نقش بانکداری الکترونیکی در پولشویی و روش‌های مقابله با آن

محمدجعفر حبیب‌زاده[1*]، سیده سپیده میرمجیدی هِشَجین[2]

۱. استاد گروه حقوق دانشگاه تربیت مدرس، تهران، ایران
۲. دانشجوی کارشناسی ارشد رشته حقوق کیفری و جرم شناسی دانشگاه تربیت مدرس، تهران، ایران

دریافت: ۸۹/۸/۱۲ پذیرش: ۸۹/۱۲/۲٤

چکیده

امروزه تحول شگرفی که در نظام پولی و بانکی جهانی به واسطه انقلاب فناوری اطلاعات و ارتباطات به وجود آمده، آثار عمیقی بر زندگی اجتماعی و اقتصادی افراد گذاشته وهمزمان حوزه مقررات ضد پولشویی کنونی را با چالش جدید مواجه کرده است. دسترسی به بانکداری الکترونیکی و شبکه‌های اینترنتی، حاشیه امن مناسبی را در اختیار پولشویان قرار داده است. این مقاله درصدد پاسخگویی به این پرسش است که بانکداری الکترونیکی چه تأثیری بر فرایند پولشویی دارد. با این فرضیه که بانکداری الکترونیکی موجب تسهیل ارتکاب جرم پولشویی گردیده، روش‌های جدیدی را جهت ارتکاب این جرم پدید آورده است، با بررسی تجارت و بانکداری الکترونیکی و ویژگی‌ها این دو، شیوه‌های پولشویی الکترونیکی، فنون رایج و مدرن برای ارتکاب پولشویی الکترونیکی مطرح و فرایند پولشویی سنتی با پولشویی مدرن مورد مقایسه واقع شده است. در همین راستا توصیه‌های گروه کار اقدام مالی برای مبارزه با پولشویی الکترونیکی مطرح می‌شود. نتیجه آن‌که فناوری اطلاعات و ارتباطات اگر در بستری ناامن ارائه شود، می‌تواند با گسترش و تحول پولشویی، شیوه‌های ارتکاب آن را توسعه دهد و تسهیل کند. بنابراین، ضرورت دارد که در تدوین سیاست اقتصادی، مالی و جنایی این موضوع مد نظر قرار گیرد.

کلید واژه‌ها: بانکداری الکترونیکی، تجارت الکترونیکی، پولشویی، پولشویی الکترونیکی، فناوری اطلاعات و ارتباطات

---

* نویسنده مسؤول مقاله: Email: habibzam@modares.ac.ir

۱. مقدمه

فناوری اطلاعات و ارتباطات[1] نمونه بارزی از تغییر و تحولات بسیار سریع و شگفت‌آور هزاره دوم میلادی است که آثار گسترده‌ای در تمامی عرصه‌های اجتماعی و اقتصادی داشته و جهان را به‌سرعت به یک جامعه اطلاعاتی تبدیل کرده است. گسترش روز افزون ابزارهای ارتباطی و اطلاعاتی تأثیرهای مثبت و منفی بی‌شماری به دنبال داشته است. یکی از تأثیرهای مثبت این فناوری، فراهم کردن بستری مناسب جهت برقراری مراودات تجاری و اقتصادی است. این پدیده نوظهور که در بستر فناوری اطلاعات و ارتباطات شکل گرفته، «تجارت الکترونیکی»[2] نام دارد که اگر در بستری مناسب و امن ارائه شود، می‌تواند مؤثرتر از تجارت سنتی باشد. تجارت الکترونیکی انجام هرگونه امر تجاری و بازرگانی از طریق شبکه جهانی اینترنت ویا انجام معامله از طریق شبکه یا خرید و فروش خدمات از طریق فروشگاه‌های ایترنتی وب است [۱، ص ۳۸٤].

در این میان، «صنعت بانکداری»[3] با بهره‌گیری از فناوری اطلاعات و ارتباطات دچار تغییر و تحول بسیار از جمله سرعت، دقت، آسانی استفاده و امنیت در مبادلات مالی و تجاری گردیده که موجب در دسترس بودن ابزارهای متنوع الکترونیکیِ خدمت‌رسان برای مشتریان بانک‌ها شده است. از آن جمله می‌توان به پرداخت‌های الکترونیکی و اینترنتی، بانکداری از طریق تلفن‌های ثابت و سیار، پایانه‌های فروش[4]، ماشین‌های خودپرداز[5] و... اشاره کرد. اما فناوری اطلاعات و ارتباطات با همه قابلیت‌ها و پیچیدگی‌هایش به‌شدت در برابر تهدیدها آسیب‌پذیر است؛ از آن جهت که فناوری اطلاعات، علاوه بر تسهیل ارتکاب جرائم سنتی، فرصت‌های تازه و بسیار پیشرفته‌ای را در «فضای مجازی» در اختیار مجرمان قرار داده و باعث به وجود آمدن گونه جدیدی از جرائم با عنوان «جرائم سایبر»[6] شده است. دسترسی به فضای اینترنتی و شبکه‌ها با ایجاد فضای مطمئن برای مجرمان، ارتکاب پاره‌ای از جرائم را در محیط مجازی تسهیل می‌کند که از جمله می‌توان به جرم پولشویی اشاره کرد.

---

1. information and communication technologies
2. electronic commerce
3. electronic banking
4. Pos=poin of sale
5. ATM= automatic teller machin

٦. نوع جدیدی از جرائم رایانه‌ای که در محیط سایبر به وجود می‌آید.

تطهیر پول یا پولشویی عبارت است از مخفی کردن منبع و منشأ اصلی اموال و درآمدهای ناشی از جرم و پاک نمایاندن آن‌ها، به گونه‌ای که یافتن منبع اصلی مال غیرممکن یا بسیار دشوار می‌شود. به عبارت دیگر، پولشویی فرایندی است که مجرم سعی می‌کند منشأ واقعی پول‌های حاصل از فعالیت‌های مجرمانه را مخفی نگه دارد. اگر مجرم موفق شود، پول ماهیت غیر قانونی خود را از دست می‌دهد و به شکل قانونی ظاهر می‌شود.[1]

اولین مرحله از فرایند پولشویی، «مکان یابی»[2] یا «جایگزینی» نام دارد و آن عبارت است از عرضه منابع غیر قانونی به شبکه مالی با هدف وارد کردن آن‌ها به زنجیره گردش مالی. این عمل با سپرده گذاری نقدی در مؤسسات مالی رسمی، غیر رسمی و خرید کالاهای قیمتی انجام می‌شود. مرحله دوم با عنوان «طبقه‌بندی»[3] یا «لایه لایه کردن»، ناظر است بر تبدیل درآمدهای حاصل از جرم به شکل‌های دیگر به منظور مبهم ساختن یا اختفای منبع و مالکیت وجوه و منابع. این مرحله با انجام عملیاتی مانند حواله وجه، خرید مستغلات و انتقال منابع به خارج از کشور صورت می‌گیرد. آخرین مرحله در فرایند پولشویی، «یکپارچه‌سازی»[4] یا «ادغام کردن» است و آن عبارت است از وارد کردن پول شسته شده توسط استفاده‌کننده نهایی به سیستم مالی کشور تا از تجسسات و تحقیقات سازمان‌های رسمی در جهت یافتن علت موجودی پول در امان ماند[۲، ص ۱۲۰].

