فصلنامه بین المللی قانون یار

License Number: 78864 Article Cod:Y6SH24A99612 ISSN-P: 2538-3701

نقد و بررسی جرم کلاهبرداری رایانه‌ای و راهکارهای مقابله با آن

(تاریخ دریافت ۱۴۰۱/۰۷/۱۵، تاریخ تصویب ۱۴۰۱/۱۲/۱۸)

دکتر حسین یار احمدی[۱]

استادیار موسسه آموزشی مجازی عالی فاران مهر دانش موسسه آموزشی عالی مجازی فاران مهر دانش

محبوبه براتی بارویی

دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی موسسه آموزشی مجازی عالی فاران مهر دانش

چکیده

طبق ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲ هرکس در بستر مبادلات الکترونیکی با سواستفاده و یا استفاده غیر مجاز از داده ها برنامه ها و سیستم های رایانه ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف، مداخله در عملکرد برنامه یا سیستم رایانه ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم های پردازش خودکار و نظایر 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، کلاهبرداری رایانه ای باید به تحصیل مال یا منفعت یا خدمات مالی یا امتیازات مالی بینجامد. این تحصیل می تواند برای خود مرتکب یا دیگریدباشد. دیگری، کسی است که مرتکب تحصیل را برای وی خواسته باشد، در این مقاله روش های حفاظت از سیستم رایانه ایی شیوه مقابله با آن ، پیشگیری کیفری و صلاحیت رسیدگی دادگاهها به جرایم رایانه ای مورد بررسی قرار گرفته است.

واژگان کلیدی: کلاهبرداری، رایانه ایی، جرایم، صلاحیت، مال

[۱] نویسنده مسئول

مقدمه

جرم به فعل یا ترک فعلی گفته می شود که قانون گذار برای آن مجازاتی در نظر گرفته است و برای آنکه جرم تلقی شود باید عنصر قانونی، عنصر مادی و عنصر روانی یا معنوی جرم فراهم باشد. و با تعریفی که از جرم رایانه ای داریم به آن دسته از اعمالی مجرمانه ای گفته می شد که ماهیتی سنتی دارند اما از طریق ابزار مدرنی مانند رایانه و اینترنت صورت می گیرد هرچند تدابیر کلی در مقابله با انواع روش های کلاهبرداری تقریبا مشابه است اما با تفاوت های موجود در شیو ههای گوناگون کلاهبردای بهر هگیری از رو شها ی مقابله متناسب ضرورت می یابد، 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 روبه رو نمی شوند در تعریفی از کلاهبرداری رایانه ایی یکی از مهم ترین جرایم علیه اموال و مالکیت می باشد که برخی از آن به عنوان بحران قرن بیستم نام برده اند. و همانند کلاهبرداری سنتی جرمی مقید به حصول نتیجه مجرمانه است و باید به واسطه سوء استفاده از رایانه از طریق افعالی نظیر ایجاد، محو، توقف داده و یا اختلال در سیستم رایانه ای، مال یامنفعت یا مزایای مالی عاید مرتکب شود.

بخش اول: بررسی پیشینه تحقیق

پیشینه تاریخی و اجتماعی : سابقهٔ تاریخی کلاهبرداری جرم پدیده ای است انسانی اجتماعی، انسان در هر جامعه به اقتضای انگیزه هایروانی خود، مرتکب جرمی می شود که زمینه های ارتکاب آن را از سازمانهای فرهنگی، سیاسی و اقتصادی جامعه خود کسب کرده است از این جرم و عوامل جرم رای اجتماعی همبستگی نزدیک و مستقیم وجود دارد، به نحوی کهتغییرات پیوسته عوامل مذکور در تغیر چهره جرایم کاملا مشهود است و در کیفیت و کمیت جرایم تأثیر بسزایی دارد عمل زشت مورد توجه بوده است .منتها شیوه این تجاوز و چهرهٔ آن با تحولات اجتماعی و پیچیده شدن روابط اجتماعی، رنگهای متنوعی به خود گرفته است ولی تحول جوامع و صنعتی شدن این نوع ربودن در تغییر داده و به جای ربودن خدعه آمیز مال غیر که معمولاً دور از انتظار صاحب مال صورت می گرفت است کلاهبرداران امروزه با توسل به

وسایل متقلبانه و از راه خدعه و نیرنگ بدون هیچگونه خشونتی مال دیگران را حتی با رضایت مال از چنگال آنها خارج می کنند و در ظاهر هم خود را از نخبگان جامعه به شمار می آورد.
در این مورد می توان به مقالات و کتابهای دکتر حسین میر محمد صادقی اشاره نمود که در یکی از نوشته های خود چنین بیان نموده اند : کلاهبرداری رایانه ای از جمله جرایم کلاسیکی است از ابتدا در جوامع بشری موجود بود و مسئولان ادارهٔ جوامع هرگز نتوانستند این جرایم را ریشه کن کنند البته این است که امروزه با ظهور فناوری نویسی به نام کامپیوتر طریقهٔ های ارتکاب این جرم متنوع تر و به دام انداختن مجرمان سخت تر شده است در حقوق ایران کلاهبرداری رایانه ای جرم انگاری شده است.[1]

