فصلنامه مطالعات نوین بانکی

شماره مجوز: ۸۳۲۸۹ ((شماره شانزدهم-پاییز ۱۴۰۱)) ISSN : 2645-5420

بررسی و تحلیل جرایم مالی و اقتصادی در فضای مجازی

(تاریخ دریافت ۱۴۰۱/۰۲/۰۲، تاریخ تصویب ۱۴۰۱/۰۵/۲۰)

محمد مزیدی شرف آبادی[1]

مسعود اخلاص

چکیده

اقتصاد به عنوان یکی از اساسی ترین پایه های اقتدار هر کشور باید به اساس قواعد و اصول علمی و مبتنی بر واقعیت ها باشد تا چرخه مالی کشور با مشکل رو به رو نشود. امروزه سرویس‌های متنوعی در فضای مجازی ارایه می‌شود که به رفع نیازهای روزمره مردم و بنگاه‌های اقتصادی می‌پردازد. با وجود این، در کنار خدماتی که این سرویس‌ها ارایه می‌دهند، آسیب‌هایی هم وجود دارد. جرایم اقتصادی دامنه وسیعی دارد در واقع می توان گفت ویژگی جرایم اقتصادی به طور کلی این است که به نظم و امنیت موجود در اقتصاد دولت صدمه می زند و منجر به بیماری و اخلال در این نظام می شود. به هرصورت باید توجه داشت شناخت مهمترین جرایم مالی و اقتصادی در بستر فضای مجازی می تواند در پیشگیری از ارتکاب اینگونه جرایم جلوگیری به عمل آورد. البته باید اذعان داشت در رسیدگی به جرائم مالی در فضای مجازی دادستانی کل کشور، بانک مرکزی، پلیس فتا و شرکت های حاکمیتی در آن نقش دارند. سامانه تعاملی کاشف توانسته با مشارکت و همکاری با ذی نفعان نیازهایی که در راستای ایجاد سرعت بخشیدن به رسیدگی به جرائم مالی در فضای مجازی در نظام بانکی را بالا ببرد.

واژگان کلیدی: جرایم اقتصادی، فضای مجازی، کلاهبرداری اینترنتی، پلیس فتا، اقتصاد کشور، پولشویی

---

[1] نویسنده مسئول

بخش اول: بررسی و شناخت تاریخچه جرایم در فضای مجازی

گروهی معتقدند که ایجاد فضای سایبر در زمان اختراع تلفن توسط الکساندر گراهام بل در ۱۸۷۶ پا به عرصه گیتی نهاد، چرا که پیش از این رویدادهای بشر محدود به روابط و تماس‌های فیزیکی بود و بشر تصور نمی‌کرد هیچ‌گاه بتواند فراتر از دنیای فیزیکی خود با دیگران ارتباط برقرار نماید، اگر چنین قدمتی را برای ایجاد فضای مجازی در نظر بگیریم می‌توان گفت با ورود این تکنولوژی به داخل هر کشور تاریخچه ورود فضای مجازی به داخل آن کشور دانست و در واقع اولین اقدامات خلاف قانون اعم از فعل یا ترک فعلی که جرم انگاری شده باشد در حیطه این تکنولوژی را می‌توان اولین جرایم ایجاد شده در فضای مربوطه را اولین جرایم آن در کشورها دانست ولی عموم مردم فضای مجازی را با اختراع کامپیوتر (رایانه) همسان می‌دانند و معتقدند که ایجاد چنین فضای همزمان با ایجاد پیدایش رایانه‌ها بوده، لذا باید اشاره‌ای به پیدایش رایانه نمود. اینترنت در سال ۱۹۶۴ توسط محقق بنام پائل باران ($Paul\ Baran$) در شرکت $Rand$ (راند) ابداع شد، وی به دنبال روش برای مطمئن سازی ارتباط پنتاگون (وزارت دفاع ایلات متحده آمریکا) با اعضای ارتش در هنگام حمله واقعی اتمی بود و یک شبکه ارتباطات رایانه‌های غیر متمرکز را پیشنهاد کرده که در آن رایانه مرکزی وجود نداشت.[۱] چون آنها می‌دانستند که سیستمی که تنها دارای یک رایانه مرکزی باشد در مقابل صدمات وارده آسیب پذیر خواهد بود، لذا تصمیم گرفتند به جای آن که اطلاعات را در یک رایانه جمع‌آوری، ذخیره و پردازش نمایند، آن را در تعدادی رایانه که در جاهای مختلف و دور از همدیگر هستند قرار داده و از طریق خطوط تلفنی بین آنها ارتباط برقرار کنند. و

۱-www.hamshahrine.ir/details/۲۴۱۲

صدمه به قسمت‌های مهم و حیاتی سیستم‌های ارتباطی و عدم توانایی یک مسیر برای ارسال اطلاعات، سایر سیستم‌های مربوط به تأسیسات نظامی در اطراف کشور از طریق مسیرهای دیگر با هم به تبادل اطلاعات می‌پردازند.[۲] بر این اساس آژانس پروژه تحقیقاتی پیشرفته(آرپا)۳ که بخشی از وزارت دفاع محسوب می‌شود پیش نمونه اینترنت را در سال ۱۹۶۹ با عنوان آرپانتبا همکاری چندین دانشگاه ایجاد کرد. علاوه بر وزارت دفاع آمریکا دانشگاه‌های کالیفرنیا در لس آنجلس و سانتا باربارا، یوتا و مؤسسه تحقیقاتی استفرد، در همان ابتدا به آپارانت متصل شدند در سال ۱۹۷۱ آرپانت گسترش یافت و دانشگاه ها و آژانس های دولتی بیشتری را در بر گرفت که دانشگاه هاروارد و مؤسسه صنعتی ماساچوست و سازمان ملی هوانوردی و فضایی آمریکا را شامل می‌شد.[۱] در سال ۱۹۸۶ بنیاد ملی علوم آمریکا (NSF) یک سیستم ارتباط بین شبکه‌ای با مسیر طولانی را به وجود آورد و نام آن را «ان. اس. اف. نت» **($NSFNFT$)** گذاشت این شبکه قادر به برقراری ارتباط با آرپانت نیز بود(ان. اس. اف. نت) شبکه‌های دیگری نیز ایجاد کرد که همگی از پروتکل‌های (تی. سی. پی. آی. پی) استفاده می‌کردند. در همین زمان شبکه-های رایانه‌ای زیادی به این دو شبکه متصل شدند. بدین ترتیب شبکه‌های رایانه‌ای (ان. اس. اف. نت) با کمک آرپانت تبدیل به ستون فقرات اینترنت شد. در سال ۱۹۸۹ آرپا مدیریت آرپانت را متوقف کرد، چرا که آرپانت بر اثر مجتمع شدن با شبکه‌ای دیگر

---

[۱]– عبدالصمد خرم آبادی، جرایم فنآوری اطلاعات، پایان‌نامه دوره دکتری، دانشگاه تهران، ۱۳۸۴، ص۳۷.

[۲]- Advanced Research project Agency (ARPA)

[۳]– جینادی آنجلیز، جرایم سایبر، ترجمه عبدالصمد خرم آبادی و سعید حافظی، انتشارات شورای عالی اطلاع رسانی، تهران، ۱۳۸۳، ص۹.

