هفتمین همایش ملی بنیاد علمی قانون یار
همایش پژوهش های علمی علوم اسلامی و انسانی در عصر نوین

بنیاد علمی قانون یار - آموزش و پرورش استان کرمانشاه – واحد پژوهش سپاه پاسداران
(با همکاری و حمایت معنوی دانشگاه رازی، دانشگاه آزاد، دانشگاه فرهنگیان، دانشگاه پیام نور کرمانشاه، دانشگاه علمی و کاربردی، جهاد دانشگاهی واحد کرمانشاه، دانشگاه صنعتی کرمانشاه، بنیاد شهید و سازمان ارشاد و....

سردبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی (نمایه مقالات در پایگاه های ملی و بین المللی)
تاریخ برگزاری همایش: ۸ اسفندماه ۱۴۰۳ شماره مقاله: ۲۸/۹۱۱۸ رده بندی کنگره: ب ۵۶/۶۰۰

بررسی و تحلیل جزایی جرایم سایبری در نظام کیفری ایران

جواد چراغی

چکیده

جرایم سایبری به طیف وسیعی از فعالیت‌های مجرمانه اطلاق می‌شود که با استفاده از ابزارهای دیجیتال و شبکه‌های کامپیوتری انجام می‌شوند. این جرایم می‌توانند شامل موارد زیر باشند: کلاهبرداری رایانه‌ای، هک و نفوذ، تخریب و اخلال در داده‌ها، انتشار محتوای مجرمانه، جعل و تقلب، جاسوسی سایبری، نقض حریم خصوصی و.... با توجه به آثار مخرب و پیچیدگی فزاینده جرایم سایبری، آگاهی بخشی و تحلیل حقوقی این پدیده از اهمیت بالایی برخوردار است. تحلیل جزایی جرایم سایبری در نظام کیفری به بررسی و تبیین جنبه‌های کیفری جرایمی می‌پردازد که در فضای سایبر یا با استفاده از فناوری اطلاعات و ارتباطات رخ می‌دهند. این تحلیل شامل شناسایی و تعریف جرایم سایبری، بررسی عناصر تشکیل‌دهنده آنها، تعیین مجازات‌های قانونی و همچنین تحلیل چالش‌های مرتبط با شناسایی، تعقیب و محاکمه مرتکبان این جرایم است. با توجه به اهمیت بالای موضوع مطروحه در این مقاله قصد داریم به بررسی جزایی جرایم سایبری در نظام کیفری ایران بپردازیم. روش تحقیق از نوع تحلیلی-توصیفی بوده و ابزار گردآوری اطلاعات و داده ها فیش برداری و بهره از کتب و مقالات مربوطه است.

واژگان کلیدی: جرایم سایبری، جرایم کامپیوتری، اینترنت، محتوای مجرمانه، فضای مجازی

بخش اول: کلیات

بند اول: تعریف اینترنت

اینترنت را مجموعه ای از شبکه ها گویند و از طریق آن شبکه ها ی مختلف رایانه ای توسط سخت افزار و نرم افزارهای مربوط و با قرار دادهای ارتباطی یکسان به یکدیگر متصل شده و با اختصاص آدرس های الکترونیکی خاص هر یک از آنها می توانند به صورت متن، صدا، تصویر و حتی فیلم تبادل اطلاعات کنند. بنابراین اینترنت موجب دسترسی آسان و سریع به حجم عظیمی از اطلاعات در کوتاه ترین زمان ممکن گردیده و هر روز در حال گسترش و توسعه می باشد بطوریکه امروز مانند اشعه ای نور خود را بر پنج قاره جهان افکنده و دنیای شگفت انگیزی را بوجود آورده که با ورود در آن می توان مطالب فراوانی در ماهیت شبکه ها و پایگاه آموخته و علاوه بر آن می توان به تمامی موضوعات موجود و قابل بررسی در جهان دست یافت.سال واقعی پیدایش اینترنت را سال ۱۹۸۳ می دانند چرا که در این سال تغییرات مهمی در کنترل شبکه ها صورت گرفت و بسیاری از شبکه ها از شبکه های اروپا و ژاپن، توسط دروازه هایی به آرپانت وصل شدند. در سال ۱۹۹۰ آرپانت منحل شد و وظائف آن به ساختار گسترده تری بنام اینترنت محول شد و به دنبال آن ممنوعیت جابجایی پیام های تجاری نیز برداشته شد و با تبدیل سیستم عامل یونیکس دیگر برنامه ی کاربردی علمی به واسطه های تحت ویندوز استفاده از اینترنت برای عموم راحت شد و اینترنت کنونی بوجود آمد.[1]

بند دوم: مفهوم جرائم رایانه ای

در کشور ما تعاریفی که در پیش‌نویس جرائم رایانه‌ای آمده جرم‌ها را به جرم‌هایی از قبیل کلاهبرداری کامپیوتری، جعل کامپیوتری، جاسوسی کامپیوتری، سابوتاژ کامپیوتری (تغییر، محو، متوقف سازی و شنود در خطوط ارتباطی و...) تخریب کامپیوتری، دستیابی غیرمجاز، شنود غیرقانونی و... تقسیم کرده و مجازات‌هایی برای برخورد با این جرائم در نظر گرفته شده است. انتشار اخبار کذب، ارسال مطالب، تصاویر و فیلم‌های مستهجن، آموزش و تبلیغ تروریسم، هتک حرمت افراد، استفاده از فضای متعلق به

[1]. مقالهٔ دکتر میرمحمد صادقی – کلاهبرداری رایانه

دیگران، ارسال پیام های مخرب، اخلال در دسترسی به دیگران، نقض حق مالکیت، هک و ویروسی کردن سایت‌ها و ورود غیرمجاز به حریم خصوصی افراد از طریق ایمیل‌ها بخشی از جرم‌های رایانه‌ای محسوب می‌شوند.[۱]