بخش دوم: چارچوب نظری تحقیق

از دیدگاه دینی طبق آیه ۱۸۸ سورهٔ بقزه، کل مال به باطل حرام است.
و لا تا لکوا اموالکم بینکم بالباطل و بدلوا بها الی الحکام لتاکلوا فریقا من اموال الناس بالایم و انتم تعلمون. از دیدگاه حقوق دانان دو تعریف برای جرم کلاهبرداری در نظر گرفته شده است

الف- توسل به وسایل متقلبانه و تحصیل (تصاحب) مال غیر

ب- تحصیل مال غیر با توسل به وسایل متقلبانه یا مانور متقلبانه

موضوع جرم: موضوع کلاهبرداری رایانه ای وجه یا مال یا منفعت یا خدمات یا امتیازات مالی است. کلاهبرداری رایانه ای به لحاظ موضوع از کلاهبرداری سنتی عام تر است و علاوه بر وجه و مال، منفعت و خدمات و امتیازات مالی را نیز در بر می گیرد.
رفتارمرتکب: با توجه به قید واژه هرکس، مرتکب این بزه همانند کلاهبرداری سنتی هر شخصی می تواند باشد، البته به جز اشخاص حقوقی که بدون تصریح خاص قانونگذار فعلاً در حقوق ایران فاقد مسوولیت کیفری می باشند. کلاهبرداری رایانهای بزهی مرکب و دو رفتاری است. رفتار اول در آن که به طور تمثیلی در ماده ۱۷ق.ج.ر. به آن اشاره شده است اعمالی چون وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده ها یا مختل کردن سامانه می باشند.

[1] پایگاه حقوقی، حق گستر

این رفتارها باید به طور غیر مجاز صورت گیرند و اگر با اجازه انجام شوند، کلاهبرداری رایانه ای رخ نداده، هرچند که به تحصیل مال به طور غیر قانونی بینجامد.

رفتاردوم، تحصیل اعم از دریافت واقعی یا مجازی یا منظور کردن اعتبار مالی برای خود می باشد. بستر انجام این بزه، فضای سایبر است. بنابراین رفتارهای فیزیکی و تحصیل باید در فضای سایبر انجام گیرد. اگر فرد از رایانه و فضای سایبر تنها به عنوان وسیله ارتکاب جرم کلاهبرداری استفاده کند مثل اینکه از طریق تبلیغ ناروا در وبلاگ خود، دیگری را فریفته و خود را دارنده مؤسسه اعزام دانشجو به خارج بشناساند و با دادن شماره حسابی، کاربر یا کاربرانی را بفریبد تا پولی به حسابش بریزد یا در محیط بیرون پول یا مال را دریافت دارد، کلاهبرداری سنتی انجام داده است نه رایانه ای.

نتیجه حاصله: کلاهبرداری رایانه ای باید به تحصیل مال یا منفعت یا خدمات مالی یا امتیازات مالی بینجامد. این تحصیل می تواند برای خود مرتکب یا دیگری باشد. دیگری، کسی است که مرتکب تحصیل را برای وی خواسته باشد

بخش سوم: توسل به وسایل تقلبی

بدست آوردن وجوه یا اسناد و بلیط ها و قبوض و مفاصاحساب و امثال آن و بالاخره « خوردن » مقداری از اموال دیگری. بدیهی است تا وقتی این نوع سه عمل جمع نشده و نتیجه مجرمانه که به تعبیر قانون گذار سابق ما واژه « خوردن » مال دیگری بود تحقق نیافته باشد جرم کلاهبرداری مصداق پیدا نخواهد کرد و به تعبیری دیگر تحقق جرم مشروط و مقید به آنست که نتیجه مجرمانه ای بر فعل مرتکب شده باشد و از این نظر جزء جرائم مقید است. با وقوع انقلاب اسلامی و بوجود آمدن تحولات مختلف سیاسی و اجتماعی قوانین جزایی نیز متحول شد.در قانون مجازات اسلامی در فصل یازدهم آن از عبارات ارتشاء و ربا و کلاهبرداری نام برده ولی عملا " در این فصل ماده ای در این زمینه وجود ندارد که می توان از اشکالات و نواقص قانون مجازات اسلامی بر شمرد. مطابق ماده ۱ قانون مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری « هر کس از راه حیله و تقلب مردم را بوجود شرکت ها یا تجارتخانه ها یا کارخانه ها یا موسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیر واقع امیدوار نماید یا از حوادث و پیش آمدهای غیر واقع بترساند یا اسم یا عنوان مجحول