تبدیل به اینترنت شده بود و عموم مردم می‌توانستند از خدمات ان استفاده کنند.[۲] لذا با این اوصاف تاریخچه مشخص از پیدایش جرایم اینترنتی وجود ندارد ولی به هر حال این دسته از جرایم را باید زائیده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست و بر اساس مطالعات صورت گرفته منشاء پیدایش جرایم اینترنتی به قضیه رویس برمی‌گردد: او که بعد از بی مهری مسئولان یک شرکت فروش عمده میوه و سبری به عنوان حسابدار آنها انتخاب می‌شود از طریق کامپیوتر اقدام به حسابرسی کرده و با تغییر قیمت‌ها و تنظیم درآمد جنس، مبلغی از مراجع آن کاهش و به جای خاص واریز می‌کند. رویس با ظرافت خاص قیمت‌ها را تغییر می‌داد، بعد از آن با نام ۱۷ شرکت محل و طرف قرار داد چک‌های جعلی صادر و از آن حساب برداشت می‌کرده به طوری که در کمتر از ۶ سال بیش از یک میلیون دلار به دست آوردهاست، اما به علت نداشتن مکانیزم برای توقف این روند، رویس خودش را با محاکم قضایی معرفی می‌کند و به ۱۰ سال حبس محکوم می‌شود. بدین ترتیب زمینه جرم رایانه‌ای شکل می‌گیرد و دادگاه را به تدوین قوانین مدون وا می‌دارد.[۳] لذا به طور کلی تحول تاریخی جرایم رایانه‌ای را از مان پیدایش رایانه تا اوایل هزاره سوم می‌توان به سه نسل طبقه‌بندی نمود. نسل اول این گونه جرایم که تا اواخر دهه ۸۰ مصداق داشت تحت عنوان جرایم رایانه‌ای بیان گردید که بیشتر شامل سرقت و کپی برداری از برنامه‌ها و جرایم علیه حریم خصوصی در رایانه بود که با گسترش تکنولوژی تبادل اطلاعات و ارتباطات بین المللی در دهه ۹۰ جرایم نسل دوم تحت عنوان جرایم علیه داده‌ها نمود بیشتری پیدا نمود، به طور که در این دهه تمامی

[۱] – خرم آبادی، احمد، حقوق کیفری فناوری اطلاعات مسئولیت کیفری ارایه دهندگان خدمات اینترنتی، نشر دادیار، ۱۳۹۱.

[۲]- WWW.hamshahrionline.ir /details/۱۰۶۷۵

جرایم علیه تکنولوژی اطلاعاتی، ارتباطی، رایانه‌ای، ماهواره‌ای و شبکه‌های بین المللی تحت عنوان جرایم علیه داده‌ها اطلاق می‌شود. در اوسط دهه ۹۰ با گسترش شبکه‌های بین المللی و ارتباطات ماهواره‌ای نسل سوم جرایم رایانه‌ای، تحت عنوان جرایم مجازی(سایبر) یا جرایم در محیط سایبر شکل گرفته است که با توجه به ماهیت خاص خود بیش از هر زمانی نظامات حقوقی را به خصوص در حقوق جزای ماهوی و حقوق جزایی بین الملل و آئین دادرسی دچار چالش‌های جدی نموده است. پیشینه تاریخی جرایم ناظر به توسعه و تحول جهانی «تکنولوژی اطلاعاتی» به دهه ۱۹۶۰ بر می‌گردد، زمانی که اولین مواردی که بدان «جرم رایانه‌ای» نام نهادند، به مطبوعات عمومی و مجلات علمی آن زمان منعکس شد، این موارد در برگیرنده ظهور اولیه و ساده به کارگیری رایانه شامل جاسوسی رایانه‌ای، خرابکاری رایانه‌ای و سوء استفاده غیر قانونی از سیستم‌های رایانه‌ای بود. از اواسط دهه ۱۹۷۰ مطالعات تجربی در مورد جرایم رایانه‌ای آغاز شد. این مطالعات تعداد محدودی از جرایم رایانه‌ای را مطرح نمود اما در همان زمان تعداد بسیاری جرایم رایانه‌ای صورت گرفته بود که یا گزینش نشده بود یا اصولاً شناخته شده نبود، از نمونه این جرایم می‌توان به قضیه «امریکن اکویتی فوندینگ» در آمریکا(کلاهبرداری از طریق سوء استفاده از ۵۶ هزار مورد بیمه به ارزش حداقل ۳۰ میلیون دلار) و قضیه «هراشتات» در آلمان (مربوط به معاملات ارزی خارجی به ارزش چند میلیون دلار که منجر به ورشکستگی بانک هراشتات در سال ۱۹۷۴ و ورود ضرر بالغ بر ۱/۲ میلیون مارک آلمان به مشتریان گردید) اشاره نمود. در دهه ۹۰ میلادی همزمان با رشد سریع تکنولوژی رایانه و فراگیر شدن شبکه جهانی اینترنت جرایم رایانه‌ای شکل و ابعاد جدیدی به خود گرفته است در این دهه علاوه بر جرایم شناسایی شده می‌توان به جرایم جدیدی از قبیل قاچاق کلمات رمز در اینترنت جرایم در محیط مجازی یا جرایم

سایبری، جرایم مولتی مدیا (چند رسانه‌ای) اشاره نمود فعالیت‌های فراملی مجرمانه در خصوص جرایم رایانه‌ای و اینترنتی امروزه ابعاد جدیدتری یافته و روز به روز به گستردگی آن افزوده می‌گردد. به طوری که برخی از مؤسسات و سازمان‌های بین المللی در این زمینه اقداماتی نمودند که ذیلاً به آنها اشاره می‌شود. تصویب موافقتنامه جرایم رایانه‌ای در سال ۱۹۸۶ – ۱۹۸۵ توسط شورای اروپا که نتیجه تلاش سازمان همکاری و توسعه اقتصادی اروپا (OECD) کمیته تخصص شورای اروپا، سازمان ملل و انجمن حقوق جزاء (AIDP) می‌باشد که هر یک از سازمان‌های مذکور گام‌های بلندی برای تدوین قوانین مرتبط به جرایم رایانه‌ای بردشاته و تقسیم بندی‌های در ارتباط با این گونه جرایم پیشنهادی نموده‌اند.

در سال ۱۹۸۹ کمیته تخصص شورای اروپا در خصوص جرایم رایانه‌ای پس از بررسی نظریه‌های ارائه شده توسط سازمان همکاری و توسعه اقتصادی اروپا (OECD) و نیز بررسی‌های حقوقی دو فهرست تحت عنوان فهرست حداقل یا اجباری و فهرست اختیاری برای تدوین و یکنواخت نمودن سیاست جنایی مربوط به جرم رایانه‌ای به شورای اروپا پیشنهاد نمود که مورد تصویب واقع شد در سال ۱۹۹۴ انجمن بین‌المللی حقوق جزا (AIDP) در نشست خود یک‌سری اعمال و افعال را به عنوان جرایم مستقل رایانه‌ای تدوین نمود تا این که بالاخره شورای اروپا در ۲۳ نوامبر سال ۲۰۰۱ میلادی مبادرت به وضع موافقتنامه جرایم رایانه‌ای نمود که بدون شک نتیجه سال‌ها تلاش مستر آن شورا و سازمان‌های مختلف بین‌المللی بوده است. لازم به ذکر که این موافقتنامه در چهار فصلی و چهل و هشت گفتار تصویب شده است[۱].

