Prevention of E-Money Laundering: Defensive Approach and Offensive Approach

Shahyar Abdillahi Ghahfarokh[i] Batol Pakzad*[2] Hassan Alipour[3] Mohammadreza Elahimanesh[4]

1. Ph. D. Student in Criminal Law and Criminology, Faculty of Humanities, North Tehran Branch, Islamic Azad University, Tehran, Iran.
Email: sabdolahigh@yahoo.com
2. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Humanities, North Tehran Branch, Islamic Azad University, Tehran, Iran.
*. **Corresponding Author:** Email: b_pakzad@iau-tnb.ac.ir
3. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Farabi Campus, University of Tehran, Tehran, Iran.
Email: hassan.alipour@ut.ac.ir
4. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Humanities, North Tehran Branch, Islamic Azad University, Tehran, Iran.
Email: m.elahimanesh92@yahoo.com

S.D.I.L.
The SD Institute of Law Research & Study

Publisher:
Shahr-e- Danesh Research And Study Institute of Law

Article Type:
Original Research

DOI:
10.22034/JCLC.2021.290298.1510

Received:
17 June 2021

Accepted:
13 October 2021

Published:
19 February 2022

ABSTRACT

Prevention of e-money laundering has a defensive aspect from two perspectives. One of the perspectives of the crime scene is cyberspace, which, with protecting the subject of crime takes precedence over preventing the occurrence of crime, and preventive measures are in the position of protecting computer values so that the perpetrator does not touch them. Unlike crime prevention in the traditional or physical space, the authority to act is in the hands of the perpetrators, but in cyberspace, the perpetrator is in the hands of the perpetrators, and the perpetrator is more of a guard than an opportunity to commit a crime. The second is from the perspective of electronic financial exchanges, which are based on features such as speed, mass and spatial diversity in practice, out of reach of

preventive measures. What will be an open environment for mastering and creating controlling software measures is only the limited financial institutions, but this mastery in exchanges is minimized. In this regard, the prevention officer inevitably resorts to a defensive approach in crime prevention.
This article, based on library and Internet resources and in a descriptive and analytical manner, tries to examine the challenges and strategies to prevent e-money laundering from the point of view of defensive and offensive measures. The approach is based on the defense approach in the prevention of e-money laundering, according to which the values of cyberspace on the one hand and the effectiveness of preventive measures in cyberspace on the other require financial exchanges in cyberspace in terms of origin. And control the origin and the direction of the exchange path.

Keywords: e-money laundering, crime prevention, confidentiality, defense approach, value protection.

Excerpted from the dissertation entitled "Prevention of Electronic Money Laundering in Iran with a Look at International Documents", Islamic Azad University - North Tehran Branch, Faculty of Humanities.

Funding: The author(s) received no financial support (funding, grants, sponsorship) for the research, authorship, and/or publication of this article.

Acknowledgements:

The authors would like to thank the esteemed professors, especially Professor Hassan Alipour,for their cooperation in preparing and writing this research.

Author Contributions:

Shahyar Abdollahi Ghahfarokhi: Conceptualization, Methodology, Validation, analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Writing - Review & Editing, Supervision, Project administration.

Batol Pakzad: Conceptualization, Methodology, Validation, analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Writing - Review & Editing, Supervision, Project administration.

Hassan Alipour: Conceptualization, Methodology, Validation, analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Writing - Review & Editing, upervision, Project administration.

Mohammadreza Elahimanesh: Methodology, analysis, Resources, Data Curation, Supervision.

Competing interests: The authors declare that they have no competing interests.

Citation:
Abdillahi Ghahfarokhi, Shahyar, Batol Pakzad, Hassan Alipour & Mohammadreza Elahimanesh "Prevention of E-Money Laundering: Defensive Approach and Offensive Approach" Journal of Criminal Law and Criminology 9, no. 18 (February 19, 2022): 385-406.

Extended Abstract

Prevention of electronic money laundering is an undeniable necessity to control this phenomenon, in particular the priori control of this phenomenon has priority in all respects over its a posteriori and judicial control. This necessity is justified by understanding a preventive triangle. On the one hand, there is committing money laundering, for which most of the criminal measures are proposed. These measures are not effective in eliminating the phenomenon of money laundering, and the perpetrators, who indicate the existence of high criminal talent and capacity, indicate that calculation plays a key role in money laundering. Calculation and foresight in money laundering make the perpetrator-centered preventive measures practically ineffective. The second side is money laundering behavior. Money laundering is not a primitive crime and its existence depends on the origin of crime. The usual precautionary measures for public crimes cannot be used. As long as the crimes of origin are committed, money laundering also lasts, and if measures are needed to prevent money laundering, in fact, they should be applied to crimes of origin, otherwise money laundering alone will not be curbed. The third side is the context of money laundering. Preventing context-based is the most effective way to deal with money laundering. Since the main context of money laundering is financial and economic institutions, it is possible to find measures to this context. Cyber or electronic environment is used as a space for money laundering. Poster-centric preventive measures will not be just physical space and will be associated with important challenges, the most important of which are the collective and intervening aspects of crime prevention that take their place is given to a defensive and passive aspect.

The prevention of E-money laundering has a defensive aspect from two perspectives. One of the perspectives of the crime scene is cyberspace, where the protection of the subject of crime takes precedence over the prevention of crime, and preventive measures are in the position of protecting computer values so that the perpetrator does not reach them. Unlike traditional crime prevention, the authority to act is in the hands of the perpetrators, but in cyberspace the perpetrators are in the hands of the perpetrators, and the perpetrator is more on guard than to disrupt the opportunity to commit a crime. Because speed, density and spatial diversity in practice are out of reach of preventive measures. The environment for creating controlling software measures is the environment for financial institutions, but this dominance in financial transactions is minimized. In this regard, the prevention officer inevitably resorts to a defensive approach in crime prevention.

Defensive face of anti-money laundering approach is applicable due to the incompatibility of the crime environment with the powers of the crime prevention officer or measures. In fact, the restriction of the application of preventive measures in field, which is very widespread for money laundering, leads to an inefficiency, and the only main measure to eliminate such a situation is the expansion of the application of preventive measures in the form of global crime prevention. Accordingly, countries such as Iran, which are not in the process of globalization, are more unsuccessful in preventing money laundering. Based on library resources this article tries to describe and analyze the challenges and preventive measures of E-money laundering in aspects of defense and offensive approach.

Measures to prevent e-money laundering that take place in a global context are international in nature and are generally a global anti-money laundering enterprise with a focus on the Financial Action Task Force. As a result, Iran cannot act alone in the fight against money laundering without international cooperation. That is why it must be said that the fight against money laundering in Iran is a wonderful and sad story that ignores both the principle of confidentiality and the principle of transparency to the altar. Ignoring the principle of confidentiality in this regard, the Anti-Money Laundering Law is essentially a burden to control and access financial and banking information, and sacrificing the principle of transparency because Iran does not accept international cooperation in the fight against money laundering and in Its corrupt bed seeks to combat money laundering. A struggle that leads to corruption itself.

The main strategy of this paper is to emphasize the safeguard approach to the protection of financial data and electronic financial transactions. However, this protectionist approach does not really meet the goals of prevention, and the path to preventive measures should be taken and paved in the face of the globalization of e-money laundering prevention, especially where cryptocurrencies are used or in-depth money laundering. New rules for the prevention of e-money laundering must be established, for a phenomenon that occurs in a global context with distinctive features requires global measures to address it. In fact, the achievement of this article is to emphasize the balance between these two approaches, so that the principle is on the defensive approach in the prevention of electronic money laundering, according to which the values of cyberspace on the one hand and the effectiveness of preventive measures in cyberspace to monitor financial transactions in cyberspace in terms of origin, control and exchange path on the other.

پیشگیری از پول‌شویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی

شهیار عبدالهی قهفرخی[۱] بتول پاکزاد*[۲] حسن عالی‌پور[۳] محمدرضا الهی‌منش[۴]

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشکده علوم انسانی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.
Email: sabdolahigh@yahoo.com

۲. استادیار، گروه حقوق جزا و جرم‌شناسی، دانشکده علوم انسانی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.
*: نویسنده مسؤول: Email: b_pakzad@iau-tnb.ac.ir

۳. استادیار، گروه جزا و جرم‌شناسی، دانشکده پردیس فارابی، دانشگاه تهران، تهران، ایران.
Email: hassan.alipour@ut.ac.ir

۴. استادیار، گروه حقوق جزا و جرم‌شناسی، دانشکده علوم انسانی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.
Email: m.elahimanesh92@yahoo.com

چکیده:

پیشگیری از پول‌شویی الکترونیکی از دو منظر، جنبه دفاعی دارد. یکی از منظر بستر ارتکاب جرم یعنی فضای سایبر که صیانت از موضوع جرم نسبت به پیشگیری از جرم اولویت دارد و تدابیر پیشگیرانه در مقام حفاظت از ارزش‌های رایانه‌ای‌اند تا دست مرتکب به آنها نرسد. برخلاف پیشگیری از جرم در فضای سنتی، اختیار عمل در دست متصدیان پیشگیری است ولی در فضای سایبر، اختیار عمل در دست مرتکبان است و متصدی پیشگیری بیشتر نگهبانی می‌کند تا برهم زدن فرصت ارتکاب جرم. دوم از منظر مبادلات مالی الکترونیکی که بر پایه ویژگی‌هایی چون سرعت، انبوهی و تنوع مکانی در عمل از دسترس تدابیر پیشگیرانه به دور است. محیط ایجاد تدابیر نرم‌افزاری کنترل‌کننده، محیط نهادهای مالی است ولی این تسلط در مبادلات مالی به حداقل می‌رسد. دراین‌راستا، متصدی پیشگیری ناگزیر به رویکرد دفاعی در پیشگیری از جرم متوسل می‌شود.

