فصلنامه بین المللی قانون یار

License Number: 78864 Article Cod: 2021S4D16SH5M141 ISSN-P: 2538-3701

سیاست پیش گیری و مبارزه با جرم کلاهبرداری اینترنتی

(تاریخ دریافت ۱۳۹۹/۰۹/۱۵، تاریخ تصویب ۱۴۰۰/۰۱/۱۸)

دکتر علی نجفی توانا[۱]

عضو هیئت علمی دانشگاه آزاد اسلامی

فاطمه کریمی

دانشجوی دکتری حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد تهران مرکزی

چکیده

کلاهبرداری رایانه ای از عناوین مجرمانه ای است که در یکی دو دهه ی اخیر به دلیل گسترش فضای اینترنت،شبکه های اجتماعی یا سیستم های مخابراتی یا رایانه ای و مشکلات اقتصادی به خصوص در کشورهای جهان سوم با هدف کسب سود سرشار،بخش بزرگی از جرایم را به خود اختصاص می دهد.دولت ها با سیاست های مختلف حاکمیتی سعی در کنترل این جرایم دارند.ایران نیز به دلیل مشکلات عدیده به عنوان یکی از کشورهای جهان سوم و تحمل تورم و تحریم های اقتصادی شدید در قرن بیست و یک شاهد تعداد زیادی از این دست جرایم بوده و با آن به مبارزه پرداخته است،اما به دلایل مختلفی در کاهش دادن آن موفق نبوده است. در این تحقیق سعی می شود با بررسی سیاست های مختلف تقنینی،قضایی و اجرایی و مشارکتی،عملکرد بخش های مختلف را در نظر گرفته و با پرداختن به روش های ارتکاب کلاهبرداری رایانه ای و اتخاذ سیاست های اصولی حاکمیتی متناسب با شرایط امروز در جامعه،نقش مؤثری در مبارزه و پیش گیری و کاستن از تعداد مرتکبان و به تبع قربانیان این جرم ایفا نماییم.

واژگان کلیدی: سیاست جنایی، قانونگذاری،کلاهبرداری، رایانه ای، کنش، واکنش

[۱] نویسنده مسئول

مقدمه

کلاهبرداری رایانه ای صرفاً کلاهبرداری از طریق رایانه نیست تا به واسطه آن رایانه در حد یک وسیله معرفی گردد، بلکه جرمی است که رایانه در آن نقش اساسی ایفا کرده و عمدتاً برخی از اجزای تشکیل دهنده رکن مادی کلاهبرداری را تحت تأثیر قرار می دهد و به همین دلیل است که کلاهبرداری رایانه ای از کلاهبرداری سنتی متمایز بوده و نسبت به آن جرم انگاری با نگاه جدیدی صورت گرفته است. در کلاهبرداری رایانه ای امکان فریب دستگاه ها و سیستم های پردازش خودکار جداگانه یا با وجود کاربران هر دو امکان پذیر است. در این جرم سوءاستفاده از داده های برنامه و سیستم های کامپیوتری از راه دور در جهت کسب سود و منفعت بیش تر صورت می گیرد و اغلب کلاهبردار و قربانی با هم روبه‌رو نمی شوند. چند مورد تحقیق درمورد سیاست های جنایی ایران در حدود سال ۹۵ تا ۹۸ وجود دارد که واجد اطلاعات به روزتری هستند.به خصوص سیسات جنایی ایران و آمریکا در جرم کلاهبرداری رایانه ای که نگاه تطبیقی در آن وجود دارد.اما با نگاه انتقادی کم تری بیش تر به توصیف شرایط موجود و قانونگذاری پرداخته و نگاه جامع بخش تقنینی،قضایی، اجرایی و هم چنین نگاه مشارکتی حاکمیتی و مردم و حتی سیاست مشارکتی جامعوی در آن ها کم تر بوده و به روش های مختلف کلاهبرداری رایانه ای نیز به طور وسیع نپرداخته اند که سعی شده در این مقاله گنجانده شود. در پاسخ به این سؤال که آیا می توان با شرایط موجود و فقر اقتصادی شدید در جامعه ی ایرانی با اتخاذ و بررسی روش های اصولی و هدفمند،به اصلاح ساختار سیاست تقنینی و قضایی و اجرایی و کاهش مجرمان جرایم کلاهبرداری رایانه ای در کشور رسید،با پرداختن به نگاه قانونگذار ایران و جنبه های مختلف مفهوم پیش گیری و سیاست های اتخاذی دولت تا کنون و تأثیرپذیری از نظریات دانشمندان و جرم شناسان متخصص،به انتقاد و ارائه ی راهکار برای حل این مسئله پرداخت. در زمینه ی پیشگیری از این جرم نیز نخست باید با توسل به نقش آموزش،فرهنگ و حوزه های تربیتی و برطرف کردن مشکلات اساسی کشور زمینه ی شناخت و آگاهی رسانی عموم مردم را در این زمینه بالا برد و با استفاده از سیاست و دستورالعمل های موفق شناخته شده در سراسر جهان با استفاده از انواع پیش گیری های

اجتماعی،مشارکتی و وضعی این سیاست ها را اعمال کرد تا در کاهش این دسته ازجرایم نقش مؤثری داشت.در صورت عدم تأثیرپذیری پیش گیری غیرکیفری جرایم،می توان با اعمال مجازات و بروز واکنش اصولی و ساختارمند و بازدارنده به عنوان آخرین راه حل به برخورد با آن ها پرداخت.

بخش اول: روش های مختلف کلاهبرداری رایانه ای

امروزه شیوه های مختلفی برای فریب افراد در فضای مجازی طراحی و اجرا می گردد.یکی از شایع ترین جراییم در این ارتباط،فیشینگ است.با راه اندازی سایت های مختلف جعلی و تبلیغات گوناگون در فضای مجازی و ارسال پیامک به شهروندان با موضوعات مختلف از قبیل ثبت نام برای جلوگیری از قطع یارانه ها،اختصاص سهمیه بنزین، دریافت مجوز طرح تردد زوج و فرد و سایر مواردی که بسته به موقعیت احتمال مطرح شدن آن ها نیز از سوی فرد کلاهبردار وجود دارد،اقدام به فریب دادن قربانیان برای دریافت هزینه ارائه این خدمات می کنند.روش های مختلف دیگری نیز وجود دارد که در ادامه به آن می پردازیم.

۱-فیشینگ

فیشینگ جرمی که رتبه نخست جرایم اینترنتی کشور را به خود اختصاص داده و مجرم های اینترنتی با هوش نسبتاً بالا حتی هکرهایی با سنین پایین نیز مرتکب آن می‌شوند. مجرمانی که از این روش استفادهمی‌کنند ابتدا با ساختن صفحه‌ای جعلی مشابه صفحه اصلی بانک‌ها شماره کارت،رمز دوم و کد سی وی وی دو را به دست آورده و در فرصتی مناسب اقدام به برداشت از حساب کاربر می‌کنند. این دسته از مجرمان برای این‌که کاربر به موضوع مشکوک نشود با قراردادن پیغام این‌که سیستم بانک قطع است اعتماد فرد را جلب می‌کنند. گاهی نیز بعد از ثبت مشخصات فرد را وارد سایت اصلی بانک می‌کنند.

۲-اسکمیر؛ روشی در حال فراگیرشدن

در این روش که اسکمیر نام دارد، مجرمان با قرار دادن مدارهای مغناطیسی در دستگاه‌های کارتخوان فروشگاه‌ها اطلاعات کارت‌های بانکی مشتریان را ذخیره می‌کنند و با تخلیه

اطلاعات از جمله رمز دوم، کارت بانکی جعلی ساخته و از حساب مشتری سرقت‌های میلیونی می‌کنند؛ البته براساس آمار پلیس فتا در این روش که در حال فراگیر شدن است، مجرمان ممکن است دستگاه اسکمیر را داخل کارتخوان‌های فروشگاه‌ها قرار داده و بدون اطلاع صاحب مغازه اطلاعات مشتریان آنها را سرقت کنند. راهکار مقابله با این تخلف، استفاده از کارت‌های بانکی هوشمند است که در صورت استفاده از آنها، میزان اسکیمینگ به صفر خواهد رسید.شبکه بانکی کشور و پرداخت از طریق پایانه‌های فروش برای کارت‌های مگنتی (فعلی) طراحی شده که تغییر آن برای استفاده از کارت‌های اسمارت طولانی و زمان‌بر است، زیرا باید زیرساخت‌ها و نرم‌افزارها تغییر کند.البته گفته می‌شود با توجه به قرار گرفتن در دوران تحریم در انتقال فناوری‌های مربوط به کارت‌های اسمارت و هوشمند محدودیت‌هایی وجود دارد. با این حال، بانک مرکزی تصمیمات لازم را برای رفع این مشکلات و ایجاد زیرساخت‌ها اخذ و به شبکه بانکی ابلاغ کرده است.