درباره زمان شروع پدیده پولشویی، عده‌ای معتقدند که این واژه از دهه بیست و سی در آمریکا رواج یافته و اشاره به شستشوخانه‌هایی دارد که مافیا آن‌ها را از پول نامشروع حاصل از قمار، قاچاق، فحشا و نظایر آن‌ها می‌خرید و از این طریق پول کثیف را به داخل آن‌ها تزریق می‌کردند. برخی معتقدند کاربرد این اصطلاح به رسوایی واترگیت در اواسط دهه هفتاد، در زمان ریاست جمهوری نیکسون، مربوط است. از لحاظ حقوقی هم آغاز استفاده از آن را به دعوای آمریکایی[5] در سال ۱۹۸۲ مرتبط کرده‌اند [۳، ص ۷۳].

به هر حال به دلیل اهمیت زیاد جرم پولشویی، جامعه بین‌المللی توجه خاصی به این دسته از جرائم داشته و دولت‌ها را موظف کرده است تا متعهد به مبارزه با پولشویی شوند. این

1. finacial supervision commission, money laundering the financing of terrorism (FSC).see: www.govim
2. placement
3. layering
4. integration
5. iu.s v.$ 4255.625, 39 (1982) 551 F5u, pp.314.

تعهدات شامل احراز هویت مشتری، ثبت اسناد، شناسایی تراکنش‌های مشکوک و غیره است. ولی این گونه سازوکارها براساس مفروضات خاصی از قبیل استفاده از بانک‌ها جهت انجام دادن تراکنش‌های خاص، توانایی مؤسسات مالی برای نظارت بر فعالیت‌های مشتریان و استفاده از پول فیزیکی توسعه داده شده‌اند. عدم کارایی روش‌های سنتی پولشویی و ریسک بالای آن‌ها موجب شده تا پولشویان با توجه به امکانات موجود در بستر بانکداری الکترونیکی، به نوع جدیدی از پولشویی تحت عنوان «پولشویی الکترونیکی» روی آوردند. پولشویی الکترونیکی عبارت است از «فرایند قانونی کردن درآمدهای نامشروع و حاصل از فعالیت‌های مجرمانه با استفاده از خدمات موجود در فضای مجازی تا با استفاده از این امکانات به درآمدهای خود شکل قانونی دهند و از آن به‌عنوان یک ابزار انتقال وجوه غیر قانونی استفاده کنند».[1]

تجارت و بانکداری الکترونیکی تنها در شرایطی که به نحو غیر ایمن ارائه شود، می‌تواند به بستر مناسبی برای سوءاستفاده پولشویان تبدیل شود. بنابراین، منظور ما درمقاله حاضر در این که تجارت و بانکداری الکترونیکی بستر مساعدی برای پولشویی ایجاد می‌کند، تنها محدود به تجارت و بانکداری غیر ایمن است.

۲. تجارت الکترونیکی

کمیسیون اروپا در سال ۱۹۹۷ تجارت الکترونیکی را پردازش و انتقال الکترونیکی داده‌ها، شامل متن، صدا و تصویر متنی دانسته که خود فعالیت‌های گوناگون از قبیل مبادله الکترونیکی کالاها و خدمات، تحویل فوری مطالب دیجیتال، انتقال الکترونیکی وجوه، مبادله الکترونیکی سهام، بارنامه الکترونیکی، طرح‌های تجاری، طراحی و مهندسی مشترک، منبع‌یابی، خریدهای دولتی، بازاریابی مستقیم و خدمات بعد از فروش را در بر می‌گیرد. بنابراین در تجارت الکترونیکی، بدون حضور افراد معاملات انجام می‌گیرد، امکان قبض و اقباض ثمن و برخی از مبیع در آن وجود دارد،از طریق فناوری اطلاعات و ارتباطات امکان تحقق دارد و حجم و وسعت آن به صورت روزافزونی گسترش می‌یابد. این امکان جدید در

1. Filipkowski, Wojciech, « Money Laundering via Internet: The Used Methods», See at: http://www .slideshare .net/wofi/cyberlaundering

معاملات، زمینه مناسبی برای پولشویی الکترونیکی فراهم می‌سازد.

ویژگی‌های تجارت الکترونیکی عبارتند از: عدم نیاز به حضور فیزیکی افراد برای انجام تجارت و کسب و کار، استفاده از امکانات فناوری اطلاعات و ارتباطات جهت ایجاب و قبول و انعقاد قرارداد، امکان پرداخت و دریافت ثمن معامله به شیوه الکترونیکی، امکان قبض و اقباض الکترونیکی کالا یا خدمات، تغییر ساختار بازار، بهبود کیفیت کالاها و خدمات و کاهش قیمت‌ها. لازم به ذکر است که اقدامات پیشگیرانه‌ای که توسط کاربران، سازمان‌ها و شرکت‌ها و دولت انجام می‌پذیرد، مانند نصب ضد ویروس‌ها، آموزش مناسب، آشنایی با مخاطرات دنیای مجازی، اجرای استانداردهای امنیتی، ایجاد زیر ساخت کلید عمومی، ایجاد فرهنگ امنیت فناوری اطلاعات و ارتباطات و ... می‌تواند به ایجاد اطمینان در تجارت الکترونیکی بینجامد [٤، ص ۲۰ - ۲۳].

۳. بانکداری الکترونیکی

«به طور کلی بانکداری الکترونیکی عبارت است از فراهم آوردن امکاناتی برای کارکنان در جهت افزایش سرعت و کارایی آن‌ها در ارائه خدمات بانکی در محل شعبه و همچنین فرایندهای بین شعبه‌ای و بین بانکی در سراسر دنیا و ارائه امکانات سخت‌افزاری و نرم‌افزاری به مشتریان که با استفاده از آن‌ها بتوانند بدون نیاز به حضور فیزیکی در بانک، در هر ساعت از شبانه روز از طریق کانال‌های ارتباطی ایمن و با اطمینان، عملیات بانکی دلخواه خود را انجام دهند» [۱، ص۲۲].

بانکداری الکترونیکی با در اختیار گذاردن فناوری‌های نرم‌افزاری و سخت‌افزاری مبتنی بر شبکه و مخابرات، این امکان را برای مشتریان فراهم می‌آورد که بدون نیاز به حضور فیزیکی در بانک، و با رعایت سرعت، دقت، آسانی استفاده و امنیت، فعالیت‌های مورد نیازشان را انجام دهند [۱، ص ٢٤].

۳-۱. ویژگی‌های پول و بانکداری الکترونیکی

ویژگی‌های بانکداری الکترونیکی عبارت است از: غیر شخصی بودن تعامل بین مشتری و مؤسسه، عدم نیاز به حضور فیزیکی فرد برای انجام امور بانکی، سهولت انجام تراکنش‌های

الکترونیکی و خدمات بین‌الملل و نظارت مستقیم مشتری بر نقل و انتقال وجوهِ خود، بدون دخالت مؤسسات اعتباری یا حتی بانک‌های مربوط [٥، ص ٢٦].