اختیار و به یکی از وسایل مذکور یا وسایل تقلبی دیگر وجوه یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصا حساب و امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردا محسوب و علاوه بر رد مال به صاحبش به حبس از یک تا هفت سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می شود...» از این ماده چنین بر می آید که برای تحقق جرم کلاهبرداری توسل به وسایل تقلبی و بردن مال غیر که همان نتیجه جرم است باید صورت گیرد. مطابق این ماده توسل به وسایل تقلبی باید موجب اغفال فرد شود و سپس مالی ربوده شود فی المثل ترک فعل نمی تواند توسل به وسایل متقلبانه باشد. اغفال و یا به تعبیر دیگر (فریب) برداشت نادرست و غلط از واقعیت را موجب می شود از شرایط اغفال این است که فرد مجنی علیه علم به تقلبی بودن وسیله متقلبانه نداشته باشد و هم چنین موضوع اغفال باید یک فرد یا افراد انسانی باشد تا غفلت صورت پذیرد مثلا "افرادی که محجور هستند اغفال در مورد آنها امکان ندارد زیرا این افراد فاقد بعضا" اراده و گاه تفکر لازم برای انجام امور هستند. البته ملاک و معیار تشخیص افراد انسانی متعارف در جامعه هم نیز متفاوت است که عده ای معتقد بر معیار نوعی و بعضی دیگر معیار شخصی را مورد پذیرش قرار داده اند. باب چهارم قانون تجارت الکترونیکی مصوب ۱۷ دیماه ۱۳۸۲ مجلس شورای اسلامی تحت‌عنوان جرایم و مجازاتهاست که مبحث اول آن به کلاهبرداری کامپیوتری ضمن ماده ۶۷ و مبحث دوم آن‌به جعل کامپیوتری ضمن ماده ۶۸ قانون مزبور اختصاص دارد. در واقع، ضرورت اجتناب‌ناپذیر استفاده‌از کامپیوتر در امور و امکان سوء استفاده از آن که از موارد بحران مهم در عصر دیجیتال است، قانونگذاررا به عکس‌العمل قانونی واداشت.

بخش چهارم: روش های کلاهبرداری رایانه ای

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 نیزوجود 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 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 نیزبعد 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 پایانه های 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 دستگاه های 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 قرعه کشی

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 بهجای 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 مراجعه کنندگان میخواستیم برای قرعه کشی 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 سایت های 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 خانه هایی که خبری از صاحبانشان نیست، به جعل سند دست میزنند. آنها عموما چنین خانه هایی را با قیمت پایینتر و ارزانتر از چیزی که در بازار است به افراد متقاضی خرید پیشنهاد می دهند.

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 نقطه های جهان رواج یافت. اما پلیس ایران توانست در مقابله با این شگرد موفق عمل نماید.

بخش پنجم: روش های حفاظت از سیستمهای رایانه ای

تدابیر متنوعی برای حفظ سیستم های رایانه ای از حملات وجود دارد، از جمله آن: تدابیرنظارتی است که در فضای فیزیکی نیز نمونه هایی از آن در قالب دوربین های مداربسته جهتکنترل اماکن وجود دارد. اما آنچه در فضای سایبر به کار می رود، مجموعه ای از برنامه هایرایانه ای است که بر حسب نوع برنامه ریزی ای که برای شان صورت گرفته، کلیه داده های راجعبه مبادلات الکترونیکی کاربرانی که به هر دلیل در مظان ارتکاب جرم هستند را جمع آوریمی کنند تا مسئولان ذیربط به صورت زنده آنها را بررسی کنند. این اقدام تا حدی مورد توجهمجریان قانون کشورها قرار گرفته که برخی از آنها پلیس گشت سایبر[1]نامیده شده اند، زیرابه گونه ای اوضاع سایبری را تحت کنترل دارند که هر گونه وقوع جرم یا دیگر ناهنجاری را بهاطلاع مراجع ذیربط می رسانند(گزارش حریم خصوصی در فضای سایبر، ۱۳۸۵: ص۲۱). به طور کلی روش های حفاظت از سیستم های رایانه ای عبارتند از: حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت عملیات، که هدف همه آنها سخت تر ساختن دسترسیمجرمان به سیستم های رایانه ای می باشد که مورد بررسی قرار خواهند گرفت. از جمله مهمترین تدابیر لازم برای مقابله با جرم کلاهبرداری رایانه ای بهره گیری از روشهای حفاظتی و امنیتیاست. سیستم امنیتی نامطلوب در اکثر موارد، علت وقوع جرم است. تدابیر امنیتی نامطلوب در بیشتر موارد حاصل بی اطلاعی از مشکلات موجود در زمینه امنیت داده ها است.

[1] Cyber Patrol

الف)حفاظت فیزیکی[۱]

حفاظت فیزیکی به معنای حفظ رایانه، تجهیزات رایانه، رسانه های رایانه ای و تمامی سیستم، در مقابل سوانح طبیعی، انواع مختلف حوادث و حملات عمومی است (استرکی، ۱۳۸۳: ص۷۵). جرایم رایانه ای قابل پیش بینی نیستند، به همین جهت اتخاذ تدابیری که ارتکاب آن ها را بادشواری مواجه سازد ضرورت دارد. اولین حلقه حفاظت فیزیکی اقداماتی است که مجرمین را ازنفوذ به ساختمان محل استقرار رایانه ها مایوس نماید، به طوری که تدابیر مناسب برای درب هایورودی اطاق های محل نگهداری سیستم رایانه ای اتخاذ شود. همچنین جهت جلوگیری از استراق سمع تلفنی اتخاذ اقدامات لازم جهت حفاظت از رمز عبور، نام فایل ها و سایر اطلاعات محرمانهضروری است. پیش از نفوذ افراد غیرمجاز و وقوع جرم، می توان برنامه های حفاظت فیزیکی را از طریق بازرسی منظم از تمهیدات حفاظت فیزیکی یا بازرسی غیر مترقبه از فیلترها و موانعحفاظت فیزیکی مورد ارزیابی قرار داد.(استرکی، همان: ص۱۷۲)

