

شناخت کلی جرایم کمپیوتری و اینترنتی (جرایم مدرن)

Computer and Internet Based Crimes

DOI: 10.64104/v3.Issue5-6.n3.2014

امین الله وزیری^۱

چکیده

این مقاله درباره «جرایم رایانه‌ای و اینترنتی» نوشته شده است. این مطالعه با روش توصیفی و تحلیلی خود تلاش کرده است تا جرایم مدرن از طریق رایانه و اینترنت را که در اکثر کشورهای جهان رخ داده و روز به روز در حال افزایش است، شناسایی کند.

هرچند رایانه و اینترنت ابزارهایی هستند که به طور چشمگیری دنیای ما را تغییر داده و امکانات و اطلاعات زیادی را در اختیار بشر قرار داده‌اند، اما با توسعه فناوری رایانه و اینترنت، جرایم نیز در سطح بین‌المللی ظهور کرده و به عنوان جرایم رایانه‌ای یا اینترنتی شناخته شده‌اند. جرایم رایانه‌ای، اعمال غیرقانونی‌ای هستند که توسط شخصی با استفاده از رایانه انجام می‌شوند. جرایم اینترنتی، اعمال غیرقانونی‌ای هستند که توسط شخصی با استفاده از اینترنت انجام می‌شوند.

امروزه در اکثر کشورهای جهان، این جرایم بسیار بحرانی تلقی می‌شوند و کشورها تلاش می‌کنند قوانین و مقرراتی را وضع کنند و راه‌هایی برای پیشگیری از این جرایم بیابند. متأسفانه، در افغانستان عزیز ما، هنوز توجه کافی برای مقابله با این مسئله حیاتی صورت نگرفته است.

واژگان کلیدی: جرایم کمپیوتری، اینترنت، سرقت، کلاهبرداری، سایبر

^۱. عضو کادر علمی پوهنځی حقوق و علوم سیاسي پوهنتون سلام، Waiswaziry@gmail.com

مقدمه

امروزه تحولات عظیمی در تکنولوژی بوقوع پیوسته و شاهد انقلابات بزرگ در زمینه فن آوری ارتباطات فراملی طی چند دهه اخیر بوده ایم. پیدایش کامپیوتر و پس از آن دنیای مجازی اینترنت، همراه خود دستاوردهای مثبت و منفی بسیاری داشته و دارد.

کامپیوتر و اینترنت علیرغم تمامی امکانات و اطلاع رسانی در عرصه بین المللی که برای ما به ارمغان آورده است ولی متأسفانه بعضی افراد سودجو و فرصت طلب با فراگرفتن دانش و مهارت لازم، راه های ورود به سیستم های کامپیوتر های دولتی، خصوصی و ... را به دست آورده اند که موجب بروز مشکلات و خسارات فراوانی گردیده است.

با توسعه و تحول یافتن اینترنت، در مقابل انقلاب عظیمی در ایجاد جرایم در سطح بین المللی بوجود آمده و جرایم جدیدی تحت عنوان جرایم اینترنتی ظهور کرد که در بیشتر کشورهای دنیا این جرایم به عنوان یک معضل حاد و بسیار مهم تلقی می گردد و دولتها در صدد پیدا نمودن راه حل های مختلفی در جهت جلوگیری از وقوع آن می باشند. بناً برای شناخت از این جرایم نو ظهور و مدرن، در این مقاله ابتدا تعریفی از این جرایم ارائه داشته، سپس به تاریخچه آن پرداخته و به تعقیب آن تفاوت این دسته جرایم را با سایر جرایم مشخص نموده و در پایان انواع آنرا مورد مطالعه قرار خواهیم داد.

مبحث اول- تعاریفات

همانطوریکه همه می دانیم جرم یک پدیده اجتماعی بوده و از بدو پیدایش انسان تا کنون بحیث یک عمل زشت و نادرست و زجر دهنده در جامعه بشری شناخته می شود، هر عقل سلیم و وجدان پاک و بی آلایش آنرا پدیده بد و ناپسند می بیند و بدون شک، دارای تاثیر قبیح و منفی بالای جامعه بشری بوده است و از همان زمان آغاز زندگی بشری همه در صدد آن بوده اند تا جلو ارتکاب آنرا بگیرند که پیامبران الهی دستورات پروردگار را برای بشریت به ارمغان آورده اند از هر کسی دیگری در این زمینه پیش قدم بودند و دساتیر معینی را در این زمینه برای انسانها تبلیغ نمودند و انسانها هم هر کدام به نوبه خود سعی ورزیده اند تا راه و چاره ای برای کاهش اعمال جرمی و ارزش ستیز، دریابند. از اینکه سخن به درازا نکشد در این جامعه نیز ما بر آنیم تا بتوانیم با این پدیده مبارزه کنیم²، که برای نایل شدن به این هدف ابتدا باید تعریفی از جرم داشته باشیم.

الف- تعریف جرم

جرم و جرمیه از ماده جرم- به فتح جیم- اخذ شده، که به معنای قطع کردن و بریدن آمده است و به معنای هر کسب و کار زشت و مکروه و همچنان به معنای باعث شدن و وادار کردن بر کار زشت و ناپسند نیز اطلاق گردیده است.³ همچنان جرم در لغت به معنای گناه، خطا، بزه⁴ آمده است. که خداوند جل جلاله در آیه 29 سوره المطففین می فرماید: إِنَّ الَّذِينَ أَجْرَمُوا كَانُوا مِنَ الَّذِينَ آمَنُوا يَضْحَكُونَ (29). کسانی که گناه می کردند آنان را که ایمان آورده بودند به نیشخند می گرفتند.

² سیغانی، محمد اختر، 1393، حقوق جزای عمومی، ص 55.

³ نذیر داد محمد، 1389، حقوق جزای عمومی اسلام، ص 44.

⁴ عمید حسن، 1389، فرهنگ عمید، ص 336.

و اما در اصطلاح از جرم تعاریف متعددی صورت گرفته است که به بعضی آنها می پردازیم:

جرم عبارت از اجرای یک عملی است که شریعت اسلامی و قانون جزا آنرا نا مشروع خوانده و منع نموده باشد و یا عبارت از امتناع از عملی است که شریعت اسلامی و قانون جزا آن عمل را مشروع خوانده و به اجرای آن امر کرده باشد و برای متخلفین آن مجازات یا تدابیر امنیتی پیش بینی کرده باشد.

و یا هم جرم عبارت از ارتکاب اعمال غیرقانونی و امتناع از اعمال قانونی است که در مقابل آن مؤیدات جزایی از طرف قانونگذار وضع شده باشد.

و یا به عبارت دیگر، جرم یک حرکت ضد اجتماعی است که در برابر آن مجازات یا اقدامات تأمینی و تربیتی در نظر گرفته شده است.⁵

ب- تعریف جرم کمپیوتری

چون در اکثر کشورها اینگونه جرایم در قوانین پیش بینی نشده است، نمیتوان (یا بسختی میتوان) اینگونه اعمال را (با توجه به اهمیت آن) مورد تعقیب قرار داد و مجازات کرد. این موضوع فقط مخصوص کشورهای خانواده حقوق نوشته⁶ نیست بلکه کشورهای خانواده کامن لا⁷ نیز بعلمت نبود رویه های قضایی مربوط به این نوع جرایم که قبلاً مطرح شده باشد در اینگونه رسیدگی ها دچار اشکال می شوند.

بعلاوه مسئله دیگری که باید مورد توجه قرار گیرد این است که چون تعریف مشخصی از جرم کمپیوتری نشده است، معلوم نیست که این جرایم در چه دسته هایی قرار می گیرند، یعنی معلوم نیست که جزو جرایم علیه اموال اند یا جرایم علیه اشخاص و یا جرایم علیه امنیت ملی.... این مسئله نه تنها در مرحله اول (کشف و تعقیب) بلکه در مراحل بعدی (رسیدگی و صدور حکم) نیز ایجاد مشکل می کند.

و اما نهایتاً می توان جرایم کمپیوتری را چنین تعریف نمود:

هرگونه عمل خلاف قانون که با سوء نیت، از طرف شخص یا اشخاص با بکارگیری از کمپیوتر صورت پذیرد جرایم کمپیوتری نامیده می شود.