ویژگی‌های مذکور با افزایش کارایی بانکداری و کاهش هزینه خدمات مالی و توسعه حوزه فعالیت، مکان امنی برای افراد پولشو فراهم می‌کند.

ویژگی‌های پول الکترونیکی عبارت است از: سرعت حمل و انتقال پول الکترونیکی، ضریب اطمینان بالاتر پول الکترونیکی و بی‌نام تر بودن پول الکترونیکی نسبت به پول سنتی. می‌توان گفت گمنامی[1] پول الکترونیکی مهم‌ترین ویژگی آن نسبت به پول فیزیکی است و همین خصیصه همیشه نظر پولشویان را به خود جلب کرده است.

بانکداری الکترونیکی بر حسب امکانات و نیازهای بازار می‌تواند در زیرشاخه‌ها و انواع مختلفی ارائه شود که عبارتند از: بانکداری اینترنتی،[2] بانکداری مبتنی بر تلفن همراه[3] و فناوری‌های مرتبط با آن، بانکداری تلفنی، بانکداری مبتنی بر نمابر، بانکداری مبتنی بر دستگاه‌های خودپرداز، بانکداری مبتنی بر پایانه‌های فروش و بانکداری مبتنی بر شعب الکترونیکی.

بانکداری اینترنتی شیوه‌ای است که فرد می‌تواند توسط یک رایانه شخصی با اتصال به وب‌سایت بانک، عملیات بانکی مورد نظرش را انجام دهد و از خدماتی مثل دسترسی به اطلاعات حساب، مرور صورتحساب‌ها، جابه‌جایی وجوه، درخواست اعتبار یا داد و ستدهای امن استفاده کند. بانکداری از طریق تلفن همراه نیز سرویسی است که مشتریان را قادر می‌سازد اطلاعاتی مانند مانده حساب بانکی خود، درخواست صورتحساب، درخواست دسته‌چک، دستور انتقال پول از یک حساب مشتری به حساب‌های دیگر او یا سایر اشخاص را در اختیار داشته باشند. بانکداری تلفنی انجام یک معامله تجاری خرد بین بانک و مشتری از طریق تلفن است که در آن به طور معمول از سه روش واکنش صوتی، تشخیص صدا ویا تلفن‌های برنامه‌ریزی استفاده می‌شود. ماشین خودپرداز نیز به عنوان یک شعبه از یک بانک عمل می‌کند و بسیاری از وظایف اصلی بانکداری را انجام می‌دهد [١، ص٣٥٦].

دستگاه پایانه فروش نیز به وسیله ارتباط تلفنی یا شبکه‌ای به سیستم بانکی، امکان انتقال

1. anonymity
2. internet banking
3. M-Banking = mobile banking

خودکار مبلغ خریداری شده از حساب مشتری (دارنده کارت) به حساب فروشنده (پذیرنده) کارت را فراهم می‌سازد. به‌عنوان آخرین زیر شاخه از بانکداری الکترونیکی می‌توان به شعبه‌های الکترونیکی ٢٤ ساعته اشاره کرد. شعبه الکترونیکی ممکن است در بخشی از شعبه ویا مستقلاً راه‌اندازی شود و کاربر می‌تواند با داشتن یک کارت بانکی وارد پایگاه بشود و عملیات دریافت، پرداخت و انتقال وجه و سایر خدمات بانکی را انجام دهد.

همچنین از دیگر تأثیرات چشمگیر فناوری اطلاعات و ارتباطات بر حوزه بانکداری، می‌توان به تحول شگرفی که در نظام‌های پرداخت بانکی روی داده، اشاره کرد. هدف از ایجاد سامانه‌های پرداخت الکترونیکی بر روی اینترنت، قبض و اقباض الکترونیکی ثمن معاملات مربوط به خرید و فروش کالاها و خدمات است. از عمده‌ترین ابزارهای پرداخت الکترونیکی عبارتند از: انواع کارت‌های بانکی،[1] چک الکترونیکی،[2] پول الکترونیکی،[3] حواله الکترونیکی، کارت ویا کوپن مخصوص فروشنده (ابزارهای تخصیص اعتبار به اشخاص).

پول الکترونیکی مهم‌ترین ابزاری است که بسیار مورد استفاده پولشویان است. در سال ١٩٩٦ بانک تصفیه بین‌المللی[4]، پول الکترونیکی را به عنوان «ارزش ذخیره شده» یا محصولات «پیش پرداخت شده» تعریف کرد که در آن، ثبت وجوه یا ارزش موجود برای مصرف‌کننده براساس ابزارهای الکترونیکی در دارایی مصرف‌کننده ذخیره می‌شود. در واقع، پول الکترونیکی سازوکاری است که اجازه پرداخت ارزش ذخیره شده یا پیش پرداخت شده را می‌دهد و در یک حامل داده ذخیره می‌شود و در تصرف مشتری است.

پول الکترونیکی گاه به صورت «ناپیوسته»[5] وگاه به صورت «پیوسته»[6] ارائه می‌شود. پول‌های «ناپیوسته» می‌توانند در قالب کارت‌های مختلف، مانند کارت‌های اعتباری، کارت‌های بدهی یا حتی کارت‌های تلفن باشند. علت این‌که این نوع از پول الکترونیکی را کارت‌های ناپیوسته می‌نامند این است که نقل و انتقال وجوه به وسیله آن فقط از طریق دستگاه‌های خودپرداز انجام می‌گیرد. جهت استفاده از پول الکترونیکی کامپیوتری ابتدا باید نزد مؤسسه اعتباری یا بانکی که این فناوری را دارد، وجه یا اعتباری سپرده شود. در مرحله بعد یک

1. charg cards/ debit cards/ credit cards
2. electronic cheque
3. electronic cash (e-cash)
4. bank for inter national settlements (BIS)
5. offline
6. 0nline

شماره اعتباری را در اختیار مشتری قرار می‌دهند. بعد مشتری می‌تواند به صورت اینترنتی کالاهای مورد نیاز را خریداری کند و فقط لازم است شماره اعتباری را به سایتی که از آن خرید انجام داده، بدهد. این سایت هم با اتصال به سایت بانک یا مؤسسه مالی که مشتری در آن حساب دارد، وجه مربوط را به حساب خودش منتقل می‌کند. باید توجه کرد که مشتری همان کاربر اینترنت است و کارمندان بانک هم تعدادی برنامه رایانه‌ای هستند که با این هدف طرح‌ریزی شده‌اند.[1]

بنا بر آنچه تاکنون عنوان گردید می‌توان گفت زمانی که ابزارهای پرداخت فوق و ویژگی‌های تجارت و بانکداری الکترونیکی و خصوصیات فناوری اطلاعات و ارتباطات با تمایل مجرمانه پولشویان سنتی همگرا می‌شود، پولشویی الکترونیکی نمود پیدا می‌کند. با این حال لازم است مشخصاً تأثیر انقلاب فناوری اطلاعات بر جرم پولشویی مورد بررسی واقع شود.