ب) حفاظت کارکنان[۲]

تدبیر حفاظت کارکنان، افرادی را پوشش می دهد که به نحوی مجاز به کار با سیستممی باشند. اغلب جرایم مالی رایانه ای توسط افراد مذکور و نه حریم شکنان مجرم صورت می گیرد (گزارش طرح شناخت کلی جرایم رایانه ای و شیوه های مبارزه با آن، همان: ص۶۹). در برخیموارد، اعمال سیاست های سازمان، منظم و مدون نیست. به عنوان مثال در برخی از سازمانهاکارکنان اجازه ندارند اطلاعات محرمانه سازمان را با خود به منزل ببرند. از سوی دیگر به آنهااجازه داده می شود از منازل خود با استفاده از یک مودم به بانک اطلاعاتی سازمان متصل شوند.در این صورت اطلاعات سازمان قابل نسخه برداری خواهد بود. از نظر حفاظت کارکنان، اقداماتلازم جهت ارتقاء سطح امنیت پرسنلی عبارتند از: ۱)تحقیقات لازم پیش از استخدام ۲) نظارت وکنترل کافی مدیران بر عملکرد کارکنان ۳)دادن آموزش های لازم به کارکنان، زیرا گاهی وقوعجرم ناشی از ثبت اشتباه یا تغییر اطلاعات به وسیله

[۱] Physical Security

[۲] Personnel Security

کارمند است ۴)اجرای برنامه کاری چرخشیبرای کارکنان، زیرا برخی حملات نفوذکنندگان غیرمجاز به زمان زیاد و یا کنترل مستمر نیازمنداست که در صورت اجرای راهکار فوق امکان شناسایی برخی حملات درازمدت خواهد بود.(استرکی، همان: ص۸۳) قابل ذکر است که در این باره، بایستی شدیدترین احتیاط ها در موردکارکنان اخراجی یا کارکنانی که داوطلبانه از کار کناره گیری کرده اند اتخاذ شود.

ج)حفاظت ارتباطات[۱]

گونه ای دیگر از تدابیر امنیتی و حفاظتی، حفاظت ارتباطات است که شامل حفاظت از پست، نمابر، تلفن، ارتباطات پست صوتی و همچنین حفاظت از اطلاعات انتقال داده شده از یک رایانهبه رایانه دیگر از طریق اتصال شبکه می شود. مجرمین حرفه ای ممکن است سیستم رایانه رابرای ارتکاب کلاهبرداری یا مستقیما برای منفعت خودشان، مورد هدف قرار دهند. در این صورت تدابیر حفاظت ارتباطات (به عنوان مثال کلمات رمز عبور) مهمترین عامل برای دور نگهداشتنمجرمین حرفه ای است. حفاظت ارتباطات، روش ها و وسایل مختلفی را در بر می گیرد که شاملاستفاده از کلمات رمز مناسب، حفظ اطلاعات انتقال داده شده، ایجاد یک حفاظ که سیستم ها وشبکه های داخلی را از دیگر شبکه ها حفاظت کند، کنترل دسترسی، روش های رمزنگاری، فناوری دیواره آتشین[۲] و... میباشد. شیوه های دسترسی در ایجاد امنیت رایانه های متصل به شبکه اهمیت زیادی دارند. یکی ازابزارهای کنترل دسترسی استفاده از رمز عبور است. فردی قادر به دسترسی خواهد بود که رمزصحیح عبور را در رایانه وارد نماید و سرقت یا نسخه برداری غیرمجاز از اطلاعات محرمانه نوعی تهدید آشکار است و نفوذ کنندگان غیرمجاز درصدد دستیابی به رمز عبور یا سایر اطلاعات جهتنفوذ در سیستم هستند. یکی از شیوه های محدود نمودن دسترسی افراد به اطلاعات محرمانه، رمز نگاری اطلاعات و داده ها می باشد. در این فرآیند اطلاعات یا محتویات یک متن به اطلاعات و متون رمز تبدیل می شود. برخلاف گذشته که از یک کلید جهت رمز نمودن اطلاعات استفادهمی شد، در شیوه های رمزنگاری جدید از دو کلید، جهت رمزنگاری یک پیام استفاده می شود.

[۱] Communications Security

[۲] Fire Wall

دراین روش ها حتی امکان امضاء پیام نیز فراهم شده تا گیرنده پیام از هویت فرستنده آن مطلعشود. دیگر اینکه کابل ها و خطوط ارتباطی به راحتی قابل شنود و استراق سمع هستند. تمامیدستگاه های الکترونیکی از خود پرتوهای الکترومغناطیسی منتشر می کنند. دریافت و آشکار سازیآن پرتو ها یکی از روش های استراق سمع است. افرادی که قصد استراق سمع دارند با استفاده ازیک سری تجهیزات قادر به دریافت سیگنال هایی هستند که در اثر فشردن کلیدهای صفحه کلید رایانه در محیط منتشر می شوند. با تحلیل این سیگنال ها می توان به اطلاعات روی صفحهنمایشگر سیستم دست یافت. یکی از شیوه های جلوگیری از انتشار پرتو های الکترومغناطیسیاستفاده از عایق است.