پژوهشکدهٔ حقوق

نوع مقاله:
پژوهشی

DOI:
10.22034/JCLC.2021.290298.1510

تاریخ دریافت:
۲۷ خرداد ۱۴۰۰

تاریخ پذیرش:
۲۱ مهر ۱۴۰۰

تاریخ انتشار:
۳۰ بهمن ۱۴۰۰

این مقاله بر اساس منابع کتابخانه‌ای به شیوه توصیف و تحلیل می‌کوشد تا چالش‌ها و راهکارهای پیشگیری از پول‌شویی الکترونیکی را از زاویه دفاعی بودن تدابیر و هجومی بودن آنها بررسی کند و دستاورد نوشتار تأکید بر ایجاد توازن میان این دو رویکرد است به‌گونه‌ای که اصل بر رویکرد دفاعی در پیشگیری از پول‌شویی الکترونیکی است که بر اساس آن، ارزش‌های فضای سایبر از یک‌سو و کارآمدی تدابیر پیشگیرانه در فضای سایبر از سوی دیگر اقتضا می‌کند تا مبادلات مالی در فضای سایبر از جهت منشأ، کنترل و از جهت مسیر تبادل، دیده‌بانی شود.

کلیدواژه‌ها:
پول‌شویی الکترونیکی، پیشگیری از جرم، حق محرمانگی، رویکرد دفاعی، صیانت از ارزش.

برگرفته از پایان‌نامه با عنوان « پیشگیری از پولشویی الکترونیکی در ایران با نگاه به اسناد بین المللی»، دانشگاه آزاد اسلامی– واحد تهران شمال، دانشکده علوم انسانی.

حامی مالی:
این مقاله هیچ حامی مالی ندارد.

سپاسگزاری و قدردانی:
بدین وسیله از اساتید ارجمند به ویژه استاد حسن عالی پور، بابت همکاری در تهیه و نگارش این پژوهش سپاسگزاری می‌شود.

مشارکت نویسندگان:
شهیار عبدالهی قهفرخی: مفهوم سازی، روش شناسی، اعتبار سنجی، تحلیل، تحقیق و بررسی، منابع، نظارت بر داده‌ها، نوشتن – پیش‌نویس اصلی، نوشتن – بررسی و ویرایش، نظارت، مدیریت پروژه.
بتول پاکزاد: مفهوم‌سازی، روش شناسی، اعتبار سنجی، تحلیل، تحقیق و بررسی، منابع، نظارت بر داده‌ها، نوشتن – پیش‌نویس اصلی، نوشتن – بررسی و ویرایش، نظارت، مدیریت پروژه.
حسن عالی پور: مفهوم‌سازی، روش‌شناسی، اعتبار سنجی، تحلیل، تحقیق و بررسی، منابع ، نظارت بر داده‌ها، نوشتن – پیش‌نویس اصلی، نوشتن – بررسی و ویرایش، نظارت، مدیریت پروژه.
محمدرضا الهی منش: روش‌شناسی، تحلیل، منابع، نظارت بر داده‌ها، نظارت.

تعارض منافع:
بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

استناددهی:
عبدالهی قهفرخی، شهریار، بتول پاکزاد، حسن عالی‌پور و محمدرضا الهی‌منش «پیشگیری از پول‌شویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی». *مجله پژوهش‌های حقوق جزا و جرم‌شناسی* ۹، ش. ۱۸ (۳۰ بهمن، ۱۴۰۰): ۳۸۵–۴۰۶.

مقدمه

پیشگیری از پول‌شویی الکترونیکی ضرورتی غیرقابل‌انکار در میان همه تدابیر رویارویی با پدیده پول‌شویی است. این ضرورت از جهت درک یک مثلث پیشگیرانه توجیه می‌شود. در یک ضلع، مرتکب پول‌شویی قرار می‌گیرد که در قبال آن بیشتر تدابیر کیفری مطرح می‌شود. این تدابیر برای از میان برداشتن پدیده پول‌شویی کارایی ندارند و ویژگی‌های مرتکب که حاکی از وجود استعداد و ظرفیت جنایی بالاست، بیانگر این است که محاسبه در پول‌شویی حرف نخست را می‌زند. محاسبه و دوراندیشی در پول‌شویی سبب می‌شود تا عملاً تدابیر پیشگیرانه مرتکب‌محور، کارایی نداشته باشند. ضلع دوم، رفتار پول‌شویی است. پول‌شویی یک جرم ابتدایی و اصیل نیست و موجودیتش وابسته به جرم منشأ است؛ بنابراین در قبال این جرم نمی‌توان از تدابیر پیشگیرانه معمول برای جرایم عمومی استفاده کرد. تا زمانی که جرایم منشأ ارتکاب می‌یابند، پول‌شویی نیز دوام می‌یابد و اگر تدابیری برای پیشگیری از پول‌شویی لازم آید در واقع باید برای جرایم منشأ اعمال شود وگرنه پول‌شویی به‌تنهایی با تدابیر پیشگیرانه مهار نمی‌شود. ضلع سوم، بستر انجام پول‌شویی است. پیشگیری بسترمحور تأثیرگذارترین شیوه رویارویی با پول‌شویی است. ازآنجاکه بستر اصلی تحقق پول‌شویی نهادهای مالی و اقتصادی یا فعالیت‌های تجاری است، می‌توان متناسب با این بستر، تدابیری را در نظر گرفت ولی هنگامی‌که فضای سایبر یا محیط الکترونیکی به‌عنوان فضای انجام پول‌شویی قرار می‌گیرد، تدابیر پیشگیرانه بسترمحور به‌سادگی فضای فیزیکی نخواهد بود.

چالش‌های پیشگیری از پول‌شویی الکترونیکی می‌تواند هم رویارو با ذات و هدف پیشگیری از جرم باشد و هم نسبت به کارکرد آن. علت ظهور این چالش تابعی از سه عامل است: اقتضای محرمانگی، اقتضای زمانی و مکانی فضای سایبر و میزان همکاری‌های بین‌المللی در کنترل فضای سایبر. چالش پیشگیری از پول‌شویی الکترونیکی فقط درخصوص ویژگی‌های فضای سایبر از منظر ویژگی‌های مرتبط با داده‌ها و سامانه‌ها که محرمانگی و اقتضائات زمانی و مکانی ازجمله مهم‌ترین آنها به شمار می‌روند، نیست بلکه خودِ شیوه‌های رویارویی با پول‌شویی الکترونیکی نیز حکایت از مسئله مهم‌تری دارد. این مسئله درباره گزینش رویکرد دفاعی یا رویکرد هجومی در پیشگیری از پول‌شویی الکترونیکی است. از یک‌سو، رویکرد دفاعی متناسب با ویژگی‌های فضای سایبر، توجیه‌پذیر است و متصدی را در مقام دفاع از ارزش‌ها و موضوعات موردِحمایت قرار می‌دهد. در این رویکرد، متصدی پیشگیری یا نرم‌افزارهای پیشگیرانه که نام آنها را پیشگیری وضعی در فضای سایبر می‌گذاریم، در مقام بر هم زدن فرصت ارتکاب جرم در یک محیط لایتناهی نیستند، بلکه در اصل در مقام صیانت از موضوع یا همان امنیت تبادل پول مشروع و قانونی‌اند؛ یعنی به‌جای زدودن جرم، حمایت از موضوع جرم در اولویت قرار می‌گیرد. از سوی دیگر، رویکرد هجومی اقتضای یک پیشگیری واقعی از جرم خواهد بود. فضای سایبر همانند فضای سنتی نباید محیطی امن برای مرتکبان باقی بگذارد و باید تدابیر پیشگیرانه با حضور در همه فضاها و محیط‌های سایبری، هر جا که زمینه انجام بزه را ببینند، فرصت ارتکاب آن را بر هم بزنند؛ اما در اینکه چنین رویکردی می‌تواند

Abdillahi Ghahfarokhi, Shahyar, Batol Pakzad, Hassan Alipour & Mohammadreza Elahimanesh “Prevention of e-money laundering: Defensive approach ...” Journal of Criminal Law and Criminology. 9, no. 18 (February 19, 2022): 385-406.

هم‌زمان با پاس داشتن محرمانگی، خلوت و دیگر ارزش‌های فضای سایبر باشد، تردید جدی وجود دارد که این نوشتار در مقام بررسی آن خواهد بود.

این نوشتار در صدد بررسی جدال یا تعارض رویکرد دفاعی و رویکرد هجومی در پیشگیری از پول‌شویی الکترونیکی است و دراین‌راستا ابتدا به بایسته‌های بستر پیشگیری از پول‌شویی الکترونیکی اشاره می‌کند و سپس در جستار اصلی به نسبت این دو اشاره خواهد کرد.

۱- بایسته‌های بستر پیشگیری از پول‌شویی الکترونیکی

محیط الکترونیکی در اولین شاخصه خود در پی عرض‌اندام در برابر محیط فیزیکی است که دو مشخصه اصلی دارد؛ اول آنکه کاشف یا آفرینش‌گر و درنتیجه کنترل‌گر آن انسان است و دوم اینکه محیطی است مبتنی‌بر مبادله اطلاعات؛ بنابراین چنین محیطی قابلِ‌مقایسه با محیط طبیعی نیست تا بتوان از قواعدش بهره گرفت. ازاین‌رو، پیشگیری از وقوع پول‌شویی الکترونیکی در اولین گام خود؛ با این چالش روبه‌روست که تدابیر پیشگیری از جرم در فضای بیرونیِ ممکن است متناسب فضای الکترونیکی نباشد. تفاوت محیط الکترونیکی با فضای بیرونی عموماً حول محور گستره مکانی، سرعت و وسعت مبادلات اطلاعاتی و ویژگی برجسته گمنامی است.

