پول‌شویی الکترونیکی و راه‌کارهای فنی و بین‌المللی دفاع در برابر آن

محمدرضا داوری[۱]، مجید داوری[۲]

تاریخ دریافت: ۸۹/۰۷/۱۲
تاریخ پذیرش: ۸۹/۱۱/۲۶

چکیده

با شروع دوره انقلاب علوم و فناوری‌ها، بخصوص فناوری اطلاعات، ارتباطات، الکترونیک و رایانه در سال‌های اخیر، جنگ‌های نسل چهارم طراحی و در چند جنگ اخیر نیز تجربه شده است و سیر تکاملی خود را طی می‌کند. یکی از اصلی‌ترین اهداف جنگ‌های مبتنی بر فن‌آوری‌های نوین اطلاعاتی و ارتباطی، بازارهای مالی و بانکی کشورها می‌باشد که در جهت تخریب و مسموم‌سازی بازارهای اقتصادی آن کشورها انجام می‌گیرد. در طی سه دهه گذشته مفهومی جدید از جرم در امور اقتصادی پا به منصه ظهور گذاشته که به‌دلیل ابعاد بسیار مخرب آن در سطح ملی و بین‌المللی، توجه نظام‌های اقتصادی، سیاسی، و حقوقی کشورها و سازمان‌های بین‌المللی را به خود معطوف داشته است و این جرم چیزی نیست جز پول‌شویی. پول‌شویی یا تطهیر پول، فعالیتی است مجرمانه، در مقیاس بزرگ، گروهی، مستمر و درازمدت که می‌تواند از محدوده سیاسی یک کشور مفروض نیز فراتر رود. پول‌شویی آثار زیانباری بر اقتصاد، جامعه و سیاست دارد. آلوده شدن و بی ثباتی اقتصاد، تضعیف بخش خصوصی و برنامه‌های خصوصی سازی، کاهش کنترل دولت بر سیاست‌های اقتصادی، فاسد شدن ساختار حکومت، بی‌اعتمادی مردم، بی‌اعتباری دولت‌ها و نهادهای اقتصادی کشور، گسترش تجارت‌های خلاف، بالارفتن هزینه‌های دولت و هزینه‌های مراقبت‌های پزشکی، کاهش درآمدهای مالیاتی دولت، ایجاد عدم ثبات و پایداری در بازار جهانی، صدمه رساندن به تلاش‌های جهانی برای ایجاد بازارهای آزاد و رقابتی و اختلال در رشد اقتصاد ملی، و... تنها بخشی از این آثار است. در طی دهه اخیر نیز سامانه‌های مالی از شکل جدیدی از کارکرد به‌نام الگوی الکترونیکی بهره‌مند شده‌اند. به‌تبع آن، تبهکاران از اقتصاد و جهانی‌سازی آن و پیشرفت‌های ناشی از فن‌آوری ارتباطات و اطلاعات در جهت مخفی‌سازی منابع درآمد نامشروع خود سوء استفاده می‌کنند. آنها از گروهی از تکنیک‌ها مثل انتقال سریع پول از یک کشور به دیگر کشورها یا شرکت‌ها و همکاری‌های شرکتی برای پاک کردن منبع ناصحیح آن استفاده می‌کنند. از طرفی به‌دلیل ماهیت فوق تخریبی آن، به نظر می‌رسد بعضی از قدرت‌های مافیایی و حکومتی برای فروپاشی نظام‌های اقتصادی کشورها و به‌تبع آن، نظام‌های سیاسی آنها، اقدام به بهره‌گیری از این روش به‌عنوان یک حمله غیر عامل نمایند. لذا شناخت این پدیده نوین و راه‌کارهای مناسب حقوقی و فنی برای جلوگیری از آن در راستای نیل به امر دفاع غیر عامل که امروزه ضرورتی غیر قابل کتمان می‌باشد، امری ضروری است.

کلیدواژه‌ها: پول‌شویی، پول‌شویی الکترونیکی، سامانه‌های پرداخت الکترونیکی، پول الکترونیکی، بانکداری الکترونیکی، انتقال سیمی

۱- کارشناس ارشد مهندسی فن‌آوری اطلاعات – تجارت الکترونیکی E-mail: mreza.davari@gmail.com
۲- دانشجوی کارشناسی ارشد مهندسی فن‌آوری اطلاعات

مقدمه

واژه پول‌شویی برای توصیف فرایندی مورد استفاده قرار می‌گیرد که در آن، پول غیرقانونی یا کثیفی که حاصل فعالیت های مجرمانه مانند قاچاق موادمخدر، قاچاق اسلحه و کالا، قاچاق انسان، رشوه، اخاذی، کلاهبرداری و بسیاری از جرائم یقه‌سفید[1]، و یا هم‌چنین برای فرار از مالیات در چرخه‌ای از فعالیت‌ها و معاملات، با گذر از مراحلی، شسته و به پول قانونی و تمیز تبدیل می‌شود. پول‌شویی به عنوان یک جرم در دهه ۱۹۸۰ بویژه در مورد عواید حاصل از قاچاق مواد مخدر و داروهای روان گردان مورد توجه کشورهای غربی قرار گرفت. این امر به دلیل آگاهی کشورهای مزبور از سودهای کلان حاصل از این فعالیت‌های مجرمانه و نگرانی آنها درباره گسترش مصرف موادمخدر در جوامع غربی بود که انگیزه مبارزه با فروشندگان مواد مخدر را برای دولت‌ها از طریق تدوین قوانینی که آنها را از عواید غیرقانونی محروم کند به وجود آورد. پیش‌بینی‌ها حاکی از آن است که ۲ تا ۵ درصد تولید ناخالص داخلی کشورها به پول‌شویی اختصاص دارد(رقمی بین ۶۰۰ میلیارد تا ۱/۸ تریلیون دلار) [۱].

ظهور فن‌آوری‌های پول الکترونیکی[2]، پرداخت الکترونیکی[3]، انتقالات سیمی[4]، پرداخت سیار[5]، بانکداری سیار[6]، و بانکداری الکترونیک[7]، عامل افزایش گونه‌ای از رویه‌ها از جمله پول‌شویی الکترونیک[8] گردیده است.

پول الکترونیکی از دو جهت می‌تواند برای پول‌شویان جذابیت داشته باشد. اول آنکه تراکنش های الکترونیکی ممکن است قابل رهگیری نباشد و به‌طور غیر قابل باوری ناشناس باقی بماند. لذا امکان بازرسی و حسابرسی‌های سنتی به شکلی کارآ برروی این *نوع* تراکنش‌ها وجود ندارد. دوم آنکه سامانه پول الکترونیکی امکان جابجایی آنی پول به شکلی مؤثر بدون محدودیت قلمروی را می‌دهد[۲]. کشورهای کوچک با اقتصاد ضعیف مکان مناسبی برای سازمان های پول‌شویی می‌باشد. چرا که با توان اقتصادی بالایی که این سازمان های پول‌شویی به‌دست آورده‌اند می‌توانند اقتصاد این‌گونه از کشورها را تحت اختیار قرار دهند. در کشورهایی با قوانین ناکارآمد در این زمینه، و یا با شرایطی که امکان اجرای قوانین در آنها وجود نداشته باشد، فضای خوبی برای اعمال تبهکارانه پول‌شویی و بالاخص پول‌شویی الکترونیکی به‌وجود می‌آید، که بتوانند به‌دلیل کمبود و خلأ ناشی از قوانین، منافع حاصل از درآمدهای غیرمشروع خود را حفظ نمایند [۳].

مطالب یاد شده، وضع قوانین و عملکردهای قانونی، پیگیری‌ها، مباحث، روش‌های اجرایی، و بحث مهم هماهنگی و همکاری بین‌المللی جهت جلوگیری، شناسایی، و آشکارسازی پول‌شویی الکترونیکی را ضروری می‌کند. این موضوعات ممکن است به همراهی چندین محیط نیاز داشته باشد:

- اقدامات محلی تا به بخش های اجرایی قانون ابزار موثر بیشتری داده شود.
- آموزش، هم در بخش های اجرایی قانون و هم در بخش‌های مالی از جمله قوانین مالی[9] .
- ضبط و پخش اطلاعات در هر کشور و در سطح بین‌المللی.
- قوانین پنهان برای ممانعت کردن از پول‌شویی، بدون جلوگیری از تراکنش های قانونی.