۳-کلاهبرداری نیجریه‌ای

کلاهبرداری نیجریه‌ای یکی دیگر از روش‌های سرقت اینترنتی است که در سال اول شناسایی، ۱۰ درصد جرایم اینترنتی کشور را به خود اختصاص داد. شاید معمولا طعمه‌های این روش تجار و بازرگانان هستند که به راحتی و برای لحظه‌ای غفلت میلیون‌ها و میلیاردها تومان سرمایه‌شان را به کلاهبرداران ناپیدا می‌دهند.در این روش که از سال ۹۰ در کشور ما با شکایت چند تاجر شناسایی شد مجرمان اینترنتی بانفوذ به نشانی پست الکترونیکی این افراد از دادوستد آن ها با شرکت‌های بین‌المللی باخبر می‌شوند. مجرمان ابتدا پست الکترونیکی مشابه شرکت با تغییراتی کوچک در یک یا دو حرف ساخته و با مشتری وارد گفت‌وگو می‌شوند.آن ها هنگامی که قرار است فرد خریدار پول را واریز کند با پست الکترونیکی جعلی شماره حساب خود را داده و فرد تاجر نیز که متوجه تغییر کوچک در نشانی پست الکترونیکی نمی‌شود،هزاران دلار را به حساب کلاهبرداران می‌ریزد.چند روزی که از واریز پول به حساب شرکت گذشت و تماسی با تاجر برقرار نمی‌شود او به موضوع مشکوک شده و در تماس با

شرکت متوجه کلاهبرداری و واریز پول به حساب کلاهبرداران به جای شرکت می‌شود. به دلیل فعالیت این کلاهبرداران در کشورهای دیگر شناسایی و دستگیری آنها امری محال است.سرهنگ حسین رمضانی معاون امور بین‌الملل پلیس فتا نیز در مورد این نوع کلاهبرداری به تپش می‌گوید: چون این جرم ابتدا از سوی اتباع کشور نیجریه رخ داد به این روش کلاهبرداری نیجریه‌ای می‌گویند. این جرم بیشتر از سوی اتباع آفریقایی در کشورهای جنوب و جنوب شرق آسیا رخ می‌دهد و با وجود تلاش شبانه‌روزی پلیس فتا هنوز هم تعدادی از پرونده‌های کلاهبرداری نیجریه‌ای به دلیل فرار مجرمان به کشورهای مختلف بی‌نتیجه مانده است.

۴-خالی کردن حساب با رسیدهای خودپرداز

جدیدترین روش کلاهبرداری سایبری در ایران با دستگیری متهمی سی ساله فاش شد. در این روش سارقان با برداشتن رسیدهای خودپرداز و شناسایی صاحب حساب با مراجعه به بانک با ارائه مدارک جعلی حسابی به نام فرد باز کرده و با دریافت کارت بانکی اقدام به برداشت غیرمجاز از طعمه خود می‌کنند. حامد مرد سی ساله‌ای که توسط پلیس فتا در تهران دستگیر شده است، در گفت‌وگو با خبرنگار تپش درباره استفاده از این شگرد گفت: با پرسه‌زنی در کنار دستگاه‌های خودپرداز رسیدهای بانکی جا مانده را نگاه می‌کردم و هر حسابی را که پول زیادی در آن بود، شناسایی و با مراجعه به بانک اطلاعات صاحب حساب را به دست می‌آوردم. سپس با مدارک جعلی درخواست عابربانک کرده و از این طریق طی چند مرحله حساب را خالی می‌کردم.

۵-کلاهبرداری به بهانه برنده شدن در قرعه‌کشی

این روش که جزو قدیمی‌ترین روش‌های کلاهبرداری است، هنوز هم قربانیان زیادی را می‌گیرد. در این روش کلاهبرداران سایت‌های قرعه‌کشی راه‌اندازی کرده و هر فردی را که به این سایت مراجعه کند، به عنوان برنده اعلام می‌کنند. سپس کلاهبرداران در تماس با قربانی خود مدعی می‌شوند او برنده صدها هزار تومان پول نقد در قرعه‌کشی شده و با گرفتن شماره

کارت مدعی می‌شوند پول به حساب فرد واریز می‌شود. شیادان اینترنتی پس از چند روز با قربانی تماس گرفته و مدعی می‌شوند پول به حساب آنها واریز شده و در صورتی که پول در حساب نیست طعمه با آنها تماس گرفته تا مشکل رفع شود.هنگامی که قربانی برای بررسی حساب مراجعه می‌کند، متوجه می‌شود پولی در حسابش نیست و با کلاهبرداران تماس می‌گیرد. در این لحظه متهمان با چرب‌زبانی طعمه خود را پای دستگاه خودپرداز کشانده و به جای واریز پول به حسابشان از حساب آن ها برداشت می‌کنند. تنها در یک پرونده در تهران شیادان موفق شده بودند از هزاران نفر به این شیوه کلاهبرداری کنند که با مراجعه چند مالباخته سرانجام اعضای چهار نفره این باند شناسایی و دستگیر شدند.میلاد، سردسته این باند که دارای مدرک تحصیلی دیپلم است و یک سابقه کیفری نیز در پرونده‌اش دارد، در مورد راه‌اندازی باند کلاهبرداری اینترنتی به روش قرعه‌کشی و شناسایی طعمه‌هایش به تپش گفت: همراه همدستانم با مدارک جعلی به آسانی در چند بانک حساب باز کردیم و با راه‌اندازی سایتی، از مراجعه‌کنندگان می‌خواستیم برای قرعه‌کشی شماره تلفن خود را در اختیار ما قرار دهند. پس از تماس با طعمه‌ها مدعی می‌شدیم آنها برنده شده‌اند، اما به دلیل مشکل فنی نمی‌توان پول را به حسابشان واریز کرد. با کمک سه هم دستم، مالباخته را پای دستگاه‌های خودپرداز می‌کشاندیم و سپس به جای واریز پول از حسابشان پول برداشت کرده و بلافاصله پول را از حساب خودمان خارج می‌کردیم.

۶-رشد قارچی سایت‌های شرط‌بندی

شرط‌بندی که در سال‌های دور در قهوه‌خانه‌ها انجام می‌شد، امروزه به سایت‌های اینترنتی راه یافته و کلاهبرداران سالانه میلیاردها تومان از این طریق به جیب می‌زنند. در این روش به دلیل این‌که از هر فرد بین ده تا صد هزار تومان کلاهبرداری می‌شود، افراد به خاطر مبلغ پایین و ترس از جرم شرط‌بندی از شکایت صرف‌نظر می‌کنند.

۷-پیشنهادهای شغلی

شاید در نگاه اول کلاهبرداری با چنین روشی کمی سخت و یا حتی ناممکن به نظر برسد. اما روش کار بدین ترتیب است که پیامی با مضمون پیشنهاد شغلی به قربانی داده می‌شود. در این پیام صاحب شرکت که در کشوری دیگر است، اعلام نیاز برای استخدام یک کارمند در کشو قربانی دارد. کلاهبرداران می‌گویند که کار پیشنهادی بسیار ساده و راحت است و کارمندان می‌توانند با صرف بازه زمانی ۳ تا ۴ ساعته در منزل به آن بپردازند و در صورتی که پیشنهاد همکاری آنها قبول شود،در روز مبلغی ۳۰۰۰ دلاری را پرداخت خواهند کرد. اما این‌ها فقط یک ادعای کذب است که از سوی ارسال کننده پیام صورت گرفته است. در صورتی که قربانی چنین پیشنهادی را قبول کند، در ادامه از وی اطلاعات بانکی اش خواسته می‌شود تا از این اطلاعات برای سرقت پول استفاده شود. پس از واریز پول به حساب کاربر، از او خواسته می‌شود تا آن مبلغ را از طریق شرکت وسترن یونیون ارسال نماید. با این کار کاربر قربانی فقط به یک دلال پول بدل خواهد شد و پس از فاش شدن ماجرا از جانب پلیس، قربانی هم به عنوان همدست شناخته می‌شود و قطعاً دستگیر خواهد شد. متاسفانه در این روش کلاهبرداران بسیار هوشیارانه عمل می‌کنند و با پنهان کردن هویت واقعی خود، افراد بی گناه را گرفتار می‌کنند.

۸-جعل اسناد خانه های بدون مالک

برخی از کلاهبرداران تمام وقت خود را در جست و جوی خانه‌های متروک و بدون مالک صرف می‌کنند. آن‌ها پس از پیدا کردن خانه‌هایی که خبری از صاحبانشان نیست، به جعل سند دست می‌زنند. آن‌ها عموما چنین خانه‌هایی را با قیمت پایین‌تر و ارزان‌تر از چیزی که در بازار است به افراد متقاضی خرید پیشنهاد می‌دهند.