۴. روش‌های پولشویی الکترونیکی

پولشویی از طریق بانکداری الکترونیکی به دو روش مستقیم و غیر مستقیم انجام می‌شود. در روش مستقیم پولشو (عامل پولشویی) از طریق رابطه متقابل مستقیمی که با مؤسسه مالی دارد با ارائه هویت به روشی که نیت و قصد واقعی‌اش پنهان بماند، به‌راحتی عملیات پولشویی را انجام می‌دهد. ممکن است این شبهه ایجاد گردد که اگر پولشویی از طریق فضای مجازی و در بستر بانکداری الکترونیکی در حال انجام است، چرا روش به کار رفته را روش مستقیم می‌نامیم؟

در پاسخ باید گفت منظور از روش مستقیم این است که فرد پولشو با استفاده از فناوری «امضای دیجیتال»[2] و از طریق اینترنت به صورت مستقیم با مؤسسه مالی مربوط ارتباط پیدا می‌کند و بدون حضور فیزیکی در بانک یا مؤسسه مالی حساب باز کرده، با ارائه هویت‌های ساختگی و حتی جعل امضای دیجیتال، بدون این‌که توجه کسی را به خود جلب کند، مراحل پولشویی را انجام می‌دهد. پولشو در روش مستقیم می‌تواند از طریق پنهانکاری در ساختارهای تجاری، استفاده نادرست از تجارت‌های قانونی، به کار بردن اسناد و هویت‌های ساختگی، سوءاستفاده از مسائل مربوط به صلاحیت قانونی بین‌المللی و استفاده از امتیاز

---

1. Financial crimes Enforcement Network (Fin CEN) , US Department of Treasury, A Survey of Electronic Cash , Electronic Banking and Gaming, 2000.
2. digital compression

گمنامی و ناشناختگی در فضای مجازی به اهداف خود برسد، بدون این‌که تراکنش‌های انجام شده به عنوان تراکنش‌های مشکوک گزارش شود.

روش دیگر مورد استفاده در پولشویی الکترونیکی، روش غیر مستقیم است. در این روش از رابطه مستقیم با مؤسسه مالی اجتناب می‌شود. هدف از چنین رابطه‌ای آن است که این معامله به عنوان یک معامله مشکوک گزارش نشود. پولشویی الکترونیکی اغلب با استفاده از روش غیر مستقیم صورت می‌گیرد؛ زیرا در این روش، کار سریع‌تر پیش می‌رود؛ بدون این‌که توجه مقامات را به این نکته جلب کند که پول از منشأ غیر قانونی و غیر مشروع به دست آمده است. حوزه‌های تجاری که عمدتاً تحت تأثیر پولشویی الکترونیکی یا در معرض تهدید آن قرار دارند عبارتند از: بانک‌های تجاری، مؤسسات اعتباری، اداره‌های پست، تجارت‌های بین‌المللی، کارگزاران سهام، شرکت‌های سرمایه‌گذاری و شرکت‌های بیمه و بانکداری الکترونیکی [٦، ص ١٢].

از این حوزه‌ها می‌توان به عنوان «بزه‌دیدگان بالقوه» پولشویی الکترونیکی نام برد. در هریک از حوزه‌ها، پولشو به روشی به مقاصد خود می‌رسد. از میان موارد ذکر شده اختصاصاً به بیان فرصت‌های مناسبی که بانکداری الکترونیکیِ غیر ایمن در مفهوم عام آن در اختیار پولشو می‌گذارد و با بحث ما نیز مرتبط است، می‌پردازیم.

۴-۱. بانکداری پیوسته[1]

پولشویی الکترونیکی به سه روش بانکداری «پیوسته» را مورد تهدید قرار می‌دهد:

۱- افتتاح حساب با استفاده از اینترنت، بدون ارائه هویت مشتری.

مقررات بین المللی و داخلی، بانک‌ها را موظف می‌کند هرگونه تراکنش مشکوک را گزارش دهند. از طرفی پولشویان هم به‌سادگی می‌توانند از چنین محدودیتی بگریزند. این فرصت برای پولشویان از طریق امکاناتی که بانکداری پیوسته در اختیارشان می‌گذارد، فراهم می‌شود. مثلاً پولشو از طریق باز کردن حساب‌های «پیوسته» نزد تعدادی از شرکت‌ها که حساب بانکی اینترنتی دارند و فاقد مقررات و نظارت کافی هستند، از سیستم‌های پرداخت

۱. زمانی که یک دارنده حساب، موجودی خود را از طریق دستگاه‌های خودپرداز، اینترنت یا موبایل و سایر خدمات پرداخت الکترونیکی منتقل می‌کند می‌توان از یک «بانک پیوسته» سخن گفت. در حقیقت «بانک پیوسته» از زیرمجموعه‌های بانکداری الکترونیکی است.

الکترونیکی استفاده می‌کند. مهم‌ترین امتیازی که بانکداری اینترنتی برای پولشویان دارد، احراز هویت مشتری است؛ چون در بانکداری اینترنتی مشکل بتوان هویت مشتری را احراز و اطلاعات را ثبت و نگهداری کرد و تراکنش‌های مشکوک را گزارش داد.

در اولین گام تعامل بین مشتری جدید و مؤسسه مالی، همیشه یک ریسک بالقوه وجود دارد. سازوکارهای جاری ضد پولشویی در اغلب کشورها حداقل در آغاز روابط تجاری بر احراز هویت مشتری تأکید دارند. درباره بانکداری اینترنتی در صورتی که رویه‌های گشایش حساب و سایر تعاملات بانک بدون حضور فیزیکی مشتری و ارتباط چهره به چهره با او یا بدون ارتباط با حساب‌های سنتی موجود صورت پذیرد، مشکلات مؤسسات مالی افزایش می‌یابد. حتی اگر مؤسسات مالی تعهدات مربوط به احراز هویت را در زمان گشایش حساب مراعات کرده باشند، به لحاظ عدم تعامل چهره به چهره در تراکنش‌های جاری اینترنتی، استفاده کننده از حساب ممکن است غیر از فردی باشد که حساب را باز کرده است. در واقع با حذف تعامل شخصی بین مشتری و مؤسسه، بسیار مشکل می‌توان فهمید که چه کسی به طور واقعی حساب را کنترل می‌کند و چه چیزی صحت عملکرد تجاری را تأیید می‌کند.
مؤسسات مالی به صورت عادی تنها قادر به تعیین این نکته هستند که یک حساب خاص صرفاً در یک زمان خاص قابل دسترسی است. بانک تنها قادر است معین کند که دسترسی به وسیله نگهدارنده حساب صوری صورت می‌گیرد و هیچ روشی برای تعیین محلی که مشتری تراکنش را انجام می‌دهد، وجود ندارد؛ به این معنا که شخص در نهایت قادر است تعدادی از حساب‌ها را هم زمان کنترل کند، بدون این‌که توجه مؤسسات مالی یا مؤسسه‌ای را که در آن حساب دارد، جلب کند. بنابراین، مؤسسات مالی راهی جهت مظنون شدن به تبادلات عادی ندارند و به طور کلی معیارهای خاصی برای ارائه گزارش نسبت به این گونه تراکنش‌های مشکوک در نظر نمی گیرند.

