חשיפת זהות משתמשי מטבעות אלקטרוניים

הדר ז׳בוטינסקי, מיכל לביא*

התקפות טרור הן איום חמור על ביטחון הציבור והביטחון הלאומי. טכנולוגיות חדשות עלולות לסייע להתקפות אלה ולהביא לכך שתהיינה קטלניות יותר. ככל שארגוני טרור מצליחים לגייס יותר מימון, כך עולה היכולת שלהם לגייס חברים ולארגן ולבצע התקפות טרור. מאז התקפות הטרור בארצות הברית באחד עשר לספטמבר 2001, גורמי אכיפת החוק בעולם הגבירו את מאמציהם להיאבק בטרור. בין היתר, מדינות שונות הידקו את הרגולציה הנוגעת לאיסור מימון טרור והלבנת הון. מטרת הרגולציה היא לאתר, לחסום ולחלט כספים שנועדו למימון טרור ופשיעה ולמנוע מארגוני טרור את הספקת הכספים המהווים חמצן לפעילותם.

עד לאחרונה רוב מאמצי ההסדרה התמקדו באמצעי תשלום מסורתיים ובגופים המוסדיים בשוק ההון. לדוגמה, בישראל הוצאו צווי איסור הלבנת הון המופנים כלפי הבנקים, נותני שירותי אשראי, נותני שירותי מטבע ועוד. ברם, ההסדרה של אמצעי התשלום החלופיים, וביניהם המטבעות האלקטרוניים, נותרה מאחור. מטבעות אלקטרוניים הם טוקנים המוחלפים בין המשתמשים בהם על גבי רשת הבלוקצ׳יין. ככל שהמאמצים האסדרתיים הנוגעים לאיסור הלבנת הון ומימון

* **ד״ר הדר ז׳בוטינסקי** היא ד״ר למשפט וכלכלה, מייסדת ועמיתת מחקר במרכז הדר ז׳בוטינסקי לחקר בין־תחומי של שוקי הון, משברים וטכנולוגיה; עמיתת מחקר, בית הספר למשפטים - המכללה האקדמית צפת.
ד״ר מיכל לביא, ד״ר למשפטים, מחברת הספר אחריות מתווכי תוכן לעוולות ביטוי: הקשר חברתי, משפט וטכנולוגיה (2018), עמיתת מחקר במרכז הדר ז׳בוטינסקי לחקר בין־תחומי של שוקי הון, משברים וטכנולוגיה; עמיתת מחקר, בית הספר למשפטים – המכללה האקדמית צפת.

תודה מקרב לב למרכז חת לחקר התחרות והרגולציה במסלול האקדמי המכללה למינהל על התמיכה במחקר; תודה גם לחן ספייב, לישראל קליין, לרועי שראל, לשופטת המאמר, למערכת כתב העת מחקרי רגולציה, לעורכת הלשונית של כתב העת ולכל המשתתפים בכינוסים New Payment Products and Services, Anti-Money Laundering and Counter Terrorist Financing Risks" workshop (Macquarie University, Sydney Australia (Zoom)) (July 2020), The U.S. National Business Law Conference (University of Tennessee, U.S.; June 2021)., שבהם הוצגו טיוטות מוקדמות של גרסת המאמר המותאמת לדין האמריקאי, על ההערות המצוינות.
המאמר מוקדש לזכרה של אימה של מיכל – אביבה לביא, שליבה הענק נדם לפתע פתאום והיא בליבנו לעד.
גרסה מוקדמת יותר של המאמר המתואמת לדין האמריקאי פורסמה בכתב העת של פורדהאם לקניין רוחני: Hadar Y. Jabotinsky & Michal Lavi, *Speak Out: Verifying and Unmasking Cryptocurrency User Identity*, 32 FORDHAM INTELL PROP, MEDIA & ENTERTL. J.L 518 (2022).

טרור דרך המוסדות הפיננסיים המסורתיים מתגברים וקוצרים הצלחות, כך הופך השימוש במטבעות אלקטרוניים לאטרקטיבי יותר בעיני ארגוני הטרור. נוסף על כך, בעקבות וירוס הקורונה והירידה בשימוש במזומנים בעולם, גבר מאוד השימוש במטבעות אלה להלבנת הון ומימון טרור. על כן, בניסיון למנוע תופעות אלה, החקיקה במדינות שונות התפתחה גם בכיוון זה, וכיום יש מדינות שמסדירות, בין אם בצורה חלקית ובין אם בצורה מלאה, את נושא איסור הלבנת ההון ומימון הטרור דרך המטבעות האלקטרוניים.

הבעיה העיקרית הטמונה במטבעות האלקטרוניים בהקשר של מימון טרור והלבנת הון היא שחלק ממטבעות אלה הם אנונימיים. כלומר, אין כמעט דרך לדעת מי עומד מאחורי המטבע ואל מי המטבע מועבר. תכונה זו של המטבע יוצרת תשתית לזרם של עסקאות אנונימיות ופותחת בפני ארגוני טרור ופשיעה אפשרות לגייס מימון נרחב, לנהל, להעביר ולמשוך את הכסף לפעילות לא חוקית ביתר קלות. היכולת של ארגוני טרור וגורמים המממנים אותם להגביר את פעילותם ולקדם התקפות טרור שממומנות על ידי מטבעות אלקטרוניים מציבה איום ניכר לביטחון הלאומי. מאחר שהשימוש במטבעות אלקטרוניים הופך לנפוץ יותר, הצורך להסדיר את השימוש בהם גובר, והצורך בתגובה משפטית הופך לצו השעה.

המאמר יגיב לרפורמה בהסדרת מטבעות אלקטרוניים ויציע להטיל חובות משפטיות ברמה הגלובלית על חברות שמנפיקות מטבעות אלקטרוניים, מאפשרות מסחר בהם או מפתחות את הארנקים האלקטרוניים שבהם נשמרים המטבעות. החובה העיקרית שיכולה לסייע במלחמה במימון טרור והלבנת הון היא לאמת את הזהות של המשתמשים על גבי הבלוקצ׳יין ולהכיר את הלקוחות. אימות זהות משתמשי הבלוקצ׳יין יאפשר לבתי משפט להוציא צווים שיחייבו את החברות האמורות לחשוף את זהותם של משתמשי המטבעות האלקטרוניים כשיש חשש של ממש שפעילותם תומכת בטרור או בפעילות אחרת של הלבנת הון. רפורמות אלה יאפשרו לצמצם מימון טרור והלבנת הון שמתאפשרים באמצעות מטבעות אלקטרוניים, למנוע תכנון התקפות קטלניות ולקדם את הביטחון הלאומי. קיימת כבר רגולציה מדינתית ברמה זו או אחרת לצמצום האנונימיות של משתמשי המטבעות האלקטרוניים, אולם נכון להיום, הרגולציה נשארת ברמה המדינתית או האזורית בלבד ומתמקדת רק בנקודת הקצה כשבאים להמיר את המטבע למטבע מדינתי. על כן, הרגולציה אינה מאפשרת ידיעה אם נעשו במטבע האלקטרוני פעולות אסורות לאורך הדרך בטרם ההמרה למטבע המדינתי. הפתרון המוצע לזיהוי המשתמשים על גבי שרשרת הבלוקצ׳יין מקיף יותר ומאפשר אכיפה משמעותית יותר של איסורי מימון טרור והלבנת הון.

המאמר יעמוד על המתח שבין הפתרון המוצע לבין הזכות לאנונימיות כנגזרת של פרטיות ושל חופש ביטוי. הוא אף יתייחס לאתגרים שמציב הפתרון המוצע ולביקורות אפשריות בדבר פגיעה בחדשנות, בפרטיות, בחופש הביטוי וביעילות ויסביר כיצד הפתרון המוצע מאזן בין כל אלה לבין הרצון להגן מפני פעילות טרור והלבנת הון.

הקדמה. א. מתווכים כשומרי סף – רגולציה של מתווכים לקידום מלחמה בהפרות דין; 1. גורמים המאפשרים את התשתית לפעילות פיננסית כשומרי סף של העברה לא חוקית של כספים למימון טרור ופשיעה; 2.שימוש במתווכים פיננסיים מסורתיים לקידום הביטחון הלאומי;

nevo.co.il

(א) חוקי איסור הלבנת הון; (ב) מוסדות פיננסיים והמאבק בטרור. ב. מהם מטבעות אלקטרוניים? כיצד הם עובדים? וכיצד משתמשים בהם לקידום טרור?; 1. מטבעות אלקטרוניים; 2. מדוע וכיצד משתמשים ארגוני טרור ופשע במטבעות אלקטרוניים?; 3. האנונימיות של חלק מן המטבעות האלקטרוניים וחשיבותה לפעילות טרור ופשיעה; (א) הקושי בסיכול מימון טרור Counter Terrorism Financing (CTF) המתבצע במטבעות אלקטרוניים; (ב) מגבלות קיימות על אימוץ מטבעות אלקטרוניים בידי טרוריסטים. **ג. מתווה לרגולציה גלובלית של אימות זהות משתמשי מטבעות אלקטרוניים אקס אנטה וחשיפתם אקס פוסט;** 1. הדין המצוי – צעדים רגולטוריים ראשונים לאכיפת חוקי איסור הלבנת הון ומימון טרור על מטבעות אלקטרוניים; 2. הדין הרצוי – הצעה לרגולציה גלובלית של אימות זהות משתמשי מטבעות אלקטרוניים אקס אנטה וחשיפה אקס פוסט; (א) אימות זהות המשתמשים הפועלים על גבי הבלוקצ׳יין; (ב) חשיפת שמות המשתמשים כשמתעורר חשש ממשי למימון טרור או הלבנת הון תהיה כפופה לצו שיפוטי; (ג) מודל הסדרה גלובלי: שיתוף בין מדינות ואמנות בין־לאומיות. **ד. התייחסות למגבלות וביקורות על הרגולציה המוצעת**; 1.הזכות לפרטיות; 2.הזכות לחופש ביטוי; (א) חופש הביטוי של משתמשי מטבעות אלקטרוניים; (ב) אימות זהות, חשיפת זהות וחופש הביטוי של החברות המנפיקות, ספקי הארנקים ושירותי ההמרה; 3. חשש מריכוזיות של כוח: מהקתדרלה לבזאר וחזרה לקתדרלה? 4. עלויות מנהליות של אימות זהות אקס אנטה וחשיפתה אקס פוסט; 5. חשש מפריצה למידע וגנבת זהות. **סיכום**.

הקדמה

מטבעות אלקטרוניים הם מטבעות שנוצרים ומאוכסנים בצורה אלקטרונית בלבד על גבי טכנולוגיה מבוזרת שנקראת בלוקצ׳יין. מערכת זו היא רשת peer-to-peer, שמאפשרת למשתמשים להחליף מטבעות ולהעביר תשלום ממחשב של משתמש אחד למחשב של משתמש אחר ללא תיווך, מבלי להסתמך על בנקים, או מוסדות פיננסיים אחרים, או להיזקק למתווכים פיננסיים ולשלם להם עמלות.[1] בשונה מכסף מזומן, השימוש במטבעות אלה אינו מצריך מפגש פיזי של נותן התשלום ומקבלו כדי להשלים את פעולת התשלום, וניתן לבצעה באופן וירטואלי, חוצה גבולות.[2] המטבע האלקטרוני הראשון שהונפק נקרא ביטקוין.[3] מאז

1 נציין כי ביטקוין אינו המטבע היחיד. למעשה, יש 5,000 מטבעות אלקטרוניים בעולם כרגע, והמספר הזה גדל בהתמדה. ראו Primavera De Filippi, *Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream*, DECENTRALIZED THRIVING: GOVERNANCE AND COMMUNITY ON THE WEB 3.0. (January 23, 2019), https://ssrn.com/abstract=3524352.

2 עידו באום ״איסור הלבנת הון, חידושים מקומיים ומגמות גלובליות״ **דין ודברים** י 289, 297 (2017).

nevo.co.il

הנפקת הביטקוין הונפקו עוד אלפי מטבעות אלקטרוניים, וכיום ישנם סוגים שונים של מטבעות המותאמים לקהלים שונים ולצרכים שונים.[4]

טכנולוגיה זו מהווה חדשנות משבשת של השוק הפיננסי הקיים (disruptive innovation) והיא זכתה לכינוי ״מכונת האמון״ (trust machine), מאחר שהיא מייתרת את הצורך להסתמך על מוסדות ששימשו כמתווכי אמון בשווקים פיננסיים. בשונה ממתווכים אלה, הטכנולוגיה החדשה מבוססת על זהות סוברנית.[5] ככזו, למערכת מטבעות אלקטרוניים יש פוטנציאל להוביל למהפכה בהרבה סקטורים בחיי היום יום שלנו.[6] יש אף המאמינים שמהפכת המטבעות האלקטרוניים תשנה תפיסות של קניין, ביטוי וזהות.[7]

השימוש במטבעות האלקטרוניים הולך וגובר, ויותר חברות עושות בהם שימוש. לדוגמה, ענקית הרכב החשמלי טסלה רכשה ביטקוין בסכום של 1.5 מיליארד דולר ואף אפשרה לרכוש את רכביה באמצעות ביטקוין.[8] גם חלק ממדינות העולם החלו להכיר במטבע. כך, נשיא אל סלבדור נאיב בוקלה אף הפך את הביטקוין למטבע הרשמי של המדינה.[9] ברם, בד בבד עם השימושים הלגיטימיים החשובים והמועילים במטבע, נולדו גם שימושים פליליים להלבנת הון ומימון טרור. ככל שמתפתחים יותר שימושים לגיטימיים במטבעות האלקטרוניים והשימוש בהם הופך לנפוץ וזמין, כך קל יותר לארגוני טרור להלבין כספים ולגייס משאבים באמצעות המטבע. כדוגמה, לאחרונה הצליחה ממשלת ארצות הברית לתפוס מטבעות ביטקוין בשווי של 2 מיליון דולר וכן מטבעות אלקטרוניים (המכונים גם מטבעות קריפטוגרפיים) אחרים מחשבונות קריפטו ששלחו או קיבלו מימון כדי לממן ארגוני טרור זרים כמו אל קעידה וארגון המדינה האסלאמית (דאע״ש). גיוס מימון זה שנעשה באמצעות מטבעות אלקטרוניים התבצע

3 Cynthia Dion-Schwarz, David Manheim & Patrick B. Johnston, Terrorists Use of Cryptocurrencies, Technical and Organizational Barriers and Future Threats, RAND National Security Research Division (NSRD) 57 (2019) ("Bitcoin, which was launched by the pseudonymous Satoshi Nakamoto in early 2009, is both a protocol for securely storing and transmitting tokens (virtual coins) and the name of the unit of value in the system").