در اقتصاد ایران تاکنون به دلیل ناشناخته ماندن پیامدها و آثار زیانبار پول‌شویی و بالاخص پول‌شویی الکترونیکی، اقدام قابل توجهی صورت نگرفته است. تنها اقدام مثبت در این زمینه، لایحه منع پول‌شویی تقدیمی دولت به مجلس شورای اسلامی است که مراحل بررسی مقدماتی آن انجام شده است. اما با توجه به آنکه نظام جمهوری اسلامی ایران در اشکال مختلف مورد اهداف سوء قدرت های جهانی بوده و هست، بهره گیری از پول‌شویی و پول‌شویی الکترونیکی برای تضعیف نظام های پولی و سرمایه‌ای کشور در راستای هدف نهایی براندازی نظام جمهوری اسلامی، توسط این قدرت ها امری محتمل می‌باشد. لذا در این مقاله تلاش گردیده است تا ابتدا به تعریف و مراحل فرایند پول‌شویی و پول‌شویی الکترونیکی و آثار آن در نظام

1- White Collar Crime
(به تخلفاتی گویند که مرتبط با شغل‌های دفتری و فرهنگی باشد. در مقایسه باBlue Collar Crime که مربوط به شغل‌های مرتبط با کارهای بدنی است)

2- e-Money
3- e- Payment
4- Wire Transfer
5- Mobile Payment
6- Mobile Banking
7- e- Banking
8- Electronic Money Laundering

9- Financial Regulations

بانکی پرداخته شود و آنگاه به معرفی اقدامات و مستندات بین‌المللی دفاعی در مقابل این پدیده شوم مبادرت گردد.[1]

۱- هدف و پیشینه

در این مقاله تلاش گردیده با شناخت کامل جرم پول‌شویی الکترونیکی و با توجه به ظرفیت‌های موجود در حوزه بانکداری ایران در قلمرو الکترونیکی، قوانین و دستورالعمل‌های توصیه شده توسط سازمان‌ها و مراجع ذیصلاح بین‌المللی را جهت حضور پررنگ‌تر در تعاملات بین‌المللی مورد کنکاش و بررسی قرارداده، و راه های عملیاتی چه در حوزه فنی و چه در حوزه حقوقی - ارایه گردد. لذا نتایج این تحقیق می‌تواند برای بخش های مالی(بانک ها، موسسات مالی و اعتباری، صندوق های قرض‌الحسنه، سازمان های بیمه‌گری، موسسات لیزینگ و غیره) و همین‌طور نهادهای قانون‌گذار کشور در جهت محدودسازی تخریب‌های ناشی از این پدیده در بازاز مالی و در نهایت، کل نظام اقتصادی و اجتماعی کشور، مورد استفاده قرار گیرد.

متأسفانه به نظر می‌رسد در ایران تاکنون تحقیق مشخصی در حوزه پول‌شویی الکترونیک انجام نپذیرفته است. هم‌چنین اطلاعاتی دقیق و مستند از اشکال مختلف انجام آن و مبالغ تطهیرشده احتمالی در حوزه بانکی و مالی کشور وجود ندارد. لذا در این مقاله با در نظرگیری وضعیت بانکداری الکترونیک (در شکل عام آن) در کشور و بررسی مقالات و تحقیقات بین‌المللی که توسط سازمان‌های ذیصلاح انجام پذیرفته و مطابقت آن با شرایط بالقوه موجود در کشور، سعی گردیده در ابتدا این مقوله مورد بررسی و شناخت قرار گرفته و در امتداد آن، راه‌های قانونی پیشنهادی ارایه گردد (تحقیقات کتابخانه‌ای).

۲- تعاریف

۲-۱- پول‌شویی

در دستورالعمل جامعه اروپایی مصوب مارس ۱۹۹۰ تعریف پول‌شویی به صورت زیر است: «تبدیل یا انتقال یک دارایی، با علم به اینکه از فعالیت‌های مجرمانه به‌دست آمده باشد، به‌منظور پنهان داشتن یا گم کردن رد منشأ غیرقانونی آن دارایی، یا کمک به شخصی که مرتکب چنین جرمی شده است برای گریز از پیامدهای قانونی جرم مزبور».

تعریف پول‌شویی در پیمان‌نامه شورای اروپا مربوط به نشست اوت ۱۹۹۰ استراسبورگ تکمیل شد و موارد زیر به تعریف ارائه شده در دستورالعمل جامعه اروپا افزوده شد: «تحصیل، تملک یا استفاده از دارایی‌های به‌دست آمده از منابع غیرقانونی و نیز هرگونه مشارکت، مباشرت، تبانی برای ارتکاب، اقدام به ارتکاب یا کمک، ترغیب، تسهیل و پنهان‌کاری هرگونه جرم مرتبط با پول‌شویی» [۱۴].

«گروه کاری اقدام مالی برای مبارزه با پول‌شویی»[2] در گزارش خود فرایند عمل با رفتار پول‌شویی را شرح داده است که شامل اجزای زیر است:[۵]

- تبدیل یا انتقال مال با علم به اینکه چنین مالی از یک جرم کیفری حاصل شده است به‌منظور مخفی کردن یا تغییر ظاهر منشأ غیرقانونی مال مورد نظر یا کمک به شخصی که مرتکب چنین جرمی شده است برای فرار از پیامدهای قانونی عمل خود.
- پنهان کردن یا تغییر ماهیت واقعی، منشا، محل، جابه‌جایی یا مالکیت مال با علم به اینکه چنین مالی از فعالیت‌های مجرمانه حاصل شده است.
- تملک، تصرف، یا استفاده از مال با علم به اینکه چنین مالی حاصل فعالیت‌های مجرمانه است. [۱۵]
- پول‌شویی یعنی تبدیل یا انتقال سرمایه، سرمایه‌ای که مطلع هستیم از روش‌های غیر قانونی به‌دست آمده است، با هدف پنهان کردن ماهیت نامشروع و منبع سرمایه از حسابرسی های دولتی [۲]. طبق آمار منتشر شده، حجم پول‌شویی جهانی از طریق تجارت مواد مخدر به‌تنهایی بین ۳۰۰ تا ۴۰۰ میلیارد دلار در سال ۱۹۹۸ بوده است، در حالیکه آمار، رقم دو برابر این میزان را برای پول‌شویی به‌طور کلی در صحنه جهانی نشان می‌دهد. به‌طور مثال

1- سرنوشت لایحهء تأثیرگذار و چالش‌برانگیز «مبارزه با جرم پول‌شویی» که حدود سه سال از تدوین و تصویب آن در مجلس می‌گذرد هنوز مبهم و نامشخص است و براساس آخرین اظهارنظرها، پس از نرسیدن به جمع‌بندی‌های لازم در مورد اصلاحات موردنیاز این لایحه در مجمع تشخیص مصلحت نظام -که از ۲۹ اردیبهشت بررسی آن را شروع کرده بود- حدود دو هفته پیش دوباره به مجلس بازگردانده شده است و به گفته مرتضی تمدن، عضو کمیسیون برنامه و بودجه مجلس، قرار است با تشکیل کارگروهی شش نفره برای بررسی و اصلاح آن، مجدداً به مجمع تشخیص مصلحت نظام بازگردانده شود. (روزنامه سرمایه، ۸۶/۰۵/۲۸)

2- Financial Action Task Force(FATF)

آمار بیانگر آنست که ۵۰ تا ۷۰ درصد از سود فروش مواد مخدر در کانادا تطهیر گردیده و در سرمایه‌گذاری‌های بعدی مورد استفاده قرار می‌گیرد. علاوه بر این ۵۰ تا ۷۰ درصد پول‌های تطهیر شده در کانادا از تجارت مواد مخدر استحصال شده است [۵]. تحقیقات اخیر در انگلستان حاکی از آن است که جرایم مالی ۲درصد از تولید ناخالص داخلی[1] این کشور را تشکیل می‌دهد [۶]. دلیل دیگر برای پول‌شویی، گریز از مقدار بالای مالیات در سیستم اقتصادی زیرزمینی است. در این مورد مرتکبان در جستجوی راهی برای پنهان کردن سودهایشان و یا انتقال آن به خارج از کشور هستند

۲-۲- پیامدهای پول‌شویی

گروه کاری اقدام مالی برای مبارزه با پول‌شویی وابسته به سازمان همکاری اقتصادی و توسعه[2] تهدیدهای اساسی پدید آمده از معضل جهانی پول‌شویی را چنین برشمرده است:

- کوتاهی در مبارزه با پول‌شویی، عاملی است در جهت آسان‌سازی سودآوری فعالیت‌های مجرمانه یا غیرقانونی؛
- کوتاهی در مبارزه با پول‌شویی، دست سازمان‌های مجرم را در تامین مالی فعالیت‌های مجرمانه و گسترش آن فعالیت‌ها آزادتر می‌گذارد.
- امکان به‌کارگیری شبکه مالی رسمی از سوی پول‌شویان، خطر فسادپذیری نهادهای مالی و کل بخش مالی اقتصاد ملی را به همراه می‌آورد.
- انباشت قدرت و ثروت توسط مجرمان و گروه‌های بزهکار برخوردار از امکان پول‌شویی، تهدیدی جدی برای اقتصاد ملی و بویژه برای نظام های مردم‌سالار به‌شمار می‌آید.
- تضعیف بخش خصوصی؛ پول‌شویان با هدف پنهان کردن عواید حاصل از فعالیت‌های غیرقانونی خود، با استفاده از شرکت های پیشرو، عواید مزبور را با وجوه قانونی مخلوط می‌کنند. از آنجایی که این شرکت‌ها به وجوه غیرقانونی قابل توجهی دسترسی دارند که به آنها کمک می‌کند تا محصولات و خدمات خود را با قیمتی کمتر از سطح قیمت بازار ارائه دهند، این امر رقابت را برای شرکت های قانونی بسیار مشکل می‌سازد و باعث بیرون راندن آنها توسط شرکت‌ها و سازمان‌های مجرم از بازار و تضعیف بخش خصوصی قانونی در اقتصاد می‌شود.
- تضعیف یکپارچگی و تمامیت بازارهای مالی؛ مؤسسات مالی متکی به عواید حاصل از فعالیت‌های مجرمانه در مدیریت مناسب دارایی‌ها و انجام به‌موقع تعهدات و عملیات خود با مشکلات و چالش‌های بیشتری مواجه‌اند.
- کاهش کنترل دولت بر سیاست‌های اقتصادی؛ در بعضی از کشورهای در حال توسعه این عواید غیرقانونی ممکن است میزان بودجه دولت را تحت‌الشعاع قرار دهد و در نتیجه، کنترل دولت بر سیاست‌گذاری‌های اقتصادی را کاهش دهد.
- اخلال و بی‌ثباتی در اقتصاد؛ اشخاصی که اقدام به پول‌شویی می‌کنند به دنبال سود حاصل از سرمایه‌گذاری وجوه غیرقانونی خود در فعالیت‌های اقتصادی نیستند، بلکه هدف آنها نگهداری اصل وجوه و عواید مزبور است. بنابراین، آنها وجوه خود را به لزوم در فعالیت‌هایی که برای کشور محل استقرار وجوه مزبور، سودآور باشد سرمایه گذاری نمی‌کنند. آنها سرمایه‌های خود را به بخش های ساختمان سازی و هتلداری سوق داده و این موضوع خسارت شدیدی به بخش‌های مزبور و کل اقتصاد وارد می‌کند.
- ایجاد موانعی برای خصوصی‌سازی و کاهش درآمد دولت و خطرپذیری اعتباری برای دولت‌ها در شرایط کنونی اقتصاد جهانی از دیگر آثار جانبی منفی اقتصادی پدیده پول‌شویی است.