عایق، سیگنالهای الکترومغناطیسی را تضعیف نموده و آن ها را به زمین هدایت می کند. (استرکی، همان: ص۲۱۱) یکی از شیوه های موثر حفاظت در مقابل نفوذ افراد غیرمجاز نصب دیواره آتشین می باشد.دیواره آتشین یک روش نرم افزاری یا سخت افزاری است که بر کلیه ارتباطات شبکه اعم ازارتباطات بین شبکه داخلی و اینترنت یا بالعکس نظارت می کند. نرم افزاری که دیواره آتشین راتشکیل می دهد اطلاعات و داده های در حال تبادل شبکه را بررسی و مبادله اطلاعات و سایرعملیات مشابه را مجاز یا متوقف مینماید.(استرکی، همان: ۲۱۴)

د)حفاظت عملیات[1]

آخرین نوع از تدابیر حفاظتی، حفاظت عملیات است. حفاظت عملیات به معنی وضع تدابیریجهت شناسایی و مقابله با تهدیدهایی است که سیستم ها را به مخاطره میاندازد.

حفاظت عملیات دو مقوله از حفاظت رایانه را در بر می گیرد: ۱)روش هایی که می تواند آگاهی و اطلاع از وقوع جرایم احتمالی را در بین قربانیان بالقوه افزایش دهد. ۲) روش هایی که می تواند مجرمین رایانه ای را از ارتکاب جرم باز دارد. این فرآیند سه مرحله دارد: مرحله اول : مشخصکردن اطلاعاتی که یک مجرم رایانه نیاز دارد. مرحله دوم: مشخص کردن روش های احتمالیمجرمین برای کسب اطلاعات و مرحله آخر، توسعه اقدامات لازم جهت مقابله با عملی شدنروشهای احتمالی. (استرکی، همان: ص۲۲۵). حفاظت عملیات فعالیتی پویاست. بنابراین با تغییر غیر منظم روش ها و دسترسی ها می توان تعادل حریف را بر

هم زد. برای رسیدن به این منظور، فهرست اجزای ضروری اطلاعات، روش های نفوذ و شگردهای مقابله باید دائما تغییر پیدا کنند. مهمترین رکن حفاظت عملیات استمرار در توسعه روش های مقابله و حفاظت، آموزش کارکنان و کاربران سیستم است.

بخش ششم: پیشگیری کیفری از جرم کلاهبرداری رایانه ای

وجود بزهکار نه فقط نظم اجتماعی را در خطر قرار می دهد، بلکه »قدرت دولت« را نیز درقبال جامعه تهدید می کند زیرا افزایش بزهکاران آشکار کننده ضعف دولت است و لذا دولت به شدت درصدد سرکوبی بزهکاری و به خصوص بزهکاران بر می آید (نوربها، ۱۳۷۷: ص۲۳) در سیاست جنایی، مسئله مقابله با جرم نیز نهفته است و چگونگی و کیفیت و انتخاب نوع کیفر وبرخورد با بزهکاران نیز بیان می شود. (گزارش پیرامون پیشگیری از وقوع جرم، ۱۳۷۵: ص۲).

(پیشگیری واکنشی) پس از ارتکاب جرم و با استفاده از ابزارهای کیفری اعمال میشود. این نوع پیشگیری خود بر دو گونه است:

۱)پیشگیری واکنشی عام، که از طریق رعب انگیزی و عبرت آموزی به دنبال پیشگیری ازارتکاب جرم از سوی افراد جامعه می باشد.

۲)پیشگیری واکنشی خاص، که با اعمال کیفر بر فرد بزهکار درصدد پیشگیری از تکرار جرماست. صرف نظر از اقدامات پیشگیرانه، به هرحال باید انتظار داشت که همچون سایر جرایم، جرم کلاهبرداری رایانه ای از سوی مجرمین در جامعه روی دهد. بنابراین مقابله با این جرم جدای ازاقدامات عملی نیازمند اتخاذ تدابیر مناسب قانونی و قضایی است. اصولا جرم انگاری افعال بعنوان آخرین حربه علیه هنجار شکنان مورد توجه قرار می گیرد. وضع قانون مناسب یکی ازمهمترین راهکارهای مقابله با وقوع جرم از سوی افرادی است که نقض هنجار نموده و تدابیرپیشگیرانه وضعی را هم خنثی کرده اند. در مورد مقابله کیفری آنچه حائز اهمیت است، این استکه صرف جرم انگاری رفتار و تعیین ضمانت اجرای کیفری در رسیدن به مقصود یاری می رساند. این موضوع از آن جهت اهمیت دارد که با توجه به ناملموس بودن فضای سایبر در اکثر موارد، کشف و تعقیب جرایم ارتکابی در این محیط و

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹

اعمال مجازات مجرمان، چه در سطح ملی و چهدر سطح بین المللی (به علت واجد جنبه فرامرزی بودن جرایم ارتکابی در فضای سایبر) بامشکلات و چالش هایی روبروست جعل رایانه ای و استفاده از داده های مجعول: رکن مادی، موضوع جرم: موضوع جعل رایانه ای، داده و یا حامل داده و یا جای انباشت داده می باشد مانند علامت، کارت حافظه و تراشه. داده های موضوع جعل رایانه ای باید قابلیت استناد داشته باشند و به همین دلیل است که دیگری نیازی به ایراد ضرر برای تحقق این جرم نیست و اگر زیانی حاصل شود می تواند باعث افزایش کیفر شود.