۹-روش چارلز پونزی

چارلز پونزی نام ابداع کننده طرح شرکت‌های هرمی است. او با هوش سرشار اما منفی خود، توانست سایرین را مجاب کند تا بدون ارائه محصول و یا خدمتی، در شرکتش سرمایه گذاری کنند. این روش بعد از مدتی توسط شخصی دیگر به نام برنی مدوف دنبال شد و پس از آن در

سرتاسر جهان از جمله ایران شناخته شد و پس از مدتی با سرعت زیادی در تمامی نقطه‌های جهان رواج یافت. اما پلیس ایران توانست در مقابله با این شگرد موفق عمل نماید.[1]

بخش دوم: نگاه تقنینی به جرم کلاهبرداری رایانه ای

بر اساس آثار بعضی از حقوقدانان، گروهی بر این عقیده هستند که جرم کلاهبردار اینترنتی، ساختاری شبیه کلاهبردار سنتی دارد و نیاز به تعریف جدید و تغییر در دیدگاه جرمشناسی مرتبط با این دو نیست[2]. برخی نیز قائل به تفاوت در بحث پیشگیری و جرمشناختی فی مابین این دو جرم هستند[3]. به نظر می رسد، نظر گروه دوم با واقعیت همخوانی بیشتری دارد. دربارهٔ تاریخچه وقوع کلاهبرداری اینترنتی در ایران، با توجه به این که کاربرد کامپیوتر و اینترنت در ایران از ابتدای ورود آن تا دهه ۱۳۷۰ بسیار محدود بوده است، جرائم اینترنتی سابقه ی زیاد در ایران ندارد. طبق بررسی های انجام گرفته، وقوع جرم کامپیوتر به تدریج از دهه ی ۱۳۷۰ در ایران شروع شد که متأسفانه آمار دقیقی در این زمینه در دست نیست.از همین رو، قانونگذار در سال ۱۳۷۹ در برابر برخی جرائم کامپیوتر واکنش نشان داد و با الحاق تبصرهٔ ۳ به مادهٔ۱ قانون مطبوعات، مقرر کرد که «کلیات نشریات الکترونیکی مشمول مواد این قانون است». این قانون را می توان اولین واکنش قانونی ایران در برابر بعضی از جرائم کامپیوتری دانست. دومین واکنش قانونی ایران در مقابل جرائم کامپیوتری، وضع «قانون حمایت از حقوق پدیدآورندگان نرم افزارها رایانه ای » بود که در مجلس شورای اسلامی تصویب شد. ماده ۱۳ قانون یادشده،نقض حقوق پدیدآورندگان آن دسته از نرم افزارهای رایانه ای را که مورد حمایت این قانون قرار گرفته اند، جرم تلقی کرده است. سومین واکنش قانونگذار ایران در سال ۱۳۸۲،تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۹/۱۰/۹ توسط مجلس شورای اسلامی بود. بر اساس ماده ۱۳۱ این قانون، این قانون، جعل اطلاعات و داده ها رایانه ای،.... و سوءاستفاده ی مالی از طریق رایانه (کلاهبردار و اختلاس) توسط نظامیان جرم تلقی شده و

---

[1] . باشگاه خبرنگاران جوان،روش های کلاهبرداری در فضای مجازی،تاریخ انتشار:۲۸ خرداد ۱۳۹۵،کد خبری ۵۶۵۵۵۲۳

[2] . Brenner, 2010, p.73; Gercke, 2012, p.11; Chung, Schjolberg & Ghernaouti, 2011, p.4

[3] . Kleve et al., 2011, pp.162–167; Kerr, 2010, p.1584

مرتک حسب مورد، به مجازات جرم ارتکابی محکوم می شود. چهارمین واکنش قانونی، تصویب قانون تجارت الکترونیک مصوب ۱۳۸۲/۱۰/۱۷ مجلس شورای اسلامی بود.بر اساس ماده ۶۶،۶۷،۶۸،۶۹،۷۴،۷۵،۷۶،۷۷ این قانون،کلاهبرداری،جعل،دستیابی و افشای غیرمجاز اسرار تجاری و... از طریق رایانه قابل مجازات قرار گرفت.با این وجود نیاز به یک قانون جامع احساس می شد که در نهایت قانون جرایم رایانه ای در سال ۱۳۸۸ مورد تصویب قرار گرفت و در ماده ۱۳ خود،جرم کلاهبرداری را مورد بررسی قرار داد.در این ماده می خوانیم: «هر کس به طور غیرمجاز از سامانه های رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا توقیف کردن داده ها 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 سال تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد». با توجه به متن قانون مـذکور، مشخص می شود که قانونگذار ایران، تعریف کلاهبرداری اینترنتی را از شکل سنتی گرفته است، در صورتی که در دیگر کشورها به دلیل وجـود تفـاوت بـین موضـوع کلاهبرداری اینترنتی با نوع سنتی آن و همچنین کیفیات مجزا و متفاوت در شکل گیری این دو جرم، کلاهبرداری اینترنتی را جرمی با تعریف و ماهیت جداگانـه از کلاهبـرداری سنتی می دانند.در ماده ۶۷ قانون تجارت الکترونیک آمده است: «هرکس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده غیر مجاز از «داده‌پیام»ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسائل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف داده‌پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظائر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال ماخوذه محکوم می‌شود.

تبصره- شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرّر در این ماده می‌باشد» [1].

بهتر بود قانون گذار به یک تعریف در جرم کلاهبرداری رایانه ای با میزان مجازات یکسان می پرداخت تناقض و عدم مشابهت در قانون جرایم رایانه ای و قانون تجارت اکترونیک موجب گمراهی محاکم قضایی در استناد به قوانین نگردد.با این حال به نظر می رسد ماده ۱۳ قانون جرایم رایانه ای و ماده ۶۷ قانون تجارت الکترونیکی با هم قابل اعمال بوده و هیچ یک ناسخ دیگری نیست.این یکی از اشکالات قانونگذاری است که نیازمند بازنگری است.

بخش سوم: پیش گیری نظری

پیش گیری از جرم یک امر غریزی است. انسان بالفطره پیش گیرنده از جرم بوده، همین که انسان از زمانی که تاریخ به یاد دارد،به طور غریزی از خود دفاع به عمل می آورده است. خود این یک نوع پیش گیری به حساب می آید. پیش گیری به طور عمده دارای دو مفهوم است؛ هم به معنای پیش دستی کردن و به جلوی چیزی رفتن و هم به معنای آگاه کردن و هشدار دادن است. اما در جرم شناسی پیش گیرانه، پیش گیری در معنای اول آن مورد استفاده قرار می گیرد، یعنی با به کار بردن متد و روش های مختلف به منظور جلوگیری از وقوع بزهکاری، هدف به جلوی جرم رفتن و پیشی گرفتن از بزهکاری است. بر همین اساس علمای حقوق جزا و جرم شناسی، دو مفهوم از پیش گیری را مورد توجه قرار داده اند و به تعریف و تبیین آن پرداخته اند که یکی از آن ها، مفهوم موسع پیش گیری است و مقصود از آن هر اقدامی است که در مقابله با جرم و به منظور سد کردن ارتکاب آن باشد و جرم را کاهش دهد. طبق این تعریف از پیش گیری، می توان مواردی همچون مجازات بزهکار و ترمیم کردن خسارت وارد بر بزه دیده در فرآیند وقوع جرم را نام برد. این برداشت و استنباط از پیش گیری نزد افرادی همچون "انریکوفری" وجود داشته است؛ مقصود وی از این

۴.جلال انصاری،علیرضا انصاری،«نقد سیاست جنایی ایران در قبال کلاهبرداری اینترنتی»،حقوق جزا و سیاست جنایی،دورهٔ ۱ ،شمارهٔ ۱ ،بهار و تابستان ۱۳۹۵

اصطلاحات همان اقدامات پیشگیرانه غیرکیفری است که جایگزین مجازات و به عبارتی «هم عرض های کیفری» می باشند.(نجفی ابرنـدآبادی،۱۳۷۹،ص ۷۴۲) هم چنین "آنسلگ قاضی فرانسوی به این مفهوم تمایل دارد. در دیدگاه آنسـل، سیاسـت جنـایی بـه معنـای اعـم اولاً عـلاوه بـر جـرم، انحراف را نیز در بر می گیرد و علاوه بـر مجـازات بـه پیش گیری نیـز توجـه دارد؛ ثانیـاً علاوه بر نظام کیفری به تدابیر نظام اجتمـاعی نیـز توجـه دارد؛ ثالثـاً، سیاسـت جنـایی از مفهوم سیاست کیفری خارج شده و به مثابه سیاست عمومی یـک کشـور یـا یـک دولـت است. (لاژرز،۱۳۸۱.صص ۱۳-۱۵) خانم "می ری دلماس مارتی" یکی دیگر از دانشمندان است که به این مفهوم گرایش دارد. از دیـدگاه او، سیاسـت جنـایی ماهیت صرفاً کیفری ندارد و صرفاً از نظام های کیفری ناشی نمی شود ؛ بلکـه سـایر نظـام حقوقی مانند نظام حقوقی اداری، انضباطی، اجتماعی مالیاتی و... را نیز در بر مـی گیرد.ثانیاً، علاوه بر پاسخ های نهادهای رسمی دولت با رعایت تشـریفات خـاص علیـه پدیـده، پاسخ مجرمانه هـای منبعـث از جامعـه مـدنی و نهادهـای مختلـف مردمـی را نیـز دربـر می گیرد. ثالثاً، از دولت به کل پیکر اجتماع تعبیر می کند،بـه شـرط آنکـه بدنـه اجتمـاعی های خود را پاسخ سازماندهی کرده باشد؛ رابعاً، پدیده مجرمانه هم جـرم و هـم انحـراف را شامل می شود و در نهایت، سیاسـت جنـایی عـلاوه بـر سـرکوب کـردن و مجـازات، اقـدامات پیش گیرانه علیـه جـرم و انحـراف را نیـز شـامل مـی شود.(لاژرز،۱۳۸۱،صص ۱۷ و ۱۶؛رشادتی،۱۳۸۷.ص ۳۴۱) در مقابل مفهوم موسع پیش گیری، مفهوم مضیق قرار دارد که مقصود از آن مجموعه ابزار و وسایلی است که دولت برای مهار بهتر پدیده ی بزهکاری از دو طریق مورد استفاده قرار می دهد:اول از طریق حذف یا محدود کردن عوامل جرم زا و دوم از طریق اعمال مدیریت مناسب نسـبت بـه عوامـل محیطـی، فیزیکـی و اجتمـاعی کـه بـه نوبـه خـود فرصت های مناسبی را برای ارتکاب جـرم ایجـاد مـی کننـد.(نجفی ابراندآبادی،۱۳۷۹،ص ۷۵۰)مفهوم اخیر به وضعیت پیش گیری قبل از وقوع جرم اشاره می کند نه پس از آن. این مفهوم در نظریه ی تعدادی از حقوق دانان مورد پذیرش قرار گرفته است.از جمله این که:سیاست جنایی توسط " فویر باخ" در پایان قرن هجدهم،به "حکمت گرایی" در برخورد با جرم مربوط بوده و زاییده