هم‌چنین در تحقیقی که در بخش قضایی کشور کانادا انجام پذیرفته نتایج دیگری از جمله موارد زیر بیان گردیده است:

- باعث بالا رفتن هزینه‌های اجرای قوانین و هزینه‌های مراقبتهای پزشکی می‌شود (مثلاً خطرات تأثیر مواد مخدر)
- به‌عنوان عاملی بالقوه برای از زیر نقب زدن در مجامع اقتصادی و بی‌اعتباری اقتصاد دولتی بوده و نیز پتانسیلی برای افزایش تباهی و ارتشاء با حجم وسیعی از پول های غیرقانونی در چرخه اقتصادی است.
- پول‌شویی، درآمد مالیاتی دولت‌ها را کم کرده و بنابراین به‌صورت غیر مستقیم به راستگویی و صداقت پرداخت‌کنندگان مالیات صدمه وارد می‌کند.
- تصور ورود آسان به کشورها، عاملی غیرمطلوب ولی جذاب در میان مرزهاست، که باعث پایین آمدن سطح کیفی زندگی و بالا رفتن تهدیدات امنیتی در کشورهاست.

1- Gross Domestic Product(GDP)
2- Organization for Economic Co-operation and Development (OECD)

- ۲-۳- کوشش‌های جهانی برای مبارزه با پول‌شویی
- پیمان‌نامه وین اولین سند بین‌المللی است که در آن تعریفی دقیق از پول‌شویی ارائه شده و راه‌هایی برای محروم کردن اشخاص دست‌اندرکار قاچاق مواد مخدر از عواید فعالیت‌های مجرمانه آنها و درنتیجه، کاهش انگیزه آنان برای ادامه این فعالیت‌ها پیشنهاد شده است.
- اعلامیه کمیته بال در سال ۱۹۸۸ برای جلوگیری از کاربرد مجرمانه شبکه بانکی به قصد پول‌شویی به امضا رسید.
- نیروی ویژه اقدام مالی در نشست پاریس به وسیله هفت کشور به منظور تدوین دستورالعمل هماهنگ بین‌المللی برای مبارزه با پول‌شویی تاسیس شد.
- گزارش گروه اقدام مالی برای مبارزه با پول‌شویی [۱۲] که فرضیه آن شناسایی و تدوین راهکارهای مناسب برای مبارزه با پول‌شویی است، در این راستا با انتشار رویکردهای سیاسی و توصیه هایی در این باره، کشورهای جهان را به همکاری بین‌المللی فرا می‌خواند.
- پیمان‌نامه شورای اروپا که در تاریخ ۸ نوامبر ۱۹۹۰ برای تحقیق و بازرسی، ضبط و مصادره عواید حاصل از جرم تأکید شده است.
- علاوه بر موارد فوق در سال ۱۹۹۰، کمیسیون بین‌المللی آمریکایی مبارزه با اعتیاد[1] در سال ۱۹۹۲ به تصویب نهایی رسید و در سال ۱۹۹۷ اصلاح شد.
- در ۱۰ ژوئن ۱۹۹۱ جامعه اروپا دستورالعملی را به‌منظور منع استفاده از نظام مالی برای مقاصد پول‌شویی تصویب کرد. و قوانین دیگری نیز تا سال ۲۰۰۰ میلادی به تصویب رسیده و یا اقدامات ویژه‌ای در این مورد صورت گرفته است.
- دیگر اقدام جدی بین‌المللی به‌منظور تدوین راهکارهایی برای مبارزه با معضل جهانی پول‌شویی عبارت است از: «پیمان‌نامه مبارزه با جرایم سازمان‌یافته فراملی». این پیمان‌نامه در دسامبر ۲۰۰۰ توسط سازمان ملل تدوین شد. براساس ماده یک این پیمان‌نامه، هدف از تدوین آن تقویت همکاری به‌منظور پیشگیری و مبارزه مؤثرتر با جرایم سازمان یافته است. ماده ۵ این پیمان‌نامه، مشارکت در گروه جرائم سازمان یافته را جرم اعلام کرده است و ماده ۶ آن نیز پول‌شویی و عواید حاصل از جرم سازمان یافته را جرم شناخته است. در تعریف جرم پول‌شویی در پیمان‌نامه مزبور بر ارتباط منشأ جرائم مربوط به قاچاق مواد مخدر و نیز ارتباط جرم پول‌شویی با جرائم سازمان یافته در سطح بین‌المللی تأکید شده است. در موارد ۷ و ۸ این پیمان‌نامه تدابیری برای مبارزه با پول‌شویی و همچنین مجازات‌هایی برای فساد مالی پیشنهاد شده است [۱۵].
- در سپتامبر ۲۰۰۱، شورای امنیت سازمان ملل طی قطعنامه۱۳۷۳ اعضاء را به وظایفی ملزم نمود که شامل جلوگیری و سرکوبی اقدامات تروریستی و فعالیت‌های وابسته به تروریسم بود. هم‌چنین همکاری برای کشف این اعمال.
- در قطعنامه‌ای مشابه، شورا، کمیته مقابله با تروریسم[2] را برای نظارت بر اجرای قطعنامه، ایجاد نمود.
- در آوریل ۱۹۹۰، گروه اقدام مالی برای مبارزه با پول‌شویی، مرجعی شامل ۴۰ پیشنهاد برای توسعه سیستم قانون ملی کشورها در جهت بهسازی نقش و جایگاه بخش‌های مالی و هم‌چنین تشدید همکاری‌ها در مقابله با پول‌شویی ارایه داد که این مرجع در سال‌های ۱۹۹۶و ۲۰۰۳ مورد تجدید نظر قرار گرفت.
- هم‌چنین در سال ۲۰۰۱، گروه اقدام مالی برای مبارزه با پول‌شویی، اساسنامه‌ای شامل ۸ پیشنهاد برای مبارزه با امور مالی تروریسم ارایه داد. نهمین پیشنهاد نیز در سال ۲۰۰۴ به آن اضافه شد.
- همراه ۲ پیشنهاد بالا، پیشنهادات FATF 40+9، مجموعه‌ای برای ارزیابی قوانین کارآمدتر و رژیم اداری در مقابله با پول‌شویی و امور بانکی تروریسم می‌باشد که گروه اقدام مالی برای مبارزه با پول‌شویی ارایه کرده است.

دیگر انجمن‌ها هم‌چون کمیته بال در امور نظارت بانکداری[3] و همین طور بخش‌های منطقه‌ای هم‌چون شورای اروپا[4] و اتحادیه اروپایی[5]، قوانینی در جهت جلوگیری از کاربرد سامانه های مالی (بانکی و غیربانکی) برای تطهیر پول‌های نامشروع به‌تصویب رسانده‌اند.

۲-۴- توصیه‌نامه‌های جهانی برای مبارزه با پول‌شویی

- پیشنهاد بانک جهانی در خصوص مقابله با پول‌شویی در فضای مجازی [۶].

1- Inter-American Drug Abuse Control Commission (CICAD)

2- Counter-Terrorism Committee (CTC)
3- Basel Committee on Banking Supervision
4- Council of Europe
5- European Union

- یادداشتی برای ارزیابی و سنجش در راستای مبارزه با پول‌شویی و مبارزه با سرمایه‌گذاری های گروه‌های تروریستی [۷].
- گزارش وزارتی برای ارزیابی و سنجش در راستای مبارزه با پول‌شویی و مبارزه با سرمایه‌گذاری‌های گروه‌های تروریستی [۸].
- مدل قانونی در مقابل پول‌شویی و بخش مالی تروریسم [۳].
- گزارش سالیانه پول‌شویی آسیا / پاسیفیک [۹].

دستورالعمل امنیت بانکی / روش بررسی ضد پول‌شویی، توسط مؤسسه مالی فدرال ایالات متحده آمریکا [۱۰].

