که در حال حاضر بحث از وجود یا عدم وجود جرایم مجازی محض تا حدودی مشکل می نمایند، لکن به نظر می رسد پس از این همه بحث و جدل که میان حقوقدانان روی داده است، دیگر مجال پرداختن به مسائل وجودی و عدمی این جرایم از میان رفته باشد و می بایست قائل به وجود جرم مجازی محض باشیم، هر چند که این تعارضات درنام گذاری[2]جرایم این حوزه نیز به چشم می خورند و البته به نوعی می توان آنها را شدت گرفته از پذیرش صریح و یا ضمنی این جرایم دانست.

حال آنکه اندیشه همه آنها یک چیز و آن جرمی ارتکابی در خارج از جهان مادی است و حال آنکه تمامی آنها از یک واقعیت حقایق گوناگونی را بسته به توان خویش درک می کنند و در واقع همان مثال فیل درکلام مولانا است که درتاریکی هرکدام قسمتی ازبدن فیل را لمس می کردند وآن را ملاک قرار می دادند در حالی که همه آنها در مجموع یک چیز که همانا فیل باشد را لمس کرده‌اند، که این مثال کاملاً بر دیدگاه‌های مطروحه در خصوص جرم سایبر ساری و جاری است.

با این تفاسیر جرایم سایبر با پیشوند سازمان یافته منجر به استنباط جرم سازمان یافته سنتی می شوند، لکن به مجرمین عادی که از فضای سایبر به شیوه سازمان یافته استفاده می کنند باز می گردد. بر همین منوال به نظر می رسد که برخورد با گروه‌های مجرمین سایبر درست به منزله آن است که آنها به لحاظ اندازه، پیچیدگی، ساختارو زمان، درست معادل همتایان سنتی خویش که جنبه مجازی ندارند هستند و این امر به گروه‌های مجرمین سایبراجازه می دهد که مشابه تحول و توسعه سازمانی را داشته باشند که گروه‌های جرایم سازمان یافته سنتی از خودشان نشان می دهند.

---

[1].زرخ ، احسان ، پیشین ،ص۵۳

[2].در قسمت قبلی و در بحث معمای نامگذاری به تفصیل این موضوع مورد بررسی قرار گرفته است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

حال به این سؤال می رسیم که آیا جرم سایبر به وسیله گروه‌های سازمان یافته سنتی واقع می شود یا صرفاً به شیوه سازمان یافته در محیط آن لاین ارتکاب می یابد؟[1]

به هر حال به نظر می رسد که جرم سایبر وقتی سازمان یافته است که عامل آن در راه رسیدن به نمونه یک هکر تنهای اولیه متوقف شده باشد، چرا که بدل شدن به یک هکر برجسته هدف غایی تمامی طبقات هکر[2] است و اگر در این مسیر باشکست روبرو شوند، به سوی گروه‌های منزوی هکرها گرایش پیدا می کنند[3]. با این وصف اگر فعالیت غیر قانونی توأم با هماهنگی، تنها عامل جرم سازمان یافته به حساب آید، درآن صورت به نظر می رسد که هر شکلی از رفتار مجرمانه که مستلزم درجاتی از برنامه ریزی باشد، نوعی جرم سازمان یافته به حساب می‌آید.

شورای اروپا چنین استدلال کرده که: داده‌ها و اطلاعات درباره ارتباط میان جرم سازمان یافته و جرم سایبر هنوز ناچیز است و به ما اجازه نمی دهد که بتوانیم تجزیه و تحلیل مطمئنی از آن داشته باشیم.

با وجود این دیدگاه‌ها به نظر می رسد که همچنان نگرشی عمیق تر در خصوص جرایم سازمان یافته مجازی می بایست مطمح نظر قرار گیرد. چه آنکه اداره اطلاعات مرکزی امریکا (FBI) در گزارش

---

[1]. زرخ ، احسان ، پیشین ،ص۵۶

[2]. هولینگر (Holinger) بر مبنای درجه بندی پیشرفت، از مبتدی تا نخبهٔ فنی جرایم رایانه‌ای، هکرها را به سه دسته تقسیم کرد: دزدان،(pirates) مرورگران(browsers) و رخنه گران(crackers) دزدان، هکرهایی هستندکه کمترین تبحر فنی دارند و فعالیت‌هایشان به نقض حق نشر از طریق دزدی نرم افزار محدود می شود.
مرورگران افرادی با تبحر فنی متوسط هستند که به طور غیر مجاز به فایل‌های سایرین دسترسی می یابند، اما معمولاً به فایل‌ها آسیب نمی زنند یا کپی نمی کنند. رخنه گران که چیره دست ترین هکرها هستند، از توانایی فنی شان برای کپی کردن فایل‌ها یا صدمه زدن به برنامه‌ها و سیستم‌ها سوء استفاده می کنند. شرکت مک آفی(mcafee) هکرها را به دو دستهٔ کلاه سفید(Hat white) و کلاه سیاه (black Hat) تقسیم می کند.
Fitch,Cynthia (۲۰۰۳), crime and punish meant: The psy chology of hacking in new millennium, retrieved from: http://www.giac.org/practical/gsec/cynthia-fitch -gsec.pdf.

[3]. هکرهای تنهای اولیه، در واقع پیشتازان هک هستند که به نوعی سمبل هکرهای فعلی اند که از جمله آنها می توان به مایک میتنیک اشاره نمود.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

خود درباره یکی از گروه‌های جرم سازمان یافته مجازی بیان داشته است که: کاردل پلانت[1] درست مانند مافیای ایتالیا خود را قاعده مند و سازماندهی نموده است.

پذیرش درگیری گروه‌های مجرمانه سازمان یافته سنتی در فعالیت‌های جنایی مجازی، دستگاه‌های مجری قانون را در یک موضع ناخواسته قرارداده که مجبور شوند جرایم مجازی پیچیده تر را همچنان در چهار چوب محیط فیزیکی اجرای قانون و به گونه‌ای برجسته مورد بررسی و تحقیق قرار دهند.

در واقع برخلاف جرایم سازمان یافته قرن ۲۰جرم سازمان یافته مجازی قرن ۲۱ مستنداً بیشتر شبیه پذیرش و سازگار نمودن جرم سنتی به فناوری جدید است تا خلق جرم جدید با ساختاری جدید.[2]

بخش دوم :شناخت جاسوسی سایبری

جاسوسی سایبری در تعبیری ساده و در نگاه نخست، همان جاسوسی است که در فضای سایبر رخ می دهد. از این منظر، جاسوسی سایبری چیزی نیست که ارزش شناسایی داشته باشد؛ زیرا به تبع شناخت و بررسی جاسوسی، جاسوسی سایبری نیز شناخته می شود و چون پیش از این، مطالب عدیده و جستارهای فراوان درباره جاسوسی به رشته تحریر درآمده یا گفته‌های بسیاری در این باب بر زبان برآمده، دیگر نیازی به طرح مجدد یک موضوع تکراری نخواهد بود. هرچند این ادعا درست است ولی باید گفت که فرض بر نو بودن جاسوسی سایبری و فرض بر متفاوت بودنش با جاسوسی است و از این رو، چیزی که دو ویژگی جدید بودن(نسبت به محیط واقعی) و متفاوت بودن (نسبت به خود جاسوسی) را یدک می کشد باید شناخته شود.

جدید بودن جاسوسی سایبری به اعتبار جدید بودن بستری است که در آن ارتکاب می‌یابد ولی متفاوت بودن آن با خود پدیده جاسوسی به معنای تمایز در برخی شرایط و اجزای رکن مادی جرم یا به تعبیر دقیق‌تر رفتار سرزنش پذیر است وگرنه چنان نیست که جاسوسی در یک سرزمین گام نهاده و جاسوسی سایبری در سرزمینی دیگر. برعکس، جاسوسی سایبری چهره نوین خود جاسوسی است.

---

[1]. Cardelplanet(یک گروه هکری سایبری)

[2]. زرخ ،احسان ، پیشین، ص۵۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۲-۲-۱ انواع جاسوسی اینترنتی

پیش از پرداختن به انواع جاسوسی ها باید ذکر کنیم که این تفکیک انواع جاسوسی بر مبنای روش های ارتکاب جرم انجام شده است.یعنی ملاک تفکیک نوعی از نوعی دیگر،روش مورد استفاده بوده است و می بینیم که زمانی که جاسوسی از طریق نصب برنامه بر روی کامپیوتر در فضای مجازی رخ می دهد دقیقاً نقطه ی تفکیک ۲ نوع عمده ی جاسوسی اینترنتی و رایانه ای می باشد.

باتوجه به روش ارتکاب جاسوسی به ۴ نوع آن اشاره می کنیم.[۱]

۱)"رایج ترین راه جاسوسی رایانه ای،کپی کردن فایل های داده است به خصوص در زمینه ی برنامه هایی که به تعداد انبوه تولید و به فروش می رسند.در خصوص برنامه هایی که به تعداد انبوه تولید نمی شوند و دیگر داده ها،کپی کردن عمدتاً به وسیله ی برنامه های کمکی یا به وسیله ی برنامه های خود ساخته،صورت می گیرد."

۲)نوع دیگر جاسوسی رایانه ای،جاسوسی سنتی است که آن هم به دو دسته ی جاسوسی شخصی سنتی ،جاسوسی فنی سنتی تقسیم می شود:

الف)جاسوسی شخصی سنتی:روش های این نوع جاسوسی عبارتند از "رشوه دادن به کارمندان یا اخاذی از آنها،فرستادن مأمور در قالب کارمند تازه وارد برای دوره های کوتاه کاری(این روش به سلام-خداحافظ معروف است) یا به وسیله ی مصاحبه با کارمندان شرکت مورد نظر که در جستجوی کارجدید به سراغ آگهی های دروغین می آیند و در ضمن مصاحبه وضعیت فعلی کارشان راهم توصیف می کنند."

ب) جاسوسی فنی سنتی:"روش های فنی سنتی تحصیل اطلاعات ذخیره شده درکامپیوترنیز بر مبنای ۱.سرقت فایل های داده،۲.اتصال یک کابل مخفی به کامپیوتر مورد نظر یا۳. نصب بخش انتقال دهنده در سیستم کامپیوتر مورد نظر صورت گرفته است.روش دیگر سوءاستفاده از داده هایی است که تاریخ اعتبار آنها گذشته است،شامل موارد:۱.جستجو در سطل زباله برای یافتن برگه های چاپ شده یا کاغذ

---

[۱]. حسینی فرد ، آیدا، مطالعات فضای مجازی ،http://cyberhosseinifar.blogfa.com

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

کاربن هایی که در تهیه ی چند نسخه از یک نوشته به کار رفته است ۲.نوترها یا دیسکت های که برای مبادله ی حامل های داده به کار رفته ولی محتویات آنها کاملاً محو نشده است ۳.برداشتن داده هایی که کارمند بعد از اتمام کارش در قسمت ذخیره داده های مورد نیاز برای مراجعه های بعدی کامپیوترش ذخیره می کند."

۳)برداشت داده از طریق فرکانس:دستیابی به میدان های الکترونیکی و فرکانسی تولید شده ی پایانه های رایانه ای و شنود و تحلیل و حتی ضبط آنها با استفاده از امکانات استاندارد صوتی و تصویری که با قیمت ارزان به دست می آید به راحتی در یک ماشین نزدیک مرکز رایانه قابل جاسازی است.[۱]

۴)استفاده از سیستم های مخابراتی:در این نوع،نفوذ به مراکز داده جهت دسترسی غیر مجاز به اطلاعات به روشهای خاصی صورت می گیرد: ۱.استفاده از گذرواژه (به ویژه اگرمدت زمان طولانی تغییر نکند) ۲.استفاده از تماسهای تلفنی دروغین و۳.شنود و استراق سمع از طریق جمع آوری میکروبهای سرگردان ارسالی از ماهواره ها یا ایستگاه های زمینی و نفوذ به کامپیوترهای حاوی داده ها.

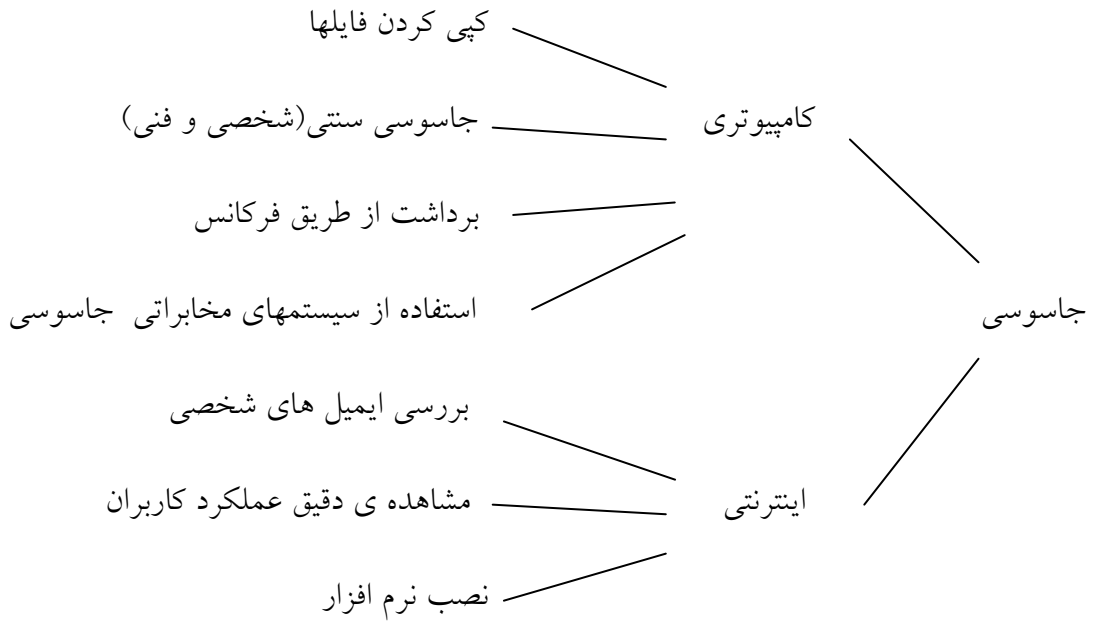
و نوع پنجم جاسوسی که در واقع جاسوسی اینترنتی است و خود دارای انواع و شیوه های متفاوت است:

۵)کسب اطلاعات از طریق معرفی برنامه هایی که از راه نصب نرم افزارها و یا حین گردش افراد در محیط وب وارد کامپیوترشخصی آن ها شده وتازمانی که کاربر به شبکه جهانی وصل است، اطلاعاتی را که روی هارد دیسک او ذخیره شده است برای پایگاههای مطلوب خویش می فرستند.

[۱]. حسینی فرد ، آیدا، پیشین

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

پس تفکیک انواع جاسوسی به این شکل می باشد.[1]



۲-۲-۲جاسوسان سایبر

زیبر به ۳ دسته از جاسوسان سایبر اشاره می کند:

۱)کارمندان نه چندان وفادار

۲)کپی برداران برنامه های رایج یعنی کاربران کامپیوتر و دلالان نرم افزار

۳)هکرها (زیبر در مبحث دسترسی غیر مجاز به سیستمهای پردازش داده ها – که به عنوان یک جرم مجزا به آن اشاره می کند – در مورد هکرها چنین می گوید "دسترسی غیر مجاز ناب به سیستمهای پردازش،عمدتاً به وسیله ی هکرها صورت می گیرد.")[2]

۲-۲-۳ خصوصیات رفتاری مرتکبین جرائم رایانه ای و انگیزه آنان

روشهای گوناگونی برای دسته بندی وبررسی مرتکبین جرایم رایانه ای وجود دارد.دراین مبحث مرتکبین جرائم رایانه ای باتوجه به انگیزه آنها تقسیم می شوند .

مرتکبین جرائم کامپیوتری شامل طیف گسترده ای از افراد می باشند.نوجوانان ، دانشجویان ، کارمندان ناراضی ، خلافکاران وتروریست های بین المللی وغیره که منحنی سنی مجرمین کامپیوتری سنی بین

---

[1]. حسینی فرد ، آیدا، پیشین

[2].اولریش ، زیبر، پیشین ، ص۶۸

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۱۰ تا۶۰ سال رانشان می دهد ودامنه مهارت آنان از تازه کار تاحرفه ای گسترده است .مرتکبین جرائم کامپیوتر باتوجه به نوع انگیزه آنها به ۳ گروه تقسیم می شوند.

۱)مزاحمان کامپیوتری

۲)خلافکاران

۳)خرابکاران[۱]

انگیزه گروه اول صرفاً دستیابی به سیستم های کامپیوتری واطلاعات موجود درآن می باشدواکثراً جوانانی هستند که برای تفریح دست به این کارمی زنند.

انگیزه دسته دوم کسب منفعت مالی است وعمدتاً دردومقوله جاسوسی وکلاهبرداری فعالیت دارند که روز به روزبرجمعیت آنها افزوده می شود .

انگیزه دسته سوم تنها صدمه زدن وخسارت به دیگران است وافرادی هستند که دارای اختلالات روانی بوده وقصد انتقام جویی دارند.[۲]

قطعاً به دنبال هر عملی انگیزه و قصدی وجود دارد.جاسوسی هم مستثنی نیست و تمام جاسوسان با انگیزه و هدفی به دنبال کسب اطلاعاتی که اجازه ی دستیابی به آن را ندارند هستند.

۲-۲-۴ علل گرایش به جاسوسی اینترنتی

۱. هزینه : سالانه هزاران دلار برای پشتیبانی از جاسوسان درخارج از کشورهزینه می گردد.

۲.حفاظت:ارتباطات الکترونیک اگربه خوبی پنهان شده یاتحت پوشش انجام گیردبسیاربرترازارتباطات بی سیر،نامرئی نویسی،ناقلهای مرده یا قرارهای حضوری می باشد چراکه خطر کشف تمام این روشها از ارتباطات الکترونیک بیشتراست .

۳.سرعت : هک کردن واقعاً سریع وآنی انجام می شود ، ارسال پیام های جاسوسی ازطریق اینترنت فقط چند ثانیه طول می کشد .

۴.دسترسی آسان : کلیه اطلاعات رامی توان از طریق اینترنت ، بسیار سریع وباحداقل هزینه برای همگان ویاگروه مشخص دسترس پذیر نمود.[۳]

---

[۱].Vandals

[۲]. باستانی ، برومند، پیشین ،ص ۳۳

[۳].بوجار، الیاس، ۱۳۸۸،**جرم جاسوسی با توجه به فناوری نوین**، تهران، دانشگاه پیام نور مرکز تهران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی ،ص ۱۱۴

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بخش سوم : شناخت جاسوسی سنتی

یکی ازمصادیق بارزوقدیمی جرایم علیه امنیت جرم جاسوسی است،که معمولاً یک جرم «سازمان یافته»[۱] و در عین حال «فراملی»[۲]می باشد چرا که در آن اطلاعات حیاتی یک کشور از طریق یک نظام سازمان یافته و منابع انسانی نه ابزاری مثل ماهواره های اطلاعاتی کشورها در اختیار کشوریا کشورهای دیگر قرار می گیرد .

نظامی را که جاسوسی در آن ارتکاب می یابد می توان به یک هرم تشبیه کرد که در آن کنترل و هدایت از رأس هرم نسبت به پایین انجام می گیردو اطلاعات بر عکس،از قاعده هرم به بالا داده می شود .

به دلیل ماهیت فراملی جرم جاسوسی برخی از معاهدات و کنوانسیونهادرسطح بین المللی به این جرم ـ مخصوصاً در حالتی که در زمان جنگ ارتکاب می یابد ـ پرداخته اند که، از آن جمله می توان به کنوانسیون چهارم لاهه در مورد قوانین و عرف جنگهای زمینی[۳]، منعقده در سال ۱۹۰۷ م . اشاره کرد که به مسئله جاسوسی در زمان جنگ و شیوه رفتار با جاسوسان از سوی دولت متخاصم پرداخته است . پروتکل دوم کنوانسیونهای ۱۹۴۹ م . ژنو[۴]در مورد حقوق بشر نیز که در هشتم ژوئن ۱۹۷۷ به اتفاق آراء تصویب شد به موضوع جاسوسان و رفتار با آنان جدا از مسئله اسرای جنگی می پردازد.

وقتی سخن از جاسوسی به میان می آید ذهن عامه مردم – که اطلاعات کمی از جزئیات این جرم دارند – بیشتر متوجه شبکه ها و سازمانهای جاسوسی معروف کشورهای مختلف از جمله :(سی . آی . ای) (سیا)[۵] در آمریکا ، (ام .ای . پنج) و(ام . ای . شش)[۶]در انگلستان ، (موساد) در اسرائیل (کا.گ. ب) در اتحادجماهیر شوروی سابق می شود برخی از این سازمانها ، مثل سیا ضمن استخدام جاسوس تا حدزیادی به شکل خود مختار از قوه اجرائیه عمل کرده و گاهی حتی دست به عملیات هم می زنند که نمونه بارز آن اقدام همین سازمان در کودتای ۲۸ مرداد ماه ۱۳۳۲ در ایران علیه دولت

---

۱. organized Crim
۲. transnational
۳. FourthHagueConvetiononntheLawsandCustomsWaronland
۴.Geneva Convetions
۵. C.I.A
۶. M.l.5 و M.l.6 به ترتیب ، به مسایل امنیتی داخلی و خارجی می پردازد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دکتر مصدق و آموزش شرکت کنندگان در قیام سال ۱۹۵۶ م . مجارستان توسط (ام . ای . شش) انگلستان بود.[۱]

با این حال نباید تصورکرد که جاسوسی در سطح دنیا محدود به این سازمانها می شود بلکه این جرم در کشورهای مختلف وتوسط افراد و سازمانهای گوناگون ارتکاب می یابد و در دههٔ هشتاد میلادی ، که به دلیل رشد ارتکاب این جرم در این دهه آن را (دهه جاسوسی)[۲] نامیده اند ، حدود پانصد کتاب در مورد این جرم توسط مورخان ، روزنامه نگاران تحلیل گران نظامی ، سیاستمداران و تا حد کمتری حقوقدانان وجرم شناسان نگاشته شده است .

۲-۳-۱ انگیزه جاسوسی

انگیزه جاسوسان برای ارتکاب این جرم متعدد است،برخی مزدورهستند و به انگیزه های مالی و از روی حرص و آز دست به ارتکاب این جرم می زنند که شاید بیشتر تعداد جاسوسان را این افراد تشکیل دهند. نمونه این افراد در آمریکا ،الدریچ آمس[۳] بوده که در سال ۱۹۹۴ . م . در سن ۵۲ سالگی در حالی که ۳۲ سال برای سیا کارکرده وپدرش نیز جزوکارکنان سیا بود ، به اتهام ارتکاب جاسوسی به نفع روسیه از سال ۱۹۸۵ . م . دستگیر و به حبس ابد محکوم شد .

