مجـــله علـمـــی پـــوهنتون ســـلام

https://salam.edu.af/magazine/14

شناخت کلی جرایم کمپیوتری و انترنتی (جرایم مدرن)

استاد امین الله وزیری[1]

1- عضو کادر علمی پـوهنځی حقـوق و علـوم سیاسـی پوهنتون سلام

Waiswaziry@gmail.com

چکیده

تحقیق حاضر پیرامون جرایم کمپیوتری و انترنتی به رشته تحریر درآمده است. این تحقیق در صدد شناخت جرایم مدرنی است که به وسیله کمپیوتر و انترنت در اکثریت کشورهای جهان اتفاق افتـاده و همـه روزه در حـال گسترش می باشد.

شیوه تحقیق در این مقاله، تحلیلی- توصیفی بوده و نتیجه ایـن تحقیـق آن اسـت کـه کمپیـوتر و انترنـت از جمله وسایلی بوده که برای بشریت تمامی امکانات و اطلاع رسانی را در عرصه بین المللی به ارمغان آورده است؛ اما با توسعه و تحول آن، انقلاب بزرگی در ایجاد جـرایم در سـطح بـین المللـی بوجـود آمـده، تـا آنجـا کـه جـرایم جدیدی تحت عنوان جرایم کمپیوتری و انترنتی ظهور کرده است. جرایم کمپیوتری عبارت است از هرگونه عمـل خلاف قانون که با سوء نیت، از طرف شخص یا اشخاص با بکارگیري از کمپیوتر صورت می پذیرد و جرایم انترنتی به جرایمی اطلاق شده که در فضای مجازی یا غیر ملموس (سایبری)رخ می دهد.

امروزه در بیشتر کشورهای جهان، این جرایم به عنوان یکی از مشکلات حـاد و بسـیار مهـم تلقـی گردیـده و کشور ها در صدد آن اند تا قواعدی و مقرراتی را وضع نمـوده و راه حـل هـای مختلفـی را در جهـت جلـوگیری از وقوع آن دریابند، که متأسفانه تا هنوز در کشور عزیز ما افغانستان به این امر مهم و اساسی توجه مبذول نگردیده است.

معلومات مقاله

تاریخ نشر: 1392/05/24

شماره مقاله در ژورنال: 03

تعداد صفحات: 10

شماره نوبتی مجله: 5 و 6

کلید واژه ها

جرایم کمپیوتری، انترنت، سرقت، کلاهبرداری، سایبر

معلومات مجله:

مجله علمی پوهنتون سلام، نشرات خویش را از سال 1390 هـ.ش آغاز نموده و دست آورد های زیادی در این زمینه دارد، در ادامه سلسله فعالیت های خویش به تاریخ 1401/03/22 اعتبار نامه خویش را به عنوان یکی از معتبرترین مجله از وزارت محترم تحصیلات عالی کشور به دست آورد،

آدرس: افغانستان، کابل، ناحیه چهارم، کلوله پشته، چهار راهی قلعه بست (گل سرخ)، پوهنتون سلام.

آدرس ارتباطی؛ ویب‌سایت: https://salam.edu.af/magazine ، **ایمیل:** salamuk@salam.edu.af ، **شماره های تماس:** +93202230664 و +93788275275

مقدمه

امروزه تحولات عظیمی در تکنولوژی بوقوع پیوسته و شاهد انقلابات بزرگ در زمینه فن آوری ارتباطات فراملی طی چند دهه اخیر بوده ایم. پیـدایش کمپیـوتر و پـس از آن دنیاي مجازي انترنت، همراه خود دستاوردهاي مثبت و منفي بسیاري داشته و دارد.

کمپیوتر و انترنت علیرغم تمامی امکانات و اطلاع رسانی در عرصه بین المللی که برای ما به ارمغان آورده است ولی متأسفانه بعضی افـراد سـودجو و فرصـت طلـب بـا فراگرفتن دانش و مهارت لازم، راه های ورود به سیستم های کمپیوتر های دولتی، خصوصی و ... را به دست آورده اند که موجب بروز مشکلات و خسارات فراوانی گردیـده است.

با توسعه و تحول یافتن انترنت، در مقابل انقلاب عظیمی در ایجاد جرایم در سطح بین المللی بوجود آمده و جرایم جدیدی تحت عنوان جرایم انترنتی 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 ارایه 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- تعریفات

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 کنیم[1]، که برای نایل شدن به این هدف ابتدا باید تعریفی از جرم داشته باشیم.

الف- تعریف جرم

جرم و جریمه 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.[2] همچنان جرم در لغت به معنای گناه، خطا، بزه[3] آمده است. که خداوند جل جلاله در آیه 29 سوره المطففین می فرماید: إِنَّ الَّذِينَ أَجْرَمُوا كَانُواْ مِنَ الَّذِينَ آمَنُوا يَضْحَكُونَ (29). کسانی که گناه می کردند آنان را که ایمان آورده بودند به نیشخند می گرفتند.

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.[4]

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 نوشته[5] نیست بلکه کشورهای خانواده کامن لا[6] نیز بعلت 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 مي‌توان جرایم کمپیوتري را چنین تعریف نمود:

هرگونه عمل خلاف قانون که با سوء نیت، از طرف شخص یا اشخاص با بکارگیري از کمپیوتر صورت پذیرد جرایم کمپیوتري نامیده مي‌شود.