و یا هم هر عمل مثبت غیرقانونی که کمپیوتر در آن ابزار یا موضوع جرم باشد جرم کمپیوتری است.⁸

ج- تعریف جرم اینترنتی

همانگونه که قبلاً اشاره گردید دانشمندان بدین باور اند که هرگونه عمل خلاف قانون که با سوء نیت، از طرف شخص یا اشخاص با بکارگیری از کمپیوتر صورت پذیرد جرایم کمپیوتری نامیده می شود، و میتوان این تعریف را برای جرایم اینترنتی نیز در نظر گرفت؛ یعنی بصورت مشخص از جرایم اینترنتی کدام تعریفی را ارائه نکرده اند و اما هرگاه تعریفی از جرایم اینترنتی ارائه نماییم، میتوان گفت که:

جرایم اینترنتی به جرایمی اطلاق می شود که در فضای مجازی یا غیر ملموس (سایبری) رخ می دهد.⁹

⁵ سیغانی، همان اثر، صص 55-56.

⁶ حقوق نوشته یا رومی- ژرمنی به نظام حقوقی اطلاق می شود که تدوین مجموعه قوانین، مهمترین ویژگی آن بوده و قانون منبع اصلی آن به شمار می رود.

⁷ خانواده کامن لا شامل کشورهای انگلستان، ایالات متحده آمریکا، کانادا، استرالیا و ... شده، که پایه و اساس حقوق این کشورها را اخلاق ناشی از مذهب مسیح و سیاست مربوط به حمایت از افراد و آزادی او تشکیل می دهد و منبع اصلی قواعد در این کشورها را رویه قضایی تشکیل می دهد.

⁸ <http://www.beytoote.com/computer/sundries-web/computer1-crimes.html>، بی توت، بی تا

مبحث دوم- تاریخچه جرایم کامپیوتری و اینترنتی

با پیدایش کامپیوتر، جرایم کامپیوتری نیز بوجود آمد. تاریخچه جرایم کامپیوتری را می توان به سه نسل طبقه بندی نمود. نسل اول که تا اواخر دهه ۱۹۸۰ می باشد، شامل سرقت و کپی برداری از برنامه ها و جرایم علیه حریم خصوصی اشخاص مانند سرقت از آثار و تحقیقات افراد بود. نسل دوم که تحت عنوان جرایم داده ها نامیده می شود تا اواخر دهه ۱۹۹۰ ادامه داشته است. در این دهه تمامی جرایم علیه تکنولوژی اطلاعاتی، ارتباطاتی، کامپیوتری، ماهواره ای و شبکه های بین المللی تحت عنوان جرایم علیه داده ها اطلاق می شود. نسل سوم که از اواسط دهه ۱۹۹۰ شروع می شود جرایم کامپیوتری تحت عنوان جرایم سایبر یا جرایم در محیط سایبر معروف گردید.

پیشینه تاریخی جرایم کامپیوتری به سال ۱۹۸۵ بر می گردد که جرایم کامپیوتری در بر گیرنده جرایمی مانند جاسوسی کامپیوتری، سرقت های آثار ادبی و سوء استفاده غیر قانونی از سیستم های کامپیوتری بود. در دهه ۱۹۷۰ مقالات زیادی پیرامون جرایم کامپیوتری در روزنامه ها و در بعضی از کتابها نوشته شد ولی با توجه به اینکه نوشته های آنها مبتنی بر تحقیقات تجربی نبوده است لذا ارزش علمی نداشته تا بتوان به آنها استناد نمود ولی در اواسط دهه ۱۹۷۰ مطالعات تجربی پیرامون جرایم کامپیوتری صورت پذیرفت که در این مطالعات تمامی جرایم کامپیوتری بوقوع پیوسته را شامل نمی گردید.^{۱۰}

اولین تحقیقاتی که پیرامون جرایم کامپیوتری صورت گرفت در امریکا بود که در این تحقیقات به قضیه کلاهبرداری از طریق سوء استفاده از ۵۶ هزار مورد بیمه به ارزش حدوداً ۳۰ میلیون دالر اشاره نمود. مورد دیگر را می توان به قضیه «هراشتات» در آلمان که مربوط به معاملات ارزی خارجی به مبلغ ۲۰۰ تا ۳۰۰ هزار مارک از حساب ارزی بانک هراشتات خارج گردیده و همین امر باعث ورشکستگی این بانک و وارد شدن خسارت به مشتریان گردید.

در دهه ۱۹۸۰ که بعنوان نسل دوم جرایم کامپیوتری محسوب می گردد، جرایم کامپیوتری فقط محدود به جرایم اقتصادی نبوده و سایر زمینه ها را هم که جنبه اقتصادی نداشته مانند دستکاری کامپیوتر شفاخانه ها، جعل اسناد با استفاده از کامپیوتر و ورود به اطلاعات خارجی محرمانه آمریکا، انگلستان و چند کشور دیگر دست یافته و این اطلاعات را به K.G.B بفروشنند.

در دهه ۱۹۹۰ که شبکه جهانی (انترنت) فراگیر شد جرایم کامپیوتری از جنبه اقتصادی وسیعتر گردیده و ابعاد جدیدتری به خود گرفته است. جرایم جدید مانند ورود کرم اینترنتی که برای اولین بار توسط یک دانشجوی امریکایی ساخته شده بود و باعث شد تا سیستم کامپیوتری حدود ۶۲۰۰ کاربر اینترنت شامل دانشگاهها، سرویسهای نظامی و سایت های شفاخانه ها را مختل نماید. و هزینه تعمیرات سیستمها حدوداً به مبلغ ۹۸ میلیون دالر بود که بعد از مدتی این دانشجو دستگیر و پس از محاکمه محکوم به پرداخت کلیه مبالغ فوق گردید.

در زمینه جرایم کامپیوتری می توان به اقدامات زیر اشاره نمود:

^۹ www.hamshahronline.ir/details/10675، مهدی فتاحی، ۲۱ آذر ۱۳۸۵

^{۱۰} <http://www.tebyan.net/newindex.aspx?pid=90065> 3/2/1388، ندا پاک نهاد،

تصویب موافقتنامه جرایم کمپیوتری در سال 1985-1986 توسط شورای اروپا گام‌هایی زیادی برای تدوین قوانین مرتبط با جرایم کمپیوتری برداشته شد. در سال 1989 کمیته تخصصی شورای اروپا برای تدوین و یکنواخت نمودن سیاست جنائی مربوط به جرایم کمپیوتری پیشنهادهایی نمود که مورد تصویب شورا نیز قرار گرفت.

در همایشی که انجمن بین المللی حقوق جزا در سال 1994 داشت یکسری از مسائل را به عنوان جرایم مستقل کمپیوتری تدوین نمود. نهایتاً در سال 2001 میلادی شورای اروپا، مبادرت به وضع موافقتنامه جرایم کمپیوتری نمود که این موافقتنامه شامل چهار فصل و چهل و هشت گفتار می‌باشد.¹¹

اولین قانون راجع به جرایم اینترنتی در سال 1984 در آمریکا به تصویب رسید و در سال‌های 1994 و 1996 این قانون اصلاح گردید. در حال حاضر 44 کشور دنیا همچون: ایالات متحده آمریکا، انگلستان، کشورهای عضو اتحادیه اروپا، استرالیا و هندوستان، پولیس‌هایی دارند که به پولیس اینترنتی مشهور است و به طور رسمی از طریق کانال‌های دولتی، جرایم مجازی را پیگیری می‌کنند.

مبحث سوم- تفاوت جرایم کمپیوتری و اینترنتی با سایر جرایم

علاوه بر پیشرفت سریع کمپیوتر، علل دیگری که باعث شده قوانین راجع به این پدیده در حال حاضر موجود نباشد، خصوصیات اینگونه جرایم است، که آنها را از دیگر جرایم متمایز می‌سازد. عبارت دیگر جرایم کمپیوتری ویژگی‌های خاصی دارد که نه تنها وضع قوانین را مشکل می‌سازد، بلکه در مقام رسیدگی به اینگونه جرایم کار ماموران رسیدگی کننده (پولیس، سارنوال و قاضی...) را نیز پیچیده می‌سازد.

در اینجا بصورت مختصر ویژگی‌های اینگونه جرایم را که باعث دشواری عمل قانونگذاری و نیز سختی رسیدگی به قوانین ایجاد شده می‌شود را مورد بررسی قرار خواهیم داد. در ابتداء ویژگی‌های که وضع قانون را دشوار می‌کند:

امکانات بسیار وسیع کمپیوتر و اینترنت در انجام امور مختلف: این ویژگی باعث می‌شود که از یکطرف وضع یک قانون کلی، اساساً بی‌فایده باشد؛ زیرا به سادگی میتوان بدون اینکه آنرا نقض کرد از دیگر امکانات کمپیوتر سوء استفاده کرد و از طرف دیگر ایجاد قوانین خاص و موردی نیز عملاً غیر ممکن باشد، زیرا وضع چنین قانون حجیمی نه تنها عملی نیست، بلکه حتی اگر پس از صرف مدت فراوانی چنین کاری صورت پذیرد با پیشرفت سریع کمپیوتر، قانون مزبور خیلی زود متروک می‌افتد.