وی بالاترین مقام سیا که تاکنون به اتهام جاسوسی دستگیر شده،بوده است . هر چند شاید هیچگاه نتوان میزان دقیق خساراتی را که وی به آمریکا وتلاشهای امنیتی آن وارد کرده است تخمین زد ولی حداقل یک مورد آن کاملاً مشخص می باشد و آن این که بر اثر اطلاعات داده شده توسط این شخص ، یازده جاسوس آمریکا درروسیه بین سالهای ۱۹۸۵.م. تا ۱۹۸۷.م. دستگیر و اعدام شدند که

---

[۱]. به خبر زیرازروزنامه ابرارمورخ۱۳۷۵/۸/۶توجه کنید : (روزنامه ایندپیندیت چاپ لندن در چهلمین سالگرد سرکوب قیام مجارستان از سوی اتحاد شوروی سابق در سال ۱۹۵۶ میلادی فاش کرد که برخی از افرادشرکت کننده در آن قیام توسط نیروهای جاسوسی انگلیس آموزش دیده بودند.) این روزنامه درگزارش خودبه نقل از یک افسر عضو سازمان (ام آی شش) انگلیس افزود: این آموزشهااز سال ۱۹۵۴ میلادی با انتقال برخی از مجاریها به منطقه ای در اتریش که تحت تسلط ارتش انگلیس قرارداشت آغاز شد . وی اضافه کرد:ما آنها را به کوهستانها بردیم وبه آنان آموزش عملیات براندازی دولت را دادیم.این افسر انگلیس گفت : سپس ما به آنان آموزش کار با مواد منفجره و سلاح داده وآنان را برای قیام آماده ساختیم (توضیح آن که در جریان این قیام یازده روزه ۲۵۰۰نفر کشته ودویست هزارنفربه غرب گریختند.)

[۲]. Espionage Decade
[۳]. Aldrich Ames

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

یکی از آنهاژنرال دیمیتری پولیاکوف[1]،افسر عالی رتبه سازمان اطلاعات نظامی روسیه بود .

انگیزه دیگر جاسوسان برای ارتکاب این جرم به دلایل عقیدتی وایدئولوژیک بر می گردد ، یعنی این که جاسوس خود را از لحاظ فکری و عقیدتی به کشوردیگری غیراز کشور محل تولد یا اقامت خود وابسته می داند و در نتیجه برای آن کشورجاسوسی می کند. جاسوسیهای حزب توده در ایران به نفع شوروی و بلوک شرق سابق ،ازجمله، به این وابستگی فکری به اردوگاه شرق و طرز فکر مارکسیستی اعضای این حزب برمی گردد .در آمریکا مواردی از این دست مشاهده شده است . از جمله این که اسراراتمی آمریکا پس ازجنگ جهانی دوم توسط افرادی که به نظام مارکسیستی معتقدبودند دراختیار شوروی سابق قرار گرفت[2] برخی از این افراد در آغاز پولی هم قبول نمی کردند.

اهمیت این جاسوسی ازآن جهت بودکه درآن زمان این اطلاعات اتمی منحصراًدراختیارآمریکاقرار داشت.

عکس موضوع هم صادق بوده است که در مواردی افراد در روسیه به دلیل سرخوردگی از نظام مارکسیستی شرق و علاقه به نظام لیبرالیستی غرب علیه شوروی وبه نفع آمریکا جاسوسی کرده اند. ژنرال دیمیتری پولیاکوف ،که قبلاً از او نام برده شده ، معمولاً جزو این دسته قرار داده می شود[3].

گاهی انگیزه جاسوسان از جاسوسی انتقام گیری است ،یعنی این که فرد جاسوس به دلیل مشکلاتی که یک کشور برای وی ایجاد کرده اند و برای انتقام گرفتن از آن کشور ، اطلاعات کشور مذکور را در اختیار دیگران قرار می دهد . نمونه این افراد ادواردلی هووارد[4]است که کارمند سیا بود و به دلیل خودداری از منتقل شدن به مسکو و دلایل دیگر از سیا اخراج شد.اوسپس اطلاعات خود را در اختیار کا.گ. ب.قرار داد .

در مواردی دلیل مبادرت به جاسوسی گرفتار شدن در جریانات رمانتیکو عشقی است .

(کا.گ .ب) در این موارد مشهور بود که دختران زیبایی را برسر راه مأموران خارجی که به اطلاعات آنان نیاز داشت قرار می داد و این دختران بابرقراری رابطه با اشخاص مذکور اطلاعاتی راازآنها

---

[1]. General Dimitei polyakov

[2].این کارازجمله،ازسوی Julis Rosenberg و Ethel Rosenberg و Klaus Fuchs و Allen Nunn may انجام می گرفت فرد اخیرالذکر عضو تیم اتمی بریتانیا بود و به همراه نفر سوم در آغاز ازگرفتن پول امتناع می کردند.

[3]. F.E. Hagan , Political crim P.١٢٦

[4]. Edward lee Howard

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بدست می آوردند. از جمله دوکارمند نظامی سفارت آمریکا در روسیه از این طریق به دام جاسوسی گرفتار شده بودند .

در برخی از مواقع این زنان هنگام روابط و مراودات عاشقانه ،عکسهای نامناسبی را به طور محرمانه از فرد مورد نظر گرفته و در اختیار سازمان جاسوسی متبوع خود قرار می دهند. سازمان مذکور نیز با در دست داشتن این عکسها به عنوان برگ برنده ، شخص مربوطه را مجبور به همکاری می کند.[۱]

گاهی جاسوسی ناشی از فریب خوردن جاسوس است ، یعنی این که وی تصور می کند برای یک سازمان و یک کشور کار می کند در حالی که در واقع از اطلاعات اوبرای سازمان و کشور دیگری استفاده می شود.[۲]

مثال بارز این مورداستفاده ادوین ویلسون[۳] ،کارمندسابق سیابودودرسال۱۹۸۰ .م .دستگیرشد،وی از افرادی بودکه به عنوان جاسوس برای لیبی درحالی که به آنان وانمود کرده بود که اطلاعات آنها مورد استفاده سیا قرار می گیرد، فعالیت می کرد . وی بیش از سی نفر را به این طریق جذب کرده بود[۴].

در برخی از موارد جاسوسی توسط کسی انجام می گیرد که به دلیل مشکلاتی که در کشورخود با آنها مواجه است به کشور دیگری گریخته یا در کشور دیگری ماندگار شده و اطلاعات خود را در اختیار مأموران کشور مذکور می گذارد. برخی ازمأموران سابق (کا.گ.ب) پس از مدتی اقامت در کشورهای غربی و یافتن علائق جدید،ماندن در آن کشورها را به بازگشت به روسیه ترجیح می دادند و با اخذ اجازه اقامت دراین کشور اطلاعات خود را در اختیارآنها می گذاشتند .

گاهی ارتکاب جاسوسی به مسائل روانی و شخصیتی باز می گردد جاسوس با انجام این کار احساس قدرت وهیجان کرده وازاین طریق ارضاء می شود.ازجمله کریستوفربویس[۵] دانشجوی۲۱ ساله آمریکایی،که یک کار نیمه وقت مرتبط باتجهیزات مخابراتی ماهواره ای نیزبه دست آورده بود، این اطلاعات رابه روسهافروخت.وی همواره میل داشت که خودرایک ماجراجوشبیه دزدان دریایی توصیف کند.[۶]

---

۱. F.E. Hagan , IbId . P .۱۲۸-۱۳۰

۲.میرمحمد صادقی، حسین،پیشین ،ص ۸۲

۳. Edwin Wilson

۴. F.E. Hagan , IbId, P.۱۳۰

۵. Christopher Boyce

۶. F.E. Hagan ,IbId, p.۱۲۸

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

آن چه در بالا اظهار شد به شناخته شده ترین انواع جاسوسان وانگیزه های آنها اشاره دارد ،ولی قطعاً می توان موارد متفرقه ای را یافت که تحت هیچیک از این فقرات قرار نمی گیرد .

برای مثال برخی از جاسوسان را به عنوان شبه جاسوس می شناسند که بطور علنی مثلاً با انتشار نشریه و کتاب ، اطلاعاتی را دراختیار بیگانگان قرار میدهند. این افراد معمولاً از سیستم خود ناراضی ولی برخلاف جاسوسان ایدئولوژیک ، لزوماً علاقه ای به سیستم خاص دیگری هم ندارند. از جمله این افراد می توان از فیلیپ آگی[۱] نام برد که باانتشار کتابی اطلاعات ذی قیمتی را در مورد عملیات محرمانه و مأموران سیا در آمریکای لاتین در اختیار کوبا و کشورهای بلوک شرق قرار داد.[۲]

طریقه برخورد کشورها با جاسوسان متفاوت است گاهی جاسوس ،به دلیل برخورداری از مصونیت دیپلماتیک ،عنصرنامطلوب اعلام و اخراج می شود و گاهی وی دستگیر و بلافاصله مجازات می شود و گاهی نیز با دادن اطلاعات غلط به او سعی درگمراه کردن کشور مورد نظر می شود .

برخی از کشورها نیز سعی می کنند جاسوس را ، به جای مجازات کردن، به یک جاسوس دو جانبه تبدیل نمایند وازاو بخواهند که به آنها اطلاعات بدهد و درمقابل ، برای لونرفتن او ، گاهی اطلاعات به اصطلاح سوخته ای را نیز جهت ارائه به کشوردیگر دراختیار وی می گذارند .
بدین ترتیب در حالی که کشور اول این فرد راجاسوس خود می داند وی در واقع برای کشور دوم جاسوسی می کند. هارولد نیکلسون ، استادی که در آموزشگاه تربیت جاسوس برای سازمان سیا روشهای جاسوسی تدریس می کرد ، را می توان از جمله این افراد دانست .
مأموران سازمان اطلاعات مرکزی آمریکا (سیا) بانصب دوربینهای مخفی در دفترکارنیکلسون متوجه شده بود که وی با دستگاه مخصوصی از اسناد محرمانه در زیر میزش عکسبرداری می کند. در جریان تحقیق روشن شد که وی هنگام انجام مأموریت در مالزی به دام جاسوسان روسیه افتاده و جاسوس آنان شده است.[۳]

---

۱. Philip Agee
۲. F.E. Hagan ,IbId, p.۱۳۰

۳.میرمحمد صادقی، حسین،پیشین ،ص ۸۵-۸۳

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بخش چهارم : شیوه های دست یابی به اطلاعات وروشهای جاسوسی

جاسوسی رایانه ای درگام نخست متضمن نفوذ یا دسترسی غیرمجاز به سیستم رایانه ای یا حامل داده است که اطلاعات طبقه بندی شده یا داده های حساس درآن ذخیره یا پردازش می شوند. بنابراین ، معمولاً هک[۱] یا نفوذ به سیستم رایانه ای مقدمه جاسوسی است . اما دستیابی به سیستم وجمع آوری اطلاعات می تواند به شیوه های مختلفی انجام شود که مهم ترین آنها عبارتنداز:[۲]

۲-۴-۱ مهندسی اجتماعی[۳]

این حملات شامل روند نفوذ به سیستم های رایانه ای با بکارگیری حیله های گوناگون درخصوص افرادجهت افشای کلمات عبورواطلاعات مربوط به نکات آسیب پذیر شبکه می شود.[۴] مهندسی اجتماعی نوعی نفوذ غیرمجاز یاهک شفاهی به شمارمی رود که درآن مرتکب باتماس تلفنی یاارتباط از طریق پست اینترنتی یاگپ زنی وبا معرفی خود به عنوان یکی از کارکنان شرکت یا یک شخص معتبرمی کوشد مخاطب خودرادرباره سیستم رایانه ای مربوطه تخلیه اطلاعاتی کند. درمهندسی اجتماعی ، بیش ازآنکه مرتکب به دانش فنی نفوذ به سیستم رایانه ای متکی باشد، به میزان نفوذ کلامی یا رفتاری خویش وابسته است صید اطلاعات مالی[۵] نوعی مهندسی اجتماعی است که با توجه به جنبه مالی آن شیوه مناسبی برای جاسوسی صنعتی وتجاری است.

۲-۴-۲ جاسوس افزارها

به دستیابی غیر مجاز به سیستم با استفاده از جاسوس افزارها یا تروجان[۶] گفته می شود.

۲-۴-۳ افشای اطلاعات سیستم

عبارت است از افشای غیرمجاز اطلاعات سیستم ، اعم از اینکه دستیابی مجاز باشد یا غیرمجاز.

۲-۴-۴ سرقت اطلاعات

عبارت است از تحصیل غیر مجاز اطلاعات ازطریق دستیابی به سیستم یا سخت افزار دیگری.

---

۱. Hack

۲.جلالی فراهانی ، امیر حسین ، پیشین ، ص ۳۲۸

۳.Social Engineering

۴. فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، هیأت مؤلفان و ویراستاران انتشارات مایکروسافت، ص ۶۸۸

۵. Phishing Fishing

۶.Trojan Horse

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۲-۴-۵ رهگیری داده

عبارت است ازردیابی ودریافت اطلاعات(شنوداطلاعات)درحال انتقال، به ویژه درشبکه های بی سیم. به علاوه ،ممکن است جاسوسی ازطریق ارسال پیام های ناخواسته الکترونیکی(اسپم)ارتکاب یابد. این پیام ها هم می توانندحامل نرم افزارهای جاسوسی باشندوهم ممکن است شرایط تخلیه اطلاعاتی دریافت کننده پیام رافراهم آورند وساده تراز همه ممکن است جاسوسی رایانه ای با فریب یا تحریک متصدی حفاظت ازاطلاعات رایانه ای طبقه بندی شده بابهره گیری ازمسائل شخصی یاعاطفی صورت گیرد.درحال حاضر ، جاسوسی رایانه ای ، اعم از سیاسی ، اقتصادی ، وصنعتی روندروبه رشدی دارد.

روش‌های جاسوسی سایبری متنوع است که دراین مبحث به چند مورد اشاره می شود.

الف : یک روش عملیاتی که ممکن است توسط سازمان‌های تروریستی بکار رود روشی است که توسط یک شرکت امنیتی آزموده شد. این شرکت حافظه های کوچکی[۱] را با طرحی سفارشی از برنامه‌ای جدید از اسب تروجان که توسط ویروس یاب ها قابل کشف نبود، آماده ساخت. بیست عدد از این حافظه هادر یک مؤسسه واگذاری وام مفقود شدند. ۱۵ عدد از آنها توسط کارکنان پیدا شد و به شبکه وصل شدند. دراینجا تروجان شروع به جمع آوری کلمات رمز و دیگر اطلاعات ارزشمند کرد و این اطلاعات راازطریق ایمیل برای مجرمین فرستاد. شیوه بکار گرفته شده در این حمله توسط سازمان های تروریستی برای عملیات ضد جاسوسی بکار گرفته می‌شود.[۲]

ب : یکی از روش‌های دیگر جاسوسی در فضای سایبر سرقت هویت[۳] است. سرقت هویت عبارت است از تصاحب یا ادعای داشتن هویت شخص دیگر است . اتخاذ عنوان یا هویت دیگری برای کسب مال یا خدمات است یا برای ارتکاب جرم. از آنجا که سرقت مشخصات هویتی دیگری چه در

---

۱. stickUSB

۲ .یک روش دیگر وارد کردن چنین نرم افزارهایی می تواند از طریق کانال های مجاز صورت گیرد. در سال ۲۰۰۰ اداره پلیس پایتخت ژاپن از سیستمی نرم افزاری برای مسیریابی ۱۵۰اتومبیل پلیس و همینطور اتومبیل‌های بدون آرم، استفاده کرد. اداره پلیس بعداً متوجه شد که این نرم افزار توسط فرقه Aum Shinrikyo تولید شده بود، همان گروهی که در سال ۱۹۹۶ با پخش گاز به قطار زیرزمینی توکیو حمله کرد. همچنین متوجه شد که اعضاء این فرقه نرم افزارهایی را برای حداقل هشتاد شرکت و ده سازمان دولتی تولید کرده است. این فرقه توانسته بود که در سطح گسترده‌ای کار خود را انجام دهد و به عنوان پیمانکاری فرعی به تولید نرم افزارها می پرداخت. ر.ک

L. Janczewki, A. Colarik; Op.cit , P.۹۷

۳. Identity theft

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

محیط واقعی و چه در محیط سایبر موجب فراهم شدن زمینه های رفتارهای غیر قانونی همچون کلاهبردای ،تروریسم و جاسوسی می گردد. در برخی از کشورها و به ویژه در اکثر مقررات کیفری داخلی ایالتهای آمریکا به عنوان جرم مستقل جرم انگاری شده است.[۱]

سرقت هویت می‌تواند به روش‌های مختلف فنی ازجعل ساده هویت تا کلاهبرداری‌های ماهرانه الکترونیکی انجام شود. سرقت هویت افراد از طریق پست الکترونیکی امری رایج است. اخیراً موج خروشانی در ارسال پیام‌های الکترونیکی ناشناس وجود داردکه در ظاهر به نظر می‌رسند که این پیام-ها از طرف شرکتی معروف ارسال می شوند،اما بسیاری ازآنها به منظور دسترسی به سیستم وسرقت اطلاعات مربوط به هویت افراد انجام می شود.

ازاین میان مهندسی اجتماعی یکی از مهمترین روشهای جاسوسی ودست یابی به اطلاعات تلقی می شود.[۲] یکی ازمشهورترین رخنه گرهای جهان، کوین میتنیک[۳]برآن بود که مهندسی اجتماعی آسان-ترین روش برای دسترسی غیر مجاز به منابع فناوری اطلاعات است.

بخش پنجم :مراحل جاسوسی سایبری

همانند جاسوسی سنتی،جاسوسی رایانه ای درقالب رفتارهای متفاوت وطی مراحل گوناگون ارتکاب می یابد:

۲-۵-۱ دسترسی به دادها یا تحصیل آنها یا شنود محتوای سری درحال انتقال

این اقدام به موجب مواد دیگر قانون جرم انگاری شده است ، امادرماده۳ ق.ج.ر به لحاظ اهمیتی که موضوع جرم (داده های سری) دارد ونیز درراستای باز دارندگی از مرحله نهایی ، یعنی ارائه اطلاعات به دشمن یا اشخاص ناصالح ، به عنوان وصف مجرمانه جدید معرفی شده اند.

۲-۵-۲ دردسترس قراردادن داده های سری برای اشخاص فاقد صلاحیت

اشخاص فاقد صلاحیت راقانون تعیین می کند . شخص اعم از حقیقی وحقوقی است .اشخاص

---

[۱].CRS report for congress,Op.cit ,2008,P.13

[۲].فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، پیشین ،ص ۶۸۸

[۳]. Kevin Mitnik

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

حقیقی لزوماً ایرانی نیستند ، اما اشخاص حقوقی باید ایرانی باشند.زیرادربند بعدی به اشخاص حقیقی خارجی اشاره شده که این حالت ازنقایص قانون است. همچنین مرتکب لزوماً دشمن نیست ، اما قابلیت ایجاد پل ارتباطی با دشمن را دارد . از این رو ، هنوز چرخه جاسوسی کامل نگشته ومجازات آن از مجازات افشاء یا ارائه اطلاعات به دشمن یا دولت بیگانه خفیف تر است .

۲-۵-۳ افشا یادردسترس قرار دادن داده های مذکور برای دولت ، سازمان ، شرکت یا گروه بیگانه یا عاملان آنها.

افشای داده ها به صورت عمومی وعلنی ودردسترس قراردادن به صورت موردی وغیر علنی است. جرایم فوق با فعل ارتکاب می یابند ومرتکب باید هم به موضوع جرم دایربر سری بودن داده ها وهم به دریافت کننده موضوع ، یعنی اشخاص فاقد صلاحیت یا دولت ، سازمان، هرچند آئین نامه طرز نگاه داری اسناد سری ومحرمانه دولتی وطبقه بندی ونحوه مشخص کردن نوع اسناد واطلاعات ، مصوب ۱۳۵۴/۱۰/۱ هیأت وزیران ، بین اسناد سری واسناد به کلی سری با توجه به ارائه طبقه بندی از اسناد سری ومحرمانه دولتی درماده یک تفاوت قائل شده ، امادرقانون مجازات انتشاروافشای اسناد محرمانه وسری دولتی مصوب ۱۳۵۳/۱۱/۲۹ ، اسناد دولتی سری اعم است از اسناد سری وبه کلی سری وبراساس همین قانون ، موضوع جرم داده های سری است که اعم از سری وبکلی سری است. یکی از خلاء های این قانون درمقایسه با ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح ، عدم پیش بینی جاسوسی اقتصادی وصنعتی است . هرچند دربند «ج» ماده مورد بحث از شرکت یا گروه بیگانه صحبت شده ، اما با توجه به اینکه شرکت ها وگروه ها می توانند نقش واسطه برای دشمن داشته باشند وبه ویژه با توجه به اینکه موضوع جرم داده های سری است ، این خلاء بیشتر به چشم می آید. عنوان مجرمانه دیگر درلایحه که عنوان جاسوسی یافته است ، نقض تدابیر امنیتی سیستم های رایانه ای یا مخابراتی به قصد دسترسی به داده های سری است که نوعی جرم سابق (بازدارنده) تلقی می شود تا حفاظت سیستم های رایانه ای یا مخابراتی حساس تأمین ومقدمات تحقق جرم جاسوسی برچیده شود . نقض تدابیر امنیتی دراین ماده با دسترسی غیر مجاز (هک) متفاوت واخص از آن است فارغ از اینکه دردسترسی غیر مجاز لزوماً نقض تدابیر امنیتی شرط نیست ، دراین ماده به قصد خاص

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نیز اشاره نشده است . اما درماده۴ ق.ج.ر نقض تدابیر امنیتی سیستم های رایانه ای یا مخابراتی باید به قصد دسترسی به داده های سری باشد.[۱]

هرچند درحال حاضر نهادهای حساس درایران ، نظیر وزارت اطلاعات ، داده های خودراهنوز درفضای دیجیتالی وارد نکرده اند، اما **اوّل اینکه** دیر یا زود آنها نیزکارآیی وکارآمدی خود را درکسب اطلاع وحفظ اطلاعات رادررایانه ای کردن آنها خواهند دانست و**دوّم اینکه** جاسوسی رایانه ای که براحتی ازهرشخص متبحر دراستفاده از رایانه ساخته است ، به جاسوسی سیاسی از نهادهای حساس منحصر نیست تادورکردن اطلاعات آنها از فضای سایبر ریشه جاسوسی رایانه ای را بخشکاند . این نوع جاسوسی انواع مختلفی دارد که نهایتاً مهم ترین چاره برای کنترل آن جرم انگاری ودیگری اتخاذ اقدامات پیشگیرانه ، به ویژه پیشگیری فنی وبکارگیری نرم افزارهای ایمن ساز سایبری مانند دیوار آتشین است.[۲]

بخش ششم : بررسی برخی از مصادیق جرم جاسوسی وارکان آن

۲-۶-۱ : بررسی ارکان مرتبط با جاسوسی

برای آنکه عملی جرم محسوب شود، وجود عناصری ضرورت دارد. برخی ازعناصرجنبه ی عمومی وبرخی جنبه اختصاصی دارند.