و یا هم هر عمل مثبت غیرقانونی که کمپیوتر در آن ابزار یا موضوع جرم باشد جرم کمپیوتری است.[7]

ج- تعریف جرم انترنتی

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

جرایم انترنتی به جرایمی اطلاق می شود که در فضای مجازی یا غیر ملموس (سایبری)رخ می دهد.[8]

---

[1] سیغانی، محمد اختر، 1393، حقوق جزای عمومی، ص 55.

[2] نذیر داد محمد، 1389، حقوق جزای عمومی اسلام، ص 44.

[3] عمید حسن، 1389، فرهنگ عمید، ص 336.

[4] سیغانی، همان اثر، صص 55- 56.

[5] 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.

[6] خانواده کامن لا شامل کشورهای انگلستان، ایالات متحده امریکا، 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.

[7] http://www.beytoote.com/computer/sundries-web/computer1-crimes.html ,.بی توت، بی تا

[8] www.hamshahrionline.ir/details/10675 ,.مهدی فتاحی، 21 آذر 1385

مبحث دوم- تاریخچه جرایم کمپیوتری و انترنتی

با پیدایش کمپیوتر، جرایم کمپیوتري نیز بوجود آمد. تاریخچهٔ جرایم کامپیوتري را مي‌توان به سه نسل طبقه بندي نمود. نسل اول که تا اواخر دهۀ 1980 مي‌باشد، شامل سرقت و کپي برداري از برنامه‌ها و جرایم علیه حریم خصوصي اشخاص مانند سرقت از آثار و تحقیقات افراد بود. نسل دوم که تحت عنوان جرایم داده‌ها نامیده مي‌شود تا اواخر دهه 1990 ادامه داشته است. در این دهه تمامي جرایم علیه تکنولوژي اطلاعاتي، ارتباطاتي، کمپیوتري، ماهواره اي و شبکه‌هاي بین المللي تحت عنوان جرایم علیه داده‌ها اطلاق مي‌شود. نسل سوم که از اواسط دهۀ 1990 شروع مي‌شود جرایم کمپیوتري تحت عنوان جرایم سایبر یا جرایم در محیط سایبر معروف گردید.

پیشینۀ تاریخي جرایم کمپیوتري به سال 1985 بر مي‌گردد که جرایم کمپیوتري در بر گیرندۀ جرایمي مانند جاسوسي کامپیوتري، سرقتهاي آثار ادبي و سوء استفاده غیر قانوني از سیستم‌هاي کامپیوتري بود. در دهۀ 1970 مقالات زیادي پیرامون جرایم کمپیوتري در روزنامه‌ها و در بعضي- از کتابها نوشته شد ولي با توجه به اینکه نوشته‌هاي آنها مبتني بر تحقیقات تجربي نبوده است لذا ارزش علمي نداشته تا بتوان به آنها استناد نمود ولي در اواسط دهۀ 1970 مطالعات تجربي پیرامون جرایم کمپیوتري صورت پذیرفت که در این مطالعات تمامي جرایم کمپیوتري بوقوع پیوسته را شامل نمي‌گر دید.[1]

اولین تحقیقاتي که پیرامون جرایم کمپیوتري صورت گرفت در امریکا بود که در این تحقیقات به قضیۀ کلاهبرداري از طریق سوء استفاده از 56 هزار مورد بیمه به ارزش حدوداً 30 میلیون دالر اشاره نمود. مورد دیگر را مي‌توان به قضیه «هراشتات» در آلمان که مربوط به معاملات ارزي خارجي به مبلغ 200 تا 300 هزار مارك از حساب ارزي بانك هراشتات خارج گردیده و همین امر باعث ورشکستگي این بانك و وارد شدن خسارت به مشتریان گردید.

در دهۀ 1980 که بعنوان نسل دوم جرایم کمپیوتري محسوب مي‌گردد، جرایم کمپیوتري فقط محدود به جرایم اقتصادي نبوده و سایر زمینه‌ها را هم که جنبۀ اقتصادي نداشته مانند دستکاري کمپیوتر شفاخانه ها، جعل اسناد با استفاده از کمپیوتر و ورود به اطلاعات خارجي محرمانۀ آمریکا، انگلستان و چند کشور دیگر دست یافته و این اطلاعات را به K.G.B بفروشند.

در دهۀ 1990 که شبکۀ جهاني (انترنت) فراگیر شد جرایم کمپوتري از جنبۀ اقتصادي وسیعتر گردیده و ابعاد جدیدتري به خود گرفته است. جرایم جدید مانند ورود کرم انترنتي که براي اولین بار توسط یك دانشجوي امریکایي ساخته شده بود و باعث شد تا سیستم کمپیوتري حدود 6200 کاربر انترنت شامل دانشگاهها، سرویسهاي نظامي و سایتهاي شفاخانه ها را مختل نماید. و هزینۀ تعمیرات سیستمها حدوداً به مبلغ 98 میلیون دالر بود که بعد از مدتي این دانشجو دستگیر و پس از محاکمه محکوم به پرداخت کلیه مبالغ فوق گردید.

در زمینه جرایم کمپیوتري مي‌توان به اقدامات زیر اشاره نمود:

تصویب موافقتنامۀ جرایم کمپیوتري در سال 1986-1985 توسط شوراي اروپا گامهاي زیادي براي تدوین قوانین مرتبط با جرایم کمپیوتري برداشته شد. در سال 1989 کمیتۀ تخصصي شوراي اروپا براي تدوین و یکنواخت نمودن سیاست جنائي مربوط به جرایم کمپیوتري پیشنهادهایي نمود که مورد تصویب شورا نیز قرار گرفت.