4 שם, בעמ׳ 2. דוגמאות למטבעות נוספים הן Omni Layer (MasterCoin), BlackCoin, Zcash, Ether, Libra

5 *The Trust Machine*, The Economist (Oct. 31, 2015).

6 Don Tapscott & Alex Tapscott, *How the Tech Behind Bitcoin Will Change Your Life*, Time (May 6, 2016) time.com/4320254/blockchain-tech-behind-bitcoin.

7 Timothy C. May, '*The Crypto Anarchist Manifesto*', groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html.

8 ראו מור בסן ״טסלה משקיעה בביטקוין – תאפשר לרכוש רכב במטבע דיגיטלי״ **14 עכשיו** (8.2.2021) https://bit.ly/3ykWaI7, אם כי בהמשך הודיע מנכ״ל טסלה כי היא תעצור את האפשרות לקנות רכבים של החברה באמצעות מטבע הביטקוין בשל השפעות כריית המטבע על הסביבה, ראו שירות גלובס ״ההודעה של מאסק שהפילה את מניית טסלה וגרמה לביטקוין לצנוח״ **גלובס** (13.5.2021) https://bit.ly/3IpPFIv.

9 ראו דן רבן ״הראשונה בעולם: אל סלבדור הפכה את הביטקוין למטבע רשמי״ **Ynet** (9.6.2021) https://bit.ly/3OMr2YN; סנטיאגו פרז ״נשיא אל סלבדור הלך על ביטקוין בכל הכוח, ואז המטבע החל לצנוח״ **גלובס** (16.5.2022) https://bit.ly/3amOaOz.

nevo.co.il

במדיה החברתית. ארגוני הטרור האמינו שהשימוש במטבעות אלקטרוניים מבטיח אנונימיות. אולם, ממשלת ארצות הברית פיתחה כלים להשתלט על האתר ששימש לשידול מימון טרור והצליחה לקבל מידע על החשבונות המעורבים. החקירה בנוגע לזהות התורמים ממשיכה. פעולה זו הייתה פעולת החילוט הראשונה שבה נתפסו מטבעות אלקטרוניים כחלק מחקירה של מימון טרור.[10]

ב־28 לאוגוסט 2015 נגזרו על עלי שוקרי אמין, שקשר קשר לספק תמיכה ממשית לארגון המדינה האסלאמית, 11 שנים בכלא בנוסף לפיקוח מתמיד על פעילות האינטרנט שלו לאחר שחרורו. שוקרי אמין הודה באשמת שימוש ברשת החברתית טוויטר כדי לספק ייעוץ, לעודד הצטרפות ולתת תמיכה מורלית ורעיונית לתומכי ארגון הטרור. שוקרי אמין השתמש בשם המשתמש @Amreekiwitness כדי לספק הוראות בנוגע לאיך להשתמש בביטקוין כדי למסך את העברת הכספים לארגון המדינה האסלאמית ולאפשר לתומכי הארגון לטוס לסוריה כדי להשתתף בלחימה מטעם הארגון. שוקרי אמין השתמש בחשבון הטוויטר כדי לקיים שיחות על דרכים לגיוס תמיכה כספית לארגון המדינה האסלאמית בשימוש במטבעות אלקטרוניים. מאחר שמטבעות אלה מאפשרים למשתמשים לסחור זה עם זה בצורה אנונימית, הם מהווים בסיס תשתיתי למערכת תרומות בטוחה למימון ארגון המדינה האסלאמית וארגוני טרור ופשיעה אחרים.[11]

ב־2015 עיתון "הארץ" דיווח על דוגמה ראשונה של גיוס הון של תא של ארגון המדינה האסלאמית בשימוש בביטקוין ברשת האפלה (dark net).[12] מגייס הכספים זיהה את עצמו בשם אבו מוסטפה, ולפי חשבון הביטקוין שלו הוא הצליח לגייס חמישה מטבעות ביטקויין (ששוויים נאמד אז בסכום של 1,000 דולר), לפני שרשות ה־FBI סגרה את חשבונו.[13]

המטבע האלקטרוני ששימש בכל העסקאות מעלה הוא הביטקוין, המטבע האלקטרוני הראשון וככל הנראה הידוע ביותר. השימוש במטבעות אלקטרוניים אנונימיים גבר לאחר התפשטות וירוס הקורונה.[14] הסבר אפשרי אחד לכך הוא שהאמון במוסדות ובמתווכים

10 Charlie Savage, U.*S. Seizes Bitcoin Said to Be Used to Finance Terrorist Groups*, N.Y Times (Aug. 13, 2020) nyti.ms/3aPiDAL.

11 FATF Report Emerging Terrorist Financing Risks 1, 36 (2015) www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (Last accessed 13 Jan. 2021).

12 הרשת האפלה היא רשת מוצפנת של אתרים המקושרים אחד לשני והיא חלק מהרשת העמוקה. הרשת העמוקה כוללת את כל האתרים שאינם מאונדקסים ואינם מאותרים כאשר עורכים חיפוש במנועי החיפוש המסורתיים. ראו Gabriel Weimann, *Going Darker? The Challenge of Dark Net Terrorism*, Wilson Ctr. (2018), https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_ter rorism.pdf.

13 Danna Harman, *US-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*, Haaretz, Jan. 29, 2015, https://bit.ly/3AuM0qL להרחבה על השימוש במטבעות אלקטרוניים לסיוע לטרור ראו Zachary K. Goldman et al., *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, Ctr. For A New Am. Sec. 12–13 (May 2017), https://bit.ly/3RbJZWt.

14 Hadar Jabotinsky & Roee Sarel, *How Crisis Affects Crypto: Coronavirus as a Test Case*, 74 Hastings L.J. 433 (2023).

nevo.co.il

הפיננסיים המסורתיים ירד. אובדן האמון הוביל לצורך גובר באלטרנטיבות. המודל של המטבעות האלקטרוניים המבוזרים הוא מועמד טבעי, שכן מטבעות אלקטרוניים נושאים ערך ואינם מוגבלים לגבולות גאוגרפיים או מדינתיים. למעשה, אפשר לרכוש מטבע אלקטרוני כמעט בכל מקום בעולם ולהשתמש בו אחר כך ברוב המדינות מבלי להידרש לשירותי החלפת מטבעות מסורתיים. מנקודת המבט של הלקוח, לאפשרות להשתמש במטבעות אלה יתרונות רבים, מאחר שהמטבע האלקטרוני מאפשר לעקוף את המתווכים, מוזיל את השירותים הפיננסיים ומנגיש אותם. זוהי למעשה מערכת פיננסית שבה האמון מתמקד בטכנולוגיה, ולא באנשים אחרים או במתווכים, ודבר זה מאפשר לשפר את השווקים ואת העסקים.[15]

אולם, כפי שציינו קודם, לשימוש במטבעות אלקטרוניים יש גם חסרונות: עם החדשנות הגדולה מגיעות עלויות חברתיות, ובמקרה זה, מתן פתח לפושעים ולטרוריסטים להלבין הון. הסיבה שבשלה מטבעות אלקטרוניים חשופים במיוחד לשימוש לרעה ומאפשרים פעילות מזיקה כמו הלבנת הון ומימון טרור היא שהמשתמשים במטבע נהנים מאנונימיות. בשל העובדה ששימוש במטבע אלקטרוני אינו עובר דרך מתווכים פיננסיים מסורתיים, יש קושי רב לזהות את בעליו ולעקוב אחר תנועותיו.[16] לכן, המטבע יכול להיות מנוצל לרעה על ידי גורמים פליליים ומהווה קרקע פורייה לפשיעה, מימון טרור והלבנת הון.[17] לדוגמה, קיימים כיום קניונים וירטואליים שבהם פועלים עשרות ואולי מאות עסקים בכל רחבי הארץ, שמסייעים ללקוחותיהם להעלים הון שחור מעיני הרשויות.[18] דוגמה נוספת היא שימוש במטבעות אלקטרוניים על ידי פושעים המשתייכים לארגון פשע מאורגן על מנת להלבין הון.[19] דוגמה נוספת היא שימוש במטבעות אלקטרוניים במסגרת מתקפת כופרה על מחשבים של ארגונים ועסקים לגיטימיים.[20] בנוסף, מטבעות אלקטרוניים יכולים להיות מנוצלים לקמפיין מימון המונים לשם גיוס כספים שיאפשר לארגוני טרור לקבל מימון.[21]

וירוס הקורונה ומגבלות ה״ריחוק החברתי״ שהוטלו בעקבותיו על ידי ממשלות ברחבי העולם כללו סגרים, בידודים וסגירת גבולות פיזיים ושדות תעופה ברחבי העולם. כתוצאה

15 על גבי טכנולוגיה זו התפתחה מערכת שלמה של נכסים קריפטוגרפיים כדוגמת אן אף טיז (NFT's), שמאפשרים להצמיד ביטוי, תמונה או וידאו למטבע קריפטוגרפי וכך לנהל מידע שקשור לבעלות על גבי הבלוקצ׳יין. לדיון באן אף טיז ובבעיות הרגולטוריות שמתעוררות כתוצאה מהתפתחות הטכנולוגיה (וגם לפתרונות המדיניות המוצעים) ראו Hadar Y. Jabotinky & Michal Lavi, *NFT for Eternity*, U. MICH. J. LAW REFORM (forthcoming) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4077695.

16 ריקרדו בן אוליאל ולירן חיים **דיני בנקאות – מערכת התשלומים** 359 (מהדורה שנייה, 2021)

17 שם.

18 ראו גור מגידו ״מעביר לך חצי מיליון שקל בביטקוין בלי קבלות, בלי עניינים״, אמר הסוחר וסינן: ״כ** אמא של מס הכנסה״ **The Marker** (16.7.2021) https://www.themarker.com/law/.premium.HIGHLIGHT-MAGAZINE-1.10002894.

19 ראו לדוגמה המאפיה האיטלקית Alex Vet, *Italian Mafia Launders Money through Crypto*, COINATORY (Apr. 6, 2019) bit.ly/2G0u1P8

20 ראו לדוגמה רפאל קאהן ״האקרים איראנים פרצו שוב למחשבי חברה ישראלית; ״לתקוע אצבע בעין״ **כלכליסט** (13.3.2021) https://bit.ly/3yMLx2e.

21 Brenna Smith, *The Evolution of Bitcoin in Terrorist Financing*, BELLINGCAT (Aug. 9, 2019) https://bit.ly/3ylcM2f.

nevo.co.il

מזאת, אנו עדים לעלייה בשימוש במטבעות אלקטרוניים לפשיעה כלכלית מסוגים שונים. לדוגמה, הלבנת הון[22] ותמיכה מהותית בטרור באמצעות מימון טרור.[23] עלייה זו נובעת, בין היתר, מירידה בשימוש בכסף מזומן באוכלוסייה הכללית, עובדה שהערימה קשיים בדרכם של המבקשים להלבין הון באמצעות מזומן.[24] האנונימיות של המשתמשים על גבי הבלוקצ׳יין מקשה על גורמי אכיפת החוק לזהות את המשתמשים ולעקוב אחר עסקאות לא חוקיות.