یکی ازارکان عمومی هرجرم این است که : آن عمل ازطرف قانون به عنوان جرم پیش بینی ومجازاتی برای آن مقرر شده باشد (عنصر قانونی).[۳]

اصل وعنصرفوق،مستفادازبرخی ازآیات شریفه قرآن کریم مانند(ماکُنّامُعذّبینَ حتّی نَبعَثُ رسولاً)[۴]

---

[۱].دولتشاهی ، شاهپور، ۱۳۸۴ ،**مجموعه مقاله های همایش بررسی جنبه های حقوقی فناوری اطلاعات**، قم سلسبیل

[۲]. Fire.Wall برنامه کاربردی است که در هنگام اتصال به اینترنت مانع از دسترس سایر افراد به رایانه می‌شود ؛ این برنامه هرگونه فعالیت غیرمجاز نفوذگرها را متوقف کرده وتلاش‌های ناموفق آنها را ثبت می‌کند.

[۳]. صانعی، پرویز، **حقوق جزای عمومی** ، جلد ۱ ، ص ۱۷۳ و۱۷۴

[۴]. قرآن کریم ، سوره مبارکه اسراء آیه ۱۵

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ومستفادبرخی ازروایات معصومین علیهم السلام وطبق حکم عقل برقبح عقاب بدون بیان است ودرعبارت لاتین چنین آمده است: Nullum Crimen Sine Lege[1]

با توجه به اصل فوق ، قوانین معتبر ولازم الاجرایی که جاسوسی راجرم اعلام کرده اند به دو دسته تقسیم می شوند :

دسته ی اول ، شامل مقررات وقوانینی است که صراحتاً به جاسوس وجاسوسی اشاره کرده اند که ازاین دسته مواد ۷،۶و۸ قانون مجازات اسلامی (تعزیرات) مصوب ۱۳۶۲/۵/۱۸ وماده ۱۲ قانون مجازات جرایم نیروهای مسلح مصوب ۷۱/۵/۱۸ ومواد ۵۰۱، ۵۰۲ و ۵۱۰ قانون مجازات اسلامی سال ۱۳۷۵ را می توان نام برد .

دسته دوم ، قوانین ومقرراتی است که صراحتاً به «جاسوس » و«جاسوسی » اشاره نکرده اند ، امّا با درنظرگرفتن مفهوم وماهیت آنها ورعایت اختصاصات وضوابط جاسوسی ،امکان صدق تعریف جاسوسی وانتصاب عنوان جاسوسی به آنها وجوددارد که ازآن جمله مواد ۵،۴،۳و۹ قانون مجازات اسلامی (تعزیرات) وماده ۳۱۳ قانون مجازات جرایم نیروهای مسلح ومواد ۵۰۳، ۵۰۵ و۵۰۹ قانون مجازات اسلامی سال ۷۵ را می توان نام برد.

بنابراین، قانون جمهوری اسلامی ایران، جاسوسی را از جرایم اعلان نموده ورکن قانونی این جرم با توجه به موادی که درفوق به آن اشاره شد تمام است.

درنظام های جزایی کنونی ، کسی را تنها به خاطر اندیشه وفکرمجرمانه ، محاکمه ومجازات نمی کنند برهمین اساس یکی از عناصر تشکیل دهنده جرم ، عنصر مادی است ؛ یعنی تنها حالت ذهنی برای تحقق جرم کافی نیست ، بلکه باید عمل وفعل همراه با سوء نیتی که قانون آنرا جرم شناخته است،ازطرف شخص ظهور وبروز پیداکند.بنابراین ، اندیشه ی مجرمانه ای که همراه با عمل مجرمانه نباشد غالباً جرم نیست.

[1]. هیچ جرمی بدون قانون ممکن نیست

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

پس برای تحقق جرم ، عنصر مادی، یعنی واکنش خلاف قانون ومقررات ،ضروری است . مصادیق واکنش متفاوت است وگاهی از مواقع ممکن است حالت منفی وترک فعل باشد.ازنظرحقوقدانان مصادیق عنصر مادی را به طورکلی به شکل ذیل می توان تقسیم نمود:[1]

۱- فعل؛

۲-ترک فعل؛

۳-جرم فعل ناشی ازترک فعل؛

۴-داشتن ونگهداری؛

۵-حالت و وضعیت.

باتوجه به آنچه ازمتون قانونی استفاده می شود، ملاک تحقق عنصرمادی جرم جاسوسی ، فعل مثبت است وترک فعل یا فعل ناشی از ترک فعل نمی تواند ،بوجودآورنده ی عنصرمادی جاسوسی باشد.

برای تحقق جرم علاوه برعنصر قانونی ومادی ، وجودعنصرروانی هم ضرورت دارد.ارتکاب یک عمل مجرمانه به خودی خود دلیل وجود عنصر روانی نیست، ودرمواردی باآنکه عمل مجرمانه ای صورت می گیرد ، قانون ،مرتکب آنرا به خاطر فقدان قصدمجرمانه یامسؤولیت جزایی ، قابل مجازات نمی داند.

برای تحقق عنصر روانی وجود دو عامل ضرورت دارد:

۱- اراده ی ارتکاب(یعنی شخصی بخواهد فعل مجرمانه ای راانجام دهد)؛

۲- قصدمجرمانه.

بنابراین ، اراده ی ارتکاب فعل ، بدون قصد مجرمانه موجب بوجودآمدن جرم نمی شود یعنی اگرفعل تجسس وجمع آوری اطلاعات با اراده ، ارتکاب یابد، ولی قصد مجرمانه (یعنی استفاده خلاف قانون ازآن وجود نداشته باشد) جرم جاسوسی محقق نمی شود.

پس علاوه برارتکاب عمل تجسس ،باید قصد مجرمانه درجرایم عمدی جاسوسی وخطای جزایی درمصادیق غیر عمدی جاسوسی ، محقق ومحرز باشد.

بنابراین درجرم جاسوسی با توجه به تعریف آن وموادقانونی باید گفت: عنصر معنوی که مشتمل برسوء نیت عام وخاص (قصدواراده جاسوسی درارتکاب اعمال) که قانون آنرا منع کرده وآن عمل را مجرمانه

---

[1]. ساریخانی، عادل، پیشین ،ص ۲۲۵

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

اعلام نموده واین عمل غالباً دربردارنده ضرروزیان به کشور ، ملت ودولت است، زیرا اسنادسری ومحرمانه اصولاً تاوقتی مفید هستند که افراد غیر صالح به آن دست نیافته باشند ووقتی افراد غیر صالح ومجرم ازطریق ارتکاب اعمال مجرمانه به آن دست یافتنداصولاً ضررکشور تحقق می یابد.

ازآنچه گفته شد معلوم گردید که جاسوسی از جرایم عمدی است ، ولی درپاره ای از مواقع ممکن است مرتکب جرم جاسوسی، عمل را با اراده مرتکب شود، ولی نتیجه مجرمانه ونتیجه حاصل از جاسوسی رااراده نکرده باشد ودرپاره ای از مواقع حتی نتیجه راپیش بینی نکرده است. دراین صورت، به تعبیر حقوقدانان عنصر روانی جرم از خطا تشکیل می یابد وجرم ارتکابی غیر عمدی محسوب می گردد.[1]

۲-۶-۲: بررسی برخی ازمصادیق جاسوسی

ماده۳۱۳ قانون آئین دادرسی وکیفری ارتش به ارائه مصادیق جاسوسی پرداخته است که دراین قسمت به بررسی آن می پردازیم.

ماده ۳۱۳ قانون آئین دادرسی وکیفری ارتش :« اشخاص ذیل جاسوس ومحکوم به مجازات اعدام هستند:

الف : هرکس که برای بدست آوردن اسناد یا اطلاعات به نفع دشمن به یک قلعه یا مکان مستحکم یا پاسگاه یا هر بنگاه نظامی یا استحکامات واردوگاهها یا منزلگاههای ارتش داخل شده باشد.

ب: هرکس که برای دشمن اسناد یا اطلاعاتی بدست آورد که ممکن است نسبت به عملیات ارتش یا نسبت به تأمین قلاع یاامکنه مستحکم یا پاسگاهها یا بنگاههای نظامی مضر باشد .

ج: هرکس که جاسوسان یاافراد دشمن راکه برای اکتشافات مأمور شده باشند عمداً مخفی نموده یاسبب اختفاء آنها گردد.

د: هرکس که اسرارنظامی یاسیاسی یا مفاتیح رمز رابرخلاف مصالح کشور به اجنبی تسلیم کند .»

برطبق این ماده برای تحقق جاسوسی شرایط ذیل لازم است :

اول: قصد جاسوسی ، دوم : تحصیل اسناد یا اطلاعات ، سوم : ورود ضررویاامکان آن ، چهارم : دشمن بودن طرف منتفع از اطلاعات.

---

[1].ساریخانی، عادل، پیشین ،ص ۲۲۶ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ارکان مادی جرم جاسوسی برطبق این ماده عبارتند از: ۱- ورود به مکانهای نظامی وارتشی برای کسب اطلاعات به نفع دشمن ومضربه عملیات ارتش، ۲- اختفای عمدی جاسوسان یا افراد دشمن ، ۳- تسلیم اسرار نظامی ، سیاسی ومفاتیح رمز به اجنبی .

دراین ماده اطلاق هرکس اعم از نظامی یا غیر نظامی ، مرد یا زن، مسلمان با غیر مسلمان وغیره خواهد بود.

ماده ۱۲ قانون مجازات نیروهای مسلح « اشخاص زیر جاسوس شناخته شده وبه مجازات مقرر محکوم می شوند :

۱- هرنظامی که اسناد یا اطلاعات یا اشیاء دارای ارزش اطلاعاتی راتحصیل کند ودراختیار دشمن قراردهد واقدام اوبرای عملیات نظامی یا نسبت به امنیت تأسیسات،استحکامات،پایگاهها، کارخانجات ، انبارهای دائمی وموقتی تسلیحاتی ، توقفگاههای موقت ، ساختمان های نظامی ، کشتی یا هواپیماها یا وسایل نقلیه زمینی نظامی یا امنیت تأسیسات دفاعی کشور مضرباشد به مجازات محارب ومفسدمحکوم خواهد شد.

۲- هرنظامی که اسناد یااطلاعاتی برای دشمن تحصیل کند وبه هردلیل موفق به تسلیم آن به دشمن نشود به حبس از سه تاپانزده سال محکوم می گردد.

۳- هرنظامی که اسرارنظامی یاسیاسی یا اقتصادی یا صنعتی یا کلیدهای رمزرابه دشمن داخلی یاخارجی تسلیم نماید یا آنان را ازمفاد آن آگاه سازد ، به مجازات محارب ومفسد محکوم خواهد شد.[۱]

۴- هرنظامی که برای بدست آوردن اسنادیا اطلاعاتی به نفع دشمن به محل نگهداری اسناد ویا اطلاعات داخل شود، چنانچه به موجب قوانین دیگر مستوجب مجازات شدیدتری نباشد به حبس از دوتاده سال محکوم می گردد.

۵- هر بیگانه ای که برای کسب اطلاعات به نفع دشمن به پایگاهها، کارخانجات ، انبارهای تسلیحاتی ، اردوگاههای نظامی ، یگانهای نیروهای مسلح ، توقفگاههای موقتی نظامی ، ساختمانهای دفاعی نظامی یا وسائط نقلیه زمینی، هوایی، دریایی یادرمحلهای نگهداری اسناد یا اطلاعات داخل شود به اعدام ودرغیر اینصورت به دو تا ده سال حبس محکوم می گردد.»

---

[۱].خداقلی، زهرا ، پیشین ، ص۱۰۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۱-۱ : عنصر مادی جرم عبارت است از اینکه یکی ازپرسنل نظامی مخفیانه اطلاعات یا اسناد واشیاء دارای ارزش اطلاعاتی رابه دست آورده وآنها رابه دشمن جمهوری اسلامی بدهد.

۲-۲: شروع به جرم جاسوسی رابیان داشته وآن عبارتست از تحصیل اسناد واطلاعات اما عدم تکمیل واتمام جرم جاسوسی به دلیل موفق نشدن به تسلیم آن به دشمن بنا به هردلیلی.

۳-۳: تسلیم اسرارنظامی ، سیاسی یا اقتصادی یا صنعتی که این اسرارمی تواند شامل اسناد شود چه عین آنها چه رونوشت یا کپی آنها وچه به صورت شفاهی یا کتبی.

۴-۴: ورود به امکان نظامی ومحل نگهداری اسناد برای تحصیل آن به نفع دشمن ،رکن مادی آن عبارتست ازاین است که فعل مادی مرتکب به صورت داخل شدن به محلهای نگهداری اسناد است ومحل وقوع جرم هم یکی ازمؤسسات ویا اماکن نظامی است.

۵-۵: مرتکب آن باید بیگانه باشد پس نظامی نیست فعل مادی او ورود وداخل شدن به محلهای نظامی وبیان شده توسط قانون است.

معاونت درجاسوسی طبق تبصره ماده ۱۲ قانون مجازات جرائم نیروهای مسلح:

عبارتست از هرگونه همکاری ومعاونت با عنصر جاسوسی مانند مخفی نمودن وپناه دادن وچنانچه عمل معاون موجب افسادواخلال درنظم یا شکست جبهه اسلام گردد درحکم محارب والا به ۵ سال حبس محکوم می گردد.

۲-۶-۳ جرم جاسوسی درقانون مجازات اسلامی

ازآنجاییکه درقانون مجازات اسلامی درمواد ۵۰۱ و۵۰۲ و۵۰۳ و۵۱۰ قانونگذار درمقام اطلاق از قید هرکس استفاده نموده است لذااین جرم شامل افراد غیر نظامی می گردد اعم از ایرانی یا خارجی ، مسلمان یا غیر مسلمان ، کارمند یا غیر کارمند.

ماده۵۰۱« هرکس نقشه ها یااسراریااسناد وتصمیمات راجع به سیاست داخلی یاخارجی کشورراعالماً یاعامداً دراختیار افرادی که صلاحیت دسترسی به آنها را ندارندقراردهد یاازمفادآن مطلع کندبه نحوی که متضمن نوعی جاسوسی باشد، نظربه کیفیات ومراتب جرم به یک تاده سال محکوم می گردد.»[۱]

[۱].خداقلی، زهرا ، پیشین ،ص۱۱۱

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ماده۵۰۲« هرکس به نفع یک دولت بیگانه وبه ضرردولت بیگانه دیگری درقلمرو ایران مرتکب یکی از جرایم جاسوسی شود به نحوی که به امنیت ملی صدمه وارد نماید، به یک تاپنج سال حبس محکوم خواهد شد.»

۲-۶-۳-۱رکن مادی جرم جاسوسی

طبق ماده۵۰۱و۵۰۲ این است که هرکس (اعم از ایرانی یا خارجی ، مسلمان یا غیرآن ، کارمند یا غیر کارمند) به نحوی موفق به تحصیل اسراری شود حال این اسرار خود می تواند شامل نقشه ها ، اسناد وتصمیمات راجع به تأسیسات واستحکامات یا پایگاههای جنگی ونظامی باشد ویا نقشه های غیر جنگی ونظامی که اطلاع افراد عادی جامعه برآن ممنوع است وآنها رادراختیار افرادی قراردهدکه صلاحیت دسترسی به آنرا نداشته اند.

پس عمل مرتکب یک فعل مثبت مادی خارجی است که ابتداعالماً وعامداً تحصیل اسراری کرده که وقوف برآنها برای او بدون درنظر گرفتن قسمت یا شغل یا درجه او ممنوع بوده وبعدعالماً وعامداً این اسرارکه جنبه سری داشته اند تسلیم اشخاص دیگری نموده است .

دراین جرم تفاوتی بین افشاء تمام یاقسمتی ازآن نمی کند ونیز افشاء شفاهی یا مکتوب این اسرارنیز تفاوتی دروقوع جرم ندارد.

ماده ۵۰۳« هرکس به قصد سرقت یا نقشه برداری یا کسب اطلاع از اسرار سیاسی یا نظامی یا امنیتی به مواضع مربوط داخل شود وهمچنین اشخاصی که بدون اجازه مأمورین یا مقامات ذیصلاح ، درحال نقشه برداری یا گرفتن فیلم یا عکسبرداری از استحکامات نظامی یا اماکن ممنوعه دستگیر شوند به شش ماه تا سه سال حبس محکوم می شوند.»

دراین ماده فعل مرتکب فعل مثبت مادی خارجی است وآن عبارت است از۱- داخل شدن به مراکز نگهداری اسرارواسناد به قصد دزدی ؛ ۲- داخل شدن به مراکز نگهداری اسرارواسناد به قصد نقشه برداری ؛ ۳- نقشه برداری، فیلمبرداری یا عکسبرداری از استحکامات نظامی واماکن ممنوعه.

ماده۵۱۰« هرکس به قصد برهم زدن امنیت ملی یا کمک به دشمن ، جاسوسانی راکه مأمور تفتیش یا وارد کردن هرگونه لطمه به کشور بوده اند ، شناخته ومخفی نماید یا سبب اختفای آنها شود به حبس از شش ماه تا سه سال محکوم می شود.»

فعل مرتکب به صورت فعل مثبت مادی خارجی اختفای جاسوسان است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۲-۶-۳-۲رکن معنوی جرم جاسوسی

این جرم از جرائم عمدی است وشرط تحقق جرم هم سوء نیت مرتکب است یعنی مرتکب عالماً وعامداً مرتکب این جرم می شود وقصد جاسوسی دارد او می داند که این اطلاعات سری است وشامل موارد مهم نظامی یاسیاسی یا اقتصادی یا صنعتی یا علمی یا کلیدهای رمز می باشد[۱]ولی بااین حال با آگاهی وسوء نیت این اسرار راپس از تحصیل تسلیم به دیگری می کند ومی داند که تسلیم آنها مضربه مصالح کشور است .

بنابراین درجرم جاسوسی احراز سوء نیت با دادرس دادگاه است اگر تسلیم اسرار اززوی نادانی واشتباه یا غفلت واکراه صورت یافته باشد رکن معنوی رامتزلزل ساخته وعمل مصداق جرم جاسوسی نمی شود ممکن است جرم جاسوسی بالواسطه یا مستقیم باشد که تفاوتی درموضوع آن ندارد.

بخش هفتم: بررسی مواد وارکان مرتبط با جاسوسی رایانه ای

ماده۳ قانون جرایم رایانه‌ای مقرر می‌دارد: « هرکس به طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰)ریال تا شصت میلیون (۶۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات.

ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت به حبس از دو تا ده سال.

ج) افشاءیا دردسترس قراردادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.»

[۱] .خداقلی، زهرا ، پیشین ،ص۱۱۵

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

عنصر مادی این جرم به طور کلی عبارت است از ارتکاب برخی اعمال غیرمجازبه شرح بندهای الف و ب و ج نسبت به داده‌های سری در حال انتقال یا ذخیره شده درسامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده.

۲-۷-۱بررسی رکن مادی بند«الف» ماده ۳

در بند الف ماده۳ اعمال مجرمانه عبارتند از: ۱- دسترسی به داده‌های سری۲-تحصیل داده‌های سری۳- شنود محتوای سری در حال انتقال.

برای روشن شدن مفاد این بند توجه به این مطلب لازم است که «جاسوسی در معنی وسیع کلمه دو دسته اقدامات را شامل می‌شود: دسته اول، اقدامات مقدماتی که عبارت است از تفحص و تحصیل اطلاعات مخفی، دسته دوم، عملیات اجرایی که عبارت است از ایجاد ارتباط و رساندن اطلاعات مزبور به کسانی که باید از آن بهره‌برداری‌کنند. دسته اول ممکن است متضمن قصد جاسوسی یا خیانت نباشد، مثلاً متهم صرفاً از لحاظ کنجکاوی یا میل به دانستن یا اینکه برحسب غفلت و بی‌احتیاطی اقدام‌کرده یا اینکه اقدام به تحصیل اطلاعات محرمانه نموده تا بتواند مردم مملکت خود را آگاه سازد نه خارجیان را، اما دسته دوم همیشه کاشف از وجود اراده خاص بر آگاه کردن عوامل غیرمجاز وغیر صلاحیت دار است.»[۱]

سیاق تنظیم بند «الف» و وجود قرائنی از جمله عدم مقید کردن اعمال غیر مجاز مذکور به رساندن این اطلاعات به افراد غیر صلاحیت دار، ما را به این نتیجه رهنمون می‌سازد که اقدامات ذکر شده در بند الف در زمره اقدامات مقدماتی پیش گفته قرار می‌گیرد. یعنی اگر قراین و اماراتی دال بر جاسوسی وجود نداشته باشد نمی‌توان صرف انجام این اعمال را جاسوسی قلمداد کرد. آنچه دسترسی، تحصیل و یا شنود محتوای سری را صبغه جرم می‌بخشد، ارتکاب آنها به صورت غیرمجاز است لذا بهتر بود قید غیرمجاز به جای ابتدای ماده در ابتدای این بند به کار می‌رفت.

دسترسی از نظر لغوی عبارت است از: قدرت، توانایی، قدرت دست یافتن به چیزی[۲] لذا باتوجه به این معنی فردی که دسترسی غیرمجاز به داده‌های سری پیدا کند، خود رأساً این کار را می‌کند بدون

---

[۱] .گلدوزیان، ایرج، ۱۳۸۲، **حقوقی جزای اختصاصی**، تهران، انتشارات دانشگاه تهران

[۲] .عمیدی، مهدی،۱۳۸۷، مطالعه تطبیقی جرایم رایانه‌ای ازدیدگاه فقه وحقوق کیفری ایران ، تهران، دانشگاه آزاد اسلامی‌واحد تهران مرکزی، پایان نامه کارشناسی ارشد حقوق جزا وجرم شناسی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

آنکه از کسی یاری بگیرد، برای مثال با توسل به روش‌هایی مثل هک کردن، داده‌های مزبور را جمع آوری می‌کند و تفاوت آن با تحصیل داده‌های سری در این است که مجرمی‌که داده‌های سری را تحصیل می‌کند خود، ابتدا به ساکن امکان دسترسی مستقیم به این داده‌ها را ندارد بلکه برای مثال با ایجاد ارتباط با کسی که این داده‌ها را در اختیار دارد، این داده‌ها را برای خود فراهم می‌آورد. توجه به معنی لغوی واژه تحصیل استدلال فوق را تقویت می‌کند، در فرهنگ فارسی یکی از معانی تحصیل عبارت است از: به دست آوردن، کسب کردن[1] بنابراین طبیعی است که هرگاه مراد ما تحصیل دانش باشد آن را از طریق معلم و استاد کسب می‌کنیم و هرگاه تحصیل داده‌های سری منظور باشد، آن را از طریق فرضاً یک مسؤول در اداره‌ای دولتی یا مرکزی نظامی‌کسب می‌کنیم.

شنود نیز به معنای دزدیده گوش دادن به مکالمات دیگران است[2] که در اینجا در خصوص محتوای سری در حال انتقال به کار رفته است. البته شنود غیرمجاز در حالی که محتوا، داده‌های سری نباشد به صورت مجزا در ماده۲ق .ج.رجرم انگاری شده است. مطابق این ماده«هرکس به طور غیرمجاز محتوای درحال انتقال ارتباطات غیرعمومی‌درسامانه‌های رایانه‌ای یا مخابراتی یاامواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰/۰۰۰/۰۰۰) ریال تا چهل میلیون (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

جرم بند الف م.۳ ق. ج. رجرمی‌مقید است از این جهت برای تحقق آن،عملیات اجرایی مجرم جهت دسترسی،تحصیل شنود داده‌های سری می‌باید منجر به حصول به این داده‌ها گردد در غیر این صورت (عدم حصول به داده‌های سری) ممکن است عمل مرتکب مشمول ماده۴ قانون مارالذکر گردد.