این ویژگی بانکداری اینترنتی و نیز گسترش استفاده از کارت‌های پیش پرداخت[1] مثل کارت‌های اعتباری، پولشویان را قادر ساخته تا پول الکترونیکی را به‌سادگی از یک کارت به کارت دیگر منتقل کنند. گاهی پولشویان از هکرها هویت‌های ساختگی را به قیمت نازلی می‌خرند تا بتوانند با استفاده از این هویت‌ها، حساب‌هایی را در وب‌سایت بانک مربوط باز

1. prepaid card

کنند یا اینکه خود اقدام به راه‌اندازی یک وب‌سایت کرده، با استفاده از آن به جزئیات اطلاعات کاربرانشان دسترسی پیدا کنند. سپس اطلاعات کارت‌های پیش پرداخت شده یا کارت هوشمند را به بهانه خدماتی که ظاهراً قرار است به آن‌ها ارائه شود، مطالبه می‌کنند تا پول‌های کثیف را در این حساب‌ها سپرده گذاری کنند. در واقع پولشویان در این روش با فریفتن کاربرانشان و با به دست آوردن اطلاعات کارت‌های هوشمند آنان، به‌سادگی پول‌های کثیف را به این حساب‌ها منتقل می‌کنند و عملیات پولشویی را انجام می‌دهند.

۲- استفاده از فناوری رمزنگاری[1] و امضای دیجیتال.

«از مهم ترین فناوری‌هایی که در پول و بانکداری الکترونیکی برای اجرای صحیح امور و بالا بردن ضریب اطمینان کارکردها به کار می‌رود، فناوری رمزنگاری و امضای دیجیتال است. به طور خلاصه، کارکرد فناوری رمزنگاری این است که محتوا را به شکلی نامفهوم و غیر قابل درک تبدیل می‌کند و برای اینکه به حالت اولیه برگردد، لازم است فرایند رمزگشایی[2] اجرا شود که بدیهی است فقط سازنده و واگذارنده این فناوری و ارسال‌کننده و دریافت‌کننده محتوا توانایی انجام آن را دارند.

با توجه به این توضیحات مشخص می‌شود که اگر پول الکترونیکی رمزنگاری شود، دیگر محتوای آن نامفهوم خواهد شد و تنها دریافت‌کننده آن که مشخص نیست در کدام نقطه از جهان قرار داد، می‌تواند با اجرای کامل برنامه رمزگشایی مربوط از آن آگاهی یابد. به این ترتیب چنان سطحی از محرمانه ماندن[3] و ناشناس ماندن برای این مبادلات فراهم می‌شود که هرکس می‌تواند از هر جای دنیا مبلغ مورد نظر خود را به نقطه دیگر ارسال کند، بی‌آن‌که کسی از محتوای آن آگاهی یابد» [۵، ص ۱۱۸].

۳- استفاده از عاملین پولشویی

گاهی اوقات پولشویان جهت انجام فرایند پولشویی از افرادی که همان «عاملین پولشویی»[4] هستند، استفاده می‌کنند؛ اشخاص حقیقی یا حقوقی که در ظاهر وجهه قانونی دارند و به پولشویان در پولشویی کمک می‌دهند. در حقیقت این عاملین، به نوعی فعالیت‌های مجرمانه را پوشش می‌دهند. لازم به ذکر است که پولشو نه فقط در این روش، بلکه در استفاده از سایر

1. decryption
2. encryption
3. confidentiality
4. army of smurf

روش‌های موجود نیز از کمک این دسته از افراد منتفع می‌گردد تا با کمک آنان فرایند پولشوی را اجرا کند.

۴-۲. قمار اینترنتی[1]

در میان فعالیت‌های انجام شده برای شستن پول از سوی مؤسسات غیر مالی، موارد به کارگیری قمارخانه برای انجام دادن جرائم پولشویی به‌وفور یافت می‌شود.

امروزه قمارخانه‌های سنتی برای جلوگیری از جرائم پولشویی قانونمند شده‌اند و بسیاری از کشورها نیز وادار شده‌اند تا همین شیوه (قانونمند ساختن قمارخانه‌ها) را در پیش گیرند. با نظامند شدن قمارخانه‌های سنتی، قمارخانه‌های اینترنتی محل خوبی برای پولشوها شده است. در حال حاضر صدها وب‌سایت قمارخانه در منطقه کارائیب تأسیس شده که بهشت مالیاتی تلقی می‌شود. بسیاری از این وب‌سایت‌ها توسط دولت قانونمند نشده‌اند و برخی از آن‌ها هویت مشتری را نیز درخواست نمی‌کنند. تمام این ظرفیت‌های بالقوه، فرصت‌های پولشویی را برای مجرمان فراهم می‌کنند.

فرایند قمار یا شرط‌بندی اینترنتی این چنین است که مجرمان ابتدا یک حساب بر روی وب‌سایت اینترنت باز می‌کنند، سپس پول کثیف را به همان میزانی که ژتون می‌گیرند به حساب اینترنتی وب‌سایت (قمارخانه مربوط) ارسال می‌دارند و آنگاه روی پول‌های پرداخت شده، شرط‌بندی می‌کنند.[2]

این روش با استفاده از کارت‌های اعتباری، چک، انتقالات سیمی[3] (نقل و انتقال پول در شبکه) و به‌ویژه پول الکترونیکی- که گمنام‌تر از سایر ابزارها است- به‌سهولت قابل انجام بوده، مبارزه با این قبیل شیوه‌های پولشویی را بسیار دشوار ساخته است.

---

1. internet gambling

۲. ممکن است دو طرف بازی، با هم همدست باشند. به‌عنوان مثال یک طرف ۱۰۰/۰۰۰ دلار ژتون بگیرد، طرف دیگر هم ۱۰۰۰ دلار. سپس روی همین پول‌ها بازی کنند تا این‌که یک طرف صد هزار دلار را ببرد و (البته با همدستی هم) و در مجموع به صد و یک هزار دلار برسد. حال اگر از او بپرسند که این پول‌ها را از کجا آورده‌ای به‌راحتی می‌تواند بگوید که در قمار برده‌ام! و سرانجام بازپرداخت پول خود را توسط چک‌های کشیده شده از حساب‌های اینترنتی کازینو دریافت می‌کنند. گاهی مجرمان ممکن است ژتون‌های برندگان را به نام شخص ثالثی دریافت کنند و به این ترتیب به فعالیت‌های مجرمانه خود پوشش دهند و مقدار زیادی پول کثیف را به‌راحتی بشویند!