رفتار مرتکب: در بند الف ماده ۶ ق.ج.ر. دو بخش جداگانه در انجام رفتار جعل رایانه ای پیش بینی شده است: اول، تغییر یا ایجاد داده های قابل استناد که در واقع تغییر باید در داده های قابل استناد انجام شود و ایجاد نیز باید پدید آوردن داده ای باشد که توانایی استناد پذیری داشته باشد. دوم، ایجاد یا وارد کردن متقلبانه داده به آنها بند ب ماده ۶ ق.ج.ر.، تغییر داده ها یا علایم موجود در کارتهای حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها با ایجاد یا وارد کردن متقلبانه داده ها یا علایم به آنها را به عنوان رفتار مجرمانه برای جرم جعل رایانه ای مطرح می کند.

رکن مادی و موضوع جرم استفاده از داده مجعول: داده، کارت های الکترونیکی و تراشه ها موضوع رفتار مجرمانه در این جرم می باشند. رفتار مرتکب استفاده کردن از داده مجعول که باید در فضای سایبر و سامانه های رایانه ای و مخابراتی یا داده برها و کارت های حافظه انجام شود، رفتار مرتکب در بزه استفاده از داده مجعول را تشکیل می دهد. بنابراین اگرکسی در فضای بیرونی و فیزیکی از داده مجعول استفاده کند، این بزه رخ نمی دهد. به عنوان مثال اگر فردی جعل رایانه ای کند و متن یک قرارداد الکترونیکی را تغییر دهد و یا اینکه چنین قرارداد مجعولی را بیابد یا دریافت دارد و سپس آن را چاپ کرده و به نهاد یا کسی ارایه دهد مرتکب جرم استفاده از سند مجعول شده است نه جرم استفاده از داده مجعول، چرا که استفاده کردن در فضای بیرونی انجام شده است.

جرایم قابل ارتکاب از طریق رایانه: جرایم قابل ارتکاب با رایانه، به بزه هایی می پردازد که رایانه در آنها، وسیله انجام رفتار است.

جرایم مالی رایانه ای جرایم مالی ناظر به جرایمی است که مرتبط با اموال هستند اعم از اینکه مال موضوع جرم باشد یا وسیله آن.

سرقت رایانه ای: این بزه، یک بزه رایانه ای محض است چرا که ربودن داده در جایی که عین داده در جای خود باقی است، مانند جاسوسی و شنود غیر مجاز است که بر ضد محرمانگی داده رخ می دهد و در جایی که به وسیله برش، عین داده از سامانه برداشته می شود، همانند تخریب داده است. بنابراین در دسته جرایمی قراردارد که رایانه، هدف یا موضوع بزه است و نباید در کنار کلاهبرداری که در آن رایانه نقش ابزار انجام بزه را دارد، آورده شود.

رکن مادی موضوع جرم سرقت رایانه ای: موضوع بزه سرقت رایانه ای، داده است. این داده به تعبیر ماده ۱۲ ق.ج.ر. باید متعلق به دیگری باشد. دادهای که متعلق به دیگری است باید در رایانه او یا جایی که به طور قانونی مکان قرار گرفتن دادههای آن فرد است، باشد بنابراین اگر کسی نوشته دیگری را که بطور آزاد در اینترنت هست، بارگذاری کند و دریافت دارد، سارق نیست. ولی اگرکسی مقاله دیگری را از رایانه وی برباید، حتی اگر متن آن مقاله در اینترنت و به طور آزاد، دسترس پذیر باشد، عمل وی قابل مجازات است.

رفتارمرتکب: رفتارسرقت رایانه ای، همچون سرقت سنتی، ربودن است. آن چه مفهوم ربایش را می سازد، دست اندازی به مال دیگری یا از آن خود کردن بدون خشنودی دارنده آن است. یعنی همین که کسی مال دیگری را بدون رضایت وی بدست آورد رفتارش، ربایش است صلاحیت رسیدگی دادگاهها به جرایم رایانه ای گسترش شبکه های جهانی رایانه ای چندیست که مرزهای جغرافیایی را با خلل روبه رو کرده است. استفاده از شبکه های جهانی اینترنتی به شدت رو به افزایش است. همین که پیوستن به شبکه های اینترنتی افزایش می یابد – یعنی جایی که بسیاری از افراد با هم تبادل دارند– مباحث حقوقی، اهم از کیفری و خصوصی به شکل تازه ای مطرح می گردد.