۲-۷-۲ بررسی رکن معنوی بند «الف» ماده ۳

عنصر روانی جرم بند الف علاوه بر عمد در دسترسی، تحصیل و یا شنود محتوای سری عبارت است از آگاهی و علم به غیر مجاز و بدون مجوز بودن دسترسی یا تحصیل ویا شنود داده‌های سری ونیز علم به سری بودن داده‌هایی که شخص به آنها دسترسی و... پیدا کرده است. از این رو اگر داده‌ها را عادی تصور کند، مرتکب این جرم نخواهد شد.

---

[1]. معین، محمد،پیشین ، دوره ۶جلدی

[2]. گلدوزیان، ایرج، ۱۳۸۲،**محشای قانون مجازات اسلامی**،تهران، مجمع علمی‌وفرهنگی مجد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۲-۷-۳ بررسی رکن مادی بند«ب» ماده۳

باتوجه به صراحت و تأکید این بند بر «در دسترس قراردادن داده‌های مذکور»منطقاً به نظر می‌رسد که این داده‌ها اعم از فیلم، عکس، متن و.... باید به طور مستقیم در اختیار فرد فاقد صلاحیت قرار گیرد. افشای مفاد این داده‌ها که شکل غیر مستقیم در دسترس قراردادن است. شامل ماده نمی‌شود و جرم نمی‌باشد. زیرا اگر قانونگذار نظر «دردسترس قراردادن مفاد داده‌ها» را جرم می‌دانست مانند ماده۵۰۱ ق.م.ا ازواژه ی «مفاد» در این ماده استفاده می‌کرد وآنگاه مقرر می‌نمود: «در دسترس قراردادن داده‌های مذکور یا مفاد آن....» این امر یکی از نقایص بندب ماده۳ ق.ج.ر. است زیرا با توجه به سری بودن داده‌ها واهمیت بالای آن عقلاً تفاوتی میان تسلیم خود و مفاد داده‌ها نیست و اطلاع افراد فاقد صلاحیت از خود داده یا مفاد آن به هر حال به امنیت کشور لطمه می‌زند.[۱]

البته می‌توان در دسترس قراردادن مفاد این داده‌ها را طبق ماده۵۰۱ ق.م.ا جرم دانست به این ترتیب اگر این داده‌ها در برگیرنده نقشه‌ها، اسراریا اسناد وتصمیمات راجع به سیاست داخلی یا خارجی کشور باشد، آن گاه در دسترس قرار دادن مفاد آنها به افراد فاقد صلاحیت، جرم محسوب می‌شود.

به هرحال، بهتر بود قانونگذار برای جلوگیری از بروز این دست ابهام‌ها، کلمه مفاد را نیز به همان ترتیبی که گفته شد به این بند اضافه می‌کرد.

۲-۷-۴ بررسی رکن معنوی بند «ب» ماده ۳

عنصر روانی این جرم نیز عبارت است از: در دسترس قرار دادن داده‌های سری به صورت عمدی، از این رو اگر فرد در حالت مستی بی‌هوشی، خواب، اجبار، اکراه و نظایر اینها، مرتکب عمل شده باشد، عمل وی مشمول این بند نمی‌شود، همچنین مرتکب باید نسبت به سری بودن داده‌ها ونیز فاقد صلاحیت بودن طرف دیگر علم داشته باشد، اما سوءنیت خاص یعنی اینکه با انجام این کار قصد ضربه زدن به نظام یا برهم زدن امنیت کشور و نظایر آن را داشته باشد، ضروری نیست.

۲- ۷- ۵ بررسی رکن مادی بند «ج» ماده ۳

درقوانین جزایی تعریف خاص از افشاء به عمل نیاورده، اما مطابق ماده ۱۹- ۲-۱ آیین‌نامه حفاظت از اسناد و مدارک طبقه‌بندی شده نیروهای مسلح مصوب۱۳۷۵ ستاد کل نیروهای مسلح، افشا عبارت

---

[۱]. میرمحمد صادقی، حسین،پیشین ، ص۸۵ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

است از: «عرضه کردن مفاد اسناد یا اطلاعات طبقه‌بندی شده به طور شفاهی،کتبی و یا هر طریقی که حفاظت و امنیت از آن سلب شود.»[1]

به نظر می‌رسد تفاوت «افشا» با «در دسترس قرار دادن» این است که زمانی عمل فرد «افشا» تلقی می‌شود که فرد رأساً داده‌های سری را در اختیار افراد مذکور بگذارد، لیکن ماهیت «در دسترس قرار دادن» انفعالی است، به این ترتیب زمانی عمل مرتکب «در دسترس قراردادن» تلقی می‌شود که وی به نحوی از انحاء موجبات دسترسی افراد مذکور را به داده‌های سری فراهم کند، بدون آنکه داده‌ها به طور مستقیم از طرف خود وی به آنها ارائه شود مانند آنکه مرتکب، گذر واژه(۱۱) رایانه خود را عمداً دراختیار عوامل بیگانه قرار داده وآنها با ورودپنهانی به اطاق محل قرار گرفتن رایانه و واردکردن گذر واژه مزبور، وارد رایانه شده و داده‌های سری را برداشت کنند.

در خصوص واژه «بیگانه»که معمولاً به خارجیان اطلاق می‌شود، پر واضح است که استعمال آن به عنوان صفت دولت، سازمان، شرکت و یا حتی گروه، ابهامی‌ایجاد نمی‌کند و شامل هر دولت، سازمان، شرکت و یا گروه غیر ایرانی می‌شود. اما ممکن است در رابطه با عاملان آن‌ها این تردید ایجاد شود که آنها نیز باید لزوماً یک فرد خارجی و غیرایرانی باشد؟ برای پاسخ باید به این نکته توجه کردکه دولت‌ها برای جاسوسی از یکدیگر معمولاً به صورت کاملاً پنهانی عمل می‌کنند و برای عادی‌سازی اقدامات خودوبرای کسب اطلاعات مورد نیازخود دست به استخدام عوامل ایرانی بزنند و به اصطلاح یک ایرانی عامل آنها باشد، بنابراین باتوجه به فرایند پیچیده جاسوسی و پنهان‌کاری‌های مختص آن، به نظر می‌رسد تفسیر صحیح تر آن باشد که چون یک ایرانی نیز می‌تواند عامل بیگانه باشد، پس افشا یا در دسترس قرار دادن داده‌های سری برای او نیز مشمول این ماده است و لزومی ندارد عاملی بیگانه هم یک فرد ایرانی باشد.

۲-۷-۶ بررسی رکن معنوی بند«ج» ماده۳

عنصر روانی مرتکب این بند علاوه بر عمد در افشا یا در دسترس قرار دادن داده‌های سری، علم و آگاهی نسبت به بیگانه بودن طرف مقابل است؛ این بیگانه می‌تواند یک دولت، سازمان و... باشد.

۱.http://www.imj.ir/index.php?option=com_content&view=article&id=۱۳۸۱:۱۳۸۹-۰۳-۰۱-۲۰-۱۳-۳۸&catid=۵۷:۱۳۸۸-۰۸-۱۹-۰۷-۴۵-۲۶.

نشریه پیام قانون به نقل از الیاس بوجار، **بررسی ابعاد جاسوسی رایانه‌ای باتوجه به قانون جرایم رایانه‌ای**، دانشجوی مقطع کارشناسی ارشد جزا وجرم شناسی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

همچنین در این بند وجود سوءنیت خاص یعنی اینکه با انجام این‌کار قصد برهم زدن امنیت کشور یا ضربه زدن به نظام را داشته باشد ضروری نیست و به صرف افشا یا در دسترس قرار دادن داده‌های سری جرم محقق می‌شود.

۲-۷- ۷ داده‌های سری

در تبصره۱ ماده۳ ق.ج.ر داده‌های سری تعریف شده است: «داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.»

برای روشن شدن این تبصره، باید به سابقه تاریخی آن در سیر مراحل تصویب در مجلس نیز توجه کرد.گفتیم در لایحه تقدیمی از سوی دولت فقط یک ماده (۴) تحت عنوان جرایم علیه امنیت مقرر کرده بود: «هرکس به طور عمدی و بدون مجوز مرجع قانونی به داده‌های رایانه‌ای به کلی سری و سری موجود در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده دسترسی یابد یا داده‌های رایانه‌ای به کلی سری و سری در حال انتقال را شنود یا دریافت کند به جزای نقدی از ده میلیون ریال تا یک میلیارد ریال متناسب با جرم اتفاق افتاده محکوم خواهد شد.»

تبصره یک این ماده نیز داده‌های به‌کلی سری و سری را چنین تعریف کرده است: «داده‌های رایانه‌ای به‌کلی سری داده‌هایی هستند که افشای بدون مجوز آنها می‌تواند با اساس حکومت و مبانی نظام جمهوری اسلامی‌ایران وبه تمامیت ارضی آن ضررجبران‌ناپذیری وارد کند و منظورازداده‌های رایانه‌ای سری، داده‌هایی است که افشای آنها بدون مجوز مرجع قانونی می‌تواند امنیت ملی و یا منافع ملی را دچار مخاطره کند.»

۲-۷-۸ بی‌احتیاطی و بی‌مبالاتی در حفظ داده‌های سری

جاسوسی اصولاً یک جرم عمدی تلقی می‌شود به این نحوکه مرتکب با سوءنیت اطلاعات طبقه‌بندی شده را در اختیار بیگانگان و عوامل غیرمجاز قرار می‌دهد، اما توجه به اهمیت حفظ اطلاعات طبقه بندی شده و ضررهایی‌که گاهی در اثر سهل‌انگاری مسؤولان مربوط و عدم حفاظت ازاطلاعات طبقه بندی شده به کشور و نظام اطلاعاتی آن وارد شده است قانونگذار را وادار به جرم‌انگاری این‌گونه سهل‌انگاری‌ها و بی‌مبالاتی‌ها در ماده۵۰۶ ق.م.ا کرده است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ماده ۵ ق.ج.ر نیز تقریباً مشابه ماده ۵۰۶ است با این تفاوت که همگام با پیشرفت فناوری وضع شده و برخلاف ماده۵۰۶ که اشاره‌ای به طبقه‌بندی اطلاعاتی خاص نمی‌کند، داده‌های سری را مورد حمایت کیفری قرار داده است.[۱]

مطابق ماده ۵ ق .ج .ر«چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده۳ این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آنها قرارگرفته است براثربی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیرامنیتی موجب دسترسی افراد فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵/۰۰۰/۰۰۰) ریال تا (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.»

۲-۷-۹ بررسی رکن مادی

برای تحقق جرم موضوع این ماده وجود پاره‌ای شرایط عمومی‌که در خصوص ماده۵۰۶ ق.م.ا نیز وجود دارد، ضروری است.

اوّل: ارتکاب این جرم به وسیله مأموران دولتی‌که دارای رابطه استخدامی اعم از رسمی، پیمانی، روزمزد، خرید خدمت و... باشند پیش‌بینی شده است از این رو شامل اشخاصی که مأمور دولت نبوده ولی داده‌های سری یا سامانه‌های مزبور را به هر دلیلی در اختیار دارند نمی‌شود.

دوّم: مأموران باید مسؤول حفظ داده‌های سری و سامانه‌های مذکور باشند؛ به عبارت دیگر شغل دولتی آنها با داده‌های سری مرتبط باشد. بنابراین صرف اینکه یک مأمور دولت داده‌های سری را در اختیار دارد. وی را مشمول ماده نمی‌سازد.

سوّم: آموزش لازم درخصوص حفظ داده‌های سری وسامانه‌های مزبوربه این مأموران دولتی داده شده باشد. چنانچه فرد این قبیل آموزش‌ها را طی نکرده باشد، عمل وی مشمول این ماده نخواهد بود.

۲-۷-۱۰ بررسی رکن معنوی

عنصر روانی این جرم خطای جزایی (بی‌احتیاطی، بی‌مبالاتی، عدم رعایت تدابیر امنیتی) است؛ البته در این ماده «عدم رعایت تدابیر امنیتی» جایگزین «عدم رعایت نظامات دولتی» شده که به نظر می‌رسد

---

[۱]. نشریه پیام قانون به نقل از الیاس بوجار، پیشین

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

با مباحث رایانه‌ای هماهنگ‌تراست.

بی‌احتیاطی معمولاً اقدام به انجام‌کاری است که فرد نباید انجام دهد، مثل آنکه فرد مأمور یک حامل داده را روی میز خود رها کند وکسی وارد اتاق شده و آن را بردارد. بی‌مبالاتی نیز عبارت است از عدم انجام‌کاری که انجام آن از وی انتظار می‌رود. مثل آنکه رایانه خود را دارای گذر واژه نکرده باشد و به این ترتیب هرکسی به راحتی بتواند صرفاً با روشن کردن رایانه به کلیه اطلاعات آن دسترسی پیدا کند.[۱] توجه به این نکته ضروری است که هرچند این جرم جزء جرایم عمدی نیست، اما احراز بی‌احتیاطی، بی‌مبالاتی و عدم رعایت تدابیر امنیتی لازم است. از این رو مأموری‌که تحت تأثیر شکنجه یا مستی اجباری و یا درحال خواب داده‌های سری را دراختیار افراد بدون صلاحیت قراردهد، مشمول این ماده نمی‌شود. نکته قابل ذکر دیگردرمورد عنصر بی‌مبالاتی و بی‌احتیاطی‌آن است‌که این دو هم می‌تواند نسبت به اصل ارائه داده‌های سری باشد و هم نسبت به شناسایی هویت گیرنده داده‌های سری، برای مثال مأمور بدون تحقیق کافی و به‌صرف ادعای شخص، او را ذیصلاح تلقی کرده و داده‌ها را در اختیار و دسترس وی بگذارد.[۲]

بخش نهم: تطبیق جرم جاسوسی کلاسیک با سایبری

درمقام تطبیق جرم جاسوسی رایانه ای با کلاسیک آنچه که بیش از همه به چشم می خورد نیازبه قانونگذاری صحیح درخصوص جرم جاسوسی رایانه ای است هرچند که وقوع جرم جاسوسی به هرطریقی امکان پذیراست بعنوان مثال می توان اطلاعات راازطریق تلفن به شخص حقوقی یا حقیقی دیگر اطلاع داد واز حیث ابزار بکار برده شده تفاوتی دروقوع جرم ندارد.

اما جرم جاسوسی رایانه ای تفاوتهایی دارد که به همین لحاظ از جلد جرم کلاسیک بیرون آمده وشکل نوینی ازاین جرم راپدیدآورده است.

بعنوان مثال درمواد جرم عمومی جاسوسی اشاره شدازحیث مجازات بین مرتکبین نظامی وغیر نظامی تفاوت وجود دارد حال سؤالی که مطرح است این است که با کامپیوتری شدن تمامی امور اگر یک

---

[۱]. میرمحمد صادقی ، حسین ، پیشین ص ۹۷ به بعد

[۲]. نشریه پیام قانون به نقل از الیاس بوجار، پیشین

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نظامی توسط کامپیوتربه مسائل امنیتی دست یابد وآنها رابه گونه ای حال چه توسط کامپیوتر ویاغیره انتقال دهدآیامستوجب حداست یا تعزیر؟

دراین فرض برای تحصیل اطلاعات از کامپیوتر بهره جسته امابرای تسلیم می تواند از کامپیوتراستفاده کند یا نه یا بالعکس به هرحال آیا دروقوع جرم جاسوسی رایانه ای توسط نظامی وغیرنظامی بازهم بایدقائل به تفکیک شد واین سؤال هایی است که باید قانونگذاران به آن پاسخ دهند.

درخصوص جرم جاسوسی رایانه ای آنچه که مسلم است بیهوده بودن قوانین موضوعه است . بعنوان نمونه برای مرتکبین عادی این جرم باید به ماده ۵۰۱ و۵۰۲ قانون مجازات اسلامی استنادکرد که بااندک تأملی به خوبی ضعف این قوانین درمقابل جرم خاص ونوین کامپیوتری وارکان خاص آن مشخص می شود.

ازآنجاییکه اکثرکشورها به وضع قوانین خاص درخصوص جرائم رایانه ای پرداخته اند لزوم وضع این قوانین درکشور مانیزبه چشم می خوردبه خصوص اینکه جرم جاسوسی کلاسیک درکشورما بیشتر ناظربه مسائل نظامی وسیاسی وامنیتی است ومسائل بازرگانی واقتصادی درآن نادیده انگاشته شده درحالیکه دراکثر کشورها جرم جاسوسی اقتصادی نیز درنظر گرفته شده است .[1]

[1]. نشریه پیام قانون به نقل از الیاس بوجار، پیشین

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل سوم:

پیشگیری از جرایم سایبری و رسیدگی به آن

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بخش اول : جرم وامنیت درفضای سایبر

یکی از عناوینی که غالباً درمتون حقوقی وقوانین جزایی جرم اطلاق می گردد « جرایم برضد امنیت داخلی وخارجی کشور» است که جاسوسی می تواند یکی ازمصادیق آن به حساب آید ؛ به عنوان مثال درحقوق جزای فرانسه ، مصر، عراق وایران ، جاسوسی یکی از مصادیق جرایم علیه امنیت داخلی وخارجی کشور به حساب آمده است.[1] لذاطرح مبحث امنیت وراههای پیشگیری وکشف جرایم سایبری دراین بخش ضروری به نظر می رسد.

امنیت به مثابهٔ یک ارزش جدی است که بقای موجودیت هر چیز متکی بر حفظ آن است؛ امنیت به خودی خود یک مفهوم انتزاعی است که ریشه در به خطر افتادن تمامیت ارزش ها اعم از ملموس و غیر ملموس دارد که در معرض نیستی و نابودی قرار دارند. بنابراین امنیت فی نفسه یک احساس است که از لزوم حفظ منابع ارزشمندی که تمامیت آن در معرض مخاطره و ناامنی قرار می گیرد درک می شود.

باید برآن بود که مفهوم امنیت متغیری نسبی است که به هر میزان که منابع ارزشمند متکثرتر گردد، به همان میزان بر گسترهٔ آن افزوده می شود. بر همین اساس موضوع امنیت که تا جنگ جهانی دوم کمتر مورد توجه قرار می گرفت، با افزایش ارزش های اجتماعی، متحول شده و رفته رفته از یک مفهوم بسته که محدود به امنیت نظامی ازنوع امنیت داخلی، همچون اغتشاشات و درگیری های مسلحانهٔ داخلی و امنیت خارجی، همچون جنگ می شد، فراتر رفته و با توجه به منابع ارزشمند هر جامعه، ابعاد جدیدتری یافته است؛ از همین رو دیگر امنیت محدود به امنیت داخلی یا خارجی نیست، بلکه با تغییر رویکرد به سوی «امنیت ملی» و ارائهٔ تعریف موسعی از آن، آن را به امنیت سیاسی، نظامی، اقتصادی، اجتماعی و به طور کلی «منافع ملی» تقسیم می کنند. بوزان[2] امنیت را بر پنج دسته تقسیم می کند : نظامی ، سیاسی، اقتصادی ، اجتماعی و زیست محیطی .[3]

---

[1] .ساریخانی، عادل، پیشین،ص۳۱

[2]. Bozan

[3] .دربارهٔ مفهوم امنیت ملی ر.ک.

الف-دایرةالمعارف دموکراسی، زمستان ۱۳۸۳،زیر نظر سیمور مارتین لیپست، ترجمه کامران فانی و دیگران، چاپ مرکز چاپ و انتشارات وزارت امور خارجه

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بنابراین امنیت ملی «نه تنها شامل حفاظت از دولت، سرزمین های تابعه و افراد آن در برابر تهاجم فیزیکی یک نیروی خارجی است؛ بلکه حفاظت از منافع مهم اقتصادی، سیاسی، نظامی، اجتماعی، فرهنگی و ارزشی دولت در برابر حمله های ناشی از منابع داخلی و خارجی را در بر می گیرد که ممکن است این منافع را تضعیف، فرسوده و نابود سازد و در نتیجه بقای دولت را به مخاطره اندازد. چنین حفاظتی ممکن است با ابزارهای نظامی یا غیرنظامی پیگیری شود.»[1] وارد ساختن گونه های دیگر از امنیت زیر امنیت ملی وابسته به خواست دولتها است.به طوریکه امروزه شاهد گونه جدید امنیت تحت عنوان «امنیت فضای سایبر » هستیم.تأمین امنیت فضای سایبر بدلیل وابستگی منافع ملی و امنیت ملی به آن مدتی است که مورد توجه دولتها قرار گرفته است .

وابستگی زیر ساختهای حیاتی کشورها به فن آوری اطلاعات وارتباطات ،آسیب پذیریهای آنها را در برابر تهدیدات سایبری افزایش داده و لذا امنیت ،اطلاعات و سیستمهای اطلاعاتی بیش از پیش حائز اهمیت شده و بلکه یکی از مؤلفه های امنیت ملی می باشد. به طوریکه متخصصان امنیت اذعان می دارند:«کارشناسان امنیت داخلی ،علی رغم به کارگیری جدیدترین انواع رایانه،ازوجودآنها در هراسند.گویی رایانه ای کردن امور بیش از آنکه موجبات امنیت ما را فراهم آورد، به آسیب پذیرتر شدن کلی جامعه می انجامد.بنا به ادعای یک کارشناس؛ رایانه ها درکلیه ی امور زندگی ما،از دفاع ملی گرفته تا شبکه های حمل ونقل،سیستم های توزیع موادغذایی، شبکه های برق رسانی و تقریباًتمامی ابعاد زیر بنایی موجود نقشی حیاتی ایفا می‌کنند و کسی که با طرز کار این نظام آشنایی داشته باشد این توانایی را دارد که آسیب های جدی بدان وارد و حتی کل اقتصاد مملکت را دچار اختلال کند. پس مشاهده می شود که یک نفر به تنهایی قادر است ،کل اقتصاد مملکت را دچار اختلال کند!برای مقابله با این قضیه باز باید مؤسسات امنیتی هر چه بیشتری را به رایانه مجهز کرد.»[2]

ب-پاپ، دانیل. س وآلبرتس. دیوید.س، پاییز ۱۳۸۵،**امنیت در عصر اطلاعات، الزامات امنیت ملی در عصر اطلاعات** ؛ ترجمه علی علی آبادی و رضا نخجوانی، انتشارات پژوهشکده مطالعات راهبردی

[1]. پاپ، دانیل. س و آلبرتس. دیوید.س؛ **پیشین**، ص ۱۵

[2] .هیبلزگری، کریس ، ۱۳۸۱، **جنگ پست مدرن سیاست نوین درگیری**، ترجمه احمد رضا تقاء، انتشارات ،دوره عالی جنگ، ص،۶۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

در این میان چند نکته قابل ذکر است؛ **نخست اینکه**، چنانچه گفته شد امنیت خود ارزشی موسع است که ازارزش‌های دیگر نشأت می‌گیرد؛ در فضای سایبر این ارزش‌ها شامل تمامیت اطلاعات و سیستم ها[۱]، محرمانگی اطلاعات[۲] و سیستم‌ها و دسترس پذیری[۳]، به عنوان ارزش‌های ماهوی (که ارزش‌های بنیادین یا ارزش‌های اولیه نیز گفته می‌شود) می باشند. ازنظر شکلی نیز معیارهایی برای این ارزشها بیان شده است که شامل: استنادپذیری[۴]، انکارناپذیری[۵] و پاسخگویی[۶] می‌باشند. بنابراین امنیت به مجموع این معیارها بار می‌شود و خود ارزشی ثانوی می‌یابد. ارزش این بحث در حملات سایبری مشخص می‌شود؛ به همین خاطر جرایم امنیتی در فضای سایبر علیه هر یک از ارزش‌های فوق واقع می شود و در اشکال مختلفی بروز می یابد که هر یک ارزش خاصی را به مخاطره می اندازند.