ככל שהאסדרה הנוגעת למניעת הלבנת הון ומימון טרור במערכת הפיננסית המסורתית משתפרת, כך גובר השימוש במטבעות אלקטרוניים לפשיעה.[25]

במלחמה בהלבנת הון ומימון טרור בשווקים פיננסיים מסורתיים מתקיים קונסנזוס כי מאחר שכסף הוא המנוע לפעילות הפלילית, יש ללכת בעקבות הכסף. גדיעת המימון היא כלי מרכזי לעצירת פשע ולמניעת פיגועי טרור. מתוך הבנה זו, אף קם בישראל כוח המשימה ״צלצל״ (הרפון) של המוסד. כוח זה נלחם בגורמים המניעים וממנים את הטרור תוך התמקדות בחיסולם של אנשי כספים הממלאים תפקידי מפתח בארגוני הטרור ובהחרמת הכסף המיועד לפעילות העבריינית. זאת, מתוך הבנה שהאסטרטגיה היעילה וארוכת הטווח ביותר בלוחמה בטרור היא ״לקטוע את הזרמת הכספים שישמשו לקניית נשק, לתשלום עבור חומרי נפץ, לשכירת מקומות מסתור, לאימון מתגייסים...״.[26] כך, במבצע ״שומר החומות״ הפציץ צה״ל את ״המוסד הפיננסי העזתי להשקעות והלוואות״ בעזה המשמש את מוסדות החמאס.[27]

מדינות פועלות למניעת טרור ופשיעה תוך כדי התמקדות, בין היתר, בעצירת הכסף המשמש למימון הפעילות האסורה. כחלק ממתווה פעולה זו נחקקו ברחבי העולם חוקים מפורטים האוסרים על מימון של פעילות טרור ופשיעה והמטילים על המתווכים הפיננסיים

22 *Crypto Money Laundering rises 30% Report Finds*, BBC NewsTech (Jan. 26, 2022) https://bbc.in/3bMzys9.

23 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 48.

24 להרחבה בדבר השפעות וירוס הקורונה על פשיעה פיננסית ראו COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses, FATF (2020) bit.ly/2M3MXzm, On the abuse of cryptocurrency for buying weapons and supporting crime see Brian Monroe, *In Pandemic Fraud, Cyber Fusillades, More Criminals Choosing Crypto to Buy Virtual Weapons, Get Paid After Successful Attacks: FinCEN* (May 15, 2020) bit.ly/3mHpws9; Money Laundering and COVID 19 Profits and Losses, UNODC (April 14, 2020) bit.ly/3rlxmLz ("Traditional cash-courier money laundering has been significantly reduced through ports and airports. It is unclear if Organized Criminals will seek alternative remittance methods for their criminal finances, such as cryptocurrencies or wire transfers, or await the reopening of borders").

25 ראו Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 29 המסבירים כי שימוש במטבעות אלקטרוניים צפוי לגבור ככל שיקבלו טכנולוגיה חדשה זו. אולם כיום, עדיין אין מכשירי כספומט אוטומטיים וקיוסקים שמאפשרים למשתמשים לרכוש מטבעות אלקטרוניים בשימוש במזומן או בכרטיסי חיוב.

26 מאיר דגן, שהיה אלוף בצה״ל ויועץ ראש הממשלה ללוחמה בטרור, הפך את איתור מקורות הממון של ארגוני הטרור למדיניות לאומית במטרה לרושש את ארגוני הטרור שאיימו על ישראל. ראו ניצנה דרשן לייטנר וסמואל מ. כץ **הרפון המלחמה החשאית בכספי הטרור** (2020).

27 אליאור לוי, יואב זיתון ״תיעוד: צה״ל מפציץ את ׳בנק הייצור׳ של חמאס בעזה״ **Ynet** (14.5.2021) https://bit.ly/3usUZoK.

nevo.co.il

בשוק ההון חובות פיקוח מוגברות על העברות כספים ודיווח על פעולות לא רגילות לחשבון.[28] זאת מתוך הבנה כי הטרור אומנם מונע מאידאולוגיה חברתית, כלכלית או דתית, אולם הוא גם זקוק למשאבים ואמצעים כלכליים על מנת להתקיים ולשגשג.[29] כך, נחקק בישראל חוק המאבק בטרור, התשע״ו–2016, המטיל חובת דיווח על עשיית פעולה ברכוש טרור או על פעולה אשר עשויה לקדם טרור.[30] עוד קודם לכן נחקק חוק איסור הלבנת הון, התש״ס–2000,[31] שמכוחו הוצאו צווים לאיסור הלבנת הון המכוונים לגופים פיננסיים כדוגמת צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), התשס״א–2001.[32] החוק והצווים שהוצאו מכוחו מטילים על גופים פיננסיים חובות בקרה שוטפת ודיווח לרשות לאיסור הלבנת הון ומימון טרור על פעולות מסוימות בחשבונות של לקוחות מעל לסכומים שנקבעו בצו או על פעולות בלתי רגילות המעוררות חשש להלבנת הון. מכוח חקיקה זו מוטל על מוסדות פיננסיים תפקיד ציבורי, מנהלי ואכיפתי, בהיותם הגורם העומד בחזית המאבק בהלבנת הון ומימון טרור, ואף קמה חובה על הבנקים לסרב לתת שירות בשל חשש מפעילות של מימון טרור או הלבנת הון.[33]

בעקבות חקיקה למאבק בטרור Counter Terrorism Financing (CTF), המתמקדת בזרימת הכספים דרך חשבונות בנק ומאפשרת מניעת עסקאות פיננסיות שיועדו לתמיכה במתקפות טרור ופעילות ארגוני טרור, אף התפתח ענף של תביעות והליכים משפטיים נגד בנקים שסיפקו שירותים והעבירו כספים לארגוני טרור.[34] בנוסף, התפתח תחום התמחות משפטי של תביעות

28 גיל לימון **המאבק בטרור בראי המשפט הבין־לאומי** 43 (2016); Joseph J. Norton & Hera Shams, *Money Laundering Law and Terrorist Financing: Post-September 11 Responses - Let Us Step Back and Take a Deep Breath*? 36 INTER'L LAWYER (ABA) 103,104 (2002). להרחבה על תחולת החוק למאבק בטרור על מוסדות פיננסיים בארצות הברית ראו Olivia G. Chalos, *Bank Liability Under the Antiterrorism Act: The Mental State Requirement Under § 2333(a)*, 85 FORDHAM L. REV. 303, 326 (2016).

29 עמיקם הרפז **אסטרטגיות שיטור – סוגיות בעיצוב מדיניות אכיפת החוק** (2012).

30 ראו ס׳ 33–34 לחוק המאבק בטרור, התשע״ו–2016, הקובעים חובת דיווח על רכוש טרור או על רכוש ארגון טרור מוכרז.

31 ראו ס׳ 7 לחוק איסור הלבנת הון, התש״ס–2000.

32 ראו רות פלאטו שנער ״הסודיות הבנקאית וחובת האמון על מזבח המלחמה בהלבנת הון – סקירה השוואתית״ **מאזני משפט** ג 253, 257 (2005).

33 רע״א 6582/15 **עמותת איעמאר לפיתוח וצמיחה כלכלית נ׳ בנק הדואר** (נבו 1.11.2015) (בנק הדואר קיבל מידע שחשבונות העמותה נסגרו מחשש למימון טרור וסירב לתת לה שירות פיננסי. נקבע כי מטילות על הבנק תפקיד ציבורי, מנהלי ואכיפתי, בהיותו הגורם העומד בחזית המאבק בהלבנת הון ומימון טרור).

34 לדוגמה, בנק לבנון־קנדה שניהל חשבונות של חיזבאללה בשם ״קרן השאהיד״ שהיוותה מרכיב חשוב במנגנון הכלכלי של חיזבאללה. תביעתו של הבנק התאפשרה בשל העובדה שבנק אמריקן אקספרס שהיווה בנק קורספונדנט שלו פעל במדינת ניו יורק. ראו הרפון, לעיל ה״ש 26, בעמ׳ 216. יצוין כי לעיתים, די היה באיום בתביעה נגד בנק ששימש צינור להעברת הכספים להביא לסגירת חשבונות של גורמים המסייעים לטרור. ראו שם, בעמ׳ 225.

nevo.co.il

שהגישו קורבנות טרור פרטיים נגד מוסדות פיננסיים על כך שלא מנעו העברת כספים לארגוני טרור ופשע.[35]

השילוב של הצווים, החקיקה והשימוש בחילוט לצורך עצירת כספים של ארגוני פשע וטרור יצר מצב שבו אותם פושעים וטרוריסטים מחפשים נתיבים חלופיים להעברה ולהלבנה של הכסף. שימוש גובר במטבעות אלקטרוניים אנונימיים בידי טרוריסטים ופושעים יכול לחתור תחת היעילות של פעולות למאבק בטרור ובפשיעה מאחר שמטבעות אלה הם מבוזרים. לפיכך, רגולטורים אינם יכולים לסמוך על שומר סף מרכזי או מתווך שיכול לזהות את הלקוחות ולעצור את זרימת הכסף למטרות לא חוקיות. טכנולוגיית הבלוקצ׳יין מאפשרת את תיעוד הבעלות וההעברה של המטבעות, אולם שמות הפרטים שמבצעים את ההעברות אינם רשומים בה. תחת זאת, הבעלות מיוצגת על ידי שילוב ייחודי של אותיות ומספרים המייצגים לציבור את ״כתובת״ משתמש המטבע. בשל תכונה זו, השימוש במטבעות אלקטרוניים מספק לטרוריסטים ולפושעים זרם של תשלומים בלתי מפוקחים, כאשר אין בנמצא כלים רגולטוריים משמעותיים לאיתור ומניעה של זרימת הכספים. המקרה של עלי שוקרי אמין שסיפק הוראות בטוויטר כיצד להשתמש בביטקוין כדי למסך את הוראת המימון לארגון המדינה האסלאמית הוא רק דוגמה אחת מני רבות המדגישה את הסיכונים שהאנונימיות הכרוכה בחלק מן המטבעות האלקטרוניים מציבה.[36]

בשל חשש להונאה, הלבנת הון ותרמית מול משקיעים ננקטה במדינות מסוימות כמו סין וצפון קוריאה גישה האוסרת על הסחר במטבעות אנונימיים לגמרי.[37] מדינות אחרות ניסו להבין יותר את השימוש במטבעות אלה כדי להגיע למדיניות קוהרנטית. אכן, יותר ויותר רגולטורים ברחבי העולם מודאגים מהשימוש במטבעות אלקטרוניים לפעילות לא חוקית כמו מימון טרור, הלבנת הון והתחמקות ממס.[38] מדינות ברחבי העולם פועלות על מנת לפתח רגולציה מדינתית שתסדיר את סוגיית האנונימיות במטבעות אלקטרוניים ברמה המדינתית ותצמצם אותה.[39] לאחרונה נעשה בישראל צעד ראשון להתמודדות עם האתגר כאשר ועדת

35 שם, בעמ׳ 223. לעניין זה אף הוקם בידי עו״ד ניצנה דרשן לייטנר ארגון ״שורת הדין״ שמטרתו העיקרית היא לרושש את הטרור, בין השאר באמצעות הגשת תביעות אלה.

36 ראו FATF Report, לעיל ה״ש 11.

37 Bloomberg News, China Widens Ban on Crypto Transactions; Bitcoin Tumbles, Bloomberg (Sept. 24,2021) https://bloom.bg/3yIPmFo; Hadar Y. Jabotinsky., *The Regulation of Cryptocurrencies: Between a Currency and a Financial Product*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 118, 120 (2020).

38 ראו Israel Klein, *Contemptuous Tax Reporting*, 2019 WIS. L. REV. 1161, 1169–70 (2019). ד״ר קליין מגדיר התחמקות ממס כהתחמקות ממיסוי אקטואלי שחבים אותו על ידי כך שלא מצייתים לחוק ומפירים אותו. ראו גם באום, לעיל ה״ש 2, בעמ׳ 297.

39 כך לאחרונה ממשל ביידן הוציא צו חדש ובו הוא מורה לרשויות רגולטוריות בממשל הפדרלי לפעול בשיתוף פעולה על מנת להסדיר את התחום – Executive Order on Ensuring Responsible Development of Digital Assets (March 9, 2022), https://bit.ly/3NKZYb9. בנוסף, קנדה הפעילה צווי חירום עקב הקורונה, וביניהם צו המורה לפלטפורמות להלוואות עמיתים להסדיר את נושא התשלום במטבעות קריפטוגרפיים שמתבצע על גבי הפלטפורמות: Sebastian Sinclair, Crypto Payment Systems Face New Restrictions Under Canada's Blockade Crackdown (Feb. 14, 2022) https://bit.ly/3Imlthl/.

nevo.co.il

החוקה של הכנסת אישרה את צו איסור הלבנת הון ומימון טרור בקשר לנותני שירותים פיננסיים, ובהם חברות המנהלות פלטפורמה לקנייה ומכירה של מטבעות אלקטרוניים.[40] הצו מותאם להוראות ארגון ה־FATF (Financial Action Task Force (on Money Laundering), ארגון בין־ממשלתי שמטרתו לקבוע כללים בנוגע למלחמה בהלבנת הון ובמימון טרור. הצו הישראלי מטיל חובות על נותני שירותים פיננסיים העוסקים במטבעות וירטואליים. כך, מטיל הצו חובה לבצע הליך ״הכר את הלקוח״ בכל פעולה מזדמנת מעל 5,000 ש״ח וחובה לרשום ולהעביר פרטי זיהוי של הצדדים בביצוע העברה של מטבע וירטואלי.[41]

בארצות הברית, משרד האוצר האמריקאי מתכנן ליצור דרישות דיווח חדשות,[42] שלפיהן שירותי ההמרה של המטבעות האלקטרוניים יידרשו לדווח יותר מידע על התזרים הנכנס והיוצא של הכסף שעובר דרך חשבונותיהם. בנוסף, יידרשו עסקים לדווח על עסקאות במטבעות אלקטרוניים מעל 10,000 דולר.[43] החוק החדש בארצות הברית לאיסור הלבנת הון,[44] שהעביר הקונגרס בראשית 2021, מרחיב את ההגדרות בחוק הסודיות הבנקאית (Bank Secrecy Act (BSA) של מוסדות פיננסיים כדי שיכללו גם עסקים שממירים מטבעות אלקטרוניים. לפי החוק, על שירותי ההמרה לאמת את זהות הצרכנים שלהם, להרכיב פרופילים של סיכון ללקוחותיהם, לעקוב אחר העסקאות ולהגיש דיווחים על פעילות לא רגילה.[45]

גם האיחוד האירופי ביקש לפתור את הבעיה של שימוש במטבעות אלקטרוניים למטרות לא חוקיות. בניסיון לעשות כן, תיקן לאחרונה האיחוד האירופי את הדירקטיבה להלבנת הון שלו. הדירקטיבה, בגרסתה החדש, מטילה חובות חדשות על שירותי המרה של מטבעות אלקטרוניים ועל החברות המספקות את ארנקי המטבעות האלקטרוניים לציית לאותן דרישות רגולטוריות כמו בנקים ושירותים פיננסיים אחרים.[46] נוסף על זה, בשנת 2021 הוצעה הצעה של המועצה האירופית לחזק את הרגולציה האמורה על ידי הוספת איסור מפורש על ארנקים אנונימיים למטבעות אלקטרוניים.[47] בשנת 2023 האיחוד האירופאי האירופאי קבע כללים חדשים המחייבים את כל מי שנותן שירותים בנכסים קריפטוגרפים לאסוף מידע על השולחים

40 צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של נותני שירותי אשראי למניעת הלבנת הון ומימון טרור) (תיקון), התשפ״א–2021, ראו בפרט סעיף 11.

