چکیده

زمینه: اطلاعات شخصی افراد مانند کالایی است که به‌گونه‌ای آسان در رایانه‌ها و دیگر وسایل ارتباطی از قبیل اینترنت و گوشی‌های همراه تبادل می‌شود. این‌گونه وسایل و ساختارها رفتار خصوصی افراد را تحت کنترل قرار داده و اطلاعات آن را در دسترس افراد فرصت طلب قرار داده است. این افراد فرصت طلب با استفاده از تکنولوژی برتر و وسایل کارآمدتر به اهداف پلیدشان دست پیدا می کنند که با ورود به اطلاعات خصوصی اشخاص منجر به وقوع جرایمی در محیط سایبر می‌گردد که در این نوشتار بطور مختصر وسایل جرم سایبری مورد ارزیابی و تجزیه تحلیل می گردد و در انتها به خصوصیات رفتاری این مجرمین پرداخته می‌شود.

واژگان کلیدی: *جرایم رایانه ای، جرایم فناوری اطلاعات، وسیله جرم سایبری، فضای سایبری.*

مقدمه

جرایم رایانه‌ای که به جرایم نسل سوم رایانه و اینترنت وابسته است در محیط مجازی یا همان *Cyber Space* قابل تحقق می‌باشد. از این رو رفتار مرتکبان جرم رایانه ای متفاوت از مرتکبان سنتی است. در این نوع از بزه مرتکبان ناشناس، در فضایی ناشناخته دست به اعمال خلاف می زنند. برخلاف جرم کلاسیک، جرم رایانه دارای تکنولوژی برتر و وسایل پیشرفته تری می باشد مرتکبین با استفاده از فناوری نوین و جدید به اهداف شوم خود دست پیدا می کنند بدون آنکه اثری همانند جرم کلاسیک به جا بگذارند. ویژگی دیگر این جرم نامعلوم و نامشخص بودن بزه‌دیدگان است چرا که افراد متعددی می‌توانند هدف شکار این مجرمان قرار بگیرند. بنابراین جرم رایانه ای نشان‌دهنده یک مجرمیت بدون بزه دیده‌ای مشخص است. پس رقم سیاه در این جرم بسیار بالاست. این موضوع نشان می‌دهد که این شکل از مجرمیت نیازمند هیچ دانش و فن خاصی نیست. این بزه هم‌اکنون جنبه فراملی و فراسرزمینی به خود گرفته است. فناوری های نوین در این عرصه وقوع جرایم جرم رایانه ای در محیط مجازی، مرتکبان را قادر ساخته است که فعالیت‌های خود را بدون داشتن ارتباطی خاص با یک محل معین و مشخص انجام دهند. پر واضح است که با وقوع این نوع از جرایم، خطر جدی برای جامعه بین‌المللی و جامعه داخلی یک کشور رقم می زند.

سوالات تحقیق:

۱- مجرمین جرایم رایانه ای چه افرادی می باشند؟
۲- وسایل ارتکاب جرم رایانه ای چه مواردی است؟
۳- خصوصیات رفتاری این دسته از مجرمان چیست؟

فرضیه تحقیق:

۱- مجرمین این جرم همانند جرایم کلاسیک هستند با این تفاوت که وسایل ارتکابی این جرم پیچیده و از علوم نوین روز استفاده شده، می باشد.

۲- وسایل این از فناوری های روز دنیا نشات گرفته است بنابراین این وسایل حصری نمیباشد با توجه به فنون و علوم جدید تغییر می‌کنند.

۳- مرتکبین این جرم افرادی باهوش و با تحصیلات می باشند که می توانند از این علوم روز دنیا استفاده نموده و به اهداف خود برسند.