دوم اینکه، تهدیدات و حملات سایبری هم می‌توانند امنیت ملی و هم امنیت بین المللی را با چالش مواجه می‌سازد. اگرچه امنیت ملی به امنیت فضای سایبر وابسته شده است اما امنیت فضای سایبر محدود به امنیت ملی نمی‌شود؛ این فضا فرامرزی و جهانی است، محدود به مرزها نیست . مبادلات، ارتباطات، تجارت و بانکداری و مواردی این چنینی، اکنون با بهره گیری از فضای سایبر، مرزها را درنوردیده و گستره ای جهانی یافته است؛ برای مثال در جهان کنونی تصور بانکداری غیر الکترونیکی

---

[۱]. تمامیت یا یکپارچگی یعنی جلوگیری از تغییر و تبدیل غیر مجاز داده ها. بدین معنی که فقط اپراتور معرفی شده می تواند تغییرات را در سیستم وارد کند. مفهوم یکپارچگی مستقیماً به قابلیت اطمینان در کارکرد مؤثر و بدون خطای سیستم اطلاعات مربوط می شود.

[۲]. محرمانگی یعنی جلوگیری از افشاء غیر مجاز اطلاعات، عرفاً، محرمانگی به معنای دستیابی کنترل شده به اطلاعات بود. این اصطلاح بدین معناست که دستیابی به داده ها تابعی از شخص طالب دستیابی و نوع دستیابی است. برای یک شخص دستیابی می تواند فقط خواندنی یا(read only) و برای دیگران می تواند خواندنی و نوشتنی (read and write) باشد. امتیازهای دیگر دستیابی نیز را می توان به همین صورت تنظیم کرد.

[۳] .دسترس پذیری به معنی جلوگیری از محدودیت غیر مجاز در استفاده از اطلاعات و منابع است. اطلاعات بایستی در هر زمانی که لازم است قابل دسترس باشد

[۴] .به معنای شناسایی قبلی عوامل مبادله اطلاعات یا اطمینان از صحت هویت شخصی که مشخصات خود را ارایه کرده است. این شناسایی صرفاً ناظر به ارایه کنندگان و کاربران نیست، بلکه تعیین هویت شامل، خدمات، ابزارها و حتی متقاضیان نیز می گردد.

[۵] .یعنی اثبات این که اطلاعات حقیقتاً برای گیرنده فرستاده شده و فرستنده حقیقتاً همان فردی بود که اطلاعات را ارسال کرده است

[۶] .با این معیار چارچوب مسوولیت های طرفین تعریف و اجرا می گردد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

چیزی غیرممکن و محال می نماید، چرا که اساس فعالیت های بانکی مبتنی بر سرعت و دقت مبادلات است که این امر جز با استفاده از تسهیلات فضای سایبر ممکن نمی نماید.

هرچند برخی از راه بررسی اهداف مجازات‌ها به پیشگیری کیفری از جرایم ارتکابی در فضای سایبر همچون فضای واقعی یا فیزیکی اندیشیده اند و با بیان اینکه سزادهی و اعمال مجازات از دیرباز به عنوان راهکاری در راستای اعاده نظم عمومی و ترمیم جراحاتی که در اثر عمل بزهکار بر پیکره جامعه وارد آمده، مورد توجه نظام‌های حقوقی مختلف قرار گرفته است و در دوران معاصر نیز ابزارهای اجبارکننده و قهرآمیز حقوق کیفری، به عنوان یکی از اشکال واکنش اجتماعی علیه بزهکاری و پیشگیری از تکرار جرم، تابع همان رسالت ها و اهداف است. به دنبال آن هستند که نشان دهند ؛ اعمال مجازات بر بزهکارانی که در فضای مجازی مرتکب جرم می‌شوند نیز از این اهداف تبعیت می‌کند. جدا از اینکه پیشگیری کیفری اساساً و به طور مستقیم از تدابیر پیشگیری از وقوع جرم به مفهومی که در سیاست جنایی به کار می‌رود، محسوب نمی شود؛ باید خاطر نشان کرد که بستر جرم سایبری یعنی فضای سایبر به گونه‌ای نیست که دقیقاً بتوان از همان چهارچوب های فضای بیرونی بهره برد.[1]

بخش دوم :پیشگیری از جرایم سایبری

جرایم سایبری، پدیده ای انکار ناپذیر در حوزه سیاست جنایی بسیاری از کشور هاست همین امر باعث شده است بحث پیشگیری از جرایم سایبر اهمیت ویژه ای یابد.

اتخاذ سیاست های پیشگیرانه مقتضی ومتناسب با فضای سایبر هرچند با توجه به ویژگی های این فضا (جهانی وبی مرز بودن، پنهانی وپوشیده بودن و کنترل ناپذیر بودن) چالش های جدی در برابر اتخاذ تدابیر پیشگیرانه ایجاد کرده است لیکن اهمیتش را به جهت ایجاد امنیت در این فضا از دست نمی دهد.

---

[1]. قناد، فاطمه؛ ۱۳۸۸، **پیشگیری کیفری از جرایم ارتکابی در فضای مجازی**، مجموعه مقالات نخستین همایش ملی پیشگیری از جرم: پیشگیری از تکرار جرم و بزه دیدگی، دفتر تحقیقات کاربردی پلیس پیشگیری ناجا، ص ۲۱۹

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

با پیشگیری اجتماعی از جرایم سایبر با توسل به کدهای رفتاری وپیشگیری کرداری در حیطه های مختلف شغلی،آموزش کاربران واطلاع رسانی واطلاع گیری ورعایت حقوق وآزادی بیان وعقیده و احترام به حریم خصوصی افرادوحکم رانی مطلوب درفضای سایبرباحاکمیت قانون،شفافیت وپاسخگویی ومسئولیت پذیری دولت می توان از برخی جرایم سایبری جلوگیری نمود.

این نوع پیشگیری علی رغم تحمل هزینه های بسیار برای دولتها وتأثیری گذاری کم به ویژه در مجرمین بالقوه، دربرخی مواردهمچون جرایم علیه کودکان مؤثر واقع شده واستفاده ازآن توصیه می شود.

در مورد پیشگیری وضعی از آنجا که پیشگیری وضعی ماهیتی فنی دارد در مورد جرایم سایبر در فضای مجازی مورد استفاده بیشتر قرار می گیرد اما در عمل عواملی مانع تحقق اهداف پیشگیری وضعی از جرایم می شود.

اوّل اینکه مجرمان سایبر تخصص ومهارت بالا دارند **دوّم** انواع ابزارهای اتکاب جرم در اختیار همگان است **سوّم** در مقابل روش های پیشگیری مانند فلیترینگ[1]، فیلتر شکن ها جهت خنثی کردن شبکه های فیلتر شده توسط کاربران استفاده می شود. علاوه بر آن محدودیت های حقوق بشری که در سه اصل آزادی بیان، جریان آزاد اطلاعات وحریم خصوصی می باشدو در قانون اساسی کشور ما نیزاز موانع پیشگیری وضعی می باشد یکی از مشکلات سد راه پیشگیری وضعی است.

۳-۲-۱ راههای پیشگیری از جرایم سایبری

۳-۲-۱-۱ حفاظت

حفاظت یا به تعبیر دیگر سد بندی در برابر حملات سایبری به اقدامات فنی گفته می شود که در سامانه ها و شبکه ها در راستای پیشگیری از رخنه گری اتخاذ می شود. نباید پنداشت که حفاظت از سامانه ها و شبکه ها تنها محدود به پیشگیری از نفوذ غیرمجاز یا رخنه گری است بلکه برخی تدابیر پیشگیرانه ناظر به زمانی است که مرتکب موفق به ورود به سامانه یا شبکه شده است؛ ولی هنوز دست به اقدامات خرابکارانه نزده است؛ از این رو حفاظت از سامانه یا شبکه و داده های موجود در آن شامل هر اقدامی است که بتواند در لباس تدابیر امنیتی ظاهر شود. با این حال حفاظت از سامانه یا

[1]. پالایش ،معادل فارسی فیلترینگ

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

سیستم بیشتر با بارو یا دیوار آتشین مشهور شده است ولی باید دانست که نصب باروی آتشین یکی از روش های حفاظت است؛ هرچند که مهمترین و برجسته ترین آنها به شمار می رود.[۱]

باروی آتشین یا دیوار آتشین[۲]« یک سیستم امنیتی است که با هدف محافظت شبکه یک سازمان در مقابل تهدیدهای خارجی طراحی شده است؛ مثلاً اشخاص کنجکاوی که بدون مجوز از شبکه های دیگری چون اینترنت وارد یک سیستم می شوند. این سیستم امنیتی که معمولاً ترکیبی از سخت افزار و نرم افزار است، از ارتباط مستقیم کامپیوترهای موجود در شبکه سازمان با کامپیوترهای خارج از شبکه جلوگیری می کند. در عوض تمامی ارتباطات از طریق یک سرویس دهنده پراکسی که خارج از شبکه سازمان است، هدایت شده و همین سرویس دهنده است که درباره امن بودن یا نبودن عبور یک پیام یا فایل از طریق شبکه سازمان تصمیم گیری می کند.»[۳]

۳-۲-۱-۲ پالایش

پالایش یا غربال داده ها از یک نظر همان حفاظت است ولی نه حفاظت داده ها و سامانه ها بلکه حفاظت کاربرها و مشترکین اینترنتی. به همین دلیل چون نمی‌توان همچون حفاظت از داده ها یا سامانه‌ها، دیوارهایی برای حفاظت کاربران کشید، پس باید اطلاعات را غربال کرد و محتویات مجرمانه و غیر قانونی را با تدابیر فنی پالایش کرد.

پالایش معادل فارسی فیلترینگ است و فیلتر واژه ای است که از زبان های انگلیسی و فرانسوی وارد زبان فارسی شده است و شیوع و کاربرد فیلتر و فیلترینگ برای اینترنت به دلیل سابقه کاربرد آن برای علومی نظیر شیمی است. عموماً فیلتر، صافی، پالایه یا به پارچه یا کاغذ یا آلتی که برای تصفیه کردن آب یا مایع دیگر به کار می رود، معنا می شود[۴] و طبعاً عملی را که فیلتر یا همان وسیله صافی کننده انجام می‌دهد، فیلترینگ گویند. بنا به انتخاب فرهنگستان ادب فارسی معادل فارسی این اصطلاح پالایش و معادل فارسی فیلتر، پالایه است.

مبنای اصلی فیلترینگ انسداد محتویات مضر و در امنیت گذاشتن کاربران و مشترکین است. در واقع فیلترینگ پرده ای نازک و خدشه پذیر بر چهره زشت و سیاه اینترنت است. اما فیلترینگ در برخی

---

[۱]. پاکزاد ،بتول ، پیشین ،ص ۲۸۱ به بعد

[۲]. Firewall

[۳] .هیأت مؤلفان و ویراستاران انتشارات مایکروسافت، پیشین، ص ۳۰۴

[۴] .عمید، حسن؛ **فرهنگ فارسی عمید**، موسسه انتشارات امیرکبیر، چاپ سی و یکم، ۱۳۸۴ ص ۹۲۸

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

موارد فراتر از انسداد محتویات مضر عمل می کند و در خدمت افراد یا دولت هایی قرار می گیرد که در صدد حذف اینترنت یا حداقل کنترل یکجانبه آن هستند.

۳-۲-۱-۳ کنترل

کنترل و نظارت به معنای دیدبانی فضای سایبر است. کنترل بر خلاف دو تدبیر حفاظت و پالایش، صرفاً جنبه فنی ندارد و بلکه می تواند چهره انسانی نیز داشته باشد؛ یعنی برخی افراد همچون پلیس یا ارایه دهندگان خدمات اینترنتی (رساها)[۱] یا حتی اشخاص و سازمانهای غیر دولتی[۲]درپی نظارت و کنترل مبادلات اینترنتی برآیند. بنابراین کنترل و نظارت را می توان پلیس سایبری نیز نام گذاشت.

نظارت سایبری نهادهای امنیتی و پلیسی نخستین ومهمترین راهکار کنترل تهدیدات اینترنتی و پیشگیری از حملات سایبری است تا جایی که برخی ارایه دهندگان بزرگ خدمات اینترنتی را به این سمت سوق داده تا همواره از پشتیبانی یک نهاد پلیسی یا امنیتی بهره‌مند باشند.

۳-۲-۲ چالشهای موجود درفضای سایبر

یکی ازچالش های جرایم رایانه ای در این است که مرتکب در بستری جرم را انجام می دهد که از دید همگان دور است و تنها خودش است و وسوسه های ذهنی که از خواست واقعی‌اش سرچشمه می‌گیرند. رسوخ به این فضای خلوت و تنها برای پیشگیری از وقوع جرم رایانه ای جز با شکستن حریم خصوصی افراد امکانپذیر نیست و در این صورت آنچه که صورت گرفته خودکامگی خواهد بود نه پیشگیری از وقوع جرم. در واقع توسل به سانسور[۳] یا پالایش فضای سایبر برای پیشگیری از جرم، خود یک جنایت بزرگتری است بر تعداد بیشماری از شهروندان.

---

[۱]. برگرفته از حروف اول عبارت «رساننده سرویس اینترنتی» ISP

[۲]. ان.جی.او. ها (ngo)به سازمان ها و انجمن های غیردولتی گفته می شود که در حوزه عمومی فعالیت دارند.

[۳]. سانسور در روزگار ما به دو صورت به کار برده می شود: سانسور بازدارنده و سانسور کیفری. سانسور بازدارنده پیش از انتشار به کار می رود و دومی بعد از انتشار. سانسور کیفری که مطابق حکم دادگاه و بر طبق قانون صورت می گیرد، معمولا در دمکراسی ها انجام می شود. سانسور ممکن است شخصی و بر اساس توافق نیز باشد، چنانکه در مسائل امنیت ملی ناشران با هم توافق کرده باشند که مطلبی را منتشر نکنند. سانسور به طور کلی ویژه جامعه های استبدادی و فراگیر است. اما در جامعه های دمکراتیک نیز سانسور چه شخصی و چه رسمی وجود دارد. .. همچنین در همه کشورها قانون هایی برای جلوگیری از نشر آثاری که خلاف اخلاق و عفت عمومی شناخته می شوند وجود دارد و دامنه کاربرد آن بستگی به عرف جامعه و تفسیر دادگاه از مفهوم خلاف اخلاق و عفت عمومی دارد.» به نقل از آشوری، داریوش؛ **دانشنامه سیاسی**، انتشارات مروارید، چاپ چهاردهم، ۱۳۸۶، ص۱۹۶

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۳-۲-۳ چالشهای حقوق کیفری درفضای سایبر

به اعتقادبسیاری ازاندیشمندان حقوقی ، جرایم محیط سایبر چالشهای جدی برای مدل سنتی موجود حقوق کیفری ایجاد کرده است به نحوی که حقوق کیفری کنونی کارایی لازم رادرمواجهه بامشکلات حادث درفضای سایبرکه به طورکلی سازماندهی متفاوتی از جهان واقعی دارد نخواهد داشت وهمین امر نیاز به ایجادسازمان نوین از حقوق کیفری را برای این فضا ضروری می نماید .یک علت این امر شاید آن است که علی الاصول براساس واقعیات تاریخی، فرهنگی واجتماعی هر جامعه ای طی اعصاروقرون ایجاد شده وشکل گرفته است وبابروز واقعیات اجتماعی خاصی که درگذرزمان ایجاد می شوند دچارتعارض شده وقادر به حل مشکلات بوجود آمده نمی گردد.

این رویکردنوین درعرصه حقوق جزای ماهوی سایبرکمترودرعرصه حقوق جزای شکلی بسیار بیشتر مشهوداست.درحقیقت،مشکلاتی که جرایم محیط سایبردرعرصه اجرا بوجودآورده است بسیاربیشتراز آنی است که قابل تصورباشدودربسیاری اوقات چنین به نظر می رسد که حقوق جزا درمرحله اجرا دربرابراین طیف جرایم نوین به استیصال وبن بستی جدی رسیده است.این مشکلات بیشتر درراستای ویژگیهای منحصر به فردمحیط سایبراست که سابقاًحقوق جزای کلاسیک باآن برخورد نکرده و در بسیاری اوقات پاسخی برای آن پیش بینی نکرده است .این مشکلات درعمل برنحوه مسؤولیت اشخاص دراین فضا نیزبی تأثیرنبوده است درواقع مشکلات اجرایی دراین فضاحتی مسؤولیت اشخاص رانیز به چالش کشیده ونیازبه طراحی یک سازماندهی نوین رادراین حوزه باعث گردیده است.[۱]

۳-۲-۴ چالشهای تحصیل ادله درفضای سایبر

یکی از چالشهای پی جویی فعالیّتهای مجرمانه در حوزه محاسبات ، گستره ی تحصیل کلیه ادله است بطور کلی چندین عامل در ایجاد این چالش نقش دارند .

نخست: اینکه ماهیّت توزیعی شبکه هاموجب توزیع صحنه های جرم شده مشکلات عملی و صلاحیتی را به وجود آورده است به عنوان مثال در اکثر موارد امکان جمع آوری ادله از رایانه ای واقع در مکانهای مختلف فراهم نیست ، حتی اگر تشریفات بین المللی یا داخلی برای تسهیل تبادل ادله دیجیتال مناسب باشد ، این کار آن قدر پیچیده است که فقط در جرایم مهم قابل اجرا می باشد .

---

[۱] .فضلی، مهدی ، ۱۳۸۸a ، پیشین،ص۶۳

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دوم : اینکه از آنجا که داده های دیجیتال به راحتی قابل حذف و یا تغییرند ، لازم است هرچه سریعتر جمع آوری و نگهداری شوند . ترافیک شبکه تنها به مدت یک ثانیه به طول می انجامد ، اطلاعات ذخیره شده در حافظه ناپایدار رایانه ها فقط به مدت چند ساعت نگهداری میشوند ، و همچنین پوشه های لوگ به خاطر حجم و ظرفیت شان فقط برای چند روزنگهداری می شوند به علاوه اگر مجرمین تخصص و فرصت کافی داشته باشند برای حفاظت از خود ادله را نابود کرده یا آنها را تغییر میدهند .

سومین عامل که دراین فرایند نقش ایفاء میکند حوزه گسترده تخصصی فنی است که در زمان مواجهه شبکه ها به افعال مجرمانه به آن نیاز می شود . از آنجا که هرشبکه متفاوت از دیگری است و فن آوریهای گوناگونی به روشهای منحصر به فرد با یکدیگر ترکیب می شوند هیچ شخصی به تنهایی قادر نیست با همه شرایط آشنا بوده به همه آنها رسیدگی نماید ، بنابراین لازم است پیش از جمع آوری ادله افرادی که با فن آوری مربوط آشنائی دارند شناسایی شوند .

چهارم: حجم زیاد داده هایی است که اغلب در یک پی جویی مرتبط با سامانه ها ی رایانه ای وجود دارد . جستجوی ادله مفید در میان حجم عظیمی از داده های دیجیتال میتواند مثل یافتن سوزنی در انبار کاه باشد .

پنجم: مرتبط ساختن یک شخص با فعالیت خاص با داده های موجود در یک رایانه یا شبکه ،یکی دیگر از مشکلات است . حتی زمانی که مجرمین برای اخفای خود هیچگونه اقدامی نکرده اند باز هم میتواند از مسؤولیتهای وارده تبری جویند ، با توجه به اینکه اخفای هویت در اینترنت تلاش چندانی لازم ندارد ، مثلاً ممکن است مرتکب با استفاده از یک رایانه کتابخانه عمومی به راحتی هویت خود را مخفی کند .

فرایناستگانوگرافی که اختفای اطلاعات نیز نامیده میشود چالشهای مشابهی را برای ارزیابی به همراه دارد و کشف داده های دیجیتال را دشوار یا غیر ممکن می سازد .[1]

۳-۲-۵ چالشهای قواعد صلاحیت درفضای سایبر

سوء استفاده های فراوان از فضای سایبرباعث پیش بینی تدابیری شده که از آن جمله جرم انگاری است. آنچه مسلم است اعمال مجازات قانونی دربسترصلاحیت کیفری رخ می دهد دراین میان

[1] .زندی ، محمد ، پیشین ،ص ۷۴ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ویژگیهای متمایزومنحصر به فرد فضای سایبر نسبت به دنیای فیزیکی باعث شده تادرزمینه صلاحیت کیفری درفضای سایبرمباحثی جدی واساسی صورت گیرد وآراء مختلفی ابراز شود، بگونه ای که برخی ازآن به فضای فاقدحاکمیت یاد می کنند وبرخی معتقدند صلاحیت کیفری با جلوه های مختلف آن می تواند درفضای سایبرهمانند دنیای فیزیکی حاکمیت داشته باشد.نامعین بودن حیطه های جغرافیایی وضرورت تعیین محل ارتکاب جرم سایبری ازجمله چالشهای اصلی مبحث صلاحیت درفضای سایبر است که به آن می پردازیم .