3. wire Transfers

۴-۳. کارت‌های از پیش پرداخت شده[1]

این کارت‌ها به‌عنوان یکی از ابزارهای پرداخت الکترونیکی، می‌توانند به شکل کارت‌های اعتباری باشند که جهت خرید خدمات اینترنتی به کار می‌روند.[2] تصور کنید فردی توانسته از طریق ارتکاب جرم، مقادیری پول تحصیل کند و سپس اقدام به خرید مقدار زیادی کارت تلفن یا کارت اینترنت می‌کند. آنگاه کارت‌های خریداری شده را به قیمت خرید یا قیمتی پایین‌تر از خرید در بازار می‌فروشد و درآمد حاصل را به حساب خود می‌ریزد و بدین ترتیب پول‌های کثیف شسته می‌شود؛ یا فردی که پول کثیف را در دست دارد، حجمی از خدمات اینترنت را از یک ارائه‌کننده خدمات می‌خرد و سپس با چاپ کارت‌های اینترنتی، آن‌ها را به مغازه‌دارها ویا دکه‌های روزنامه‌فروشی با قیمت پایین‌تر می‌فروشد و پول آن را به حساب خود واریز می‌کند. در این صورت اگر کسی او را درباره منشأ پول‌ها مورد سؤال قرار دهد، خواهد گفت پول‌ها را از طریق خرید و فروش به دست آورده، در حالی که چنین نبوده و او از این طریق، فرایند پولشویی را تسهیل کرده و امکان شناسایی و دستگیری خود را دشوار ساخته است.

۴-۴. حراج‌های پیوسته[3]

شرکت‌هایی که حراج الکترونیکی دارند و وب‌سایت‌هایی را با کارکرد حراج الکترونیکی راه‌اندازی می‌کنند، دارای حساب بانکی هستند. فروشنده کالای خود را از طریق این وب‌سایت معرفی می‌کند و خریدار پس از پسند کالا، پول آن را به حساب شرکت می‌ریزد. سپس فروشنده کالا را برای خریدار ارسال می‌کند و در صورتی که خریدار تأیید کند کالای دریافتی همان است که سفارش داده، شرکت پول را به حساب فروشنده واریز خواهد کرد [۷، ص ۲۸]. حال ممکن است عاملان پولشویی از این امکان جهت پولشویی استفاده کنند؛ بدین ترتیب که مشخصات یک کالای گرانقیمت را ظاهراً جهت فروش بر روی وب‌سایت نمایش می‌دهند و فرد دیگری به عنوان خریدار صوری اقدام به خرید آن کرده، وصول کالا را به شرکت اعلام می‌کند. بدین ترتیب، پول کثیف توسط یکی از عاملان پولشویی به عامل دیگر منتقل می‌شود.

---

1. prepaid cards

۲. کارت‌های تلفن. کارت‌های شارژ تلفن همراه اول یا کارت‌های ایرانسل در کشورمان، از نمونه‌های بارز این قبیل کارت‌ها هستند.

3. On-Line Aouction

۴-۵. بانکداری از طریق موبایل

این شیوه پرداخت هم مثل بانکداری اینترنتی است. دستور پرداخت از طریق پیام صوتی یا پیام متنی صادر می‌شود. وقتی با موبایل سفارش پرداخت صادر می‌شود، شماره تلفن و شماره سریال گوشی پرداخت‌کننده در نزد کاربرها ثبت و ضبط می‌شود. حال پولشو می‌تواند از طریق پیام‌های متنی یا صوتی یک موبایل ثبت نشده اقدام به جابه‌جایی پول از حساب‌های مختلف کند. در واقع، اگر این فناوری با سرقت هویت و افتتاح حساب‌های بانکی ترکیب شود، محیط مناسبی را جهت اختفای هویت افراد و جابه‌جایی پول فراهم می‌آورد. بدین ترتیب، بانکداری از طریق موبایل به عنوان شیوه‌ای برای پولشویی مورد سوءاستفاده مجرمان قرار می‌گیرد.

۴-۶. خرید و فروش الکترونیکی فلزات گرانبها[1]

امکان تجارت و خرید و فروش الکترونیکی فلزات و شمش‌های گرانبها در جهان از طریق برخی وب‌سایت‌های اینترنتی فراهم گردیده است. خریدار یا فروشنده (کاربر) قبل از هر اقدامی باید اقدام به ثبت نام در سایت کند تا یک حساب الکترونیکی به وی اختصاص یابد. برای ثبت نام باید نام و نام خانوادگی و سایر مشخصات هویتی، آدرس پست الکترونیکی و آدرس واقعی در یک فرم الکترونیکی درج و به وب‌سایت ارسال گردد. معمولاً تهیه و استفاده از هویت جعلی و آدرس‌های تقلبی امکانپذیر است. برخی از وب‌سایت‌ها حتی برای تخصیص حساب الکترونیکی نیاز به اعلام هویت ندارند. این شرایط امکان جعل هویت یا اختفای هویت را فراهم می‌سازد. معمولاً یک کاربر پس از ثبت نام و تخصیص حساب الکترونیکی از جانب وب‌سایت می‌تواند اقدام به خرید و فروش فلزات گرانبهای خود به سایر اعضایی که مانند وی در سایت ثبت نام کردند، کند.

کاربر می‌تواند با نام‌های مختلف در این سایت ثبت نام کرده، به این ترتیب با استفاده از آن‌ها هم به عنوان خریدار و هم به عنوان فروشنده ایفای نقش کند. حتی برخی از ارائه‌دهندگان این قبیل خدمات، فرایند اختفای هویت را در طول فرایند جابه‌جایی پول از حساب خریدار به حساب فروشنده ادامه می‌دهند و هیچ زمان خریدار و فروشنده هویت

---

1. digital precious metals (DPM)

یکدیگر را نخواهند شناخت و شماره حساب‌های بانکی آنان نیز مخفی خواهد ماند. این عملیات از طریق حساب بانکی ارائه‌کننده خدمات به‌عنوان واسطه نیز امکانپذیر است. بنابراین، بازار بورس الکترونیکی فلزات گرانبها به صورت بالقوه به ابزاری جهت پولشویی تبدیل می‌شود.

۴-۷. بازی‌های رایانه‌ای پیوسته

شیوه نسبتاً جدید دیگری که برای پولشویی پدید آمده، پولشویی مجازی نام دارد. در این روش، مجرمان از بازی‌های رایانه‌ای «پیوسته» چندین مرحله‌ای مبتنی بر وب‌سایت‌های اینترنتی که با حضور بازیکنان متعدد صورت می‌گیرد،[۱] برای پولشویی استفاده می‌کنند. در برخی از این بازی‌ها، بازیکن می‌تواند با پرداخت پول سنتی اقدام به تهیه پول مجازی کند و به این ترتیب با پرداخت حق ورود وارد بازی شود و با برنده شدن در مراحل مختلف، پول بیش‌تری به‌عنوان پاداش یا جایزه تحصیل کند. بازیکن می‌تواند پول را به سایر بازیکنان منتقل سازد ویا با استفاده از پول مجازیِ به دست آمده کالاها یا خدماتی را بخرد یا بفروشد. در این شیوه می‌توان پول سنتی را به پول مجازی یا بالعکس تبدیل و به سایر حساب‌ها منتقل کرد. برخی مواقع به جای پول مجازی یک کارت بدهی به بازیکن داده می‌شود که به وسیله آن می‌تواند پول را از طریق دستگاه‌های عابر بانک برداشت کند.