بند سوم: تعریف محیط سایبر

از لحاظ لغوی در فرهنگ‌های مختلف سایبر به معنی مجازی و غیرملموس می‌باشد، محیطی است مجازی و غیرملموس موجود در فضای شبکه های بین المللی (این شبکه ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت بهم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگها، ملتها، کشورها و به طور کلی هر آنچه در کره خاکی بصورت فیزیکی ملموس وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران می‌باشند و به طریق کامپیوتر، اجزا آن و شبکه‌های بین‌المللی بهم مرتبط می‌باشند.[۲]

بخش دوم: توصیف فضای سایبر

از جمله اصطلاحاتی که اخیراً به فرهنگ بشری وارد شده و در مدت بسیار کم ازعمر خود تمام شئون زندگی بشر را به تسخیر در آورده فضای سایبری است. فضا در مفهوم خویش به تنهایی هیچ ویژگی خاصی را مطرح نمی‌کند ولی به محض آن که یک گروه انسانی فعالیتی را در مکانی مطرح کند، معنای نمادین فضا شکل می‌گیرد و بستری برای بیان فعالیت و رفتارهای انسانی می‌گردد. واژه سایبر[۳] در سال ۱۸۳۴ در فرانسه به منظور توصیف علم حکومت ابداع شده است که از واژه‌ای یونانی به معنای سکاندار[۴] یا راهنما مشتق شده است. سایبر در زبان انگلیسی پیشوند و در زبان فارسی پسوندی است که به کلمات جدید و امروزی متصل می‌شود تا به آن‌ها معنا و مفهوم دهد به گونه‌ای که مرتبط با فضای رایانه‌ای یا

---

۱. مالمیر، محمود و زررخ، احسان، پیشگیری از بزه دیدگی سایبری،فصلنامه مطالعات پیشگیری از جرم، سال پنجم، شماره هفدهم، ۱۳۸۹

۲. همان.

۳ Cyber

۴ Sculls

برخط[1] باشد. این واژه در سال۱۹۴۸توسط ریاضیدانی بـه نـام نـوربرت وینـر[2]بـه عنـوان قسـمتی از واژه سیبرنتیک[3]مورد استفاده قرارگرفت. در همین سال یک نویسنده علمی-تخیلی به نام ویلیام گیبسـون[4]در رمانی با عنوان نیورومانسر واژه سایبر را به اسپیس چسباند تا شبکه‌های کامپیوتری دنیای آنلاین را نشان دهد و از آن زمان فضای سایبر مترادف با دنیای کامپیوترها و شبکه اینترنت قرار گرفت. «در سال ۱۹۹۰ این واژه، توسط پرفسور جان پری بارلو به هنگام صحبت در یک کنفرانس برخط آن را بکار برد و بر سـر زبان‌ها انداخت و جایگزین عناوین دیگر مانند فناوری اطلاعات و ارتباطات، حقوق انفورماتیک و... شـد و مشتقات زیادی از آن مانند (سایبر کافی)[5]، (سایبر اسپیس)[6] و (سایبرلا)[7]ساخته شد.»[8]. در ترجمه فارسـی فارسی این لغت معمولاً سه اصطلاح رایانه‌ای، سایبری و آنلاین بکار برده می‌شود؛ مثل دنیـای مجـازی آنلاین[9]، بزه‌های رایانه‌ای یا سایبری[10] یا پول رایانه ای[11]. «سـایبر در فرهنـگ‌هـای مختلـف فارسـی از لحاظ لغوی به معنای مجازی و مترادف لغت انگلیسی (ویرتال)[12] آمده است و در برخی فرهنگ‌های لغت کامپیوترهای بزرگ یا ابرکامپیوترها که بدست شرکت کنترل دیتا (سی– دی– سی) ساخته‌شده‌اند، ماننـد کامپیوتر سایبر۷۰[13] اطلاق شده است»[1].

---

[1] Online

[2] Norbert wiener

[3] سیبرنتیک شاخه‌ای از علوم، که سیستم ارتباطی مغز و سیستم اعصاب انسان را مطالعه می کند، به عبارتی سـیبرنتیک علـم مطالعـه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی است.

[4] گیبسون فضای سایبری را این گونه معرفی می کند: فضای سایبریک توهم مـورد وفـاق(consensual hallucination) اسـت که روزانه میلیاردها اپراتور و کودکانی که مفاهیم ریاضی به آن‌ها داده می‌شود آن را تجربه می کنند.