در همایشي که انجمن بین المللي حقوق جزا در سال 1994 داشت یکسري از مسائل را به عنوان جرایم مستقل کمپیوتري تدوین نمود. نهایتاً در سال 2001 میلادي شوراي اروپا، مبادرت به وضع موافقتامه جرایم کمپیوتري نمود که این موافقتنامه شامل چهار فصل و چهل و هشت گفتار مي‌باشد.[2]

اولین قانون راجع به جرایم انترنتي در سال 1984 در امریکا به تصویب رسید و در سال‌هاي 1994 و 1996 این قانون اصلاح گردید. در حال حاضر 44 کشور دنیا همچون: ایالات متحده امریکا، انگلستان، کشورهاي عضو اتحادیه اروپا، استرالیا و هندوستان، پولیس هایي دارند که به پولیس انترنتي مشهور است و به طور رسمي از طریق کانال‌هاي دولتي، جرایم مجازي را پیگیري مي کنند.

مبحث سوم- تفاوت جرایم کمپیوتری و انترنتی 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 می سازد. بعبارت دیگر جرایم کمپیوتری ویژگی های خاصی دارد که نه تنها وضع قوانین را مشکل می سازد، بلکه در مقام رسیدگی به اینگونه جرایم کار ماموران رسیدگی کنندۀ (پولیس، سارنوال و قاضی...) را نیز پیچیده می سازد.

در اینجا بصورت مختصر ویژگی های اینگونه جرایم را که باعث دشواری عمل قانونگذاری و نیز سختی رسیدگی به قوانین ایجاد شده می شود را مورد بررسی قرار خواهیم داد.

در ابتداء ویژگی های که وضع قانون را دشوار می کند:

1. امکانات بسیار وسیع کمپیوتر و انترنت در انجام امور مختلف: این ویژگی باعث می شود که از یکطرف وضع یک قانون کلی، اساساً بی فایده 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 می افتد.
2. جرایم کمپیوتری و انترنتی، جرایم بدون محدودیت: این جرایم محدودیت هایی 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

[1] http://www.tebyan.net/newindex.aspx?pid=90065 , 3/2/1388 .ندا پاک نهاد،

[2] http://www.beytoote.com/computer/sundries-web/computer1-crimes.html ,.بی توت، بی تا

با یک خط تلفن به سایر مراکز کمپیوتری متصل می شوند خیلی راحت میتوانند مورد هرگونه سوء استفاده قرار گیرند، نه تنها سرقت بلکه بسیاری از خرابکاری از همین طریق صورت می گیرد.

3. 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 انترنتی هیچ لزومی ندارد، بلکه معمولاً مجرم این نوع جرایم در زمان تحقق جرم اصلاً در محل وقوع جرم نمی باشد.

4. زمان وقوع این جرایم: این مسئله هم از موارد مهمی است که همیشه مورد توجه می باشد، مخصوصاً در کشورهائی 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)؟ بعبارت 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.

5. تفاوت نوع مجرمین کمپیوتر و انترنت با مجرمین سایر جرایم: مجرمین کمپیوتر و انترنت 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 مارکیت برباید. 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 انترنتی 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:

1- قربانیان جرایم کمپیوتری و انترنتی خود با این مسئله با بی میلی برخورد می کنند. اینگونه قربانیان که موسسات و ادارتی هستند که علاوه از بکارگیری وسیع کمپیوتر برای سهولت امور و ارائه خدمات به این استفاده و بکارگیری (کمپیوتر میبالند) و از پخش اخبار مربوط به سوء استفاده از کمپیوترها و انترنت 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.

2- در جرایم کمپیوتری و انترنتی 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).

3- پیچیدگی عملکرد و کاربرد کمپیوتر و انترنت 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.

4- سرعت وقوع جرم به نحوی یک جرم (مثلاً تخریب اطلاعات یک کمپیوتر) 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.

5- 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 کمپیوتر 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 باشد.[1]

[1] http://www.ghavanin.ir/paperdetail.asp?id=674 1372/10/00 ., محسن طاهری جبلی،

در پایان اشاره می شود علیرغم وجود تمام این موانع دولتها نه تنها بسیاری از جرایم کمپیوتری و انترنتی 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 کمپیوتری و انترنتی

جرایم کمپیوتری و انترنتی 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:

مطلب اول- دسته بندی جرایم کمپیوتری و انترنتی 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 بعلل 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 بعلت 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 مسول کیست؟ اثبات سوء نیت یا عدم آن تغییری در مسئله میدهد یا نه؟

جرایم ارتکابی 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 کمپیوتر ها مباشرتاً 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 مییابند 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 میدهیم:

اول- خروج غیر مجاز اطلاعات و دادن اطلاعات غلط

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

دریافت غیر مجاز اطلاعات از یک کمپیوتر 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 وقتیکه 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».[1] 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 نبایستی برداشته شود، زیرا از آن او نیست، استعمال گردیده است[2] 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).[3]

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 کمپیوتری فقط اطلاعات را در بر نمی گیرد بلکه نوع دیگر از این سرقتها، سرقت مستقیم توسط کمپیوتر است.

---

[1] جریده رسمی، 1382، قانون اساسی، م 27.

[2] نذیر، داد محمد، 1389، حقوق جزای اختصاصی اسلام، ص 168.

[3] ستانکزی و دیگران، 1387، قاموس اصطلاحات حقوقی، ص 145.