محیط الکترونیکی را اگر با جهانی محدود به کره زمین بسنجیم از دو زاویه، گستره مکانی بیشتری دارد: نخست اینکه محیط الکترونیکی چهره‌ای جهانی و حتی فراجهانی یافته است، دوم اینکه عمقی به نظر ناشناخته‌تر از جهان را دارد به‌گونه‌ای که محیط عمیق وب، می‌تواند با اعماق زمین مقایسه شود. همین مقایسه که بیشتر جنبه داستان‌پردازانه می‌نماید ولی پرده از سه چالش اساسی در زمینهٔ پیشگیری از پول‌شویی را برمی‌دارد:

نخست اینکه محیط الکترونیکی محیطی جهانی شده و فراتر از مرزهاست درحالی‌که تدابیر پیشگیرانه عموماً چهره ملی دارند و تا با پشتوانه همکاری‌های دوجانبه و چندجانبه همراه نشوند؛ تأثیری در فراسوی مرزها ندارند؛

دوم اینکه محیط الکترونیکی در جایی که محوریت با تارنماهای قابلِ‌مشاهده باشد؛ قابلِ‌کنترل و پیشگیری است ولی سطح عمیق یا تاریک فضای سایبر، فضایی بدون کنترل است که دور از دسترس تدابیر پیشگیرانه می‌نماید؛

سوم اینکه اگر در فضای طبیعی، ایستایی و پویایی در کنار هم‌اند ولی فضای الکترونیکی بر پویایی صرف استوار است و گستره مکانی در فضای الکترونیکی بر پایه جابه‌جایی داده درحال بزرگ‌تر شدن است.

محیط الکترونیکی سپهری ذاتاً فردگراست و نمی‌توان برای آن چهره جمعی در نظر گرفت. دلیل این امر ویژگی ذاتی فضای سایبر از یک‌سو و اقتضائات زیست‌جمعی از سوی دیگر است. ازاین‌رو، محیط الکترونیکی می‌تواند بخشی از تدابیر پیشگیرانه موسوم به تدابیر اجتماعی را که چهره همگانی دارد را به چالش بکشد. از سوی دیگر فردیت فضای الکترونیک و اولویت حریم خصوصی در این محیط به چالشی مهم‌تر برای تدابیر پیشگیرانه از پول‌شویی الکترونیکی به نام گمنامی منتهی می‌شود.

گمنامی یا ناشناس ماندن کاربران در فضای سایبر تلاشی افراطی برای حفظ حریم خصوصی است ولی به همان اندازه می‌تواند در ناکامی تدابیر پیشگیرانه نیز مؤثر باشد. سپس ویژگی‌های پیش‌گفته به ارتکاب جرایمی منتهی می‌شود که در پس پرده رخ می‌دهند و دیگر از مفهوم جرایم مشهود یا علنی نمی‌توان سراغ گرفت که بر اساس آنها بتوان تدابیر پیشگیرانه را ملاک قرار داد.

کوشش برای حفظ محرمانگی داده‌های مالی و بانکی تنها دغدغه مشتریان نهادهای مالی نیست بلکه خود نهادهای مالی نیز برای رعایت امانت، برای تأمین خواسته مشتریان در تلاش‌اند. این تلاش دو جانبه به‌طور قوی می‌تواند همکاری نهادهای مالی و خود مشتریان با متصدیان پیشگیری از پول‌شویی الکترونیکی تحت تأثیر قرار دهد. حتی خود دولت‌ها نیز خود را پایبند رازداری بانکی می‌دانند. ازاین‌رو گفته می‌شود «برای پول‌شو، خدمات بانکی اهمیت بیشتری دارد تا مبلغی که در بانک دارد. بانک الزامی به پرداخت سود با نرخ بالا به پول‌شو را ندارد. نقش مقررات رازداری بانکی در پول‌شویی به‌طور پیوسته موردِتوجه قرار می‌گیرد ولی مهم‌تر از آن شناسایی صاحبان سودهای بانکی است.»[1]

هر چند با قدرت‌گیری نهادهای بین‌المللی و دستگاه قضایی و پلیسی داخلی در مبارزه با پول‌شویی، رازداری بانکی همانند گذشته برجستگی و اهمیت ندارد ولی حتی در جایی که نهادهای مالی و بانکی در میانه رازداری بانکی و جلب نظر مشتریان از یک‌سو و همکاری با نهادهای پیشگیری و پیگیری از جرم قرار دارند؛ این وضعیت خود می‌تواند به چالشی برای پیشگیری از پول‌شویی الکترونیکی باشد؛ زیرا این وضعیت، در درجه نخست برای نهادهای مالی حق یا موقعیت انتخاب میان مشتری و دستگاه قضایی و پلیسی را ایجاد می‌کند که چنین موقعیتی می‌تواند تردیدهایی را برای همکاری واقعی نهادهای مالی و بانکی با دستگاه قضایی و پلیسی ایجاد کند. علت اصلی این تردید همانا نگرش بانک‌ها به میزان سرزنش‌پذیری پول‌شویی الکترونیکی است. بانک‌ها و نهادهای مالی پول‌شویی را پدیده‌ای غیرقابل‌مقایسه به پدیده‌های چون سرقت مسلحانه از بانک یا اختلاس می‌دانند و همین نگرش می‌تواند بانک‌ها را با پدیده‌ای رویارو کند که چندان سرزنش‌پذیر نیست.

جایگاه درونی، ملی و فردی رازداری یا محرمانگی در برابر جایگاه بیرونی، فراملی و جمعی شفافیت، پیوند این دو را به خوبی نشان می‌دهد: پیوندی حاکی از تعارض و ستیز. در قبال مبارزه با پول‌شویی این پیوند بسی آشکارتر می‌شود؛ زیرا دست کم در دو دهه اخیر، نخستین و مهم‌ترین مرجع مبارزه با این پدیده، گروه ویژه اقدام مالی است که با نگرش جهانی به اقتصاد، می‌کوشد تا با دسته‌بندی کردن وضعیت اقتصادی کشور و میزان ریسک پول‌شویی در آنها، همواره کشورها را به سمت همکاری‌های بین‌المللی در قبال اقتصاد منطقی و سالم جهانی سوق دهد. نیروی تأثیرگذاری گروه ویژه اقدام مالی آن‌چنان بالاست که دولت ایران که عضو هیچ‌یک از گروه‌های منطقه‌ای FATF نیست نیز عموم مقررات و اقدامات ضدپول‌شویی خود را به خواست این گروه انجام داده

1. Peter Alldridge, *Money Laundering Law; Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime* (London: Bloomsbury Publishing, 2003), 786.

Abdillahi Ghahfarokhi, Shahyar, Batol Pakzad, Hassan Alipour & Mohammadreza Elahimanesh "Prevention of e-money laundering: Defensive approach ..." Journal of Criminal Law and Criminology. 9, no. 18 (February 19, 2022): 385-406.

است. از همین رو، وضعیت پیشگیری از این جرم به دیگر جرایم فرق می‌کند و دولت‌های مترصد در پیشگیری از پول‌شویی باید عموماً از راهکارهای بین‌المللی پیروی کنند. ولی اگر در کشوری پیروی از این الگوها و راهکارهای بین‌المللی کم‌رنگ باشد یا نظام حقوقی یک کشور در راستای بومی‌سازی، پول‌شویی را وفق دیدگاه خود معرفی کند، در این صورت چالش پیوند محرمانگی و شفافیت عمیق خواهد بود. حتی در روابط دوجانبه کشورهایی که خود را تابع اقدامات و تصمیمات بین‌المللی می‌دانند باز این روابط شکننده و به سود محرمانگی است. به سخن دیگر، همکاری کشورها بر اساس اصل محرمانگی یا رازداری بانکی از اصل مهم دیگر یعنی تقابل نیز تبعیت می‌کند و «به اشتراک‌گذاری اطلاعات با همتایان خارجی در مبارزه با پول‌شویی یا پیشگیری از آن، بر اساس اصل متقابل و محرمانه بودن است.»[۲] این معامله متقابل به‌عنوان اصل قدیمی در روابط کشورها، همچنان بر تدابیر پیشگیری از پول‌شویی سایه انداخته است.

۲- نظارت بر مبدأ و منشأ پول‌شویی الکترونیکی

پول‌شویی الکترونیکی پدیده‌ای است که زمینه تحقق آن در دو بستر فراهم شده است. بستر مالی و بستر رایانه‌ای. بستر مالی، مؤسسات و نهادهای مالی و به‌طورکلی محیط مبادله پولی است که در واقع بزرگ‌ترین نماد ارتباط اشخاص حقیقی و حقوقی با همدیگر است. بستر رایانه‌ای نیز به‌عنوان بهره‌گیری از فضای سایبر برای مبادلات پولی و مالی در بستر مالی، نقش مکمل، تسهیل‌کننده و تحول‌آفرین دارد. ازاین‌رو، این دو بستر در کنار هم و درهم‌تنیده‌اند به‌گونه‌ای که هیچ یک از پدیده‌های مجرمانه، از چنین بسترهای مناسب و گسترده برای تحقق برخوردار نیستند و همین امر، پول‌شویی را به یک پدیده‌ای بدل کرده که در سطح گسترده درحال تحقق است و این سطح گسترده تنها نقطه کوچکی در بستر مبادلات مالی و بستر فعالیت‌های رایانه‌ای است.