41 ראו הודעה לציבור: פורסם ברשומות תיקון לצו איסור הלבנת הון שחל על נותני שירותים פיננסיים (24.3.21)https://bit.ly/3dRAIAN.

42 Department of the Treasury, The American Families Plan Tax Compliance Agenda (May, 2021) https://home.treasury.gov/system/files/136/The-American-Families-Plan-Tax-Compliance-Agenda.pdf.

43 שם.

44 The Anti-Money Laundering Act of 2020 H.R. 6395.

45 להרחבה ראו King & Spalding, *The Anti-Money Laundering Act and Crypto Collide*, Newstex Blogs (May 19,2021) kslaw.com/news-and-insights/the-anti-money-laundering-act-and-crypto-collide-non-fungible-tokens.

46 The 5th Anti-Money Laundering Directive (Directive (EU) 2018/843) (June 19, 2018).

47 *Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism rules,* European Commission, Press Release (July 20,2021) https://bit.ly/3rzfT2E (“[I]n addition, anonymous crypto asset wallets will be prohibited, fully applying EU AML/CFT rules to the crypto sector”).

nevo.co.il

והנהנים בטרנזקציות של מטבעות אלקטרונים ונכסים קריפטוגרפים, ללא קשר לגובה הסכום המועבר.[48]

אולם, הרגולציה המוצעת היא ברמה המדינתית, ואינה מייחסת מספיק משקל לעובדה שהשימוש במטבעות אלקטרוניים חוצה גבולות. ההתמקדות ברגולציה ברמה המדינתית עלולה לשמוט את הקרקע תחת יעילות הרגולציה ולאפשר המשך מימון טרור והלבנת הון באמצעות מטבעות אלקטרוניים. המאמר יציג מסגרת משפטית חדשה לקידום המשפט בנושא זה. לפיכך, המאמר יציע כי על הרגולציה שנוגעת לשימוש במטבעות אלקטרוניים וסוגיית האנונימיות בפרט להיות גלובלית ובין־לאומית באמצעות הרחבת השימוש באמנות בין־לאומיות העוסקות בתחום אכיפה של פשיעה כלכלית, כך שיכלול גם מטבעות אלקטרוניים ושיתוף פעולה שוטף שיתאפשר באמצעות ארגונים בין־ממשלתיים דוגמת ה־FATF.[49] המחקר יציע כי ההסדרה הבין־לאומית תכלול הטלת חובות על חברות שמנפיקות מטבעות אלקטרוניים, מאפשרות מסחר בהם או מפתחות את הארנקים האלקטרוניים שבהם נשמרים המטבעות האלקטרוניים. החובה העיקרית שיכולה לסייע במלחמה במימון טרור והלבנת הון היא לאמת את הזהות של המשתמשים הפועלים על גבי הבלוקצ׳יין ולהכיר את הלקוחות כדי להפחית שימוש עתידי לא חוקי במטבעות אלה. כך נוכל לנתק את הספקת החמצן המאפשרת פעילות לא חוקית. בכך נצעד צעד נוסף מעבר ליוזמות חקיקה קיימות, שמתמקדות ברמה המדינתית ומתייחסות ברובן לנקודות הקצה, ולא לאימות על גבי הבלוקצ׳יין. הבעיה בהתמקדות בשלב שבו המטבע האלקטרוני מומר ממטבע אלקטרוני לנכס פיננסי אחר (כמו מטבע מדינתי למשל) היא שאין לנו אפשרות לדעת אם לא נעשו במטבע האלקטרוני פעולות אסורות עד שהוא מומר למטבע אחר.

לפי הצעתנו, רישום משתמשי המטבע לא יהיה גלוי לכל, אלא הכוונה היא כי החברות שעליהן יוטלו החובות יצטרכו לוודא ולרשום את זהות המשתמשים וזהותם תוכל להיחשף רק באמצעות צו בית משפט שיאשר את החשיפה. בית המשפט יהיה רשאי להוציא צו ולהורות על חשיפת זהותו של המשתמש המחזיק בארנק שדרכו נעשו הפעולות במקרים שבהם מתעורר חשש של ממש שפעילות של משתמש במטבעות אלקטרוניים משמשת או מסייעת לפשיעה או לתמיכה בטרור. בדרך זו יוכלו רשויות החוק לעקוב אחרי הכספים הבלתי חוקיים גם כאשר הפעולות מתבצעות על גבי רשת הבלוקצ׳יין דרך מטבעות אלקטרוניים, ולא רק כאשר המטבע האלקטרוני מומר למטבע אחר.

מבנה המאמר הוא כדלהלן: **החלק הראשון** יסקור את תפקידם של המתווכים כשומרי הסף החדשים מפני הפרות דין של משתמשים ולקוחותיהם. הוא יתייחס לרגולציה המסורתית החלה

48 לכללים באיחוד האירופי שנקבעו בשנת 2023 ראו Council of the EU Press Release, Anti-Money Laundering: Council Adopts Rules Which Will Make Crypto-Asset Transfers Traceable (May 16, 2023) https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable.

49 Financial Action Task Force (on Money Laundering) (FATF), ארגון בין־ממשלתי שמטרתו לפתח מדיניות בנוגע למלחמה בהלבנת הון ובמימון טרור.

נבו nevo.co.il

על מתווכים פיננסיים למלחמה בהעברת כספים למטרות לא חוקיות. הוא יסביר כי המאה ה־21 יצרה מודל פלורליסטי, שזכה לכינוי "בית הספר החדש של הרגולציה", שכולל הרבה שחקנים שונים. מודל זה מתואר בהפשטה באמצעות משולש של שחקנים: המדינה, התשתית שמאפשרת הפרות דין והמפר.[50] בחלק זה של המאמר נפרט דוגמאות למודל זה ונסכם עם תיאור של חקיקת איסור הלבנת הון והמאבק בטרור אשר חלה על שומרי סף פיננסיים מסורתיים.

החלק השני בוחן את תכונות המטבעות האלקטרוניים וטכנולוגיית הבלוקצ'יין שעליה הם פועלים. חלק זה של המאמר מתמקד בבלוקצ'יין של ביטקוין ואת'ריום ומסביר שבשל המבנה המבוזר של הבלוקצ'יין והאנונימיות של מחזיקי המטבע, לעת עתה אי אפשר לאסדר את העסקה המתבצעת על גבי הבלוקצ'יין כשלעצמה. האנונימיות של העסקה בשילוב עם העובדה שהיא מתבצעת על גבי הבלוקצ'יין, שהיא כאמור טכנולוגיה מבוזרת, מאפשרת את השימוש במטבעות האלקטרוניים לשימושים לא חוקיים. חלק זה יתמקד בשימוש במטבעות האלקטרוניים לשם סיוע לטרור כמקרה מבחן ויטען כי בהיעדר רגולציה משמעותית, יציב הטרור איום גדול יותר לביטחון הלאומי ולביטחון הציבור.

החלק השלישי יציע לפתור את הבעיה של שימוש במטבעות אלקטרוניים לביצוע עבירות באמצעות מעבר מרגולציה מדינתית לרגולציה גלובלית בין־לאומית לאור השימוש חוצה הגבולות במטבעות האלקטרוניים. רגולציה זו, שתתאפשר באמצעות אמנות בין־לאומיות ושיתוף פעולה שוטף באמצעות ארגונים בין־ממשלתיים, תטיל חובות על חברות המטבעות הקריפטוגרפיים לרשום ולאמת את זהות בעלי המטבע הפועלים על גבי הבלוקצ'יין אצל החברות המנפיקות, שירותי ההמרה וספקי הארנקים. מודל זה של רישום המשתמשים הפועלים על גבי הבלוקצ'יין ואימות זהותם נוהג כבר ברשת בלוקצ'יין פרטית (permissioned (private) blockchains), כמו לדוגמה המטבע המדובר של פייסבוק – Diem (לשעבר "ליברה"), שנגנז לאחרונה. הדיאם נועד לתפקד ולהיות מוחלף על גבי רשת מורשית.[51] ברשתות מורשות קיימת שכבת גישה ושליטה נוספת כדי לקבוע למי תהיה גישה לרשת. בעל המטבע ברשת זו אמור היה להיות מאומת על ידי בעל הרשת. המאמר יציע לאמץ את ההסדר האמור ולקלוט אותו ברמה הגלובלית הבין־לאומית לכלל המטבעות האלקטרוניים. רגולציה כזו תאפשר ללחום במימון טרור ובהלבנת הון באמצעות מטבעות אלקטרוניים ביעילות, מאחר שההסדרה תהיה גלובלית ותקבע סטנדרטים מינימליים שיוטלו על חברות המטבעות האלקטרוניים. החובות כאמור יתמקדו באימות שמות המשתמשים הפועלים על גבי הבלוקצ'יין ובחשיפת המשתמש במטבע כאשר מתקיים חשש של ממש לביצוע עבירה. חשיפת בעל המטבע תהיה כפופה לצו בית משפט. העובדה שהחשיפה נעשית בכפוף לצו למעשה מאזנת את האינטרס של ביטחון לאומי עם הזכות לאנונימיות כנגזרת של הזכות לפרטיות[52] ואף מהווה איזון ראוי מול הזכות

50 ראו בהקשר משיק של עבירות ועוולות ביטוי Jack M. Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011 (2018).

51 libra.org/en-US/; The Libra White Paper: libra.org/en-US/white-paper/#cover-letter.

52 מיכאל בירנהק **מרחב פרטי** 318 (2010).

nevo.co.il

לחופש ביטוי[53] וצמצום אפקט מצנן על ביטוי ופעילות בהיעדר אנונימיות. הטלת חובה על חברות המנפיקות או המאפשרות את הסחר או את החזקת המטבעות האלקטרוניים היא מוצדקת, מאחר שחברות אלה מרוויחות מסחרית מהשימוש במוצריהן הפיננסיים.

החלק הרביעי מתייחס לביקורות אפשריות למתווה המוצע: פגיעה בפרטיות ובחופש הביטוי, פגיעה בביזוריות ופגיעה בשימוש במטבעות אלקטרוניים, עלויות מנהליות ובעיות של אבטחת מידע. נסכם כי אף רפורמה משפטית אינה חפה מקשיים וחסרונות, ועל אף הקשיים, העלויות והסיכונים באימות זהות מחזיק המטבע וחשיפת זהותו במקרה של חשש של ממש לעבירה מוצדקים בעינינו ועומדים בהלימה לעקרונות חוקתיים.

א. מתווכים כשומרי סף — רגולציה של מתווכים לקידום מלחמה בהפרות דין

רגולציה מסורתית (old-school) מטילה עונשי מאסר או קנסות כדי להסדיר או לשלוט בהפרות דין.[54] סוג זה של רגולציה הוא "דיאדי".[55] במודל זה יש שני שחקנים: המדינה ומפר הדין.[56] מודל זה התאים לעולם ישן יותר שבו אכן התקיים מיעוט של שחקנים, אולם במאה ה־21, העולם השתנה לכזה שכולל מספר רב של שחקנים ומודלים מורכבים של פעילות. עובדה זו הביאה לצורך במודל פלורליסטי שכולל חברות שעומדות במרכז הכלכלה ומספקות תשתית שמאפשרת פעילות חוקית ולא חוקית כאחת. מתווי המדיניות רתמו את המתווכים הפיננסיים בשוק ההון המסורתי, כמו לדוגמה מתווכים מקוונים, חברות טכנולוגיה, מתווכים פיננסיים ומתווכי תשלום, לאסדר את הפעילות שהם מאפשרים. רגולציה זו, שחוסה פעמים רבות תחת כנפי המשפט המנהלי, מגייסת דה פקטו חברות פרטיות לאכיפת המשפט הציבורי.[57] אולם, במקרים רבים, רגולציה זו נכפית על חברות שמספקות תשתית לעוולות אזרחיות, או עבירות פליליות, מבלי שהן רצו בכך.[58] פרופסור בלקין (Balkin) תיאר אכיפה זו כ"בית הספר החדש

53 ראו בהקשר משיק על הזכות לאנונימיות כמאפשרת ביטוי רע"א 4447/07 **מור נ' ברק אי.טי.סי. [1995] החברה לשרותי בזק בינלאומיים בע"מ**, פ"ד סג(3) 664 (2010).