[۱] – بابازاده. قاسم – خبرنامه انفرماتیک، ش ۸۱، سال ۱۳۸۱

بخش دوم: بررسی حقوقی جرایم مالی و اقتصادی در فضای مجازی

جرایم مالی و اقتصادی یکی از انواع جرایم کلاسیک و سنتی محسوب می‌شوند که در فضای سایبر نیز قابلیت تحقق دارند. بین جرایم مالی و اقتصادی تفاوت‌هایی وجود دارد. جرایم مالی و اقتصادی یکی ازانواع جرایم کلاسیک و سنتی محسوب می‌شوند که در فضای سایبر نیز قابلیت تحقق دارند. بین جرایم مالی و اقتصادی تفاوت‌هایی وجود دارد. جرایم مالی جرایمی هستند که معمولاً به صورت فردی ارتکاب می‌یابند و هدف مرتکب بردن یا تخریب مال دیگری است در حالی که جرایم اقتصادی به صورت سازمان یافته ارتکاب می‌یابد و موجب آسیب دیدن اساس و پایه‌های اقتصادی کشور می‌شود....

جرایم اقتصادی، موضوع رشته مستقلی از حقوق کیفری اقتصادی می‌باشند. ارزش‌های که مورد حمایت این قانون قرار می‌گیرند. غالباً ماهیت فنی دارند و این جرایم را به جرایم مادی صرف تبدیل می‌کنند. و طی آن، عمل مجرمانه مرتکب صرف نظر از عنصر روانی وی قابل مجازات است و حتی بی احتیاطی و بی مبالاتی مرتکب نیز با پاسخ کیفری همراه می‌شود. ضمانت اجرای جرایم مالی و اقتصادی عمدتاً جنبه مالی دارد و در غلب جریمه متبلور می‌شود زیرا هدف مرتکبین این جرایم کسب سود و منفعت مالی می‌باشد. لذا مجازات‌های نقدی که باعث کاهش درآمدهای آنان و برگرداندن درآمدهای نامشروع آنان می‌شود، مجازات مناسبی برای آنان می‌باشد. عنوان جرایم مالی و اقتصادی در گزارش یازدهیمن کنگره پنج سالانه پیشگیری از جرایم و عدالت کیفری سازمان ملل متحد به کار رفته است که در بند ۱۸۷ این گزارش آمده است، که افزایش جرایم اقتصادی و مالی ناشی از پدیده جهانی شدن و پیشرفت‌های فناوری اطلاعات است و این جرایم نه تنها بر اوضاع اقتصادی و مالی تأثیر منفی گذاشته و منجر به بی اعتمادی

در دنیای تجارت می‌شوند بلکه آثار منفی دراز مدت بر دموکراسی و حکمرانی مطلوب خواهند گذاشت و این تأثیر منفی در کشورهای در حال توسعه به مراتب بیشتر از کشورهای توسعه یافته است. در کنگره پیشگیری از جرایم سازمان ملل متحد آثار مخرب جرائم مالی در فضای مجازی را خطرناکتر از جرایم سنتی علل خصوص برای کشورهای در حال توسعه پیش‌بینی نموده و کارشناسان خطرات ناشی از آن را بی اعتمادی در دنیای تجارت و تأثیر منفی بر دموکراسی عنوان نموده‌اند که در این فصل سعی می‌شود تا دو جرم از مهم‌ترین جرایم مالی و اقتصادی که در فضای سایبری ارتکاب می‌یابد مورد بررسی قرار می‌گیرد در مبحث اول جرم کلاهبرداری در فضای مجازی و در مبحث دوم جرم پولشویی که از اصلی‌ترین جرایم اقتصادی می‌باشد مورد بررسی قرار می‌گیرد.

بند اول: کلاهبرداری رایانه‌ای

در حقوق جزایی کلاسیک کلاهبرداری از جمله جرایم علیه اموال محسوب می‌شود. بعد از پیشرفت سیستم‌های رایانه‌ای کلاهبرداری رایانه‌ای یکی از مطرح‌ترین و مهم‌ترین جرایمی است که بوجود آمده است. این جرم در زمره جرایمی است که توسط یقه سفیدها[1]صورت می‌گیرد. یقه سفیدها افرادی هستند که به دلیل موقعیت اجتماعی و سیاسی و اقتصادی بالای خود کمتر در مظان اتهام قرار می‌گیرند و به دلیل هوش و توانایی بالایی که دارند مرتکب جرایم مدرن و نوین می‌شوند. به همین دلیل جرایم آنان کمتر کشف می‌شود و رقم سیاه آن بالاتر می‌باشد[2]. جرم کلاهبرداری کلاسیک متفاوت

۱-White *Colour*

۲- نجفی،ابرند آبادی، علی حسین، تقریرات درس جرم شناسی، مقطع ارشد حقوق جزا، دانشگاه شهید بهشتی سال ۸۵

از کلاهبرداری رایانه‌ای می‌باشد هر چند نتیجه هر دوی آنها برای مال دیگری می‌باشد ولی روش ارتکاب جرم کلاهبرداری کلاسیک با کلاهبرداری رایانه‌ای متفاوت می‌باشد. زیرا عنصر فریب شرط لازم و ضروری برای تحقق کلاهبرداری کلاسیک می‌باشد و مرتکب باید با انجام مانور متقلبانه، فرد را فریب دهد و از این طریق مال وی را ببرد، در حالی که در کلاهبرداری رایانه‌ای نیازی به فریب دیگری نیست و به صرف این که کاربر با انجام اقداماتی و از طریق اخلال در داده‌های رایانه‌ای در فضای سایبر یا عملکرد سیستم‌های رایانه‌ای به منفعت یا مالی دست پیدا کند جرم کلاهبرداری رایانه‌ای تحقق پیدا می کند. از طرفی مصادیق توسل به وسایل متقلبانه در کلاهبرداری کلاسیک با کلاهبرداری رایانه‌ای متفاوت است و حتی در قوانین برخی کشورها شرط متقلبانه بودن رفتار مرتکب یا صاحب مال با امور فیزیکی توسل به وسایل متقلبانه مواجه نیست وی تماماً با داده‌های اطلاعاتی و سیستم‌های رایانه‌ای سرو کار دارد و با برنامه نویسی نادرست یا تغییر داده‌ها یا هر گونه تقلب در سیستم رایانه‌ای بانک یا مؤسسات دیگر اموال را به دست می آورد. بنابراین قوانین مربوط به کلاهبرداری کلاسیک نمی‌تواند جوابگوی کلاهبرداری رایانه‌ای باشد، در قوانین بسیاری از کشورها مثل آلمان و نروژ، دانمارک، سوئد و پرتقال تعاریف قانون کلاهبرداری محتاج به این است که شخص فریب بخورد. قوانین این کشورها شامل مواردی که مرتکب صرفاً از طریق سوء استفاده از رایانه و بدون فریب انسان مال دیگری را می‌برد، نمی‌شود. بنابراین قوانین کلاسیک این کشورها شامل مواردی مانند سوء استفاده از صندوق‌های پرداخت و سایر صور کلاهبرداری رایانه‌ای نمی‌شود این کشورها با اصلاح قوانین کیفری خود یا وضع قوانین جدید در