۲-۵- پول الکترونیکی

پول الکترونیکی با اسامی مختلف eCash, Digital money, و eMoney به انگلیسی و در فارسی با عباراتی نظیر پول بر پایه اطلاعات، پول غیرقابل لمس، پول رقمی و پول الکترونیکی شناخته شده است. هویت پول الکترونیکی از لحاظ ساختاری, عبارت است از بیت‌های موجود در حافظه رایانه, که دارای ارزشی برابر با ارزش پول نقد می‌باشد[۲۰].

پول الکترونیکی مانند کارت‌های اعتباری، چک الکترونیکی و موارد مشابه آن، فقط حاوی اطلاعات پولی نیست بلکه دارای خاصیت پول حقیقی است. وجه نقد الکترونیکی روشی برای پرداخت‌های رایانه‌ای و اینترنتی می‌باشد، بدین نحو که یک فرد می‌تواند با انتقال یک «عدد» از یک رایانه به رایانه دیگر، کالا یا خدمات مورد نیاز خود را تهیه کند، این اعداد که نشان‌دهنده جمع پول واقعی فرد است به‌صورت کد درآمده و حالت مجازی دارد.

یکی از شیوه‌های مورد استفاده پول الکترونیکی کش‌نت[1] می‌باشد. روش عمل کش‌نت (شبکه پول الکترونیکی) عموماً به این نحو است که استفاده‌کننده، شماره‌ای انحصاری از کش‌نت خریداری می‌کند. این شماره معرف ارزش پولی است و تنها برای مالک آن قابل تعریف می‌باشد. دارنده آن می‌تواند هر آنچه را که می‌خواهد و از هر جا که می‌خواهد، خریداری نموده و پس از ارسال آن به فروشنده کالا و خدمات، قابلیت استفاده مجدد آن برای فروشنده وجود دارد. بنابراین فروشنده می‌تواند آن را از طریق کش‌نت، نقد نماید و یا در گردش معاملاتی از آن استفاده کند. این پول از طرق مختلف قابل خریداری است و از آنجا که این پول در سطح جهان رایج است از تمام مراکز اقتصادی و بانکی قابل تهیه می‌باشد.

نقش‌ها و وظایف پول الکترونیکی عبارت است از:

- پول الکترونیکی ارزش را به صورت اطلاعات دیجیتالی و بدون وابستگی به حساب بانکی در خود نگه می‌دارد.
- پول الکترونیکی می‌تواند از طریق انتقال اطلاعات دیجیتالی ارزش را به دیگری منتقل نماید.
- پول الکترونیکی برای پرداخت‌های از راه دور مخصوصاً در شبکه‌های عمومی (مثل شبکه‌های ارتباطی و اینترنت), بسیار مناسب است.
- در بعضی موارد پول الکترونیکی نیازی به طرف سوم برای نظارت و تأیید معامله ندارد.
- پول الکترونیکی برای پرداخت‌های با مبالغ کم (کم ارزش) مناسب می‌باشد[2].
- پول الکترونیکی را به شیوه‌های مختلف تقسیم‌بندی می‌نمایند، در یکی از تقسیم‌بندی‌ها پول الکترونیکی را به دو دسته تقسیم می‌نمایند:

■ **پول الکترونیکی شناسایی شده:**

❑ این نوع پول الکترونیکی حاوی اطلاعاتی دربارهٔ هویت مالک آن می‌باشد که تا حدودی مانند کارت‌های اعتباری است. این پول‌ها دارای قابلیت ردگیری می‌باشند و هویت دارنده آن قابل شناسایی است. قابلیت استفاده از این پول در دو روش برخط[3] و برون خط[4] امکان‌پذیر است.

■ **پول الکترونیکی غیرقابل شناسایی (بی‌نام و نشان):**

❑ این نوع پول دیجیتالی[5] خصوصیت مخفی بودن هویت فرد دارنده‌اش را در بردارد, و از این لحاظ درست مانند پول کاغذی سنتی عمل می‌کند. هنگامی که پول دیجیتالی از حسابی برداشت شد، بدون باقی گذاشتن هیچ اثری می‌توان آن را خرج نمود و با توجه به این نکته که هنگام ایجاد کردن پول دیجیتالی از امضاهای نامشخص استفاده می‌شود، لذا امکان پی‌گیری آن برای هیچ بانکی وجود ندارد [۱۳].

1- Cashnet

2- Reed & Davies (1995), P.1.
3- On-Line
4- Off-Line
5- Digital Cash

با عدم تمرکز و طبیعت پخش شدنی پول الکترونیکی، این نوع پول دارای همان توانمندی جابجایی ساختار اقتصادی است که رایانه های شخصی برروی ساختار ارتباطات و مدیریت نظارتی و مراقبتی داشتند.

پیشرفت ها در سه زمینه فن‌آوری باعث به‌کارگیری وسیع پول نقد الکترونیکی در اقتصاد گردید، این پیشرفت‌ها عبارتند از :

- ارتباط شبکه‌ای سریع و قابل اعتماد با هزینه کم به‌ازای هر تراکنش.
- فن‌آوری رایانه‌ای بهتر که باعث تولید انبوه بردهای کامپیوتری شده است.
- رمزنگاری عمومی قدرتمند که باعث کمک به ایجاد اطمینان بیشتر و امنیت در مقابل خطاها شده است.

آنچه که برای سامانه‌های پول الکترونیکی «انقلاب» محسوب می‌شود، جایگزینی آنها به‌جای پول نقد کاغذی می‌باشد. یعنی هدف از ابداع آنها، برعهده گرفتن مسئولیت تراکنش های کوچک الکترونیکی است که بخش عمده‌ای از تراکنش‌ها را شامل می‌شوند.

پول الکترونیکی از چند جهت اصلی برای پول‌شویان جذاب است:

- ره‌گیرناپذیری[1]؛ به‌کارگیری پول الکترونیکی به منزله کمترشدن تراکنش‌های مالی رودررو است. ناشناس بودن پول الکترونیکی، شناسایی مشتری را بسیار مشکل می‌سازد. سامانه‌های پول الکترونیکی این امکان را می‌دهد که طرف‌های مورد معامله به‌صورت مستقیم و بدون واسطه‌های مالی رسمی عمل تراکنش را انجام دهند، بنابراین امکان بازرسی‌های سنتی وجود ندارد. در این سامانه به خریدار کش‌نت (دارنده پول الکترونیکی) تضمین داده می‌شود که هویت وی کاملاً ناشناس باقی مانده و برای وی هیچ‌گونه تبعات و عواقب منفی (بعد از خرید) در پی نخواهد داشت. در واقع استفاده‌کننده اگر قصد مخفی نمودن هویت خود را داشته باشد می‌تواند از دستگاه خودپرداز[2] یا از سامانه کش‌نت که به شبکه متصل است و یا از طریق شبکه بانکی که در آن حساب دارد، اقدام به تهیه آن نماید. بدین ترتیب پول الکترونیکی غیرقابل ردیابی می‌باشد.
- تحرک[3]؛ پول الکترونیکی می‌تواند از هر جا بیاید و به هرجا برود. بنابراین سامانه پول الکترونیکی تحرک سریع پول برروی بستر شبکه را که در حقیقت موضوعی برای هیچ کدام از محدودیت‌های قانونی نیست، امکان‌پذیر می‌سازد.
- قابلیت گردش و چرخش نامحدود[4] (تا زمان از بین رفتن خود آن[5])، پس از صادر کردن شماره پول الکترونیکی، مالک شماره می‌تواند از طریق اینترنت هر آن چیزی را که در توان دارد بخرد. پس از خرید آن در شبکه کش‌نت، فروشنده بلافاصله شماره را دریافت و می‌تواند در همان شبکه، پول الکترونیکی خود را نقد یا در چرخه خرید و رد و بدل پولی به فرد دیگری انتقال دهد. بدین نحو پول الکترونیکی تا زمان نامحدود و تا وقتی که پول مفقود یا به سرقت نرفته قابلیت کاربرد خود را حفظ می‌کند.
- قابلیت کار در حالت برون‌خط[6]، یکی دیگر از ویژگی های پول الکترونیکی، قابلیت پرداخت به‌صورت برون‌خط می‌باشد. ضمن داشتن این قابلیت، این امکان را به کاربر خود می‌دهد که بدون این‌که مستقیماً بانکی را درگیر کند معامله را انجام دهد. در این روش مشتری می‌تواند امور پولی و تبادل مالی خود را بدون مراجعه به بانک یا مؤسسه مالی مرجع انجام دهد.

۲-۶- مراحل پول‌شویی در سامانه الکترونیکی

۲-۶-۱- جایگذاری الکترونیکی

قدم اول در پول‌شویی، رهایی فیزیکی از پول نقد است. به‌طور سنتی، جایگزینی با ذخیره‌سازی پول در بانک‌ها یا مؤسسات مالی، امن می‌باشد. یا این‌که ممکن است پول نقد بصورت قاچاق به خارج از مرزهای کشور برای سپرده‌گذاری در یک حساب خارجی منتقل شود و یا برای خرید کالاهای با قیمت بالا مصرف گردد، مانند کارهای هنری، هواپیما، فلزات گرانبها و سنگ‌های قیمتی، که بعدا بتوان آن را فروخت. با پول‌شویی الکترونیکی، پول نقد را می‌توان در مؤسسات مالی غیرمعمول ذخیره کرد. آنگاه به‌وسیله کارت هوشمند یا انتقال از طریق اینترنت برای خرید دارایی‌ها و یا محصولات و کالاها در خارج از کشور، استفاده کرد. این در حالی است که رمزنگاری قدرتمند نیز می‌تواند ناشناس ماندن را در تراکنش تضمین کند.