بیان مسئله

مبحث اول: شناخت وسیله جرم سایبری

در حالت سنتی بزه دیده یا "مجنی علیه " که هدف جرم است انسان می باشد و در جرایم علیه اشخاص، تمامیت جهانی و معنوی فرد هدف ارتکاب جرم است. در جرایم علیه اموال جرم علیه مال متعلق به انسان است. شکل اولیه بزه دیده در جرایم سایبری رابطه انسان و ماشین بود. در کلاهبرداری کامپیوتری اولیه و کلاسیک، فرد مرتکب با دادن دستور العمل اضافی بدون این که آنان را بفریبد یا حتی دیده باشد وجوه دیگران را به خود اختصاص می داد. در شکل جدید و اخیر این شکل از بزه دیده به صورت ماشین-ماشین تغییر یافته است که بیشترین مورد تحقق آن در جرایم تجارت الکترونیکی و جرایم بانکداری الکترونیکی است.[۱] بنا به طبع این نوع جرایم که در بالا بیان شد، هم وسیله ارتکاب این جرایم متفاوت و مدرن است و هم مرتکبین آن ها اشخاص خاص و اکثرا ماهری هستند. ابزارهایی که در اینگونه جرایم به کار می رود انواع مختلفی دارد و آنگونه که پیداست، متنوع تر هم خواهند شد. از لحاظ مرتکبین هم این جرایم دارای خصیصه های خاصی هستند که ذیلا به بررسی آن ها می پردازیم.

---

[۱] عالی پور، حسن، حقوق کیفری فناوری اطلاعات، چ اول، تهران، نشر خرسندی سال ۱۳۹۰ ص ۸۹

گفتار اول: تعاریف و مفاهیم وسیله

وسیله هایی که برای ارتکاب جرایم رایانه ای به کار می روند در نوع خود خاص هستند. اصولا در ارتکاب بسیاری از جرایم وسیله نقش چندانی ندارد اما در برخی جرایم هم وسیله می تواند در تعیین مجازات نقش داشته باشد، برای مثال در قتل عمد وسیله باید کشنده باشد. در این قسمت به بررسی وسایل ارتکاب جرایم رایانه ای می پردازیم.

بند اول: رایانه

رایانه در واقع اولین ابزار لازم برای ارتکاب جرایم رایانه ای است. رایانه یا کامپیوتر دستگاهی است که برای پردازش اطلاعات تحت یک روال معین استفاده می شود. می توان به همه ماشین های مکانیکی محاسبه مانند خط کش محاسبه و یا چرتکه نیز به همان صورت که برای ماشین های امروزی به کار می رود[1]، رایانه گفت.

در بند و از ماده ۲ قانون تجارت الکترونیک سیستم رایانه ای چنین تعریف شده است: «سیستم رایانه‌ای» (*System :(Computer*) هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری- نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خود کار «داده‌پیام» عمل می‌کند». همین تعریف در ماده ۱ قانون جرایم رایانه ای هم آمده است. در ماده ۱ از کنوانسیون جرایم سایبر، سیستم رایانه ای چنین تعریف شده است: سیستم رایانه ای دستگاهی است که از نرم افزار و سخت افزاری که برای پردازش خودکار داده های دیجیتالی طراحی شده، تشکیل یافته و ممکن است شامل ورودی، خروجی و امکانات ذخیره‌ساز اطلاعات شود، سیستم رایانه ای می تواند به صورت مستقل یا متصل به شبکه ای از سایر دستگاه‌های مشابه عمل کند. منظور از خودکار این است که انسان دخالت مستقیم ندارد. منظور از پردازش داده‌ها این است که داده-های سیستم رایانه ای با اجرای یک برنامه رایانه ای عمل کند. یک برنامه رایانه ای مجموعه ای از دستورالعمل هاست که رایانه می تواند آن ها را برای نتیجه مورد نظر اجرا کند. رایانه می‌تواند

[1] شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی، ۱۳۷۹ ص ۷۶

برنامه های مختلفی را اجرا کند. معمولا سیستم رایانه ای از دستگاه های مختلفی تشکیل شده است که به پردازشگر یا واحد پردازش مرکزی وسایل جانبی تفکیک می شود.[۱]