ی آن است. این عبارت در مفهومی مضیق مبتنی بر "جرم و مجازات" و "قانون و قضا" بوده و به انحرافات اجتماعی توجهی نداشته است.هم چنین "فون لیست"،"کوش"،"دندی یود وابر" تعاریف سیاست جنایی را در مفهوم مضیق خود به کار برده و فقط مختص به سیاست کیفری و جرم می دانند.(نجفی ابرند آبادی،۱۳۸۱.ص ۷۵۰) به دلیل تأثیرعلوم مربوط به جرم شناسی در پیش گیری از جرم، گسترش و بعضاً به وجودآمدن شکل جدید جرائم و پیچیده ترشدن آن ها، مباحث مربوط به پیش گیری همیشه در حال تغییر و رو به رشد است.در مورد مفهوم پیش گیری،می بایست معنای موسع به واسطه ی نگاه جامع آن و پرداختن به جنبه های غیرکیفریپدیده ی پیش گیری مدنظر باشد. درباره نوع شناسی پیش گیری غیرکیفری در کلاهبردار اینترنتی باید به دو نوع آن اشاره کرد: پیش گیری اجتماعی و پیش گیری وضعی. پیش گیری اجتماعی را نیز می توان به دو دسته تقسیم کرد؛ پیش گیری اجتماعی رشد مدار که سعی دارد چنان چه هر شخصی به هر دلیلی از خود نشانه هایی از بزهکاری را بروز داد، از طریق مداخله هر چه سریع تر در خود وی و محیط اطرافش از مزمن شدن بزهکاری در آینده جلوگیری کند و پیش گیری اجتماعی جامعه مدار که در پی خنثی سازی عوامل جرم زا در محیط اجتماعی است.در پیش گیری اجتماعی،سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آن ها به ویژه قشر جوان و نوجوان جامعه و همچنین از بین بردن زمینه های اجتماعی وقوع جرم نظیر فقر و بیکاری، انگیزه های مجرمانه از مجرمان سلب شود (نجفی ابرندآبادی، ۱۳۸۲،ص۱۲۰۸) هم چنین شامل اقدام هایی است که به طور مستقیم یا غیرمستقیم، هدفشان تأثیرگذاری بر شخصیت افراد است تا از سازمان دادن فعالیت خود حول انگیزه های بزهکارانه بپرهیزند (گسن، ۱۳۷۰،ص۷۸) در جرایم سایبری،پیش گیری اجتماعی در قالب رشدمدار و جامعه مدار قابل اجرا است.در پیش گیری اجتماعی رشدمدار اینترنتی،نکته بسیار مهم در برخورد و مبارزه با جرائم اینترنتی به ویژه کلاهبرداری، استانداردهای فنی و اخلاق حرفه ای افراد است؛ بدین منظور که مسلماً زمانی می توان از افراد انتظار عملکرد درستی داشت که به خوبی به وی تفهیم شود که چه تدابیر امنیتی باید به کار گیرد و چه اخلاق شغلی را رعایت کند. (باستانی، ۱۳۹۰،ص۱۲۸)در پیش گیری

اجتماعی جامعه مدار سایبری،هدف،شکل گیری یا بروز انگیزه مجرمانه در عموم جامعه به وسیله ی دو اقدام اصلی است: یکی ایجاد علاقه و آسان سازی بروز افکار مشروع و مفید و دیگری بر حذر داشتن از ناهنجاری های اینترنتی. یکی از مهمترین راه های پیش گیری از کلاهبرداری اینترنتی به وسیله پیشگیری اجتماعی جامعه مدار سایبری از طریق آموزش های عمومی و رسانه های جمعی است. باید توجه داشت که اهمیت خاص تحقیق در زمینه رسانه و پیش گیری از وقوع جرم از آن روست که این وسیله تمامی زندگی انسان را در برمی گیرد. کارکرد رسانه های جمعی در مورد پیش گیری از کلاهبرداری اینترنتی می تواند از طریق آگاه کردن مردم از پیامدهای ناگوار این جرم چه بزهکار باشد و چه بزهدیده و نیز دادن الگوهای مناسب رفتاری جهت جلوگیری از ارتکاب و تکرار آن باشد که از این طریق می توانند نقش مهمی در پیش گیری از جرم داشته باشند. (دیندار و صدرنیا، ۱۳۸۸،صص۴۱-۴۰) همچنین، اثربخشی هر چه بیش تر انواع راه های پیش گیری ذکرشده نسبت به کلاهبرداری، نیازمند یک سیاست جنایی مشارکتی فعال است.کارکرد این نوع از سیاست جنایی نسبت به کلاهبرداری اینترنتی، اقدامات در مرحله کشف جرم، تعقیب دادرسی و اجرای حکم است که با همکاری وسیع جامعه مدنی، نهادهای مردمی و نیروهای دولتی مانند پلیس، سازمان زندان ها و غیره با دستگاه قضایی انجام می شود. (باصری، ۱۳۸۷،ص۳۷) برنامه هایی که در ایران مبتنی بر این نوع پیش گیری هستند، عموماً با محوریت مسئولیت دولت یا وزارت ارتباطات و فناوری اطلاعات و وزارت ارشاد است. برای اثربخشی بیشتر این نوع پیش گیری در کلاهبرداری اینترنتی، لازم است به سیاست جنایی مشارکتی بهای بیش تری داد و مردم را به عنوان عضوی مؤثر در این نوع پیش گیری وارد برنامه ها کرد که این امر نیز متأسفانه کمتر مورد توجه قرار گرفته است. در پیش گیری وضعی،اقدامات پیش گیرانه معطوف به اوضاع و احوالی است که جرائم ممکن است در آن وضعیت به وقوع بپیوندد. چنین اقداماتی در مورد جرم کلاهبرداری اینترنتی شامل روش هایی همچون مصونیت بخشی به آماج، نظارت بر مراکز ارائه دهنده اینترنت، فیلترینگ و غیره می شود. این نوع پیشگیری خود نیز دارای نقاط ضعف و قوت است، اما مجال توضیح

این موارد در این تحقیق نمی گنجد.مخاطبان اصلی پیش گیری وضعی از جرم کلاهبرداری اینترنتی، کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیش تر سعی می کنند با امکاناتی که فضای اینترنت در اختیار آن ها قرار می دهد مرتکب جرم شوند؛ نه اینکه خود دست به ابتکارعمل بزنند که در این صورت، کاری از پیش گیری وضعی جهت مقابله با جرم کلاهبرداری ساخته نخواهد بود.البته این نکته را نباید از یاد برد که علی رغم تأثیرات مثبتی که پیش گیری وضعی در برابر کلاهبرداری اینترنتی دارد، بعضاً به دلیل ماهیت این جرم دارای نقاط ضعف است؛ از جمله این محدودیت ها، هزینه بر بودن و زمان گیر بودن این اقدامات، تفاوت در میزان دانش طرفین نسبت به اینترنت و تفاوت در به کارگیری روش ها چه در جهت فیلترینگ و چه در جهت اقداماتی ضد آن. در نهایت، از جمله اقداماتی که مبتنی بر این نوع پیشگیری است می توان به این موارد اشاره کرد؛فیلترینگ، استفاده از پراکسیها، استفاده از رمز ورود، کنترل موجودی حساب و نظارت بر فضای مجازی[۱].

بخش چهارم: انواع سیاست جنایی ایران در برابر کلاهبرداری رایانه ای

به تعبیر لازرژکه تعریف نسبتاً خوبی از سیاست جنایی ارائه می دهد، در بردارنده ی مطالعه ی اقدامات و تدابیری است که دولت و جامعه ی مدنی به طور مستقل یا با مشارکت یکدیگر برای سرکوب پدیده ی مجرمانه،پیش گیری از آن و حمایت از بزه دیدگان مستقیم و غیر مستقیم است. بر اساس یک دسته بندی کلی،سیاست جنایی در سه دسته ی تقنینی،مشارکتی و قضایی تقسیم بندی می شود که در ادامه به آن خواهیم پرداخت.