با رایانه‌ای شدن امور، فعالیت‌های بانکی هم آسان‌تر و هم سریع‌تر از گذشته انجام می‌شوند. این روند طبیعی، فعالیت مالی و بانکی را به سمت در سایه یا حتی سیاهی قرار گرفتن برده است. «با حذف تعامل شخصی بین مشتری و مؤسسه، بسیار مشکل می‌توان فهمید که چه کسی به‌طور واقعی حساب را کنترل می‌کند و چه چیزی صحت عملکرد تجاری را تأیید می‌کند. مؤسسات مالی به‌صورت عادی تنها قادر به تعیین این نکته هستند که یک حساب خاص صرفاً در یک زمان خاص قابلِ‌دسترسی است. بانک تنها قادر است معین کند که دسترسی به‌وسیله نگهدارنده حساب صوری صورت می‌گیرد و هیچ روشی برای تعیین محلی که مشتری تراکنش را انجام می‌دهد وجود ندارد.»[۳]

به تبع الکترونیکی شدن، بانک‌ها و نهادهای مالی نیز بی‌میل به اصل گمنامی و رازداری در

2. Madeline Lee, "*Anti money laundering laws and regulations in Singapore*," in *A comparative guide to Anti-Money Laundering, A critical analysis of system in Singapore, Switzerland, the UK and the USA*, edited by Mark Pieth and Gemma Aiolfi, (Massachusetts: Edward Elgar Publishing, 2004), 64-99.

۳. محمدجعفر حبیب‌زاده و سیده سپیده میرمجیدی هشجین، «نقش بانکداری الکترونیکی در پولشویی و روش‌های مقابله با آن»، *پژوهش‌های حقوق تطبیقی* ۱۵ (۱)(۱۳۹۰)، ۳۲.

فضای سایبر نیستند؛ چون چنین بستری با اساسنامه و هدف آنها که تحصیل سود است، مطابقت دارد. از سوی دیگر همین تعامل مشتری و بانک سبب شکل‌گیری خطر یا ریسک در سطح گسترده و عمیق می‌شود که حتی برای نظارت‌های بانکی نیز امری چالش‌برانگیز می‌گردد. دراین‌راستا، «دو گونه گستره از خطر را می‌توان در عمل تشخیص داد که عبارتند از «خطرپذیری»، جایی که اقدامی برای فرصت‌جویی انجام می‌شود درحالی‌که احتمال رویارویی با خطرات وجود دارد و «در معرض خطر بودن» که تهدیدی از سوی عامل‌های بیرونی است. در هر دو مورد یک مشکل اساسی وجود دارد و آن اینکه ناظر باید بدون اطمینان فعالیت خود را شروع کند. نیازی به تمایز بین خود ریسک و آگاهی از ریسک نیست، زیرا عدمِ‌آگاهی داخل در عدمِ‌اطمینان است. ناظر شرایط را درک می‌کند و سپس نوعی از ساختار فکری را معَرفی می‌کند که واسطه است و ابهام عدمِ‌اطمینان را به خطر تبدیل می‌کند. ریسک چیزی است که قابلیت نمایش دارد. از طرف دیگر عدمِ‌اطمَینان وضعیت ذهنی است که ناشناخته است و قابلِ‌فهم نیست.»[۴]

بدین‌حال پول‌شویی پدیده‌ای مرکب می‌نماید که نه‌تنها عملکرد بانک‌ها را؛ بلکه به‌تدریج نظارت و حسابرسی را نیز تحت تأثیر قرار می‌دهد؛ به‌گونه‌ای که در کشورهای مختلف به وضعیت اداری و اقتصادی متفاوت، نظارت و حسابرسی می‌تواند از یک بُعد نقش تدابیر ضدپول‌شویی داشته باشد ولی از سوی دیگر می‌تواند زمینه‌ساز عدمِ‌تحقق مبارزه با پول‌شویی یا حتی بسترسازی برای ارتکاب آن باشد.[۵] ازاین‌جهت به اثر وارونه حسابرسی بر پول‌شویی، این پدیده «می‌تواند حق‌الزحمه حسابرسی را به دو صورت تحت تأثیر قرار دهد؛ نخست از طریق از بین بردن کیفیت گزارشگری مالی است که در بسیاری از پژوهش‌های حسابداری و مالی، کیفیت گزارشگری مالی میزان صداقت مدیران در ارائه اطلاعات منصفانه و حقیقی برای تصمیم‌گیرندگان تعریف شده است. ... گزارش حسابرس با آگاهی ایشان از خسارت‌های ناشی از تقلب و فساد در گزارشگری مالی که می‌تواند به پول‌شویی نیز مربوط باشد، تأثیر می‌پذیرد. بدین‌صورت می‌توان اظهار داشت پول‌شویی باعث افزایش ریسک مرتبط با تحریفات مالی می‌شود که درنتیجه به تلاش و حق‌الزحمه حسابرسی بیشتر منتج می‌شود.[۶]»«عامل مؤثر دوم تقویت ریسک حسابرسی در مواردی غیر از کیفیت گزارشگری مالی است. پول‌شویی می‌تواند با افزایش ریسک تجاری صاحبْ‌کار، باعث افزایش حق‌الزحمه حسابرسی شود ... حق‌الزحمه حسابرسی با ریسک‌های مالی، عملیاتی و تجاری رابطه مستقیم و معناداری دارد و مؤسسه‌های حسابرسی حق‌الزحمه حسابرسی بالاتری را برای شرکت‌هایی که دارای ریسک‌های

4. Dionysios S Demetis, *Technology and Anti Money Laundering: A system theory and risk-based approach*, (Massachusetts: Edward Elgar Publishing, 2010), 133.

۵. موارد بسترساز به عامل‌های متعددی همچون فقدان اهداف مشخص، تحقق عمل اقتصادی در کشورهای ویژه و اقدام اقتصادی در راستای اعمال مجرمانه است. نک: به باب والش، *حسابرسی ضدپولشویی و کنترل‌های مربوط به آن*، ترجمه وحید ملا امینی و احمد خالق‌بیگی، چاپ اول (تهران: انتشارات کتیبه، ۱۳۹۷).

۶. علی ابراهیمی کردلر، آرش تحریری و علی محمدی، «عدمِ‌رعایت قانون مبارزه با پولشویی و حق‌الزحمه حسابرسی»، *مجله دانش حسابداری* ۱۰(۴)(۱۳۹۸)، ۶۹.

Abdillahi Ghahfarokhi, Shahyar, Batol Pakzad, Hassan Alipour & Mohammadreza Elahimanesh "Prevention of e-money laundering: Defensive approach ..." Journal of Criminal Law and Criminology. 9, no. 18 (February 19, 2022): 385-406.

مذکور هستند، مطالبه می‌کنند. در واقع حسابرسان احتمالاً صاحب‌کارانی را که قانون مبارزه با پول‌شویی را رعایت نمی‌کنند، پُرریسک‌تر در نظر می‌گیرند و رفتار مدیران را متأثر از این عدمِ‌رعایت قوانین در نظر می‌گیرند.»[۷]

۳- دیده‌بانی مسیر مبادلات مالی الکترونیکی

دیده‌بانی پول‌شویی در یک بستر جهانی، نقش پیشگیرانه پلیس را که بیشتر محصور در محدوده سرزمینی است، به چالش می‌کشد. فرامرزی بودن محیط الکترونیک در درجه نخست چالش مالکیت و سپس مسئله کنترل را مطرح می‌کند. این فضا در مالکیت هیچ نهاد یا کشوری نیست و حتی اگر سهمی از مالکیت یا دارندگی فضای الکترونیکی را بتوان برای اشخاص قائل شد، این سهم بیشتر برای اشخاص حقوقی و شرکت‌هاست و نه دولت‌ها. به همین نحو کنترل‌ناپذیری فضای سایبر از سوی دولت‌ها سبب شده است تا دولت‌ها در برابر بستری قرار بگیرند که همکاری‌های متقابل آنها را توجیه می‌کند. همکاری‌هایی که برآمده از احساس ناتوانی در برابر یک رقیب نیرومند به نام فضای سایبر است. با آنکه زادگاه اینترنت، آمریکاست، حتی برای این کشور که قدرت کنترل بالایی نسبت به فضای سایبر دارد، احساس وابستگی متقابل هم به کشورهای دیگر و هم به نهادهای بین‌المللی دارد. «آمریکایی‌ها در آینده با نوع تازه‌ای از دستور کار سیاست خارجی روبه‌رو خواهند شد. ما ناگزیر خواهیم بود برای سازمان‌دهی اقدامات جمعی به دیپلماسی چندجانبه پناه ببریم. در اینجا دست‌کم دو موضوع روشن است: یکی اینکه ما از این به بعد باید توجه بیشتری به پیوند میان سیاست داخلی و خارجی معطوف کنیم و دیگر اینکه لازم است به شیوه نوآورانه‌تری درباره رابطه خود با نهادهای بین‌المللی بیاندیشیم.»[۸]

فرامرزی بودن محیط سایبر از سه جهت برای پیشگیری از پول‌شویی الکترونیکی، چالش پدید می‌آورد؛ نخست از جهت اعمال صلاحیت. ازآنجاکه محیط سایبر، بیرون از محدوده مرزی و سرزمینی دولت‌هاست، قواعد صلاحیت برای اعمال مقررات شکلی که مقررات پیشگیرانه دراین‌راستا قرار می‌گیرد، ناکافی است. مقرره‌های پیشگیرانه عموماً حول محور برنامه‌های قهرآمیز از سوی دولت‌اند و این برنامه در محدوده سرزمینی قابلیت اعمال دارند. وقتی رفتارهای پول‌شویی در فضایی جهانی ارتکاب می‌یابد ولی صلاحیت برای پیشگیری از آن در محیط ملی اعمال می‌شود، همین امر، برای درک عدمِ‌موفقیت تدابیر پیشگیرانه کافی است؛ دوم، از جهت مسؤولیت در برابر پیشگیری از پول‌شویی الکترونیکی در فراسوی مرزها. کشورها تدابیر پیشگیری از وقوع جرم را با سیستم بومی پلیس و نهادهای قضایی و اجرایی پیوند زده‌اند و این نهادها هنگامی‌که تهدید سایبری را متوجه کشور متبوع خود ببینند حساس می‌شوند و به همین اندازه اگر این توجه به جهت بیرون بودن کشور

---

۷. همان، ۷۰-۷۱.