[5] Cyber coffee

[6] Cyber space

[7] Cyber-Law

[8] قاجار قیونلو، سیامک،(۱۳۹۱)،«مقدمه حقوق سایبر»،چاپ اول،ص ۱۳۲

[9] Cybers Pace

[10] Cyber crime

[11] Cyber cash

[12] Virtual

[13] Cyber Zo

بخش سوم: نگاهی اجمالی به تاریخچه جرایم اینترنتی

نسل اول جرائم رایانه ای، که تا اواخر دهه ۱۹۸۰ است شامل سرقت و کپی‌برداری از برنامه‌ها و جرائم علیه حریم خصوصی اشخاص مانند سرقت از آثار و تحقیقات افراد بوده است. نسل دوم جرائم رایانه ای، که تحت عنوان جرائم داده ها نامیده می شود تا اواخر دهه ۱۹۹۰ ادامه داشت. در این دهه تمامی جرائم رایانه ای علیه تکنولوژی اطلاعاتی، ارتباطاتی، کامپیوتری، ماهواره‌ای و شبکه‌های بین‌المللی تحت عنوان جرائم علیه داده‌ها اطلاق می‌شود. نسل سوم جرائم رایانه ای، که از اواسط دهه ۱۹۹۰ شروع می‌شود به جرائم رایانه ای تحت عنوان جرائم سایبر یا جرایم در محیط سایبر معروف شد. پیشینه تاریخی جرائم رایانه ای به سال ۱۹۸۵ بر می گردد که جرائم رایانه ای در برگیرنده جرایمی مانند جاسوسی کامپیوتری، سرقت‌های آثار ادبی و سوءاستفاده غیرقانونی از سیستم‌های کامپیوتری بود. در دهه ۱۹۷۰ مقالات زیادی پیرامون جرائم رایانه ای در روزنامه‌ها و در بعضی از کتاب‌ها نوشته شد ولی با توجه به اینکه آن نوشته ها مبتنی بر تحقیقات تجربی نبوده است لذا ارزش علمی نداشته تا بتوان به آنها استناد کرد. نخستین تحقیقاتی که پیرامون جرائم رایانه ای صورت گرفت در آمریکا بود که این تحقیقات به قضیه کلاهبرداری از طریق سوءاستفاده از ۵۶ هزار مورد بیمه به ارزش حدودا ۳۰ میلیون دلار اشاره کرد. مورد دیگر، قضیه «هراشتات» در آلمان مربوط به معاملات ارزی خارجی بود که به مبلغ ۲۰۰ تا ۳۰۰ هزار مارک از حساب ارزی بانک هراشتات خارج و همین امر موجب ورشکستگی این بانک و وارد شدن خسارت به مشتریان شد. در دهه ۱۹۸۰ که به‌عنوان نسل دوم جرائم رایانه ای محسوب می شود، جرائم رایانه ای فقط محدود به جرایم اقتصادی نبوده و دیگر زمینه ها را هم که جنبه اقتصادی نداشته شامل می‌شود مانند دست کاری کامپیوتر بیمارستان‌ها، جعل اسناد با استفاده از کامپیوتر و دست یافتن به اطلاعات خارجی محرمانه آمریکا، انگلستان و چند کشور دیگر و فروختن این اطلاعات به ک.گ.ب. در دهه ۱۹۹۰ که به شبکه جهانی (اینترنت) فراگیر شد سبب شد جرائم رایانه ای از جنبه اقتصادی وسیع‌تر شده و ابعاد جدیدتری به خود گیرد.[۲]

---

[۱] آریا، ناصر،(۱۳۷۲)، «فرهنگ اصطلاحات کامپیوتر و شبکه‌های کامپیوتری»، انتشارات مرکز تحقیقات تخصصی حسابداری و حسابرسی، تهران. ص۱۱۴

[۲] ولیدی، محمد صالح، حقوق جزای اختصاصی، جلد ۲، ص۱۲۵

جرایم جدید مانند ورود کرم اینترنتی برای نخستین بار توسط یک دانشجوی آمریکایی ساخته شده بود و موجب شد تا سیستم کامپیوتری حدود شش هزار و۲۰۰ کاربر اینترنت شامل دانشگاه‌ها، سرویس‌های نظامی و سایت های بیمارستان ها را مختل کند و هزینه تعمیرات سیستم‌ها حدودا مبلغ ۹۸ میلیون دلار بود که بعد از مدتی این دانشجو دستگیر و پس از محاکمه، محکوم به پرداخت همه مبالغ فوق شد.[۱] از زمان ابداع اینترنت تا زمانی که استفاده از اینترنت شکل عمومی پیدا کرد، تصور از پیش تعیین شده ای درباره این امکان ارتباطاتی و اتفاقاتی که در آن می افتد وجود نداشته است.بسیاری از اتفاقات افتاده است و سپس کسانی به دنبال تبیین و در مواردی برخورد یا جلوگیری از آن برآمده اند.اینترنت در سال ۱۹۶۴ توسط محققی به نام پائول باران[۲] در شرکت راند [۳] ابداع شد. وی به دنبال روشی برای مطمئن سازی ارتباط پنتاگون (وزارت دفاع ایالت متحده آمریکا) با اعضای ارتش در هنگام حمله واقعی اتمی بود و یک شبکه ارتباطات رایانه ای غیر متمرکز را پیشنهاد کرد که در آن رایانه مرکزی وجود نداشت.در چنین شبکه ای که اینترنت شبکه آرپانت[۴] نام داشت حتی در صورت انهدام و خراب یک یا چند رایانه، همچنان امکان تبادل اطلاعات بین سایر رایانه های باقی مانده وجود خواهد داشت.در اوایل دهه ۷۰ میلادی محققان دریافتند که اینترنت علاوه بر روشی برای برقراری ارتباطات بین قسمت های مختلف ارتش، روش کم هزینه ای برای برقراری ارتباطات بین اشخاص و سازمان هاست.[۵]در واقع انگیزه بنیادین شکل گیری اینترنت حصول اطمینان از امکان برقراری ارتباطات پیوسته است.[۶]. گفته می شود هدف اصلی از انجام پروژه آرپانت، افزایش امنیت اطلاعات محرمانه و نظامی این کشور(آمریکا) در مقابل مخاطرات ناشی از حملات هسته ای روسیه بود.[۷] تاریخچه مشخصی از پیدایش جرم اینترنتی و کامپیوتری زمان وجود ندارد ولی به هرحال این دسته از جرائم را باید زائیده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست.براساس مطالعات صورت گرفته منشاء پیدایش جرم کامپیوتری و اینترنتی به قضیه

---

[۱] مرشدی نیا، محمد رضا، رایانه و معضلات آن، چاپ اول، تهران، ص۱۲۵

[۲]. PAUL BARAN

[۳]. RAND

[۴]. ARPANET

[۵]. تاریخچه اینترنت، تکنولوژی و اطلاعات، شهریور ۸۵

[۶]. تاریخچه پیدایش اینترنت، وب سایت مدرسه رشد... ۲۰۰۶

[۷]. مروری بر تاریخچه و روند شکل گیری جرایم رایانه ای، روزنامه دنیای اقتصاد، ۲۲ ابان ۱۳۸۱

