۱۴۰۱/۱۲/۱۹ ۱۴۰۱/۰۷/۲۹
نمدید شد
سومین همایش ملی فقه، حقوق و علوم اسلامی
3RD NATIONAL CONFERENCE ON JURISPRUDENCE, LAW AND ISLAMIC SCIENCES

آنالیز حجم کلاهبرداری رایانه ای و بررسی روش های جلوگیری از آن

سیمین وطن خواه تربه بر

چکیده

کلاهبرداری رایانه ای از قدیمی ترین جرایم رایانه ای با ابعاد مالی است. با توجه به توسعه سریع تکنولوژی رایانه‌ای و تغییر عصر اطلاعات و گسترش ارتباطات شبکه ای و در عین حال آسانی در ارتکاب جرایم مرتبط با فناوری های نوین، بحث روز آمد شدن و لزوم تدوین قوانین بسیار مهم است. هر نوع کلاهبرداری ارتکاب یافته به وسیله رایانه، لزوما کلاهبرداری رایانه‌ای نامیده نمی شود، چرا که مجرمین از رایانه‌ها هم به عنوان وسیله ارتکاب کلاهبرداری کلاسیک و هم کلاهبرداری رایانه‌ای استفاده می‌کنند. جرم کلاهبرداری رایانه‌ای یکی از مهمترین جرائم رایانه‌ای است. این جرم نیز مانند جرم کلاهبرداری کلاسیک ازجمله جرائم علیه اموال و مالکیت محسوب می‌شود. هرچند تدابیر کلی در مقابله با انواع شیوه های کلاهبرداری تقریبا شبیه به هم است اما با تفاوت های موجود در شیوه های گوناگون کلاهبرداری استفاده از روش های مقابله متناسب ضرورت می یابد. در بیشتر کشورهای دنیا جرایم اینترنتی بعنوان یک معضل حاد و بسیار مهم تلقی می‌گردد و لذا دولتها به دنبال پیدا کردن راه حل‌های متفاوتی در جهت ریشه‌کن کردن و یا کم کردن یا حتی جلوگیری از جرایم ذکر شده می‌گردند.

واژه‌های کلیدی: اطلاعات و ارتباطات، کلاهبرداری رایانه ای، جرایم رایانه ای، جلوگیری از کلاهبرداری.

۱- مقدمه

به موازات گسترش فناوری های نوین اطلاعات و ارتباطات، بشر شاهد ظهور نسل جدیدی از جرایم می باشد که شناخت آن، مستلزم مطالعات جرم شناختی جدیدی است. با توسعه روابط افراد در فضای سایبر (مجازی) اغلب کشورها به منظور قاعده مند کردن روابط و اقدامات افراد در محیط مجازی به تدوین قوانینی در این زمینه مبادرت نموده اند. اگرچه نمی توان هیچ جامعه ای را بدون جرم تصور نمود. در مقابل، انسان نیز هیچ‌گاه نسبت به وقوع جرم بی تفاوت نبوده و در راستای مبارزه با آن در تلاش است. با این حال جهت مقابله با ارتکاب جرم در محیط مجازی نیازمند تدابیر و راهکارهای نوینی هستیم (صادقی، ۱۳۷۸).

کلاهبرداری رایانه‌ای یکی از جرائم ناشی از سوءاستفاده از فناوری اطلاعات است. فناوری اطلاعات پدیده منحصر به فرد عصر حاضر است که موجب پیشرفت و تغییر و تحول عظیم و عمیقی در تمام ابعاد و شئون زندگی انسان شده است. این پدیده با طرح مسائل جدید بسیاری از علوم را با چالش‌های جدی مواجه ساخته و آنها را تحت تاثیرقرار داده است. علم حقوق نیز به عنوان شاخه‌ای از علوم اجتماعی که تنظیم وتنسیق روابط انسانها را درچارچوب حیات جمعی برعهده دارد، عمیقا تحت تاثیر فناوری اطلاعات قرار گرفته است. در این راستا حقوق جزا بیشتر از سایر شاخه‌های حقوق تاثیر پذیرفته، چرا که این پدیده نه تنها امکان ارتکاب رفتارهای مجرمانه جدیدی را به وجود آورده که قبل از این به هیچ وجه امکان پذیر نبوده، بلکه با خلق

دنیای جدیدی به نام فضای سایبر[1] ارتکاب بسیاری از رفتارهای مجرمانه مرسوم را تسهیل نموده است.کلاهبرداری رایانه‌ای از جمله جرائمی است که با پیدایش فناوری اطلاعات وارد عرصه حقوق جزای اختصاصی شده و اصول وقواعد حاکم برکلاهبرداری سنتنی را به چالش کشیده است. کلاهبرداری رایانه‌ای ازجهت اسمی ونتیجه حاصل از جرم با کلاهبرداری کلاسیک شباهت دارد، اما تفاوت آنها از جهت فرایند ارتکاب وعناصراختصاصی تشکیل دهنده جرم باعث شده است که کلاهبرداری رایانه‌ای به‌عنوان جرمی مستقل از کلاهبرداری کلاسیک مطرح شود. خاطرنشان می‌شود که هرگونه ارتکاب کلاهبرداری به‌وسیله رایانه کلاهبرداری رایانه‌ای محسوب نمی‌شود (ابراهیمی، ۱۳۹۱).

رایانه از دوجهت در ارتکاب کلاهبرداری دخیل است:

۱- استفاده از رایانه برای ارتکاب کلاهبرداری کلاسیک، به این صورت که مرتکب از طریق رایانه، متوسل به وسایل متقلبانه گردیده و دیگری را فریب می‌دهد و مال او را می‌برد. در این صورت چون رایانه صرفا به عنوان وسیله ارتکاب جرم مورد استفاده قرار می‌گیرد و نوع وسیله در تحقق کلاهبرداری کلاسیک موثر نیست، لذا عمل مرتکب با قوانین کیفری مربوط به کلاهبرداری کلاسیک قابل تعقیب و مجازات بوده وجرم ارتکاب‌یافته کلاهبرداری کلاسیک است که می‌توان آن را "کلاهبرداری کلاسیک رایانه- ای" نیز نامید.