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 مناطقي که هم رزرف هواپیما و نیز رزرف هوتل در محلي که شخصي قصد مسافرت به آنجا را دارد، بوسیله کمپیوتر انجام شود، اگر هر کس بتواند این اطلاعات را از کمپیوتر مزبور بدست آورد براحتي میتوان حدس زد که اطاق شخص نیز می تواند مورد سرقت قرار گیرد.[1]

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

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.[2]

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

در این تقسیم بندي جرایم کمپیوتري و انترنتی را به سه دسته می توان تقسیم نمود:

جرایم کمپیوتري و انترنتی علیه اشخاص، جرایم کمپیوتري و انترنتی علیه اموال و دارائي اشخاص یا جرایم کمپیوتري و انترنتی اقتصادي و جرایم کمپیوتري و انترنتی علیه دولتها یا وظایف دولتها، که هر یک را ذیلاً مورد بحث قرار می دهیم:

یک- جرایم کمپیوتري و انترنتی علیه اشخاص:

جرایم کمپیوتري و انترنتی علیه اشخاص عبارتند از:

الف- نوشته‌ها و عکسهاي شهوت انگیز[3]: فروش یا به تصویر کشاندن عکسهاي مبتذل جهت تحریك کردن نوجوانان و یا پیدا نمودن اشخاص از طریق چت (گپ زدن) جهت به نمایش گذاشتن عکسهاي آنها در انترنت و معرفي آنها به دیگر اشخاص جهت داشتن ارتباط نامشروع.

ب- اذیت و آزار کردن[4]: این نوع جرم ممکن است به صورت ارتباطات و دست انداختن و استهزا کردن، بي حرمتي به مقدسات و مطالبه کردن وجه از دیگران باشد.

ج- تهدید به قتل: یکي از جرایمي که ممکن است از طریق انترنت و یا ارسال پیغام به ایمیل اشخاص صورت پذیرد تهدید به قتل مي‌باشد.

دو- جرایم کمپیوتري و انترنتی علیه اموال و مالکیت

جرایم علیه اموال و مالکیت یا جرایم اقتصادي که از طریق کمپیوتر یا شبکهٔ جهاني (انترنت) صورت مي‌پذیرد عبارتند از:

الف- سرقت و تکثیر غیر مجاز برنامه‌هاي کمپیوتري حمایت شده: بدیهی است که تهیه برنامه های کمپیوتری توسط متخصصین این عرصه که در شرکت های تولید کمپیوتر یا شرکت های متخصص در عرصه تولید برنامه های کمپیوتری کار می کنند، صورت می گیرد. به هر حال در تهیه این گونه برنامه ها، خواه به وسیله شرکت های تولید کمپیوتر باشد یا به واسطه شرکت های متخصص در عرصه تولید برنامه های کمپیوتری، هزینه هنگفت و نیروی بشری بزرگ مورد استفاده قرار می گیرد، پس چون آماده کردن برنامه های کمپیوتری مدت طولانی می خواهد، تکالیف مالی هنگفت می طلبد و خیلی ها مشکل و دشوار می باشد، خیلی ها نادر خواهد

---

[1] http://www.ghavanin.ir/paperdetail.asp?id=674،1372/10/00. محسن طاهری جبلی

[2] http://www.ghavanin.ir/paperdetail.asp?id=674،1372/10/00. محسن طاهری جبلی

[3] pornography

[4] Harassment

بود که یک شخص از عهده تهیه برنامه های کمپیوتری کامل بر آید.[1] لذا تکثیر و استفاده غیر مجاز از آن برای صاحبان قانونی زیان های زیادی را به بار خواهد داشت. مثلاً زماني كه يك كارگردان و تهيه‌كنندة فلم سينمائي با زحمات زيادي كه كشيده و هزينه‌هاي هنگفتي كه براي ساخت فلم صرف نموده بعد از به نمايش گذاشتن آن فلم ممكن است همان فلم از طريق انترنت بفروش رسيده و زيانهاي زيادي به سازندة فلم وارد شود.

ب- سابوتاژ و اخاذي كمپيوتري: واژه سابوتاژ به معنای خرابکاری و کارشکنی می باشد[2] و سابوتاژ كمپيوتري عبارت است از اصلاح، موقوف سازي و يا پاك كردن غير مجاز داده‌ها و يا عمليات كمپيوتري به منظور مختل ساختن عملكرد عادي سيستم. سابوتاژ كمپيوتري ممكن است وسيله‌اي براي تحصيل مزاياي اقتصادي بيشتر نسبت به رقيبان يا براي پيش‌برد فعاليتهاي غير قانوني تروريستی براي سرقت داده‌ها و برنامه‌ها به منظور اخاذي باشد.

ج- كلاهبرداري: كلاهبرداری 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.[3]

كلاهبرداري كمپيوتري از جمله جرايم اصلي سوء استفاده هاي كمپيوتري عليه اشخاص و يا دارائي افراد محسوب مي‌گردد.

دارايي عيني غير ملموس در قالب داده‌هاي كمپيوتري مانند وجوه سپرده و پس انداز، تغيير و دست كاري كردن در ساعات كاري، متداولترين راه هاي كلاهبرداري كمپيوتري مي‌باشد. در تجارت الكترونيك نقل و انتقال پول نقد و خريد و فروش كالاهاي تجاري، به سرعت جاي خود را به انتقال سپرده‌ها از طريق سيستم هاي كمپيوتري داده‌است كه نتيجتاً موجبات سوء استفاده كردن افراد سودجو و فرصت طلب را فراهم كرده است.[4]

وارد كردن رمزها به خودپردازها و سوء استفاده كردن از كارتهاي اعتباري ديگران معمول ترين شيوة ارتكاب در كلاهبرداري كمپيوتري مي‌باشد.