جرایم کمپیوتری و اینترنتی، جرایم بدون محدودیت: این جرایم محدودیت‌هایی بسیار کمی دارند (چه از نظر زمانی و چه از نظر مکانی). مثلاً برای سرقت یک بانک مدت مشخصی لازم است که سارق با حضور در محل دست به چنین عملی بزند، ولی این جرایم در مدتی کوتاه و بدون حضور در محل امکان پذیر است. مثلاً اطلاعات بسیار سری یک مرکز نظامی میتواند ظرف چند ثانیه بسرقت رود. محدودیت مکانی نیز در این جرایم وجود ندارد. کمپیوترهای که فقط با یک خط تلفن به سایر مراکز کمپیوتری متصل می‌شوند خیلی راحت میتوانند مورد هرگونه سوء استفاده قرار گیرند، نه تنها سرقت بلکه بسیاری از خرابکاری از همین طریق صورت می‌گیرد.

¹¹ <http://www.beytoote.com/computer/sundries-web/computer1-crimes.html>، بی‌توت، بی تا

عدم حضور فاعل در صحنه جرم: در اکثر جرایم حضور فاعل در صحنه جرم از ملزومات وقوع حادثه یا لااقل انتساب جرم به او است و این امر در جرایم کمپیوتری و اینترنتی هیچ لزومی ندارد، بلکه معمولاً مجرم این نوع جرایم در زمان تحقق جرم اصلاً در محل وقوع جرم نمی باشد.

زمان وقوع این جرایم: این مسئله هم از موارد مهمی است که همیشه مورد توجه می باشد، مخصوصاً در کشورهایی که مرور زمان وجود ندارد. حتی اگر چنین تأسیسی نیز در قانون وجود نداشته باشد، زمان وقوع جرم از حیث قانون حاکم بر آن مورد، مسئله ای است قابل توجه. صحبت از آن دسته جرایم نیست که در زمان مشخصی اتفاق می افتد بلکه نوع دیگری از جرایم مد نظر است که در زمان معینی اتفاق نمی افتد. مثلاً: یک برنامه نویس کمپیوتر که در یک بانک مشغول کار است میتواند برنامه نوشته شده برای کمپیوترهای بانک را به نحوی تنظیم کند که تا مدت مشخصی تمام مسایل بخوبی و بدون اشکال پیش بروند ولی پس از این مدت معین (که با محاسبات برنامه نویس تعیین شده است) ناگهان روش کار عوض شود و کمپیوتر از تمام حسابهای بانکی مبلغ ناچیزی برداشت کرده و به حساب برنامه ریز واریز نماید و او این مبلغ هنگفت را از حسابش خارج نموده و متواری شود، در باره زمان وقوع چنین جرمی چگونه میتوان نظر داد؟ آیا هنگامیکه این برنامه با قصد سوء نوشته می شده است زمان ارتکاب جرم است؟ یا زمانیکه جرم محقق می شود (در صورتیکه در این هنگام عمل مجرمانه ای از سوی شخص مذکور سر نمیزند)؟ آیا میتوان این قضیه را با نظریاتی مثل تحقق عنصر مادی حل کرد؟ مثلاً شخص برنامه ریز در زمان دادن برنامه (بر فرض محال کشف جرم در این زمان) به این اتهام که سوء نیت داشته محاکمه کرد؟ یعنی بگوییم سوء نیت وجود داشته، عمل مادی هم قبلاً انجام شده (نوشتن برنامه)، رابطه سببیت هم که وجود دارد پس مجرم را باید محاکمه کرد و محکوم نمود (آن هم قبل از آن که نتیجه محقق شده باشد)؟ عبارت دیگر قبل از تحقق جرم مجرم را دریافته باشیم؟ یا اینکه بگوییم چنین کاری محاکمه شخصی قبل از وقوع جرم) خلاف عدالت است و با این استدلال فقط وقتی جرم محقق شد آن فرد را تحت پیگرد قرار دهیم، یعنی وقتیکه او با پولها فرار نموده است؟ محاکمه چنین شخصی با عنوان شروع به جرم هم بدلیل عدم برابری بین اتهام و مجازات با احتمال نفعی که مجرم در صورت موفقیت میبرد ظاهراً موثر و نیز عادلانه نخواهد بود، یعنی اثر مجازات که تخفیف مجرم و جامعه و نیز تأدیب آنها است نمایان نخواهد شد.

تفاوت نوع مجرمین کمپیوتر و اینترنت با مجرمین سایر جرایم: مجرمین کمپیوتر و اینترنت اکثراً از طبقات روشنفکر و تحصیلکرده میباشند (بر عکس دیگر مجرمین) بعلاوه آنها عموماً قادر به انجام حتی یک جرم ساده به معنی فعلی آن نیستند، یعنی سارق نرم افزار شاید نتواند یک قوطی کنسرو از سوپر مارکت برآید. این مسئله مهم نه تنها در تعقیب اینگونه افراد مهم است بلکه در تعیین نوع مجازات آنها نیز اهمیت دارد (تعقیب آنها معمولاً دشوارتر است زیرا با هوشیاری و درایت عمل می کنند و آثاری که ممکن است منجر به دستگیری آنان شود، محو می کنند، بعلاوه مجازات آنان باید با رعایت موقعیت اجتماعی آنها صورت گیرد).

موارد فوق پاره های از تفاوتهای جرایم کمپیوتری و اینترنتی با دیگر جرایم بوده که کار وضع قوانین مربوطه به آنرا دشوارتر ساخته و بعلاوه لزوم دقت زیاد در این امر را بیان می نماید.

بعضی تفاوتهای دیگری نیز وجود دارد که کشف و تحت پیگرد قرار دادن این جرایم را دشوار می نماید:

قربانیان جرایم کامپیوتری و اینترنتی خود با این مسئله با بی میلی برخورد می کنند. اینگونه قربانیان که موسسات و ادارتی هستند که علاوه از بکارگیری وسیع کامپیوتر برای سهولت امور و ارائه خدمات به این استفاده و بکارگیری (کامپیوتر میبایند) و از پخش اخبار مربوط به سوء استفاده از کامپیوترها و اینترنت که منجر به از بین رفتن اعتبار موسسه و نیز بی اعتمادی افراد و اشخاص می شود خوشحال نخواهند شد؛ بلکه برعکس سعی بیشتری برای سکوت ماندن قضیه می نمایند و از هرگونه کمک برای کشف جرم خودداری می کنند.

در جرایم کامپیوتری و اینترنتی معمولاً موضوع جرم روشن نیست و این نه تنها در تحقیقات ایجاد اشکال می کند حتی در مرحله قبل از آن یعنی کشف خود جرم نیز زحمت آفرین است، یعنی نمیتوان بسادگی پی به وقوع جرم برد، از اینرو در اکثر مواقع گزارش جرم توسط مجنی علیه امری لازم است (بنابر این عنوان جرم مرئی یا جرم علنی هم اکثراً در اینگونه جرایم مصداق نخواهد داشت).

پیچیدگی عملکرد و کاربرد کامپیوتر و اینترنت که عموماً دارای تکنالوژی دایماً پیشرونده است کار رسیدگی و تعقیب را دشوار می سازد و درک نوع جرم و تحلیل عناصر آنرا برای ضابطین عدلیه دشوار می کند. البته میشود با تاسیس بخشی یا قسمتی از سیستمهای کشف و تعقیب جرم در این زمینه، تا حدی مشکل مزبور را حل کرد.

سرعت وقوع جرم به نحوی یک جرم (مثلاً تخریب اطلاعات یک کامپیوتر) ممکن است ظرف چند ثانیه صورت پذیرد، یعنی قبل از اینکه هرگونه عکس العملی از جانب مقامات مربوطه برای جلوگیری از تحقق این جرم یا حتی اطلاع از وقوع آن جرم برای ممانعت از فرار مجرم انجام گیرد، و به همین ترتیب کلیه آثار نیز محو می شود که کار تعقیب جرم و مجرم را در بسیاری موارد غیر ممکن می سازد.