۸. جوزف. اس نای، *قدرت در عصر اطلاعات: از واقع‌گرایی تا جهانی شدن*، ترجمه سعید میرترابی، چاپ اول (تهران: انتشارات پژوهشکده مطالعات راهبردی، ۱۳۸۷)، ۲۶۹.

از موقعیت تهدید کم‌رنگ باشد، توجه چندانی نسبت به تدابیر پیشگیری نمی‌نمایند؛ بنابراین نهادهای پیشگیری از وقوع جرم، عادت‌وار، مسؤولیت خود را برای تهدیدهای در راستای کشور متبوع خود تنظیم می‌کنند و حتی این مسؤولیت بیشتر برای تهدیدهای سنتی است تا سایبری. این امر سبب می‌شود تا نگاه جدید و جهانی برای مواجهه با پدیده پول‌شویی الکترونیکی در میان نباشد. سوم از جهت سازکارهای فراملی در رویارویی با پول‌شویی الکترونیکی. گرچه کشورها به‌تدریج درحال اجتماع برای رویارویی با برخی پدیده‌های تهدیدآفرین بین‌المللی‌اند ولی واقعیت این است که تدابیر پیشگیرانه مشترک و یکپارچه، عموماً پیشنهاد نهادهای مرتبط با سازمان ملل متحد یا نهادهای بین‌المللی دیگر است. در واقع نهادهای بین‌المللی دراین‌زمینه تدبیرها یا رهنمودهایی را پیشنهاد می‌کنند که اجرایی شدن آنها به‌طور کامل به همکاری کشورها بستگی دارد. میزان همکاری کشورها دراین‌زمینه نیز چالش دیگر است؛ یعنی اگر هم همه کشورها یا اکثریت آنها در پی همکاری متقابل یا همکاری جهانی برای مبارزه با پول‌شویی برآیند، باز هم میزان همکاری این کشورها به یک اندازه نیست.

چالش دیگر، فضای عمیق و فضای تاریک است. دارک نت‌ها شبکه‌های اینترنتی خصوصی هستند که افراد می‌توانند به‌صورت ناشناس فایل‌هایی را از طریق آنها به اشتراک بگذارند. ردیابی و شناسایی کاربران این شبکه‌ها بدون نرم‌افزار ویژه تقریباً غیرممکن است. فضای عمیق عموماً به محیطی مناسب برای پول‌شویی الکترونیکی و نیز دیگر جرایم سازمان‌یافته دانسته می‌شود. این فضا، مستعد به‌کارگیری ارتباطات پنهانی میان بازیگران جرایم سازمان‌یافته به همراه پرداخت‌های پولی مخفیانه است. پول اصلی برای این محیط هم‌رمز ارزهایند و هم ارزهای معمول که در پی ارتباط در فضای عمیق در محیط بیرون، مبادله می‌شوند. چالش آشکار چنین محیطی در اینکه بتوان در آن از تدابیر پیشگیرانه بهره گرفت خود پیداست. اول اینکه چنین محیطی بیرون از نظارت معمول و شناخته‌شده است. برای چنین محیطی تدابیر متفاوت از محیط اینترنتی معمول که با تارنماهای دارای آدرس شناخته می‌شود، خواهد بود. همین امر به دوگانگی تدابیر پیشگیرانه در فضای سایبر می‌انجامد که گروهی برای محیط سایبری که با صفحات و نشانی‌های اینترنتی شناخته می‌شود، پیوند دارند و گروهی برای محیطی کاملاً ناشناخته. این محیط به همان اندازه ابهام و تاریکی با تدابیری شکننده همراه خواهند بود. ثانیاً وقتی محیط نامعلوم و نظارت‌ناپذیر باشد، متصدی پیشگیرانه سردرگم و بلاتکلیف است. چنین وضعیتی می‌تواند به اقدام‌های نامعلوم در راستای تحدید آزادی‌های سایبری یا اقدامات زیان‌زننده به مبادلات و معاملات سایبری مشروع و ارتباطات سایبری قانونی منجر شود. سیالیت محیط الکترونیکی تنها به اراده و برنامه یک فرد برای شیوه استفاده از یک دستگاه رایانه‌ای دارد. «تمام آن چیزی که فرد به آن نیاز دارد دسترسی به کامپیوتری است که متصل به اینترنت باشد. این کامپیوتر می‌تواند متعلق به فرد تروریست باشد یا اینکه کامپیوتری عمومی باشد، مثل کامپیوترهای مستقر در کتابخانه‌ها یا کافی‌نت‌ها. اگرچه یک تروریست بلندپرواز به سطحی از دانش

Abdillahi Ghahfarokhi, Shahyar, Batol Pakzad, Hassan Alipour & Mohammadreza Elahimanesh “Prevention of e-money laundering: Defensive approach ...” Journal of Criminal Law and Criminology. 9, no. 18 (February 19, 2022): 385-406.

کامپیوتر نیاز دارد، اما نوع و دامنه دقیق تخصص به ماهیت حوادث تروریستی سایبری بستگی دارد.»[9] درباره پول‌شویی نیز همین ویژگی سیالیت داده‌ها و اطلاعات مهم‌ترین انگیزه‌بخش برای پول‌شو خواهد بود.

سیالیت محیط الکترونیکی با تدابیر پیشگیرانه از وقوع جرم سر ناسازگاری دارد. البته در محیط فیزیکی نیز جابه‌جایی جرم را به‌عنوان چالشی برای پیشگیری از وقوع جرم است. جابه‌جایی باعث می‌شود تا هم هزینه‌های پیشگیری بالا برود و هم تدابیر پیشگیرانه نتوانند فرصت ایجاد جرم را به‌طور کامل از بین ببرند. همین وضعیت برای فضای الکترونیک نیز صدق می‌کند؛ چون محیط جرم در فضای سایبر بر استفاده از اطلاعات استوار است و اطلاعات نیز مدام درحال مبادله‌اند. همین امر می‌تواند گویای مشکلات طراحی پیشگیری برای رویارویی با پول‌شویی الکترونیکی باشد.

تدابیر پیشگیرانه در محیط سیال ناگزیر چهره‌ای تدافعی به خود می‌گیرد تا تهاجمی. درحالی‌که در فضای سنتی، تدابیر پیشگیرانه وضعی از وقوع جرم به‌صورت فعال و هجومی به محیط‌هایی می‌رود که محل انجام جرم‌اند ولی در فضای سایبر چنین نگرشی عموماً به جهت سیالیت اطلاعات ناموفق است. برعکس تدابیری مانند استفاده از پالایه‌شکن یا باروی آتشین یا نرم‌افزارهای شناسایی افراد مجاز عموماً چهره‌ای تدافعی دارند تا حتی‌الامکان از ورود متجاوز یا اقدام متجاوز جلوگیری کنند. این چنین تدابیری نمی‌توانند برای سالم‌سازی محیط سایبر از وقوع جرایم سایبری و به‌طور ویژه پول‌شویی الکترونیکی کارساز باشند مگر اینکه متناسب با سیال بودن محیط الکترونیکی، نرم‌افزارهای سیال و ناظری برای تهاجم به محیط شکل‌گیری جرم طراحی شوند.

۴- دیده‌بانی بستر پول‌شویی الکترونیکی در تعارض محرمانگی و شفافیت

پول‌شویی در زمره جرایمی است که رفتارهای آن، پشت میز، مخفیانه، ارتباط‌محور و گاه اشاره‌محور انجام می‌شود. چنین ویژگی‌هایی، تدابیر گوناگون پیشگیری به‌ویژه تدابیری که نیاز به مجری دارد را با چالش جدی مواجه می‌کند؛ ازاین‌رو، پیشگیری از پول‌شویی تماماً وابسته به همکاری نهادها و مؤسسات مالی یا همه اشخاص حقوقی و حقیقی است که به‌گونه‌ای با عواید حاصل از جرم مرتبط‌اند. بااین‌حال این اشخاص در عمل به رازداری بانکی گرایش دارند. بر اساس یک پژوهش «شناسایی ارزیابی و مدیریت ریسک پول‌شویی بیشترین تأثیر را در پیشگیری و مبارزه با پول‌شویی و تأثیر سازمان‌های غیربانکی در پیشگیری و مبارزه با پول‌شویی از سهم کمتری نسبت به متغیرها برخوردار است.[10] ازاین‌رو، پیشگیری از پول‌شویی تا زمانی نهادهای مالی دراین‌زمینه مصمم نباشند، به فرجام نمی‌رسد. متغیرهای «اراده، دانش، تعامل و شناخت»[11] چهار متغیر بنیادین برای نهادهای مالی در

9. Susan. W. Brenner and Mark D. Goodman, "in defense of Cyber terrorism: An argument for anticipating cyber-attacks", *Journal of law, technology and policy*, (2002): 24.

۱۰. اصغر ابوالحسنی هستیانی و قربان دانیالی، «تدوین الگوی راهبردی پیشگیری از پولشویی در ساختار بانکی کشور ایران (مطالعه موردی: بانک صادرات ایران)»، *فصلنامه علمی پژوهشی مدیریت سازمان‌های دولتی* (۶) (۴)(۱۳۹۷)، ۲۳.