در ذيل به نمونه‌هائي از كلاهبرداري هاي كمپيوتري اشاره می نماييم:

- سوء استفاده از شبكة تلفني: امروزه بعضي از افراد سودجو با استفاده از تكنيك هايي وارد خطوط تلفني مي‌شوند كه آنها مي توانند مكالمات تلفني خود را با هزينه‌هاي مشتركين ديگر انجام دهند.
- سوء استفاده از صندوقهاي خود پرداز: در گذشته، سوء استفاده از صندوقهاي خود پرداز با استفاده از كارت بانك هايي كه به سرقت مي‌رفت صورت مي گرفت ولي امروزه، با استفاده از سخت افزار و نرم افزار ويژة كمپيوتري، اطلاعات الكترونيكي غير واقعي به صورت كد (رمز) روي كارتهاي بانك ثبت شده مورد سوء استفاده قرار مي‌گيرد.
- سوء استفاده از كارتهاي اعتباري: در حال حاضر، بيشتر معاملات از طريق انترنت صورت مي گيرد. مثلاً پرداخت بل صرفيه برق، آب، تلفن و همچنين خريد كالا، شركت در همايش هاي بين المللي و غيره معمولاً با استفاده از كرديت كارت (كارت اعتباري) استفاده مي‌شود و معمولاً مشتري مي‌بايستي رمز كارت خود و ديگر جزئيات را قيد نمايد. بدين جهت بعضي از افراد سودجو با فاش شدن رمز كارت اعتباري مشتريان سوء استفاده مي‌نمايند.

د- قاچاق مواد مخدر از طريق اينترنت: با توجه به دسترسي آسان افراد به همديگر از طريق انترنت و ارسال ايميل، هرگونه خريد و فروش و پخش مواد مخدر از طريق شبكه‌هاي كمپيوتري انجام مي‌شود. ضريب اطمينان قاچاق كنندگان مواد مخدر از طريق كمپيوتر نسبت به نوع سنتي آن بالاتر مي‌باشد. زيرا پوليس به راحتي نمي‌تواند از برنامه‌هاي قاچاق كنندگان مطلع شود و لذا اقدامات پوليس در خصوص كشف فروشندگان و خريداران مواد مخدر غير ممكن است.

هـ- پولشويي كمپيوتري: 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.[5]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.[6]

پولشويي و غارت يكي از جرايم كلاسيك بوده كه داراي سابقه طولاني است كه با پيشرفت تكنولوژي اين جرم از طريق كمپيوتر و انترنت صورت مي‌پذيرد. نحوة ارتكاب بدين صورت است كه باندهاي بزرگ نامشروع با ارسال ايميل پيشنهاد انجام يك كار تجاري را به شخصي- مي‌نمايند و بدون اينكه اثر و نشاني از خود بجاي بگذارند پيشنهاد ارسال مبالغي پول به حساب شخصي را كه براي او ايميل فرستاده‌اند مي‌نمايند و در تقاضاي خود نحوة ارسال و سهم هر يك از طرفين را بيان نموده و در صورت توافق طرف مقابل (گيرندة ايميل) نوع و نحوة تضمينات لازم را اعلام مي‌كنند و اصولاً در زمان استرداد پول يك عنوان مشروع در تجارت الكترونيك را با منشأ تجاري انتخاب و با هدف خود هماهنگ مي‌نمايند.

سه- جرايم كمپيوتري و انترنتی عليه دولتها

بعضي از جرايم كمپيوتري عليه دولتها ممكن است به انگيزه‌هاي سياسي صورت پذيرد كه مي‌توان به موارد زير اشاره نمود:

الف- تهديد به گروگان گيري، اخاذي و كشتن مسئولين و يا اعضاي خانوادة آنها: يكي از جرايم مدرن كمپيوتري كه معمولاً قاچاقبران و يا افراد سياسي براي رسيدن به اهداف خود از آنها استفاده مي‌نمايند، تهديد مقامات كشور و يا خانوادة آنها به گروگان گرفتن و يا كشتن است. اين جرم به دليل آنكه عليه مقامات بلند رتبه يک دولت صورت می گيرد، در زمره جرايم كمپيوتری عليه دولتها قرار می گيرد. معمولاً جرايمي كه توسط افراد سياسي صورت مي گيرد با قاچاقبران متفاوت است.

---

[1] نذیر، داد محمد، 1393، در آمدی بر حقوق ملکیت معنوی، ص 219.

[2] عمید، حسن، 1389، فرهنگ عمید، ص 519.

[3] جعفری لنگرودی، محمد جعفر، 1385، ترمینولوژی حقوق، ص 574.

[4] http://hefazateetelaat.blogfa.com/87114.aspx اطلاعات، 3 بهمن، 1387،.

[5] www.bokhdinews.af/political/17195 سردار امیری، 26جوزا، 1393،.

[6] حبیبی ، خلیل الله، 1392، پول شویی و آثار زیانبار آن، ص 19.

قاچاقبران معمولاً از طريق تهديد به گروگان‌گيري و همچنين تهديد به كشتن و اخاذي از مسئولين اقدام مي‌نمايند ولي افراد سياسي از طريق اعلام در انترنت دولت را تهديد به جنگ مسلحانه و براندازي حكومت مي‌نمايند بدون آنكه آثاري از خود بجاي بگذارند.