رویس برمی گردد؛ او که بعد از بی مهری مسئولان یک شرکت فروش عمده میوه و سبزی، به عنوان حسابدار آنها انتخاب می شود از طریق کامپیوتر اقدام به حسابرسی کرده و با تغییر قیمت ها و تنظیم درآمد جنس، مبلغی از مرجع آن را کاهش و به جای خاص واریز می می کند. 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.[۱] براساس اطلاعات موجود 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.براساس آمارهای موجود در سال ۱۳۸۴، ۵۳ مورد پرونده مربوط به جرایم اینترنتی در کشورتشکیل شد که کشف جرائم آمار ۵۰ درصدی را نشان می دهد.از مهمترین موارد جرم اینترنتی و رایانه ای در سال گذشته، ۳۲ مورد سوء استفاده از کارت های اعتباری ۱۱ مورد کلاهبرداری اینترنتی، ۷ مورد ایجاد مزاحمت از طریق اینترنت، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوعات متفرقه بوده است.باتوجه به آمارهای سال ۸۴ میزان کشفیات مربوط به کلاهبرداری، جعل و سایر جرائم رایانه ای و اینترنتی ۱۱ درصد رشد را نشان می دهد[۲].

[۱]. خداقلی – زهرا – جرایم کامپیوتری، تهران – انتشارات آریان – چاپ اول ۱۳۸۳،ص۴۷

[۲]. شیرزاد، کامران؛ جرایم رایانه-ای، تهران، نشر بهینه فراگیر، ۱۳۸۸، چاپ اول،ص۲۳

بخش چهارم: ویژگی های جرایم کامپیوتری

جرایمی که توسط کامپیوتر یا شبکه و یا علیه آنها انجام می شود از ویژگی های متمایزی نسبت به جرایم کلاسیک دارند.چرا که ماهیت این گونه جرایم به دلیل تکنولوژی پیچیده و بالا،خصوصیات منحصر به فردی داشته که می توان به شیوه ارتکاب آسان، خسارات و ضررهای هنگفت با حداقل منابع و هزینه، عدم حضور فیزیکی در محل ارتکاب جرم،عدم شناسایی جرایم در برخی موارد،خصوصیت فراملی بودن و وسعت دامنه جرم را نام برد.

الف–خصوصیات مرتکبین جرایم کامپیوتری معمولا مرتکبین جرایم کامپیوتری در دو دسته از هم قابل تمایز هستند.مرتکبین اتفاقی و مجرمین واقعی.دسته اول معمولا شامل جوانانی می شوندکه به انگیزهٔ بازی و تفنن مرتکب جرایم رایانه ای می شوند.ارتکاب این جرایم از آنجایی که منعکس کننده معایب سیستم ها و نحوهٔ نفوذ پذیری به شبکه و سیستم های کامپیوتری است لذا اتخاذ تدابیر پیشگیرانهٔ امنیتی مفید است.جرایم خطرناک و جدی که موجب خسارات مالی هنگفت می گردد از سوی مرتکبینی که دارای تخصص فنی یا تحصیلات دانشگاهی هستند وقوع می یابند که این دسته از مجرمین را باید جدی گرفت.در یک سری از جرایم کامپیوتری انگیزه اصلی کسب منفعت مالی است و لیکن انگیزه های دیگری چون انتقام جویی شغلی،سرگرمی،اثبات برتری قدرت،خودنمایی، چالش و... وجود دارد.لذا یکی از وجوه تمایز مرتکبین جرایم کامپیوتری از یکدیگر نوع انگیزه آنان می باشد.بر این اساس سه گروه از مجرمین از یکدیگر شناخته شده اند.مزاحمان کامپیوتری،خلافکاران،خرابکاران.انگیزه گروه اول صرفا دستیابی به سیستم های کامپیوتری و اطلاعات موجود در آن می باشد و اکثراً نوجوانانی هستند که برای تفریح و سرگرمی و ارضای حس برتری جوئی است که دست به این اقدامات می زنند.انگیزه دسته دوم یعنی خلافکاران کسب منفعت مالی است و عمدتاً در دو مقوله ی جاسوسی و کلاهبرداری فعالیت دارند که روز به روز بر تعداد اینها در جهان افزوده می شود.و انگیزه گروه سوم تنها صدمه زدن و ایراد خسارات به دیگران است که نه به قصد کسب منفعت و نه سرگرمی و تفریح می باشند.بلکه افرادی هستند که دارای اختلالات روانی بوده ویا قصد انتقام جویی دارند.این گروه در اجتماع و در اذهان عمومی مردم

جایگاه چندان نامطلوبی ندارند و از مقبولیت بیشتری برخوردارند و چه بسا به عنوان یک قهرمان و یا بزرگترین بزهکاری کامپیوتری سال در تمام دنیا مشهور شده و نامشان زبانزد عام می شود.[1]

ب: ملموس نبودن جرایم کامپیوتری و عدم تخمین میزان جرایم ارتکابی با افزایش و بکار گیری کامپیوتر در تمام عرصه های زندگی و همچنین سهولت استفاده از آن و گسترش شبکه جهانی اینترنت امروزه جرایم کامپیوتری می تواند به وسیله هر کسی در هر نقطه ای از دنیا به وقوع بپیوندد.ملموس نبودن جرایم کامپیوتری مبتنی بر چند عامل می باشد.اول آنکه تکنولوژی پیشرفته یعنی ظرفیت حافظه ی فشرده کامپیوتر و سرعت بالای عملیات موجب کشف دشوار جرایم کامپیوتری است.دوم آنکه به دلیل عدم وجود سابقه و شناخت در خصوص جرایم کامپیوتری بزه دیدگان و مامورین اجرای قانون پس از مدتی متوجه وقوع جرم می شوند و دسته آخر اینکه بسیاری از بزه دیدگان توان تشخیص،پیشگیری و مقابله با حوادث مربوط به اینگونه جرایم را ندارند.از طرف دیگر مرتکبین زبده،غالبا از خود مدرکی به جای نمی گذارند. چون اطلاعات نسخه برداری می شوند بدون آنکه از محل خود برداشته شود و سوابق عمل هم قابل پاک شدن است.بخش جرایم کامپیوتری سازمان اطلاعات آمریکاFBIتخمین زده که بین ۸۵ تا ۹۵ درصد جرایم کامپیوتری حتی کشف نمی شوند.[2]