۱۱. ابراهیم عباسی و محمدصادق رومی، «بررسی نقش دستگاه‌های نظارتی و حسابرسی در قبال قانون مبارزه با←

زمینه تجهیز معنوی برای پیشگیری از پولشویی‌اند که باید در کنار هم و به‌صورت هماهنگ مستقر باشند تا تأثیر اقدامات پیشگیرانه ملموس باشد ولی در عوض هر یک از این متغیرها می‌تواند بنا به دلایل متفاوتی با دیگری ناسازگار گردد یا تأثیر منفی بر آن گذارد.

هرچند اقدام‌های کیفری، تأمینی، انضباطی و اداری برای مبارزه با پول‌شویی به‌تدریج درحال افزایش است ولی حتی اقدام‌های قهرآمیز یا برهم زدن قواعد رویارویی با جرم نیز دراین‌زمینه کارساز به‌نظر نمی‌رسد؛ برای نمونه «معکوس کردن بار اثبات چندان معقول به‌نظر نمی‌رسد. حتی اگر نهادهای داخلی بخواهند دراین‌زمینه عمل کنند باز موقعیت خود را در گرو رازداری می‌بینند و اطلاعاتی که با آن پیوند دارد.»[۱۲] در واقع رازداری بانکی به‌عنوان یک مقرره الزام‌آور همواره می‌تواند در کنار قواعد مبارزه‌کننده با پول‌شویی جای بگیرد و دست کم بخشی از نیروی مبارزه را خنثی کند.

از سوی دیگر، با وجود گرایش‌های نهادهای مالی به رازداری، امکان تشخیص پول‌شویی و پیشگیری از آن همچنان برای این نهادها فراهم است؛ زیرا در مبادلات مالی که هسته اصلی آن قواعد مشخص اقتصادی و نیز الزامات حسابرسی است؛ درهرحال امکان تشخیص عملیات مشکوک و یا رفتارهای ناهمخوان با رفتارهای معمول و قانونی وجود دارد؛ چراکه «برخی داده‌ها تنها در صورتی شک‌برانگیز و تعجب‌آور هستند که در مقایسه با داده‌های حوزه یا بافت خود مقایسه شوند. این داده‌ها داده پَرت بافتاری نامیده می‌شوند ... ازآنجاکه تناسبی بین صورت‌حساب‌های بانکی مرتکبین جرم پول‌شویی (قاچاقچیان مواد مخدر، سارقان، گردانندگان باندهای فساد و فحشا، آدم‌رباها و غیره) و درآمدهای قانونی (شغل قانونی و واقعی این افراد) وجود ندارد؛ لذا وضعیت مالی ایشان در مقایسه با سایر افراد از بافت قانونی ایشان در دسته داده‌های (تراکنش‌های) پَرت بافتاری قرار می‌گیرد.»[۱۳]

باز تشخیص مسیرهای متفاوت مبادلات مالی ناشی از رفتارهای قانونی ـ غیرقانونی بستگی بسیار زیاد به نوع و ساختار اقتصادی یک کشور دارد. هر چند «فرمولی که در عملیات پول‌شویی محاسبات و مناسبات اقتصادی را به هم می‌ریزد جز این نیست که اگر اقتصاد یک جامعه را به‌مثابه یک مجموعه منسجم در نظر بگیریم که ورودی و خروجی معین و کنترل‌شده‌ای دارد، عواید حاصل از پول‌شویی که در مجموعه اقتصاد تولید نشده و جزء ورودی اقتصاد نیست، ناگهان و بدون رعایت تناسب در به‌کارگیری، وارد چرخه اقتصاد شده و چون از سیطره کنترل نهادهای کنترلی (دولت یا بخش خصوصی) خارج است، موجب ایجاد اختلال و صدمه جبران‌ناپذیر می‌گردد.»[۱۴] ولی اگر بخش

پولشویی»، *مجله دانش حسابرسی* ۱۸ (۷۰)(۱۳۹۷)، ۲۲۶.

۱۲. A.C.H Alexander, *Insider Dealing and Money Laundering in the EU: Law and Regulation*, (United Kingdom: Ashgate Publishing Limited, 2007), 53

۱۳. علی فرخیان و عبدالله چاله چاله، «کشف تراکنش‌های مشکوک به پول‌شویی بر اساس الگوی بافتاری حساب‌های بانکی»، *دانش حسابرسی* ۱۹ (۷۴)(۱۳۹۸)، ۲۴۲.

۱۴. کرم جانی‌پور و مختار معروفی، «تحلیلی در لزوم جرم انگاری پول‌شویی (با نگاهی تطبیقی به مدل جرم‌انگاری پالایش)»، *آموزه‌های حقوق کیفری* (۶)(۱۳۹۲)، ۱۳۸.

Abdillahi Ghahfarokhi, Shahyar, Batol Pakzad, Hassan Alipour & Mohammadreza Elahimanesh "Prevention of e-money laundering: Defensive approach ..." Journal of Criminal Law and Criminology. 9, no. 18 (February 19, 2022): 385-406.

قابلِ‌توجهی از اقتصاد یک کشور، محصول اقتصاد سیاه یا قاچاق و پول‌شویی باشد در این صورت نمی‌توان فرمول مشخصی ارائه داد که نشان‌دهنده فعالیت‌های اقتصادی نامشروع و به‌ویژه پول‌شویی یک پدیده استثنایی و نادر در کنار رفتارهای اقتصادی مشروع است و به‌راحتی قابلِ‌تشخیص می‌باشد. در یک اقتصاد ناسالم و مبتنی‌بر رانت یا قاچاق، فرمول‌های تشخیص داده‌های پَرت یا عملیات بیرون از چرخه اقتصادی غیرقابلِ‌تشخیص است.

بستر اقتصادی ناسالم و جلوه‌های تحقق غیرمتعارف یا بیرون از نظم و چرخه اقتصادی جهانی، ذاتاً با پیشگیری از پول‌شویی متعارض است و اساساً در چنین اقتصادی نمی‌توان سخن از شفافیت گفت. در تعارض میان رازداری بانکی و اقدامات پیشگیرانه گفته می‌شود «گرچه افراد و حقوق آنها مصون از تعرض‌اند ولی در صورت ارتکاب جرم یا وجود امارات یا دلایل قوی بر وقوع جرم با رعایت موازین قانونی، حقوق مزبور قابلِ‌خدشه است. چون یک مصلحت مهم‌تر از حفظ حقوق شخصی افراد یعنی حفظ نظم اجتماعی و تضمین امنیت جامعه وجود دارد. در واقع این به معنی حرکت به سمت‌وسوی امنیت‌گرایی است.»[۱۵]

رویه‌های مشخص و آزموده شده در پیشگیری از پول‌شویی نیز نشان می‌دهد که تدابیر پیشگیری پدیده عموماً به‌وسیله نهادهای بین‌المللی ازجمله گروه ویژه اقدام مالی، سازمان ملل متحد و برخی گروه‌های بین‌المللی غیردولتی مانند کمیته بازل و گروه ولفسبورگ ارائه می‌شود تا به‌طور یکسان و هدفمند در سطح بین‌المللی پیاده شود. اگر کشوری بخواهد به زعم خود با تدابیر پیشگیرانه متفاوتی در راستای مبارزه با پول‌شویی قدم بردارد در این حال با شفاف‌سازی مالی مسیری جز بر هم زدن معادله امنیت و حق و درنتیجه امنیت‌سازی را در پیش نخواهد گرفت. بدین‌حال باید پذیرفت که شفافیت ارزشی است که از دو بُعد کلان می‌تواند در عمل ناکام شود؛ یکی ازاین‌حیث که نهادهای مالی دراین‌زمینه گرایشی ندارد و باید برای شفاف‌سازی در مبادلات مالی الزام شود. دیگری بسترهای لازم برای یک جامعه پویا با اقتصاد سالم و الگو گرفته از شیوه‌های شناخته‌شده بین‌المللی که اگر این بسترها نباشد باز شفافیت امکان‌پذیر نخواهد بود.

۵- تقویت رویکرد هجومی با افزایش همکاری‌های بین‌المللی

رویکرد هجومی یک پیش‌شرط مهم دارد و آن تسلط متصدی پیشگیری یا شیوه‌های پیشگیرانه بر محیط ارتکاب جرم است. زمانی که محیط پول‌شویی ذاتاً جهانی و رهیده از مرزهای سرزمینی باشد، در حال این پیش‌شرط برای تدارک رویکرد هجومی، وجود ندارد؛ بنابراین باید به اقتضای جهانی بودن بستر انجام جرایم سایبری به‌خصوص پول‌شویی الکترونیکی، زمینه تسلط جهانی بر این محیط نیز فراهم شود و این زمینه تنها از رهگذر همکاری‌های بین‌المللی امکان‌پذیر خواهد بود.

بستر اصلی پول‌شویی الکترونیکی، ارتباطات مالی فرامرزی است. ارتباط فرامرزی بانک‌ها و

۱۵. باقر شاملو، مجید مرادی، «تحدید تضمینات دادرسی عادلانه در پرتو امنیت‌گرایی در جرم پول‌شویی»، *مجله حقوقی دادگستری* (۸۱)(۱۳۹۲)، ۱۳۷.

نهادهای مالی در بیشتر کشورهای جهان سبب می‌شود تا نقل‌وانتقال‌های مالی در لوای یک توافق امن و محرمانه میان بانک‌ها و نهادهای مالی انجام شود.