ب- جاسوسي كمپيوتري: جاسوسي كمپيوتري به عملي گفته مي‌شود كه شخصي يا گروهي براي يك دولتي اطلاعات مخفيانه از دولت ديگر را براى دريافت پول انجام مي‌دهد. بعنوان مثال مي‌توان به موارد زير اشاره نمود: در آلمان سازمان اطلاعاتي K.G.B روسيه به شخصي پول داده بود تا اطلاعات مخفيانه ارتش امريكا را بدست آورد. يا در مورد ديگر مي‌توان به قضيه لوس آلماس دانشمند هسته‌اي اشاره نمود كه اطلاعات بسيار محرمانة هسته‌اي خود را در اختيار دولت چين قرار داده بود.

ج- تروريسم: تروريسم عبارت است از كاربرد سيستماتيک ترور (وحشت و ترس زياد) است، به ويژه به عنوان وسيله اجبار يا روا شمردن اقدامات داراى ماهيت وحشت آفرينى در اذهان عامه و گروه هاى انسانى براى ساقط كردن حكومت، حفظ حكومت يا تغيير حكومت[1]. امروزه برخي اقدامات تروريستي با دسترسي به اطلاعات حفاظت شده صورت مي‌پذيرد. تروريست هاي اطلاعاتي فقط با استفاده از يك كمپيوتر مي‌توانند بصورت غير مجاز وارد سيستم‌هاي كمپيوتري امنيتي شوند، مثلاً با تداخل در سيستم ناوبري هوائي باعث سقوط هواپيما شده يا باعث قطع برق سراسري شوند.

جرايم عليه كمپيوتر

كمپيوتر يک شخص حقيقى (و حتى حقوقى) نيست كه جرمى عليه آن متصور باشد و اين عنوان را براى سهولت كار و تقسيم بندى موضوعات به آن داده ايم وگرنه جرايم مورد نظر در اين قسمت عموماً به دارندگان آن نرم افزار ضرر ميزند.

اساس كار برد هر كمپيوتر، نرم افزارهايى است كه در آن بكار برده ميشود، به همين علت است كه نرم افزارها از ارزش خاصى برخوردار هستند و همچنان به همين علت است كه جرايم مربوط به آنها رو به افزايش بود و بعلاوه خصوصيات خاصى را نيز دارا ميباشند.

براى جلوگيرى از اطاله كلام از جرايمى مثل سرقت نرم افزارها كه با عناوين فعلى جرايم هم قابل پيگيرى است خودددارى ميكنيم. اما موارد ديگرى هم وجود دارد كه اگر چه از نظر نتيجه همانند سرقت ميباشند ولى شرايط خاص خود را دارا ميباشند، از جمله كاپى بردارى از نرم افزارها، مسئله اى بسيار مهم كه در صدر تمام جرايم كمپيوترى قرار گرفته است. شايد به همين دليل باشد كه سالانه ميليونها دالر صرف هزينه هاى نگهدارى و حفاظت از نرم افزارها ميشود. بنظر بعضى از دست اندركاران كمپيوتر كاپى بردارى از نرم افزار براى كسانيكه آنها را نخريده اند نوعى سرقت «اموال فكرى» ميباشد.

همانگونه كه روند پيشرفت كمپيوتر سريع است، جرايم وابسته به آن نيز با همان سرعت بوجود مى آيند. يكى از اين آخرين جرايم كه جنبه تخريبى دارد ويروس كمپيوتر است. ويروس كمپيوتر يک اصطلاح عاميانه براى اطلاعاتى است كه بطرق مختلف بصورت غير مجاز وارد يک سيستم پردازش داده ها مى شود. اينگونه قاچاق اطلاعات ميتواند به تخريب اطلاعات يا حتى نابودى كامل اطلاعات ذخيره شده در سيستم منجر گردد. اين ويروسها ميتوانند به آسانى توسط يک فرد كه بوسيله يک سيستم ارتباط از راه دور با كمپيوتر تماس مى گيرد وارد آن شود. ويروس كمپيوتر بيمارى خطرناكى است و فرديكه به چگونگى بوجود آوردن و تزريق يک ويروس به كمپيوتر آشنا باشد، سلاح خطرناكى در دست دارد. بدينترتيب كه او ميتواند ويروسى ايجاد كند كه به اطلاعات خاصى حمله كرده و آنها را از بين ببرد يا اينكه تمام فايلهاى داده ها را مورد حمله قرار داده و خيلى سريع اطلاعات را از بين ببرد بنحويكه امكان بازسازى آن نباشد، همچنين امكان ايجاد ويروسى هست كه ميتواند با تغيير برنامه هاى حفاظتى دادها، دسترسى فرد خرابكار را به اطلاعات محرمانه ممكن سازد.

مطلب دوم- طبقه بندی جرايم كمپيوتری و انترنتی از لحاظ تاريخی

به‌طور كلي از اين لحاظ، جرايم كمپيوتری و انترنتی را مي‌توان به دو دسته تقسيم كرد، قديمی و مدرن:

1- جرايم كمپيوتری و انترنتی قديمی

جرايم كمپيوتری و انترنتی سنتي جرايمي هستند كه با همان شرايط قانوني كه از طرق مرسوم ارتكاب مي‌يابند، به‌وسيله كمپيوتر نيز ارتكاب مي‌يابند و قانون‌گذار ارتكاب به‌وسيله كمپيوتر را به عنوان جزئي از اجزاي عنصر مادي آن‌ها يا عامل تشديد و يا تخفيف مجازات آن‌ها ذكر نكرده باشد.