۱-سیاست جنایی تقنینی ایران

سیاست جنایی تقنینی، وظیفه قانون گذاری در یک کشور است که در کشور ما بر اساس قانون اساسی بر عهده مجلس شورای اسلامی و در موارد خاص بر عهده نهادهای دیگر شده است. البته فرآیند قانون توسط مجلس انجام می شود اما در فرآیند تهیه و تنظیم

[۵] جلال انصاری،سعید عطازاده،محمود قیوم زاده.«سیاست جنایی ایران و آمریکا در قبال جرایم کلاهبرداری و سرقت سایبری»،فصلنامهٔ پژوهشهای اطلاعاتی و جنایی،سال چهاردهم شمارهٔ سوم، پاییز۱۳۹۸

یک پیش نویس قانونی تا تحقیقات علمی عوامل مختلفی نقش دارند.از جمله: افکار عمومی، روشنفکران، سازمان های مستقل، احزاب و و گرو ها برای آگاه سازی مردم، نحوه تصویب، نوع تصویب،مفاد قوانین گذشته و....(باصری،۱۳۸۷،ص ۳۶؛سوتهیل و دیگران،۱۳۸۳،ص ۲۰۲) در قوانین و مقررات مربوط به فضای سایبر، قانون گذار گاه به طور طور ضمنی و گاه به صریح به استفاده از تدابیر فنی جهت تحقق امنیت فضای سایبر پرداخته که در ذیل مورد اشاره قرار گرفته اند؛

۱-نخست مصوبات شورای عالی فضای مجازی است. این شورا به تاریخ ۱۷ اسفند ۱۳۹۰ به فرمان رهبری تشکیل و موظف گردید تا به طور کامل و روز آمد بر فضای درونی و بیرونی اینترنت اشراف داشته و امنیت این فضا را تأمین نماید.در مصوبه این شورا به شماره ۹۴/۱۰۰۱۵۱/ش مصوب ۱۳۹۴/۰۱/۳۰ به تعریف فضای مجازی امن پرداخته شده که بیان می دارد:

«فضای ایمن فضایی است متشکل از شبکه های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش های اسلامی و مقررات کشور ارائه می شود و کاربران می توانند بر اساس ویژگی های جمعیتی از قبیل شغل و جنس، یا سن، تحصیلات از محتوا و خدمات مورد نیاز بهره مند شوند و حتی الامکان در برابر محتوا و رفتارهای آسیب زا محفوظ بمانند». در عنوان این مصوبه هرچند به توسعه فضای مجازی سالم، مفید و ایمن پرداخته شده است اما در تعریفی که از فضای ایمن ارائه شده، به نظر می رسد فضای ایمن به لحاظ محتوایی یعنی فضایی که محتوای آن در چارچوب مبانی اسلامی باشد.در این مقرره قانون گذار صرفاً به پالایش محتوا توجه داشته در حالی که پالایه ی یک اقدام حفاظتی از اطلاعات در نظر گرفته نشده است. دلیل این امر این است که پالایه همواره از سوی مقامات دولتی و برای پاک سازی یک وب سایت یا سایت از اطلاعاتی که به لحاظ مضمون با مبانی اخلاقی و اسلامی ناسازگار اند به کار رفته و جنبه حفاظتی ندارد. در حالی که آن چه حفاظت از اطلاعات مالی مدنظر است این است که از اطلاعات مالی حفاظت به عمل

آیـد تـا ایـن اطلاعـات افشـاء، تخریب، محو نشوند که این حفاظت می تواند هم از سوی اشـخاص حقیقـی و هـم حقوقی باشد.

۲-در مصوبه دیگر این شورا با موضـوع سیاسـت هـای سـامان دهـی خـدمات پیـامکی ارزش افزوده و پیامک انبوه در شـبکه هـای ارتباطی به شماره ۹۳/۱۰۳۶۸۱/ش مصوب ۱۳۹۳/۱۱/۰۱ در بند ۴ آمده که بیان می دارد:

« به منظور حفظ و صیانت از اطلاعات خصوصـی مخاطبـان پیـام براساس قوانین به ویـژه قـانون جـرائم رایانـه ای،ارائه دهنـدگان خـدمات ارتبـاطی و ارائه دهندگان خدمات محتوایی حق واگـذاری،فـروش و یـا در اختیـار قـرار دادن ایـن اطلاعات به دیگران را ندارند». در این مصوبه به حفاظت و حمایت از اطلاعات اشاره شده است. اما تنها به حفاظـت از اطلاعـاتی کـه مربـوط بـه حـریم خصوصـی شهروندان است، پرداخته شده و به اطلاعات مالی بـه طـور خـاص تـوجهی نشـده اسـت. دلیل این امر چندان مشخص نیسـت، امـا بـه نظـر مـی رسـد یـا وصف اطلاعات مالی برای مقنن ناشناخته بوده و این از رو حمـایتی از ایـن اطلاعـات بـه عمل نیاورده و یا اطلاعات مالی را نیز بخشی از اطلاعات شخصی افراد قلمـداد نمـوده و آن ها را همانند اطلاعات شخصی مشمول حمایت قرار داده است. بـه ایـن اسـتدلال ایـن اشکال وارد می شود که اولاً از اطلاعات مالی اشخاص حقـوقی در ایـن قالـب نمـی تـوان حفاظت نمود؛ ثانیاً اقداماتی که جهت حفاظت از اطلاعات شخصـی بـه عمـل آمـده، تدابیر واسطه ای هستند. تدابیری هستند کـه در پـی تنظیـم مقـررات مناسـب از حفاظت از اطلاعات شکل گرفته اند.

۳-مصوبه دیگر این شورا در خصوص طرح های کلان مرکز ملـی فضـای مجـازی کشور جهت تدوین لایحـه در تصـویب بودجـه و نامـه ایـن شـورا در خصـوص شـرح وظایف، اختیارات و اعضای کمیسیون عالی فضای مجـازی بـه ارتقـای امنیـت سـایبری است، اما هیچ سخنی از چگونگی حفاظت از اطلاعات مالی میان نیامده است.در این مصوبه قانون گذار به تولید محتـوای فضـای مجـازی بـه صـراحت توجـه نموده است در حالی که مفهوم امنیت و ابعاد آن در اینجـا تشـریح نشـده اسـت.

۴-مصوبه دیگر این شورا در خصوص تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه درسال ۱۳۹۳ است که در بند چهارم مقرره دوم به ایجاد شبکه ای با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتال پرداخته است. در این مقرره، قانون گذار تنها به امنیت شبکه توجه داشته و اشاره ای به امنیت اطلاعات نکرده است.امنیت شبکه به فرآیند ایمن سازی گفته می شود که که طی آن یک شبکه با استفاده از استانداردهای امنیتی در مقابل انواع مختلف تهدیدات اعم از داخلی و خارجی امن می شود.با این حال در امنیت شبکه، متخصصان بیشتر بر عملکرد صحیح سیستم کامپیوتری تمرکز دارند؛ در حالی که در امنیت اطلاعات،بیش تر تأکید بر حفاظت از اطلاعات خصوصاً اطلاعات با ارزش اشخاص است تا در پرتو این حفاظت بتوان از ضررهای هنگفتی که ممکن است در اثر رفتارهای مخرب به اشخاص وارد آید جلوگیری نمود. تدابیر پیشنهاد شده در این ماده جهت خدمت رسانی امن به کاربران، همگی در قالب تدابیر پیش گیری از میان تدابیر فنی، تنها به رمزنگاری و امضای دیجیتال اشاره شده، در حالی که این دو راهکار بیش تر جهت تأمین امنیت اطلاعات خود و نه شبکه در معنی یاد شده به کار می رود. از این رو بهتر بود مقنن به طور تمثیلی به این تدابیر می پرداخت تا این که بتواند امنیت شبکه را در قالب این اقدامات به طور کامل تأمین سازد.

۵-در مصوبه دیگر این شورا تحت عنوان سیاست های حاکم در بند ۱۰ به حفظ حریم خصوصی و حمایت از حقوق مصرف کننده اشاره شده، اما تدابیر واسطه ای پیش بینی شده در این بند نیز تنها ناظر به حفظ حریم خصوصی است و اطلاعات ما لی اشخاص حقوقی تحت شمول این مقرره قرار نمی گیرند. با این حال حمایت از حقوق مصرف کننده می تواند شامل حمایت از اطلاعات مالی مشتریان نیز شود که این مشتریان می توانند هم اشخاص حقوقی هم و اشخاص حقیقی باشند. در مقررات و ضوابط شبکه اطلاع رسانی رایانه ای مصوب قانون ۱۳۸۰ قانون گذار در بند ب ماده ۶ به استفاده از تدابیر فنی جهت صیانت از شبکه ها و اطلاعات تصریح کرده است.در این بند آمده است:

«سیستم بارو مناسب به منظور صیانت شبکه ها از تخریب،فریب و سرقت اطلاعات به کار می رود».در این مقرره قانون گذار به تآمین اطلاعات به طور صریح پرداخته است.اطلاعات موجود در این متن مطلق و شامل اطلاعات مالی و غیرمالی می گردد. در این مقرره تنها به حفاظت از اطلاعات سرقت،فریب و تخریب اشاره شده،در حالی که بهتر بود مقنن به حفاظت از اطلاعات در برابر تهدیدات به نحو مطلق اشاره کند. راهکار فنی ارائه شده در این ماده نیز تنها فایروال است و مقنن به سایر تدابیر فنی وقعی ننهاده است.در آیین نامه ارائه دهنده ی خدمات اطلاع رسانی و اینترنتی در ماده ۸-۳-۵ استفاده از تدابیر فنی جهت تبادل اطلاعات در فضای سایبر را منوط به موافقت مرجع ثبت اطلاعات نموده است. قانون گذار استفاده از این تدابیر را تنها جهت انتقال و مبادله اطلاعات در سیستم پیشنهاده داده و مشخص نیست که آیا یک شخص حقیقی یا حقوقی می تواند اطلاعات خود را در سیستم با استفاده از الگوریتم رمزنگاری ذخیره سازد، حتی اگر قصد تبادل آن اطلاعات را نداشته باشد؟ اطلاعات به کار رفته در این متن نیز مطلق و شامل اطلاعات مالی و غیرمالی می گردد.در این بند آمده است: «به کارگیری هرگونه رمز برای تبادل اطلاعات مستلزم کسب موافقت مراجع مربوط و ثبت مشخصات، الگوریتم و کلید رمز مربوط و همچنین مشخصات متقاضی در دبیرخانه شورای عالی اطلاع رسانی یا مرجعی که معرفی می نماید، بوده،در غیر این صورت ممنوع است». در سایر موارد این آیین نامه نیز به حفظ و حراست از حریم خصوصی اطلاعات و ارتباطات اشاره شده که پیش تر قانون گذار،تدابیر واسطه ای را پیش بینی نموده و تنها اطلاعات خصوصی را ملحوظ نظر قرار داده است. در بند ه ماده ۱ آیین نامه استنادپذیری ادله الکترونیک مصوب ۱۳۹۰ آمده است:

« برای حفاظت از داده ها باید زنجیره حفاظتی ایمن که امکان ردیابی داده ها را از مبدأ تا مقصد فراهم می سازد،در نظر گرفت».