مقابل کلاهبرداری رایانه‌ای عکس العمل نشان داده‌اند[۱]. لازم به ذکر است که کاربر ممکن است از طریق رایانه یا شبکه‌های رایانه‌ای مانند اینترنت در فضای مجازی برای فریب دیگری استفاده کند مثلاً فردی در حین چت با دیگری وی را با حرف‌های خود فریب می‌دهد مثلاً به او وعده می‌دهد که اگر پول خود را در اختیار وی قرار دهد وی با سرمایه‌گذاری آن پول سود خوبی نصیب وی خواهد کرد و آن فرد نیز این کار را انجام می‌دهد، در این صورت جرم کلاهبرداری رایانه‌ای تحقق پیدا نمی‌کند بلکه این عمل مصادیق کلاهبرداری کلاسیک می‌باشد و با همان قوانین کلاسیک قابل تعقیب و مجازات می‌باشد، زیرا در این مثال کاربر از رایانه به عنوان یک وسیله برای ارتکاب جرم استفاده کرده است و با فریب وی مال را برده است. و این عمل متفاوت است با کاربردی که از طریق اخلال در داده‌های رایانه‌ای با عملکرد سیستم‌های رایانه‌ای بدون این که دیگری را فریب دهد مال وی را می‌برد و از لحاظ تاریخی اولین کلاهبرداری رایانه‌ای مربوط به دهه ۱۹۶۰ قضیه الدون رویس که در مبحث تاریخچه جرائم توضیح داده شده می‌باشد. بنابراین دهه ۱۹۶۰ تاریخ وقوع اولین جرم کلاهبرداری رایانه‌ای می‌باشد. از آن تاریخ به امروز کلاهبرداری رایانه‌ای اشکال متنوع‌تری پیدا کرده است.

الف) سوء استفاده از شبکه تلفنی

سوء استفاده از شبکه تلفنی در دهه‌های ۷۰ و ۸۰ میلادی به منظور اجتناب از پرداخت هزینه مکالمات تلفنی انجام می‌شد ولی شکل جدیدی سوء استفاده از شبکه تلفنی در دهه ۹۰ شکل گرفت که به منظور سوء استفاده مالی و انتقال پول به وسیله شرکت‌های

[۱] – ریک، کاسپرسنوبرژ، امنیت اطلاعات و تحقیقات جنایی، ترجمه محمد حسن دزیانی سازمان برنامه بودجه ۱۳۷۶

تلفنی میسر شد. در این نوع کلاهبرداری نفوذگران[۲] که اغلب افرادی جوان هستند با سوء استفاده از تکنیک‌های فنی و به وسیله اختلال در سیستم‌های صوتی و پستی، مکالمات تلفنی خود را با هزینه مشترکین دیگر انجام می‌دهند.

ب) سوء استفاده از صندوق‌های پرداخت

این گونه کلاهبرداری از قدیم با استفاده از کارت‌های مسروقه صورت می‌گرفت ولی امروزه با استفاده گسترده از سخت افزار و نرم افزار به ویژه کامپیوتر، اطلاعات الکترونیکی کذب به صورت کد روی لبه‌های مغناطیسی کارت‌های الکترونیکی و کارت‌های بانک و اعتبار ثبت شده مورد سوء استفاده قرار می‌گیرد. مرتکبین این نوع کلاهبرداری شماره‌های محرمانه ضروری برای سوء استفاده از کارت‌ها را اغلب از طریق تجاوز با مکالمه تلفنی، از طریق تدارک صفحه کلید، نفوذ کردن یا مختل نمودن خطوط مخابرات داده‌ها بدست می‌آورند.[۱]

ج) سوء استفاده از کارت‌های اعتباری

این کارت‌ها به سه گروه تقسیم می‌شوند. اولین گروه، کارت‌های دارای ارزش ذخیره شده می‌باشند که ارزش مورد نظر به طور الکترونیکی روی آن ثبت شده است و مشتریان برای انجام معاملات از آن استفاده می‌کنند این کارت‌ها ممکن است فقط حافظه باشند که مملو از ارزش هستند و برای انجام اعمال ویژه از جمله مکالمات تلفنی به کار می-

---

۱- Hackers

۲– شورای اروپا، جرم کامپیوتری، ۱۹۹۰ ترجمه دبیرخانه شورای عالی انفورماتیک، سازمان برنامه بودجه سال ۱۳۷۶ ص ۱۱۷.

روند که معمولاً پس از پایان ارزش قابل استفاده نیستند و یا این که کارت‌های هوشمند که برای ذخیره کردن اطلاعات دارای حافظه‌های کوچک کامپیوتری می‌باشند.

دومین گروه به کارهای بدهی مربوط می‌شود که قابلیت انجام معاملات و عملیات را دارد و حساب‌های بانکی بلافاصله از طریق ارتباط پیوسته ایجاد شده بین ماشین‌ها و تحویلدار خودکار (ATM) و پایانه‌های انتقال وجود الکترونیکی در محل فورش و بانکها ثبت می‌شود. گروه آخر کارتهای که برای خرید کالا و خدمات مورد استفاده قرار می‌گیرد که پرداخت قیمت آنها در آینده انجام خواهد شد. کارتهای بکار رفته برای کلاهبردارای عموماً کارت‌های سرقت شده یا مفقودی‌اند که ممکن است بدون اینکه تغییری در آن ایجاد شده مورد استفاده قرار گیرند و یا از طریق علامت گذاری مجدد و رمز گذاری مجدد دچار تغییر و یا جعل شوند طرق انجام شده معمول بر روی کارت‌ها برای سوء استفاده شامل رمز گذاری، روخوانی کارت، کلاهبرداری از طریق درخواست و کلاهبرداری از طریق شماره شناسایی شخص می‌باشد.[۱]

بند دوم: پولشویی

پولشویی عنوان کیفری جدیدی است که حقوق جزای بین‌الملل به قلمرو حقوق جزای داخلی راه پیدا کرده است و عبارت از مجموعه اقداماتی است که از طریق آن درآمدهای نامشروع حاصل از فعالیت‌های مجرمانه سازمان یافته، قانونی جلوه داده می‌شود.[۲] ساز و کار پولشویی عمدتاً معطوف به جرایم اقتادی سازمان یافته است و از طریق

[۱] – دزیانی، محمد حسن، کلاهبرداری از طریق کارتهای پلاستیکی، خبرنامه انفورماتیک، شورای عالی انفورماتیک کشور شماره ۶۸ ص ۸۴

[۲] – ولیدی، محمد صالح، حقوق کیفری اقتصادی، چاپ اول، زمستان۸۶، نشر میزان، ص ۲۵۹.

همکاری بین‌المللی و منطقه‌ای جستجو می‌شود. همین امر از جمله عواملی است که ضرورت جرم انگاری پولشویی را فراهم کرده است، به طوری که اقدامات زیادی در دهه‌های اخیر از س وی سازمان‌های بین‌المللی و منطقه‌ای در این زمینه صورت گرفته است. پولشویی دارای خصوصیات خاصی می‌باشد که آن را از سایر جرایم متمایز می-کند. این خصوصیات عبارتند از:

الف) پولشویی یک جرم مستقل است

جرم پولشویی اگر چه وابسته به وجود جرم منشا است ولی دارای ماهیت حقوقی مستقل و پیچیده‌ای است که شامل یک رشته از اعمال مجرمانه‌ای است که از ناحیه مرتکب از طریق تبانی با عده‌ای و با سبق تصمیم به هدف پنهان نگه داشتن یا کتمان واقعیت یا تغییر ماهیت غیر قانونی درآمدهای حاصل از جرم منشا قابل تحقق خواهد بود.