1- Untraceablity
2- ATM (Automatic Teller Machine)

3- Mobility
4- Infinite Duration
5- Until Destroyed
6- Off-Line

۲-۶-۲- لایه‌بندی الکترونیکی

در این قدم نیاز به لایه‌های مجتمع از تراکنش های مالی برای ایجاد فاصله بین درآمدهای کثیف از منبع آن و گمراه کردن بازرسی‌ها می‌باشد. در این مرحله تبدیل پول ذخیره شده به ابزارآلات پولی، و سرمایه‌گذاری در مسکن و تجارت‌های قابل قبول و به‌طور خاص در امور تفریحی و گردشگری، وشرکت‌های مشارکتی که به‌طور معمول در خارج از کشور نیز ثبت شده‌اند، یک رفتار عامه‌پسند برای مرحله لایه‌بندی در پول‌شویی سنتی می‌باشد. در یک سامانه پول الکترونیکی، لایه‌بندی از طریق یک رایانه شخصی به‌راحتی انجام می‌پذیرد. این روش معمولاً بازرسی را پیش رو ندارد، به‌علاوه سامانه پول الکترونیکی جابه‌جایی پول در یک سیستم بدون مرز را پشتیبانی می‌کند.

۲-۶-۳- یکپارچه‌سازی الکترونیکی

قدم پایانی آن است که پول‌های هنگفت به‌وجود آمده از راه خلاف، به‌نظر قانونی بیاید. بطور سنتی یکپارچه‌سازی ممکن است ناشی از چندین روش باشد. روش‌هایی از جمله: استفاده از شرکت‌های پیشخوان برای قرض دادن پول به صاحب اصلی آن یا سرمایه‌گذاری پول در مؤسسات مالی خارج از کشور به‌شکلی امن برای دادن وام‌های قانونی. روش دیگر مانند ایجاد رسیدهای فروش و یا حتی جعل رسیدهای اجناس فروش رفته در میان مرزها می‌باشد. در سامانه پول الکترونیکی این مرحله نیز با استفاده از یک رایانه شخصی برای پرداخت در سرمایه‌گذاری هایی مثل خرید ملک، بدون نیاز به کمک یک مؤسسه مالی واسطه انجام می‌پذیرد.

۲-۷- روش‌های پنهان‌سازی منبع پول در سامانه‌های پرداخت سیمی و الکترونیکی [۹]

روش‌های متنوعی توسط تبهکاران و مؤسسات جرایم سازمان‌یافته برای پنهان‌سازی مبدا و منبع پول‌های کثیف در سامانه‌های پرداخت سیمی و الکترونیکی، به‌کار گرفته می‌شود. از آن جمله می‌توان به موارد زیر اشاره کرد:

- ساختار و چیدمان[1]؛ به مفهوم نگهداری مقدار پول انتقالی به میزان کمتر از محدوده گزارش‌دهی. یعنی مثلاً اگر میزانی از انتقال که باید مورد بررسی‌های قانونی قرار گیرد ده هزار دلار باشد، فرد مجرم مقدار پول کثیف را به رقم‌های کمتر از این میزان تقسیم‌بندی کرده، و به تکرار پول کثیف را انتقال دهد.
- استفاده از شخص ثالث[2]؛ استفاده از فرد دیگری که به‌طور مستقیم دخیل در فعالیت‌های غیرقانونی نمی‌باشد (به‌طور مثال افراد فامیل یا بیگانه).
- پوشش شرکتی دادن[3]؛ ارسال و/ یا دریافت پول تحت عنوان نام‌های تجاری که نشان دهد تراکنش در قالب تجاری انجام گرفته است.
- مخلوط کردن[4]؛ ترکیب پول‌های ناشی از فعالیت‌های غیرقانونی با پول‌های ناشی از فعالیت‌های قانونی.
- صورتحساب اشتباه[5]؛ بیان اشتباه مقادیر بدهکاری بر کالاهای وارداتی برای ارایه دلایل قانونی جهت ارسال پول‌های اضافه به خارج.
- مشخصات غلط[6]؛ ارسال پول و/ یا تأسیس و افتتاح حساب به‌صورت محلی یا خارجی با استفاده از مشخصات غلط.
- پوشش خیریه[7]؛ استفاده از پوشش سازمان‌های خیریه و یا سازمان‌های غیر انتفاعی و استفاده از بخشی از پول در قالب خیریه و یا قرض‌الحسنه.[8]

1- Structuring
2- Smurfing
3- Shell Companies
4- Co-Mingling
5- False invoicing
6- False Identification
7- Charities or non-Profit organizations

۸- پول‌شویی در صندوق‌های قرض‌الحسنه شایعه است. اما از جمله موضوعاتی که در سال‌های اخیر درباره پولشویی، پیوسته مطرح بوده، مبادی پول‌شویی و راه‌های ورود پول‌های کثیف به سیستم پولی کشور است و در این میان، صندوق‌های قرض‌الحسنه همواره در صف اول آماج این اتهامات قرار داشته‌اند؛ اما عضو هیأت مدیره سازمان اقتصاد اسلامی در گفت‌وگو با «سرمایه» ضمن رد این اتهامات، تمام این حرف‌ها را شایعاتی بیش نمی‌داند. میرمحمد صادقی در پاسخ به این سوال که «آیا به نظر شما صندوق‌های قرض‌الحسنه پوششی برای اعمال خلاف چون پولشویی محسوب می‌شوند یا خیر؟» به تأکید گفت: «این‌گفته‌ها شایعه است، در تمام صندوق‌های قرض‌الحسنه که حدود چهار هزار صندوق هستند اگر به دنبال صندوق‌های متخلف باشند به عدد ۱۰ هم نمی‌رسند (روزنامه سرمایه ۱۳۸۶/۵/۲۸).

۳- چارچوب‌های قانونی بین‌المللی پیشنهادی برای مبارزه با جرم پول‌شویی الکترونیک

۳-۱- مدل قانونی پیشنهادی توسط دفتر جرایم و مواد مخدر سازمان ملل[1] در سال ۲۰۰۵

این مدل قانونی در سال ۱۹۹۹ توسط دفتر مواد مخدر و جرایم سازمان ملل برای کمک به کشورها برای وضع قوانین مدنی در مقابله با پول‌شویی و همین‌طور کمک به استانداردسازی قوانین موجود در کشورها در این حوزه، وضع گردید. این چارچوب بر مبنای ابزارهای قانونی در کشورهای مختلف برای مقابله با پول‌شویی و هم‌چنین بر مبنای پیشنهادات ۹+۴۰ سازمان گروه کاری اقدام مالی برای مبارزه با پول‌شویی، بنا نهاده شده است.

طبق این دستورالعمل همه کشورها موظف به هماهنگ نمودن قوانین داخلی‌شان با این مقررات و هم‌چنین بهسازی و بازسازی سیستم و قوانین حقوقی‌شان می‌باشند.

این مدل قانونی شامل ۶ عنوان می‌باشد:

- تعریف
- جلوگیری از پول‌شویی و جرایم مالی تروریسم
- کشف پول‌شویی و جرایم مالی تروریسم
- قوانین رسیدگی پنهانی
- میزان کیفر
- همکاری‌های بین‌المللی

دستورالعمل‌های این مدل قانونی توسط گروهی از کارشناسان بین‌المللی که در ماه می ۲۰۰۴ در وین و در ماه می ۲۰۰۴ در بروکسل و در سپتامبر ۲۰۰۴ و مارچ ۲۰۰۵ در واشنگتن گردهم‌آیی داشتند، بررسی و نهایی گردیده است. این گروه شامل کارشناسان مبارزه با پول‌شویی[2]، مؤسسه آموزشی غذای سلامت[3] و هم‌چنین مشاورانی از دفتر مواد مخدر و جرائم سازمان ملل، صندوق بین‌المللی پول[4]، بانک جهانی و یک سازمان از ایالات متحده می‌باشد.