ج-فراملی و بین المللی بودن جرایم کامپیوتری و الکترونیکی جرایم کامپیوتری به دلیل ماهیت و تکنولوژی خاص،اختصاص به محیط فیزیکی معین و محدودی ندارد و به راحتی در مقیاس بین المللی قابل تحقق می باشد.مسافت،زمان و مکان مانعی برای آن به حساب نمی آید.حضور فیزیکی شخص در محل حادثه معنایی ندارد.با کمک کامپیوتر و از طریق اینترنت سرقت از یک بانک یا دستیابی به اطلاعات محرمانه نظامی در ظرف چند ثانیه امری بعید و دور از دسترس نمی باشد.از طریق دسترسی به سیستم کامپیوتری در کشور و یا در کل کشورهای دنیا،این امکان را به کاربر غیر مجاز اینترنت می دهد که به راحتی به بانک های اطلاعاتی مستقر در قاره ای دیگر دسترسی پیدا کند.با توجه به گسترش روز افزون جرایم کامپیوتری و بدون مرز شدن جرایم جدید تر جرایم سایبر،عدم حضور فیزیکی مجرم در

[1] شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۸۹،ص۶۸

[2] فضلی، مهدی، مسوولیت کیفری در فضای سایبر، انتشارات خرسندی، چاپ اول، تهران ۱۳۸۹،ص۸۷

محل،سرعت بالا و زمان اندک ارتکاب جرم،لزوم هر چه سریعتر تعاون بین المللی را برای دستیابی به یک سیاست کیفری هماهنگ را ایجاب می کند[۱].

د–حجم و وسعت ضرر و خسارت وارده از طریق جرایم کامپیوتری به وسیله تکتولوژی کامپیوتر،مرتکبین با کمترین سرمایه و هزینه می توانند با ورود به شبکه اطلاعاتی و نفوذ در آن خسارات هنگفتی وارد نمایند.سهولت ارتکاب با حجم زیاد موضوعات مطروحه،سرعت عملکرد کامپیوتر،عدم نیاز به تخصص خاص یا بالا عدم نیاز به حضور فیزیکی مرتکب در محل و... همگی موجب گردیده تا حجم صدمات و خسارات وارده افزون گشته و گاه به چندین هزار برابر جرایم معمولی برسد.وسعت خسارات وارده ناشی از یک نفوذ غیر قانونی یا گسترش ویروس در اینترنت می تواند در کسر ثانیه صدها هزار استفاده کننده در سراسر جهان را متحمل خسارت نماید.به عنوان نمونه کوچک از جرایم کامپیوتری که منجر به خسارت فراوانی گردیده،می توان به ویروس ملیسا در سال ۱۹۹۹ میلادی اشاره کرد که این ویروس با ایجاد اختلال در سیستمهای پست الکترونیکی [۲]در سراسر جهان موجب بروز میلیونها دلار خسارت گردیده.خالق این ویروس ادعا نموده که ویروس را روی کامپیوتر شخصی خود تولید کرده بود و برای ورود به سایت American on line فقط از یک نام و رمز عبور به سرقت رفته استفاده کرده است .با این وجود عواقب جرایم کامپیوتری علاوه بر خسارات سنگین می تواند تهدیدی جدی برای امنیت بشر باشد.وابستگی امور حساس کشورها در زمینه های پزشکی،مخابراتی،هواپیمایی،و... به عملکرد کامپیوتر باعث می شود تا کوچکترین اختلال و خدشه در کار این سیستم ها عواقب وخیم و جبران ناپذیری را به دنبال داشته باشد.[۳]

ه–نحوه تعقیب و رسیدگی به جرایم کامپیوتری و اینترنتی نوین بودن جرایم کامپوتری و اینترنتی و شیوه ی ارتکاب اینگونه جرایم،نحوه رسیدگی و تعقیب را از جهت مسائل آیین دادرسی با چالش هایی روبرو کرده است.به طوری که تدابیر کلاسیک حقوقی به هیچ عنوان پاسخگو نبوده و با مشکلات عدیده ای در

---

[۱] همان،ص۴۷

[۲] E-mail

[۳] عمیدی، مهدی، مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز، ص ۶۵

این زمینه روبرو می باشد.نوع تحقیق،بازرسی محل،و وقوع جرم،توقیف اسباب و آلت جرم با جرایم کلاسیک متفاوت بوده و بدون تخصص و مهارت کافی مقامات قضایی کشف جرم میسر نیست.تخصص نداشتن مامور تحقیقاتی از محیط کامپیوتری و جرایمی که از سوی کاربران سایر کشورها بوقوع می پیوندد،محل وقوع جرم را از دایره تحقیقات و کشف به دور و بسیار دشوار و غیر قابل دسترس می کند.و یا تحقیقات از شبکه ای یا بانک اطلاعاتی گاهی باعث تجاوز به حاکمیت کشوری و یا تجاوز به شبکه و یا بانک اطلاعات مادر می شود که اطلاعات در آن ذخیره کرده اند.در واقع جایگزین شدن موضوعات غیر ملموس و مجازی به عوض ادله ی مثبت ملموس و عینی در عرصه ی تکنولوژی اطلاعات،مسائل حقوقی نوینی را مطرح ساخته و از خصوصیات بارز جرایم کامپیوتری و اینترنتی می باشد[۱].