در ماده ۳۸ این آیین نامه نیز به روش توقیف داده ها پرداخته که اکثر راهکارهای ارائه شده در این مقرره تدابیر فنی در این ماده اند. در این ماده واژه به طور مطلق استعمال شده و

می توانـد هم ناظر به اطلاعاتی که در مورد حریم خصوصی است و هم اطلاعـات مـالی باشد؛ امـا نکته قابل توجه این است که هرچند قانون گذار به استفاده از تدابیر فنـی جهـت حفاظـت مطلق ازاطلاعات پرداخته است، اما این ماده ناظر بـه اطلاعـاتی اسـت کـه جنبـه اثبـاتی دارند و قرار است به عنوان ادله الکترونیک مورد اسـتفاده قـرار گیرنـد. در قـوانین موجـود در حوزه فضای سایبر نیز به بحث حمایت از اطلاعات پرداخته شده اسـت.برای نمونه در ماده ۴۰ قانون جرایم رایانه ای آمده است: «در توقیف داده ها با رعایت تناسب،نوع،اهمیت و نقش آن ها در ارتکاب جرم به روش هایی از قبیل چاپ برداری،کپی غیـر قابـل دسـترس کردن داده ها با روش هایی از قبیل تغییر گذرواژه یا رمزنگـاری عمـل مـی شود».

واژه " از قبیل" نشان می دهد تدابیر فنی ذکر شـده در ایـن مـاده حصـری نیسـتند و تمثیلـی اند.می توان از سایر تدابیر فنی نیز در توقیف داده ها استفاده کرد. تدابیر فنی پـیش بینـی شـده در این ماده جهت حفظ و حراسـت از داده هـایی مـورد اسـتفاده قـرار مـی گیرنـد کـه در کشف یا اثبات این جرایم به کار می روند. از این رو به کار بردن این تدابیر یک اقـدام تمهیـداتی قضایی یا اقدام چاره ساز است و نه یک تدبیر پیش گیرانه غیر کیفری که اختصاصاً بـرای حفاظت از اطلاعات مالی پیش از ارتکاب جرم به کار می رود. این تدابیر بـرای توقیـف تمـام داده ها صرف نظر از مالی یا غیرمالی بودن استفاده می شوند[۱].

۲-سیاست جنایی قضایی ایران

این نوع سیاست جنایی از میان رویه های مختلف قابل استنباط است کـه قـوه قضـاییه در رأس این نهادها با رویکرد پیش گیرانه اقدام به آن می نماید. اما در کنار آن، نهادهـای دیگـر نیز می توانند با قوه قضـائیه همکـاری کننـد.قانون اساسی در بند ۵ اصل ۱۵۶، اقـدام مناسب برای پیش گیری از جرم را وظیفه قوه قضائیه دانسته است.با توجه به بند ۴ این اصل، به نظر می رسد قانون گذارکیفـری در قانون اساسی بـه دنبـال پیش گیری بوده است.همان طور که در

[۱]. امیر وطنی،حمید اسدی،۱۳۹۵ ،،سیاست جنایی جمهوری اسلامی ایران در جرایم سایبری با تأکید بر ویژگی های خاص این جرایم، پژوهشنامه حقوق اسلامی،سال هفدهم،شماره اول(پیاپی ۴۳)

مفهوم شناسی پیش گیری گفته شد، پیشگیری به معنای مانع ایجاد جرم شـدن اسـت و در سـه مرحلـه پـیش از وقـوع جـرم، وقوع جرم، و پس از آن جایگاه دارد. از یک دیدگاه می توان گفت قوه قضاییه تنهـا پـس از وقوع جرم وارد می شود و وظیفه پیش گیری از جرم بـه معنـای خـاص آن را بـر عهـده ندارد ؛چرا که پیشگیری برعهده مقامات اجرایی است. پیش گیری در برنامـه کوتـاه مدت وظیفه دستگاه های انتظامی است که این قوا از طریـق گشـت هـای پلیسـی متفـرق کـردن افراد شرور و... به پیش گیری می پردازند و یـا پیش گیری در برنامـه بلند مـدت کـه همـان پیش گیری اجتماعی است،از وظایف مربوط به آموزش و پرورش و رسانه های ارتباط جمعی است. آن ها معتقدنـد، قـوه قضـائیه بـرای پیش گیری از وقـوع جـرم نقـش مدیریتی دارد و سیاست گذاری می کند، اما اجرای سیاست ها بـر عهـده نهادهـای اجرایـی بر عهده ی نهاد های اجرایی است. تدابیری که قوه قضائیه در این جایگاه از آن استفاده می کند، شامل مواردی چون اتخاذ تدابیر بازپرورانه، مشاوره درمانی، مددکاری، کاهش عناوین کیفری، زندان زدایـی و اعمـال مجازات های جایگزین زندان، بازگرداندن زندانی به دامان خـانواده، بـازپروری زنـدانیان، بسترسازی برای ایجاد اشتغال در زندان، آزادی مشـروط از زنـدان، کیفرزدایـی کـه جـزء سیاست های استراتژی توسعه ی قضایی است می باشد. در مرحلـه پـیش از وقـوع جـرم نیـز قـوه قضـائیه بـا هـدف پیش گیری از جـرم از راهکارهایی چون تأمین عدالت و رفاه اجتماعی، مبارزه با فقر و گرفتـاری، تـأمین امنیـت اجتماعی با استفاده از سـازوکارهای ارعـابی و بازدارنـده، حمایـت از خـانواده، بـا جلـب همکاری دستگاههای مختلف دولتی و غیردولتی ماننـد مـدارس، رسـانه هـای هـا، سـازمان غیردولتی، تشکلهای مردمی، پلیس و خود مـردم، دامنـه آمـوزش را بـه همـه نهادهـای اجتماعی گسترش داده و به مقابله با جرم می پردازد. در کنار قوه قضائیه مراکز بی شماری در عرصه فضـای سـایبر فعالیـت مـی کنند که از جمله آن عملکرد این مراکز نیز بعدی پیش گیرانه دارد.می تـوان بـه مرکـز مـاهر(مرکز مدیریت امداد و هماهنگی امور رخداد) و مرکز آپا(مرکز آگاهی رسانی،پشتیبانی و امداد رایانه ای) اشاره کرد.مرکز ماهر در سال ۱۳۸۵ شکل گرفت و به سیاست گذاری و توسعه و بهینـه سـازی روش هـای امنیتـی، بررسـی امکانـات بالقوه ایجاد

امنیت در فضای تبادل اطلاعات کشور و کمک به بالفعل نمودن این امکانات، کمک به تشکیل گروه های ضربت جهت حفاظت از امنیت اطلاعات و شبکه می پردازد.با تدقیق در وظایف این مراکز متوجه می شویم که این مرکز بیش تر تدابیر پیش گیرانه را در قالب تدابیر پیش گیرانه اجتماعی از جمله هشداردهی وآگاه سازی عمومی جهت حفاظت از اطلاعاتی که تنها مربوط به حریم خصوصی شهروندان است،و افراد آن اطلاعات را در شبکه های اجتماعی خود بارگذاری نموده توجه داشته است و از توجه به وصف اطلاعات مالی و حتی هشدار در خصوص حفاظت از این اطلاعات غافل مانده است.مرکز آپا نیز در سال ۱۳۸۶ زیر نظر دانشگاه امیرکبیر شکل گرفت.این مرکز با استفاده از تکنولوژی مناسب امنیت اطلاعات را در مقابل حملات سایبری تأمین می کند.این مرکز نیز همانند ماهر به شهروندان هشدارهایی برای حفاظت از اطلاعاتشان در فضا ی سایبر می دهد اما این امر نافی اقدامات فنی این مرکز در حفاظت مطلق از اطلاعات نیست؛چرا که به دلیل اقدامات مهندسی بیش تر در حوزه ی فنی فعالیت دارد.پلیس فتا یا سایبر که با هدف حفاظت از اطلاعات مالی زیر نظر نیروی انتظامی شکل گرفت، هدف اصلی آن مقابله با جرایم سایبری و حفاظت از اطلاعات بر روی شبکه اینترنت است.این نهاد به دو پلیس ستادی و عملیاتی تقسیم می گردد.پلیس های ستادی بنا به دستور مقام قضایی به رصد سایت ها یا درگاه های الکترونیکی در صورت مجرمانه بودن محتوای این سایت ها یا صورت گرفتن یکی از جرائم مندرج در قانون پرداخته و به مراجع قضایی اطلاع می دهند. اما هیچ تدبیر فنی جهت حفاظت از اطلاعات مالی اتخاذ نکرده است و تنها به هشداردهی و آگاه سازی عمومی از فواید و مضرات فضای سایبر بسنده کرده که بیشتر این هشدارها در خصوص حفظ حریم خصوصی است. پلیس های عملیاتی نیز ماهیت عملکردشان اساساً پیگیری است و نه پیش گیری در معنای خاص. این گروه از پلیس بنا به دستور مقام قضایی در صورت تحقق یافتن جرم سعی در اعمال تدابیر واکنشی از جمله فیلتر نمودن سایت می کنند و اقداماتشان بیش تر واکنشی و در جهت پالایه محتوا است.