در بند ۳-۱ این مدل، منظور از انتقال سیمی به شرح زیر می‌باشد:

انتقال سیمی شامل هر تراکنش انجام شده از طرف یک فرد ایجادکننده (حقیقی یا حقوقی) از طریق یک سازمان مالی به‌وسیله ابزار الکترونیکی با هدف انتقال میزانی از پول قابل دسترس به شخص ذینفع در سازمان مالی طرف مقابل می‌باشد. در بندهای ۷ و۲ و۲ این مدل، الزامات و تعهدات قانونی در خصوص انتقال سیمی در قالب مواد قانونی به شرح زیر بیان گردیده است:

- بخش‌ها و موسسات مالی که فعالیت‌شان شامل انتقال سیمی هستند موظف به مشخص‌سازی، بررسی، و ثبت اسم کامل، شماره حساب، و آدرس و یا در غیاب آدرس، شماره کد ملی یا تاریخ و محل تولد فرد موضوع انتقال و در صورت لزوم نام مؤسسه ایجادکننده انتقال، می‌باشند. اطلاعات باید در داخل پیام یا فرم پرداخت که همراه انتقال می‌باشد، قرار داشته باشد. در صورت نبود شماره حساب، باید شماره ارجاع منحصر به‌فرد همراه انتقال باشد.
- مؤسسات اشاره شده در ماده ۱ بایستی تمام اطلاعات ذکرشده در ماده را در زمانی که به‌عنوان واسط در یک زنجیره پرداخت عمل می‌کنند نگهداری و ارسال کنند.
- مراجع ذی‌صلاح قانونی می‌توانند قوانین مشابهی در خصوص جابه‌جایی‌ها و انتقالات مرزی متقاطع که مانند یک نقل و انتقال دسته‌ای یا انتقال محلی عمل می‌نماید، وضع نمایند.
- مواد ۱ و۲ در خصوص پرداخت‌های انجام شده ناشی از تراکنش‌ها از طریق کارت‌های اعتباری (اعتباری[5] و بدهی[6]) مشروط بر آن که شماره کارت همراه نتایج انتقال وجود داشته باشد ضرورتی ندارد. هم‌چنین در خصوص انتقالات میان موسسات مالی -۰جایی که مبدأ ایجادکننده و ذینفع در همان موسسه مالی می‌باشد - ضرورتی ندارد.
- اگر مؤسسات مرتبط در ماده ۱، انتقال سیمی دریافت کنند که شامل مشخصات کامل ایجادکننده آن نمی‌باشد، این موسسات موظفند جهت دریافت اطلاعات فراموش شده و تأیید صلاحیت آن از مؤسسه در خواست‌کننده و سفارش‌دهنده انتقال یا طرف ذینفع آن اقدام نمایند. در صورتی که موفق به دریافت اطلاعات نشود، این مؤسسات دو انتخاب در پیش رو دارند:

الف) پذیرش انتقال را رد نمایند.

ب) پذیرش انتقال را رد نمایند و همچنین به واحدهای امنیتی مالی گزارش دهند.

1- United Nations Office on Drugs and Crimes (UNODC)
2- Anti Money Laundering (AML)
3- Clean Food Training (CFT)
4- International Monetary Fund (IMF)

5- Credit Card
6- Debit Card

۳-۲- مدل قانونی پیشنهادی سازمان کاری اقدام مالی برای مبارزه با پول‌شویی در سال ۲۰۰۶[۷]

این مدل قانونی شامل ۴۰ توصیه‌نامه عمومی و ۹ توصیه‌نامه اختصاصی برای مبارزه با جرم پول‌شویی و مبارزه با بخش مالی تروریسم می‌باشد. بخش‌هایی از توصیه‌نامه دهم و توصیه‌نامه اختصاصی هفتم این مدل قانونی، به پرداخت‌های الکترونیکی پرداخته است[1].

۳-۲-۱- توصیه‌نامه دهم

مواد توصیه‌نامه دهم (نگهداری سوابق اطلاعات و انتقالات سیمی) به شرح زیر است:

- ۱-۱۰) موسسات مالی موظف به نگهداری کلیه سوابق اطلاعاتی تراکنش، اعم از محلی یا بین‌المللی برای مدت ۵ سال می‌باشند. در موارد خاص که به درخواست مراجع صلاحیت‌دار انجام می‌پذیرد، این زمان قابل تمدید می‌باشد.
  - ❑ این دستورالعمل برای کلیه موارد اعم از اینکه حساب بانکی و یا ارتباط تجاری هنوز موجود می‌باشد یا اینکه پایان یافته است، لازم‌الاجراء می‌باشد.
  - ❑ تبصره۱۰-۱-۱): سوابق تراکنش باید حاوی اطلاعات جامع باشد تا امکان بازسازی آن برای کشف فعالیت‌های غیرقانونی وجود داشته باشد.
- ۲-۱۰) مؤسسات مالی موظف به نگهداری سوابق داده‌های شناسایی، پوشه‌های حساب‌ها، و مکاتبات بازرگانی برای مدت حداقل ۵ سال، اعم از این که آن حساب یا آن مراوده بازرگانی به پایان رسیده یا نه، می‌باشند. در موارد مورد نظر مراجع ذی‌صلاح حقوقی، این زمان قابل افزایش است.
- ۳-۱۰) مؤسسات مالی باید اطمینان یابند که تمام اطلاعات مشتریان و تراکنش‌های مالی و اطلاعات‌شان در زمان مورد نیاز توسط مراجع رسمی قانونی ذیصلاح، قابل دسترس می‌باشد

۳-۲-۲- توصیه‌نامه اختصاصی هفتم

مواد توصیه‌نامه اختصاصی هفتم در خصوص کلیه انتقالات بین مؤسسات مالی محلی و یا برون‌مرزی می‌باشد. البته این توصیه‌نامه قابل ارجاع به موارد زیر نمی‌باشد:

- هر انتقالی ناشی از تراکنش‌های انجام پذیرفته توسط کارت‌های اعتباری (اعتباری و بدهی)، مادامی که شماره کارت در حین تراکنش انتقال یابد می‌باشد.
- مؤسسه مالی به موسسه مالی؛ جایی که انتقال‌دهنده و ذی‌نفع، یک موسسه مالی می‌باشد.

مواد توصیه‌نامه هفتم اختصاصی مرتبط با پرداخت الکترونیک به شرح زیر می‌باشد:

- ۱-۷) برای هر انتقال سیمی از ۱۰۰۰ (دلار/یورو) به بالا، مؤسسه مالی درخواست‌کننده باید اطلاعات زیر مربوط به ایجاد کننده انتقال سیمی را نگهداری نماید:
  - ❑ نام درخواست کننده
  - ❑ شماره حساب درخواست‌کننده (یا یک شماره منحصر به‌فرد ارجاع اگر شماره حساب موجود نباشد)
  - ❑ آدرس درخواست‌کننده (کشورها ممکن است به مؤسسات مالی اجازه دهند که آدرس را با یک کد ملی شناسایی جابه‌جا نمایند، شماره شناسایی مشتری، یا تاریخ و محل تولد)
  - ❑ برای تمام انتقال‌های سیمی ۱۰۰۰ دلار/ یورو به بالا، مؤسسات مالی دستور دهنده پرداخت باید مشخصات فرد درخواست‌کننده پرداخت را تأیید صلاحیت کنند.
- ۲-۷) برای انتقالات بین مرزی سیمی از ۱۰۰۰ دلار/یورو به بالا، مؤسسه مالی دستوردهنده پرداخت باید اطلاعات کامل درخواست‌کننده پرداخت را در پیغام یا فرم پرداخت همراه آن انتقال بگنجاند.

به هرحال اگر تعدادی از انتقالات بین مرزی انفرادی (از هزار دلار/یورو به بالا) به شکل یک پوشه بسته‌ای برای انتقال به ذی‌نفع‌ها در دیگر کشورها ایجاد شود، موسسه مالی ایجادکننده باید تنها شماره حساب درخواست‌کننده یا یک مشخصه انحصاری شناسایی را به هر کدام از انتقالات سیمی بین مرزی ملحق نماید و تنها فایل بسته انتقالات باید شامل اطلاعات کامل درخواست‌کننده انتقال باشد به‌طوری‌که قابل ره‌گیری درون کشور دریافت‌کننده باشد.

- ۳-۷) برای انتقالات داخلی (محلی)، مؤسسه مالی درخواست‌کننده باید:
  - ❑ بخش ۷-۲ را انجام دهد.
  - ❑ شماره حساب یا یک شناسه منحصر به‌فرد درخواست‌کننده را درون پیام یا فرم پرداخت قرار دهد. البته انتخاب دوم زمانی مجاز می‌باشد که اطلاعات کامل

1- Record Keeping and Wire transfer Rules

درخواست‌کننده توسط موسسه مالی طرف ذینفع و مراجع مربوطه ظرف ۳ روز کاری از دریافت درخواست برای مراجع اجرای قوانین محلی در دسترس باشد.

- ۷-۴) هر واسطه و یا هر مؤسسه مالی ذی‌نفع در زنجیره پرداخت، لازم است اطمینان از همراهی اطلاعات درخواست کننده در انتقال سیمی پیدا کند.
  - ۷-۴-۱) جایی که محدودیت‌های فنی از انتقال کامل اطلاعات در یک انتقال بی‌سیم بین مرزی، جلوگیری می‌کند، ثبت سابقه اطلاعاتی شامل تمام اطلاعات که توسط مؤسسه ایجادکننده انتقال ارایه گردیده و نیز نگهداری این اطلاعات برای مدت ۵ سال توسط موسسه مالی واسط، الزامی است.
- ۷-۵) مؤسسات مالی ذی‌نفع باید یک روش و رویه کارآمد بر مبنای خطرپذیری[1] را برای مدیریت انتقالات سیمی فاقد اطلاعات کامل درخواست‌کننده را بکار گیرند. کمبود در اطلاعات کامل مربوط به درخواست‌کننده ممکن است به‌عنوان عاملی برای مشکوک ساختن یک انتقال سیمی یا تراکنش‌های مربوط شناخته شود، که گزارش باید به مراجع ذی‌صلاح قانونی ارسال گردد. در بعضی از موارد مؤسسه مالی ذی نفع باید از ادامه ارتباط با مؤسسه مالی که از ارایه اطلاعات کامل خودداری می‌کند، اجتناب نماید.
- ۷-۶) کشورها باید مقیاس‌هایی را توسعه دهند که به شکلی کارا ناظر بر مؤسسات مالی بر مبنای قوانین و دستورالعمل‌های توصیه‌نامه مخصوص ۷-۲ باشد.
- ۷-۷) کشورها هم‌چنین باید اطمینان یابند که بخش‌های ۱۷-۱ و ۱۷-۴ از توصیه‌نامه در ارتباط با الزامات توصیه‌نامه ۷-۲ اجراء گردیده است.
- ۷-۸) کشورها ممکن است به اطلاعات کامل درخواست‌کننده حتی برای انتقالات کمتر از ۱۰۰۰ دلار/یورو نیز نیاز داشته باشند (در انتقالات ورودی به کشور).
- ۷-۹) کشورها ممکن است که به اطلاعات کامل درخواست‌کننده حتی برای انتقالات کمتر از ۱۰۰۰ دلار/یورو نیز نیاز داشته باشند (در انتقالات خروجی از کشور).