۳-۲-۵-۱ نامعین بودن حیطه های جغرافیایی

بی تردید قوانین ومقررات حاکم بربسترعبورومروردرفضای دادوستدهای اینترنتی بامقررات موجود برای دادوستدهای تجاری درجهان واقعی بسیارمتفاوت خواهندبود. بخش عمده ای ازاین تفاوت ناشی از ویژگیهایی است که زمینه حضورراه دور را دراینترنت فراهم کرده ،شبکه رابلحاظ فن آوری از بعد مکانی وفیزیکی متمایز می کند درحقیقت شبکه آنچنان نسبت به موقعیت جغرافیایی بی ربط است که تعیین مکان فیزیکی یک منبع یا کاربراینترنتی اغلب ناممکن است.آگاهی از این موقعیت مکانی برای عملکرد شبکه وایجاد کنندگان آن اهمیتی ندارد.آدرسهای اینترنتی جایگاه آنهارا درشبکه مشخص می کند نه درمکان وموقعیت زمینی ،البته برخی از آدرسهای اینترنتی مشخص کننده ی جغرافیایی یا مشخص کننده هایی راکه ازنظر جغرافیایی تعیین شده اند درخود دارند برای نمونه یک آدرس اینترنتی دارای پسوند uk دربریتانیای کبیر قراردارد ولی بیشتر آدرسهای اینترنتی فاقد این گونه تعیین کننده های جغرافیایی هستند.مهمترازآن همه آدرس های اینترنتی به راحتی انتقال پذیرند.دراین حالت هماهنگی وهمسویی میان فضا ومکان واقعی از یک سو وفضای مجازی رایانه ای وجود ندارد. براساس قواعد صلاحیت قضایی[۱] اگر رکن مادی یک جرم درون حوزه قضایی شروع یا کامل شده باشد آن حوزه قضایی صالح به رسیدگی خواهد بود. باتوجه به ماهیت جرم های اینترنتی تعیین محل ارتکاب جرم یا محل حصول نتیجه همیشه وبه آسانی امکان پذیر نیست.[۲]

۳-۲-۵-۲ ضرورت تعیین محل ارتکاب جرم سایبری

جرم سایبری به لحاظ ماهیت مجازی نمود عینی وملموس شبیه آنچه درجرمهای سنتی مانند ضرب

---

[۱] .صلاحیت قضایی درقبال مجرمان

[۲] .زندی ، محمد ، پیشین ،ص ۷۸ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

وجرح یا سرقت مشاهده می کنیم از خود به نمایش نمی گذارد بلکه جرم سایبر درواقع دربستر دادوستد های الکترونیکی وعلیه داده ها واطلاعات وگاه به ندرت علیه سامانه های فیزیکی وسخت افزاری رخ می دهد. درجایی که جرم سایبر برداده ها ارتکاب یافته تعیین محل ارتکاب جرم، کاری بس دشوار به نظر می رسد. محل وقوع جرم سایبر به طور دقیق عبارت است از:محل ومکانی که این داده ها دستخوش حمله های مجرمانه قرارگرفته ودگرگون شده اند. چگونه می توان یک رخداد غیر فیزیکی ومجازی رادردنیای فیزیکی ودربعد مکانی جستجوکرد؟

بااین وصف قوانین دادرسی سنتی که باپارامترهایی همچون محل ارتکاب جرم (صلاحیت سرزمینی) تبیین شده اند کارایی خودرااز دست خواهد داد،چون ما نمی دانیم جرم درکجا واقع شده است.

۳-۲-۵-۳ صلاحیت قضایی در قبال مجرمین

مسائل مربوط به صلاحیت قضایی در قبال جرائم ، تقریباً همیشه با در نظر گرفتن محل ارتکاب آنها بیان می‌شوند. این بدان دلیل است که صلاحیت قضایی جنایی همواره بر مبنای حضور واقعی و فیزیکی مجرم در درون حوزهٔ استحفاظی و در مقابل میز محاکمه تعیین می‌شود. براساس قواعد صلاحیت قضایی اگر عنصر مادی یک جرم درون حوزهٔ قضایی شروع یا کامل شده باشد، آن حوزه قضائی صالح برسیدگی خواهد بود. در مورد جرائم چند صلاحیتی، مانند آدم‌ربایی، تنها کافی است که یک عنصر مادی از جرم، درون یک حوزه قضائی در حال انجام باشد تا آن حوزه صالح برسیدگی شناخته شود.

تعامل و ادغام این قوانین ممکن است کاربران اینترنتی را با احتمال مجرم بودن درهرحوزه ذی صلاحی که با اینترنت در ارتباط است روبرو کند. همچنین ماهیت اینترنت امکان ارتباط متقابل بین چندین حوزهٔ قضایی را فراهم آورده و عناصر یک جرم ممکن است نه تنها در مکان و حوزه‌ای با حضور فیزیکی مجرم شروع شده، و یا به نتیجه رسیده باشند، بلکه این امکان نیز هست که در تمام حوزه‌های دیگری که در اثر عملکرد کاربر به صورت الکترونیکی درگیر شده‌اند نیز بحث وقوع جرم مطرح باشد.[۱]

اما مسئله مهم اینجاست که با توجه به ماهیت جرایم اینترنتی تعیین محل وقوع جرم و یا محل حصول نتیجه همیشه و به آسانی مقدور نیست و به فرض شناسایی محل ارتکاب جرم و یا محل

[۱]. زندی ، محمد ، پیشین ،ص ۷۸ به بعد

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

حصول نتیجهٔ جرم (در صورت تعدد محلهای ارتکاب)، کدام حوزه صالح به رسیدگی خواهد بود و اگر چندین کشوردرگیر چنین جرایمی شده باشند، اینکه کدام کشور و مهمتر اینکه داخل هر کشور، کدام‌یک از حوزه‌های قضایی داخلی، صالح به رسیدگی خواهند بود، موضوع بحث‌است!

قریب به اتفاق کشورهای پیشرفته(حدود ۴۰ کشور)، با عضویت در کنوانسیون بین المللیِ جرایم محیط سایبر، تحت عنوان کنوانسیون بوداپست ـ۲۰۰۱، سیستم واحدی را که کنوانسیون در خصوص کلیات، تعاریف، جرایم، مجازاتها و دادرسی کیفری جرایم محیط سایبر پیشنهاد نموده، بطور متحد پذیرفته‌اند.

۳-۲-۶ کنوانسیون جرایم محیط سایبر (بوداپست ۲۰۰۱)

بخش دوم از فصل دوم کنوانسیون، تحت عنوان صلاحیت، به تبیین اصول کلی صلاحیت کشورهای عضو در رسیدگی به جرایم محیط مجازی پرداخته.

در این بخش تنها یک ماده (ماده ۲۲) دارای ۵ بند، به این مهم اختصاص یافته. هر چند نقد ماده ۲۲ کنوانسیون، در حوصله این مقال نمی‌گنجد، اما بناچار و به نحو گذرا به بررسی این ماده می‌پردازیم:

بند ۱:«هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و مقررات بنماید که در صورت لزوم در زمانی که جرم در موارد ذیل به وقوع می‌پیوندد، صلاحیت رسیدگی به هر یک از جرایم مندرج در مواد ۲ تا ۱۱ کنوانسیون را بوجود آورد:

الف) جرم در قلمروش بوقوع پیوسته باشد. یا:

ب) جرم در کشتی‌ای بوقوع پیوسته که پرچم آن کشور بر فراز آن برافراشته باشد. یا

ج) جرم در هواپیمایی بوقوع پیوسته که مطابق مقررات آن عضو به ثبت رسیده. یا:

د) در جایی که جرم مورد نظر مطابق قوانین جزایی قابل مجازات شناخته شده و توسط تبعه‌اش ارتکاب یافته یا جرم ارتکابی از جمله جرایم واقع در حوزه صلاحیت جهانی حقوق جزا باشد.»[۱]

صدر بند ۱ ماده ۲۲ به گونه‌ای نگارش یافته که این امید را زنده می‌کند: که کشورهای عضو مجاز شناخته شده‌اند تا قوانین خاص و جدیدی در راستای پیشگیری و مبارزه با جرایم محیط سایبر و

---

[۱]. جلالی فراهانی، امیر حسین ، ۱۳۸۸b، **کنوانسیون جرایم سایبر وپروتکل الحاقی آن** ، معاونت حقوق وتوسعه ی قضایی قوه قضائیه ، خرسندی ،ص ۹۳

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

منطبق با ماهیت مجازی شبکه، وضع نمایند. اما بلافاصله با برشمردن شقوق ۴ گانه، این گمان را از ذهن بیرون می‌برد و وضع به حالت دادرسی‌های سنتی برمی‌گردد.

شقوق چهارگانهٔ بند ۱ ماده ۲۲ دقیقاً همان مواردی را دربرمی‌گیرد که در دادرسی‌های کیفری سنتی خوانده‌ایم. حال آنکه ورود آنها در قوانین محیط سایبر نه تنها هیچگونه انطباقی با اوضاع و احوال و شرایط ارتکاب جرایم سایبر ندارد بلکه با آن منافات نیز دارد.

مثلاً در خصوص کشتی صاحب پرچم و یا هواپیما، فرض ارتکاب جرم سایبر، بسیار نادر و حتی در بسیاری موارد غیر ممکن بنظر می‌رسد. حتی اگر عقیده داشته باشیم که: «فرض محال، محال نیست» ، باز هم این ماده بسیار ناقص بنظر می‌رسد چون زمانیکه ما درگیر بحث تعیین صلاحیت سرزمینی کشورها در جرایم سایبر هستیم، بحث از جرایم ارتکابی در کشتی و هواپیما، لغو و بیهوده است چرا که این موارد (کشتی، هواپیما و ...) تحت شرایط خاص خود، جزئی از قلمرو حاکمیت کشور صاحب پرچم به حساب آمده و ابهام و اجمالی در صلاحیت کشور صاحب پرچم در مورد رسیدگی به جرایم ارتکابی در این گونه ادوات وجود ندارد و فرقی نیست میان جرایم سنتی مثل قتل و یا ضرب و جرح و ... و جرایم سایبری ارتکاب یافته در کشتی و هواپیما.

در خصوص جرایم ارتکابی توسط تبعه و یا جرایم حوزه صلاحیت جهانی، در قوانین دادرسی سنتی هیچ‌یک از کشورها ابهامی در صالح بودن کشور صاحب قلمرو نیست و اصلاً نیازی به دوباره نویسی این موارد در بند ۱ نبوده است.

بحث اصلی، حل این مسئله است که در جرایم سایبر، اصلاً محل وقوع جرم کجاست ؟! و مجرم کیست ؟!

زمانیکه این سؤا لات پاسخ داده نشده چگونه می‌توان به تبیین صلاحیت سرزمینی و یا شخصی برای کشورها پرداخت ؟ آیا ابتدا نباید دانست جرم در حوزه کدام کشوروتوسط چه شخصی ارتکاب یافته و بعد، حوزهٔ ارتکابی را صالح برسیدگی دانست ؟!

بند ۲ ماده ۲۲ نیز، چون ناظر به شقوق ب تا د بند ۱ است، تبعاً با سؤالات فوق روبروست.[1]

بند ۲:«هریک از اعضاء می‌توانندحق عدم اجرایا اجرای موضوعات یا شرایط بخصوصی را درمحدوده مقررات صلاحیتی مندرج در شقوق ب تا د این ماده یا قسمتی از آن برای خود محفوظ دارند.»

[1] .جلالی فراهانی، امیر حسین ، ۱۳۸۸b، پیشین ،ص۹۴

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

به صراحت قسمت دوم بند ۳ ماده ۲، این قواعد صلاحیت را در جایی مجری دانسته که متهم در حوزه کشور عضو قرار دارد و کشور عضو آن متهم را با استناد به اصل عدم استرداد تبعه، به کشور تقاضا کنندهٔ استرداد، مسترد نمی‌دارد. پس کشور عضوی که متهم در آن قرار دارد را ملزم به احراز صلاحیت کیفری خود و محاکمه و مجازات مرتکب نموده است.

بند ۳:«هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم امکان وضع صلاحیت درباره جرایم مندرج در پاراگراف ۱ ماده ۲۴ این کنوانسیون وجود داشته باشد. این موارد درجایی است که متهم در قلمرو آن عضو قرار دارد و آن عضو نیز متهم مورد نظر را صرفاً به خاطر تابعیت و پس از دریافت درخواست استرداد از طرف دیگر دولت عضو، مسترد نمی‌کند.»

در بند ۴ ماده ۲۲کنوانسیون را معارض قوانین صلاحیت داخلی کشورها ندانسته و به نوعی خواسته تاکشورها را ترغیب به وضع قواعد صلاحیتی در این باب نماید.

بند ۴: « این کنوانسیون مانع اجرای هرگونه صلاحیت کیفری که مطابق قانون داخلی به مرحله اجرا درمی‌آید نمی شود. »

همانطور که ملاحظه میشود بازهم کنوانسیون راه حل عملی و منطقی در راستای حل معضلات صلاحیت ارائه نمی‌کند.ازسوی دیگر بدیهی است که کشورهای عضو در هرکنوانسیون ،اختیارات داخلی قانونگذاری خود در مسایل مختلف حقوقی ، خصوصاً حوزه قانونگذاری حقوق کیفری را ساقط و یا محدود نمی‌کنند وتصریح بند ۴ به این اختیار دولتها ،امری راهگشا نخواهد بود.[۱]

دربند ۵ ماده ۲۲°بحث تعارض صلاحیت دولتها در جائیکه چند کشور صالح به رسیدگی هستند مطرح گردیده اما تنهاراه حلی که ارائه شده به شور نشستن کشورهای صالح و انتخاب یک کشور و تفویض اختیار تعقیب و رسیدگی قضایی به کشور منتخب بوده است. چنانچه گذشت ، حتی بند ۵ نیز راه حلی در جهت حل تعارض صلاحیتها ارائه نداده و تنها شوروانتخاب نماینده رابرای رسیدگی کیفری پیشنهاد نموده.

مسئله اول ـ تعیین محل ارتکاب جرم سایبر :

جرم سایبر بلحاظ ماهیت مجازی وغیر واقعی خود، حقیقتاً نمود عینی و ملموسی، شبیه آنچه در جرایم سنتی مثل ضرب وجرح و یاسرقت و ... مشاهده می‌کنیم از خود به نمایش نمی‌گذارد . بلکه

[۱] .جلالی فراهانی، امیر حسین،۱۳۸۸b،پیشین، ص ۹۴

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

جرم سایبر در واقع در بستر مبادلات الکترونیکی و برروی داده‌ها و اطلاعات وبعضاً (بندرت) بر روی سیستم‌های فیزیکی و سخت افزاری ارتکاب می‌یابد .

در جائیکه جرم سایبر برروی داده‌ها ارتکاب یافته ،تعیین محل ارتکاب جرم کاری بس دشوار ودر برخی موارد حتی غیر ممکن بنظر می‌رسد . محل وقوع جرم سایبری بطور دقیق یعنی محل و مکانی که این داده‌ها دستخوش حملات مجرمانه قرار گرفته ودگرگون شده‌اند .

چگونه می‌توان یک رخداد غیر فیزیکی ومجازی رادر دنیای فیزیکی و در بعد مکانی جستجو کرد؟ حتی اگر جرم سایبری بر روی قطعات فیزیکی و سخت افزاری ارتکاب یافته و باعث بروز اختلالات و یا از کارافتادگی آنها گردد، باز هم بطور قطع نمی‌توان نظر داد که محل وقوع جرم سایبری همان محل وجود قطعات سخت افزاری آسیب دیده خواهدبود . چرا که در قریب باتفاق اینگونه جرایم ، عمل مجرمانه در مکانی دیگر انجام گرفته وتنها نتیجه مجرمانه بر روی قطعات سخت افزاری پدیدار گشته است .

در هر صورت ،تعیین محل ارتکاب فعل مجرمانه(سایبری) در فضای مجازی مبادلات داده‌ها، براحتی امکان پذیر نبوده و نیست . برای مثال : کاربری در شهر لندن با مخاطب خود در شهر پاریس ارتباط اینترنتی برقرار نموده و در طی این تماس ، با نفوذ غیر مجاز به بانک داده‌های شخص مخاطب خود در پاریس اقدام به سرقت اطلاعات مورد نیاز خود از مخاطب نموده و سپس با تخریب اطلاعات باقیمانده ، بانک اطلاعات وی راترک مینماید.

حتی در این مثال ساده نیز نمی‌توان معین نمود محل ارتکاب این جرائم (نفوذ غیرمجاز_ سرقت داده _ تخریب داده) کجاست ![1]

چرا که شخص مرتکب در لندن با استفاده از برنامه‌های خاص نرم افزاری اقدام به نفوذ غیر مجاز به سیستمهای مخاطب خود در شهر پاریس نموده ودر همین حین مرتکب جرائم دیگری نیز برروی داده‌های کاربرفرانسوی گردیده و کاربرفرانسوی برروی رایانه خودنتیجه این افعال مجرمانه رابصورت بروزاختلالات در برنامه‌ها و سیستمهای خودمشاهده می‌کند. این‌ها همه درحالیست که در واقع پایگاه داده‌ها در شهر تورنتوکانادا واقع است واگر سرقت،تخریب و هرگونه جرمی بر روی داده‌ها رخ داده

[1]. دولتشاهی ، شاهپور، ۱۳۸۴ مجموعه مقاله های همایش بررسی جنبه های حقوقی فناوری اطلاعات، قم سلسبیل

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

باشد در واقع آن پایگاه داده‌ها مورد حمله قرار گرفته و کاربرفرانسوی فقط نمایشی از آنرا در پاریس مشاهده خواهد کرد.

ملاحظه میشود که جرایم محیط سایبر بر خلاف جرایم سنتی که در مکانهای مشخص و یامحصوری اعم از یک اتاق ، یک ساختمان و یا یک منطقه رخ میدهند،ممکن است درچندگوشه کره زمین ارتکاب یابند همچنین با این تفاوت که نه تنها از نقطه نظر فنی وتکنیکی بلکه از نقطه نظر حقوق کیفری نیز نمی‌توان بطور حتم مکان واحدی رابعنوان محل ارتکاب جرم برگزید .

این اوصاف تدابیرقوانین دادرسی سنتی که با پارامترهایی همچون محل ارتکاب جرم (صلاحیت سرزمینی) تبیین شده‌اند،کارائی خود را از دست خواهندداد.زیرا اصلاً دروهله نخست شروع به تعقیب و رسیدگی به این جرائم خاص نمیدانیم جرم در کدام حوزه واقع شده تا بنابه اصل صلاحیت سرزمینی کشورصالح و سپس باتوجه به قواعد پیش بینی شده در قوانین دادرسی، حوزه قضایی صالح راشناسایی نمائیم .

مسئله دوم ـ شناسائی تابعیت شخص مرتکب :

هنگامیکه بحث از تابعیت شخص مرتکب به‌میان می‌آید بلافاصله مفهوم صلاحیت شخصی در آئین دادرسی کیفری به ذهن متبادر می‌شود. اینکه مرتکب دارای چه تابعیتی است در بسیاری موارد کشور متبوع وی را صالح به رسیدگی به اتهامات وی می‌نماید چنانکه در ماده۷ قانون مجازات اسلامی نیز رسیدگی به کلیه جرائم ارتکابی توسط ایرانیان در هر کجای جهان را در صلاحیت دادگاههای کیفری داخلی دانسته است .[1]

اما در جرائم سایبری ،حتی تابعیت مرتکب نیز ناشناخته است.چرا که درفضای مجازی کاربران باشناسه‌های قرار دادی همچون IP ها (قراردادهای اینترنتی) که تماماً مجازی وغیر قابل مشاهده و لمس هستند، شناسایی میشوند و حتی در صورت شناسایی کاربر مرتکب جرم ، در واقع ما، هویت مجازی و قراردادی وی راشناسایی کرده‌ایم نه هویت واقعی او را همچنان که در ادارات تشخیص هویت پلیس کشورها صورت می‌پذیرد .

مسئله سوم ـ حل تعارض صلاحیت‌ها:

فرضی رادر نظر می‌گیریم که صلاحیت قضایی بیش از یک کشور ویا در سیستم داخلی ،بیش از یک

---

[1] . دولتشاهی ، شاهپور، پیشین

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

حوزه قضایی در رسیدگی به یک جرم و یا اتهام مرتکب احراز گردیده . ظاهراً این تعارض پدید آمده شبیه به تعارضات سنتی وتابع قواعد حل تعارضات سنتی خواهدبود.امامیدانیم درتعارض صلاحیت‌ها درحالت سنتی ،ابعاد دامنه جرم یاجرائم، مشخص ومحدود است و با توسل به راهکارهای ارائه شده ازجمله استردادو.... تا حد قابل توجهی می‌توان به این تعارضات خاتمه داد. اما نظر به دامنه شمول جرایم موضوع این بحث وفراگیر بودن وامکان ورود خسارات و زیانهای غیر قابل تصور (همانند خواباندن شبکه سراسری برق رسانی یک کشور یا چند کشورهمجوار) دیگر به سادگی قبل نمی‌توان تعارض پیش آمده در صلاحیت دولتهارا حل نمود . چرا که هر دولت آنچنان از این جرایم صدمه دیده که براحتی حاضر نیست از صلاحیت خود صرف نظر نموده و اختیار رسیدگی رابه دولتهای دیگر محول نماید.

در یک رویکرد کلی در خصوص جرایم سایبری می‌بایستی فضای ذهنی قانونگذار را از محیط واقعی و فیزیکی خارج نموده ودر محیط کاملاً مجازی و غیر واقعی قرارداد . از سوی دیگر ماهیت غیر واقعی جرایم سایبری باعث گردیده تا مرزهای جغرافیایی و مفهوم سرزمینهای مجزا، رنگ باخته و اصطلاحاً عبارت «صلاحیت غیر مبتنی برمرز» یا «صلاحیت فرامرزی» جایگزین صلاحیت های مبتنی بر حیطه بندیهای جغرافیایی سیاسی و طبیعی گردد. چرا که ماهیت جرائم سایبر اصولاً ماهیتی فرامرزی بوده و می‌بایست بدون در نظر گرفتن مکان وموقعیت فیزیکی مرتکب، محل ارتکاب و ... مورد بررسی قرار گیرند .[1]

راه حل پیشنهادی درتعیین دادگاه صالح ، تنها عبور از قواعد سنتی و در نظر گرفتن موقعیت بزه دیده است . یعنی چنانچه بزه دیده جرائم سایبر به دادگاه کیفری محل اقامت خود، تقدیم شکوائیه نماید دادگاه،تنهابر مبنای اینکه بزه دیده درحوزه آن دادگاه ساکن است می‌بایدخودراصالح برسیدگی دانسته و با قبول شکایت، اقدام به تعقیب و رسیدگی قضایی نماید . زیرا تنها محلی که می‌توان تحقیقات مقدماتی را از آنجا آغاز نمود و امکان جمع آوری آثار جرم درآن وجود دارد، محلی است که متهم در آن اقامت داشته وحداقل، نمایشی از وقوع جرم سایبر بر روی داده‌ها ویا سیستمهای او قابل رؤیت می‌باشد.

---

[1] .دولتشاهی ، شاهپور، پیشین

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مشکلی که در پی این قضیه پیش خواهد آمد، تعدد بزه دیدگان ودر نتیجه تعدد مراجع قضایی صالح به رسیدگی خواهدبود . مثلاً در جرم انتشار ویروسهای مخرب رایانه ای که صدها ویا هزاران کاربر را در سطح یک کشوروحتی درسطح جهان، بزه دیده خودواقع می‌سازد،چنانچه هریک از بزه دیدگان به دادگاه محل اقامت خود اعلام جرم وتقدیم شکوائیه نماید ، دهها و دهها مرجع قضایی اقدام به پیگیری ، تعقیب و رسیدگی نسبت به یک جرم واحد واحتمالاً بامتهم واحد، خواهند نمود . ناگفته پیداست که مهمترین تبعات چنین اقدامی، تراکم پرونده‌های کیفری در دادگاههای متعدد و تهافت و تعارض آراء صادره خواهد بود .