54 Michal Lavi, *Do Platforms Kill?*, 43 HARV. J.L. & PUB. POL'Y 477, 505 (2020).

55 Balkin, לעיל ה"ש 50, בעמ' 2014 מתייחס להקשר משיק של רגולציה של ביטוי.

56 שם, בעמ' 2013.

57 Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467 (2020), מתייחס לעליית התופעה של חברות אוכפות רגולציה. ראו גם Rory Van Loo, *The Revival of Respondent Superior and Evolution of Gatekeeper Liability*,109 GEO. L.J 141, 172 (2020) ("new gatekeeper governance paradigm is propelling some businesses into higher control relationships, thereby making it more likely courts will see them as principals under the common law").

58 ראו לדוגמה בתחום של עבירות מחשב Thomas E. Kadri, *Digital Gatekeepers*, 99 TEXAS L. REV. 4 (2021) "[U]nder cyber-trespass laws like the CFAA, some courts have treated platforms as digital gatekeepers—as property owners that may permit and restrict access to their websites much like landowners may do with private land in the real world".

nevo.co.il

של הרגולציה״ (“the new-school regulation”).[59] במאמריו התמקד בלקין בתפקידו של מודל זה ברגולציה שמאסדרת ביטויים המועלים על פלטפורמות שאותן מספקות חברות תשתית כמו ספקי שירותי אינטרנט, אתרי אינטרנט שמארחים תוכני משתמשים (ספקי תוכן) ואפילו מנועי חיפוש.[60] התשתית שחברות אלה מספקות מאפשרת אכיפת הפרות דין. המודל כולל כמה שחקנים, אבל אפשר לתאר אותו כמשולש של שחקנים: המדינה, מפר הדין והתשתית שמשמשת כשומר סף. הפרות דין מתבצעות פעמים רבות תחת מסך של אנונימיות, לעיתים הן מגיעות מפרטים אשר מצויים במדינה אחרת, עובדה המקשה על אכיפת החוק באשר לעבירות או העוולות שאותן ביצעו. מפירים אלה מציבים אתגר לאכיפת החוק. כדי להתמודד עם אתגר זה ולהפחית את הנזק שנגרם על ידי אותם מפירים, האכיפה נסמכת על מתווכים שמספקים את התשתית לפעילות המפירה ומאפשרים אותה.[61] לדוגמה, כאשר אוכפי החוק מבצעים חקירה לגבי עבירה שבוצעה, דרישות משפטיות מופנות כלפי צדדים שלישיים, פרטים ועסקים שלמעשה שימשו רק כתשתית על ידי מי שחשוד בעבירה.[62] כך, חובות משפטיות ואחריות נכפות על הגורמים שסיפקו את התשתית להפרות של צד שלישי. חובות אלה הן תמריץ חזק עבור גורמים אלה להביא לצמצום נזקיהן של עבירות ועוולות והן מבטיחות שיתוף פעולה של חברות אלה עם גורמי אכיפת החוק. מאחר שחברות שמספקות את התשתית לפעילות במרחב הדיגיטלי ממוקמות בצוואר הבקבוק להתערבות רגולטורית, הן בעמדה הטובה ביותר לפעול להסדרה ואף הוגדרו בספרות כמושלות בביטוי המקוון.[63] הטלת חובות על ספקי התשתית והתוכן לפקח ולהסדיר את הפעילות של משתמשיהן נראית טבעית. היא אף מאפשרת פעמים רבות ממשל יעיל בביטוי מזיק באמצעות הסדרה פרטית של תכנים ואכיפת תנאי השימוש ומדיניות הקהילה בידי הפלטפורמות ומחזקת במקרים רבים את הביטחון הלאומי (למשל כשמסירים ביטויים שמעודדים להסתה או לפעולות טרור).

59 Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 Harv. L. Rev. 2296, 2297–2299 (2014); Jack M. Balkin, *Free Speech Versus the First Amendment*,UCLA L. Rev. (forthcoming) (at 7) *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4413721, בלקין התמקד בתפקיד מודל זה לרגולציה של ביטוי והסביר כי מדינות עושות מאמצים להסדיר, לכפות או לשתף פעולה עם שחקנים מרכזיים כדי לעצב את האינטרנט כדי לקבל תשתית למעקב, שיטור ושליטה בביטוי.

60 ראו לדוגמה ה״זכות להישכח״ באיחוד האירופי שהתבססה בפסק דינו של בית הדין האירופי לצדק שאפשר לחייב מנועי חיפוש להסיר מתוצאות החיפוש מידע שקרי או לא רלוונטי. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014); Michal Lavi, *The Good, The Bad and the Ugly Behavior*, 40 Cardozo L. Rev. 2597, 2630 (2019).

61 ראו בהרחבה Aniket Kesari, Chris Hoofnagle & Damon McCoy, *Deterring Cyber Crime Focus on Intermediaries* 32 Berkeley Tech L.J. 1093, 1131 (2017).

62 שם, בעמ׳ 1096.

63 Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*,131 Harv. L. Rev. 1598, 1603(2018) (“platforms should be thought of as operating as the New Governors of online speech”).

nevo.co.il

לאחרונה עלה לכותרות בישראל תפקיד המתווכים כאוכפי חוק פרטיים באפיק וולונטרי[64] בעניין **עדאלה נ׳ פרקליטות המדינה, יחידת הסייבר**,[65] שם נדונה עתירה שהגישה עדאלה בהצטרפות התנועה לחופש המידע (שהצטרפה כידיד בית המשפט) ועסקה בעניין האכיפה האלטרנטיבית במסלול הוולונטרי של יחידת הסייבר בפרקליטות המדינה, אשר כוללת פנייה אל פלטפורמות ומנועי חיפוש כגון פייסבוק וגוגל, בבקשה להסיר אלפי תכנים בשנה או להגביל גישה אליהם, ולעיתים גם להשעות משתמשים ואף להרחיקם. פעילות זו נעשתה, כך נטען, ללא סמכות משפטית ולרוב אף ללא ידיעת המפרסם. העותרים טענו כי מנגנון ״האכיפה האלטרנטיבית״ פוגע קשות בזכויות החוקתיות לחופש הביטוי ולהליך הוגן, וזאת ללא הסמכה בחוק ומבלי לעמוד בתנאי פסקת ההגבלה. בפסק הדין קבע בג״ץ כי פעילות מחלקת הסייבר ״חיונית לשמירה על הביטחון הלאומי והסדר החברתי״[66] וכי למרות שהאופן הוולונטרי שבו פועלת מחלקת הסייבר אינו חף מקשיים בשל היעדר הסמכה לכך בחקיקה, היא תוכל להמשיך לפעול כך גם טרם שחקיקה כזו תתקבל. השופט מלצר הגדיר הסדר זה כ״רגולציה הופכית״, שבמסגרתה אכיפת החוק ואסדרת מערכת היחסים בין השחקנים השונים בשוק (המדינה, המשתתפים ברשתות החברתיות ומפעילי הפלטפורמות המקוונות עצמם) נעשות ״כאשר המדינה ממלאת תפקיד של גורם מדווח, המפנה את דבר קיום ההפרות לכאורה – לעיונם ולהחלטתם של מפעילי הפלטפורמות המקוונות, מסגרת פעילות זו, שניתן לכנותה ״רגולציה הופכית״, שכן ההחלטה הסופית היא בידי מפעילי הפלטפורמות המקוונות״.[67] דחיית העתירה העניקה למעשה משנה תוקף למודל זה.

תפקיד המתווכים כאוכפי חוק פרטיים בא לידי ביטוי לא רק באפיק וולנטרי, אלא שהם נרתמו על ידי הדין הפורמלי גם לצורך ביצוע פעולות אכיפה דרך דיני האחריות למעשי צדדים שלישיים. לדוגמה, הרגולטורים רותמים את מתווכי התוכן להסדרה ואכיפה כנגד ״ביטוי מזיק״.[68] אפילו בארצות הברית, שבה מתווכים נהנים מחסינות לתוכן שהופץ על ידי ספק תוכן אחר,[69] מתווכים פועלים להסרת תכנים מזיקים בצל איום בשינויי חקיקה פוטנציאליים שעלולים להגביל את האוטונומיה שלהם להביא לרגולציה עצמית של השיח בפלטפורמות

64 חיים ויסמונסקי ״הפללה של התנכלות מקוונת ומקרי המבחן של התנכלות כלפי עובדי ציבור וקטינים במרחב המקוון״ **משפט ועסקים** כג 345, 406 (2020); חיים ויסמונסקי ״אכיפה אלטרנטיבית של עבירות ביטוי במרחב הסייבר״ **משפט, חברה ותרבות: משפט צדק? ההליך הפלילי בישראל – כשלים ואתגרים** 691, 711 (2017).

65 בג״ץ 7846/19 **עדאלה המרכז המשפטי לזכויות המיעוט הערבי בישראל נ׳ פרקליטות המדינה יחידת הסייבר** (נבו 12.4.2021).

66 שם פס׳ 72 לפסק דינו של השופט מלצר.

67 שם, פס׳ 49.

68 Elena Chachko, *National Security by Platform*, 25 STAN. TECH. L. REV. 55, 83 (2021).

69 Section 230(c)(1) of the Communications Decency Act (CDA)(47 U.S.C. § 230 (2018)); JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 246 (2019); Eric Goldman, *Why Section 230 Is Better than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33 (2019); Michal Lavi, *Content Providers' Secondary Liability: Asocial Network Perspective*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L. J 855, 889 (2016).

nevo.co.il

שבבעלותם.[70] במדינות רבות מחוץ לארצות הברית מתווכים יכולים לשאת באחריות לכשל להסיר ביטוי המסית לטרור,[71] ביטויי שנאה,[72] ביטויי לשון הרע[73] ואפילו באשר לכשל להסיר חדשות כזב.[74] גם בארץ הדין רותם את המתווכים לאכיפת הפרות דין שביצעו צדדים

70 ראו Michal Lavi, *Targeting Exceptions,* 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 65 (2021).

71 ראו M.R. Leiser & Edina Harbinja, *Content Not Available, Why The United Kingdom's Proposal For A "Package Of Platform Safety Measures" Will Harm Free Speech*, TECH. REG. 78 (2019). לביקורת ראו Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1043–1045 (2018). יצוין שלאחרונה, האיחוד האירופי התווה חקיקה באשר לביטויי טרור באינטרנט, אשר דורשת מפלטפורמות אינטרנטיות להסיר תוכני טרור מהר ולאמץ אמות מידה פרואקטיביות למנוע את ההפצה של תוכני טרור לכתחילה. ראו Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online ("TERREG"); Hannah Bloch-Wehba, *Content Moderation as Surveillance,* 36 BERKELEY TECH L.J. 117 (2021).

72 ב־2017, הממשל הגרמני ניסח את Network Enforcement Act (NetzDG) כדי לתת מענה לבעיה הגוברת של ביטויי שנאה. החוק חל באשר לביטוי פלילי שפוגע והוא מוגדר ב־ German Penal Code ככזה שכולל גם לשון הרע. החוק קובע לוח דיפרנציאלי להסרת תוכן מזיק בידי המתווכים. אלה צריכים להבטיח את הסרת התכנים מפירי הדין תוך 24 שעות מרגע שהוגשה תלונה. להרחבה ראו Act] Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [NetzDG] [Act to Improve Enforcement of the Law in Social Networks], Oct. 1, 2017, NETZWERKDURCHSETZUNGSGESETS VOM 1 at § 3(2)(4) (Ger.); Wolfgang Schulz, *Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG*, *in* PERSONALITY AND DATA PROTECTION RIGHTS ON THE INTERNET 289 (2022); Meg Leta Jones, *Silencing Bad Bots: Global, Legal and Political Questions for Mean Machine Communication*, 23 COMM. L. & POL'Y 159, 177 (2018); Evelyn Mary Aswad, *The Future of Freedom of Expression Online*, 17 DUKE L. & TECH. REV. 26, 43 (2019). מתייחסת לאימוץ כללי התנהגות נגד ביטויי שנאה על ידי רוב התאגידים אונליין כדי לעמוד בסטנדרטים שהוצעו על ידי האו״ם לעניין זה)

73 ראו לדוגמה Delfi AS v. Estonia, Eur. Ct. H.R. App. No. 64569/09, 43 (Grand Chamber 2015). בית הדין האירופי לזכויות אדם קבע שהאתר הפופולרי דלפי אחראי ללשון הרע שפורסם בו על איש עסקים מאסטוניה, זאת בעקבות תגובות שהופיעו למאמר מערכת שפורסם באתר. בית הדין האירופי לזכויות אדם קבע שדלפי אחראי אפילו שהסיר את התגובות בעקבות ידיעה. ראו גם ECJ Judgment in Case C-18/18 Eva Glawischnig-Piesczek v. Facebook Ireland Limited (Oct. 3, 2019) (בית הדין האירופי לצדק באיחוד האירופי קבע שעל פייסבוק להסיר תוכן מזיק ואף תכנים זהים ואקוויוולנטיים לאותו התוכן לאחר שנקבע שהוא מפר דין). להרחבה ראו מיכל לביא ״מהודעה והסרה לחובת סינון תכנים? בעקבות פס״ד של בית הדין האירופי לצדק בעניין פיסזק״ **JOKOPOST (6.11.2019)** https://tinyurl.com/y4t6gl3p.