پیشگیری از پول‌شویی در بُعد بین‌المللی خود به‌طور فراگیر سمت و سوی شفافیت را دارد تا محرمانگی. نهادهای بین‌المللی هم طراح تدابیر پیشگیری از پول‌شویی و هم ارائه‌کننده الگو در رویارویی با این پدیده‌اند و همین‌که در زمینه سخت‌گیری دراین‌راستا اِبایی ندارند. رهنمودهای چهل‌گانه گروه ویژه اقدام مالی و نظارت مستمر و دقیق این سازمان بین‌دولتی از یک‌سو و رهنمودها و راهکارهای دقیق و گاه سخت‌گیرانه کمیسیون اروپا برای کشورهای اروپایی از سوی دیگر بیان‌کننده جدّیت در زمینه شفاف‌سازی است؛ به‌گونه‌ای که در برخی برنامه‌ها و طرح‌هایی که کمیسیون اروپا در پی آن است «نقض پیوند محرمانگی میان وکیل و موکل دیده می‌شود به‌گونه‌ای که وکیل باید فعالیت‌های مشکوک موکل خود را به‌منظور مقابله با پول‌شویی به مقام‌های صلاحیت‌دار گزارش کند.[۱۶]»

دو نهاد مهم بین‌المللی دیگر نیز در زمینه مبارزه با پول‌شویی فعال‌اند: نخست، کمیته بازل درباره نظارت بانکی. این کمیته تدابیر پیشگیری از به‌کارگیری مجرمانه سامانه بانکی برای ارتکاب پول‌شویی را در سال ۱۹۸۸ تصویب کرد. این کمیته «بر اصول اخلاقی و کدهای رفتاری متمرکز است و سه اصل شناسایی مشتری و درک تجارت وی، عدم‌پذیرش معاملات مشکوک و همکاری با نهادهای مجری قانون را در پیش گرفت. در اکتبر ۲۰۰۱، کمیته بازل «کوشش شایسته مشتری برای بانک‌ها» را منتشر کرد که راهنمایی‌های عمیقی درباره این قاعده ارائه می‌دهد. زمینه‌های کلیدی این سند عبارتند از: اهمیت استانداردهای شناخت مشتری برای متصدیان بانکی و بانک‌ها. عناصر اساسی استانداردهای شناخت مشتری و نقش متصدیان اجرای استانداردهای شناخت مشتری در یک زمینه فرامرزی. عناصر فرایند شناخت مشتری بیشتر غالباً عبارتند از: سیاست پذیرش مشتری، شناسایی مشتری، نظارت مداوم بر حساب‌ها و معاملات و مدیریت ریسک.»[۱۷]

دوم، گروه ولفسبورگ. «در اکتبر سال ۲۰۰۰، تعدادی از بانک‌های خصوصی بین‌المللی (گروه ولفسبورگ) در مورد مجموعه دستورالعمل‌های جهانی ضدپول‌شویی برای اداره تجارت بانکی خصوصی توافق کردند. این دستورالعمل‌ها در می ۲۰۰۲ تجدیدنظر شده، به‌عنوان راهنمای مهم جهانی برای تجارت سالم در بانکداری خصوصی بین‌المللی در نظر گرفته می‌شود. این انتشارات آموزنده توسط گروه ولفسبورگ شامل بیانیه‌هایی در زمینه سرکوب تأمین مالی تروریسم، اصول ضدپولشویی در بانک‌ها و دیده‌بانی، غربالگری و تحقیق بانکی است.»[۱۸]

این رویه‌ها، مقرره‌ها، اقدام‌ها و نگرش‌های بین‌المللی همگی در راستای موظف کردن دولت‌ها به

16. Franco Frattini, "initiatives of the European commission", in *anti money laundering: international law and practice*, edited by Wouter H. Muller and Christian H, Kalin and John G. Goldsworth, (New Jersey: Wiley; 1st edition (June 5, 2007) John Wiley and Sons Ltd, 2007), 61

17. The World Bank; *Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide*,)Washington: The International Bank for Reconstruction and Development, 2009), 269

18. Ibid., 270.

فرعی‌سازی اصل رازداری بانکی در برابر اصل شفافیت است. به‌ویژه آنکه ارتباط تنگاتنگ پول‌شویی با تأمین مالی تروریسم همواره نهادهای بین‌المللی را نگران می‌کند. ازاین‌رو در دید نهادهای بین‌المللی «شناسایی مشتری برای ایجاد رژیم مؤثر در قبال مبارزه با پول‌شویی و تأمین مالی تروریسم کلیدی است. احتیاط مرتبط با مشتری و رویه‌های جاری به این منظور انجام می‌شود که یک مؤسسه مالی بتواند گرایش معقولی مبنی‌بر اینکه هویت واقعی هر مشتری را می‌داند و با اطمینان از انواع مشاغل و معاملات مشتری آگاه است؛ انجام دهد. ارائه‌دهندگان خدماتی که پول یا ارزش را انتقال می‌دهند باید شناسایی مشتری و تأیید هویت مشتری با استفاده از اسناد، داده‌ها یا اطلاعات منبع معتبر و مستقل انجام دهند.»[19]

نهاد اصلی که در عموم کشورهای جهان برای شفاف‌سازی می‌کوشد و تا حد امکان در راستای کم‌رنگ کردن محرمانگی بانکی گام برمی‌دارد؛ واحد اطلاعات مالی[20] است. هر چند که «بیشتر واحدهای اطلاعات مالی، موضوع مقررات مربوط به محرمانگی قرار می‌گیرند که مبادله اطلاعات را با نهادهای دیگر هم در بُعد ملی و هم در بُعد بین‌المللی محدود می‌کند. گرچه بیشتر مقررات رازداری امکان تبادل اطلاعات با واحدهای اطلاعات مالی خارجی را فراهم می‌کند، اما همچنان تحت مقررات سخت‌گیرانه رازداری بانکی قرار می‌گیرند. مفاد مقررات مربوط به رازداری داخلی دولت پذیرنده تقریباً به‌طورقطع در مورد اطلاعات دریافتی از خارج اعمال می‌شود. علاوه‌بر این در بیشتر تفاهم‌نامه‌های مربوط به همکاری در پیشگیری از پول‌شویی، به مقررات محرمانگی اشاره می‌شود.»[21] این واحدهای اطلاعات مالی بر اساس مقررات سخت‌گیرانه بین‌المللی و تقریباً به‌صورت هماهنگ اقدام می‌کنند که در ایران نیز به‌موجب ماده ۷ مکرر قانون اصلاح مبارزه با پول‌شویی ۱۳۹۷ مرکز اطلاعات مالی زیر نظر شورای عالی مقابله و پیشگیری از جرایم پول‌شویی و تأمین مالی تروریسم تأسیس شد. این واحد با الگوبرداری از توصیه‌های گروه ویژه اقدام مالی تشکیل شده و پیش از این در بیشتر کشورهای جهان، چنین واحدی بنیاد گرفته است.

برخی وظایف واحد اطلاعات مالی دقیقاً منطبق با شفافیت و نقطه مقابل رازداری است که در صورت اجرای دقیق می‌تواند به‌طور فراگیر از یک‌سو به نقض محرمانگی اطلاعات مشتریان بانکی و از سوی دیگر مبارزه با فساد شود. به‌موجب ماده ۷ قانون اصلاح مبارزه با پول‌شویی، اشخاص نهادها و دستگاه‌های مشمول این قانون (موضوع مواد ۵ و ۶) برحسب نوع فعالیت و ساختار سازمانی خود مکلف به رعایت مواردی‌اند که برخی از آنها مستلزم ارائه اطلاعات مشتریان بانکی حتی در غیر موارد معاملات مشکوک است. ارائه اطلاعات، گزارش‌ها، اسناد و مدارک لازم به مرکز اطلاعات مالی در چهارچوب قانون و آیین‌نامه مصوب هیئت‌وزیران مقرر در بند ب این ماده، یکی از الزام‌ها درباره

19. Pierre-Laurent Chatain et al., *Integrity in mobile phone financial service; Measures for Mitigating Risks from Money Laundering and Terrorist Financing*, (The International Bank for Reconstruction and Development/ The World Bank, 2008), 35

20. Financial Intelligence Unit

21. Guy Stessens, *money Laundering: A new international law enforcement model*, (England: Cambridge University Press, 2000), 278.

مؤسسه‌های مالی و بانک‌هاست.[۲۲] همچنین به‌موجب بند ت این مقرره، نگهداری سوابق مربوط به شناسایی ارباب‌رجوع، مالک، سوابق حساب‌ها، عملیات و معاملات داخلی و خارجی حداقل به مدت پنج سال پس از پایان رابطه کاری یا انجام معامله نیز یکی از مصداق‌های برجسته در دسترس گذاردن اطلاعات حساب بانکی مشتریان و یا دیگر اطلاعات از سوی بانک‌ها برای واحد اطلاعات مالی است. در واقع با این دو مقرره و به‌جهت سکوت قانون درباره رعایت اصل رازداری بانکی، کاملاً روشن است که قانون اصلاح مبارزه با پول‌شویی اصل شفافیت را بر محرمانگی ترجیح داده است و واحد اطلاعات مالی را بر همه تراکنش‌های بانکی مسلط کرده است.

نتیجه‌گیری

کارایی و موفقیت پیشگیری از پول‌شویی الکترونیکی، مشروط به وجود عامل‌های متعددی است که باید در کنار هم قرار بگیرند تا بتوان از تأثیر پیشگیری سخن گفت. این تدابیر از هماهنگی تدبیرهای وضعی و اجتماعی گرفته تا بهره‌گیری از آموزش از سنین کودکی و نوجوانی و سپس استفاده از نرم‌افزارهای پاسبان و طرق دیده‌بانی و کنترل مبادلات. بااین‌حال قوت عامل‌های خنثی‌کننده تدابیر پیشگیری از پول‌شویی الکترونیکی به‌اندازه‌ای پررنگ است که سبب می‌شود تا همواره نسبت به کارایی پیشگیری تردید کرد. در واقع برای پیشگیری از پول‌شویی الکترونیکی، هماهنگی همه تدبیرها لازم است و برای عدم‌موفقیت آن، تنها به یک عامل خنثی‌کننده نیاز است. مهم‌ترین عامل خنثی‌کننده تدبیرهای پیشگیرانه، بستر انجام پول‌شویی الکترونیکی یعنی فضای سایبر است.