۳-۲-۳- توصیه‌نامه ۱۷-۱

کشورها باید اطمینان یابند که ابعاد کارا و مناسب مدنی یا مجوزهای اداری برای رسیدگی به اشخاص حقیقی و حقوقی مندرج در توصیه‌های سازمان گروه اقدام مالی برای مبارزه با پول‌شویی در جایی که قوانین AML/CFT ملی امکان پذیرش و رسیدگی به آن را ندارد، در دسترس می‌باشد.

۳-۲-۴- توصیه‌نامه ۱۷- ۴

محدوده مجوزهای در دسترس باید وسیع و متناسب با شرایط سخت باشد. آنها باید دارای توان اجرایی برای اعمال نفوذ کردن در مجوزهای مالی، و هم‌چنین توان پس گرفتن، مسدود کردن یا به حالت تعلیق درآوردن مجوزهای شرکت‌های مالی در مواقع لزوم را داشته باشند.

۴- ارایه پیشنهادات و راه‌کارهای اجرایی و قانونی برای مقابله با پول‌شویی الکترونیک

۴-۱- راه‌کارهای پیشنهادی به بانک‌های ارایه‌دهنده سامانه بانکداری الکترونیک [۱۰]

سامانه‌های بانکداری الکترونیکی که محصولات بانکداری را از مجاری الکترونیکی به مشتریانشان ارایه می‌دهند، از جمله تراکنش‌های دستگاه‌های خودپرداز[2]، بانکداری تلفنی[3]، بانکداری اینترنتی[4]، افتتاح حساب برخط[5] می‌باشند. به‌طور مثال کارت‌های اعتباری، حساب‌های سپرده، وام‌های رهنی، و انتقال پول که به‌صورت برخط و بدون تماس چهره به چهره، انجام می‌شود. مدیریت نیاز به شناخت این پتانسیل خطرپذیری عظیم را دارد. هم‌چنین بایستی نسبت به ارایه دستورالعمل‌ها، راه‌کارها، مراحل شناخت هویت مشتری و پایش کردن بخش‌های خاصی از بانکداری، اقدام نماید.

حساب‌هایی که بدون تماس حضوری افتتاح می‌گردند ممکن است به دلایل زیر برای جرایمی هم‌چون پول‌شویی پر خطر باشند:

- سخت بودن شناسایی هویت افراد به‌صورت کاملاً صحیح.
- مشتری ممکن است خارج از محدوده جغرافیایی و یا کشوریِ بانک باشد.
- مشتری ممکن است تراکنش‌ها را به‌صورت غیر شفاف ببیند.

1- Risk Based Procedure

2- Automated Teller Machine (ATM)
3- Telephone Banking
4- Internet Banking
5- Online Opening Account

- تراکنش‌ها به‌صورت آنی انجام می‌پذیرد.
- تراکنش‌ها ممکن است به‌وسیله شرکت سوم شخص ناشناخته انجام پذیرد.

بانک‌ها باید روش‌های نظارت دستورالعمل امنیت بانکی / مبارزه با پول‌شویی[1]، شناسایی مشتری، و سیستم‌های گزارش‌دهی عملکردهای غیر معمول را در امور بانکداری الکترونیک انجام دهند.

در سیستم‌های مدیریت اطلاعات کاربردی برای تشخیص فعالیت‌های غیرمعمول در حساب‌های با ریسک بالا می‌توان به موارد زیر اشاره نمود:

- گزارش فعالیت دستگاه‌های خودپرداز
- گزارشات انتقال پول
- گزارشات فعالیت‌های حساب‌های جدید
- گزارشات تغییر آدرس‌های اینترنتی
- گزارشات آدرس‌های IP
- گزارشات برای شناسایی حساب‌های وابسته (از جمله آدرس‌های مشترک، شماره‌های تلفن، آدرس‌های پست الکترونیک، و شماره‌ها و کدهای شناسایی مالیاتی)

برای نظارت[2] یک حساب، بانک باید شکل گشایش حساب را به‌عنوان یک عامل مد نظر قرار دهد. در صورتی‌که مشتری نیاز به گشایش حساب به‌صورت اینترنتی داشته باشد و بانک‌ها خدمات مبتنی بر اینترنت را ارایه دهند، باید یک سامانه قابل اعتماد و شناسایی هویت مشتری را به‌کار گیرند. البته در بعضی موارد لازم است از دیگر کنترل‌ها نیز استفاده نمایند، ازجمله محدود کردن حجم انتقالات پولی در مورد اقلام بزرگی که نیاز به مداخله دستی دارند.

۴-۲- راه‌کارهای پیشنهادی به کشورها برای همکاری‌های بین‌المللی [۲]

اسلحه مهم برای جنگ با پول‌شویی الکترونیکی، همکاری جهانی است، زیرا پول الکترونیکی بی‌مرز است. لذا قوانین ضد پول‌شویی و بررسی‌ها و روش‌های مؤثر تنها بستگی به ارتباط در این زنجیره بین‌المللی دارد. این ارتباطات در قالب‌های زیر مشهود است:

- اقدامات محلی[3]
- اطمینان از اینکه سازوکار همکاری‌های قانونی شامل باورها در شرایطی هستند که می‌توانند محصولاتی از سوابق اطلاعاتی به‌وسیله مؤسسات مالی در سطح بین‌المللی ایجاد کنند.
- ایجاد و فعال کردن قوانین اجرایی برای شناسایی، جلوگیری، و یا اجرای روش‌های تنبیهی و بازدارنده ارایه شده در کمیسیون جرایم مالی در سطح بین‌المللی.
- کارآمدسازی روش‌های شناسایی و ثبت سوابق اطلاعاتی و همکاری بین‌المللی در جهت نیل به این هدف.
- فعال سازی دستورالعمل‌های حقوقی که مسئولیت‌های اعمال مجرمانه را برای اجزاء مختلف در شرکت‌ها تبیین نماید.

■ **آموزش**[4]

- ❑ پیاده‌سازی برنامه‌های آموزشی بین‌المللی در جهت کمک‌رسانی به کشورهای همکار برای اجرای برنامه‌های پیشگیرانه فعال در مقابل جرایم مالی.
- ❑ اجرای برنامه‌های آموزشی متناسب در داخل صنایع مالی برای مشخص‌سازی نقاط ضعف منظم و اجرای راه‌کارها
- ❑ اجرای برنامه‌های آموزشی برای سازمان‌های مالی قانونی و بازرسان آنها برای ایجاد رشد در توانمندی‌های آنها در کشف جرایم مالی.

■ **ثبت و اشتراک اطلاعات**[5]

- ❑ فعال‌سازی بخشی در پلیس بین‌الملل[6] برای راه‌اندازی امور مربوط به جرایم مالی و پول‌شویی.
- ❑ بررسی سازوکارهای همکاری حقوقی برای درک و فهم اینکه در کجا و چگونه نیازمندی‌های بیشتری برای مبارزه با جرایم مالی وجود دارد.
- ❑ تبلیغ و هدایت سازمان‌های بین‌المللی چند منظوره برای جستجوی جرایم مالی.
- ❑ فعال‌سازی سازمان‌های مالی برای نگهداری اطلاعات. تراکنش‌های مالی داخلی و بین‌المللی برای مدت پنج سال.

■ **قوانین امنیتی**[7]

مطالعه مجدد قوانین امنیتی برای اطلاع از نیازمندی‌های قانون‌گذاری و آیین‌نامه‌ها و مقررات برای مشخص‌سازی

1- Bank Secrecy Act / Anti Money Laundering (AML)
2- Monitoring
3- Domestic Measures
4- Training and Education
5- Information Sharing and Retention
6- Interpol
7- Secrecy Law

این‌که سوابق مؤسسات مالی و دیگر اطلاعات وابسته چگونه بین مؤسسات حقوقی و قانونی بین دولت‌ها مبادله شوند.

۴-۳- کشف پول‌شویی و فساد مالی با بهره‌گیری از روش‌های داده‌کاوی[1]

داده‌کاوی، یکی از عناوین پرطرفدار در فن‌آوری اطلاعات است. امروزه اکثر سازمان‌ها از لحاظ حجم داده‌ها بسیار غنی می‌باشند، چرا که آنها به جمع‌آوری روز افزون داده‌ها مشغولند. عموماً سازمان‌ها از این انبوه داده‌ها برای ارائه اعداد و واقعیت‌ها استفاده می‌کنند؛ اما این اعداد و واقعیت‌ها نمایشگر دانش نیستند و حتی می‌توان اذعان داشت که امروزه سازمان‌ها با فقر دانش روبرو هستند. تعریف ما از داده‌کاوی فرآیند استخراج دانش از داده‌ها می‌باشد. این امر از طریق کشف الگوها در داده‌های مربوط به رفتار گذشته فرآیندها امکان‌پذیر است.