البته خود موضوع مدارک جرم (و رسیدگی و جستجو برای یافتن آنها) مسئله های مهم است، زیرا در این جرایم معمولاً مدرک جرم با آن همانگونه که در دیگر جرایم وجود دارد پیدا نمی شود. علت را هم در خصوصیت اصلی و اولیه کامپیوتر حذف واسطه ای و بالنتیجه سرعت و سهولت کارها است که طبعاً در صورت بروز هرگونه سوء استفاده دسترسی به مدارک کلاسیک را غیر ممکن می نماید. مثلاً در مورد کلاهبرداری نمیتوان بدنبال نوشته هائی بود که حاکی از مقدمات انجام جرم باشد¹².

در پایان اشاره می شود علیرغم وجود تمام این موانع دولتها نه تنها بسیاری از جرایم کامپیوتری و اینترنتی را با قوانین فعلی تعقیب می کنند بلکه قوانین جدیدی را نیز کمابیش در این زمینه بوجود آورده اند که متأسفانه در کشور عزیز مان افغانستان شاهد این نوع قوانین نمی باشیم.

مبحث چهارم- دسته بندی جرایم کامپیوتری و اینترنتی

جرایم کامپیوتری و اینترنتی را از چندین لحاظ می توان دسته بندی نمود، از لحاظ مرتکب، از لحاظ تاریخی، نوع تأثیر و ... که ذیلاً هر یک را مورد بحث قرار می دهیم:

¹² <http://www.ghavanin.ir/paperdetail.asp?id=674> 1372/10/00، محسن طاهری جبلی،

مطلب اول- دسته بندی جرایم کمپیوتری و اینترنتی از لحاظ فاعل (مرتکب)

جرایمی که خود کمپیوتر مرتکب می شود:

این سوال وجود دارد که آیا خود کمپیوتر قادر به ارتکاب جرم است یا نه؟

همانطوریکه قبلاً هم اشاره کردیم کمپیوتر فقط کاری که از آن خواسته شده است انجام میدهد. اگر چنین است پس چرا این سوال پیش می آید؟

فرض ما در مورد کمپیوتر های محاسب است که بعزل مختلف ممکن است دچار اختلال شوند، مثالی ساده از این نوع اختلالات کمپیوترهای محاسب مراکز آب و برق و ... است. بسیار دیده شده است که کمپیوترها در برآورد وجوه آب و برق و تلفن و گاز و ... اشتباهاتی کرده اند که باعث زیادی پرداخت بعضی از مشترکین و گاه پرداخت کم دیگر آنها می شود. آیا میتوان در این مورد سوء نیت کمپیوتر را ثابت کرد و آنرا مسئول دانست؟ شاید این حرف خنده دار باشد ولی اگر همین کار را انسانها انجام میدادند، اثبات این امر بعید نبود. بعلاوه اگر چنین فرضی امکان نداشته باشد مسئول چه کسی خواهد بود؟ البته این فرض شاید در موارد مزبور بعزل آنکه یکطرف دولتها هستند زیاد مطرح نشود ولی اگر چنین موردی در حسابهای بانکی اشخاص پیش آید موضوع محسوستر خواهد بود.

همین فرض ساده موضوع مباحث بسیاری در کشورهای صاحب تکنولوژی کمپیوتر شده است. یعنی اگر کمپیوتر با اشتباهی این چنین در اموال افراد دخل و تصرف کند مسئول کیست؟ اثبات سوء نیت یا عدم آن تغییری در مسئله میدهد یا نه؟

جرایم ارتكابی توسط خود کمپیوتر شاید امروزه به اندازه دیگر مسایل به چشم نخورد ولی با پیشرفت سریع کمپیوترها بعید بنظر نمیرسد روزی فرا رسد که خود کمپیوترها مابشرتاً مرتکب جرایمی شوند.

جرایمی که با استفاده از کمپیوتر مرتکب می شوند:

کمپیوتر امروزه به عنوان یکی از آلات جرم مطرح شده است. رقم خسارات وارده از چنین جرایمی در انگلستان به صد میلیون دالر در سال میرسد و مقدار خسارات این جرایم در امریکا بالغ بر چهار میلیارد دالر در سال است.

شرایط خاص کمپیوتر آنرا وسیله مطلوب برای انجام بسیاری از جرایم درآورده است به نحویکه بزرگترین سرقتها و نیز کلاهبرداری ها توسط آن صورت می گیرد. البته این جرایم علاوه بر عناوین شناخته شده ای مثل: دزدی - گم شدن - اختفاء و اتلاف و بعضی مفاهیم دیگر که قدیمی هستند ولی در جرایم کمپیوتری نیز مصداق دارند، با توصیف های دیگری نیز مطرح میشوند که در حقوق فعلی عنوان مشخصی ندارند، مثل شنود یا مطالعه غیرقانونی اطلاعات یک کمپیوتر، و یا دادن اطلاعات غیر واقع به یک کمپیوتر راجع به یک شخص (آیا میتوان در این صورت مثلاً جرم افترا یا تهمت را محقق دانست؟).

جرایمی که توسط کمپیوتر ارتکاب میابند را میتوان به چندین دسته تقسیم نمود. در یک تقسیم بندی این جرایم یا گرفتن غیرمجاز اطلاعات از کمپیوتر است و یا دادن اطلاعات غلط به کمپیوتر؛ و در یک تقسیم بندی دیگر این جرایم یا علیه اشخاص، اموال و دارایی اشخاص است و یا هم علیه دولتها و وظایف دولتها. که هر دو دسته بندی را بطور جداگانه ذیلاً مورد بررسی قرار میدهم:

اول- خروج غیر مجاز اطلاعات و دادن اطلاعات غلط

اگر چه اصولاً کار اصلی کامپیوترها حفظ و ذخیره و طبقه بندی اطلاعات و بازپس دادن آنها در مواقع لزوم است، ولی اخذ این داده‌ها از کامپیوتر همیشه تحت شرایطی امکان پذیر است.

دریافت غیر مجاز اطلاعات از یک کامپیوتر اگر چه همیشه یک کار غیر اخلاقی است ولی فقط هنگامی جنبه جرم بخود می گیرد که اطلاعات سری باشند.

اما واقعاً این عمل چه نام دارد؟ اگر چه اصل قانونی بودن جرایم هیچ عملی را تا وقتی که صریحاً از طرف مقنن جرم معرفی نشده باشد، جرم نمی شناسد؛ که در زمینه بند اول ماده 27 قانون اساسی افغانستان نیز چنین صراحت دارد: «هیچ عملی جرم شمرده نمی شود مگر به حکم قانونی که قبل از ارتکاب آن نافذ گردیده باشد».¹³ ولی نمیتوان به این بهانه عمل مذکور را از هر گونه تعقیبی معاف دانست. بعلاوه در بحث ما که جنبه تئوریک دارد بررسی این امر لازم است. چیزی که اولاً به ذهن میرسد عنوان سرقت است. آیا میتوان ربودن این اطلاعات را سرقت دانست؟ ابتدا باید دید تعریف سرقت چیست؟

(سرقت کلمه عربی است و به معنی دزدی یا گرفتن و برداشتن چیزی در خفا و پنهانی، که نایستی برداشته شود، زیرا از آن او نیست، استعمال گردیده است)¹⁴ و در اصطلاح عبارت است از اخذ مال منقول متقوم غیر از محل محرز طور خفیه، بعباره دیگر ربودن مال متقوم، منقول غیر بطور خفیه به قصد تصاحب).¹⁵

توجه به تعریف فوق، دشواری استناد به آن و تعاریف مشابه را در سرقت اطلاعات بیان می کند که لزوم تدوین قوانین خاص را ایجاب می کند و این مسئله نه تنها در تحقق خود جرم بلکه در مسائل جانبی آن مثل محل وقوع جرم، شرکاء و معاونین و تعدد و تکرار نیز مطرح است.

البته باید توجه داشت که سرقت کامپیوتری فقط اطلاعات را در بر نمی گیرد بلکه نوع دیگر از این سرقتها، سرقت مستقیم توسط کامپیوتر است.