بخش هفتم: بررسی یافته های تحقیق

در رابطه شناسایی با خطرات متوجه سیستم رایانه ای، مهمترین اقدام در جهت ایجاد یک برنامه حفاظتی مناسب برای مقابله با جرم کلاهبرداری رایانهای است. سیستم های سخت افزار و نرم افزار رایانه ای به شیوه های مختلفی در معرض خطر قرار می گیرند لذا باید تدابیر متنوعی برای

فصلنامه علمی-حقوقی قانون یار – دوره ششم – شماره ۲۴ – زمستان ۱۴۰۱ – دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹

حفاظت از سیستمهای رایانه ای در مقابل حملات احتمالی اتخاذ گردد، که از آن جمله می توان به تدابیرحفاظت فیزیکی از رایانه و تجهیزات مربوط به آن در مقابل حوادث و حملات احتمالی اشاره نمود و همچنین با توجه به اینکه غالب حملات مالی رایانه ای به وسیله کارکنان ادارات و موسسات دولتی و غیردولتی صورت می گیرد اتخاذ تدابیر حفاظت کارکنان که افراد مجاز به کار باسیستم های رایانه ای را تحت پوشش قرار می دهد ضرورت دارد. دیگر اینکه تقویت تدابیر حفاظت ارتباطات که اطلاعات انتقال داده شده از یک سیستم به سیستم دیگر از طریق اتصال به شبکهرا در بر می گیرد و همچنین تدابیر حفاظت عملیات که با شناسایی اطلاعاتی که مجرمان در صدد دستیابی به آن هستند و شناخت روشهای احتمالی کسب اطلاعات، اقدامات لازم را جهت مقابله با عملی شدن روش های احتمالی ارائه می دهد، امری اجتناب ناپذیر است در بیانِ علت جرم میگوید:(شرط لازمی که بدون آن رفتارمجرمانه بروز نخواهد ۳ ژان پیناتل.)علت شناسی ازاصول پایه ای دانش جرمشناسی محسوب میگردد ۵ص، ۱۳۳۱ کرد) (کی نیا، به گونه ای که اهداف جرمشناسی در زمینه پیشگیری و درمان یک بزه، با شناخت علل ارتکابی آن مقدور میباشد. لذا جرمشناسان برای مقابله بایک جرم با ترسیم یک رابطه ی علت و معلولی، سعی در خنثی نمودن علل موثر در ایجاد نتیجه مجرمانه می نمایند. امروزه با گسترش فضای مجازی میتوان از اختراع شدن بزهکاری تنوع سیکلت یا چرخه جنایی نیز صحبت به میان آورد که منجر به سهولت بزهکاری و احتمال پایین دستگیری مجرمین در فضای مجازی خواهد شد سیاست جنایی مقابله با این جرایم نیز به سمت فنی شدن پیش رفته است کلاهبرداری رایانه ای و تحصیل مال ازطریق حیله و تقلب نوع مخصوصی از جرایم رایانه ای است که به جهت وسعت ارتکاب آن نگاه و توجه سیاست جنایی را به خود جلب نموده است و به نظر میرسد که اقدامات غیر کیفری و راهکار های پیشگیرانه برای ممانعت و جلوگیری از تشکیل و اجرایی شدن این جرم به موازات واکنش مستقیم و کیفری علیه آن نتیجه مثبت و مطلوبی را به بار خواهد آورد ویژگی های جرائم رایانه ای با توجه به قابلیت های رایانه از قبیل قابلیت تراکم اطلاعات قابلیت دستیابی به سیستم های رایانه ای در سراسر دنیا آسیبپذیری سیستم های الکترونیکی

درهم آمیختگی شبکه جهانی با تجارت گنجینه های اطلاعاتی و قومیت گستردگی این شبکه ویژگی های زیر را میتوان برای جرایم رایانه ای برشمرد.

نتیجه گیری

راهکارهای مناسب در جهت مقابله و جلوگیری از وقوع جرم درمحیط مجازی که از اوصاف و ویژگی متفاوتی نسبت به محیط واقعی برخوردار است امری ضروری است. در تدابیراجتماعی 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 نقشتربیتی و آموزشی والدین و موسسات آموزشی در کاهش ارتکاب جرم مورد تاکید قرار گیرد. باعدم توفیق مقابله اجتماعی در کاهش یا مهار جرم، مقابله وضعی با آن مطرح خواهد شد. هدفاز مقابله وضعی، سلب فرصت ارتکاب جرم از سوی نفوذ کنندگان به سیستم های رایانه ای 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 سیستم های رایانه ای، اتخاذتدابیر 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 ومنسجم با این جرم تنها بر پایه شناخت درست از ماهیت و شیوه های ارتکاب جرم امکان پذیراست. کلاهبرداری رایانه ای به لحاظ خلاقیت مرتکب آن و سهولت و کثرت ارتکابش مهمترین و شایع ترین جرم اقتصادی فضای مجازی رایانه و اینترنت محسوب می شود هر چند به ظاهر در ارتکاب این جرم رایانه در حد وسیله جرم ظاهر می شود اما رایانه و اینترنت کلاهبرداری را تأم با کیفیات و شرایط غیر قابل انکاری می کنند که قانون گذاران ناگزیر به شناسایی جدید در کنار کلاهبرداری سنتی هیتند کلاهبرداری رایانه ای چون در دنیای جدید به نام دنیای مجازی رایانه و اینترنت (فضای سایبر) با امکانات بیشماری تحقق می یابد فقط علیه انسان نیست و بلکه غالباً سیستم رایانه ای و نرم افزارهای آن است و بنابراین شرط فریب قربانی در آن تا مرز حذف شدن تضعیف می شود. موضوع جرم کلاهبرداری رایانه ای نیز فراتر از مال یا وسیله تحصیل مال است و شامل خدمات و امتیازات مالی و حتی داده های رایانه ای و دارای ارزش مالی نیز می شود.