بند دوم: اینترنت

شورای تحلیل شبکه دولت فدرال ایالات متحده امریکا در سال ۱۹۹۵، کلمه اینترنت را به شرح ذیل تعریف کرده است: اینترنت به یک نظام اطلاعاتی اطلاق می شود که اول، توسط فضای منحصر به فرد جهانی که مبتنی بر پروتکل اینترنت است، به گونه ای منطقی به هم پیوسته باشد، دوم، می تواند با استفاده از مجموعه پروتکل تی سی پی و آی پی از ارتباطات پشتیبانی کند و سوم، خدمات سطح برتری از ارتباطات و زیر ساخت های مربوط را به صورت خصوصی و عمومی تامین کند، به کار گیرد و قابل دسترس سازد.[۲] اینترنت یک موضوع فیزیکی یا ماهیت مادی نیست. اینرنت یک مجموعه فضای مجازی آکنده از اطلاعات است که واقعیات دنیای مادی آن را قابل درک می کند. ارتباط بین کاربر واقعی در اینترنت با کاربر یا یک سیستم دیگر برقرار می شود و در واقع فضای مشترک بین هزاران رایانه را فضای مجازی یا اینترنت می گویند.

همان‌گونه که تاکنون بحث شد، این فضا هم می تواند ابزاری باشد برای ارتکاب جرم و هم مکانی برای ارتکاب جرم. بنا به نظر صاحب نظران، اینترنت هیچ هیئت کنترل کننده ای ندارد زیرا بدون مکانیسم کنترل مرکزی طراحی شده است و فقط به وسیله تعداد بی شماری از رایانه ها و شبکه هایی که به آن متصل می شوند به وجود می آید.[۳] بعضی از عواملی که تعدد مکان جرم را موجب می شود عبارتند از: محل ارتکاب، محل وقوع نتیجه، محل وجود ادله، محل فرار مرتکب. در جرایم سایبری به واسطه زیر ساخت جهانی مکان ارتکاب جرم به تمام کره زمین توسعه یافته است. فردی که مطالب افترا آمیز در شبکه منتشر می کند در زمان بسیار کوتاه پیام خود را به منطقه وسیعی از زمین می رساند. یا کسی که ویروسی نوشته و منتشر می کند

---

[۱] جلالی فراهانی، امیر حسین، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، چ اول، تهران، خرسندی سال ۱۳۸۹ ص ۱۹

[۲] خرم آبادی، عبدالصمد، جرایم فناوری اطلاعات، پایان نامه مقطع دکتری، دانشگاه حقوق و علوم سیاسی دانشگاه تهران سال ۱۳۸۴ ص ۵

[3] *Bowrey, Kathy, Law and Internet Cultures, Cambridge, Cambridge University Press, 2005, p. 12*

چندین کامپیوتر را در کشورهای مختلف آلوده می کند. با این اوصاف، اینترنت یکی از ابزارهای خطرناک ارتکاب جرم است که هر کاربری در آن ممکن است قربانی قرار گیرد. به واسطه فقدان نظارت در این فضا، مکان مناسب تری برای ارتکاب برخی جرایم سنتی به وجود آمده است و از سوی دیگر تمامیت این فضا و کاربران هم در معرض خطر وقوع جرم هستند. حال که در دو قسمت گذشته با مفهوم رایانه و اینترنت به عنوان ابزار جرم آشنا شدیم، توضیحی پیرامون جرم رایانه ای و جرم اینترنتی ضروری است. جرم اینترنتی یا جرم شبکه ای جرمی است که در ارتباط با شبکه جهانی اینترنت و نه صرفا رایانه به وقوع می پیوندد و با توجه به مفهوم عام رایانه که در بالا توضیح داده شد، می توان گفت که جرم اینترنتی نوع خاصی از جرایم رایانه ای است.[۱]