داده‌کاوی، استخراج اطلاعات پیش‌گویانه پنهان از پایگاه‌های داده بزرگ و یک فن‌آوری جدید قدرتمند با توان زیاد برای کمک به شرکت‌هاست تا برروی اطلاعات مهم موجود در انبار داده‌های خود تمرکز کنند. ابزارهای داده‌کاوی، رفتارها و روندهای آینده را پیش‌گویی می‌کنند و بدین ترتیب به شرکت‌ها اجازه می‌دهند که بر پایه دانش و پیش‌گویی‌ها تصمیم‌گیری کنند. ابزارهای داده‌کاوی سوالاتی را می‌توانند جواب دهند که در گذشته زمان زیادی برای جوابگویی آنها لازم بود. امروزه از این تکنیک در بخش‌های مالی اعم از بانکی و غیر بانکی و مؤسسات حسابرسی برای کشف رفتارهای مشکوک به جرایم مالی از جمله پول‌شویی استفاده می‌گردد.

۵- نتیجه‌گیری

کشورهای کوچک با اقتصاد ضعیف، مکان مناسبی برای سازمان‌های پول‌شویی می‌باشند. چرا که با توان اقتصادی بالایی که سازمان های پول‌شویی به‌دست آورده‌اند می‌توانند اقتصاد اینگونه از کشورها را تحت اختیار قرار دهند. در کشورهایی با قوانین ناکارآمد در این زمینه، و یا با شرایطی که امکان اجرای قوانین در آنها وجود نداشته باشد، فضای خوبی برای اعمال تبهکارانه پول‌شویی و بالاخص پول‌شویی الکترونیکی به‌وجود می‌آید، که بتوانند به دلیل کمبود و خلاء ناشی از قوانین، منافع حاصل از درآمدهای غیرمشروعشان را حفظ نمایند.

امروزه در کشورمان در حوزه بانکداری تلاش‌های بسیاری برای بهره‌گیری از فن‌آوری‌های نوین انجام پذیرفته است. هر روز عناوین جدیدی از این نوع خدمات مورد توصیه قرار می‌گیرد. ولی متأسفانه اقدامات جدی در خصوص پیش‌گیری از جرایم مالی الکترونیکی از جمله پول‌شویی انجام نپذیرفته است.

مطالب یاد شده وضع قوانین و عملکردهای قانونی، پیگیری‌ها، مباحثات، روش های اجرایی، و بحث مهم هماهنگی و همکاری بین‌المللی جهت جلوگیری، شناسایی، و آشکارسازی پول‌شویی الکترونیکی را ضروری می‌کند.

در اقتصاد ایران تاکنون به‌دلیل ناشناخته ماندن پیامدها و آثار زیانبار پول‌شویی و بالاخص پول‌شویی الکترونیکی، اقدام قابل توجهی صورت نگرفته است. تنها اقدام مثبت در این زمینه، لایحه منع پول‌شویی تقدیمی دولت به مجلس شورای اسلامی است که مراحل بررسی مقدماتی آن انجام شده است.

جهت‌گیری قانون مبارزه با پول‌شویی و آئین‌نامه‌های اجرایی آن باید طوری باشد که راه‌های مصرف و نقل و انتقال وجوه حاصل از قاچاق و سایر فعالیت‌های مجرمانه را محدود و قابل شناسایی کند. از این رو وظیفه اصلی قوه مقننه تصویب قوانین و ابزارهای حقوقی لازم برای مراجع مسئول مبارزه با پول‌شویی است.

اولین قدم در این راه، «جرم» اعلام کردن پول‌شویی است. یعنی مجلس با تصویب قانونی باید به مراکز قضایی و انتظامی، اختیار مجازات پول‌شویان و مصادره دارائی های حاصل از ارتکاب جرم پول‌شویی را بدهد. هم‌چنین باید چارچوبی تدوین شود که طبق آن، مراکز مسئول مبارزه با پول‌شویی بتوانند اطلاعات به‌دست آمده را بین خود و همتایان خارجی مبادله کنند.

به نظر می‌رسد کم توجهی به این جرم در نهادهای قانونی و بازرسی کشور نه تنها می‌تواند صدمات جبران ناپذیری از این ناحیه به بدنه اقتصادی کشور وارد کند، بلکه می‌تواند شرایط را جهت انجام دیگر جرائم الکترونیکی در حوزه‌های مختلف در بازارهای پولی و سرمایه‌ای کشور، مهیا نماید.

1- Data Mining

مراجع

1. Camdesos, The Past Manager of IMF , Money Laundering in Cyberspace, The World Bank – Financial Sector Working Paper, Nov. (**2004**).
2. Electronic Money Laundering-An Environmental Scan, Department of Justice Canada, Solicitor General Canada, Oct. (**1998**).
3. Model Legislation on Money Laundering and Financing of Terrorism, UNITED NATIONS – Office on Drugs and Crime, Dec. (**2005**).
4. Financial Action Task Force(FATF) Site
5. Porteous 1998, Electronic Money Laundering-An Environmental Scan, Department of Justice Canada, Solicitor General Canada, Oct. (**1998**).
6. Money Laundering in Cyberspace, The World Bank – Financial Sector Working Paper, Nov. (**2004**).
7. AML/CFT Evaluation and Assessments, Handbook for Countries and Assessors, FATF. GAFI, June (**2006**).
8. Mutual Evaluation/Detailed Assessment Report, Anti Money Laundering and Combating the Financing of Terrorism, Ministerial Final, CFATF . GAFIC, Oct. (**2006**).
9. APG Yearly Typologies Report 2005-2006, The Asia / Pacific Group on Money Laundering
10. Bank Secrecy Act / Anti Money Laundering Examination Manual, Federal Financial Institutions Examination Council , (**2007**)
11. The Vienna Convention: The 1988 UN Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances UNDOCS. E/Conf. 82/IS And E/Conf. 82/14, Dec. 19. (**1988**).
12. The FATF Report: The Report of The Financial Action Task Force (FATF) on Money Laundering, April 19, (**1990**).

۱۳. اباذری, پردازشگر, شماره ۹, سال دوم

۱۴. انتقال الکترونیکی وجوه و بانکداری الکترونیکی در ایران،معاونت برنامه‌ریزی وبررسی‌های اقتصادی وزارت بازرگانی، (**۱۳۸۳**).

۱۵. بهرامزاده، حسینعلی و شریعتی، حسین، روشهای مبارزه با پول‌شویی، ماهنامه تدبیر، شماره ۱۵۱، (**۱۳۸۵**).

۱۶. مجله علمی - پژوهشی مجلس شورای اسلامی - شماره ۳۷ سال دهم بهار (**۱۳۸۲**).

۱۷. روزنامه سرمایه، ۸۶/۰۵/۲۸

۱۸. طرح مطالعاتی مبارزه با جرم پول‌شویی، مرکز پژوهشهای مجلس شورای اسلامی، تیرماه ، مرداد، و شهریور ماه (۱۳۸۲).

۱۹. جلیلی و آبادی, ص‌ص ۷۷ـ۴۱، (**۱۳۷۹**).

Money Laundering, Technical and International Ways of Defense Against it

Mohammad Reza Davari[1]

Madjid Davari[1]

Abstract

With the inception of science and technology revolution, especially information, communications, electronic and computer technology in the recent years, the fourth generation wars have been designed and experienced in recent wars as well and continue their evolutionary routes. One of the most significant aims of information and communications-based wars is the financial and banking markets of countries which are waged to destroy and corrupt economic markets of these countries. Within the past three decades, a new definition of crime has appeared in the economic affairs which due to its highly destructive dimensions in the national and international levels have attracted the attention of economic, political , legal systems of countries and international organizations and this crime is nothing but money laundering. Money laundering or money cleansing is a criminal activity in a large scale, group, continuous and long term which can go beyond the political boundaries of a hypothetical country. Money laundering has harmful effects on economy, society and politics, corruption and instability of economy, weakening private sector and privatization plans, reduction of government control on economic policies, corruption of government systems, public mistrust, discredit of governments and state economic organizations, development of criminal business, government and medical care costs upheaval, reduction of government tax revenues, instability and lack of sustainability in the world market, damaging global efforts to establish free and competitive markets and disruption in the economic growth and so on, are only parts of these effects.

In the recent years, the financial systems have taken advantage of a new form of performance called electronic model. Criminals misuse the economy and its globalization and advances derived from information and communications to conceal their illegitimate income. They use plenty of techniques including swift money transfer from one country to other countries or companies and corporate cooperation in order to clean inappropriate sources. On the other hand, due to its destructive nature, Mafia-like powers and governments attempt to take advantage of this method as a passive defense attack in order to disintegrate the economic systems of other countries and therefore their political systems. Therefore recognizing this new phenomenon and the appropriate legal and technical methods to prevent it is consistent with achieving the passive defense which is an undeniable necessity these days.

Key Words: *Money Laundering, Electronic Money Laundering, Electronic Payment Systems, e-Money, Electronic Banking, Wire Transfer*

1- M. S in It Engineering, E-Commerce