۲- استفاده از رایانه برای ارتکاب کلاهبرداری رایانه‌ای، به‌این صورت که مرتکب بدون فریب قربانی و یا نماینده وی از طریق مداخله ناروا در داده‌های رایانه‌ای یا عملکرد سیستم‌های رایانه‌ای مال او را می‌برد، یا از خدمات مالی متعلق به او بهره‌مند می‌شود. این نوع کلاهبرداری که عنصر مادی آن با کلاهبرداری کلاسیک متفاوت است و با قوانین کیفری مربوط به کلاهبرداری کلاسیک قابل تعقیب ومجازات نیست، کلاهبرداری رایانه‌ای نامیده شده است. در برخی از اسناد بین‌المللی این نوع کلاهبرداری، کلاهبرداری مرتبط با رایانه نامیده شده است (اردبیلی، ۱۳۸۰).

نتایج پژوهش‌های انجام شده نشان می‌دهد که اولین کلاهبرداریهای رایانه‌ای در دهه ۱۹۶۰ واقع شده‌اند. این جرم از دهه ۶۰ تا امروز، اشکال متنوعی به خود گرفته است و نسل به نسل و گام به گام همپای ارتقاء وپیشرفت فناوری اطلاعات، متحول شده است. جرم کلاهبرداری رایانه‌ای از جمله اولین جرائم رایانه‌ای است که نظام‌های حقوقی کشورهای مختلف نسبت به آن عکس‌العمل قانونی نشان داده‌اند.در سیستم‌های قضایی بسیاری از کشورها مانند آلمان، بریتانیا، ایتالیا، اتریش، فنلاند، دانمارک، نروژ، سوئیس، سوئد، پرتغال، استرالیا و ژاپن، تعاریف قانونی کلاهبرداری کلاسیک محتاج این است که شخص(انسان زنده) فریب بخورد. بنابراین قوانین مربوط به کلاهبرداری کلاسیک در این کشورها شامل مواردی مانند سوءاستفاده ار صندوق‌های پرداخت و سایر صور کلاهبرداری رایانه‌ای که مرتکب صرفا از طریق سوءاستفاده از رایانه و بدون فریب انسان مال دیگری را می‌برد، نمی‌شود. این کشورها با اصلاح قوانین کیفری خود یا وضع قوانین جدید در مقابل کلاهبرداری رایانه‌ای عکس‌العمل نشان داده‌اند (زیبر، ۱۳۷۶).

هدف این نوشتار این است که در جهت مقابله با جرم کلاهبرداری رایانه ای که یکی از مصادیق جرایم مالی[2] رایانه ای محسوب می شود تدابیر و راهکارهای لازم را برای پیشگیری از آن ارائه نماید.

۲-تاریخچه کلاهبرداری رایانه‌ای

اولین کلاهبرداری رایانه‌ای را می توان به قضیه الدن رویس در دهه ۱۹۶۰ که در واقع تاریخ قطعی اولین سوء استفاده مالی است، دانست. رویس یک حسابدار شرکت در آمریکا بود که به علت اختلافش با شرکت، با گنجاندن دستورالعمل اضافی در برنامه‌های سیستم های رایانه‌ای شرکت، در قیمت کالاها تغییراتی را ایجاد نمود و مبالغ به دست آمده را به حساب خاصی واریز می‌کرد. او توانست در مدت شش سال بیش از یک میلیون دلار برداشت کند اما چون نتوانست سیستم را متوقف کند در نهایت خود را به مراجع قضایی معرفی و به ده سال حبس محکوم شد (دزیانی، ۱۳۷۸).

این قضیه در ابتدا از حیث ساختار توصیفی متنازع فیه بود چون با پدیده جرم کلاهبرداری رایانه ای به مفهوم دهه نود آشنایی دقیقی وجود نداشت لذا هر یک از افراد نامی بدان نهادند. در نهایت با تعریف کلاهبرداری رایانه ای امروزه این قضیه را جرم کلاهبرداری رایانه ای توصیف می کنند (دزیانی، ۱۳۷۶).

نخستین و اولین پرونده مطروحه در زمینه جرایم رایانه‌ای در ایران در دهه ۱۳۷۰ و باید گفت شکایت شرکت نرم افزاری سینامند شرکت واژه پرداز مبنی بر تکثیر و فروش غیرمجاز نرم افزارهای تهیه شده شرکت نرم افزاری سینا که موجب صدور رای در تاریخ ۱۳۷۲ /۴/۳ در مورد نرم افزارهای کامپیوتری با استناد به قانون حمایت حقوق مؤلفان و مصنفان هنرمندان مصوب ۱۳۴۸ شد (نوربها، ۱۳۷۷).

با توجه به مطالب مارالذکر و گفته شده طبق سند نهایی جرایم رایانه‌ای در ایران یعنی قانون جرایم رایانه‌ای که مصوب پنجم خرداد ۱۳۸۸ است که مربوط به جرمانگاری رفتارهای قابل ارتکاب در فضای سایبرات در فصل سوم تحت عنوان سرقت و کلاهبرداری مرتبط با رایانه، به جرم انگاری کلاهبرداری رایانه‌ای مبادرت نموده است.

۳- ارکان کلاهبرداری رایانه‌ی

کلاهبرداری رایانه‌ای از سوی کمیته تخصصی شورای اروپا در زمینه جرایم کامپیوتری در خصوص کلاهبرداری رایانه‌ای تعریفی بدین شرح ارائه شده است:

وارد کردن، محو یا موقوف سازی دادههای کامپیوتری یا برنامه‌های کامپیوتری یادگیر مداخلات در پردازش دادهها که بر نتیجه پردازشها داده ها که بر نتیجه پردازش اثر بگذارد و موجب ضررهای اقتصادی یا هر تصرفی در اموال شخصی دیگر به قصد تحصیل منفعت اقتصادی غیرقانونی برای خود یادگیری شود (باستانی، ۱۳۹۰).