جرايم كمپيوتری و انترنتی قديمی را مي‌توان به پنج دسته به شرح ذيل تقسيم كرد:

1. جرايم كمپيوتری و انترنتی عليه اشخاص؛
2. جرايم كمپيوتری و انترنتی عليه اموال؛
3. جرايم كمپيوتری و انترنتی عليه آسايش و امنيت عمومي؛
4. جرايم كمپيوتری و انترنتی عليه عصمت و عفت و اخلاق حسنه؛
5. جرايم كمپيوتری و انترنتی عليه خانواده.

2- جرايم كمپيوتری و انترنتی مدرن

جرايم كمپيوتری و انترنتی مدرن جرايمي هستند كه غالباً پس از پيدايش كمپيوتر بوجود آمده‌اند و با پيشرفت كمپيوتر تحول پيدا كرده‌اند و به موجب وضع قوانين در زمينه عنصر مادي آن‌ها نيز به شكل جداگانه مشخص گرديده است.

جرايم كمپيوتری و انترنتی مدرن را مي‌توان به شش دسته به شرح ذيل تقسيم كرد:

1. جرايم كمپيوتری و انترنتی عليه محرمانگي، تماميت و در دسترس بودن داده‌ها، مانند: دستيابي غير مجاز، شنود غيرمجاز و اختلال در داده؛
2. جرايم كمپيوتری و انترنتی عليه سيستم كمپيوتری مانند اختلال در سيستم؛
3. جرايم كمپيوتری و انترنتی عليه اموال مانند كلاهبرداري انترنتی؛

[1] مينود افشاری و علی آقا بخشی، 1386، فرهنگ علوم سياسی، چاپ دوم، تهران، نشر چاپار، ص 677.

4. جرايم كمپيوتری و انترنتی عليه امنيت و آسايش عمومي مانند جعل انترنتی؛
5. جرايم كمپيوتری و انترنتی عليه مالكيت معنوي؛
6. جرايم كمپيوتری و انترنتی عليه محتوي مانند انتشار پورنوگرافي كودك.

به طور كلي، آنچه مبنا و محور اين نوع از تقسيم‌بندي‌ها قرار گرفته است، ارزش‌هايي هستند كه مورد حمايت قانون‌گذار بوده و مورد تجاوز و تعدي مجرمان قرار گرفته‌اند.

مطلب سوم- جرايم كمپيوتری و انترنتی از نظر نوع تأثير

جرايم كمپيوتری و انترنتی را از لحاظ نوع تأثير به سه طبقه كلي تقسيم می كنند، فرهنگی، امنيتی و مالی.

1- جرايم فرهنگي

كه شامل جرايم بر ضد مالكيت فكري و جرايم بر ضد ارزش‌هاي فرهنگي چون، جرايم توهين و اهانت به دين مبين اسلام و مقدسات آن، جرايم محتوا (Content Crime)، افشاي اسرار خصوصي افراد و ... می شود.

2- جرايم امنيتی

كه اين جرايم شامل موارد ذيل می شود:

1. جرايم عليه امنيت داده‌ها، از جمله: جرايم عليه كاربرد مجاز داده‌ها مثل جاسوسي دسترسي غير مجاز؛ و جرايم عليه صحت داده‌ها، همچون جعل؛
2. جرايم عليه امنيت سيستم؛

3- جرايم مالی

كه شامل كلاهبرداري و سرقت و ... می شود.[1]

در پايان بايد لازم به ذكر است كه بعضی از نويسندگان و دانشمندان، جرايم انترنتی را به انواع ذيل نيز دسته بندی می نمايند:

1- هك كردن

هک كردن عبارت است از نفوذ به يك سيستم كمپيوتري بدون داشتن مجوز، مالكيت يا صلاحيت لازم. هك كردن يعني غلبه كردن بر سيستم هاي امنيتي يك سيستم كمپيوتري براي دسترسي غير قانوني به اطلاعات ذخيره شده در آن سيستم. فاش كردن رمز عبور به قصد دسترسي به اطلاعات خصوصي افراد يك سازمان يكي از رايج ترين تخلفات انترنتی است. يكي از خطرناكترين خلاف كاري هاي انترنتی عبارتست از هك كردن آدرسIP تا بدين وسيله خلافكار خود را به جاي كس ديگر جا بزند و افكار شوم يا جنايات مورد نظر خود را اجرا كند.

2- Phishing

فيشينگ عبارتست از تلاش براي بدست آوردن اطلاعاتي مانند رمز عبور، شناسه عبور و جزئيات كارت اعتباري با جا زدن خود به عنوان يك منبع قابل اعتماد. فيشينگ از طريق سرويس هاي ايميل يا با وعده هاي دروغ انجام مي گيرد يا با ايجاد برخي جذابيت ها كاربران انترنتي را ترغيب مي كنند اطلاعات خود را در سايت هايي كه توسط كلاه برداران ساخته شده است وارد كنند. اين خلاف كاران معمولاً وب سايت هايي طراحي مي كنند كه در كاربر احساس اعتماد و وارد شدن در يك سايت امن را مي دهد و معمولاً هم موفق مي شوند يعني كاربر در دام آنها افتاده و اطلاعات خود را وارد مي كند.[2]

3- گروه ويروس هاي كمپيوتري

دسته ای از ويروس هاي كمپيوتري (شامل ويروس ها، كرم ها، نرم افزار هاي جاسوسي و...) در حقيقت نرم افزارهايي هستند كه خود را تكثير و منتشر مي كنند و كمپيوترهاي موجود در يك شبكه را بدون اطلاع كاربران آلوده كرده و به آنها صدمه مي زند. ويروس ها از طريق فايل هاي سيستم يك شبكه كمپيوتري، انترنت يا هر وسيله نقل انتقال اطلاعات مانند حافظه فلش، CD و ...وارد كمپيوترهاي ديگر مي شوند.