منابع و مآخذ

۱-اردبیلی، محمدعلی، ۱۳۸، حقوق جزای عمومی، جلد نخست، چاپ هشتم، تهران، نشر میزان.

۲-برگرفته از سایت ایران هشدار، کد خبر ۲۸۰۷، ۵ مرداد۱۳۹۴. http://www.iranhoshdar.ir

۳- بیات، شیرین، فرهاد، بهار۱۳۹۶، شرح جامع حقوق مدنی، چاپ دوازدهم، انتشارات ارشد.

۴-جعفری لنگرودی، محمد جعفر، ۱۳۸۸، ترمینولوژی حقوق، کتابخانه گنج دانش، چاپ بیست و دوم.

۵- حبیب زاده، محمد جعفر، ۱۳۸۵، حقوق جزای اختصاصی جرایم علیه اموال و مالکیت، چاپ پنجم، تهران، انتشارات سمت.

۶- حبیب زاده، محمد جعفر، ۱۳۸۹، تحلیل جرائم کلاهبرداری و خیانت در امانت در حقوق کنونی ایران، چاپ اول، تهران انتشارات دادگستر.

۷- حبیب زاده، محمد جعفر، ۱۳۷۷، مروری بر جرم کلاهبرداری در حقوق ایران، ماهنامه دادرسی، سال دوم، شماره هشتم، خرداد و تیرماه.

۸-خرم آبادی، عبدالصمد.۱۳۸۶، کلاهبرداری رایانه ای از دیدگاه بین المللی و وضعیت ایران فصلنامه حقوق مجله دانشکده حقوق و علوم سیاسی، سال ۳۷، شماره۲.

۹-دزیانی، محمد حسن، ۱۳۸۵. مقدمه ای بر سیاست جنایی ایران در باب جرائم سایبری، قضاوت، شماره ۳۸، خرداد ماه و تیر ماه.

۱۰- روضه ای، منصور. توانبخش، جعفر. حسن زاده کرد احمد، حمید.تابستان۱۳۹۶، ابزار های پیشگیری از جرایم نو ظهور در فضای مجازی، فصلنامه علمی پژوهشی مطالعات امنیت اجتماعی شماره ۵۰.

۱۱- سالاری شهر بابکی، میرزا مهدی، ۱۳۸۶، حقوق کیفری اختصاصی کلاهبرداری و ارکان متشکله آن، چاپ اول، تهران، نشرمیزان.

۱۲-سالاری شهربابکی، میرزا مهدی، ۱۳۹۳.کلاهبرداری و ارکان متشکله آن، تهران، میزان.

۱۳-شامبیاتی، هوشنگ، ۱۳۷۲، حقوق جزا عمومی، جلد اول، چاپ سوم، تهران، انتشارات ویراستار.

۱۴-علی نژادی، محسن. علی نژادی، زهرا، ۱۳۹۶، مقاله اعتبار داده پیام در قرارداد های داخلی و بین المللی در تجارت الکترونیک، ، فصلنامه علمی، حقوقی قانون یار، دوره سوم پاییز.
۱۵-عمید، حسن، ۱۳۵۱، فرهنگ عمید، چاپ ششم، تهران، انتشارات جاویدان.
۱۶- عباسعلی، اکبری، ۱۳۹۰، مقاله کلاهبرداری رایانه ای جلوه های نوین و متمایز از کلاهبرداری سنتی همایش منطقه ای چالش های جرایم رایانه ای در عصر امروز.
۱۷- قیاس، جلال الدین.نیک شب، عباسعلی.۱۳۹۳، پژوهش نامه حقوق کیفری، سال پنجم، شماره دوم، پاییز و زمستان.
۱۸-کاتوزیان، ناصر، بهار ۱۳۸۴، دوره مقدماتی حقوق مدنی، اموال و مالکیت، چاپ نهم، انتشارات میزان.
۱۹- گلدوزیان، ایرج، ۱۳۸۳، حقوق جزا اختصاصی جرائم علیه تمامیت جسمانی، شخصیت معنوی اموال و مالکیت، امنیت و آسایش عمومی، چاپ دهم، تهران، انتشارات دانشگاه تهران.

فصلنامه علمی-حقوقی قانون یار - دوره ششم - شماره ۲۴ - زمستان ۱۴۰۱ - دبیرخانه مرکزی ۰۲۱۶۶۹۷۹۵۱۹