تعریف دیگر که در بیشتر سیستم‌های قانونی نسبت به کلاهبرداری است مانند، اتریش، دانماارک، فنلاندف آلمان غربی، یونان، ایتالیا، لوگزامبورگ، نروژ، سوئیس و سوئد است متضمن این امر است که شخصی فریب بخورد (معظمی، ۱۳۸۴). از انجا که در این موارد « فریب» کامپیوتر کفایت نمی‌کند، قابلیت اعمال مقررات مربوط به کلاهبرداری در این کشورها، همیشه به این بستگی دارد که آیا مجرم شخصی را که مسئول کنترل دادهها بوده فریب داده است یا نه ؟ با این حال، در بعضی کشورها

مقررات مربوط به کلاهبرداری، به صورت موسع‌تری مورد تفسیر قرار می‌گیرد؛ برای مثال این موضوع با دقت در اصطلاح « مانور متقلبانه» در تعریف قانونی از کلاهبرداری (escroquerie) در بلژیک و فرانسه به خوبی روشن می‌شود. کلاهبرداری اینترنتی: در واقع یکی از جرایم یقه سفیدهاست که ساترلند که بنیانگذار این اصطلاح است در دو کتاب خود یعنی سارق حرفه‌ای ۱۹۳۷ و اصول جرمشناسی ۱۹۲۴ به بررسی بزهکاری یقه سفیدها می‌پردازد و آن را مطرح کند. (White collar criminality و قلمرو مطالعات جرمشناسی را گسترده تر می‌کند (نجفی ابرندآبادی، ۱۳۹۰).

کلاهبرداری اینترنتی عبارت است از: هرگونه کلاهبرداری که بوسیله برنامه‌های کامپیوتری و رایانه‌ای یا ارتباطات شبکه اینترنتی صورت گیرد مثلا از طریق سایتها (web) پست الکترونیک (email) یا اتاقهای گفت و گو (chatrooms) در واقع کلاهبرداری اینترنتی به هر نوع طرح متقلبانه‌ای گفته می‌شود که یک یا چند بخش از اینترنت را به کار می‌گیرد تا درخواست‌های متقلبانه‌ای را به منظور بردن اموال و انجام معاملات جعلی با قربانیان احتمالی مطرح می‌سازد. تفاوت کلاهبرداری رایانه‌ای با اینترنتی در این است که در واقع کلاهبرداری کامپیوتری یا رایانه‌ای مفهوم اعم‌تر و عامتر نسبت به کلاهبرداری اینترنتی دارد و لذا دو مقوله جدا از هم هستند. در مقابل گفته شده است کلاهبرداری رایانه‌ای یا کامپیوتری قبل از به وجود آمدن اینترنت بوده است ولی بعد از آنکه اینترنت به وجود آمد و محیط مجازی (cyberspace) کم کم و به مرور زمان اصطلاح کلاهبرداری کامپیوتری به کلاهبرداری اینترنتی تغییر نام پیدا کرد و عدهای معتقدند که کلاهبرداری رایانه‌ای همان کلاهبرداری اینترنتی می‌باشد و این دو اصطلاح را به جای هم به کار می‌برند (حبیب زاده، ۱۳۸۰).

۱- رکن قانونی: منظور از عنصر قانونی جرم اصل قانونی بودن جرم است. این اصل در متم قانون اساسی و قانون مجازات عمومی ایران پذیرفته شده است. (باهری، ۱۳۸۴، ص۱۰۹) در حال حاضر در اصل ماده دوم بیست و دوم قانون اساسی هم به این مسئله اشاره شده است. اصلی‌ترین سند عنصر قانونی بودن جرم ماده دوم قانون مجازات اسلامی ایران است که مقرر می‌دارد « هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد جرم محسوب می‌شود» اصل قانونی بودن جرم در قرن هیجدهم‌پدید آمد و بکار یا صراحتا در کتاب خود به نام «جرایم و مجازاتها» که به سال ۱۷۶۴ منتشر شد از آن دفاع نمود. (باهری، ۱۳۸۴، ص ۱۱۱مجموعا) در ارتباط با کلاهبرداری رایانه‌ای از جانب کشورهای جهان سه رویکرد در امر قانونگذاری اتخاذ شده است.

الف) برخی از کشورها صراحتا مقررات جزایی جداگانه‌ای در ارتباط با کلاهبرداری رایانه‌ای وضع کردهاند که عملا در این کشورها دو نوع کلاهبردرای وجود دارد: کلاهبرداری سنتی و کلاهبرداری رایانه‌ای، مثل مواد ۹۳ و ۱۱۵ قانون جرایم اقتصادی مرتبط با رایانه مصوب ۱۹۸۵ یا ماده ۳۶۳ قانون جزای آلمان اصلاحی ۱۹۸۶ و یا ماده ۲۷۹ قانون جزای دانمارک مصوب ۱۹۸۵ که در این کشورها تحصیل مال یا منفعت از طریق روشهای غیرقانونی دادهپردازی یا محو یا تغییر یا ایجاد داده در سیستم رایانه‌ای به عنوان کلاهبردرای رایانه‌ای شناخته شده است.

ب) برخی از کشورها هر چند مقرره جدیدی برای کلاهبردرای رایانه‌ای وضع نکردهاند اما با وضع یک مقرره کلی بیان کردهاند که چنانچه جرمی از طریق رایانه ارتکاب یابد براساس مقررات کیفری فعلی (سنتی) قابل مجازات است مثل قانون

جزای هند. در حقوق جزای ایران هم نسبت به جرایمی که نظامیان از طریق سیستم رایانه‌ای مرتکب می‌شند، همین سایت اتخاذ شده است.

ج) برخی کشورها نیز اصولا نسبت به جرم کلاهبرداری رایانه‌ای سکوت اختیار کردهاند و جرایم مرتبط با آن را با مقررات کیفری موجود پاسخ می‌دهند. این دسته از کشورهای عمدتا در حال توسعه هستند که رایانه و اینترنت هنوز به‌طور کامل در آنها رشد نیافته است (عالی‌پور، ۱۳۹۰).

با توجه به مطالب فوقالذکر ایران در خصوص کلاهبرداری رایانه‌ای جز دست اول به شمار می‌آید که در واقع در مورد کلاهبرداری سنتی طبق قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری که در ماده یک به جرم مذکور اشاره می‌کند و در مورد کلاهبرداری رایانه‌ای هم قانونگذار طبق ماده ۱۳ قانون جرایم رایانه‌ای (۷۴۱ قانون مجازات اسلامی) کلاهبرداری رایانه‌ای را به این شکل معرفی می‌کند: هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن دادهها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال یا یکصد میلیون (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

رکن مادی: شرط تحقق جرم آن است که قصد سوء با ارتکاب عمل خاصی دست کم به مرحله فعلیت برسد. فعل یا عمل خارجی که تجلی نیت مجرمانه و یا تقصیر جزایی است عنصر مادی جرم را تشکیل می‌دهد. عنصر مادی جرم در واقع حقیقت و ماهیت عمل ضد اجتماعی است و آن رفتار آدمی بر طبق نشانه‌هایی است که قانونگذار در متن قانون از آن به دست داده است یعنی رفتار آدمی غیر از پندار او است، در حقوق جزا پندار انسان هر چند زشت و نکوهیده باشد قابل مجازات نیست (باهری، ۱۳۸۴، ص ۱۹۲). عنصر مادی و ضروری جرم گاه رفتاری[۱] است که در وضع خاصی از انسان بروز می‌کند و گاه به ندرت حالتی[۲] است که بر او مستولی می‌گردد (اردبیلی، ۱۳۸۰).