ب) پولشویی جرمی سازمان یافته است

منظور از جرم سازمان یافته، جرمی است که توسط گروه متشکلی که حداقل از سه نفر تشکیل شده و این ساختار برای مدت زمان معینی استمرار پیدا می‌کند و هدف آن نیز، اقدام هماهنگ اعضا گروه برای ارتکاب یک یا چند جرم شدید از قبیل قاچاق مواد مخدر، قاچاق زنان و.. می‌باشد که به منظور کسب مستقیم یا غیر مستقیم منافع و عواید مالی است.[1]

[1] – شمس ناتری، محمد ابراهیم، سیاست کیفری ایران در قبال جرایم سازمان یافته، پایان‌نامه دکتری حقوق جزا، دانشگاه تربیت مدرست، سال ۸۰

ج) پولشویی جرم فرا ملی است

با توجه به این که پولشویی بعد از وقوع جرم سازمان یافته‌ای مانند قاچاق مواد مخدر به وجود می‌آید. مجرمان برای از بین بردن منشأ غیر قانونی درآمد حاصله از قاچاق مواد مخدر اقدام به انتقال آن از طریق معاملات صوری و مبادلات خاص با استفاده از سیستم-های پیشرفته بانکی و مؤسسات مالی به خارج از کشور می‌نمایند و موجبات فرآیند پولشویی را فراهم می‌نمایند. با ظهور فضای سایبر یکی از مهم‌ترین و متداولترین جرایمی که در این فضا و در بستر فناوری مالی نوین ارتکاب می‌یابد پولشویی الکترونیکی می-باشد. پولشویان برای تطهیر درآمدهای حاصل از فعالیت‌های مجرمانه، از روش‌های متعددی استفاده می‌کنند تا در مدت زمان کوتاهی و با گریز ازموانع قانونی به اهداف خود دست پیدا کنند. از این رو روش‌های مورد استفاده پولشویان با توجه به قوانین وضع شده کشورها و امکانات تکنولوژیکی کشورها و همچنین نحوه نظارت آنها بر سیستم-های مالی متنوع می‌باشد. یکی از متداول‌ترین راه‌های پولشویی، استفاده از نظام بانکی و تحت پوشش بانکداری الکترونیکی می‌باشد که پولشویان با شیوه‌های مختلفی که اتخاذ می‌کنند از عدم وجود مقررات کافی برای نظارت بر نقل و انتقالات بانکی استفاده نموده واز این طریق اقدام به تطهیر درآمدهای مجرمانه خود می‌نمایند. باید توجه داشت که پولشویان قادر نیستند بدون کمک بانک‌ها و مؤسسات اعتباری که پیشنهاد تأمین اعتبار ارائه می‌دهند و همچنین بدون استفاده از گریزگاه‌های مالیاتی و دور از کرانه که عبور مقادیر عظیم پول‌های ناپاک از آن طریق ممکن می‌شود، موفقیتی کسب نمایند. لذا با توجه به اهمیتی که پولشویی الکترونیکی دارد در این مبحث به بررسی پدیده پرداخته می‌شود.

یکی از بزرگ‌ترین دغدغه‌های جهانی جامعه بشری، نحوه برخورد با جرائم سازمان یافته فرا ملی ریشه کن کردن این جرایم با همکاری کلیه دولت‌های جهان است. غلبه‌ی پدیده جهانی شدن و تسهیل مبادلات و ارتباطات فرامرزی موجب گسترش جرائم سازمان یافته فرا ملی شده و این نکته را به اثبات رسانیده است که تنها هیچ دولتی از بلایای آن در امان نیست بلکه به خاطر ساماندهی پیچیده و فرامرزی آن هیچ دولتی نیز نمی‌تواند به تنهایی به مقابله و انهدام این شبکه بپردازد. در گذشته، تنها جرایمی چون دزدی دریایی، تجارت برده و نیز برخی از جرایم جنگی به عنوان پدیده جرایم فراملی شناخته شده و مورد تعقیق قرار می‌گرفتند، اما از اوایل دهه‌ی ۹۰ جامعه بشری دریافته است که اهمیت و مضار جرایمی چون قاچاق زنان و کودکان، قاچاق مهاجران، تطهیر پول و فساد مالی بیش از جرایم سنتی فرا ملی است به گونه‌ای که حتی موجودیت و استقلال سیاسی برخی از دولت‌ها را نیز در معرض تعهدید قرار داده‌اند. بدون شک یکی از ویژگی‌های مهم جرایم سازمان یافته فراملی(گذشته از فرا مرزی بودن آن) داشتن تشکیلات و سازماندهی بسیار قوی به همراه بهینه مالی کلان و بالطبع داشتن نفوذ در ارکان دولت‌هاست که مبارزه با این جرم را بسیار دشوار ساخته و همکاری میان دولت‌ها جهت ریشه کنی این گونه جرایم را بیش از پیش ضروری نموده است.[۱] در ماده ۲ قانون مبارزه با پولشویی اینگونه تعریف شده است:

الف- تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از فعالیت‌های غیر قانونی با علم بر اینکه به طور مستقیم یا غیر مستقیم در نتیجه ارتکاب جرم به دست آمده باشد.

[۱] – باقر زاده، احد، جرایم اقتصادی و پولشویی، انتشارات مجد مراد، ۱۳۸۲، ص۹.

ب – تبدیل، مبادله یا انتقال عوایدی به منظور پنهان کردن منشاء غیر قانونی آن با علم به اینکه به‌طور مستقیم یا غیر مستقیم ناشی از ارتکاب جرم بوده یا کمک به مرتکب به نحوری که وی مشمول آثار و تبعات قانونی ارتکاب آن جرم نگردد.

ج – اخفاء یا پنهان یا کتمان کردن ماهیت واقعی، منشاء، منبع، محل، نقل و انتقال جابجایی یا مالکیت عوایدی که به طور مستقیم یا غیر مستقیم در نتجه جرم تحصیل شده است.

ب) نحوه پولشویی در فضای مجازی (سیبری)

پولشویی برای تطهیر درآمدهای مجرمانه خود از روش‌های نوین و مدرنی بهره می‌برند. از جمله این روش‌ها استفاده از پول الکترنیکی و خدمات بانکداری الکترونیکی و همچنین بازار بورس می‌باشد. که در این بخش به بررسی این روش‌ها می‌پردازیم.

پول الکترونیک، همان تکانه‌های الکترونیکی یا داده‌های رایانه‌ای است که واجد اعتبار مالی شده است و با به‌طور کلی دو نوع می‌باشد:

۱.کارت‌های هوشمند[۱]: که به آنها پول الکترونیک آنلاین هم گفته می‌شود و در قابل کارت‌های اعتباری یا بدهی **(debit cards)** یا حتی ساده‌ترین شکل یعنی کارت‌های

[۱]-Smart Cards

[۲]-کارت‌های هوشمند دارای یک پردازنده کوچک می‌باشند که حاول یک مدار مجتمع است که تعداد محدوی حافظه و هوش دارد که به آن توانایی استقلال در تصمیم گیری را می‌دهد. این کارت‌ها برای ذخیره کردن داده‌ها و اطلاعات دارای حافظه‌های کوچک کامپیوتری به کار می‌روند. این کارت‌ها قابلیت انجام عملیات و معاملات را دارند و حساب-های بانکی بلافاصله از طریق ارتباطات پیوسته ایجاد شده بین ماشین‌های تحول‌دار خودکار و پایانه‌های انتقال وجوه الکترونیکی،در محل فروش و بانک‌ها ثبت میشود.

تلفن ظهور پیدا کرده‌اند. دلیل نامگذاری این کارت‌ها به پول الکترونیک آنلاین است که نقل و انتقال وجوه به وسیله آنها از طریق دستگاه‌های خاصی نظیر خود پردازها صورت می‌گیرد.