در پایان مطلب یادآوری این نکته ضروری است که در اخذ غیر مجاز اطلاعات همیشه نباید بدنبال این باشیم که عنوان جرم سرقت را به آن اطلاق دهیم بلکه گاهی این کسب اطلاعات فی نفسه جرم نیست ولی میتواند زمینه جرمی باشد. مثلاً در مناطقی که هم رزف هواپیما و نیز رزف هتل در محلی که شخصی قصد مسافرت به آنجا را دارد، بوسیله کامپیوتر انجام شود، اگر هر کس بتواند این اطلاعات را از کامپیوتر مزبور بدست آورد براحتی میتواند حدس زد که اطاق شخص نیز می تواند مورد سرقت قرار گیرد.¹⁶

قبلاً اشاره شد که کامپیوتر اطلاعات را جمع بندی، دسته بندی، نتیجه گیری و ... می کند و مبنای کار آن همان اطلاعات (داده های) اولیه است که به آن میدهم، پس اگر اطلاعات غلط به کامپیوتر بدهیم نباید انتظار داشته باشیم که در نگهداری و نیز محاسبات جواب صحیحی بگیریم.

¹³ جریده رسمی، 1382، قانون اساسی، م 27.

¹⁴ نذیر، داد محمد، 1389، حقوق جزای اختصاصی اسلام، ص 168.

¹⁵ ستانکزی و دیگران، 1387، قاموس اصطلاحات حقوقی، ص 145.

¹⁶ <http://www.ghavanin.ir/paperdetail.asp?id=674>، 1372/10/00. محسن طاهری جبلی

اگر دادن اطلاعات غلط بدون سوء نیت باشد خارج از بحث ما واقع میشود ولی اگر این عمل با سوء نیت صورت گیرد چه حالتی خواهد داشت؟

فرض کنیم در محل اشتغال هر شخصی سوابق او در کمپیوتری نگهداری شود. اگر بتوان در پرونده هر کس چیزهای خلاف واقع وارد نمود، هنگام ارائه آن به دیگر مراکز چه جرمی محقق خواهد شد؟

حالت جرم بودن این گونه اعمال در موارد خاصی بیشتر نمایان میشود. مثلاً استفاده از کمپیوتر در سارنوالی ها کم کم رواج پیدا میکند. در چنین وضعی اگر در حفظ سابقه اشخاص سوء نیتی بخرج داده شود (مثلاً جرایم اشخاص سابقه دار را در پرونده کمپیوتری آنها منعکس ننمایند) ظاهراً اشکالات خاصی پدیدار می گردد، مخصوصاً در رعایت مواردی مثل یافتن مجرم، تعدد و تکرار جرم، تخفیف مجازات، آزادی مشروط و ...

برعکس حالات فوق نیز متصور است: یعنی ثبت مواردی در پرونده شخص بدون آنکه واقعاً وجود داشته باشد، آیا میتوان اینرا جرم خاصی تلقی کرد یا باید آنرا در زمره جرایم موجود مثل افتراء و یا حتی قذف دانست؟ اگر اهانت باشد، اهانت در علن است یا در خفا؟ البته ممکن است اهداف دیگری از دادن اطلاعات اشتباه به کمپیوتر دنبال شود مثل بی اعتبار کردن یک اداره.

در صنایع امروز که بسیاری از محاسبات و طراحی ها و نقشه کشی ها برای تولید و ساخت پروژه های عظیم و یا کوچک با کمپیوتر صورت می گیرد با یک اشتباه عمدی میتوان خسارات مالی و حتی جانی زیادی پدید آورد. چه عنوانی از جرایم را میتوانیم به مسئول این خسارات انتساب دهیم؟ البته نتیجه دهی غلط کمپیوتر ممکن است علل مختلفی داشته باشد از جمله:

اشتباه در اطلاعات ورودی؛

اشتباه در برنامه های کاربردی؛

اشتباه عملیاتی از سوی متصدی کمپیوتر؛

اشتباه کشف نشده در نرم افزار سیستم؛

اشتباه بر اثر خرابی سخت افزار؛

که مسئول هر قسمت در صورت سوء نیت یا آگاهی ممکن است مجرم شناخته شود.¹⁷

دوم- جرایم کمپیوتری و اینترنتی علیه اشخاص، اموال و دولت ها

در این تقسیم بندی جرایم کمپیوتری و اینترنتی را به سه دسته می توان تقسیم نمود:

جرایم کمپیوتری و اینترنتی علیه اشخاص، جرایم کمپیوتری و اینترنتی علیه اموال و دارائی اشخاص یا جرایم کمپیوتری و اینترنتی اقتصادی و جرایم کمپیوتری و اینترنتی علیه دولتها یا وظایف دولتها، که هر یک را ذیلاً مورد بحث قرار می دهیم:

یک- جرایم کمپیوتری و اینترنتی علیه اشخاص:

جرایم کمپیوتری و اینترنتی علیه اشخاص عبارتند از:

¹⁷ <http://www.ghavanin.ir/paperdetail.asp?id=674>. 1372/10/00. محسن طاهری جبلی

الف- نوشته‌ها و عکسهای شهوت انگیز¹⁸: فروش یا به تصویر کشاندن عکسهای مبتذل جهت تحریک کردن نوجوانان و یا پیدا نمودن اشخاص از طریق چت (گپ زدن) جهت به نمایش گذاشتن عکسهای آنها در اینترنت و معرفی آنها به دیگر اشخاص جهت داشتن ارتباط نامشروع.

ب- اذیت و آزار کردن¹⁹: این نوع جرم ممکن است به صورت ارتباطات و دست انداختن و استهزا کردن، بی حرمتی به مقدسات و مطالبه کردن وجه از دیگران باشد.

ج- تهدید به قتل: یکی از جرایمی که ممکن است از طریق اینترنت و یا ارسال پیغام به ایمیل اشخاص صورت پذیرد تهدید به قتل می‌باشد.

دو- جرایم کمپیوتری و اینترنتی علیه اموال و مالکیت

جرایم علیه اموال و مالکیت یا جرایم اقتصادی که از طریق کمپیوتر یا شبکه جهانی (اینترنت) صورت می‌پذیرد عبارتند از:

الف- سرقت و تکثیر غیر مجاز برنامه‌های کمپیوتری حمایت شده: بدیهی است که تهیه برنامه‌های کمپیوتری توسط متخصصین این عرصه که در شرکت‌های تولید کمپیوتر یا شرکت‌های متخصص در عرصه تولید برنامه‌های کمپیوتری کار می‌کنند، صورت می‌گیرد. به هر حال در تهیه این گونه برنامه‌ها، خواه به وسیله شرکت‌های تولید کمپیوتر باشد یا به واسطه شرکت‌های متخصص در عرصه تولید برنامه‌های کمپیوتری، هزینه هنگفت و نیروی بشری بزرگ مورد استفاده قرار می‌گیرد، پس چون آماده کردن برنامه‌های کمپیوتری مدت طولانی می‌خواهد، تکالیف مالی هنگفت می‌طلبد و خیلی‌ها مشکل و دشوار می‌باشد، خیلی‌ها نادر خواهد بود که یک شخص از عهده تهیه برنامه‌های کمپیوتری کامل بر آید.²⁰ لذا تکثیر و استفاده غیر مجاز از آن برای صاحبان قانونی زیان‌های زیادی را به بار خواهد داشت. مثلاً زمانی که یک کارگردان و تهیه‌کننده فیلم سینمایی با زحمات زیادی که کشیده و هزینه‌های هنگفتی که برای ساخت فیلم صرف نموده بعد از به نمایش گذاشتن آن فیلم ممکن است همان فیلم از طریق اینترنت بفروش رسیده و زیانهای زیادی به سازنده فیلم وارد شود.

ب- سابوتاژ و اخاذی کمپیوتری: واژه سابوتاژ به معنای خرابکاری و کارشکنی می‌باشد²¹ و سابوتاژ کمپیوتری عبارت است از اصلاح، موقوف سازی و یا پاک کردن غیر مجاز داده‌ها و یا عملیات کمپیوتری به منظور مختل ساختن عملکرد عادی سیستم. سابوتاژ کمپیوتری ممکن است وسیله‌ای برای تحصیل مزایای اقتصادی بیشتر نسبت به رقیبان یا برای پیش‌برد فعالیتهای غیر قانونی تروریستی برای سرقت داده‌ها و برنامه‌ها به منظور اخاذی باشد.

ج- کلاهبرداری: کلاهبرداری عبارت است از استعمال اسم یا عنوان ساختگی به منظور متقاعد ساختن یک طرف بتأسیسات مجهول و اقتدارات و اعتبارات موهوم و امیدوار کردن بوقایع موهوم یا بیم دادن از امور موهوم تا باین ترتیب مال یا سند یا اوراق بهادار و قولنامه از طرف بگیرند و ضرر به او برسانند.²²

¹⁸ pornography

¹⁹ Harassment

²⁰ نذیر، داد محمد، 1393، در آمدی بر حقوق ملکیت معنوی، ص 219.