74 ראו לדוגמה חקיקה חדשה בסינגפור שמאפשרת לממשל להורות למתווכים להסיר תוכן שקרי. For example, Singapore allows the government to order intermediaries to remove false statements. Bill No. 10/2019 Protection from Online Falsehoods and Manipulation Bill bit.ly/30hacIC. Part four of the law refers to directions to internet intermediaries and providers of mass media services. ראו Jason Luger, *Planetary Illiberalism and the Cybercity-state: in and Beyond Territory*, *in* TERRITORY, POLITICS, GOVERNANCE 1 (2019); להרחבה ראו Niharika Mandhana & Phred Dvorak, *Ordered by Singapore, Facebook Posts*

נבו nevo.co.il

שלישיים. לעניין זה הוצעה בעבר הצעת חוק מסחר אלקטרוני[75] במטרה לרתום את המתווכים להסרת תכנים מזיקים במישור האזרחי, לדוגמה תוכני לשון הרע ותכנים מפירי קניין רוחני. במסגרתה, הוצע להכפיף מתווכים למשטר של "הודעה והסרה". משמעות משטר מעין זה היא שלמתווך יוענק פטור מאחריות אם מילא את חובותיו לטפל בתלונות על תכנים אלה בפלטפורמה.[76] המתווך לא יהא חשוף לאחריות בגין אי־סינון תכנים מזיקים מיוזמתו. אולם מתווך שלא יטפל בתלונות בעניינם יחויב באחריות אם ייקבע שהתכנים הם לשון הרע. הצעה זו לא השתכללה לכדי חוק. אולם הפסיקה בערכאות הנמוכות לעיתים הטילה אחריות על מתווכים לעוולת הרשלנות, לדוגמה בגין מחדל למנוע עוולות ביטוי או לצמצם את נזקיהן.[77]

דוגמה שנייה היא אכיפה חלופית לאפיק הפורמלי של הדין הפלילי, שמתבצעת בידי המתווכים כאוכפי חוק פרטיים. אכיפה זו ממוקדת בעיקרה בתוכן, ופחות במבצעי העבירות עצמם. מטרת אכיפה זו היא לצמצם את החשיפה לתוכן המזיק עצמו באמצעות חסימת גישה, סינון, הסרת התוכן המזיק וניתוק המשתמש שהפר את הדין.[78] חוק הגנת הפרטיות וחוק איסור לשון הרע, התשכ"ה–1965 אפשרו, בצד נקיטת הליכים פליליים (או אזרחיים) נגד המפרסם, לדרוש הן מהמפרסם והן מספקית הגישה או השירות להסיר את התוכן.[79] לעניין זה אף הסביר ד"ר חיים ויסמונסקי כי אסטרטגיית האכיפה החלופית כלפי עבירות פליליות במרחב הסייבר קודמה בעת האחרונה במידה ניכרת, עם כניסתו לתוקף של חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע"ז–2017, אשר מקנה למדינה כלים לאפשר התמודדות עם תופעות של פרסומים לא חוקיים באינטרנט באמצעות צווים שיפוטיים שיוצאו בידי שופט

a Correction, THE WALL STREET JOURNAL (Nov. 30, 2019) on.wsj.com/2L9FU4P, להרחבה על חקיקה שרותמת מתווכים למלחמה בחדשות כזב באסיה ראו *The Rise of "Fake News" Laws Across South East Asia*, PUBLIC MEDIA ALLIANCE (Dec, 6, 2019) bit.ly/2Xbl3TO.

75 ס' 10 להצעת חוק מסחר אלקטרוני, התשס"ח–2008, ה"ח הממשלה 356. ההצעה הוגשה שנית שלוש שנים לאחר מכן. ראו הצעת חוק מסחר אלקטרוני, התשע"א–2011, פ/3418/18.

76 ראו מיכאל בירנהק **מרחב פרטי – הזכות לפרטיות בין משפט לטכנולוגיה** 379 (2010). הוא מסביר כי המשטר שהוצע הוא "הודעה, הודעה והפניה לבית המשפט". במשטר זה האתר אינו צריך לפקח על התכנים מראש ואינו צריך למהר ולהסיר את התוכן עם קבלת ההודעה. תפקידו לשמש מתווך בין המתלונן לגולש הפוגע. לאחר קבלת תלונה מצד הנפגע נדרש המתווך להעבירה לידי הפוגע לכאורה. אם אינו מגיב, או אינו מסכים להסרה, יוסר התוכן. ביתר המקרים יישאר על כנו.

77 אפשר להטיל אחריות לעוולת הרשלנות בגין מחדל רשלני למנוע עוולת ביטוי או מחדל להסיר ביטויים משמיצים בכפוף להוכחת יסודות האחריות לעוולה (התרשלות, קשר סיבתי ומסננת שיקולי מדיניות). ע"א 4486/11 **פלוני נ' פלוני** (נבו 15.7.2013); ישראל גלעד **דיני נזיקין – גבולות האחריות** 420 (2012); על האפשרות להטלת אחריות מוגבלת מכוח עוולת הרשלנות ראו ע"א 9183/09 **The Football Premier League Association Ltd. נ' פלוני**, פס' 4 לפסק דינו של השופט הנדל (נבו 13.5.2012) להרחבה ראו מיכל לביא "התפשטות שמועות לשון הרע ברשתות: הצעות לפעולה" **חוקים** יג 59, 93 (2020).

78 ויסמונסקי "הפללה של התנכלות מקוונת", לעיל ה"ש 64, בעמ' 404–405.

79 שם, בעמ' 405; ס' 9(א)(1) לחוק איסור לשון הרע, התשכ"ה–1965; ס' 29(א)(1) לחוק הגנת הפרטיות, התשמ"א–1981.

nevo.co.il

מחוזי.[80] אסטרטגיה זו גם מקודמת לאחרונה, כך למשל אישרה ועדת השרים לחקיקה את הצעת החוק למניעת הסתה ברשתות החברתיות,[81] אשר מבקשת להסמיך שופט מחוזי לתת צווים שיפוטיים אשר יחייבו בעלי אתר אינטרנט להסיר תוכן על פי בקשת פרקליטות המדינה. על פי ההצעה, השופט אף יוכל לחייב מנוע חיפוש להסיר את התוכן מתוצאות החיפוש. עוד על פי ההצעה, צו יינתן אם בית המשפט סבור כי הפרסום מהווה עבירה פלילית וכי קיימת אפשרות ממשית שהמשך פרסומו יפגע בביטחונו של אדם מסוים, בביטחון הציבור או בביטחון המדינה. דיון יתקיים בתוך 48 שעות.[82] נציין כי על הצעת החוק נמתחה ביקורת, מאחר שהיא עלולה לפגוע פגיעה שאינה מידתית בחופש הביטוי ובזכות להליך הוגן.[83]

דוגמה שלישית לרתימת המתווכים לאכיפת החוק היא אכיפת הפרות זכויות יוצרים. ככלל, תחת הדירקטיבה האירופית למסחר[84] והתיקונים המוצעים לה בהצעת חוק השירותים הדיגיטליים, אשר אושר לאחרונה בפרלמנט האירופי[85] ועתיד להיכנס לתוקף ב־2024,[86] חוק

80 ויסמונסקי ״הפללה של התנכלות״, לעיל ה״ש 64, בעמ׳ 405–406; ויסמונסקי ״אכיפה אלטרנטיבית של עבירות ביטוי במרחב הסייבר״, לעיל ה״ש 64, בעמ׳ 719–720.

81 הצעת החוק למניעת הסתה ברשתות החברתיות, התשפ״ב–2021.

82 ראו ס׳ 2 להצעת החוק.

83 ראו התנגדות לטיוטת החוק למניעת הסתה ברשתות החברתיות, התשפ״ב–2021 (המכון הישראלי לדמוקרטיה ואיגוד האינטרנט הישראלי 23.12.2021) https://bit.ly/3OOWl5c וכן ראו דנה יפה ״חוק הפייסבוק לא יועיל הרבה, אך יפגע בחופש הביטוי״ **העין השביעית** (4.1.2022) https://bit.ly/3utSpib.

84 The European Union Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) 2000 O.J. (L 178) 1. (July 17, 2000). *See* Article 14(1).
יצוין כי האיחוד האירופי כופה חובות נוספות על מתווכים באשר להפרות זכויות יוצרים מעבר למשטר הודעה והסרה ב־Copyright Single Market Directive. ראו Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (June 7, 2019) (The “Copyright Digital Single Market Directive”) Art 17 of the Copyright Single Market Directive.

85 EFF Statement on EU Parliament’s Adoption of Digital Services Act and Digital Markets Act, EFF (July 5,2022) https://bit.ly/3NR7tNM.

86 ראו European Commission, 15 December 2020, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC,Document COM (2020) 825 final 2020/0361. Section 2 of the DSA. Ch. II; Art 5 “Where an information society service is provided that consists of the storage of information provided by a recipient of the service the service provider shall not be liable for the information stored at the request of a recipient of the service on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content”.

nevo.co.il

המילניום בארצות הברית[87] ומשטר "הודעה והסרה" הנוהג בארץ, אף שלא השתכלל לדבר חקיקה,[88] מתווכים נהנים מנמל מבטחים אם הם נקטו צעדים מסוימים לאכיפת זכויות יוצרים והגיבו לבקשות הסרת תכנים מפרים שהגישו בעלי זכויות יוצרים. כך, למעשה, המתווכים אוכפים את זכויות היוצרים בפלטפורמה שלהם.[89] אולם, אי־ציות לבקשות ההסרה עלול להוביל לאחריות שילוחית להפרות זכויות יוצרים כאשר התוכן מפר זכויות יוצרים.

דוגמה רביעית היא רתימת מתווכי תשלום כמו ויזה ומאסטרכרט, אשר מאפשרים סליקת תשלום, לסיוע באסדרת הפעילות על הפלטפורמה. סליקת אשראי מאפשרת לאתרים לא חוקיים כמו אתרי הימורים ללא רישיון או אתרים שעוסקים בהונאה לקבל תשלום עבור השתתפות בפעילות לא חוקית ומזיקה. בחלק מהמקרים מתווכים יוזמים וולונטרית את מניעת מעבר התשלום,[90] ובחלק מהמקרים הם פועלים לפי איסורים רגולטוריים. לדוגמה, הרגולטור הטיל איסורים על חברות האשראי המאפשרות שירותי סליקה לאשר עסקה אם על פי המידע שמצוי בידי חברת כרטיסי האשראי קיים חשש כי העסקה היא בגין "משחק אסור", "הגרלה" או "הימור" כהגדרתם בחוק העונשין.[91] סליקת עסקאות אלה ביודעין היא פעולה בניגוד לאיסורים אלה ובמקרים מסוימים אף יכולה להוביל לאחריות פלילית.[92] בארצות הברית בולט תפקידם של מתווכי תשלום אלה באכיפת זכויות בקניין רוחני והפחתת הפרות על ידי התמקדות בנתיב המעבר של הכסף שעובר לסוחרים במרחב המקוון, שמרוויחים מפעילות לא

87 17 U.S.C. § 512 (2012); Digital Millennium Copyright Act (DMCA).

88 ס' 10 להצעת חוק מסחר אלקטרוני, התשס"ח–2008, ה"ח הממשלה 356. ההצעה הוגשה שנית שלוש שנים לאחר מכן. ראו הצעת חוק מסחר אלקטרוני התשע"א–2011, פ/3418/18. לעניין החלת משטר הודעה והסרה על הפרת זכויות יוצרים ראו מיכל לביא **אחרית מתווכי תוכן לעוולות ביטוי, הקשר חברתי משפט וטכנולוגיה** 156, 160 (2018).

89 Jacqueline Lipton, Rethinking Cyberlaw – A New Vision for Internet Law 66 (2015); Kesari, Hoofnagle & McCoy, לעיל ה"ש 61, בעמ' 1095.

90 לדוגמה, חברת כרטיסי האשראי מקס (לשעבר לאומי קארד), שקיבלה תלונות רבות על חברת הלפ פי סי, החליטה לעצור את שירותי הסליקה לבית העסק. ראו מיכל רז־חיימוביץ' "הסוף לעושק קשישים? היועמ"ש: חברות האשראי יכולות לעצור עסקאות" **גלובס** (22.12.2019) https://bit.ly/3NRvaW5.

91 ראו הבהרות בנושא ניהול סיכונים הנובעים משימוש בכרטיסי אשראי בביצוע עסקאות לא חוקיות – בעסקה במסמך חסר, שבה לא הוצג כרטיס אשראי, ברשת האינטרנט, בנק ישראל, אגף הפיקוח על הבנקים – אגף מדיניות והסדרה, סעיף 4 (9, יוני 2009) https://did.li/VqECN.