۲. پول الکترونیک کامپیوتری: این پول حتی به اندازه کارت‌های هوشمند هم وجود خارجی ندارد و به‌طور کلی برای فضای تبادل اطلاعات طرح ریزی شده است. برای دسترسی به وجود آنلاین لازم است پیشاپیش نزد مؤسسه اعتباری یا بانکی که از این فناوری برخوردار است وجه یا اعتباری سپرده شود، سپس یک شماره اعتباری در اختیار مشتری قرار می‌گیرد که می‌تواند از طریق رایانه شخصی خود از منزل یا هر جای دیگر با اتصال به اینترنت اقلام مورد نیاز خود را تهیه و برای پرداخت وجه فقط آن شماره در اختیار سایت مورد نظر قرار می‌دهد که آن نیز به‌طور خودکار به سایت بانک یا مؤسسه مربوطه متصل می‌شود و وجه مورد نظر را به حساب خود منتقل می‌کند . با توجه به مطالب گفته شده مفهوم بانکداری الکترونیک نیز روش می‌شود که به طور کلی می‌توان آن را انجام امور بانکی به شکل الکترونیکی دانست که در اینجا به جای ساختمان، نیروی انسانی و اسناد و اوراق کاغذی با فضای تبادل اطلاعات و یک سری برنامه‌های کاربردی و اسناد دیجیتال سروکار داریم. این فناوری جدید چنان برای پولشویان شگفت انگیز بوده که آن را بهشت خود نامیده‌اند یکی از مهم‌ترین ابزارهایی که در پول و بانکداری الکترونیک برای اجرای صحیح امور و بالا برد ضریب اطمینان کارکردها به کار می‌رود، فناوری رمزنگاری و امضای دیجیتال می‌باشد. به‌طور خلاصه کارکرد فناوری رمزنگاری

۱- جلالی، فراهانیف امیر حسبن، پولشویی الکترونیکی، فصل‌نامه تخصصی فقه و حقوق، سال اول، شماره ۴،بهار ۸۴، ص ۱۲۱.

این است که محتوا را به شکلی نامفهوم و غیر قابل درک تبدیل می‌کند و برای اینکه به حالت اولیه برگردد لازم است فرآیند رمز گشایی اجرا شود که بدیهی است فقط سازنده و واگذارنده این فناوری و ارسال کننده و دریافت کننده محتوا توانایی انجام آن را دارند[۱]. با توجه به این توضیحات مشخص می‌شود که اگر پول الکترونیک رمزنگاری شود دیگر محتوای آن نامفهوم خواهد شد و تنها دریافت کننده آن که مشخص نیست در کدام نقطه از جهان قرار دارد می‌تواند با اجرای برنامه رمزگشایی مربوطه از آن آگاهی یابد. به این ترتیب چنان سطحی از محرمانه بودن و ناشناس ماندن برای این مبادلات مهیا می‌شود که هر کس می‌تواند از هر جای دنیا مبلغ مورد نظر خود را به نقطه‌ای دیگر ارسال کند، بی آنکه کسی از محتوای آن آگاهی یابد. و این حالت بهترین وضعیت ممکن را برای پولشویان فرهم می‌کند چون آنها دیگر مجبور نخواهند بود برای تطهیر اموال نامشروع خود مراحل سه گانه مورد نظر را طی کنند یا به خاطر آن مرتکب جرایم دیگری نظیر حمل، تطهیر یا تهدید کارمندان مؤسسات مالی و بانکی شوند. در کشورهایی مثل آمریکا که محل عمده خرید و فروش مواد مخدر است امکان واریز این وجوه کلان به حساب‌های بانکی یا انجام خریدهای نقدی به وسیله آنها وجود ندارد. چرا که اولاً بانک‌ها بدون شناسایی کامل مشتری از افتتاح حساب برای وی سرباز می‌زنند. ثانیاً در آمریکا نه تنها بانک‌ها که افراد و مؤسساتی مثل صرافی‌ها، بنگاه‌های ملی و حتی و کلا از اواسط دهه ۸۰ میلادی طبق قانون موظف شده‌اند موارد مشکوک و نیز معاملات نقدی بالاتر از ده هزار دلار را به مقامات دولتی گزارش دهند.[۲] بنابراین پولشویان راهی

---

[۱] – موسوی مقدم، محمد، تطهیر درآمدهای ناشی از جرم، انتشارات ابان، سال ۸۱، ص۹۶.

[۲] – جزایری، مینا، پولشویی به عنوان یک جرم مستقل، مجموعه مقالات همایش بین المللی مبارزه با پولشویی، خردید ۸۲، نشریه مبارزه با مواد مخدر، ص ۹۷.

جز انتقال اسکناس‌ها و چک‌ها به خارج از آمریکا و گذاشتن آنها در بانک‌های کشورهای دیگر و سپس در صورت لزوم، انتقال مجدد آنها از طریق نظام بانکی بین-المللی به بانک‌های آمریکایی ندارند. به‌طور کلی کشورهای جهان را از لحاظ نظام ارزی به دو دسته اصلی می‌توان تقسیم کرد: در یک دسته از کشوها، نظام ارزی حاکم می‌باشد که در آنها ورود و خروج ارز آزاد می‌باشد. دولت و بانک مرکزی در بازار ارز مداخله نمی‌کنند و بازار ارزی این دسته از کشورها در واقع یک بازار جهانی ارز را تشکیل می-دهد. در مقابل دسته دیگری از کشورها، دارای نظام کنترل ارزی می‌باشند. در این کشورها ورود و خروج ارز در کنترل و هدایت مقامات سیاسی و ارزی می‌باشد و بالطبع ارتباط آزاد با بازارهای جهانی وجود ندارد. بسیاریاز کشورها به ویژه کشورهای جهان سوم با جای گرفتن در دسته اخیر، حق دشتن حساب‌های ارزی را به شهروندان خود نمی‌دهند. کنترل‌های تبدیل ارز همچنین در کشورهایی که ارز آنها در مقایسه با ارزهای خرجی قوی‌تر، ضعیف است برای جلوگیری از اقدام شهروندان به خارج ساختن دارایی-های خود از قلمرو اختیارات کشور، اعمال می‌گردد. اگر کشوری در امور ارزش سخت‌گیری و محدودیت بیش از حد به خرج دهد، مجریان و پولشویان، پول‌های خود را به قلمرو قضایی دیگری که همکاری بیشتری با آنها می‌نماید منتقل می‌کنند.[1] یکی از شایع‌ترین روش‌ها برای انتقال سرمایه یا وجوه نقد خارج از کشور استفاده از بانک‌ها و مؤسسات مالی است که دارای فعالیت بین‌المللی می‌باشند. برای بازگرداندن پول نامشروعی که داترای پوشش مشروع است به کشور، رایج‌ترین روشی که مورد استفاده پولشویان قرار می‌گیرد اخذ وام‌های صوری است. به عنوان مثال یک جنایکتکار

[1] – جلالی فرهانیف امیر حسین، همان، ص ۱۲۳.