²¹ عمید، حسن، 1389، فرهنگ عمید، ص 519.

²² جعفری لنگرودی، محمد جعفر، 1385، ترمینولوژی حقوق، ص 574.

کلاهبرداری کامپیوتری از جمله جرایم اصلی سوء استفاده های کامپیوتری علیه اشخاص و یا دارائی افراد محسوب می گردد.

دارایی عینی غیر ملموس در قالب داده های کامپیوتری مانند وجوه سپرده و پس انداز، تغییر و دست کاری کردن در ساعات کاری، متداولترین راه های کلاهبرداری کامپیوتری می باشد. در تجارت الکترونیک نقل و انتقال پول نقد و خرید و فروش کالاهای تجاری، به سرعت جای خود را به انتقال سپرده ها از طریق سیستم های کامپیوتری داده است که نتیجتاً موجبات سوء استفاده کردن افراد سودجو و فرصت طلب را فراهم کرده است.²³

وارد کردن رمزها به خودپردازها و سوء استفاده کردن از کارتهای اعتباری دیگران معمول ترین شیوة ارتکاب در کلاهبرداری کامپیوتری می باشد.

در ذیل به نمونه هایی از کلاهبرداری های کامپیوتری اشاره می نماییم:

سوء استفاده از شبکه تلفنی: امروزه بعضی از افراد سودجو با استفاده از تکنیک هایی وارد خطوط تلفنی می شوند که آنها می توانند مکالمات تلفنی خود را با هزینه های مشترکین دیگر انجام دهند.

سوء استفاده از صندوقهای خود پرداز: در گذشته، سوء استفاده از صندوقهای خود پرداز با استفاده از کارت بانکی هایی که به سرقت می رفت صورت می گرفت ولی امروزه، با استفاده از سخت افزار و نرم افزار ویژه کامپیوتری، اطلاعات الکترونیکی غیر واقعی به صورت کد (رمز) روی کارتهای بانک ثبت شده مورد سوء استفاده قرار می گیرد.

سوء استفاده از کارتهای اعتباری: در حال حاضر، بیشتر معاملات از طریق اینترنت صورت می گیرد. مثلاً پرداخت بل صرفیه برق، آب، تلفن و همچنین خرید کالا، شرکت در همایش های بین المللی و غیره معمولاً با استفاده از کردیت کارت (کارت اعتباری) استفاده می شود و معمولاً مشتری می بایستی رمز کارت خود و دیگر جزئیات را قید نماید. بدین جهت بعضی از افراد سودجو با فاش شدن رمز کارت اعتباری مشتریان سوء استفاده می نمایند.

د- قاچاق مواد مخدر از طریق اینترنت: با توجه به دسترسی آسان افراد به همدیگر از طریق اینترنت و ارسال ایمیل، هرگونه خرید و فروش و پخش مواد مخدر از طریق شبکه های کامپیوتری انجام می شود. ضرب اطمینان قاچاق کنندگان مواد مخدر از طریق کامپیوتر نسبت به نوع سنتی آن بالاتر می باشد. زیرا پولیس به راحتی نمی تواند از برنامه های قاچاق کنندگان مطلع شود و لذا اقدامات پولیس در خصوص کشف فروشندگان و خریداران مواد مخدر غیر ممکن است.

ه- پولشویی کامپیوتری: اصطلاح پول شویی زمانی اطلاق می شود که مافیای پول، قاچاقبران، تروریستان، زورمندان، فرارکنندگان از مالیات و سایر متخلفان، پول های «سیاه» یا پول های غیر قانونی را از طریق معاملات مشروع به پول پاک یا به پول قانونی تبدیل می کنند.²⁴ دکتر میر محمد صادقی در تعریف پول شویی بیان می دارد: منظور از تطهیر مال، مخفی کردن منبع اصلی اموال ناشی از جرم و تبدیل آنها به اموال پاک می باشد به طوریکه یافتن منبع اصلی آنها غیر ممکن یا بسیار دشوار گردد.²⁵

²³ <http://hefazateetelaat.blogfa.com/87114.aspx> اطلاعات، 3 بهمن، 1387.

²⁴ www.bokhdinews.af/political/17195 سردار امیری، 26 جوزا، 1393.

²⁵ حبیبی، خلیل الله، 1392، پول شویی و آثار زیانبار آن، ص 19.

پولشویی و غارت یکی از جرایم کلاسیک بوده که دارای سابقه طولانی است که با پیشرفت تکنولوژی این جرم از طریق کامپیوتر و اینترنت صورت می‌پذیرد. نحوه ارتکاب بدین صورت است که باند‌های بزرگ نامشروع با ارسال ایمیل پیشنهاد انجام یک کار تجاری را به شخصی می‌نمایند و بدون اینکه اثر و نشانی از خود بجای بگذارند پیشنهاد ارسال مبالغی پول به حساب شخصی را که برای او ایمیل فرستاده‌اند می‌نمایند و در تقاضای خود نحوه ارسال و سهم هر یک از طرفین را بیان نموده و در صورت توافق طرف مقابل (گیرنده ایمیل) نوع و نحوه تضمینات لازم را اعلام می‌کنند و اصولاً در زمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشأ تجاری انتخاب و با هدف خود هماهنگ می‌نمایند.

سه- جرایم کامپیوتری و اینترنتی علیه دولتها

بعضی از جرایم کامپیوتری علیه دولتها ممکن است به انگیزه‌های سیاسی صورت پذیرد که می‌توان به موارد زیر اشاره نمود:

الف- تهدید به گروگان‌گیری، اخاذی و کشتن مسئولین و یا اعضای خانواده آنها: یکی از جرایم مدرن کامپیوتری که معمولاً قاچاقبران و یا افراد سیاسی برای رسیدن به اهداف خود از آنها استفاده می‌نمایند، تهدید مقامات کشور و یا خانواده آنها به گروگان گرفتن و یا کشتن است. این جرم به دلیل آنکه علیه مقامات بلند رتبه یک دولت صورت می‌گیرد، در زمره جرایم کامپیوتری علیه دولتها قرار می‌گیرد. معمولاً جرایمی که توسط افراد سیاسی صورت می‌گیرد با قاچاقبران متفاوت است. قاچاقبران معمولاً از طریق تهدید به گروگان‌گیری و همچنین تهدید به کشتن و اخاذی از مسئولین اقدام می‌نمایند ولی افراد سیاسی از طریق اعلام در اینترنت دولت را تهدید به جنگ مسلحانه و براندازی حکومت می‌نمایند بدون آنکه آثاری از خود بجای بگذارند.

ب- جاسوسی کامپیوتری: جاسوسی کامپیوتری به عملی گفته می‌شود که شخصی یا گروهی برای یک دولتی اطلاعات مخفیانه از دولت دیگر را برای دریافت پول انجام می‌دهد. بعنوان مثال می‌توان به موارد زیر اشاره نمود: در آلمان سازمان اطلاعاتی K.G.B روسیه به شخصی پول داده بود تا اطلاعات مخفیانه ارتش آمریکا را بدست آورد. یا در مورد دیگر می‌توان به قضیه لوس آلماس دانشمند هسته‌ای اشاره نمود که اطلاعات بسیار محرمانه هسته‌ای خود را در اختیار دولت چین قرار داده بود.

ج- تروریسم: تروریسم عبارت است از کاربرد سیستماتیک ترور (وحشت و ترس زیاد) است، به ویژه به عنوان وسیله اجبار یا روا شمردن اقدامات دارای ماهیت وحشت آفرینی در اذهان عامه و گروه‌های انسانی برای ساقط کردن حکومت، حفظ حکومت یا تغییر حکومت²⁶. امروزه برخی اقدامات تروریستی با دسترسی به اطلاعات حفاظت شده صورت می‌پذیرد. تروریست‌های اطلاعاتی فقط با استفاده از یک کامپیوتر می‌توانند بصورت غیر مجاز وارد سیستم‌های کامپیوتری امنیتی شوند، مثلاً با تداخل در سیستم ناوبری هوایی باعث سقوط هواپیما شده یا باعث قطع برق سراسری شوند.