ويروس هاي كمپيوتري كدهايي هستند كه با هدف ضربه زدن به يك سيستم كمپيوتری يا از بين بردن اطلاعات نوشته شده اند. نوشتن ويروس كمپيوتري در همه جاي دنيا يك جرم است به گونه اي كه نويسنده ويروس در برابر تمام خسارت هاي وارده به همه كمپيوترهاي آلوده شده مسئول است.

4- Cyber stalking

عبارت است از استفاده از فناوري ارتباطات به خصوص انترنت براي آزار و اذيت افراد. تهمت، ارسال نرم افزارهاي مخرب و تخريب اطلاعات و تجهيزات كمپيوتري در اين گروه قرار مي گيرند. اين خلافكاران اغلب كاربران را از طريق چت روم ها، تالارهاي تبادل نظر و اجتماعات انترنتي شكار مي كنند سپس اطلاعات آنها را بدست مي آورند (مثلاً شماره تلفن و آدرس، محل كار و ...) و با استفاده از اين اطلاعات قربانيان خود را مورد اذيت و آزار قرار مي دهند. ايميل هاي تهديد آميز، مزاحمت تلفني و مانند اينها انجام مي دهند و اين مورد يكي از جرم هاي رايانه اي خطرناك است كه در سراسر دنيا مجازات سنگيني برايش قرار مي گيرد.

---

[1] http://www.rahavardnoor.com/index.php/authors/item/368-jaraieme-rayaneمحمد حسين طارمی، چهارشنبه، 9 مهر 1393.

[2] http://www.tar-nama.com/fa/page/135آفتاب، 29/ 7/ 1391، /انواع%20جرايم%20رايانه%20ای!/

5- هويت جعلي

هويت جعلي يا خود را به جاي كس ديگر جا زدن يكي از جديدترين كلاه برداري هايي است كه به كمك آن پول هاي زيادي ربوده شده و سودهاي كلاني نصيب كلاه برداران مي شود. در اين شيوه كلاه بردار خود را به جاي مالك چيزي جا مي زند. يا از هويت شخص ديگري براي بدست آوردن كالا يا خدمات مورد نياز خود استفاده مي كند. مهاجرت غير قانوني، تروريسم و ايميل هاي سياه در زمره اين جرايم قرار مي گيرد.[1]

نتیجه گیری

از آنچه متذکر شدیم بر می آید که جهان امروز جهان علم و فناوری است و بدون شک پیشرفت را نمی‌توان از آن جدا کرد. این در حالی است که همگام با پیشرفت‌های علمی بویژه در زمینه کمپیوتر و انترنت، عده‌ای برخلاف خدمتگزاران بشریت که به فکر استفاده‌های مثبت از فناوری‌ها هستند به فکر سوءاستفاده‌اند؛ یعنی بعضی اشخاص اعمال خلاف قانون را با سوء نیت، با بکارگیري از کمپیوتر و انترنت مرتکب می شوند که بدان میتوان جرایم کمپیوتري و انترنتی اطلاق نمود.

جرایم کمپیوتری و انترنتی از جمله پیش‌رونده‌ترین جرایمی هستند که با سرعت زیاد در حال گسترش و بلای جان بشر امروز شده اند.

ویژگي‌هاي خاصي چون: تخصصي و علمي بودن، داراي حيثيت عمومي و خصوصي بودن، پيچيدگي خاص، دشوار بودن تعيين صلاحيت جزايي، جهاني بودن، دشوار بودن كشف مجرم كه در اين دست از جرايم بروز كرده، است آن را از ديگر جرايم متمايز مي نمايد.

در حال حاضر جرایم کمپیوتری و انترنتی با اشکال های مختلفی صورت می پذیرد که عبارت اند از: کلاهبرداری انترنتی، سوء استفاده از شبکه تلفنی، سوء استفاده از کارتهای اعتباری، وارد کردن ویروس به کمپیوترهای 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.

پیشنهادات

1. 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.
2. 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.
3. پیشنهاد می گردد تا مضمونی تحت عنوان حقوق کمپیوتر به عنوان یکی از مضامین درسی شامل کریکولم درسی پوهنحی های حقوق، شرعیات و کمپیوتر ساینس گردیده تا باشد محصلین عزیز در این زمینه آگاهی های لازم حاصل نمایند.

فهرست منابع و مأخذ

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، در آمدی 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، 26جوزا، 1393،.
18. http://www.rahavardnoor.com/index.php/authors/item/368-jaraieme-rayane.محمد حسین طارمی، چهارشنبه، 9 مهر 1393.
19. http://www.tar-nama.com/fa/page/135.آفتاب، 29/ 7/ 1391، /انواع%20جرایم%20رایانه%20ای!/
20. http://yadbegir.com/main/viruse/types.htm .علی یزدی مقدم، بی تا،

[1] http://yadbegir.com/main/viruse/types.htm علی یزدی مقدم، بی تا،