آمریکایی که از طریق ارتکاب اعمال مجرمانه ۵۰۰/۰۰۰ دلار بدست آورده است آن را با خارج کردن از کشور، به حساب بانکی‌اش در لوکزامبورگ واریز می‌کند. برای بازگرداندن پول به کشور مبدأ، مبلغ ۱/۰۰۰/۰۰۰ دلار در رستوران‌ها سرمایه‌گذاری می‌کنند. برای پرداخت این مبلغ ۵۰/۰۰۰ دلار از پول پاک حاصل از منابع مشروعی را که در اختیار دارد پرداخت می‌کند. آنگاه ۴۵۰/۰۰۰ دلار از یک بانک محلی آمریکایی وام می‌گیرد و بقیه پول مورد نیاز خود را که ۵۰۰/۰۰۰ می‌باشد، از بانک خود در لوکزامبورگ وام میگیرد. ۵۰۰/۰۰۰ دلار اخیر یک وام صوری است که در واقعی برداشت پول از حساب خودش است. در این روش پول حاصل از ارتکاب اعمال مجرمانه با پوشش قانونی وام به کشور بر می‌گردد.[۲]

بند سوم: بررسی پولشویی سایبری در حقوق ایران

با بررسی قوانین ایران به این نتیجه می‌رسیم که تا قبل از تصویب قانون مبارزه با پولشویی، آنچنان جدی به این موضوع پرداخته نشده و تنها به صور ابتدایی پولشویی اشاره شده است. مهم‌ترین قوانینی که تا قبل از قانون پولشویی در این زمینه وجود داشته، اول قانون نحوه اجرای اصل ۴۹ قانون اساسی است که بیش از آن که به دنبال جرم انگاری تطهیر پول باشد به دنبال استرداد اموال نامشروع به صاحبان آنها می‌باشد. به موجب اصل ۴۹، دولت موظف است ثروت‌های ناشی از ربا، غصب،رشوه، اختلاس، سرقت، قمار و ... را گرفته و به صاحب حق رد کند [۲]. ماده ۱۴ قانون نحوه اجرای اصل

---

[۱]- U.N.G $lobat$, $programme$. Against mony laundering U.N. office for control and crime prevention (UN-ODCCOP) $vienna,Austiria$ ۱۹۹۱

[۲] – برای آگاهی بیشتر رجوع کنید به مجموعه قوانین و مقررات مربوط به جرایم قاچاق کالا و ارز، نشر میزان، چاپ اول، پاییز ۱۳۸۲، ص۲۶۸ – ۲۸۰

۴۹ نیز برای انتقال دهنده و انتقال گیرنده چنین ثروت‌هایی مجازات کلاهبرداری تعیین کرده است. هر چند عده‌ای اعتقاد دارند که اصل ۴۹ قانون اساسی قابلیت لازم در خصوص مبارزه با جرم پولشویی را دارد لیکن، طبق اصل یاد شده وظیفه دولت صرفاً ناظر به ضبط اموال حاصل شده از مجاری غیر قانونی بوده در حالی که پولشویی، پلی است که اقتصاد رسمی و قانونی کشور را به اقتصاد غیر رسمی و غیر قانونی متصل می‌سازد به همین دلیل جلوجگیری از پولشویی و ورود وجوه و منابع غیر قانونی به سیستم مالی کشور مستلزم داشتن مبانی قانونی جهت شناسایی مشتریان، گزارش عملیات مشکوک و ... می‌باشد. ماده ۶۶۲ قانون مجازات اسلامی [۳] شکل ساده‌ای از پولشویی را که عبارت از تحصیل، مخفی یا قبول کردن و مورد معامله قرار دادن مال مسروقه می‌باشد جرم و شایسته مجازات دانسته است. همچنین برای افرادی که حرفه خود را چنین کاری قرار داده‌اند حداکثر مجازات را پیش بینی کرده است.

اوراق بهادار به سبب برخورداری از ویژگی‌های منحصر به فرد از بازارهایی است که توجه پولشویان را بیش از پیش به خود جلب می‌کند این ویژگی‌های عبارتند از :

- بازار اوراق بهادار در کار تأمین سرمایه از پیچیدگی زیادی برخوردار است.
- فرهنگ سنتی نظام مالی، براین بخش از بازار حاکم نیست.
- راهی که به واسطه آن، بسیاری از معاملات مورد تعهد این بازارها انجام می‌گیرد دارای ماهیت بین‌نام و نشانی است.

[۱]– ماده ۶۲۲ ق.م هر کس با علم و اطلاع یا با وجود قرائن اطمینان آور به اینکه مال در نتیجه ارتکاب سرقت به دست آمده است آن را به نحوی از اتحاء تحصیل یا مخفی یا قبول نماید یا مورد معامله قرار دهد به حبس از شش ماه تا سه سال و تا ۷۴ ضربه شلاق محکوم می‌شود.

دسترسی همیشگی به اوراق بهادار صرف نظر از رونق یا کسادی بازار امکان پذیری است. چنین بازارهایی برای فعالیت کارآمد نیاز به تبدیل دارایی‌های خود به پول دارند و توانایی بازار سازان در دسترسی به منابع عظیم در کوتاه مدت دارای اهمیت بزرگی است. لذا جریان یافتن بی قید و شرط سرمایه از نظر عاملان بازار، از بالاترین اولویت برخوردار است. توانایی تهیه مقادیر هنگفت پول نقد به همراه توایی تغییر چهره دادن این مبالغ است که باعث می‌گردد اوراق بهادار این چنین برای پولشویان و گروه‌های جرم گرای سازمان یافته جذاب جلوه کند.[۲] دلالان سهام شرکت‌ها ضرورتاً شناخت مستقیم و بلافصلی از مشتریان خود ندارند بلکه بیشتر این معاملات به نمایندگی وکلای دعاوی یا مشاوران مالی یا از طریق یک بانک خارجی صورت می‌گیرند. با این وجود اوراق بهادار باز هم می‌تواند به وسیله حساب‌هایی که به خود دلالان تعلق دارد، معامله شوند. در یکی از روش‌های موفقیت آمیز، سهام واحدی که در اختیار یک پولشوقرار داشت و واسطه دو مجمع مصلحت نظام و مجلس سرانجام به تصویب رسید. که به بررسی اجمالی این قانون می‌پردازیم. در ماده ۲ این قانون، پولشویی این گونه تعریف شده است:

الف) تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از فعالیت‌های غیر قانونی با علم بر این که به طور مستقیم یا غیر مستقیم در نتیجه ارتکاب جرم به دست آمده باشد.

ب) تبدیل، مبادله یا انتقال عوایدی به منور پنهان کردن منشأ غیر قانونی آنبا علم به این که به طور مستقیم یا غیر مستقیم ناشی از ارتکاب جرم بوده یا کمک به مرتکب به نحوری که وی مشمول آثار و تبعات قانونی ارتکاب آن جرم نگردد.

---

[۱]– جعفری، مجتبی، مطالعه تطبیق بورس و اوراق بهادار در حقوق جزایی ایران و فرانسه، پایان‌نامه کارشناسی ارشد، دانشگاه امام صادق، مرداد ۸۶ ص ۱۳۷

ج) اخفاء یا پنهان یا کتمان کردن ماهیت واقعی، منشأ، منبع، محل، نقل و انتقال، جابجایی یا مالکیت عوایدی که به طور مستقیم یا غیر مستقیم در نتیجه جرم تحصیل شده است. نهایتاً فهمیدیم و همان‌گونه که ملاحظه می‌شود وضع کنندگان قانون پولشویی در تبیین مقررات مربوط به تطهیر درآمدهای مجرمانه با تبعیت از کنوانسیون پالرمو مصوب سال ۲۰۰۰ معنای اعم را برگزیده و شستشوی عواید و منافع منقول و غیر منقول ناشی از کلیه جرایم را به عنوان عنصر مادی این جرم قابل مجازات می‌دانند. به علاوه سوءنیت عام مرتکب بر انجام فعل مجرمانه به گونه‌ای که در بندهای سه گانه ماده دو لایحه احصاء شده است، عنصر روانی این جرم را تشکیل می‌دهد و صرف علم مرتکب به اینکه افعل مندرج در این ماده را بر روی اموالی عملی ساخته که به طور مستقیم یا غیر مستقیم ناشی از ارتکاب جرم می‌باشد در تحقق جرم پولشویی کفایت می‌کند و سوءنیت خاص و تحصیل نتیجه شرط تحقق این جرم نمی‌باشد.