بند سوم: شبکه

به مجموعه ای از دو یا چند سیستم رایانه ای متصل به یکدیگر شبکه رایانه ای گفته می شود.[۲] در یک شبکه منابع و امکانات سیستم های رایانه ای به اشتراک گذاشته می شود به این معنا که در یک شبکه کاربر هر یک از سیستم های رایانه ای می تواند از داده های ذخیره شده روی رایانه کاربر دیگر استفاده نماید.[۳]

شبکه ها انواع گوناگونی دارند که عبارتند از:

شبکه محلی*LAN Local Area Network*: اتصال یک سری از کامپیوترها در محدوده‌ی معینی مثل یک ساختمان، تشکیل یک شبکه *LAN* می‌دهند. به علت ارتباط مستقیم و فاصله کوتاه کامپیوترها از یکدیگر سرعت تبادل اطلاعات در این نوع شبکه ها بسیار است.

شبکه منطقه‌ای *MAN Metropolitan Area Network*: این شبکه از اتصال کامپیوترها در محدوده‌های وسیع‌تر از شبکه محلی است، مثلاً محدوده‌ی یک شهر. سرعت تبادل اطلاعات

---

[۱] جاوید نیا، جواد، جرایم تجارت الکترونیک، تهران، خرسندی، ۱۳۸۸، ص ۱۲۸

[۲] خرم آبادی، عبدالصمد، همان، ص ۷۳

[۳] جاوید نیا، جواد، همان، ص ۷۳

(سرعت ارتباطی) این گونه شبکه‌ها متوسط است. ارتباط این کامپیوترها معمولاً از طریق دستگاه ها و تجهیزات ویژه مخابراتی انجام می‌شود.

شبکه وسیع *WAN Wide Area Network*: در این شبکه‌ها اتصال کامپیوترها معمولاً از طریق ماهواره یا خطوط فیبر نوری برقرار می‌شود.

شبکه اینترنت: اینترنت بزرگترین شبکه کامپیوتری موجود در جهان است که از میلیون ها کامپیوتر شخصی، مسیریاب (*Router*) و تجهیزات مخابراتی تشکیل شده است. سابقه ایجاد اینترنت به سال ۱۹۸۶ باز می‌گردد. در این سال ارتش امریکا برای تبادل اطلاعات نظامی، شبکه‌ای به نام آرپانت بین مراکز نظامی ایجاد نمود که این پروژه با موفقیت انجام شد. شبکه اینترنت تا قبل از سال ۱۹۹۲ فقط دارای متن بود اما از این سال به بعد تصویر، صدا، موسیقی، فیلم های گوناگون، انیمیشن و غیره نیز به آن اضافه شد. این شبکه جهانی دارای کتابخانه بسیار بزرگی است که کتابخانه مجازی نامیده می‌شود. در این شبکه هر نوع اطلاعاتی به صورت یک کتاب در کتابخانه ذخیره می‌شود. کتاب های این کتابخانه برخی کوچک اند و برخی بزرگ، برخی پر از تصویرها و طرح های رنگارنگ و برخی فقط شامل متن هستند، این اطلاعات در رایانه‌های خدمات شبکه پراکنده‌اند.[۱]

شبکه اینترانت: اینترانت یک شبکه خصوصی و مبتنی بر پروتکل و قوانین شبکه اینترنت است که به صورت محدود و ویژه‌ای برای کاربردهای خاص ایجاد می‌شود و به شبکه اینترنت متصل نیست مانند شبکه ارتباطی آموزشگاه ها و مدارس کشور.[۲]

در کنوانسیون جرایم سایبر، شبکه تعریف نشده است.