جرایم علیه کامپیوتر

کامپیوتر یک شخص حقیقی (و حتی حقوقی) نیست که جرمی علیه آن متصور باشد و این عنوان را برای سهولت کار و تقسیم بندی موضوعات به آن داده ایم وگرنه جرایم مورد نظر در این قسمت عموماً به دارندگان آن نرم افزار ضرر می‌زند.

²⁶ مینود افشاری و علی آقا بخشی، 1386، فرهنگ علوم سیاسی، چاپ دوم، تهران، نشر چاپار، ص 677.

اساس کار برد هر کامپیوتر، نرم افزارهایی است که در آن بکار برده میشود، به همین علت است که نرم افزارها از ارزش خاصی برخوردار هستند و همچنان به همین علت است که جرایم مربوط به آنها رو به افزایش بود و بعلاوه خصوصیات خاصی را نیز دارا میباشند.

برای جلوگیری از اطاله کلام از جرایمی مثل سرقت نرم افزارها که با عناوین فعلی جرایم هم قابل پیگیری است خودداری میکنیم. اما موارد دیگری هم وجود دارد که اگر چه از نظر نتیجه همانند سرقت میباشند ولی شرایط خاص خود را دارا میباشند، از جمله کاپی برداری از نرم افزارها، مسئله ای بسیار مهم که در صدر تمام جرایم کامپیوتری قرار گرفته است. شاید به همین دلیل باشد که سالانه میلیونها دالر صرف هزینه های نگهداری و حفاظت از نرم افزارها میشود. بنظر بعضی از دست اندرکاران کامپیوتر کاپی برداری از نرم افزار برای کسانی که آنها را خریده اند نوعی سرقت «اموال فکری» میباشد.

همانگونه که روند پیشرفت کامپیوتر سریع است، جرایم وابسته به آن نیز با همان سرعت بوجود می آیند. یکی از این آخرین جرایم که جنبه تخریبی دارد ویروس کامپیوتر است. ویروس کامپیوتر یک اصطلاح عامیانه برای اطلاعاتی است که بطرق مختلف بصورت غیر مجاز وارد یک سیستم پردازش داده ها می شود. اینگونه قاچاق اطلاعات میتواند به تخریب اطلاعات یا حتی نابودی کامل اطلاعات ذخیره شده در سیستم منجر گردد. این ویروسها میتوانند به آسانی توسط یک فرد که بوسیله یک سیستم ارتباط از راه دور با کامپیوتر تماس می گیرد وارد آن شود. ویروس کامپیوتر بیماری خطرناکی است و فردیکه به چگونگی بوجود آوردن و تزریق یک ویروس به کامپیوتر آشنا باشد، سلاح خطرناکی در دست دارد. بدینترتیب که او میتواند ویروسی ایجاد کند که به اطلاعات خاصی حمله کرده و آنها را از بین ببرد یا اینکه تمام فایلهای داده ها را مورد حمله قرار داده و خیلی سریع اطلاعات را از بین ببرد بنحویکه امکان بازسازی آن نباشد، همچنین امکان ایجاد ویروسی هست که میتواند با تغییر برنامه های حفاظتی داده ها، دسترسی فرد خرابکار را به اطلاعات محرمانه ممکن سازد.

مطلب دوم- طبقه بندی جرایم کامپیوتری و اینترنتی از لحاظ تاریخی

به طور کلی از این لحاظ، جرایم کامپیوتری و اینترنتی را می توان به دو دسته تقسیم کرد، قدیمی و مدرن:

جرایم کامپیوتری و اینترنتی قدیمی

جرایم کامپیوتری و اینترنتی سنتی جرایمی هستند که با همان شرایط قانونی که از طرق مرسوم ارتکاب می یابند، به وسیله کامپیوتر نیز ارتکاب می یابند و قانون گذار ارتکاب به وسیله کامپیوتر را به عنوان جزئی از اجزای عنصر مادی آنها یا عامل تشدید و یا تخفیف مجازات آنها ذکر نکرده باشد.

جرایم کامپیوتری و اینترنتی قدیمی را می توان به پنج دسته به شرح ذیل تقسیم کرد:

جرایم کامپیوتری و اینترنتی علیه اشخاص؛

جرایم کامپیوتری و اینترنتی علیه اموال؛

جرایم کامپیوتری و اینترنتی علیه آسایش و امنیت عمومی؛

جرایم کامپیوتری و اینترنتی علیه عصمت و عفت و اخلاق حسنه؛

جرایم کامپیوتری و اینترنتی علیه خانواده.

2- جرایم کامپیوتری و اینترنتی مدرن

جرایم کامپیوتری و اینترنتی مدرن جرایمی هستند که غالباً پس از پیدایش کامپیوتر بوجود آمده‌اند و با پیشرفت کامپیوتر تحول پیدا کرده‌اند و به موجب وضع قوانین در زمینه عنصر مادی آن‌ها نیز به شکل جداگانه مشخص گردیده است.

جرایم کامپیوتری و اینترنتی مدرن را می‌توان به شش دسته به شرح ذیل تقسیم کرد:

جرایم کامپیوتری و اینترنتی علیه محرمانگی، تمامیت و در دسترس بودن داده‌ها، مانند: دستیابی غیر مجاز، شنود غیرمجاز و اختلال در داده؛

جرایم کامپیوتری و اینترنتی علیه سیستم کامپیوتری مانند اختلال در سیستم؛

جرایم کامپیوتری و اینترنتی علیه اموال مانند کلاهبرداری اینترنتی؛

جرایم کامپیوتری و اینترنتی علیه امنیت و آسایش عمومی مانند جعل اینترنتی؛

جرایم کامپیوتری و اینترنتی علیه مالکیت معنوی؛

جرایم کامپیوتری و اینترنتی علیه محتوی مانند انتشار پورنوگرافی کودک.

به طور کلی، آنچه مبنا و محور این نوع از تقسیم‌بندی‌ها قرار گرفته است، ارزش‌هایی هستند که مورد حمایت قانون‌گذار بوده و مورد تجاوز و تعدی مجرمان قرار گرفته‌اند.

مطلب سوم- جرایم کامپیوتری و اینترنتی از نظر نوع تأثیر

جرایم کامپیوتری و اینترنتی را از لحاظ نوع تأثیر به سه طبقه کلی تقسیم می‌کنند، فرهنگی، امنیتی و مالی.

جرایم فرهنگی

که شامل جرایم بر ضد مالکیت فکری و جرایم بر ضد ارزش‌های فرهنگی چون، جرایم توهین و اهانت به دین مبین اسلام و مقدسات آن، جرایم محتوا (Content Crime)، افشای اسرار خصوصی افراد و ... می‌شود.

2- جرایم امنیتی

که این جرایم شامل موارد ذیل می‌شود:

جرایم علیه امنیت داده‌ها، از جمله: جرایم علیه کاربرد مجاز داده‌ها مثل جاسوسی دسترسی غیر مجاز؛ و جرایم علیه صحت داده‌ها، همچون جعل؛

جرایم علیه امنیت سیستم؛

3- جرایم مالی

که شامل کلاهبرداری و سرقت و ... می‌شود.²⁷

در پایان باید لازم به ذکر است که بعضی از نویسندگان و دانشمندان، جرایم اینترنتی را به انواع ذیل نیز دسته‌بندی می‌نمایند:

²⁷ <http://www.rahavardnoor.com/index.php/authors/item/368-jaraieme-rayane> محمد حسین طارمی، چهارشنبه، 9 مهر 1393.

هک کردن

هک کردن عبارت است از نفوذ به یک سیستم کامپیوتری بدون داشتن مجوز، مالکیت یا صلاحیت لازم. هک کردن یعنی غلبه کردن بر سیستم های امنیتی یک سیستم کامپیوتری برای دسترسی غیر قانونی به اطلاعات ذخیره شده در آن سیستم. فاش کردن رمز عبور به قصد دسترسی به اطلاعات خصوصی افراد یک سازمان یکی از رایج ترین تخلفات اینترنتی است. یکی از خطرناکترین خلاف کاری های اینترنتی عبارتست از هک کردن آدرس IP تا بدین وسیله خلافاً خود را به جای کس دیگر جا بزند و افکار شوم یا جنایات مورد نظر خود را اجرا کند.