منابع و مآخذ

۱) منابع فارسی

الف – کتاب‌ها

۱. باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، انتشارات بهنامی، چاپ دوم، ۱۳۸۶

۲. باقر زاده، احد، جرایم اقتصادی و پولشویی، انتشارات مجد، چاپ اول، مرداد ۱۳۸۳.

۳. پولشویی، مجموعه سخنرانی‌ها و مقالات همایش بین‌المللی مبارزه با پولشویی، نشر وفاق، چاپ اول، ۱۳۸۲.

۴. جرایم یقه‌سفیدها، ترجمه گروه مترجمین اداره کل پژوهش و تألیفات ناجا، چاپ اول، ۱۳۷۹.

۵. جلالی، امیر حسین، جزوه ادله دیجیتال (ترجمه)، دبیرخانه شورای عالی و توسعه قضایی، ۱۳۸۲.

۶. جینادی، آنجلیز، جرایم سایبری، ترجمه عبدالصمد خرم آبادی و سعید حافظی، انتشارات شورای عالی اطلاع‌رسانی، ۱۳۸۲.

۷. خرم آبادی، احمد، مسولیت کیفری ارایه دندگان خدمات اینترنتی، نشر دادیار ۱۳۹۱

۸. دزیانی، محمد حسن، جزوه آموزشی حقوق سایبر و جرایم سایبری، تهیه شده برای معاونت آموزش دادگستری تهران، ۱۳۸۲.

۹. زیبر، اولریش، مسئولیت برای خدمات بانک‌های داده آنلاین، ترجمه سیامک قاجار، انتشارات سازمان مدیریت، چاپ اول، ۱۳۸۴.

۱۰. شکری، رضا، قانون مجازات اسلامی در نظم حقوق کنونی، انتشارات نشر مهاجر، چاپ دوم، ۱۳۸۲.

۱۱. گلدوزیان، ایرج، محشای قانون مجازات اسلامی، نشر میزان، چاپ هفتم، ۱۳۸۱.

۱۲. مجموعه مقالات همایش بررسیق جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضاییه، نشر سلسبیل، چاپ اول، ۱۳۸۴.

۱۳. میر محمد صادقی، حسین، جرایم علیه اموال و مالکیت، نشر میزان، چاپ پنجم، ۱۳۸۴.

ب – تقریرات و مقالات

۱. بهروز، مسعود، جرایم مربوط به مالکیت معنوی، خبرنامه انفورماتیک، دبیرخانه شورای عالی انفورماتیک، شماره ۷۶ ، ۱۳۷۹.

۲. پاکزاد، بتول، اقدام‌های سازمان‌های بین‌المللی و منطقه‌ای در خصوص جرم‌های رایانه‌ای، مجموعه مقالات همایش بررسی ابعاد حقوق فناوری اطلاعات، ۱۳۸۳.

۳. پرویزی، رضا، جرایم کامپیوتری، مجموعه مقالات اولین همایش تخصصی بررسی جرایم رایانه‌ای، نیروی انتظامی جمهوری اسلامی ایران، ۱۳۸۰.

۴. تحیری، فرزاد، دسترسی غیر مجاز جلوه‌ای از جرایم رایانه‌ای محض، مجموعه مقالات همایش بررسی ابعاد فناوری اطلاعات، ۱۳۸۳.

۵. ترکی، غلامعباس، نگرش علمی و کاربردی به قانون جرایم رایانه‌ای، مجله دادرسی، شماره۷۸

۶. جاویدنیا. جواد نقد و بررسی جرم‌های مندرج در قانون تجارت الکترونیکی.مجله حقوقی دادگستری شماره ۵۹ سال ۱۳۸۶

۷. جزایری، مینا، پولشویی به عنوان یک جرم مستقل، مجموعه مقالات همایش بین-المللی مبارزه با پولشویی، نشریه ستاد مبارزه با مواد مخدر، ۱۳۸۲.

۸. جلالی فراهانی، امیر حسین، پولشویی الکترونیکی، فصلنامه تخصصی فقه و حقوق، سال اول، شماره ۴، ۱۳۸۴.

۹. خرم آبادی، عبدالصمد، تاریخچه، تعریف و طبقه بندی جرایم فناوری اطلاعات، مجموعه مقالات همایش بررسی ابعاد حقوق فناوری اطلاعات، ۱۳۸۳.

۱۰. دریانی، محمدحسن، جعل کامپیوتری، خبرنامه انفورماتیک، سازمان مدیریت و برنامه‌ریزی، شماره ۷۵.

۱۱. روحانی، محمدخیام، جرایم کامپیوتری، خبرنامه انفورماتیک، دبیرخانه شورای عالی انفورماتیک، شماره ۷۶.

۱۲. زرکلام، ستار، قانون تجارت الکترونیک و الفبای الکترونیکی، مجموعه مقالات همایش بررسی ابعاد حقوق فناوری اطلاعات، ۱۳۸۳.

۱۳. شهرستانی، سید محمد امین، نقض حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، مجموعه مقالات بررسی ابعاد حقوق فناوری اطلاعات، ۱۳۸۳.

۱۴. عالی‌پور، حسن، جرایم مرتبط با محتوا، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، ۱۳۸۳.

ج – پایان‌نامه‌ها

۱. باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکز، ۱۳۸۱.

۲. باقر زاده، احد، جرم تطهیر درآمد و سرمایه‌های حاصل از قاچاق بین‌المللی مواد مخدر در حقوق ایران و انگلیس و حقوق بین‌المللی، رساله دکتری، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات،۱۳۸۳.

۳. جعفری، مجتبی، مطلعه تطبیقی جرایم بورس و اوراق بهادار در حقوق جزای ایران و فرنسه، کارشناسی ارشد، دانشگاه امام صادق، ۱۳۸۶.

۴. خرم آبادی، عبدالصمد، جرایم فناوری اطلاعات، رساله دکتری، دانشاگه تهران، ۱۳۸۴.

۵. شریفی، مرسده، جرایم کامپیوتری در حقوق جزای بین‌المللی، کارشناسی ارشد، دانشگاه آزاده اسلامی واحد تهران مرکزی، ۱۳۸۳.

۶. هل فروش، فاطمه، جرایم کامپیوتری، کارشناسی ارشد، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، ۱۳۸۲.

چ) منابع انگلیسی

۱. *Access to public information, data protection and computer crime , ۱۹۹۰.*

۲. *Data protection acts and related acts " dept of justice " , USA.۲۰۰۱.*

۳. *Internet misuse and elementary internet investigations technology crime Interpol, ۲۰۰۱.*

٤. *Report on computer related crime in Latvia PC-CY cd cp ce.۱۹۹۷.*

۵. *Rick, Kaspersen, computer related crime, ۱۹۹۳.*

٦. *Sieber, ulrisb legal aspect of computer related crime in the information society, ۱۹۹۷.*

۷. *Van Duny J, A, the human factor in computer crime, ۱۹۹۹.*

۸. *Wasik, Matin, crime and computer,oxford, ۱۹۹۱.*