بند چهارم: داده و اطلاعات

در قانون جرایم رایانه ای داده تعریف نشده است. کنوانسیون جرایم سایر داده را به داده رایانه ای و داده ترافیک تفکیک کرده است. در این کنوانسیون، منظور از داده رایانه‌ای »هر گونه

---

[1] *Encyclopedia of public International law, use of force, war and neutrality, peace treaties, North Holland publishing company Vol 3*

[۲] همان، ص ۷۴-۷۶

نمایش حقایق، اطلاعات یا مفاهیم به شکلی مناسب که برای پردازش در یک سیستم رایانه‌ای که شامل برنامه‌ای مناسب است و باعث می‌شود که این سیستم عملکرد خود را به مرحله اجرا گذارد، مورد استفاده قرار می‌گیرد[۱] و منظور از داده ترافیک (هر گونه داده رایانه‌ای است که مرتبط با ارتباط برقرار شده به وسیله سیستم رایانه‌ای است. این داده از سوی سیستم رایانه‌ای ای به وجود می‌آید که بخشی از زنجیره ارتباطی را تشکیل می‌دهد. این زنجیره شامل مبدأ، مقصد، مسیر، مدت، تاریخ، اندازه، دوام یا نوع خدمات اصلی ارائه شده است).[۲]

گفتار دوم: مرتکبین جرایم رایانه ای

این دسته از جرایم، بعضا از لحاظ مرتکبین هم با جرایم سنتی تفاوت دارند. همانطور که در قسمت مربوط به جرایم طبیعی و تصنعی بحث شد، ارتکاب این نوع جرایم مستلزم میزان خاصی از اطلاعات و دانش ها است که این امر دایره افراد قادر به ارتکاب این جرایم را محدود می کند.

بند اول: مجرم کیست؟

در نظام کیفری کلاسیک و قدیم تنها به جرم و مجازات توجه می‌شد و عامل وقوع جرم یعنی مجرم تا حدّ زیادی مورد شناسائی قرار نمی‌گرفت از این رو در این نظام فاعل جرم، انسان یا حیوان بود فرقی نمی‌کرد و کودکان نیز همچون افراد بالغ مسئول و قابل مجازات بودند.[۳] در بینش قانونگذار ما مفهوم بزهکار با مفهوم بزه پیوندی نزدیک دارد و چون برای تحقق جرم علاوه بر عنصر مادی محتاج به عنصر دیگری یعنی عنصر روانی است. برای تحقّق یک جرم وجود عنصر روانی لازم و ضروری است عنصر روانی یعنی اینکه فعل مجرمانه باید نتیجه اراده و خواست مجرم باشد و مجرم به نقض قوانین هم آگاه باشد (اراده+آگاهی) بنابراین برای ارتکاب جرم و بزهکار بودن باید پیش از همه از توانائی درک و اراده برخوردار باشد پس مرتکب جرم

---

[۱] جلالی فراهانی، امیر حسین، همان، ص ۲۱

[۲] همان، ص ۲۲

[۳] ولیدی، محمد صالح، بایسته‌های حقوق جزای عمومی، تهران، انتشارات خورشید، ۱۳۸۲، چاپ اول، ص ۲۷۵.

ممکن است شخص حقیقی یا حقوقی باشد. اگر نسبت انسان را با عنصر مادی جرم بسنجیم، بزهکار مسلماً کسی است که جرم را مادتاً مرتکب شده و یا به اجرای آن مبادرت ورزیده است و مجرم و بزهکار ممکن است به عنوان مباشر، شریک و یا معاون مرتکب جرم شود.[۱]

بند دوم: مجرمین رایانه ای

مرتکبین جرایم رایانه ای به دو دسته تقسیم می شوند؛ اول، مجرمانی که هزینه و فایده می کنند و به دنبال منافع خود مرتکب جرم می شوند و دوم، مجرمانی که صرفا برای ارضای حس کنجکاوی خود مرتکب جرم رایانه ای می گردند. دسته دوم عموما افراد متخصصی هستند که قصد خرابکاری ندارند.[۲] در یک تقسیم بندی دیگر، مجرمان رایانه ای به دو دسته مجاز و غیر مجاز تقسیم می گردند، مجرمینی که مجاز به دسترسی به یک رایانه یا شبکه هستند و از آن سوء استفاده می کنند و مجرمینی که به طور غیر مجاز به این ابزارها دست می یابند و از آن طریق مرتکب جرم می گردند.[۳] در ارتکاب جرایم رایانه ای عموما نظر بر آن است که این مجرمان چندان هم باهوش نیستند بدان معنا که برای تخریب سیستم های رایانه ای یا نفوذ و افشای اطلاعات اگر چه سطح خاصی از آگاهی ها و اطلاعات لازم است اما این به معنای تیز هوش بودن مجرمان این دسته جرایم نیست.[۴]