۳- سیاست جنایی مشارکتی ایران

در این نوع سیاست جنایی برای مبارزه با جرم،از ابزار و وسایل دولتی و غیر دولتی استفاده می گردد.برای اعمال آن می توان از طرق مختلف مانند فرهنگ سازی و آموزش بهره برد. در اصل هشتم قانون اساسی اشاره شده که امر به معروف و نهی از منکربه مفهوم دینی، وظیفه ای همگانی و متقابل بر عهده مردم نسبت به یکدیگر، دولت نسبت به مردم و مردم نسبت به دولت شناخته شده است.این یعنی مطابق دستورات اسلام نیز این نوع سیاست به چشم می خورد. در واقع احکام امر به معروف و نهی از منکر با هدف پیش گیری از انحرافات اخلاقی و جرم در جامعه تعیین شده که به تعبیر جامعه ی اسلامی عبارت "گناه" برای آن به کار برده می شود.

بخش پنجم: طرق نظارت بر جرایم کلاهبرداری اینترنتی

از طرق نظارت بر جرائم سایبری توسط نهادهای مدنی و اشخاص و مشارکت مردم که می تواند مصداقی از امر به معروف و نهی از منکر باشد و موجب پیش گیری از جرائم سایبری شود، مربوط به نظارت بر ورودی هاست که سعی می کنند از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری کنند.راه های گوناگونی برای کنترل عبوری ها وجود دارد که یکی از آن ها استفاده از رمز عبور در رایانه است. بدیهی است که بالا بردن ضریب کنترل می تواند در برابر مجرمان به مثابه انگیزه عمل کند و آنها را در دستیابی به آماج جرم ناکام بگذارد. از دیگر راه های کنترل ورودی،استفاده از شبکه های مجازی کاوشگر الکترونیک است. این کاوشگرها که از آن ها به پلیس مجازی تعبیر می شود، وظیفه کنترل دسترسی به اطلاعات مالی را بر عهده دارند.علاوه بر نظارت ورودی،نظارت خروجی نیز اهمیت دارد.این نوع نظارت به صورت دو نظارت هم زمان و غیرهمزمان صورت می گیرد.در نظارت هم زمان،ابزار الکترونیکی،متصدی مربوطه را از فعالیت غیرمجاز شخص در دسترسی به اطلاعات مالی در همان زمان آگاه می کند و او می تواند اقدامات پیش گیرانه لازم را نسبت به او به عمل بیاورد.در حالت دوم بسته به میزان دقت ابزار نظارتی،صرفاً بخش گزینش شده ای از فعالیت این اشخاص ثبت می شود تا در فرصتی دیگر با بررسی آن ها موارد

غیر مجاز دسترسی اشخاص به اطلاعات مالی مشخص گردد.در این کنترل برنامه هایی روی سیستم شخص نصب می شود که از روی ضربه زدن بر صفحه کلید کیبورد یا کلیک روی نقاطی که با موس اشاره شده،نظارت لازم صورت می گیرد. در این کنترل، تمامی راهکارهای نظارتی در مورد خروج اطلاعات مالی مد نظر قرار گرفته و تمامی اطلاعات مالی ذخیره شده دارای کدبندی مشخصی می شوند و بدین ترتیب از تمامیت آن ها حفاظت می شود. نرم افزار ضدپایش نیز نوعی آنتی ویروس است که از اطلاعات مالی در برابر ویروس ها محافظت می کند.مهم ترین قسمت موتور اسکن آن است. جزئیات عملکرد هر موتور متفاوت است ولی همه آن شناسایی فایل ها وظیفه های آلوده به ویروس را بر عهده دارند که اغلب در لابه لای اطلاعات مالی بارگذاری شده اند. در بیش تر موارد در صورتی که فایل آلوده به ویروس باشد ضد ویروس قادر به پاک سازی و از بین بردن آن می باشد.این نرم افزارها به دو دسته نرم افزار نظارت و اسکن تقسیم می شوند. نرم افزار نظارت صرفاً اقدام به تشخیص ویروس ها و بلاک آن ها می کند ولی نرم افزار اسکن،ویروس های کشف شده را نه تنها از فایل اطلاعات مالی بلکه از کل سیستم پاک می نماید.[1]

نتیجه گیری

کلاهبرداری رایانه ای یکی از جرایمی است که در یکی دو دهه ی اخیر به دلیل گسترش فضای اینترنت و شبکه های اجتماعی،بخش بزرگی از جرایم امروز را به خود اختصاص می دهد.دولت ها با سیاست های مختلف حاکمیتی سعی در کنترل و مجازات مرتکبان آن دارند.ایران به دلیل مشکلات عدیده به عنوان یکی از کشورهای جهان سوم و تحمل تورم و تحریم های اقتصادی در قرن بیست و یک شاهد تعداد زیادی از این جرایم بوده و با آن به مبارزه پرداخته،اما به دلایل مختلفی در کاهش این نوع جرم ناموفق عمل کرده است. کلاهبرداری رایانه ای از کلاهبرداری سنتی متمایز بوده و نسبت به آن جرم انگاری با نگاه جدیدی صورت گرفته است. در کلاهبرداری رایانه ای امکان فریب دستگاه ها و سیستم های

[1] .همان

پردازش خودکار جداگانه یا با وجود کاربران هر دو امکان پذیر است. در این جرم سوءاستفاده از داده های برنامه و سیستم های کامپیوتری از راه دور در جهت کسب سود و منفعت بیش تر صورت می گیرد و اغلب کلاهبردار و قربانی با هم روبه‌رو نمی شوند.

دربارهٔ تاریخچه وقوع کلاهبرداری اینترنتی در ایران، با توجه به این که کاربرد کامپیوتر و اینترنت در ایران از ابتدای ورود آن تا دهه ۱۳۷۰ بسیار محدود بوده است، جرائم اینترنتی سابقه ی زیاد در ایران ندارد. طبق بررسی های انجام گرفته، وقوع جرم کامپیوتر به تدریج از دهه ی ۱۳۷۰ در ایران شروع شد که متأسفانه آمار دقیقی در این زمینه در دست نیست.از همین رو، قانونگذار در سال ۱۳۷۹ در برابر برخی جرائم کامپیوتر واکنش نشان داد و با الحاق تبصرهٔ ۳ به مادهٔ۱ قانون مطبوعات، مقرر کرد که «کلیات نشریات الکترونیکی مشمول مواد این قانون است». این قانون را می توان اولین واکنش قانونی ایران در برابر بعضی از جرائم کامپیوتری دانست.امروزه شیوه های مختلفی برای فریب افراد در فضای مجازی طراحی و اجرا می گردد.یکی از شایع ترین جراییم در این ارتباط،فیشینگ است.با راه اندازی سایت های مختلف جعلی و تبلیغات گوناگون در فضای مجازی و ارسال پیامک به شهروندان با موضوعات مختلف از قبیل ثبت نام برای جلوگیری از قطع یارانه ها،اختصاص سهمیه بنزین، دریافت مجوز طرح تردد زوج و فرد و سایر مواردی که بسته به موقعیت احتمال مطرح شدن آن ها نیز از سوی فرد کلاهبردار وجود دارد،اقدام به فریب دادن قربانیان برای دریافت هزینه ارائه این خدمات می کنند.شیوه های دیگری از جمله:اسکیمر،سایت های شرط بندی،جعل اسناد خانه های بدون مالک،برنده شدن در قرعه کشی،پیشنهاد شغلی و موارد دیگری است که منجر به ازدیاد این نوع جرم شده است.برای کنترل آن نیاز است تا دولت ها با اتخاذ تدابیر مناسب و متناسب با شرایط روز و آگاهی بخشی عمومی و هم چنین آموزش حفظ اطلاعات شخصی افراد،از افزایش بی رویه ی آن جلوگیری نماید.این پیش گیری نیازمند اتخاذ سیاست های جنایی ابتکاری و خلاقانه از سوی هر حکومت یا الگوبرداری از حکومت های موفق است.