بخش پنجم: پیشگیری اجتماعی از جرایم و انحراف های سایبری

از جمله مهم‌ترین آن‌ها شناسایی هویت و خصوصیات مجرمان و منحرفان سایبری بر اساس انگیزه‌های هر یک و همچنین، شناسایی هویت و خصوصیات بزه دیدگان سایبر ارزیابی خطرپذیری [۲]آن‌ها برای جهت‌دهی نوع و میزان آموزش‌های پیشگیرانه است. سپس با توجه به نتایج به‌دست آمده، می‌توان بر اساس الگوهای کلی پیشگیری از جرم، راهکارهای قابل اجرا و مؤثری را پیشنهاد داد. با این حال، این مباحث به مجال دیگری موکول می‌گردد.[۳]

بند اول: پیشگیری اجتماعی جامعه مدار سایبری

به‌طور کلی، با کدهای رفتاری می‌توان گروه‌های خاصی را که وظیفه‌ای به آن‌ها سپرده شده، در مقابل اعمال خود پاسخگو نگه داشت. از جمله آن‌ها، گروه‌های مشاغل هستند که در حوزه‌های مختلف به فعالیت می‌پردازند و چون که به متصدیان شبکه‌ای خود، داده‌های واجد ارزشی را واگذار کرده‌اند تا با رعایت سه اصل محرمانه بودن[۴]، تمامیت [۵]و دسترس‌پذیری[۱] در فضای سایبر منتشر کنند، ضروری است

---

[۱] همان،ص۶۶

[۲] Risk Assessment

[۳] –طارمی، محمد حسین، گذری بر جرایم رایانه‌ای ۱۳۸۷، ص ۸۸

[۴] Confidentiality

[۵] Integrity

متناسب با حرفه، نوع و میزان اطلاعات آن‌ها و دیگر شرایط،کد رفتاری مربوط را برای آن‌ها تدوین کنند. شایان ذکر است، در این مورد تاکنون برای بعضی مشاغل و موضوعات حساس، از سوی مراجعه مهم و معتبر بین‌المللی، کدهای رفتاری نمونه‌ای منتشر شده است. برای مثال، به‌تازگی برای فعالان عرصه تجارت الکترونیکی و بازاریابی شبکه‌ای[۲]،کدهای رفتار یکسانی تدوین شده تا از وقوع جرم و تخلف‌های مرتبط با پیام‌های تجاری ناخواسته الکترونیکی اجلوگیری شود.[۳] اما گروه دیگری که کدهای رفتاری برای آن‌ها از جمله ضروریات شغلی است، ارائه دهندگان خدمات شبکه‌های اطلاع‌رسانی رایانه‌ای هستند. آن‌ها در حقیقت پل ارتباطی میان دنیای فیزیکی با فضای سایبر محسوب می‌شوند و نسبت به بقیه دست‌اندرکاران این حوزه، افزون بر این‌که توانایی اقدامات بسیار متنوع و گسترده‌ای را دارند، مسئولیت-های خطیری نیز بر دوش آن‌ها گذاشته شده است. این افراد به‌راحتی می‌توانند امکان نفوذ به پایگاه‌ها را فراهم کنند یا اطلاعات حساس و کلیدی راجع به آن‌ها را در اختیار افراد ناصالح قرار دهند[۴]. به دلیل وجود چنین شرایطی، چندی است بر نحوه عملکرد ارائه دهندگان خدمات شبکه‌ای نظارت بیشتری صورت می‌گیرد که از جمله مهم‌ترین آن‌ها اقدامات انجام شده در جهت نظارت بر حفظ حریم آن‌لاین افراد از سوی این ارائه دهندگان خدمات است۰ آن‌ها به‌راحتی می‌توانند علاوه بر امکان‌پذیری ساختن شنود و ردیابی ارتباطات الکترونیکی، دسترسی به پایگاه‌های داده‌ای که ورود افراد غیرمجاز به آن‌ها ممنوع است یا اطلاعات شخصی و شخصی حساسی را که خود آن‌ها برای پیشبرد فعالیت‌های شبکه‌ای جمع‌آوری کرده‌اند میسر سازند.[۵]

---

[۱] Availability

[۲] Network Marketing

[۳] عمیدی، مهدی، مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز، ۱۳۸۷

[۴] همان،ص۸۷

[۵] شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۸۹،ص۱۰۲

بند دوم: پیشگیری اجتماعی رشدمدار سایبری

به نظر نمی‌رسد کسی در این واقعیت تردید داشته باشد که نه تنها نسل جوان و نوجوان جامعه ما، بلکه بدون استثنا در تمامی جوامع، توانسته است تعامل بهتری را با فضای سایبر برقرار کند. البته چندان جای شگفتی نیست، زیرا نسل گذشته امور خود را در دنیای فیزیکی به پیش می‌برده و شاید لزومی ندیده با این فضای جدید انس بگیرد، در حالی که نسل جدید با این فضا رشد یافته و از همان ابتدا هر آن‌چه پیرامون خود مشاهده کرده، رنگ و بوی سایبری داشته است.[۱] به هر حال، این وضعیت بیم و امیدهایی را برانگیخته است. از یک سو، می‌توان امیدوار بود نسل جدید در برپایی هرچه سریع‌تر یک جامعه اطلاعاتی[۲] تمام عیار، مبتنی بر اصول و قواعد حاکم بر این فضا، همت لازم را داشته باشد. اما از سوی دیگر، باید آن‌ها را از خطرات و آسیب‌های فراوان این فضا مطلع کرد تا با گرفتاری در آن‌ها، نتیجه عکس حاصل نشود.