فضای سایبر در پول‌شویی الکترونیکی، همه آنچه در فضای سنتی برای مبادله پول لازم است را تدارک می‌بیند. از مبدأ تا مقصد مبادله یا شیوه‌های آن، همگی می‌توانند کاملاً با شرایطی متفاوت با فضای سنتی باشند. حتی پول مبادله نیز لازم نیست پول رایج کشور دراین‌زمینه باشد رمزارزها به‌ویژه بیت‌کویین خود به‌تنهایی برای پول‌شویی کافی است. در واقع رمز ارزها، حکم مال در فضای سنتی را دارند که اگر پول‌شو نخواهد از پول برای پول‌شویی استفاده کند و به مال روی بیاورید، در فضای سایبر از رمز ارز استفاده می‌کند. همه اینها دلالت بر یک فضای متفاوت ولی جهانی با ویژگی‌های خاص خود دارد که نمی‌توان از تدابیر پیشگیرانه سنتی که در قالب وضعی خود، مداخله در فرصت یا موقعیت ارتکاب جرم است، سخن گفت، زیرا چنین تدابیر ماهیتاً جنبه هجومی و مداخله‌گرانه دارد، درحالی‌که تدابیر پیشگیرانه در فضای سایبر چهره‌ای دفاعی دارد.

چهره تدافعی رویکرد پیشگیری از پول‌شویی به جهت عدم‌تناسب محیط جرم با اختیارات متصدی پیشگیری از جرم و یا تدابیر قابل‌اعمال است. در واقع محدودیت اعمال تدابیر پیشگیرانه در سپهری بسیار گسترده برای انجام پول‌شویی به یک ناکارآمدی می‌انجامد که تنها تدبیر اصلی زدودن چنین

---

۲۲. مانند بخش ۳۵۶ قانون پتریات که در زمینه مقرره‌گزاری، گزارش‌دهی و اشتراک‌گذاری است. به نقل از دنیس کاکس، *راهنمای مبارزه با پولشویی*، ترجمه وحید ملا امینی و احمد خالق بیگی، چاپ اول (تهران: انتشارات کتیبه، ۱۳۹۷)، ۱۷۳.

Abdillahi Ghahfarokhi, Shahyar, Batol Pakzad, Hassan Alipour & Mohammadreza Elahimanesh "Prevention of e-money laundering: Defensive approach ..." Journal of Criminal Law and Criminology. 9, no. 18 (February 19, 2022): 385-406.

وضعیتی، گسترش اعمال تدابیر پیشگیرانه در قالب جهانی‌سازی پیشگیری از جرم است. بر همین اساس، کشورهایی همچون ایران که در روند جهانی‌سازی نیستند در امر پیشگیری از پول‌شویی نیز ناموفق‌ترند.

تدابیر پیشگیری از پول‌شویی الکترونیکی که در یک بستر جهانی ارتکاب می‌یابد، ماهیتاً چهره‌ای بین‌المللی دارند و عموماً هم تصدی‌گری مبارزه با پول‌شویی در سطح جهانی و به محوریت گروه ویژه اقدام مالی است؛ درنتیجه ایران نمی‌تواند به‌تنهایی و بدون همکاری‌های بین‌المللی در راستای مبارزه با پول‌شویی گام بردارد. ازاین‌جهت است که باید گفت، مبارزه با پول‌شویی در ایران داستان شگفت‌انگیز و غم‌باری است که هم اصل محرمانگی را نادیده می‌گیرد و هم اصل شفافیت را به قربانگاه می‌برد. نادیده گرفتن اصل محرمانگی را ازاین‌جهت قانون مبارزه با پول‌شویی اساساً محملی برای کنترل اطلاعات مالی و بانکی و دسترسی به آنهاست و قربانی کردن اصل شفافیت ازاین‌جهت که ایران همکاری‌های بین‌المللی در راستای مبارزه با پول‌شویی را نمی‌پذیرد و در بستر فسادآلود خود در پی مبارزه با پول‌شویی است. مبارزه‌ای که خود به فساد می‌انجامد.

راهکار اصلی این نوشتار همانا تأکید بر رویکرد صیانتی و حفاظتی در قبال حمایت از داده‌های مالی و مبادلات مالی الکترونیکی است. بااین‌حال این رویکرد صیانتی و حفاظتی به معنای واقعی کلمه اهداف پیشگیری را برآورده نمی‌کند و باید مسیر هجومی شدن تدابیر پیشگیری در لوای جهانی‌سازی پیشگیری از پول‌شویی الکترونیکی به‌ویژه در جایی که از رمزارزها استفاده می‌شود یا پول‌شویی در تارنمای عمیق انجام می‌شود، هموار شود. در واقع باید قاعده‌ای جدید در قبال پیشگیری از پول‌شویی الکترونیکی بنیاد نهاد آن اینکه برای پدیده‌ای که در یک بستر جهانی با ویژگی‌های متمایز رخ می‌دهد، تدابیری جهانی برای رویارویی با آن لازم است.

منابع

الف) منابع فارسی:

– ابوالحسنی هستیانی، اصغر و قربان دانیالی. «تدوین الگوی راهبردی پیشگیری از پول‌شویی در ساختار بانکی کشور ایران (مطالعه موردی: بانک صادرات ایران)». *فصلنامه علمی پژوهشی مدیریت سازمان‌های دولتی* ۷۰ (۱۳۹۷): ۲۲۳–۲۴۸.

– ابراهیمی کردلر، علی، آرش تحریری و علی محمدی. «عدم‌رعایت قانون مبارزه با پول‌شویی و حق‌الزحمه حسابرسی». *مجله دانش حسابداری* ۱۰(۴)(۱۳۹۸): ۶۳–۸۸.

– جانی‌پور، کرم و مختار معروفی. «تحلیلی در لزوم جرم‌انگاری پول‌شویی (با نگاهی تطبیقی به مدل جرم‌انگاری پالایش)». *آموزه‌های حقوق کیفری* ۱۰(۱۳۹۲): ۱۲۷-۱۵۴.

– حبیب‌زاده، محمدجعفر و سیده سپیده میرمجیدی هشجین. «نقش بانکداری الکترونیکی در پول‌شویی و روش‌های مقابله با آن». *پژوهش‌های حقوق تطبیقی* ۱۵(۱)(۱۳۹۰): ۲۳–۴۳.

– شاملو، باقر و مجید مرادی. «تحدید تضمینات دادرسی عادلانه در پرتو امنیت‌گرایی در جرم پول‌شویی». *مجله حقوقی دادگستری*، ۷۷ (۱۳۹۲): ۱۱۱–۱۵۹.

– عباسی، ابراهیم و محمدصادق رومی. «بررسی نقش دستگاه‌های نظارتی و حسابرسی در قبال قانون مبارزه با پولشویی«تحدید تضمینات دادرسی عادلانه در پرتو امنیت گرایی در جرم پولشویی». مجله دانش حسابرسی۷۰ (۱۳۹۷): ۲۴۸–۲۲۳.

– فرخیان، علی و عبدالله چاله چاله. «کشف تراکنش‌های مشکوک به پول‌شویی بر اساس الگوی بافتاری حساب‌های بانکی». *مجله دانش حسابرسی*۷۴ (۱۳۹۸): ۲۳۷–۲۶۸.

– کاکس، دنیس، *راهنمای مبارزه با پول‌شویی*. ترجمه وحید ملاامینی و احمد خالق‌بیگی. چاپ اول. تهران: انتشارات کتیبه، ۱۳۹۷.

– نای، جوزف. اس. *قدرت در عصر اطلاعات: از واقع‌گرایی تا جهانی شدن*؛ ترجمه سعید میرترابی. چاپ اول. تهران: انتشارات پژوهشکده مطالعات راهبردی، ۱۳۸۷.

– والش، باب. *حسابرسی ضدپول‌شویی و کنترل‌های مربوط به آن*. ترجمه وحید ملاامینی و احمد خالق‌بیگی. چاپ اول. تهران: انتشارات کتیبه، ۱۳۹۷.

ب) منابع خارجی:

- Alexander, A.C.H; *Insider Dealing and Money Laundering in the EU: Law and Regulation*, London: Routledge, 2007.

- Alldridge, Peter; *Money Laundering Law; Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime*, London:Bloomsbury Publishing, 2003.

- Brenner, Susan. W. and Goodman, Mark D. "in defense of Cyber terrorism: An argument for anticipating cyber-attacks." *U. Ill. JL Tech. & Pol'y* (2002): 1, 31-40.

- Chatain, Pierre-Laurent, Raúl Hernández-Coss, Kamil Borowik, and Andrew Zerzan. *Integrity in mobile phone financial services: measures for mitigating risks from money laundering and terrorist financing*. Vol. 146. Washington, D.C :World Bank Publications, 2008.

- Demetis, Dionysios S; *Technology and Anti Money Laundering: A system theory and risk-based approach*, Massachusetts: Edward Elgar Publishing, 2010.

- Frattini, Franco; *initiatives of the European commission*, in: anti money laundering: international law and practice, edited by Wouter H. Muller and Christian H, Kalin and John G. Goldsworth. New Jersey: John Wiley and Sons Ltd, 2007.

- Lee, Madeline; *Anti money laundering laws and regulations in Singapore*, in: A comparative guide to Anti-Money Laundering; A critical analysis of system in Singapore, Switzerland, the UK and the USA, edited by Mark Pieth and Gemma Aiolfi. Massachusetts: Edward Elgar Publishing, 2004.

- Stessens, Guy; *money Laundering: A new international law enforcement model*. England: Cambridge University Press, 2000.

- The World Bank; *Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide*. Washington: The International Bank for Reconstruction and Development, 2009.