براساس ماده ۱۳ قانون جرایم رایانه‌ای (م ۷۴۱ قانون مجازات اسلامی) رفتار مادی فیزیکی جرم کلاهبرداری رایانه‌ای فعل است و آن هم از نوع مثبت زیرا مصادیقی که برای ارتکاب این جرم به کار برده شده است، نظیر وارد کردن، تغییر، محو و. .. نوعا به شکل مثبت است لذا کلاهبرداری رایانه‌ای با ترک فعل محقق نمی‌شود. (الهی‌منش، سدره نشین، ۱۳۹۱ ص ۸۵) عنصر دوم که در رفتار نمود پیدا می‌کند تحصیل است که دریافت واقعی یا مجازی یا منظور کردن اعتبار مالی برای خودو لازم نیست حتما مال در دستان مرتکب جای بگیرد به عنوان مثال کسی به سامانه بانک رخنه کند و رقم پولی دارنده حسابی را کاهش و یا حساب خود را افزایش دهد (عالی‌پور، ۱۳۹۰، ص ۲۸۱). تحصیل مال یا منفعت و مانند آن برخلاف کلاهبرداری سنتی به معنای دارا شدن نیست بلکه ممکن است کسی با وارد شدن به سامانه یک موسسه مالی، درصد اقساط وامی را که باید برگرداند کاهش دهد یا با دستکاری در سامانه، چنان بنماید گوید برخی از اقساط وام پرداخت شده است مرتکب کلاهبرداری رایانه‌ای شده است (عالی‌پور، ۱۳۹۰).

رکن روانی: عنصر روانی که برای مسئولیت مورد توجه است در دو مطلب باید مورد توجه قرار گیرد.

۱- اراده انجام جرم آنچنان که مقنن یا قانونی مشخص کرده است.

۲- آگاهی جرم بر این مطلب که دارد از ممنوعیت‌های قانون تجاوز می‌کند این نکته مبنای سوء نیت عام است مثلا قانون می‌گوید هرکس‌عامدا این کار را انجام دهد گاهی هم ممکن است نگوید (نوربها، ۱۳۸۹).

برای تحقق جرم نقض اوامر و نواهی قانونگذار به تنهایی کافی نیست. فعل مجرمانه باید نتیجه خواست و اراده فاعل باشد، به سخن دیگر، میان فعل مادی و حالات روانی فاعل باید نسبتی موجود باشد تا بتوان مرتکب را مقصر شناخت. (اردبیلی، ۱۳۸۰، ص ۲۳۳). جرم کلاهبرداری رایانه‌ای در زمره جرایم عمدی است که متضمن وجود سوءنیت عام و خاص است. سوء نیت عام عبارت از عمد ارتکابی اعمالی از قبیل، وارد کردن، تغییر، محو و. .. است؛ یعنی فرد مرتکب جرم « شخص یا اشخاص حقیقی یا حقوقی)، عالما« »عاملا« » افعال مذکور را انجام دهد. در کلاهبرداری رایانه‌ای در واقع باید گفت که قصد نهایی بایسته نیست و وجود آن ضروری نیست (الهی منش-سدره نشین، ۱۳۹۱)

۴- شیوه های ارتکاب کلاهبرداری رایانه‌ای

۱- مهندسی اجتماعی: (Social Engineering)

حملات مهندسی اجتماعی عبارت است از روند نفوذ به سیستم‌های رایانه‌ای از طریق کاربرد حیله‌های گوناگون درخصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط به موارد آسیب‌پذیر شبکه (قلی زاده نوری، ۱۳۸۱، ص ۶۸۸) مهندسی اجتماعی نوعی نفوذ غیرمجاز یا هک شفاهی به شمار می‌رود که در آن مرتکب با تماس تلفنی یا ارتباط از طریق پست الکترونیک یا گپ‌زنی یا معرفی خود به عنوان یکی از کارکنان شرکت یا یک شخص معتبر سعی در تخلیه اطلاعاتی مخاطب خود پیرامون سیستم رایانه‌ای مربوطه می‌کند. در واقع آنچه به چشم می‌آید. این است که در مهندس اجتماعی، مرتکب قبل از این‌که به دانش فنی مربوطه به نفوذ به سیستم رایانه‌ای متکی باشد، متکی به میزان نفوذ کلامی یا رفتاری او دارد که به شیوه ی خطر ناکی در حال افزایش است. مهندسی اجتماعی اگرچه مقدمه کلاهبرداری رایانه‌ای است ولی از مقدمات بعیده است و می‌تواند معادل توسل به وسایل متقلبانه در نظر گرفته شود البته شایان به ذکر است که چه بسا هدف مهندسی اجتماعی کسب و به دست آوردن اطلاعات مالی نباشد و ممکن است به دنبالطلاعاتا امنیتی شرکت یا سیستم یا اصولا نوعی اصلاح یا بی‌هدف باشد (جوکار و سبحانی، ۱۳۹۲).

۲- فیشینگ یا کسب اطلاعات ملی: (Phishing)

فیشینگ راهی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶ رقمی عابر بانک، رمز دوم cvv۲ را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می‌برند. شبکه‌های حراجی و درگاههای پرداخت آنلاین نمونه‌ای از ابزارهای الکترونیکی ارتباطات می‌باشد. (پلیس فضای تولید و تبادل اطلاعات). کلاهبرداری فیشینگ از طریق ایمیل‌ها و پیامها صورت می‌پذیرد و قربانیان به صورت مستقیم اطلاعات حساس و محرمانه خود را در یک وب سایت‌های جعلی که در ظاهر کاملا شبیه وب سایت‌های سالم و قانونی می‌باشد وارد می‌نماید. (پلیس فضای تولید و تبادل اطلاعات) (باهری، ۱۳۸۴).