بند سوم: خصوصیات سازمانی

در تقسیم بندی مجرمین رایانه ای به مجاز و غیر مجاز دیدیم که برخی از این مجرمین، به طور غیر مجاز به یک سیستم یا شبکه دسترسی پیدا می کنند و از آن طریق مرتکب جرم می گردند. کارمند یک بانک یا یک شرکت حق استفاده و کارکردن با رایانه این موسسات را دارد در

---

[۱] همان، ص ۲۷۶

[۲] شیرزاد، کامران، جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، چ اول، تهران، نشر بهینه فراگیر،سال ۱۳۸۸ ص ۸۹

[۳] همان

[۴] خداقلی، زهرا، جرایم کامپیوتری، چ اول، تهران، انتشارات آریان سال ۱۳۸۳ ص ۳۲

حالی که یک مشتری چنین حقی ندارد. در بررسی خصایص سازمانی این دسته از مجرمان، باید به برخی جرایم سازمان یافته هم توجه کرد. برخی تروریست های رایانه ای، به صورت سازمانی عمل می کنند و اقدام به تخریب یا افشای اطلاعات یا سایر جرایم رایانه ای می کنند. خصیصه سازمان یافته این دسته از جرایم مثل ترورسیم رایانه ای، چندان تاثیری در اساس مسئله ندارد بلکه آن چه این دسته از جرایم را از هم متفاوت می کند، ماهیت این جرایم است. کسی که بدون سوء نیت مجرمانه به سیستم رایانه ای دسترسی پیدا کند با کارمند یک موسسه مالی که از حساب مشتیان وجوهی را برداشت می کند تفاوت بسیار دارد.[۱] کارمندان بی‌شماری روزانه اجازه دسترسی به سیستم های رایانه ای را دارند از جمله تحویلدارن بانک ها. در این دسته از کارمندان، بعضا سازمان مربوطه امکان دسترسی به پایانه ای اطلاعاتی زیادی را برای آنها فراهم کرده است. در حال حاضر کارمندان سازمان ها و ادارات بزرگترین دسته از مرتکبین جرایم رایانه ای به شمار می آیند.[۲] این کارمندان تمام اطلاعات لازم برای ورود به سیستم، ذخیره اطلاعات، تغییر داده ها و پردازش آن ها را در اختیار دارند لذا ارتکاب جرم برای این دسته بسیار راحت است. از سوی دیگر همین کارمندان بعد از اتمام خدمت یا اخراج از محل خدمت باز هم بسیاری از اطلاعات مهم در زمینه امنیت این سیستم ها را در اختیار دارند که آن ها را قادر به ورود و استفاده از این اطلاعات می کند.

بند پنجم: خصوصیات رفتاری

مرتکبین جرایم رایانه ای از خصوصیات و روحیات خاصی برخوردارند. بر طبق تحقیقاتی که انجام شده است مجرمین رایانه ای اکثرا درون گرا هستند.[۳] مجرمان رایانه ای اکثرا از طبقات تحصیل کرده هستند و نکته اینجاست که این دسته از افراد در ارتکاب سایر انواع جرایم اصلا موفق نیستند. از این جهات، تعقیب و دستگیری این مجرمان دشوارتر است.