با توجه به تعریف جرم کلاهبرداری اینترنتی در قانون جرایم رایانه ای و قانون تجارت الکترونیک مشخص می شود که قانونگذار ایران، تعریف کلاهبرداری اینترنتی را از شکل سنتی گرفته است، در صورتی که در دیگر کشورها به دلیل وجود تفاوت بین موضوع کلاهبرداری اینترنتی با نوع سنتی آن و همچنین کیفیات مجزا و متفاوت در شکل گیری این دو جرم، کلاهبرداری اینترنتی را جرمی با تعریف و ماهیت جداگانه از کلاهبرداری سنتی می دانند.هم چنین بهتر بود قانون گذار به یک تعریف در جرم کلاهبرداری رایانه ای با میزان مجازات یکسان می پرداخت تناقض و عدم مشابهت در قانون جرایم رایانه ای و قانون تجارت اکترونیک موجب گمراهی محاکم قضایی در استناد به قوانین نگردد.با این حال به نظر می رسد ماده ۱۳ قانون جرایم رایانه ای و ماده ۶۷ قانون تجارت الکترونیکی با هم قابل اعمال بوده و هیچ یک ناسخ دیگری نیست.این یکی از اشکالات قانونگذاری است که نیازمند بازنگری است. در نظریات پیش گیری،دو مفهوم مضیق و موسع مورد نظر جرم شناسان بوده که معنای موسع آن به دلیل نگاه جامع و اتخاذ سیاست های غیر کیفری و درمان علاوه بر بازدارندگی کیفری مورد نظر ما است. درباره نوع شناسی پیش گیری غیرکیفری در کلاهبردار اینترنتی باید به دو نوع آن اشاره کرد: پیش گیری اجتماعی و پیش گیری وضعی.

در جرایم سایبری،پیش گیری اجتماعی در قالب رشدمدار و جامعه مدار قابل اجرا است.

کارکرد رسانه های جمعی در مورد پیش گیری از کلاهبرداری اینترنتی می تواند از طریق آگاه کردن مردم از پیامدهای ناگوار این جرم چه بزهکار باشد و چه بزهدیده و نیز دادن الگوهای مناسب رفتاری جهت جلوگیری از ارتکاب و تکرار آن باشد که از این طریق می توانند نقش مهمی در پیش گیری از جرم داشته باشند. همچنین، اثربخشی هر چه بیش تر انواع راه های پیش گیری ذکرشده نسبت به کلاهبرداری، نیازمند یک سیاست جنایی مشارکتی فعال است.کارکرد این نوع از سیاست جنایی نسبت به کلاهبرداری اینترنتی، اقدامات در مرحله کشف جرم، تعقیب دادرسی و اجرای حکم است که با همکاری وسیع جامعه مدنی، نهادهای مردمی و نیروهای دولتی مانند پلیس، سازمان زندان ها و غیره با

دستگاه قضایی انجام مـی شود. برنامه هایی که در ایران مبتنی بر این نوع پیش گیری هستند، عموماً با محوریت مسئولیت دولت یـا وزارت ارتباطـات و فنـاوری اطلاعات و وزارت ارشاد است. برای اثربخشی بیشتر این نوع پیش گیری در کلاهبـرداری اینترنتی، لازم است به سیاست جنایی مشارکتی بهای بیش تری داد و مردم را بـه عنـوان عضوی مؤثر در این نوع پیش گیری وارد برنامه ها کرد که این امر نیز متأسفانه کمتر مـورد توجه قرار گرفته است.در مورد پیش گیری وضعی، علی رغم تأثیرات مثبتی که پیش گیری وضعی در برابـر کلاهبرداری اینترنتی دارد، بعضاً به دلیل ماهیت این جرم دارای نقاط ضعف است؛ از جمله این محدودیت ها، هزینه بر بودن و زمان گیر بودن ایـن اقـدامات، تفـاوت در میـزان دانش طرفین نسبت به اینترنت و تفاوت در به کارگیری روش ها چه در جهت فیلترینگ و چه در جهت اقداماتی ضد آن. در نهایـت، از جملـه اقـداماتی کـه مبتنـی بـر ایـن نـوع پیشگیری است می توان به این موارد اشاره کرد؛فیلترینگ، استفاده از پراکسیها، استفاده از رمز ورود، کنترل موجودی حساب و نظارت بر فضای مجازی.

سیاست جنایی لازم در مورد جرم کلاهبرداری رایانه ای در سه دسته ی کلی قانونی،قضایی و مشارکتی قابل اعمال است که از این میان،سیاست تقنینی و مشارکتی از اهمیت بیش تری در بخش پیش گیری کنشی برخوردار است. در این نوع سیاست جنایی برای مبارزه با جرم،از ابزار و وسایل دولتی و غیر دولتی استفاده می گردد. سیاست جنایی تقنینی، وظیفـه قـانون گـذاری در یـک کشور است که در کشور ما بر اساس قانون اساسی بر عهـده مجلـس شـورای اسـلامی و در موارد خاص بر عهده نهادهای دیگر شـده اسـت. البتـه فرآینـد قـانون توسط مجلس انجام می شود امـا در فرآینـد تهیـه و تنظـیم یـک پـیش نـویس قـانونی تـا تحقیقات علمی عوامل مختلفی نقش دارند.از جمله: افکار عمومی، روشنفکران، سـازمان هـای مستقل، احزاب و و گرو ها برای آگاه سـازی مـردم، نحـوه تصـویب، نـوع تصویب،مفاد قوانین گذشته و.... در بیش تر موارد قانون گذاری،قـانون گـذار ایرانی بـه پـالایش محتـوا توجـه داشـته در حالی که پالایه ی یک اقدام حفاظتی از اطلاعات در نظر گرفته نشده است. دلیـل این امر این است که پالایه همواره از سوی مقامات دولتی و بـرای پـاک سـازی یـک وب

سایت یا سایت از اطلاعاتی که به لحاظ مضمون با مبانی اخلاقی و اسلامی ناسازگار اند به کار رفته و جنبه حفاظتی ندارد. در حالی که آن چه حفاظت از اطلاعات مالی مدنظر است این است که از اطلاعات مالی حفاظت به عمل آید تا این اطلاعات افشاء، تخریب، محو نشوند که این حفاظت می تواند هم از سوی اشخاص حقیقی و هم حقوقی باشد.

در سیاست مشارکتی که برای اعمال آن می توان از طرق مختلف مانند فرهنگ سازی و آموزش بهره برد. در اصل هشتم قانون اساسی اشاره شده که امر به معروف و نهی از منکربه مفهوم دینی، وظیفه ای همگانی و متقابل بر عهده مردم نسبت به یکدیگر، دولت نسبت به مردم و مردم نسبت به دولت شناخته شده است.این یعنی مطابق دستورات اسلام نیز این نوع سیاست به چشم می خورد. در واقع احکام امر به معروف و نهی از منکر با هدف پیش گیری از انحرافات اخلاقی و جرم در جامعه تعیین شده که به تعبیر جامعه ی اسلامی عبارت "گناه" برای آن به کار برده می شود.

از طرق نظارت بر جرائم سایبری توسط نهادهای مدنی و اشخاص و مشارکت مردم که می تواند مصداقی از امر به معروف و نهی از منکر باشد و موجب پیش گیری از جرائم سایبری شود، مربوط به نظارت بر ورودی هاست که سعی می کنند از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری کنند.راه های گوناگونی برای کنترل عبوری ها وجود دارد که یکی از آن ها استفاده از رمز عبور در رایانه است. از دیگر راه های کنترل ورودی،استفاده از شبکه های مجازی کاوشگر الکترونیک است. نرم افزار ضدپایش نیز نوعی آنتی ویروس است که می تواند از اطلاعات مالی کاربران در برابر ویروس های رایانه ای محافظت می کند.

منابع و مآخذ

-بـاصری، علی‌اکبر،۱۳۸۷. سیاست جنایی قضایی کودکان و نوجوانان (در حقوق داخلی و اسناد بین‌المللی)، تهران:انتشارات خـرسندی

-باشگاه خبرنگاران جوان،روش های کلاهبرداری در فضای مجازی،تاریخ انتشار:۲۸ خرداد ۱۳۹۵،کد خبری ۵۶۵۵۵۲۳

-دیندار.فرکوش،فیروز و صدری نیا،حسین.۱۳۸۸؛روابط عمومی و رسانه،چاپ سوم،تهران،نشر سایه.

-نجفی ابرندآبادی،علی حسین.۱۳۷۹؛مباحثی در علوم جنایی؛تقریرات درس جرم شناسی پیش گیری،دوره ی دکتری،دانشگاه تربیت مدرس،گردآورنده:محمدعلی بابایی.

-نجفی ابرندآبادی،علی حسین.۱۳۸۱؛تقریرات درس جرم شناسی،دوره ی کارشناسی ارشد،مجتمع آموزشی عالی قم،گردآورنده:مهدی سیدزاده.

-نجفی ابرندآبادی،علی حسین.۱۳۸۲؛تقریرات درس جرم شناسی،دوره کارشناسی ارشد،دانشگاه شهید بهشتی،گردآورنده:رضا فانی.

-Brenner,w.s.(2010).Cybercrime criminal threats from cyberspace.Santa Barbara:praeger.

-Kleve,Du Mulder,R.& Van Noortwijk,K.(2010).The definition of cyber crime.Computer Law & Security Revew journal,27(2).

-Chunge,y.c.(2010).The camputer fraud and abuse act.Harvard journal of law and technology.24(1).

-Gercke,M.(2012).Understanding cybercrime:phenomena,challenges and legal response,Geneva.ITU.

-Schjulberg,S. & Ghernaouti-Helie,S.(2011).Aglobal treaty on cybersecurity and cybercrime. Stålfjæra:Aitoslo.