۳- حمله نفوذگر (Pharming)

حمله نفوذگر به منظور تغییر ترافیک وب سایت به یک وب سایت جعلی دیگر است. در این بخش از شیادی، با دستگاری سرویس دهنده DNS توسط فرد شیاد که در اصطلاح فنی به « سمی» شدن سرویس دهنده DNS کاربر معروف است. منجر می‌شود. کاربر به تصور این‌که وارد سایت اصلی بانک می‌شود وارد سایت جعلی فرد شیاد شده و اطلاعات محرمانه بانکی اعم از شماره حساب، شماره کارت و کلمه عبور را وارد می‌کند و آنگاه فرد شیاد به راحتی می‌تواند نسبت به سوء استفاده اقدام کند (جوکار و سبحانی، ۱۳۹۲).

۴- فرآیند کپی کردن: Skimming))

فرآیند کپی کردن اطلاعات نوار مغناطیسی کارت اعتبار مشتری از طریق کشیدن کارت از میان کارتخوان و استفاده از اطلاعات جهت ساخت کارت تقلبی توسط فرد شیاد را Skimming)) می‌نامند (پاکزاد، ۱۳۷۵).

۵- دزدیدن کلمه عبور Shoulder surfing))

دزدیدن کلمه عبور دارنده کارت هنگام استفاده از دستگاه خودپرداز یا پایانه فروش از طریق مشاهده کاراکترهای وارد شده توسط کاربر را شامل می‌شود (خداقلی، ۱۳۸۳).

۵- راه های پیشگیری از کلاهبرداری رایانه‌ای

مفهوم پیشگیری از جرم:

پیشگیری از جرم یک امر غریزی است. انسان بالفطره پیش گیرنده از جرم بوده، همین که انسان از زمانی که تاریخ به یاد دارد بالفطره به طور غریزی از خود دفاع به‌عمل می‌آورده، خود این یک نوع پیشگیری به حساب می آید (حسینی، ۱۳۸۳). همواره پیشگیری در ارتکاب جرم موثرتر و سودمندتر از مبارزه و مجازات می باشد. در جرایم رایانه ای نیز، پیشگیری باید به عنوان هدف عمده هرگونه سیاست گذاری در این خصوص باشد. در اصطلاحات سیاست جنایی وقتی از پیشگیری از بزهکاری سخن به میان می آید، منظور استفاده از راهکارهای متعدد برای ممانعت از وقوع جرم است (اردبیلی، ۱۳۸۳).

پیشگیری از جرم، مجموعه اقدامات پیشگیرانه با هدف تحدید خطر وقوع پدیده های جنایی از راه ناممکن ساختن یا دشوار کردن یا کاستن از احتمال وقوع آنها بدون تاکید بر تهدید به مجازات است (اظهار نظر کارشناسی درباره لایحه پیشگیری از جرم، ۱۳۸۵).

در مجموع می توان گفت پیشگیری از جرم در مفهوم کلی آن عبارتست از تاثیر گذاری بر عوامل جرم زا به نحوی که این عوامل جرم زا تقلیل یافته یا در شکلی آرمانی از بین برود (معظمی، ۱۳۸۴). در یک دسته بندی، پیشگیری از جرم به پیشگیری غیرکیفری که جلوگیری از وقوع جرم با تکیه بر مجازات ها در چارچوب نظام کیفری می باشد، در قالب دو نوع پیشگیری عام و خاص مطرح است. مقابله با جرایم رایانه ای و به‌طور اخص کلاهبرداری رایانه ای نیازمند اتخاذ یک

سیاستگذاری عالمانه و برنامه ریزی همه جانبه است و هر جرم یا هر طبقه از مجرمین برنامه های خاصی را برای مقابله می طلبند به نحوی که امروزه بایستی مقابله با جرایم رایانه ای به صورت تخصصی و مستقل مورد مطالعه قرار گیرد.

برخی پیشگیری از جرم را نوعی مداخله از طریق اتخاذ تدابیر برای جلوگیری یا کاهش خطرات ارتکاب یا کاهش نتایج احتمالی می‌داند. موریس کوسن جرمشناس کانادایی پیشگیری را چنین تعریف می‌کند « مجموعه اقدامات و تدابیر قهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم، کاهش وخامت جرم، پیرامون جرایم اتخاذ می‌شود (ابراهیمی، ۱۳۹۱). مفهوم پیشگیری بر پایه این نکته بنا می‌شود که در پیرامون جرم و بزهدیدگی عوامل بسیار زیادی دخیل هستند. دامنه این عوامل بسیار وسیع است؛ شرایطی که افراد در آن رشد می‌کنند. شرایط بومی و محلی، موقعیت‌ها و فرصت‌های تسهیل کننده جرم همگی در ایجاد جرم و بزهدیدگی دخیل هستند (جوان جعفری، سید زاده ثانی، ۱۳۹۱).

جرمشناسی پیشگیرانه (Preventional criminology) که به تعبیر استاد گسن یکی از سه شاخه جرمشناسی کاربردی است در یک تقسیم‌بندی کلی منقسم می‌شود به پیشگیری وضعی و پیشگیری اجتماعی (نجفی ابرندآبادی، ۱۳۸۳). پیشگیری وضعی از کلاهبرداری رایانه‌ای: پیشگیری وضعی یعنی تغییر اوضاع و احوال و شرایط خاص- که احتمال ارتکاب جرم در آن زیاد است- به منظور دشوار نمودن، خطر پر کردن یا جاذبه‌زدایی ارتکاب جرماین نوع از پیشگیری از لحاظ مبانی و شویه ها کاملا با دیگر گونه‌های پیشگیری متفاوت اند. پیشگیری وضعی عبارت است از تغییر در موقعیت‌های خاصی که ارتکاب جرم در آن زیاد است به منظور دشوار نمودن بر خطر کردن یا جاذبه‌زدایی برای کسانی که قصد ارتکاب دارند (ابراهیمی، ۱۳۹۱). در واقع پیشگیری وضعی با تمرکز بسیار زیاد بر فرصت‌های مجرمانه، سخت کردن سبیل‌های جرم و افزایش نظارت است که پیش می‌رود. در زمینه پیشگیری وضعی از جرایم رایانه‌ای باید گفت که با این‌که مشکلات زیادی بر سر راه آن وجود دارد اما باز هم جایگاه خاصی برخوردار است. یکی از این دلایل توجیه می‌تواند قابلیتی باشد که فضای سایبر فراهم آورده است. (فراهانی، ۱۳۸۳). از جمله اقدامات خاص پیشگیری وضعی از جرایم رایانه‌ای می‌توان به موارد ذیل اشاره کرد:

۱- نصب دیواره آشین یا لایه در شبکه‌های اطلاع رسانه رایانه‌ای (فراهانی،۱۳۸۳)

۲- پلیس گشت سایبریکی از نتایج مثبت پلیس گشت پیاده به عنوان یک اقدام وضعی پیشگیرانه است (فراهانی، ۱۳۸۳)

۳- برنامه‌های ویروسیابی یا کوکی‌یابی (فراهانی، ۱۳۸۳)

۴- استخدام یک کارمند امنیت رایانه و نیز مشاوران رایانه‌ای (رحمانی، ۱۳۹۰)

۵- یک خط تلفن اضطراری برای گزارش کلاهبرداری رایانه‌ای و یا تقلب (رحمانی،۱۳۹۰).

۶- استفاده از هکرها برای کمک به شناساندن ضعف سیستم‌های امنیتی موجود. (پلیس فضای تولید و تبادل اطلاعات).

۷- استفاده ا ز پلیس و سازمانهای خود نظارتی مثل بانک و بیمه خود یک راه پیشگیرانه است.

۸- تقویت سیستم امنیتی حفاظتی بانک و سیستم‌های و شرکت‌های مالی

۹ - تشکیل ستاد پیشگیری و مبارزه با جرایم فناوری اطلاعات در محیط سایبر (قریشی، ۱۳۹۱).

۱۰- مجهز کردن بانک و کلیه موسسات ملی به سیستم‌های حفاظتی و امنیتی برای رایانه‌ها

۱۱- حفاظت فیزیکی: حفاظت فیزیکی به معنای حفظ رایانه، تجهیزات رایانه، رسانه‌های رایانه‌ای و تمامی سیستم، در مقابل سوانح طبعی، نواع مختلف حوادث و محلات عمومی است. جرایم رایانه‌ای قابل پیش‌بینی نیستند پس در واقع نیاز به تدابیری برای دشوار کردن ارتکاب آنها نمود اولین حلقه حفاظت فیزیکی اقداماتی است که مجرمین را از نفوذ به ساختمان محل استقرار رایانه‌ها مأیوس نمود به‌طوری که تدابیر مناسب

ورودی ا تاقهای محل نگهداری سیستم رایانه‌ای اتخاذ شودو هم‌چنین جهت جلوگیری از استراق سمع تلفنی، اتخاذ تدابیر و اقدامات لازم جهت حفاظت از رمز عبور، نام فایل ها و سایر اطلاعات محرمانه ضروری است.

۱۲- حفاظت کارکنان: تدبیر حفاظت کارکنان، افرادی را پوشش می‌دهد که به نحوی مجاز به کار با سیستم می‌باشد اغلب جرایم مالی رایانه‌ای توسط افراد مذکور و نه حریم‌شکنان صورت می‌گیرد. در ضمن قابل ذکر است که در این‌باره و در بحث حفاظت کارکنان بایستی دیدیترین احتیاطها در مورد کارکنان اخراجی یا کارکنانی که داوطلبانه از کار کنارهگیری می‌کنند اتخاذ شود.

۱۳- حفاظت از ارتباطات: گونه‌ای دیگر از تدابیر امنیتی و حفاظتی، حفاظت ارتباطات است که شامل حفاظت از پست، مخابره، تلفن، ارتباطات پست صوتی و هم‌چنین حفاظت از اطلاعات انتقال داده شده از یک رایانه به رایانه دیگر از طریق انتقال شبکه می‌شود. مجرمین حرفه‌ای ممکن است سیستم رایانه را برای ارتکاب کلاهبرداری یا مستقیما برای منفعت خودشان مورد هدف قرار دهند. در این صورت تدابیر حفاظت ارتباطات، (به عنوان نمونه کلمات رمز عبور) مهم‌ترین عامل برای ذور نگهداشتن مجرمین حرفه‌ای است.

۱۴- حفاظت عملیات: آخرین نوع از تدابیر حفاظتی، حفاظت عملیات است. حفاظت عملیات به معنی وضع تدابیری جهت شناسایی و مقابله با تهدیدهایی است که سیستم‌ها را به مخاطره می‌اندازد (میرمحمد صادقی، شایگان، ۱۳۸۶).

۱۵- استفاده از کد رفتاری: کد رفتاری عبارت است از مجموعه قواعد و مقرراتی راجع به حقوق نرمافزار که مشتمل بر تظیم قواعد سازمانهای تخصصی، کدهای رویه‌های هماهنگ، کدهای رفتاری، کدهای اخلاقی و شغلی می‌باشد که مجموعا کدهای رفتاری نامیده می‌شود (باستانی،۱۳۹۰). پیشگیری اجتماعی: پیشگیری اجتماعی به فرآیند تربیت و رشد انسان تکیه می‌کند و راهبرد نسبتا زمانبری برای پیشگیری از جرم ترسیم می‌کند. این نوع از پیشگیری در ایران علاوه بر صدر بند ۵ اصل ۱۵۶ قانون اساسی که « اصل راهبردی» حقوق پیشگیری ایران محسوب می‌شود، در اصول راهبردی دیگر قانون اساسی نیز مورد اشاره قرار گرفته است (ابراهیمی، ۱۳۹۱).

پیشگیری اجتماعی در واقع خود به دو دسته تقسیم می‌گردد که عبارت است:

۱- پیشگیری اجتماعی رشدمدار یا زودرس: در واقع مداخله در رشد و شخصیت فرد مثل کودک برای جلوگیری از جرم او در آینده دارد و در واقع هدف از پیشگیری اجتماعی رشدمدار آموزش و تربیت افراد برای پیشگیری از جرم در آینده است در واقع این‌گونه از پیشگیری را آموزش و پرورش محور هم می‌نامند (ابراهیمی،۱۳۹۱).