---

[۱] شیرزاد، کامران، همان، ص ۹۰

[۲] شیرزاد، کامران، همان، ص ۹۴

[۳] همان، ص ۹۰

از سوی دیگر، علم کیفر شناسی اقتضا دارد که به خاطر موقعیت اجتماعی خاص این گونه مجرمان برخورد متفاوت و عموما ملایم تری با آن ها صورت گیرد. انگیزه این دسته از مجرمان هم عموما با انگیزه مجرمان جرایم عادی تفاوت دارد. عموم انگیزه این دسته از مجرمان چیزی غیر از سود و منفعت شخصی خودشان است. برخی از این مرتکبین در صدد نشان دادن مهارت خود هستند و برخی دیگر صرفا برای سرگرمی این کار را انجام می دهند. در برخی از این مرتکبان حتی انگیزه های بشر دوستانه هم وجود دارد. برخی دیگر از مرتکبین، اصولا با محدودیت مشکل دارند و نمی توانند با محدودیت دسترسی خود به برخی اطلاعات کنار بیایند. نکته دیگری که از لحاظ رفتار شناسی این مجرمین باید بدان توجه کرد این است که عموم این مجرمان جوان یا حتی نوجوان هستند.[1]

نتیجه‌گیری و پیشنهادها

در عصر نوین اطلاعات، نیاز جوامع انسانی به رایانه و اینترنت افزایش یافته است. این موضوع به افراد فرصت طلب و تبه کار اجازه می دهد تا مقاصد شوم خود را در فضای سایبری که به دلیل نامحدود بودن و احتمال کم ردگیری آنها، دنبال کنند. از همین رو حقوقدانان و جرم شناسان می بایست تمام تلاش خود را به کار بگیرند تا بتوانند با افزایش آگاهی در رابطه با مسائل حقوقی فضای سایبر به قانونگذاران کشورها و جوامع بین‌المللی کمک کرده تا به امنیت این دنیای مجازی کمک کنند. با افزایش فراگیر شدن استفاده از رایانه جرائم مربوط به آن نیز افزایش یافته است.

پیشنهادهای کاربردی:

۱) مطالعه جرم شناختی نظام مند در خصوص تجاوزات بالقوه کامپیوتری نسبت به حریم خصوصی که جرم انگاشته شوند یا عنوان مجرمانه بیابند.

---

[1] همان، ص ۹۲

۲) لازم و ضروری است که دولت ها با توجه به ویژگی ها و فرهنگ مردمانشان، برای ارتقای فرهنگ و سطح آگاهی های جامعه با استفاده از انواع وسایل ارتباطات جمعی و رسانه ای تلاش کنند.

۳) بررسی دقیق تر خصوصیات مجرمان رایانه ای که دستگیر شده اند تا بتوانیم خصوصیات این افراد را بهتر مورد بررسی و ارزیابی قرار دهیم.

۴) به دلیل ماهیت پیچیده فضای سایبر و نیاز به تخصص زیاد در رابطه با تصویب قوانین سایبری لازم است با کارشناسان خبره مشاوره شود تا قوانین هم سنگ و به فراخور نیازهای جامعه به تصویب برسند.

فهرست منابع

- جاویدنیا، جواد (۱۳۸۸)، جرایم تجارت الکترونیکی، چاپ دوم، تهران: انتشارات خرسندی.
- جلالی فراهانی، امیر حسین (۱۳۸۹)، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، چ اول، تهران: خرسندی.
- خداقلی، زهرا (۱۳۸۳)، جرایم کامپیوتری، چ اول، تهران، انتشارات آریان.
- خرم آبادی، عبدالصمد (۱۳۸۴)، جرایم فناوری اطلاعات، پایان نامه مقطع دکتری، دانشگاه حقوق و علوم سیاسی دانشگاه تهران.
- شریفی، مرسده (۱۳۷۹)، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی.
- شیرزاد، کامران (۱۳۸۸)، جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، چ اول، تهران، نشر بهینه فراگیر.
- عالی پور، حسن (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، چاپ اول، تهران: نشر خرسندی.
- ولیدی، محمد صالح (۱۳۸۲)، بایسته‌های حقوق جزای عمومی، تهران، انتشارات خورشید چاپ اول.

- Bowrey, Kathy(2005), Law and Internet Cultures, Cambridge, Cambridge University Press.
- Encyclopedia of public International law, use of force, war and neutrality, peace treaties, North Holland publishing company Vol.