بخش سوم :تدابیر شکلی

تدابیر شکلی ناظر به همان آیین دادرسی کیفری است. با این حال شاید بتوان گفت که تدابیر شکلی برای رویارویی با پدیده مجرمانه، عام‌تر از آیین دادرسی کیفری است و علاوه بر فرآیند رسیدگی به برخی تدابیر شکلی پیشگیرانه یا حتی برخی تدابیری که به ظاهر در مقررات ماهوی به آن اشاره می-شود مانند آزادی مشروط یا تعلیق اجرای مجازات نیز اشاره دارد. تدابیر شکلی، واپسین و عینی‌ترین پاسخ به اقدامات جاسوسی سایبری است؛ زیرا در این مرحله است که اقدامات جاسوسی سایبری با توسل به ادله خاص کشف و در برابر دیدگان عموم قرار می گیرد و در همین مرحله است که جاسوسان سایبری، به خاطر اقدام مجرمانه شان در برابر فرشته عدالت زانو زده و در انتظار حکم عادلانه هستند و بالاخره در همین مرحله است که عنوان‌های پیش بینی شده در مقررات ماهوی بر رفتار مرتکب تطبیق داده شده و کیفرهای پیش بینی شده در این قوانین به اجرا در می آید. پس تدابیر شکلی نقطه حساس برخورد مستقیم و سرکوبگر با جاسوسان است.[1]

[1] .پاکزاد ، بتول، پیشین ،ص۳۱۴

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بخش چهارم : تعقیب ورسیدگی جرایم رایانه ای درایران

اثبات جرم رایانه ای ومحکومیت متهم به مجازات های مقررقانونی همانند جرایم ، بدون تعقیب ورسیدگی ممکن نیست .مسأله تحقیق جرم رایانه ای مشکلات خاص خود رادارد . از نقطه نظر جرم یابی ، ضرورت دارد که پلیس ومقامات قضایی توانایی تحقیقات درمحیط های رایانه ای رابدون همکاری متهمان وکاربران دارا باشند .

پلیس ودیگر عوامل قضایی باید قادر به تحقیق وتعقیب جرایمی که درمحیط های رایانه ای رخ می دهد، باشند وقابل قبول نیست که جرایمی بدون مجازات باقی بمانند ، از این رو باید به آموزش این افراد وهمچنین وضع مقررات شکلی لازم درزمینه اختیارات مقامات تحقیق مبادرت نمایند.

۳-۴-۱مشکلات تعقیب وتحقیق واجرای احکام کیفری جرایم سایبری

کشف ، تحقیق وتعقیب جرایم سایبری بسیار دشوار است . بسیاری ازآنها عملاً کشف نمی شوند، لذا رقم سیاه[۱] جرایم دراین حوزه بسیارزیاداست.هنوز روش کارآمدی برای نظارت مؤثر براین فضا ایجادنشده وعواملی نظیر پلیس گشت سایبر[۲]وحتی روشهای فنی نظارت وکنترل ، نظیر پالایش اطلاعات غیرقانونی کافی نیست.همچنین روشهای تکنولوژیک وفناوری های نوین این امکان رابه مجرمین می دهند که آثارجرایم خود را استتار کنند ، بطوریکه راهکارهای جدیدی برای " نهان سازی جرایم رایانه ای " دراین فضا ایجاد شده اند که این امکان رابه مجرمین می دهند تا از طریق روش هایی چون رمز نگاری درظاهری قانونی مرتکب جرم شوند.

ارتکاب جرم درفضای سایبر راحت تراست وامکان دستگیری مجرمین نیز کمتر؛مجرمین سایبر به این نکته واقفند ، پس بهتراست که به جای ارتکاب سرقت اموال درجهان واقعی که خطرات آن به مراتب بیشتراست، مرتکب کلاهبرداری رایانه ای شوند که ریسک کمتری هم دارد . این امر سبب شده است که ارتکاب جرایم سایبر روزبروز فزونی بیشتری یابد.[۳]

---

۱. Dark Number
۲. Cyber patrol
۳. Brenner،Susan، op.cit

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مشکلات شکلی مرحله تحقیقات مقدماتی درجرایم سایبر به همین بسنده نمی شود؛دربسیاری از موارد حتی پس از کشف جرم ، مجرم کیلومترها دور از دسترس مقامات اجرای قانون ومقامات قضایی است وامکان تعقیب وتحقیق ازاووجود ندارد وهنوزهمکاری بین المللی نیزبدان سطح نرسیده است که برای مبارزه با این جرایم راهکاری قوی وهماهنگ ایجاد شود . حتی سندی بین المللی نیز وجود ندارد که به این جرایم جنبه جهانی بخشیده باشد بطوریکه مجرم درهر نقطه ای از جهان که یافت شد براساس قوانین بین المللی مورد رسیدگی ومجازات قرارگیرد . درچنین شرایطی چگونه می توان صحبت از مسؤولیت مرتکب واجرای قانون کیفری نمود ؟ چنین مشکلات اجرایی درحقوق کیفری ناشی ازجرایم سایبر عاملی است که سبب می شودبرآن باشیم سیاست ومدل کیفری کنونی دربرخورد باجرایم محیط سایبر چندان کارا نیست وبایدبه ترسیم وتدوین مدلهای مؤثرتری اقدام کرد.
لازم است بدانیم آنهایی که خلاف مصالح بشر ازرایانه واینترنت استفاده می کنند افرادی متخصص ، فنی ونسبتاً باهوشی هستند که بارمز ورازهای تخصصی وفنی امور پیچیده رایانه واینترنت آشنا می باشند ؛ به همین دلیل است است که متولیان مقابله بااین جرایم به سختی وپس از گذشت زمان نسبتاً زیادی آنها راکشف می نمایند.
بنابراین بسیار مشاهده شده است که بعضی از مجرمان ، کلاهبرداران ومتخلفان رایانه ای از افراد باضریب هوشی بالای فنی سازمان های جاسوسی پیشرفته انتخاب ودرباند های جرایم سازمان یافته به کارگرفته شده اند. به این ترتیب باندهای تبهکارتوانسته اند توسط اینگونه افراد با استفاده از ابزار پیشرفته رایانه ای ازطریق یافتن قربانیان دراینترنت به جرایم متعددی دست زنند . درواقع اینگونه افراد مصداق « دزد چون با چراغ آید، گزیده تربرد کالا» می باشند.بنابراین مجرمان رایانه ای افراد کودن ومعمولی نیستند که دست به اعمال مجرمانه ساده بزنند .لذا یافتن ادله وشواهد جرم علیه آنان به مراتب سخت وپیچیده تروفنی ترازدیگرمجرمان می باشد.[1]

۳-۴-۲ شیوه های افتراقی ناظر به اعمال ضمانت اجراها

فرآیند انجام تحقیقات مقدماتی و رسیدگی در دادگاه ها نسبت به اقدامات جاسوسی سایبری، همچون جاسوسی و جرایم رایانه ای بوده و در این پایان نامه به تکرار این مباحث پرداخته نمی شود.

[1]. فضلی، مهدی ، ۱۳۸۸a، ص ۷۳

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

یکی از موانع انجام تحقیقات سریع در فضای سایبر این است که « عموماً اطلاعات رایانه ای نسبت به اطلاعات و مدارک کاغذی سنتی کمتر ساماندهی می شوند. معمولاً اسناد کاغذی به صورت پرونده های شماره بندی شده بایگانی می شوند و هر یک دارای کارت شناسایی هستند و نسخه های اضافی نیز در پرونده هایی جداگانه اما مرتبط نگهداری می شوند. ولی در بسیاری موارد، اطلاعاتی که در سیستم های رایانه ای ذخیره می‌شوند، به خوبی سازماندهی نمی‌گردند؛ مثلاً ممکن است نام فایل‌ها دارای اندازه محدودی باشد یا اینکه اطلاعات توضیحی خوبی برای آنها فراهم نشده باشد.»

با وجود چالش‌های فوق، ولی سرعت انجام تحقیقات باید به مرحله‌ای برسد که با سرعت انجام جرم سایبری برابری کند یا دست کم نزدیک به آن باشد؛ زیرا در فضای کاملاً سیال و مبادلاتی سایبر، تأخیردرانجام تحقیقات به معنای از دست دادن ادله است؛ یکی دیگر ازوجوه تمایزرسیدگی به جاسوسی سایبری، استنادپذیری ادله دیجیتال است. هر ادله دیجیتالی قابل اعتماد واثبات کننده نیست. استناد پذیری ادله دیجیتال همچنین در راستای حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع‌آوری شده نیز صورت می گیرد. طبق ماده۵۰ قانون جرایم رایانه ای ایران، چنانچه داده‌های رایانه‌ای توسط طرف دعوا یا شخص ثالثی که ازدعوا آگاهی نداشته، ایجادیا پردازش یا ذخیره یا منتقل شده باشد و سامانه رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشده باشد، قابل استناد خواهد بود.[1]

۳-۴-۳ ادله اثبات دعاوی رایانه ای

یکی از ره آوردهای تکنولوژی رایانه ، ادله الکترونیکی یا ادله رایانه ای است. دلایل مذکور بادلایل موجود وسنتی دارای تفاوت های اساسی هستند وهمین امر سبب بروز مباحث نوین وجالبی دربین حقوقدانان پیرامون این ادله شده است .

باآنکه درحال حاضربواسطه تازگی این موضوع تنها بخشی ازامکانات رایانه فراهم شده با این وجود، دراین زمینه مسایل حقوقی متعددی مطرح گردیده است که گه گاه حس آنها دشوار است. مسایل مربوط به ادله ازاین جمله اند:آیا می توان پردازش ونگهداری اطلاعات رابصورت مدارک انفورماتیکی ، ابزارمعتبربرای دلیلی دانست که درصورت بروزاختلال مستند دعوی قرارگیردوآیا این

[1] .گاتن، آلن،۱۳۸۳، **ادله الکترونیکی**، ترجمه مصیب رمضانی، شورای عالی توسعه قضایی و دبیرخانه شورای عالی اطلاع رسانی، ص ۱۰۴

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

شیوه واسلوب با اقتضائات والزامات مطابقت دارد؟آیا معاملات وانتقالاتی که هم اکنون می توان به مدد رایانه به انجام رساند پاسخگوی الزامات واقتضائات قانونی ادله اعمال حقوقی می باشند؟

بی مناسبت نیست که گفته شوداطلاعاتی که اشخاص به موجب قانون یابه صبغه احتیاط برای مدتی نسبتاً طولانی نگهداری می کنند ، گاه چنان پرشمارمی شودکه حمل ونگهداری آنهامسئله می آفریند و بی شک درهزینه های عمومی اشخاص ،بویژه اشخاص حقوقی نیزتأثیرمی گذارد.درامور تجاری از جمله امتیازاتی که برای رایانه می توان برشمرد آن است که به تقلیل حجم مدارک مورد بایگانی وتسهیل دادرسی واستفاده ازآنها می انجامد.اکنون دیگردراین باب تردیدی وجود ندارد که مؤسسات اقتصادی بایدبه ثبت وضبط رایانه ای روی آورند.

درحال حاضردربرخی از سازمانها مثل بانکهاقریب به اتفاق کارها با استفاده از رایانه صورت می گیرد درنتیجه یکی ازمواردی که دراین زمینه باید توجه نمودلایل واسناد برجا مانده رایانه ای است. بنابراین وجود ادله رایانه ای، همانند خودرایانه ودیگرپیامدهای آن، امری فراگیروتوسعه پذیرواجتناب ناپذیراست.

بدین ترتیب واقعیت موجوداین تکلیف رابردوش نظامهای حقوقی قرار میدهد که جایگاه ادله رایانه ای رامشخص سازند، یا آنهارامردود بدانند ویااینکه به نحو متناسب ادله موصوف رابا قواعدومقررات اصولی خود منطبق گردانیده ومحلی شایسته برای آن درنظر بگیرند.

اهمیت قواعد ادله اثبات دعوی چه درامور حقوقی وچه درامور کیفری، به ویژه درمرحله عمل ، بسیار درخور توجه است ، زیرا مراجع قضایی فقط ادعایی رامورد پذیرش قرارمی دهند که مدعی وشاکی بتوان حقانیت خود ووجود حق راثابت کند.

باید گفت قابلیت پذیرش ادله وسوابق رایانه ای بااصول وقواعد بنیادین ادله درامورکیفری ایران منافاتی ندارد.[1]

۳-۴-۴ ضرررومسؤلیت مدنی درفضای سایبر

ضرر عبارت است ازنقص دراموال یا ازدست دادن منفعت مسلم یالطمه به سلامت وحیثیت وعواطف شخص که به طور کلی می توان آنها رابه دودسته ضررمادی ومعنوی تقسیم کرد. همانطور که دردنیای قابل لمس ممکن است کسی به جان یامال دیگری ضرروارد کند ، درفضای سایبر نیز این

[1]. جلالی فراهانی ، امیر حسین ،a ۱۳۸۸ ،پیشین ،ص۱۹۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

امکان وجود دارد که به جان یا مال دیگری ضرروارد وباعث تضرر آنها شود.قواعد مسئولیت مدنی به نوع خاصی ازضرر نظر ندارند وهدف آنها تدارک وجبران تمامی ضررهای وارده است ، اعم از اینکه ضرر به جسم یا حیثیت یامال زیان دیده وارد شده باشد.

ضرری که درفضای سایبروارد می شود ، می تواند هرکدام از انواع ضررهای فوق باشد . اما مطالعه آماری نشان می دهد که بیشترین پرونده های مربوط به مسئولیت مدنی درفضای سایبر، به «نقض مالکیت معنوی» وکمترین میزان ضررراینترنتی به لطمات جسمانی مربوط می شود . همچنین ایراد خسارت معنوی به اشخاص نیز درفضای سایبرشایع است . توهین به افراد دروب سایت هاووبلاگ ها ولطمه زدن به شهرت تجاری ونقض حریم خصوصی آنها از مصادیق ضررهای معنوی درفضای سایبراست. نتیجه این مطالعات آماری می تواند راهنمای خوبی برای قانونگذاران باشد تادرتنظیم قواعد مسؤولیت مدنی دراین حوزه به زمینه های آسیب پذیرتر بیشتر توجه وبه ضررهای قابل جبران نیزبادید وسیع تری نگاه کنند .درجایی که بااستفاده از اینترنت به حیثیت افراد تعرض می شود ، هم قانونگذار وهم رویه قضایی نمی تواند نسبت به عدم جبران آن بی تفاوت باشد.[1]

بخش پنجم :صلاحیت قضایی درمحیط مجازی

۳-۵-۱ صلاحیت کیفری دررسیدگی به جرایم سایبری

صلاحیت کیفری سنتی بیشتر بر پایه مکانی استوار است. صلاحیت کیفری در مفهوم سنتی را « می-توان به توانایی و شایستگی قانونی و نیز تکلیف مرجع قضایی به رسیدگی به یک دعوای کیفری تعبیر کرد.»[2] این توانایی و شایستگی با لحاظ محل وقوع جرم (و در برخی موارد استثنایی محل کشف جرم)، نوع و اهمیت جرایم یا درجه دادگاه مشخص می گردد ولی صلاحیت کیفری در فضای سایبر، تقریباً همه معادلات مربوط به صلاحیت سنتی را به هم ریخته است و مشکلاتی را به بار آورده است. **اوّل** اینکه در جرائم دنیای واقعی، قربانی و مرتکب لزوماً در منطقه‌ای یکسان مستقر هستند و از نظر فیزیکی در مجاورت یکدیگر می‌باشند. یک سارق نمی‌تواند فردی را مورد سرقت

---

[1] .جلالی فراهانی ، امیر حسین ،a ۱۳۸۸ ،پیشین ،ص۱۹۷

[2] .آشوری، محمد،۱۳۸۲، **آیین دادرسی کیفری**، انتشارات سمت، جلد دوم، ص ۳۹

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

قرار دهد مگر آن که هر دو آنها از نظر فیزیکی در مجاورت یکدیگر باشند. مجاورت فیزیکی این امکان را می‌دهد تا بر روی صحنه جرم به عنوان مکان اولیه تحقیقات تمرکز نمودوبا توجه به محل وقوع جرم مرجع صلاحیت دار را نیز تعیین نمود. **دوّمین** ویژگی مقیاس است. جرائم دنیای واقعی گرایش به جرائم یک به یک دارند. سارق قربانی الف را مورد سرقت قرار می‌دهد و سپس به سراغ قربانی ب می‌رود و الی آخر. در حالیکه درجرایم ارتکابی فضای سایبر تعداد قربانیان در خیلی موارد بی شمار و در سراسر جهان پراکنده هستند.(در جرایمی مانند انتشار محتویات مجرمانه ،تبلیغ ،تأمین مالی ،انتشار بدافزارها وحمله های ممانعت از دسترسی و...)به همین دلیل معیارهای تعیین صلاحیت در قوانین سنتی قابل اعمال در مورد این جرایم نمی باشدوبه همین دلیل رویه کشورها و حتی کنوانسیون جرایم سایبری توسعه موارد صلاحیت بوده است بدون اینکه درصددارائه معیارهایی برای تعیین محل وقوع جرم درچارچوب مقررات سنتی موجود باشند.درکنوانسیون جرایم سایبر قانون پاتریوت آمریکا به منظور حل این مشکل«محدوده صلاحیت دادگاه» را به «هر جایی در درون ایالات متحده» تغییر داد.[۱] این امر حائز اهمیت است زیرا قبل از این اصلاحیه ، مأموران اجرای قانون در پیگیری مجرمین با اتلاف زمان و منابع جهت کسب احکام در هر حوزه قضایی روبرو بودند. به طور مثال نمونه‌ای از مشکل صلاحیتی که وجود داشت محدودیت‌های صلاحیتی در دسترسی به محتویات ایمیل ذخیره شده بنابر حکم دادگاه بود.[۲] قبل از اصلاحات انجام شده به وسیله قانون پاتریوت «فقط دادگاه فدرال،ناحیه‌ای که آن ایمیل در آن ذخیره شده بود می‌توانست این حکم را صادر کند. اما اکنون دادگاه‌های فدرال در ناحیه‌ای که جرم تحت رسیدگی وقوع یافته، می‌تواند احکام قابل اجرا را بدون محدودیت جغرافیایی صادر کنند در عین حال دادگاه صادر کننده حکم باید براساس محل وقوع جرم دارای صلاحیت باشد.»[۳]بنابراین در زمانی است که یک مأمور تحقیق در شهر الف در جستجوی پست الکترونیکی تروریستی مظنون در یاهو باشد.دیگر لازم نیست ب حکم دادگاه را از دادگاه محل ذخیره ایمیل اخذ نماید بلکه حکم دادگاه محلی که در حال رسیدگی است برای تمام آمریکا قابل اجرا است .بنابراین محدودیت صلاحیتی مانع سرعت عمل لازم نمی شود .این امر به خاطر سهولت

---

[۱].۱۸ U.S.C. § ۳۱۲۳(a) (۱), *amended by* ۱*USA* PATRIOT Act § ۲۱٦(b) (۱), ۱۱۵ Stat. ۲۷۲, ۲۸۸-۸۹.

[۲].IbId, p,۲۹۱-۹۲

[۳].Schemmelt, TammyJ; **Www.Stopcybercrime.Com: How The U.S.A Patriot Act Combats Cyber-Crime** William Mitchell Law Review Vol۲۹/۳,۲۰۰۳,P.۹۳۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

جابجایی و سهولت دسترسی به اینترنت، ضروری است. مثلاً، تلفن‌های سلولی را می‌توان با امکان اتصال به اینترت خریداری کرد.[1]

۳-۵-۲ صلاحیت رسیدگی به جرایم سایبری درایران

در قانون جرایم رایانه‌ای ایران، صلاحیت رسیدگی کیفری نسبت به جرایم سایبری به قدر قابل توجهی افزایش یافته است. طبق ماده۲۸ این قانون، علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاههای ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

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

ب) جرم از طریق تارنماهای (وب‌سایتهای) دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد.

ج) جرم توسط هر ایرانی یاغیرایرانی درخارج ازایران علیه سامانه‌های رایانه‌ای ومخابراتی وتارنماهای (وب‌سایتهای) مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هرنهاد یامؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای (وب‌سایتهای) دارای دامنهٔ مرتبه بالای کدکشوری ایران در سطح گسترده ارتکاب یافته باشد.

د) جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیرایرانی باشد.

ماده۲۹ قانون جرایم رایانه ای به تأسی از ماده ۵۳ قانون آیین دادرسی دادگاه های عمومی و انقلاب در امور کیفری[2] محدوده صلاحیت های کیفری سایبری را افزایش داده است. طبق این ماده چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرارمی‌کند و دادگاه مربوط نیز رأی مقتضی را صادرخواهد کرد.البته

[1] .Schemmelt, TammyJ; IbId, p.۹۳۷

[2] .ماده ۵۳ ، چنانچه جرمی در محلی کشف شود ولی محل وقوع آن معلوم نباشد دادگاه به تحقیقاتی که شروع کرده ادامه می دهد تا وقتی که تحقیقات ختم ویا محل وقوع جرم معلوم شود، چنانچه محل وقوع جرم مشخص نگردد، دادگاه رسیدگی را ادامه داده و اقدام به صدور رای می نماید.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

این قانون فاقد مقرراتی خاص در مورد تسهیل یا لغو تشریفات نیابت قضایی می باشد و این امر مانع سرعت تحقیقات است.

بخش ششم : بررسی سیاست جنایی درایران وراه کارهای پیشنهادی

آنچه درسیاست جنایی بررسی شده وشاید باید مورد توجه باشد ، پاسخهای کیفری به پدیده مجرمانه است .« نظام تقنینی ایران » دراین خصوص با خلأ های جدّی روبروبوده واکنون نیز این خلأ مشهود است؛ یعنی ، دراین حوزه اکنون قانونی نیست که به طور دقیق جرم راتعریف کرده ، مجازاتهای مختلف راپیش بینی کندوقواعد شکلی وتشریفات دادرسی رابه دست دهد . هرچند تلاشهای خوبی صورت گرفته،این قانون هنوزدرمجلس تصویب نشده است هنوز هم با این خلأ قانونی روبرو هستیم. طبیعی است که این قانون باید صراحت ، شفافیت وجامعیت لازم راداشته باشد.

نخستین نکته ای که دربحث سیاست جنایی باید به آن اشاره کرد ، پاسخهای اداری وانضباطی است . نباید صرفاً به دنبال پاسخهای کیفری بود . این پاسخها به منزله آخرین حربه مطرح خواهند بود . نگاه ما نباید صرفاً مجازات گرا وکیفرگرا باشد .

دوّمین نکته دربحث سیاست جنایی ، پیشگیری از جرم بویژه جرمهای رایانه ای است. پیشگیری ازجرم می تواند از ضررهای مستقیم اقتصادی وضررهای مستقیم ونامستقیم جلوگیری کند .ضررهای مستقیمی که معمولاً مورد توجه قرارمی گیرد ، کشف جرم ، تعقیب مجرم ، دادرسی واجرای حکم است که این هزینه ها راپلیس ، نظام قضایی وسازمان زندانهای یک کشور متحمل می شوند . از جمله ضررهای نامستقیم نیز بروز عوارض جسمی وروانی برمجرم ونیز پیامدهای سوءبرای خانواده وجامعه دربحثهای اقتصادی واجتماعی است. .متأسفانه ، درایران ، بحث پیشگیری دراین حوزه کمتر مورد توجه بوده است.