۲- پیشگیری اجتماعی جامعه‌مدار: هدف از تدابیر پیشگیری اجتماعی جامعه‌مدار، جلوگیری از شکل‌گیری یا بروز انگیزه مجرمانه در عموم جامعه به وسیله دو اقدام اصلی است: ۱- ترغیب و تسهیل بروز انگیزشهای مشروع و سودمند ۲- برحذر داشتن از ناهنجاریهای سایبری (میرمحمد صادقی، شایگان، ۱۳۸۶).

۶-نتیجه گیری

اساسا حوزه تاثیرگذاری جرایمی که در فضای سایبر واقع می شوند نسبت به جرایم سنتی بسیار گسترده است و به مراتب خسارات بیشتری نیز بر جای خواهند گذاشت، بنابراین همانطور که جوامع با وقوع جرم در دنیای فیزیکی مقابله می کنند ارائه راهکارهای مناسب در جهت مقابله و جلوگیری از وقوع جرم در محیط مجازی که از اوصاف و ویژگی متفاوتی نسبت به محیط واقعی برخوردار است امری ضروری است. دراین نوشتار سعی بر آن شد که راهکارهای غیرکیفری و کیفری در مقابله و جلوگیری از ارتکاب جرم کلاهبرداری رایانه ای ارائه شود بنابراین آنچه در به کارگیری راهکارهای غیر کیفری مورد توجه می باشد مقابله اجتماعی و وضعی در برابر وقوع جرم است. در تدابیر اجتماعی جهت مبارزه با جرم کلاهبرداری رایانه ای باید ارتقاء سطح فرهنگ افراد در استفاده از فناوری های نوین و تغییر نگرش افراد و آشنایی آنها از کارکرد اصلی این فناوری و تقویت نقش تربیتی و آموزشی والدین و موسسات آموزشی در کاهش ارتکاب جرم مورد تاکید قرار گیرد. با عدم توفیق مقابله اجتماعی در کاهش یا مهار جرم، مقابله وضعی با آن مطرح خواهد شد. هدف از مقابله وضعی، سلب فرصت ارتکاب جرم از سوی نفوذ کنندگان به سیستم های رایانه ای است.

قابل ذکر است که در بحث امنیت سیستم های رایانه ای، امنیت مطلق وجود ندارد و همواره با دستیابی افراد به شیوه های نوین ارتکاب جرم کلاهبرداری در محیط سیستم‌های رایانه‌ای، اتخاذ تدابیر امنیتی متناسب با این شیوه ها ضرورت دارد. تنوع بسیار گسترده شیوه های ارتکاب این جرم مانع از وضع تدابیری است که بتوان تمامی آنها را تحت پوشش قرارداد بنابراین مبارزه موثر و منسجم با این جرم تنها بر پایه شناخت درست از ماهیت و شیوه های ارتکاب جرم امکان پذیر است.

اصولا جرم انگاری رفتارهای مجرمانه به عنوان آخرین حربه علیه هنجارشکنان مورد توجه جرم شناسان قرار می گیرد. لذا تدابیر کیفری به عنوان ابزاری سرکوبگر آخرین راهکار مقابله با وقوع جرم است. با این حال باید توجه داشت که صرف جرم انگاری و تعیین ضمانت اجرای کیفری کافی نیست و تدابیر کیفری در صورتی در مقابله با جرم موثر است که امکان کشف و تعقیب جرم و مجازات مجرم وجود داشته باشد. لذا با توجه به اینکه در فضای سایبر اصل بر ناشناختگی است در اکثر موارد کشف و تعقیب جرایم ارتکابی و اعمال مجازات مجرمان چه در سطح ملی و چه در سطح فراملّی (به علت واجد جنبه فرامرزی بودن جرایم سایبری) با چالش های فراوانی روبروست که در این راستا بایستی آموزش و بالا بردن سطح دانش ماموران کشف جرم در زمینه پی جویی جرایم ارتکابی در فضای سایبر و همچنین تقویت همکاری های بین المللی در سطوح مختلف طراحی سیستم های امنیتی فراملّی و انعقاد معاهدات همکاری چند جانبه در زمینه معاضدت قضایی، استرداد مجرمان و. .. از سوی کشورها مورد تاکید بیشتری قرار گیرد.

یکی از جرایم مالی که در حوزه سایبر و فضای مجازی و رایانه اتفاق می‌افتد کلاهبرداری رایانه‌ای است در واقع باید گفت از آنجا که این جرم خسارت جبراننا‌پذیری را در بردارد و چه بسا موجب نگرانی افراد از دارایی و اموال خود می‌گردد از آنجا که کلاهبرداری به تعبیری مختص افراد باهوش و زیرک است و به نوعی افرادی که از خطاها و نقص‌های موجود اطلاع دارند لذا باید گفت در پی پیشرفت‌ها و تحولات اجتماعی است که این افراد فریب‌کاریهای خود را در سایه افزارهای به وجود آمدهف پیچیدهتر و ناشناخته‌تر می‌سازند و اگر احساس کند که راههای فریب و نیرنگ در معرض شناخته شدن قرار می‌گرد به دنبال فرصت‌های نو برای ارتکاب جرم خود می‌گردند. از آنجا که راههای کلاهبرداری رایانه‌ای را ذکر کردیم و دیدم که به راحتی می‌توان دست به کلاهبرداری رایانه‌ای زد لذا هیچ‌کس مصون از جرم مذکور نیست لذا باید درصدد آن برامد که از جرم مذکور پیشگیری گردد. از هر سو و نظر که کلاهبرداری رایانه‌ای به واسطه عدم شناخت کافی یا عدم مهارت لازم در سیستم‌های رایانه‌ای و یا نبود راهکاری مناسب برای مقابله با جرم مذکور است در مطالب فوق الذکر به راههای برای مقابله با کلاهبردرای رایانه‌ای اشاره شد. آنچه مهم است این است که جرایم رایانه‌ای و به طور خاص کلاهبرداری رایانه‌ای برای مقابله و پیشگیری با آن و یا عدم تکرار دوباره جرم نیاز به همکاری همیاری تمام رشته‌ها و حوزههای علوم نظیر علوم اجتماعی، روانشناسی، جامعه‌شناسی، فناوری اطلاعات و. .. می‌باشد. باید گفت که فضای تبادل اطلاعات و حقوق فناوری اطلاعات چیزی نیست که به راحتی از آن بگذریم و عطایش را به لقایش ببخشیم بلکه چون هم ما نیاز به استفاده از فضای مجازی و سایبری داریم لذا باید چالش‌های موجود را سیاست‌گذاران در عرصه‌های خرد و کلان کشور با اتخاذ تدابیر مناسب که موجب رشد و شکوفایی افراد جامعه در تمامی ابعاد فراهم آورد. قابل ذکر است که در بحث امنیت و حفاظت از سیستم‌های رایانه‌ای، امنیت به معنی مطلق و تمام آن وجود ندارد و همواره دست‌یابی افراد به شیوههای نوین و جدید ارتکاب جرم کلاهبرداری رایانه‌ای در محیط سایبر انجام می‌گیرد و لذا این ما را بر آن می‌دارد که به دنبال یک مبارزه مؤثر و منسجم با این جرم با پایه شناخت درست از ماهیت و شیوه های ارتکاب آن است. در آخر باید گفت از آنجا که گاه پیشگیری کیفری جواب نمی‌دهد و مجازات هدف اصلی خود را یعنی اصلاح ندارد می‌توان دست به پیشگیری قبل از جرم زد و در این راستا در مورد کلاهبرداری رایانه‌ای می‌توان با آموزش و بالا بردن سطح اطلاعات والدین دانش‌آموزان در پیشگیری اجتماعی زودرس و هم‌چنین کارگاه های آموزش عمومی در پیشگیری اجتماعی جامعه‌دار و هم‌چنین راهکارهای امنیتی و حفاظتی مناسب به منظور ریسک تکابار جرم دستگیری وضعی و مجموعا با تقویت دانش مخاطبان سایبری و تقویت همکاریهای بین‌المللی می‌توان به نوعی در برابر کلاهبرداری رایانه‌ای پیشگیری و مقابله کرد به امید روزی که شاید هیچ جرمی نباشیم.