نتیجه گیری

در جمع بندی و نتیجه گیری پایانی این مقاله فهمیدیم جرایم سایبری به اعمال مجرمانه ای گفته می شود که با استفاده از ابزارهای دیجیتال و شبکه ای انجام می گیرد. برخورد با این جرایم بر اساس قانون جرایم رایانه ای، قانون مجازات اسلامی و سایر مقررات کیفری انجام می شود. برای هر جرم، مجازات سایبری به صورت مشخص تعیین شده و شامل حبس، جزای نقدی یا اقدامات تکمیلی است. جلوگیری از جرایم کامپیوتری ذر نظام امنیتی از لحاظ شغلی،اداری و جامعه ای امری مهم بوده و بستگی به کارایی و امنیت تکنولوژی مدرن اطلاعات دارد و جلوگیری از جرم رایانه ای توسط حقوق کیفری اداری و مدنی بایستی مقدم شمرده شود.به هر حال یک استراتژی جامع امنیت داده پردازی و کنترل جرم،راه حل قانونی بایستی توسط ابزارهایی همچن تدابیر امنیتی اختیاری کاربران رایانه ای بکار گرفته شود.ضمن اینکه اجرای تدابیر امنیتی و جلوگیری از جرایم باید به توسعه تکنولوژی همگام باشد.

---

[۱] همان،ص۱۰۳

[۲] Information Society

همچنین باید توجه داشت ماهیت جرم سایبری با جرایم سنتی تفاوت دارد، چرا که در فضای غیرمادی و اغلب ناشناس انجام می شود. این ویژگی موجب می شود که شناسایی مرتکب و اثبات جرم با چالش های بیشتری همراه باشد. فضای مجازی، مرزهای جغرافیایی را درنوردیده و بستر ارتکاب جرم را از سطح محلی به سطح جهانی گسترش داده است. همین موضوع سبب پیچیدگی در پیگیری و اثبات این جرایم شده است. مجازات جرایم سایبری در نظام حقوقی ایران بر اساس نوع جرم، شدت آن و قوانین حاکم متفاوت تعیین می شود. قانون گذار با توجه به تنوع جرایم در فضای مجازی، مجازات هایی از قبیل حبس، جزای نقدی و محرومیت های اجتماعی را برای مرتکبان در نظر گرفته است. این مجازات ها با هدف بازدارندگی، حفظ نظم عمومی و حمایت از حقوق شهروندان تعیین شده اند. در برخی موارد نیز بسته به آثار جرم، مجازات تشدید می شود. مبنای اصلی تعیین مجازات در حوزه فضای مجازی، قانون جرایم رایانه ای مصوب ۱۳۸۸ است که برای هر جرم، میزان دقیق حبس یا جریمه نقدی را مشخص کرده است. به عنوان نمونه، دسترسی غیرمجاز به داده ها تا یک سال حبس و جزای نقدی دارد، و انتشار محتوای مجرمانه ممکن است تا دو سال حبس به دنبال داشته باشد. برخی مواد این قانون نیز به امکان ضبط تجهیزات، محرومیت از خدمات اینترنتی یا توقیف حساب های مرتبط اشاره دارند. مجازات ها با توجه به نیت مرتکب و خسارت وارده قابل تعدیل هستند. باید توجه داشت در مواردی که جرم سایبری همراه با توهین، تهدید، افشای اسرار یا کلاهبرداری باشد، مواد مربوطه در قانون مجازات اسلامی نیز قابل اعمال است. این قانون مجازات هایی از قبیل شلاق، حبس بلندمدت یا جزای نقدی بیشتر را برای جرایم عمومی پیش بینی کرده است. همچنین در صورت ارتکاب جرم علیه امنیت ملی یا منافع عمومی، مجازات می تواند شدیدتر باشد. بنابراین، مجازات جرایم سایبری تنها محدود به یک قانون نیست و گاهی ترکیبی از قوانین برای صدور حکم به کار می رود.

منابع و مآخذ

قرآن کریم و بعد

الف-کتب

۱. بابازاده، قاسم. \"پیرامون کنوانسیون اروپائی جرائم کامپیوتری\" خبرنامه انفورماتیک، شورای عالی انفورماتیک شماره ۸۱ فروردین ۸۱، ص ۳۸.

۲. باستانی، برومند، \"جرائم کامپیوتری و اینترنتی\"، چاپ بهنامی، سال ۱۳۸۳ ص ۲۷

۳. پیمانی – دکتر ضیاء الدین : حقوق کیفری اختصاصی جرایم علیه امنیت و آسایش عمومی نشر میزان – چاپ سوم، ۱۳۷۷

۴. جعفری، محمدتقی. (۱۴۱۹ق) رسائل فقهی، تهران: مؤسسه منشورات کرامت، چاپ اول.

۵. حبیب زاده – محمد جعفر : ترجمه کلاهبرداری در حقوق تطبیقی مجلهٔ قضایی و حقوقی دادگستری – زمستان ۱۳۷۵

۶. خداقلی – زهرا – جرایم کامپیوتری، تهران – انتشارات آریان – چاپ اول ۱۳۸۳

۷. خرم آبادی – عبدالصمد – کلاهبرداری رایانه ای از دیدگاه بین المللی دانشگاه تهران سال ۳۷ شمارهٔ ۲ ۱۳۸۶

۸. دزیانی، محمد حسن، \"ابعاد جزائی کاربرد کامپیوتر و جرائم کامپیوتری\"، خبرنامه انفورماتیک شورای عالی انفورماتیک کشور، شماره ۵۸، دی و اسفند ۱۳۷۳، صص ۱۵۸-۱۵۷.

۹. ر.ک: حسینعلی بای و بابک پور قهرمانی، بررسی فقهی حقوقی جرائم رایانه ای، ص ۳۸ و جرائم رایانه‌ای در ایران

۱۰. زراعت – عباس : شرح قانون مجازات اسلامی – نشر فیض، چاپ دوم : بی تا – جلد دوم

۱۱. زندی، محمدرضا، تحقیقات مقدماتی در جرائم سایبری، تهران، انتشارات جنگل، ۱۳۸۹، چاپ اول،۵۰

۱۲. سلمان زاده، محمود، «جنگ اطلاعات و امنیت» خبرنامه انفورماتیک، سازمان برنامه و بودجه کشور، شمارهٔ ۸۰ آذرودی ۱۳۸۰، ص ۲۰.