سوّمین نکته دراین خصوص نقش انجمنهای صنفی دراین حوزه است . این انجمنها می توانند همکاری جدی تری رابامجموعه نهاد دولت داشته باشند؛ یعنی نهادهای غیر دولتی ونهادهای دولتی می توانند درفضای پیشگیری ازجرم همکاری بسیار تنگاتنگ ونزدیکی داشته باشند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

به هرحال،ره آورد سیاست جنایی ما می تواند این باشد که ضمن حمایت از ارزشهادرقالب چارچوب قوانین ومقررات ، ازحقوق جزابه منزله آخرین حربه استفاده کرده وتوجه وتفکرخودرا به طورعمده به بحثهایی از قبیل پیشگیری ازجرم سوق دهیم.

درحوزه قوانین ومقررات ، نقاط ضعف بسیاری هنوز وجود دارد؛ برای نمونه ، عدم کفایت قوانین موجود برای پاسخگویی به نیازهای امروز جامعه ؛ نبود سیاست جنایی مشخص درخصوص جرمهای رایانه ای ؛ کمبود نیروی متخصص فناوری اطلاعات وارتباطات بویژه درقوه قضائیه ونیروی انتظامی ؛ عدم آشنایی جامعه حقوقی بویژه استادان این رشته به مسایل حقوقی ، قانونی وامنیتی فناوری اطلاعات وارتباطات؛ نبود برنامه ، طرح ورشته های آموزشی منسجم درسطح ملی برای تربیت نیروی انسانی متخصص؛نبود تعامل وهمکاریهای دولتی یا کشوری ، منطقه ای وبین المللی درحوزه بحثهای حقوقی ؛ کمبود تجهیزات ، امکانات وفناوریهای پیشرفته رایانه ای والکترونیکی درمراکزمرتبط با حقوق فناوری اطلاعات وارتباطات؛وسرانجام،نبودآمار وارقام دقیق ازمیزان جرمهای ارتکابی .

درخصوص مورداخیربایدتوجه کردکه مادرواقع نظام آمار-بویژه درحوزه جرمهای رایانهای واینترنت- نداریم که البته بخشی ازاین مشکلات نیز بدین علت است که بزه دیدگان تمایلی به تسلیم شکوائیه ندارندوارائه کنندگان خدمات رایانه ای نیز کمترتمایل به گزارش دهی دارند.[1]

سیاست جنایی مؤثربرای مبارزه باجرایم کامپیوتری وپیشگیری ازآن بایستی مبتنی براصول ذیل باشد:

الف: آگاهی دادن به شرکتها وادارات درخصوص قابلیت خطرپذیری سیستمهای کامپیوتری وتشویق آنان درخصوص بکارگیری تدابیر امنیتی؛

ب :ارتقاء تدابیر امنیتی استاندارد شده؛

ج: کاهش موقعیتهای جرم زا وفرصت های استفاده از ابزار فنی درارتکاب جرم؛

د:تشویق بزه دیدگان به اعلام وقوع جرم؛

ه:تدوین قوانین مناسب وانجام اصلاحات ضروری درمقررات جاری کشورها؛

و:توسل به همکاریهای همه جانبه بین المللی درامر کشف جرایم کامپیوتری وشبکه ای وتعقیب مرتکبین این دسته؛[2]

---

[1] .دولتشاهی ، شاهپور، پیشین

[2]. باستانی ، برومند،پیشین، ص ۱۳۹

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۳-۶-۱ راه کارهای پیشنهادی برای حل مشکلات حقوقی درایران

ایجاد نهادهای ویژه‌ی حقوقی برای مطالعات حقوقی سایبر، بویژه تأسیس رشته های دانشگاهی و تربیت قضات و بازپرس ونیروهای پلیس که در زمینه جرایم سایبر تخصص داشته باشند.

ایجاد قوانین جدید و سازگار به محیط سایبر، زیرا قوانین سنتی جوابگوی مشکلات نیست.

قانونگذاری در این زمنیه نیازمند شناخت مختصات فضای جدید و تفاوت های ماهوی آن با فضای سنتی است.

به منظور قانونگذاری دراین فضا بایدمفاهیم جدیدی شکل گیردمانند صحنه جرم سایبر،ادله الکترونیکی، صلاحیت مجازی و مواردی از این قبیل.

مقررات آئین دادرسی کیفری وبین المللی وشبکه ای به گونه ای هماهنگ ومنسجم تبیین ، تدوین وسپس تقنین شوند.

فرهنگ همکاری باپلیس درزمینه کشف ،شناسایی وتعقیب جرائم سایبری گسترش یابد.

توجه به مقتضیات خاص جامعه ایرانی و ملاحظات مذهبی درتدوین متون قانونی سایبرمی تواند در بهبود وضع موجود بسیار مؤثر باشد.

همکاری وتعاون بامجامع بین المللی درزمینه ماهوی ، شکلی وبین المللی .

همکاری بامجامع علمی ودانشگاهی دنیا وتبادل افکاروتجربیات آنان.

۳-۶-۲ راه کارهای پیشنهادی برای مقابله با جاسوسی اینترنتی

ارائه ی تعریف واضح و مشخص ازاین جرم ورسیدن به توافق بین المللی درموردتعریف ازجاسوسی رایانه ای و اینترنتی .

ایمنی کردن رایانه های اداری و حتی رایانه های شخصی با ابزار و نرم افزار های ضد جاسوسی.

آموزش کاربران کامپیوتر حتی در سطحی ابتدایی برای آگاهی از خطرات جاسوسی و آشنایی اولیه با روش های آن.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تصویب قوانین جزایی برای جرایم کامپیوتری از قبیل جاسوسی رایانه ای و اعلام این قوانین و مصوبات به عموم مردم .

نتیجه گیری

جرم سایبری به دلیل ماهیت فنی خود « جرم فناوری پیشرفته » نیز نامیده می شود .لذا تنظیم مقررات مؤثر برای آن ،نسبت به بسیاری از سایر انواع جرایم، وابستگی بسیاربیشتری به راهکارها ودانش فنی کارشناسان دارد. دربرخی از کشورها جامعه قانونگذار ملی هنوز براین دانش اشراف نیافته است . همچنین ، بسیاری از موضوعاتی که درچارچوب جرم سایبری مطرح می شوند ، تنها با راهکارهای فنی استاندارد قابل حل هستند.

ازآنجا که جرم سایبری بربسیاری از حوزه های حقوقی تأثیرمی گذارد ، تحلیل فرایند های هماهنگ سازی قانونی درچارچوب جرم سایبری ، پیچیده تراز مطالعه مقایسه ای سایر انواع بزه کاری هااست. درسیاست های جنایی جوامع کنونی ، مسؤولیت کیفری اعتباری باید به عنوان یک «بد ضروری» وبه عنوان آخرین راهکار مورد توجه واعمال قرارگیرد. لذاپیشگیری از جرایم رایانه ای بهترین موضع جهت جلوگیری از این جرایم می باشد.

پیشگیری از جاسوسی رایانه ای درایران نیازمند درک این دو پدیده درکنار سایرپدیده های سایبری است.درک آنها موجب می شود تاجزباحربه قانون مصوب مجلس شورای اسلامی که عاری از شائبه اعمال سلیقه است ، نتوان به برخورد مناسب پدیده های ناامنی درفضای سایبر دل بست . دشمنی با اینترنت یا حذف آن از یک سوویپش بینی مصوبات مقطعی وسلیقه ای از سوی دیگر که درحال حاضردرکشور ما نمود یافته ، چاره کار نیست . این قبیل اقدامات برای محیط تازه متولد شده سایبری همچون توسل به خشونت یا محروم سازی برای تأدیب طفل است . روش صحیح برخورد با ناامنی موجود درفضای سایبر ، پیش بینی قوانین مناسب وکارشناسی شده است که قانون جرایم رایانه ای تا حدود زیادی دراین مسیر عقلانی پای گذاشته است . باید دانست که برای کنترل وضابطه مندی هرچیز جدید ، هم قانون زور دارد وهم سلایق مقطعی ، منتها اوّلی زور مبتنی برعقل است ،

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ولی دوّمی زور مبتنی بربازو وقدرت . اما اینکه کدام مناسب تراست،سعدی ناصح بزرگ جامعه ایرانی می گوید :

آدمی راعقل باید دربدن ورنه جان درکالبد دارد حمار[1]

وخلاصه اینکه تنها راه مبارزه برای پایان دادن به جاسوسی هایی که تا حد تهدید منافع ملی و دینی ما پیش رفته اند، جدا شدن از شبکه جهانی و تشکیل یک شبکه ملی درگام نخست وسپس گسترش پله ای این شبکه در میان ملت های مسلمان برای نیل به شبکه جهانی اسلام میباشد. در واقع لازم است که ما از شبکه جهانی فعلی جدا شده و تمام مراحلی را که مالکان آن شبکه پشت سر گذاردند طی کنیم؛ باشد که بتوانیم شبکه ای ایجاد کنیم که مالک آن مسلمانان باشند و مالک مسلمانان کیست به جز خدا؟

آیا هنوز زمان آن فرانرسیده که به مصداق آیه شریفه « یا ایَّها الذینَ آمَنوا مَن یَرتدَّ مِنکُم عَن دینِه فَسَوفَ یأتِی اللهُ بِقومٍ یُحبُّهم ویُحِبُّونَه أذِلهٍ عَلی المؤمنین أعِزَّهٍ عَلی الکافرین یُجاهدونَ فی سبیلِ الله و لا یُخافونَ لَومَهَ لائِمٍ ذلک فَضلُ اللهِ یُؤتیهِ مَن یشاءُ وَاللهُ واسعٌ علیم»[2]، ما مسلمانان؛ ما خودیها اختلافات درونی خویش را کنار گذاشته و در برابر جهان کفر قد علم کنیم و جهانی بسازیم سر تا سر امنیت، صلح و آزادی؛ جهانی که نه بر پایه نظم نوین بلکه برای پایه نظم مبتنی بر تقوا استوار باشد؟

۱.سعدی شیرازی، مصلح الدین،۱۳۷۸،**بوستان**، حکایت دوم از باب اول: در عدل و تدبیر و رای، انتشارات علمی، چاپ پنجم

۲. قرآن کریم سوره مبارکه مائده آیه ۵۴

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فهرست منابع

منابع فارسی

الف : کتب

۱. قرآن کریم
۲. نهج البلاغه ، ترجمه محمد دشتی ، انتشارات مشهور ، ۱۳۸۰ ، نامه۵۳
۳. اصلانی ، حمید رضا ، ۱۳۸۴،**حقوق فناوری اطلاعات** ،تهران ، انتشارات میزان
۴. آشوری، محمد،۱۳۸۲، **آیین دادرسی کیفری**، انتشارات سمت، جلد دوم
۵. اولریش ،زیبر،**جرایم رایانه ای**،ترجمه ی محمد علی نوری و دیگران، ۱۳۸۳،تهران،انتشارات گنج دانش
۶. باستانی ، برومند ، **جرائم کامپیوتری واینترنتی جلوه ای نوین از بزهکاری** ،تهران بهنامی ، ۱۳۸۳
۷. پاپ، دانیل. س و آلبرتس. دیوید.س؛ پاییز ۱۳۸۵،**امنیت در عصر اطلاعات، الزامات امنیت ملی در عصر اطلاعات** ؛ ترجمه علی علی آبادی و رضا نخجوانی، انتشارات پژوهشکده مطالعات راهبردی
۸. جعفری لنگرودی، محمد جعفر،**ترمینولوژی حقوق**، کتابخانه گنج دانش، ۱۳۷۶
۹. جلالی فراهانی ، امیرحسین ، ۱۳۸۸،**حقوق فناوری اطلاعات وارتباطات** (مجموعه مقالات)، تهران، روزنامه رسمی جمهوری اسلامی ایران
۱۰. جلالی فراهانی، امیر حسین ، **کنوانسیون جرایم سایبر وپروتکل الحاقی آن** ، معاونت حقوق وتوسعه ی قضایی قوه قضائیه
۱۱. حافظ شیرازی، خواجه شمس الدین محمد، ۱۳۷۰، انتشارات حافظ نوین ، مصحح عبدالرحیم خلخالی، **غزلیات**
۱۲. حسنوی، رضا، فرسایی، داریوش ، **فرهنگ تشریحی رایانه** ،ص۱۵۰و۱۵۱
۱۳. حسن بیگی ، ابراهیم ، ۱۳۸۴،**حقوق وامنیت درفضای سایبر**، تهران ، مؤسسه فرهنگی مطالعات وتحقیقات بین المللی ابرا
۱۴. خداقلی، زهرا ، **جرائم کامپیوتری**،تهران ، آریان، ۱۳۸۲
۱۵. دولتشاهی ، شاهپور، ۱۳۸۴ **مجموعه مقاله های همایش بررسی جنبه های حقوقی فناوری اطلاعات**، قم سلسبیل
۱۶. **دایره‌المعارف دموکراسی**، زمستان ۱۳۸۳،زیر نظر سیمور مارتین لیپست، ترجمه کامران فانی و دیگران، چاپ مرکز چاپ و انتشارات وزارت امور خارجه
۱۷. روزنامه رسمی جمهوری اسلامی ایران شماره ۱۸۷۴۲ شماره ویژه قانون ومقررات ۱۶۳

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۱۸. زندی ، محمد، **تحقیقات مقدماتی درجرایم سایبری** ، تهران ، انتشارات جنگل ، جاودانه
۱۹. ساریخانی، عادل، **جاسوسی وخیانت به کشور**،مرکز انتشارات دفتر تبلیغات اسلامی ،۱۳۷۸
۲۰. سعدی شیرازی، مصلح الدین،۱۳۷۸،**بوستان**، حکایت دوم از باب اول: در عدل و تدبیر و رای، انتشارات علمی، چاپ پنجم
۲۱. ضمانت اجرایی قانون **جرایم رایانه‌ای چیست**؟ آفتاب، ۸ آذر ۱۳۸۸از ویکی‌پدیا، دانشنامهٔ آزاد
۲۲. ضیابری ، سید ایمان ،**جرایم و مجرمان اینترنتی را بهتر بشناسیم**.
۲۳. عمید، حسن؛ **فرهنگ فارسی عمید**، موسسه انتشارات امیرکبیر، چاپ سی و یکم، ۱۳۸۴
۲۴. فرهنگ تشریحی **اصطلاحات کامپیوتری مایکروسافت**، هیأت مؤلفان و ویراستاران انتشارات مایکروسافت
۲۵. فصلنامه ره آورد نور – شماره ۱۱ تابستان ۱۳۸۴ صفحه ۱۴ تا ۱۷
۲۶. فضلی، مهدی؛ **تخریب و اختلال در داده ها و سیستم های رایانه ای**، مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات، مرکز مطالعات راهبردی و توسعه قضایی قوه قضائیه، تهران، ۱۷ و ۱۸ خرداد ۱۳۸۳
۲۷. فضلی، مهدی ، ۱۳۸۸ ، **مسؤولیت کیفری درفضای سایبر** ، معاونت حقوقی وتوسعه قضایی قوه قضائیه،تهران ،خرسندی
۲۸. قناد، فاطمه؛ **پیشگیری کیفری از جرایم ارتکابی در فضای مجازی**، مجموعه مقالات نخستین همایش ملی پیشگیری از جرم: پیشگیری از تکرار جرم و بزه دیدگی، دفتر تحقیقات کاربردی پلیس پیشگیری ناجا، ۱۳۸۸
۲۹. گاتن، آلن،۱۳۸۳، **ادله الکترونیکی**، ترجمه مصیب رمضانی، شورای عالی توسعه قضایی و دبیرخانه شورای عالی اطلاع رسانی، چاپ اول، خرداد
۳۰. گلدوزیان، ایرج، ۱۳۸۲،**محشای قانون مجازات اسلامی**،تهران، مجمع علمی‌وفرهنگی مجد
۳۱. گلدوزیان، ایرج، ۱۳۸۲،**حقوقی جزای اختصاصی**، تهران، انتشارات دانشگاه تهران
۳۲. مجموعه **مقاله های همایش بررسی جنبه های حقوقی ، فناوری اطلاعات**،خرداد۱۳۸۳ معاونت حقوقی وتوسعه قضایی قوه قضائیه ، مرکز مطالعات توسعه قضایی ، باهمکاری شورای عالی اطلاع رسانی کشور ، قم ، سلسبیل
۳۳. محمدقریب، **تبیین الغات لتبیان الآیات** یا فرهنگ لغات قرآن ، ج۱
۳۴. معین، محمد، ۱۳۷۶،**فرهنگ فارسی**، تهران، انتشارات امیرکبیر، دوره ۶جلدی
۳۵. معین، محمد، چاپ دوم،، ۱۳۸۶، **فرهنگ معین**، یک جلدی فارسی، انتشارات زرین
۳۶. مهدی پور،میثم ، **تاریخ اینترنت** ، ویکی پدیا فارسی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۳۷. میرمحمد صادقی، حسین،۱۳۸۱،**جرایم علیه امنیت وآسایش عمومی**، تهران، نشر میزان

۳۸. .نشریه پیام قانون ، **بررسی ابعاد جاسوسی رایانه‌ای باتوجه به قانون جرایم رایانه‌ای** ، الیاس بوجار دانشجوی مقطع کارشناسی ارشد جزا وجرم شناسی

۳۹. .نجفی ابرندآبادی ، علی حسین ، ۱۳۸۵،**تقریرات جرم شناسی** (امنیت خصوصی) دانشگاه علوم اسلامی رضوی ، سال تحصیلی ۸۲-۸۱

۴۰. هیأت مؤلفان و ویراستاران انتشارات مایکروسافت

۴۱. هیبلز گری، کریس ، سال ۱۳۸۱، **جنگ پست مدرن سیاست نوین درگیری**، ترجمه احمد رضا تقاء، انتشارات ،دوره عالی جنگ

۴۲. . هیک، استیون و اف هلپین، ادوارد و هوسکینز، اسکینز؛ ۱۳۸۶،**حقوق بشر و اینترنت**، ترجمه زمانی ، دکتر سید قاسم و بهراملو ، مهناز ،انتشارات خرسندی، چاپ اول

ب :پایان نامه ها

۴۳. .بتول ، پاکزاد ،۱۳۸۸ ،**تروریسم سایبری** ، پایان نامه دکتری حقوق کیفری وجرم شناسی ، دانشگاه شهید بهشتی ،تهران

۴۴. .زرخ ،احسان ، ۱۳۸۸، پایان نامه کارشناسی ارشد حقوق کیفری وجرم شناسی، مؤسسه غیرانتفاعی اشرفی اصفهانی

۴۵. .شمس ناتری ، محمدابراهیم ، ۱۳۸۰ **بررسی سیاست کیفری ایران درقبال جرایم سازمان یافته با رویکرد به حقوق جزای بین المللی** ، رساله دکتری ، تهران، دانشگاه تربیت مدرس .

۴۶. .عمیدی، مهدی،۱۳۸۷، **مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه وحقوق کیفری ایران** ، تهران، دانشگاه آزاد اسلامی‌واحد تهران مرکزی، پایان نامه کارشناسی ارشد حقوق جزا وجرم شناسی

۴۷. .فضلی، مهدی؛ ۱۳۸۳ ،**مسوولیت کیفری ارایه دهندگان خدمات اینترنتی**، پایان نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه پردیس قم

۴۸. . بوجار، الیاس، ۱۳۸۸،**جرم جاسوسی با توجه به فناوری نوین**، تهران، دانشگاه پیام نور مرکز تهران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ج :مقالات وکتب لاتین

۴۹.Brenner, Susan, Toward a Criminal Law for Cyberspace: Distributed Security,University of Dayton School of Law,http://law.bepress.com/expresso/eps /۱۵, p: ۵۵

۵۰.Carey, Peter, Media Law, Sweet&Maxwell, Second Edition, London, ۱۹۹۹, p ۱۷۶.

۵۱.CRS report for congress,Op.cit ,۲۰۰۸,P.۱۳

۵۲.David R. Johnson & David G. Post.Law and Borders - The Rise of Law inCyberspace,۴۸ STAN. L. REv. ۱۳۶۷, ۱۹۹۶.

۵۳.Declan McCullagh,Wiretapping the Net: Oh, Brother,Wired News, Oct. ۱۲, ۱۹۹۹.

۵۴.. F.E Hagan Political Ceim .

۵۵.. J.M.Martin and A.T.Romano,Multinational Crime(London:Saga Publications,۱۹۹۲)P.۳۹,citing .Andrew M .C.Her Majestys Secret Secret Service…(New York: Viking,۱۹۸۶)P.۱

۵۶..L. Janczewki, A. Colarik; Op.cit , P.۹۷

۵۷.. Schemmelt, TammyJ; Www.Stopcybercrime.Com: How The UsaPatriot Act Combats Cyber-Crime William Mitchell Law Review Vol۲۹/۳,۲۰۰۳,P.۹۳۷

۵۸..T.R. Sarbin et al Citizen Espionage P.۳q

۵۹..William S. Cleveland &Donald X. Sun, Bell Lab; Internet Traffic Data, (paper presented at the University of Michigan) ۲۰۰۰.

۶۰.Majid Yar.(۲۰۰۵),The novelty of cybercrim : An assessment in Light of routine activity theory. European Journal of Criminology.

۶۱ .Grabosky,Peter(۲۰۰۰),Computer Crime:A Criminological Overview, p.۱۹, retrieved

۶۲. Nisbett,C(۲۰۰۲) .New directions in cyber crime .White Paper,QineticQ

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ج: وب سایت

۶۳. http//www.magiran.com/mpview.asp/ID= ۱۴۴۶۵۳

۶۴.http://www.mpirouzi.com/modules.php?name=News&file=article&sid=۳۰

۶۵.http://www.wired.comlnews/politics/۰.۱۲۸۳.۳۱۸۵۳.۰۰.html.

۶۶.http://www.imj.ir/index.php?option=com_content&view=article&id=۱۳۸۱:۱۳۸۹-۰۳-۰۱-۲۰-۱۳-۳۸&catid=۵۷:۱۳۸۸-۰۸-۱۹-۰۷-۴۵-۲۶.

۶۷.http://www.m-pirouzi.com/modules.php?name=News&file=article&sid=۳۰۱

۶۸. http://hamidkhanzadeh.blogfa.com/post-۳۰.aspx

۶۹. http://www.rasekhoon.net/Article/Show-۵۸۱۲۳.aspx

۷۰.http://www.cli.orglX۰۰۲۵_LBFIN.html.

۷۱.http://www.stat.lsa.urnich.edulgrnichaillstat۶oo Foo/traffic.pdf.

۷۲. http://fa.wikipedia.org/wiki

۷۳. http://www. cyberhosseinifar.blogfa.com

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

Payam Noor University
Department of law

Title :
Comparison espionage in real and virtual space

By :
Seedeh Fahimeh Taheriyan

Supervisor :
D. Mehdi naghavi

Advisor :
D. Nariman Fakhery

Submitted Partial Fulfillment of the reqirements for the Degree of M.A In private lav

August ۲۰۱۱

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.