منابع

۱. نور بها، رضا،جزوه درسی عنصر معنوی جرایم،دانشکده حقوق دانشکده شهید بهشتی،سال تحصیلی ۱۳۹۰-۱۳۸۹.

۲. میر محمد صادقی- شایگان،حسین- محمد، راهکارهای مقابله با جرم کلاهبرداری رایانه ای در حقوق کیفری ایران،فصل نامه دیدگاه های حقوقی،دانشکده علوم قضایی و خمات اداری،شماره ۴۳-۴۲،۱۳۸۶

۳. نجفی ابرند آبادی، علی حسین، تقریرات جامه شناسی جنایی،دانشکده حقوق دانشگاه شهید بهشتی،سال تحصیلی ۱۳۸۴-۱۳۸۳،تنظیم مهدی صبوری پور

۴. عالی پور،حسن، حقوق کیفری فناوری اطلاعات، تهران، خرسندی،چاپ اول، ۱۳۹۰

۵. گفتگو با علی رحمانی،استاد دانشگاه الزهرا،۳۰آذر،۱۳۹۰

۶. جوان جعفری - سید زاده ثانی، عبد الرضا - مهدی،رهنمود های عملی پیشگیری از جرم، تهران،میزان ، چاپ اول، ۱۳۹۱

۷. جوکار- سبحانی، پریا- مژگان، کارشناسان خدمان انفور ماتیک،۸فروردین ،۱۳۹۲

۸. خداقلی، زهرا، بزه های کامپیوتری،تهران، آریان،چاپ اول، ۱۳۸۳

۹. ابراهیمی، شهرام، جرم شناسی پیشگیری، جلد نخست، تهران ،میزان ، چاپ دوم ، ۱۳۹۱ ۲-اردبیلی،مخمد علی، حقوق جزای عمومی، جلد نخست، تهران، میزان، چاپ دوم، ۱۳۸۰

۱۰. الهی منش- سدره نشین، محمد رضا- ابو الفضل، محشای قانون جرایم رایانه ای، تهران، مجد،چاپ اول، ۱۳۹۱

۱۱. باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، تهران، بهنامی، چاپ سوم،۱۳۹۰

۱۲. باهری، محمد، نگرشی بر حقوق جزای عمومی، تهران، مجد، چاپ دوم ، ۱۳۸۴

۱۳. پاکزاد، بتول، بزه های کامپیوتری،پیان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی،۱۳۷۵

۱۴. دزیانی، محمد حسن، (۱۳۷۸) جزوه گزارش توجیهی جرایم رایانه‌ای، مقررات لازم درحقوق جزای ماهوی، دبیرخانه شورای عالی انفورماتیک،

۱۵. دزیانی، محمد حسن،(۱۳۷۶) جرم رایانه‌ای، گزارش دستاوردهای شورای اروپا در ارتباط با توصیه‌نامه R(۸۹) ۹، (ترجمه) ، جزوه جرائم رایانه ای، جلد اول ، خانه شورای عالی انفورماتیک،

۱۶. زبیر، اولریش، (۱۳۷۶) الف " پیدایش بین المللی حقوق کیفری اطلاعات " ترجمه محمد حسن دزیانی، جزوه جرائم کامپیوتری، جلد سوم، شورای عالی انفورماتیک.

۱۷. میر محمد صادقی،(۱۳۷۸) دکتر حسین، جرائم علیه اموال و مالکیت، نشر میزان، تهران، چاپ ششم

۱۸. حبیب زاده، جعفر، »حقوق جزای اختصاصی«، جرایم علیه اموال، چاپ اول، تهران، سمت، ۱۳۸۰.

۱۹. جرایم رایانه ای«، ترجمه: محمدعلی نوری و دیگران، چاپ اول، تهران، گنج دانش، ۱۳۸۳.

۲۰. مرکز پژوهش های مجلس شورای اسلامی، »اظهار نظر کارشناسی درباره لایحه پیشگیری از جرم« شماره ۷۸۹۱، آذرماه ۱۳۸۵.

۲۱. معظمی، شهلا، »جرم سازمان یافته و راهکارهای جهانی مقابله با آن« چاپ اول، تهران، نشر دادگستر، ۱۳۸۴.

۲۲. نجفی ابرند آبادی، علی حسین، »تقریرات درس جرم شناسی دوره کارشناسی ارشد« تنظیم: رضا فانی، نیمسال اول سال تحصیلی ۸۳-۱۳۸۲.