۱۳. شاملو احمدی : محمد حسین، فرهنگ اصطلاحات و عناوین جزایی، نشر دادیار ۱۳۸۰

۱۴. گارو: استاد مطالعات نظری و عملی در حقوق جزا ترجمه دکتر ضیاء الدین نقابت جلد سوم

۱۵. گلروزیان – ایرج : حقوق جزای اختصاصی – تهران – انتشارات جهاد دانشگاهی – ۱۳۶۸

۱۶. محمد نژاد، پرویز – شناخت جرم کلاهبرداری – ماهنامه اصطلاح و تربیت سال هفتم شماره ۷۳– اردیبهشت ۸۷

۱۷. مروری بر تاریخچه و روند شکل گیری جرایم رایانه ای، روزنامه دنیای اقتصاد، ۲۲ ابان ۱۳۸۱

۱۸. مشیر – سید مرتضی : کلاهبرداری در حقوق جزای ایران – مجله کانون وکلا – شماره ۱۰۳ – ۱۳۴۵

۱۹. میرمحمد صادقی – حسین : جرایم علیه امنیت و آسایش عمومی – نشر میزان – چاپ دوم ۱۳۸۱

۲۰. میرمحمد صادقی – حسین : مروری بر حقوق جزای انگلستان (ترجمه و توضیحات) – تهران – نشر میزان –۱۳۷۳ شمسی

۲۱. میرمحمد صادقی – حسین : واژه نامهٔ حقوق جزایی – تهران – نشر میزان – چاپ دوم ۱۳۷۶

۲۲. وکیل، امیر ساعد، حمایت از مالکیت فکری در سازمان تجارت جهانی تجارت و حقوق ایـران، انتشارات مجد چاپ اول

۲۳. ولیدی – محمد صالح : حقوق جزای اختصاصی – تهران – انتشارات امیر کبیر – ۱۳۶۶

ب-منابع اینترنتی

http://www.judiciry.ir

http://www.persianlaw.tk

http://www.persianlaw.tk

ج-منابع عربی

۱. ابن‌ادریس، محمدبن‌منصور بن‌احمد. (۱۴۱۰ق) السرائر الحاوی لتحریر الفتاوی، قـم: دفتـر نشر اسلامی، چاپ دوم.

۲. ابن‌منظور، محمدبن‌مکرم. (۱۴۱۴ق) لسان‌العرب، بیروت: دارالفکر للطباعۀ و النّشر.

۳. بوشهری، جعفر. (۱۳۸۷) حقوق جزا: اصول و مسائل، تهران: شرکت سهامی انتشار، چـاپ دوم.

۴. جلالی فراهانی، امیرحسین، کنوانسیون جرایم سـایبر و پروتکـل الحـاقی آن (بـه همـراه گـزارش هـای تـوجیهی آآ)، معاونـت حقـوقی و توسـعه قضـایی قـوه قضـائیه، تهـران: نشرخرسندی، چاپ نخست، ۱۳۸۹

۵. جوهری، اسماعیل‌بن‌حمـاد. (۱۴۱۰ق) الصـحاح – تـاج اللغـۀ و صـحاح العربیّـه، بیـروت: دارالعلم للملائین، چاپ اول.

۶. حر عاملی، محمدبن حسن. (۱۳۹۲ق) وسائل‌الشیعه، تصحیح شیخ محمد رازی، تهران: مکتبهٔ اسلامیه، چاپ دوم.

۷. سلار دیلمی، حمزهٔ بن عبدالعزیز. (۱۴۰۴ق) المراسم العلویّه فی الاحکام النبویّه، تحقیق محمود بستانی، قم: منشورات حرمین، چاپ اول.

۸. شیخ مفید، محمدبن محمد نعمان. (۱۴۱۳ق) المقنعه، قم: کنگرهٔ جهانی هزارهٔ شیخ مفید، چاپ اول.

۹. طباطبایی کربلایی، علی بن محمدعلی. (بی‌تا) ریاض المسائل فی بیان الاحکام بالدلائل، قم: مؤسسهٔ آل البیت علیهم السلام، چاپ اول.

۱۰. طریحی، فخرالدین بن محمد. (۱۴۰۳ق) مجمع‌البحرین، بیروت: مؤسسه الوفاء.

۱۱. علامه حلی، حسن بن یوسف. (۱۴۲۰ه ق) تحریر الاحکام الشریعه علی مذهب الامامیه، مصحح ابراهیم بهادری، قم: مؤسسه امام صادق(ع)، چاپ اول.

۱۲. فاضل لنکرانی، محمد. (۱۳۸۶) جامع المسائل (فارسی)، قم: انتشارات امیر قلم، چاپ یازدهم.

۱۳. گسن، ریموند.(۱۳۷۰)جرم شناسی نظری، ترجمه مهدی کی نیا، انتشارات مجمع علمی و فرهنگی مجد.

۱۴. محبوبی، فرخ. (۱۳۸۱) دانش‌آموز نفوذگر، تهران: انتشارات ناقوس، چاپ اول.

۱۵. محقق حلی، جعفر بن حسن. (۱۴۰۸ق) شرایع الاسلام فی مسائل الحلال و الحرام، با تصحیح عبدالحسین محمدعلی بقال، قم: مؤسسه اسماعیلیان، چاپ دوم.

لوگو سازمان ها و نهادهای علمی، سیاسی و دولتی حامی معنوی

هفتمین همایش ملی پژوهش های علوم اسلامی و انسانی در عصر نوین