با توجه به آنچه در این بخش تحت عنوان روش‌های مورد استفاده در پولشویی الکترونیکی گفته شد، می‌توان دریافت که استفاده از این روش‌ها از طرفی سرعت عملیات مزبور را چند برابر می‌کند و سازوکارهای نظارتی و بازدارنده را نیز با مشکل مواجه می‌سازد و از طرف دیگر هویت مجرم با به‌کارگیری این روش‌ها مخفی می‌ماند. اما بررسی دقیق این نکته که استفاده از روش‌های ذکر شده در هر سه مرحله جرم پولشویی در عمل چه تأثیری بر فرایند مزبور دارد، به گونه‌ای که موجب تقسیم‌بندی این جرم- به اعتبار روش استفاده - به پولشویی سنتی و پولشویی مدرن می‌شود، موضوع قسمت بعدی است.

۵. مقایسه پولشویی سنتی با پولشویی مدرن

در مرحله اول پولشویی به روش سنتی که مرحله جایگزینی نام دارد، اولین قدم، انتقال

---

۱. مانند second life یا entropia universe

فیزیکی پول نقد است. عمده‌ترین روش‌هایی که در این مرحله مورد استفاده قرار می‌گیرد عبارت است از: سپرده‌گذاری درآمدهای ناشی از جرم و فعالیت‌های مجرمانه در بانک‌های داخلی یا سایر مؤسسه‌های مالی، سپرده‌گذاری در بانک‌های خارجی، خرید کالاهای با ارزش ویا به کار انداختن درآمدهای مجرمانه در رستوران‌ها، هتل‌ها و قمارخانه‌ها و کسب پول‌های تحصیل شده از این طریق.

اما در پولشویی الکترونیکی، جهت انجام مرحله جایگزینی، پولشو می‌تواند به‌راحتی و با استفاده از پول‌های الکترونیکی و توسط کارت‌های هوشمند، درآمدهای مجرمانه‌اش را با قابلیت بی‌نامی یا ناشناختگی که به صورت پول الکترونیکی درآمده، رد و بدل کند.

این پول‌ها می‌تواند در خرید پول‌های خارجی یا کالاهای باارزش مورد استفاده قرار گیرد تا این‌که دوباره فروخته شود و به این ترتیب از پول الکترونیکی جهت جایگزین شدن پول کثیف استفاده می‌شود. با این امکانات، دیگر پولشو نیاز به قاچاق پول یا هرگونه تراکنش چهره به چهره نخواهد داشت؛ زیرا به‌راحتی می‌تواند درآمدهای مجرمانه‌اش را که به شکل پول الکترونیکی درآمده از مرز منتقل سازد یا با آن‌ها کالاهای لوکس و ارزهای خارجی خریداری کند. بدین ترتیب مهم‌ترین امتیاز این روش در پولشویی الکترونیکی نسبت به روش‌های سنتی، حذف تراکنش‌های چهره به چهره و اختفای هویت است. در این روش اصلاً ثابت نمی شود که آیا هویت ارائه شده فرد درست است یا خیر. بنابراین، انجام این مرحله به روش الکترونیکی ریسک کم‌تری نسبت به روش سنتی آن دارد. حتی عده‌ای معتقدند نیازی به گذراندن این مرحله در پولشویی الکترونیکی نیست [۵، ص ۱۱۸]. در مرحله دوم، لایه‌های پیچیده از تراکنش‌های مالی به وجود می‌آید تا پول‌های کثیف و نامشروع از منبعشان فاصله بگیرند. در این مرحله، روش‌های سنتی زیادی وجو دارد؛ از جمله انتقالات سیمی، تبدیل پول‌های سپرده شده به سایر ابزارهای مالی یا کالا، سرمایه‌گذاری در تجارت‌های قانونی، استفاده از شرکت‌هایی تا بتوانند تحت پوشش آن عمل کنند و ... . اما برای یک پولشو همیشه سرعت، فاصله (بین پول مشروع و نامشروع) و گمنامی اهمیت زیادی دارد. تمام این ویژگی‌ها می‌تواند توسط خدمات مالی «پیوسته» ارائه شود. در این مرحله مجرم سعی می‌کند تا پول را از منشأ اصلی‌اش جدا کند. او می‌تواند به‌سادگی این کار را به وسیله انتقال پول از طریق شماره حساب در بانک‌های مختلف به منظور خرید ظاهری کالاها جهت فروش مجدد یا

از طریق شرکت‌های برون‌مرزی[۱] که در نظام‌های حقوقی مختلف قرار دارند، انجام دهد. در صورتی که به افراد اجازه داده شود به صورت اینترنتی افتتاح حساب کنند، بدون نیاز به ارائه مدارک و اسناد هویتی واقعی آنان، این مرحله می‌تواند ساده‌تر نیز انجام گیرد.

در مرحله سوم که آخرین مرحله از مراحل پولشویی است، پولشو نیاز دارد تا مطمئن شود که گردآوری پول و درآمدهایش به صورت غیر قانونی جلوه نکند. در روش سنتی پولشو می‌تواند از سازوکارهایی از جمله ارائه صورتحساب یا فاکتورهای نادرستی از کالاها،[۲] استفاده از شرکت‌های پوششی، بلیت‌های برد و باخت[۳]، هزینه‌های جابه‌جایی[٤] و قرض دادن پول‌های کثیف استفاده کند[۷، ص ١٦].

کاملاً واضح است که ریسک این سازوکارها بسیار بالا است. اما در پولشویی به روش الکترونیکی یک راه ساده این است که پولشو با ایجاد یک شرکت پوششی که قرار است ظاهراً خدماتی را ارائه کند، مانند فراهم‌کنندگان خدمات اینترنتی، یک حساب بانکی افتتاح می‌کند. پولشو حتی ملزم نیست تا خدماتی را هم ارائه دهد. در مقابل، او از این شرکت به عنوان یک پوشش استفاده می‌کند تا این طور وانمود شود که خدماتی که فراهم می‌گردد در عوض پرداخت وجوهی است که این وجوه (در حقیقت) منشأ مجرمانه داشته و از مرحله دوم (مرحله طبقه‌بندی و لایه‌لایه کردن) نیز گذشته است.

بررسی مقایسه‌ای مراحل پولشویی سنتی و مدرن این نتایج را به دنبال دارد:

۱) عدم نیاز به طی مراحل سه‌گانه جهت تطهیر اموال نامشروع، ۲) عدم نیاز به ارتکاب جرائم دیگری نظیر جعل، قتل، تهدید ویا حتی تطمیع کارمندان مؤسسات مالی و بانک‌ها، ۳) رسیدن به بیش‌ترین منفعت در کم‌ترین زمان ممکن و با کم‌ترین هزینه، ٤) تهدید رعایت حریم خصوصی کاربران شبکه‌ای و امکان سوءاستفاده از سوی پولشو، ٥) امکان اختفای هویت و عدم احراز هویت مشتری که موجب موفقیت پولشویان می‌گردد؛ زیرا به لحاظ عدم تعامل چهره به چهره در تراکنش‌های الکترونیکی ممکن است کاربر غیر از فردی باشد که حساب را باز کرده، و ٦) امکان بالقوه شکستن مرزهای ملی و دشواری تعیین مکان جرم پولشویی و مرتکب آن و تأثیر این امر صلاحیت کیفری کشورها.