Phishing

فیشینگ عبارتست از تلاش برای بدست آوردن اطلاعاتی مانند رمز عبور، شناسه عبور و جزئیات کارت اعتباری با جا زدن خود به عنوان یک منبع قابل اعتماد. فیشینگ از طریق سرویس های ایمیل یا با وعده های دروغ انجام می گیرد یا با ایجاد برخی جذابیت ها کاربران اینترنتی را ترغیب می کنند اطلاعات خود را در سایت هایی که توسط کلاه برداران ساخته شده است وارد کنند. این خلاف کاران معمولاً وب سایت هایی طراحی می کنند که در کاربر احساس اعتماد و وارد شدن در یک سایت امن را می دهد و معمولاً هم موفق می شوند یعنی کاربر در دام آنها افتاده و اطلاعات خود را وارد می کند.²⁸

گروه ویروس های کامپیوتری

دسته ای از ویروس های کامپیوتری (شامل ویروس ها، کرم ها، نرم افزار های جاسوسی و...) در حقیقت نرم افزارهایی هستند که خود را تکثیر و منتشر می کنند و کامپیوترهای موجود در یک شبکه را بدون اطلاع کاربران آلوده کرده و به آنها صدمه می زند. ویروس ها از طریق فایل های سیستم یک شبکه کامپیوتری، اینترنت یا هر وسیله نقل انتقال اطلاعات مانند حافظه فلش، CD و... وارد کامپیوترهای دیگر می شوند.

ویروس های کامپیوتری کدهایی هستند که با هدف ضربه زدن به یک سیستم کامپیوتری یا از بین بردن اطلاعات نوشته شده اند. نوشتن ویروس کامپیوتری در همه جای دنیا یک جرم است به گونه ای که نویسنده ویروس در برابر تمام خسارت های وارده به همه کامپیوترهای آلوده شده مسئول است.

Cyber stalking

عبارت است از استفاده از فناوری ارتباطات به خصوص اینترنت برای آزار و اذیت افراد. تهمت، ارسال نرم افزارهای مخرب و تخریب اطلاعات و تجهیزات کامپیوتری در این گروه قرار می گیرند. این خلافاً کاران اغلب کاربران را از طریق چت روم ها، تالارهای تبادل نظر و اجتماعات اینترنتی شکار می کنند سپس اطلاعات آنها را بدست می آورند (مثلاً شماره تلفن و آدرس، محل کار و...) و با استفاده از این اطلاعات قربانیان خود را مورد اذیت و آزار قرار می دهند. ایمیل های تهدید آمیز، مزاحمت تلفنی و مانند اینها انجام می دهند و این مورد یکی از جرم های رایانه ای خطرناک است که در سراسر دنیا مجازات سنگینی برایش قرار می گیرد.

²⁸ <http://www.tar-nama.com/fa/page/135> آفتاب، 1391/7/29، انواع 20%، جرایم 20%، رایانه 20% ای 1/

هویت جعلی

هویت جعلی یا خود را به جای کس دیگر جا زدن یکی از جدیدترین کلاه برداری هایی است که به کمک آن پول های زیادی ربوده شده و سودهای کلانی نصیب کلاه برداران می شود. در این شیوه کلاه بردار خود را به جای مالک چیزی جا می زند. یا از هویت شخص دیگری برای بدست آوردن کالا یا خدمات مورد نیاز خود استفاده می کند. مهاجرت غیر قانونی، تروریسم و ایمیل های سیاه در زمره این جرایم قرار می گیرد.²⁹

نتیجه گیری

1. از آنچه متذکر شدیم بر می آید که جهان امروز جهان علم و فناوری است و بدون شک پیشرفت را نمی توان از آن جدا کرد. این در حالی است که همگام با پیشرفت های علمی بویژه در زمینه کامپیوتر و اینترنت، عده ای برخلاف خدمتگزاران بشریت که به فکر استفاده های مثبت از فناوری ها هستند به فکر سوءاستفاده اند؛ یعنی بعضی اشخاص اعمال خلاف قانون را با سوء نیت، با بکارگیری از کامپیوتر و اینترنت مرتکب می شوند که بدان میتوان جرایم کامپیوتری و اینترنتی اطلاق نمود.
2. جرایم کامپیوتری و اینترنتی از جمله پیشرونده ترین جرایمی هستند که با سرعت زیاد در حال گسترش و بالای جان بشر امروز شده اند.
3. ویژگی های خاصی چون: تخصصی و علمی بودن، دارای حیثیت عمومی و خصوصی بودن، پیچیدگی خاص، دشوار بودن تعیین صلاحیت جزایی، جهانی بودن، دشوار بودن کشف مجرم که در این دست از جرایم بروز کرده، است آن را از دیگر جرایم متمایز می نماید.
4. در حال حاضر جرایم کامپیوتری و اینترنتی با اشکال های مختلفی صورت می پذیرد که عبارت اند از: کلاهبرداری اینترنتی، سوء استفاده از شبکه تلفنی، سوء استفاده از کارتهای اعتباری، وارد کردن ویروس به کامپیوترهای دیگر، پولشویی و ... که در اکثریت کشورها جهان قواعد و مقرراتی برای رسیدگی به آنها وجود دارد؛ ولی در کشور عزیز ما افغانستان نظر به دلایل مختلف توجه صورت نگرفته است.
5. پیشنهادات
6. به دلیل اینکه برای رسیدگی به این جرایم در کشور عزیز مان قواعدی وجود ندارد، پیشنهاد می گردد تا شورای ملی، قواعد و مقرراتی را در قانون جزا، قانون رسانه های همگانی و سایر قوانین مرتبط بگنجاند.
7. برای تأمین بهتر عدالت پیشنهاد می گردد تا نهادهای کشفی، امنیتی، عدلی و قضایی و ... مرتکبین این جرایم را دستگیر نموده و مورد محاکمه و مجازات قرار دهند.
8. پیشنهاد می گردد تا مضمونی تحت عنوان حقوق کامپیوتر به عنوان یکی از مضامین درسی شامل کریکولم درسی پوهنهی های حقوق، شرعیات و کامپیوتر ساینس گردیده تا باشد محصلین عزیز در این زمینه آگاهی های لازم حاصل نمایند.

²⁹ <http://yadbegir.com/main/viruse/types.htm> علی یزدی مقدم، بی تا،

فهرست منابع و مآخذ

1. القرآن کریم.
2. جریده رسمی، 1382، قانون اساسی جمهوری اسلامی افغانستان، کابل: وزارت عدلیه.
3. جعفری لنگرودی، محمد جعفر، 1385، ترمینولوژی حقوق، چاپ شانزدهم، تهران: کتابخانه گنج دانش.
4. حبیبی، خلیل الله، 1392، پول شویی و آثار زیانبار آن، کابل: انتشارات تمدن شرق.
5. ستانکزی و دیگران، 1387، قاموس اصطلاحات حقوقی، کابل: پروژه امور عدلی و قضایی افغانستان.
6. سیغانی، محمد اختر، 1393، حقوق جزای عمومی، کابل: انتشارات مستقبل.
7. عمید، حسن، 1389، فرهنگ عمید، نشر فرهنگ، تهران: نشر فرهنگ اندیشمندان.
8. مینود افشاری و علی آقا بخشی، 1386، فرهنگ علوم سیاسی، چاپ دوم، تهران: نشر چاپار.
9. نذیر، داد محمد، 1389، حقوق جزای عمومی اسلام، کابل: انتشارات رسالت.
10. نذیر، داد محمد، 1389، حقوق جزای اختصاصی اسلام، کابل: انتشارات رسالت.
11. نذیر، داد محمد، 1393، درآمدی بر حقوق ملکیت معنوی، کابل: خدمات چاپ و نشر الفاروق.
12. www.hamshahrionline.ir/details/10675، مهدی فتاحی، 21 آذر 1385
13. <http://www.tebyan.net/newindex.aspx?pid=90065>، 3/2/1388، ندا پاک نهاد،
14. <http://www.beytoote.com/computer/sundries-web/computer1-crimes.html>، بی توت، بی تا
15. <http://www.ghavanin.ir/paperdetail.asp?id=674>، 1372/10/00، محسن طاهری جبلی،
16. <http://hefazateetelaat.blogfa.com/87114.aspx>، اطلاعات، 3 بهمن، 1387.
17. www.bokhdinews.af/political/17195، سردار امیری، 26 جوزا، 1393.
18. <http://www.rahavardnoor.com/index.php/authors/item/368-jaraime-rayane>، محمد حسین طارمی، چهارشنبه، 9 مهر 1393.
19. <http://www.tar-nama.com/fa/page/135>، آفتاب، 29/7/1391، انواع 20% جرایم 20% رایانه 20% ای! /
20. <http://yadbegir.com/main/viruse/types.htm>، علی یزدی مقدم، بی تا.