92 ראו לדוגמה ת"פ (שלום ת"א) 16506-02-16 **פרקליטות המדינה, מחלקה כלכלית נ' בן אסולין** (נבו 14.4.2016) באותו עניין חברת כ.א.ל. קלטה לסליקה אתרי הימורים באינטרנט של מהמרים אמריקאים, הסוותה את סליקת עסקאות ההימורים ונתנה להן כסות של פעילות בתחומי מסחר לגיטימיים. לשם הסתרת הפעילות הוקמו אתרי אינטרנט פיקטיביים שנחזו להיות אתרי מסחר בענפים שאינם בסיכון גבוה ושימשו כיסוי לפעילות ההימורים, ובהתאמה ניתן להם קידוד כוזב, כך שלא זוהו באמצעות הקוד הייעודי לאתרי הימורים. על הנאשמים מנכ"ל חברת כ.א.ל ומנכ"ל חברת הבת כ.א.ל. אינטרנשיונל הוטלו עבודות שירות וקנסות כבדים. יצוין כי באותו עניין הועמדו הנאשמים לדין בגין מרמה והלבנת הון, מאחר שכ.א.ל הונתה את ויזה העולמית כדי להימנע מתשלום עמלות גבוהות על סליקת חברות בסיכון גבוה, והאחריות לא הוטלה על עצם הסליקה.

nevo.co.il

חוקית כמו הפרת סימני מסחר.[93] עצירות תשלום כמתואר הן איום משמעותי על המשך הקיום של אתרים הפועלים בניגוד לדין ולכן הן יעילות בסיכול התנהגות מפירת דין.[94]

עצירת תשלום בידי המתווכים יכולה כאמור להיות לפי דין ויכולה להתבצע וולונטרית. אולם גם כאשר פעילות זו מתבצעת לכאורה באופן וולנטרי, היא מתבצעת לעיתים בצל האיום מחקיקה עתידית פוטנציאלית. לדוגמה, הצעת חוק באשר לפעילות מתווכי התשלום גורמת למתווכי התשלום לקחת אחריות על העסקאות המתווכות על ידיהם, שכן עצם קיומו של חוק בקנה שעשוי לפגוע בעסקיהם באופן קשה מתמרצת אותם לנקוט פעולות על מנת שיוכלו לטעון בפני המחוקק כי התחום כבר מוסדר (או מוסדר במידה מסוימת).[95] יתרה מזו, עלויות עסקה ועלויות של חבות באחריות אזרחית שעלולות להיפסק בבתי משפט יכולות לתמרץ את מתווכי התשלום לעצור סליקת תשלום מלהגיע לישויות שמרוויחות מפעילות בניגוד לדין.[96]

תפקיד נוסף של מתווכי תשלום הוא פיקוח על מסחר חשוד שמתבצע בכמה בנקים דרך הפלטפורמה של מתווך התשלום. לדוגמה, ויזה יכולה לחפש הפרות פוטנציאליות במערכת התשלום, להגיב לתלונות ולבקשות חקירה ולדווח על החשד לשלטונות.[97] חובה זו אף מעוגנת בדין הישראלי.[98] מערכות הסליקה משמשות בעצם כצוואר בקבוק של השוק, ועל כן הן יכולות למעשה לעצור את זרם ההכנסות אל ומאת גורמי טרור ופשיעה ולשבש את פעילותם.

מתווכים יכולים גם לנתק את זרימת הכסף שמאפשר את שרשרת הפעילות שמובילה לפשיעה או לפגיעה בביטחון הלאומי. מוסדות פיננסיים מסורתיים מסייעים לאכיפת חוקי איסור הלבנת הון והגנה מפני טרור מזה שנים רבות. כך, מאז שנת 1989 פועל גוף בין־לאומי, ארגון גלובלי המורכב ממדינות וארגונים חוץ ממשלתיים, למאבק בכלכלת הטרור ובעיקר נגד

93 Anne Marie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523 (2016).

94 שם, בעמ׳ 1525.

95 ראו שם, בעמ׳ 1450. מצוין שמתווכים נוטים לנקוט הסכמי אכיפה וולונטרית בצל חוקים פוטנציאליים. כדוגמה מציינות הצעות חוק שהוצעו בארצות הברית Combating Online Infringements and Counterfeits Act (COICA) (Combating Online Infringements and Counterfeits Act (COICA), S. 3804, 111th Cong. (2010), the Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (1st Sess. 2011), and the Protect Intellectual Property Act (PIPA) (Protect Intellectual Property Act (PIPA)), S. 968, 112th Cong. (2011) שכולן מכוונות למנוע משירותי תשלום להשלים עסקאות שמערבות צרכנים שממוקמים בארצות הברית אשר מבקשים לבצע עסקאות עם אתרים אינטרנטיים שקשורים עם שמות מתחם מסוימים שיכולים להצביע על פעילות לא חוקית. יוזמות חקיקה מתוכננות יכולות להשפיע על מתווכי תשלום לחסום וולונטרית ישויות שמרוויחות מפעילות לא חוקית ולייתר את הרגולציה המתוכננת.

96 ראו לדוגמה Perfect 10, Inc. V. Visa Int’l Serv. Ass’n, 494 F.3d 788, 793 (9th Cir. 2007). באותו עניין פרפקט 10 תבעה את ויזה בארצות הברית, מאסטר כארד ומתווכי תשלום אחרים בעילה של הפרה תורמת ואחריות שילוחית שהתרחשה באתרים מפירי זכויות יוצרים שלהם סיפקה ויזה תשלום. רוב השופטים דחו את התביעה, אך השופט קוזינסקי התנגד. מקרה זה הוא דוגמה לחשיפת מתווכים לעלויות ליטיגציה כאשר הם בוחרים שלא לעצור סליקת תשלום).

97 Kesari, Hoofnagle & McCoy, לעיל ה״ש 61, בעמ׳ 1127.

98 בישראל חובה זו מעוגנת בצו ספציפי החל על כרטיסי אשראי (צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של נותני שירותי אשראי למניעת הלבנת הון ומימון טרור) תיקון התשפ״א).

nevo.co.il

הלבנת כספים המיועדים למימון טרור.[99] גוף בין־לאומי זה, המכונה כוח המשימה לפעולות פיננסיות – Financial Action Task Force (FATF), הוקם על ידי ה־G-7, קבוצה של שבע מדינות מפותחות.[100] גוף זה קובע ומקדם כללים בין־לאומיים בתחום איסור הלבנת הון ומימון טרור, מנחה את המדינות והארגונים החברים בעיצוב מדיניות המתמקדת בחקיקה ותקנות שנועדו למנוע הלבנת הון ומימון טרור ומנסה להצר את צעדי ארגוני הטרור והפשיעה בכך שהוא מוביל מדיניות של אימוץ רפורמות שמתבטאות בשינויי חקיקה שנועדו למגר הלבנת הון ומימון טרור בעולם.[101] בשנת 2018, ישראל צורפה כחברה מלאה בארגון זה לאחר שנתיים שבהן שימשה כמשקיפה.[102] המדינות שנרתמו למאבק בהלבנת הון מאמצות את עקרונות ה־FATF מתוך רצון להימנע מסנקצייה בגין אי־שיתוף פעולה עם המלצות הארגון. הסנקצייה בגין אי־ציות להמלצות הארגון מתבטאת בהכללת המדינה ב״רשימה שחורה״ של מדינות שפרסם ה־FATF. מדינות הנמצאות ברשימה השחורה נכנסות אליה בשל ציות לא מספק להמלצות הארגון ו/או סיכון גבוה להלבנת הון.[103] מדינה שנכנסת לרשימה השחורה של הארגון צפויה למספר רב של הגבלות, החל מהגבלות על הבנק המרכזי שלה ועד להגבלות על אנשי עסקים הנושאים את אזרחות אותה המדינה.[104]

במסגרת הקווים המנחים את חבריו, הוציא ה־FATF שורה של תשע המלצות למאבק בהלבנת הכספים המיועדים לממן את הטרור, וביניהן אשרור ויישום של החלטת האו״ם הקוראת להיאבק בדרכי המימון של הטרור, חקיקת חוקים נגד מימון טרור, הקפאת נכסים של ארגוני טרור והחרמתם ודיווח על עסקאות חשודות במימון טרור.[105]

1. גורמים המאפשרים את התשתית לפעילות פיננסית כשומרי סף של העברה לא חוקית של כספים למימון טרור ופשיעה

פעילות טרור דורשת מימון. ככל שהמימון גדול יותר, כך מאורגנות ומוצאות לפועל יותר מתקפות טרור קטלניות.[106] מאחר שכסף המיועד למימון טרור עובר דרך מתווכים פיננסיים,

99 ראו באום, לעיל ה״ש 2, בעמ׳ 290.

100 ראו HISTORY OF THE FATF www.fatf-gafi.org/about/historyofthefatf/; James T. Gathii, *The Financial Action Task Force and Global Administrative Law*, J. PROF. LAW 197 (2010); ריקרדו בן אוליאל ולירן חיים **דיני בנקאות – חלק כללי** 706 (מהדורה שנייה, 2021); דורין לוסטיג ״קאדי בירושלים דמוקרטיה בעידן של ממשל גלובלי: רגולציה של מימון טרור בישראל״ **מחקרי משפט לא** 881, 892 (2018).

101 באום, לעיל ה״ש 2, בעמ׳ 290.

102 ״הישג לאומי אסטרטגי: מדינת ישראל צורפה כחברה מלאה בארגון ה־FATF, הארגון הבינ״ל היוקרתי והחשוב ביותר בתחום המאבק בהלבנת הון ובמימון טרור״ **הרשות לאיסור הלבנת הון ומימון טרור** (10.12.2018) https://bit.ly/3yKGzml.

103 באום, לעיל ה״ש 2, בעמ׳ 291. יצוין כי כיום עבר ה־FATF לגישה מבוססת סיכון עקב ביקורת כי הארגון הכניס לרשימה השחורה על בסיס בחינת תהליכי הציות וללא התחשבות באפקטיביות המאבק בהלבנת הון באותן מדינות. שם, בעמ׳ 300.

104 Nizan Geslevich Packin & Hadar Y. Jabotinsky, *Blacklisting or Banning Technologies that Scare Us? Generative AI, Crypto and More* (Working Paper).

105 הרפז, לעיל ה״ש 29, בעמ׳ 204.

106 DION-SCHWARZ, MANHEIM & JOHNSTON, לעיל ה״ש 3.

nevo.co.il

כגון: בנקים, חברות ביטוח, בתי השקעות, חלפני כספים ועוד, מוסדות פיננסיים מהווים בעצם תשתית שמאפשרת את העברת הכספים לארגוני טרור. בנוסף, ארגוני פשיעה מנסים להחדיר למערכת הפיננסית כסף שהושג מפשיעה חמורה על מנת להסוות את מקורו ולהפוך אותו לכסף לגיטימי. בעקבות תפקידם של המתווכים הפיננסיים כתשתית לביצוע עסקאות, מתווכים אלה יכולים להקשות על הלבנת כספים שמקורם בפשיעה והעברת כספים המיועדים לטרור בכך שימנעו ממעבירי הכסף ומקבליו שירות. אם יקשו על ארגוני הטרור לקבל תרומות ומימון, יתנתק החמצן לפעילותם.[107] באותו אופן, מלחמה בהלבנת הון שמקורו בפשיעה חמורה היא חלק מהמלחמה בפשע באופן כללי. לאור מאפייניהם של מתווכי התשלום, פותחו והוטמעו כמה גישות למניעת הלבנת הון ומימון טרור באמצעות מתווכי תשלום.[108] כך, מאצילה המדינה סמכות לזיהוי תרומות ותשלומים לטרור שנועדו להלבנת הון או למימון טרור ומניעתם למתווכים הפיננסיים בשוק ההון, שכן הם משמשים כצינור להעברת הכספים.[109] רגולציה ואף הטלת אחריות המופנית אל מוסדות פיננסיים מתמרצות אותם לנקוט אמצעים וללחום בהלבנת הון ומימון טרור המתרחשים באמצעות התשתית שלהם.[110]

2. שימוש במתווכים פיננסיים מסורתיים לקידום הביטחון הלאומי

מתווכים פיננסיים מנוצלים לביצוע פעולות שמטרתן הלבנת הון והעברת כספים לארגוני טרור. כדי לעצור את מעבר הכספים שמקורם בפעילות לא חוקית, או שמיועדים לממן את הפעילות הלא חוקית, הופנו כאמור חובות משפטיות כלפי המערכת הבנקאית בחוק איסור הלבנת הון 2000,[111] בצווים שמכוחו ובחוק המאבק בטרור, התשנ״ו–2016. החלק הבא יתמקד ברגולציה זו.

(א) חוקי איסור הלבנת הון

הלבנת הון היא התהליך שבו פרטים שמשיגים כספים דרך פעילות פלילית, כולל טרור, מנסים להסתיר את מקורות ההכנסה הלא חוקיים ולגרום להם להיראות לגיטימיים תוך טשטוש או הסוואה.[112] הלבנת הון היא בעיה מערכתית אשר משפיעה רבות על כלכלות בעולם.[113] ככלל,

107 Kesari, Hoofnagle & McCoy, לעיל ה״ש 61, בעמ׳ 1106.

108 גישות רגולטוריות אלה ידועות כ־on Counter Terrorism Financing (CTF).