---

1. off shore companies
2. false invoices of goods
3. wining tickt
4. transfer pricing

از مجموع آنچه گفته شد می‌توان گفت پولشویی سنتی و مدرن به رغم وجوه اشتراکی که با هم دارند، از جمله اهداف مشترک، استفاده از عاملین پوششی و استفاده از مؤسسات مالی و بانک‌ها و... تنها تفاوتشان در روش‌های ارتکاب این جرم است؛ به این معنا که استفاده از خدمات بانکداری الکترونیکی، ارتکاب پولشویی را بسیار ساده کرده و ریسک آن را در مقایسه با پولشویی سنتی کاهش داده است.

۶. راهکارهای مقابله با پولشویی

به جرأت می‌توان گفت تاکنون بجز پیشنهادهای جزئی و پراکنده درخصوص چگونگی مبارزه با پولشویی الکترونیکی، تنها اقدام منسجم در این زمینه، پیشنهادهای گروه کار اقدام مالی برای مبارزه با پولشویی است. به منظور کاهش آسیب‌پذیری ناشی از پولشویی از طریق فناوری‌های جدید پرداخت از طریق پول الکترونیکی، اقدامات زیر پیشنهاد شده است:

محدود کردن عملیات و ظرفیت کارت‌های هوشمند، متصل کردن فناوری‌های جدید پرداخت به مؤسسات مالی و حساب‌های بانکی، الزام به داشتن رویه‌های استاندارد ثبت اطلاعات و نگهداری رکوردها برای این سیستم‌ها به گونه‌ای که بتوانند رکوردهای مربوط را به وسیله اختیارات قضایی بررسی، مستندسازی و توقیف کنند و ایجاد استانداردهای بین‌المللی برای این مقیاس‌ها و معیارها، ایجاد رویه‌های جدید که توان مالی مؤسسات را برای شناخت کامل مشتریان خود تسهیل می‌کند، تلاش برای همسان‌سازی استانداردها، توسعه ظرفیت‌های فناوری اطلاعات جدید که هم به کشف تراکنش‌های پیوسته مشکوک و هم به تأیید مشتری کمک می‌کند، محدود کردن انواع خدمات مجاز پیوسته و حجم چنین تراکنش‌هایی، محدود کردن تراکنش‌های پیوسته صرفاً به حساب‌هایی که به روش سنتی و چهره به چهره گشایش شده باشند، و جلوگیری از ارائه خدمات الکترونیکی توسط مؤسسات مالی غیر مجاز.

سرانجام این که نظارت و سرپرستی باید هم از طریق حوزه قضایی ارائه‌دهنده مجوز بانک اینترنتی و هم به وسیله آن حوزه‌های قضایی که بانک‌های اینترنتی ارباب رجوع دارند، اعمال شود. این در حالی است که تدابیر اتخاذ شده در ماده ۲ و ٦ و ... آیین‌نامه اجرایی قانون مبارزه با پولشویی ایران به‌تنهایی برای مبارزه با پولشویی کافی نیست و این انتظار از

قانونگذار می‌رود تا با استفاده از تجربه‌های کشورهای دیگر و به کار بستن راهکارهای گروه کار اقدام مالی برای مبارزه با پولشویی و سایر اسناد موجود در این زمینه، بیش از پیش از ارتکاب پولشویی الکترونیکی، پیشگیری کند.

۷. نتیجه‌گیری

پیدایش و به‌کارگیری فناوری اطلاعات و ارتباطات در جوامع امروزی و همگرایی تجارت و کسب و کار و بانکداری با آن موجب رشد و توسعه پولشویی گردیده و محیط مناسبی را برای پولشویان سنتی از طریق فضای مجازی به وجود آورده که نه‌تنها ریسک عملیات پولشویی را افزایش نمی‌دهد، بلکه موجب تسهیل فرایند پولشویی و ایجاد شکل جدیدی از پولشویی تحت عنوان پولشویی الکترونیکی گردیده است. بنابراین می‌توان گفت پول و بانکداری الکترونیکی برای پولشویان ابزار بسیار ارزشمندی محسوب می‌شود؛ زیرا با کم‌ترین هزینه، بیش‌ترین منفعت را نصیب پولشویان می‌کنید. این در حالی است که فناوری‌های جدید به دلیل مزایای بی‌شماری که برای جوامع به همراه دارند، قابل حذف نیستند و تنها راهی که باقی می‌ماند دنبال کردن سیاست‌های اصولی‌ای است که از سوءاستفاده کلانی نظیر پولشویی جلوگیری می‌کنند و در عین حال به فعالیت‌های مشروع و قانونی‌ای که موجبات پیشرفت جوامع را فراهم می‌آورند، لطمه‌ای وارد نمی آورند. به نظر می‌رسد پولشویی الکترونیکی، به رغم کشف برخی از شیوه‌های ارتکاب آن گسترش خواهد یافت و مجرمان مسیرها و شیوه‌های پیچیده‌تری را برای ادامه فعالیت‌های‌شان در این فضا ابداع خواهند کرد و همواره چند گام از دست اندرکاران مبارزه با پولشویی جلوتر خواهند بود. دولت‌ها برای موفقیت در مبارزه با جرم و آثار آن در جوامع خود باید این فاصله را کم‌تر کنند و با دقت بیش‌تر به نقش فناوری‌های نوین در ارتکاب جرم توجه کنند.

۸. منابع

[۱] حسنعلی، فرنود، سلطانی، سهیلا، ضرابیه، فرشته، *مدیریت بانکداری الکترونیکی*، تهران انتشارات سبزان، ۱۳۸۷.

[۲] رو آن با سورث دیویس، سالت مارش، گراهام، پولشویی، ترجمه نصرا... امیر بشیری، تهران، معاونت آموزش ناجا، ۱۳۷٦.

[۳] میر محمد صادقی ، حسین، «پولشویی»، مجموعه *سخنرانی‌ها و مقالات همایش بین‌المللی مبارزه با پولشویی*، چ۲، شیراز، نشر وفاق، ۱۳۸۲.

[٤] سادوسکای، جورج و همکاران، *راهنمای امنیت فناوری اطلاعات*، ترجمه مهدی میرдامادی و همکاران، تهران، انتشارات گل واژه، ۱۳۸٤.

[٥] جلالی فراهانی، امیر حسین، «پولشویی اکترونیکی»، *فقه و حقوق*، دوره اول، ۱۳۸٤.

[6] Jamali, Mohamad Salman, «Cyber Laundering» University of East London, Proposal for Dissertion Module (CNM015), Topic of Interest: Cyber laundering.

[7] Filipkowski, Wojciech, «Cyber Laundering: An Analysis of Typology and Techniques» , *International Journal of Criminal Justice Scienes*,vol. 3, 2008, p.15-27.