109 Kesari, Hoofnagle & McCoy, לעיל ה״ש 61, בעמ׳ 1096.

110 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 10 מתייחסים ל־Code of Federal Regulations, Title 31, Money and Finance: Treasury; Subtitle B, Regulations Relating to Money and Finance; Subchapter X, Financial Crimes Enforcement Network, Department of the Treasury; Parts 1010, 1021, and 1022, Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses.

111 ראו חוק איסור הלבנת הון; ובעיקר צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), התשע״ד–2014; צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של נותני שירותי אשראי למניעת הלבנת הון ומימון טרור) (תיקון), התשפ״א–2021.

112 בן אוליאל וחיים, לעיל ה״ש 100, בעמ׳ 705; פלאטו שנער, לעיל ה״ש 32.

nevo.co.il

הלבנת הון מורכבת משלושה שלבים: (1) השמה (placement), העברת הכסף ממקומו המקורי, היכן שיש זיקה בין הרכוש לעבריין, למיקום אחר במערכת הפיננסית; (2) ריבוד (layering) – מיסוך מקור הכסף וניתוק הקשר בין העבריין לרכוש דרך כמה עסקאות נפרדות באמצעות אנשי אמון או מוסדות פיננסיים ברחבי העולם; (3) הטמעה (integration), שילוב של הכסף הלא חוקי בתוך המערכת הפיננסית הלגיטימית, וכך השבת הרכוש חזרה לעבריין תוך שמוקנית לו חזות לגיטימית, ובכך מתאפשר שימוש בכסף ללא חשש.[114] רגולציה של הלבנת הון מטרתה להגביל את היקף הפשיעה על ידי צמצום האפשרות "להלבין" את הכספים הקשורים בביצוע העבירות.[115] מאפיין מרכזי של הלבנת הון הוא השימוש בכפר הגלובלי כדי להקנות לרכוש מושא העבירות לבוש לגיטימי. לפיכך, התמודדות עם הלבנת הון מצריכה שיתוף פעולה בין־לאומי בין מדינות ובין מוסדות פיננסיים ברחבי העולם.[116] קיומו של משטר הלבנת הון מדינתי הוא חלק בלתי נפרד מההסדרים המשפטיים של המדינות המערביות וכן תנאי לניהולם התקין של המוסדות הבנקאיים הפועלים בהן.[117]

רגולציה לאיסור הלבנת הון התקיימה ברוב המדינות המפותחות מאז שנות השבעים של המאה הקודמת, ונעשו נסיונות ליצור מסגרת משפטית בין־לאומית לאסדרת הסוגיה.[118] כך, ארצות הברית הייתה הראשונה בעולם לאמץ חקיקה שנועדה להיאבק בהלבנת הון.[119] אולם, ממשלות מערביות הגבירו את אכיפת החוקים הללו בעקבות התקפות הטרור בארצות הברית ב־11 לספטמבר 2001. אחרי הפיגוע במגדלי התאומים בניו יורק, מדינות הגיעו להבנה ברורה שהנשק העיקרי במלחמה בטרור הוא ללכת בעקבות הכסף.[120] על רקע ההבנה שלא המדינה לבדה ולא המוסדות הפיננסיים לבדם יצליחו להילחם בהלבנת ההון והעברת כספים לארגוני טרור, הטילו מדינות שונות חובות נוספות על מוסדות פיננסיים ורתמו אותם למלחמה בהלבנת הון.[121] זאת, כדי למנוע מהמוסדות הפיננסיים לשמש כלי שרת בידי מלביני הון וכדי לצרפם למערכת אכיפת החוק על ידי חיובם למסור מידע לרשויות על עסקאות שונות. שיתוף הפעולה

113 "The International Monetary Fund estimates that money laundering amounts to between 2 to 5 percent of the global gross domestic product, or roughly $1.45 and $3.6 trillion per year", NORMAN ABRAMS, SARA SUN BEALE & SUSAN RIVA KLEIN, FEDERAL CRIMINAL LAW AND ITS ENFORCEMENT 603 (2015).

114 בן אוליאל וחיים, לעיל ה"ש 100, שם, ראו גם באום, לעיל ה"ש 2, שם.

115 בן אוליאל וחיים, לעיל ה"ש 100, בעמ' 706.

116 שם, בעמ' 706.

117 שם, בעמ' 707.

118 לדוגמה, בארצות הברית, בשנת 1970, הקונגרס העביר את חוק הסודיות הבנקאית, שדורש כי מוסדות פיננסיים ידווחו לממשלות באשר לעסקאות מזומן מעל ל־10,000 דולר (31 U.S.C. § 5311 (2018)), וב־1996 הרגולציה הפדרלית החלה לדרוש מבנקים לדווח על עסקאות חשודות. ראו (12 CFR §§ 21.11, 163.180); ראו גם לוסטיג, לעיל ה"ש 100, בעמ' 885.

119 ראו 31 U.S.C. §§ 5311 Bank Secrecy Act 1970; באום, לעיל ה"ש 2, בעמ' 303; פלאטו שנער, לעיל ה"ש 32, בעמ' 271.

120 Goldman et al., לעיל ה"ש 13, בעמ' 4.

121 Joseph J. Norton & Hera Shams, *Money Laundering Law and Terrorist Financing: Post-September 11 Responses – Let Us Step Back and Take a Deep Breath*? 36 INTER'L LAWYER 103,104 (2002) (ABA); ראו גם פלאטו שנער, לעיל ה"ש 32, בעמ' 255.

nevo.co.il

של הבנקים במיגור ההון השחור חשוב גם לצורך שמירה על יציבות המערכת הבנקאית כולה.[122] כך, חקיקה לאיסור הלבנת הון הפכה לאלמנט בסיסי בלוחמה בטרור ובשליטה בפשיעה וחלק בלתי נפרד מסטנדרטים בנקאיים בין־לאומיים.[123]

לדוגמה, בארצות הברית, חקיקת חוק הפטריוט[124] הובילה לנקיטת צעדים נוספים נגד הלבנת הון.[125] החוק למעשה קורא לכל פטריוט אמריקאי למלא את חלקו בהגנה נגד איום הטרור. מטרת החוק היא להעניש פעילות טרור בארצות הברית וברחבי העולם ולאפשר כלים של חקירה ואכיפת חוק.[126] החוק מביא להגברת שותפות בין הסקטור הפרטי לציבורי בפיקוח על הערוצים הבין־לאומיים להעברות פיננסיות.[127] מטרתו של החוק הייתה החלתו גם על מוסדות פיננסיים זרים ופרטים שאינם אמריקאים.[128] החוק דורש ממוסדות פיננסיים להיות קו ההגנה הראשון נגד פשיעה פיננסית. על מוסדות אלה לזהות ולחסום כל תנועה של כסף שנוצרת דרך פשע או מיועדת למימון טרור שעוברת דרך מערכותיהם. מוסדות פיננסיים נדרשים להכיר את לקוחותיהם, Know Your Client (KYC), על ידי מילוי שאלונים והכרת פעילות הלקוחות בחשבונותיהם.[129] אם מתבצעת פעולה חריגה לחשבון, חלה על המוסד הפיננסי החובה לדווח על הפעולה לרשויות איסור הלבנת הון. כל זה נעשה באימוץ גישות לניהול סיכונים המקשות ניצול לרעה של המערכת הפיננסית מלכתחילה.[130]

Title III לחוק הפטריוט האמריקאי מתייחס להלבנת הון[131] ומתמקד בסוגיות גלובליות של הלבנת הון. חקיקה זו מתמקדת בהטלת חובות ספציפיות על בנקים.[132] כפי שצוין, ההוראות מחייבות מתווכים פיננסיים להכיר את לקוחותיהם ודורשות לזהותם. כלומר, שבנקים יוודאו ויאמתו את זהות הלקוחות באמצעות שני מסמכי זיהוי רשמיים. תחום נוסף של חובות מתייחס לבדיקת נאותות, due diligence, של פעילות בנקאית פרטית וכל פעילות בנקאית שנחשבת פעילות בסיכון. נוסף על זה מוטלות על בנקים חובות הקשורות ליחסים שלהם עם בנקים אחרים (קורספונדנטים), המספקים שירותים לבנק אחר, בנקים שאין להם נוכחות פיזית במדינה (shell banks) וחובות ניטור ופיקוח על העברות בנקאיות לצורך איתור דפוסים של

122 שם, וכן בעמ׳ 275.
123 Norton & Shams, לעיל ה״ש 121, בעמ׳ 105.
124 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); 18 U.S.C. § 1, החוק משנת 2000 (פטריוט הם ר״ת של שם החוק המלא). ראו Norton & Shams, לעיל ה״ש 121, בעמ׳ 104.
125 Chalo, לעיל ה״ש 28, בעמ׳ 317.
126 Norton & Shams, לעיל ה״ש 121, בעמ׳ 107.
127 שם.
128 שם, בעמ׳ 108
129 12 U.S.C. § 635(i) (2012); 31 C.F.R. § 1020.200 et. seq. (2016); Kesari, Hoofnagle & McCoy, לעיל ה״ש 61, בעמ׳ 1096; Bridy, לעיל ה״ש 93, בעמ׳ 1565.
130 Goldman et al., לעיל ה״ש 13, בעמ׳ 30.
131 USA PATRIOT Act, tit. III, 115 Stat. at 296–342.
132 Norton & Shams, לעיל ה״ש 121, בעמ׳ 106.

nevo.co.il

הלבנת הון.[133] דרישות אלה מאפשרות לבנקים לחסום ולדווח על העברות לא חוקיות וכך לאפשר לעקוב, לפקח ולחלט כספים שמקורם בפשיעה או המיועדים לטרור. על בנקים חלה החובה לדווח על פעילות לא רגילה בחשבונות לקוחותיהם ועל עסקאות מסוימות לפי חוקים והנחיות רגולטוריות. הדיווח נעשה לרשות לאיסור הלבנת הון האמריקאית Financial Crime Enforcement Network (FinCEN). אין ספק שציות לחוקי איסור הלבנת הון מטיל נטל כבד על מוסדות פיננסיים, במיוחד מאחר שהיעדר ציות יכול להוביל לאחריות.[134] על המסגרת הרגולטורית נוספו עבירות פליליות הקשורות לאיסור נגד העברות כספיות הקשורות לפעילות לא חוקית[135] ואיסור על ארגון מחדש של עסקה פיננסית כדי להימנע מדיווח.[136]

(1) איסור הלבנת הון בישראל

בשנת 2000 נחקק בישראל חוק איסור הלבנת הון, אשר נכנס לתוקף כשנתיים לאחר מכן.[137] החוק הוא דבר החקיקה המרכזי בדין הישראלי במאבק נגד התופעה חוצת הגבולות של הטמעת כספים שמקורם בפשיעה במערכת הפיננסית והעסקית הלגיטימית.[138] כפי שמסבירים ד"ר ריקרדו בן אוליאל וד"ר לירן חיים, רק לאחר חקיקתו של חוק איסור הלבנת הון החלה מדינת ישראל לקיים משטר לאיסוף וניטור הנתונים הקיימים במערכת הפיננסית על מנת לאתר עבירות פליליות ולחלט את תוצריהן הכספיים.[139] בשנת 2000 הכיר המחוקק בצורך בקיומו של החוק, וזאת מכמה סיבות: ראשית, כדי לשפר את ההתמודדות עם פעילות עבריינית ופשיעה מאורגנת;[140] שנית, להביא לשיתוף פעולה בין ממשלות, רשויות אכיפת חוק ומוסדות פיננסיים; ושלישית, לחזק ולבסס את המערכת הפיננסית של מדינת ישראל.[141] מכוחו של החוק הוקמה הרשות לאיסור הלבנת הון ומימון טרור במשרד המשפטים.[142] מטרת הרשות היא לרכז את כל המידע שמעבירים אליה מוסדות פיננסיים וליצור תמונת מודיעין של העברות הכספים מ- ואל גורמי פשע וטרור. לצורך הגשמת המטרות, ניתנו לרשות בחוק כמה כלים: ראשית, רשות זו מוסמכת לנהל מאגר מידע שכולל את הדיווחים שמעבירים אליה המוסדות הפיננסיים בזמן אמת ולעבד אותו כדי לאתר עבירות פליליות שעולות מתנועת הכספים;[143] שנית, הרשות מוסמכת להעביר חומרים ממאגר המידע לרשויות אחרות;[144] שלישית, הרשות

133 שם.
134 שם, בעמ' 118.
135 18 U.S.C. §§ 1956, 1957 (2018).
136 31 U.S.C. § 5324 (2018).
137 החוק נכנס לתוקף ביום 17.2.2002; ראו פלאטו שנער, לעיל ה"ש 32, בעמ' 257.
138 חוק איסור הלבנת הון; להרחבה ראו באום, לעיל ה"ש 2, שם.
139 בן אוליאל וחיים, לעיל ה"ש 100, בעמ' 107.
140 שם, בעמ' 108.
141 שם.
142 ס' 28–29 לחוק איסור הלבנת הון; להרחבה ראו בן אוליאל וחיים, לעיל ה"ש 100, בעמ' 108.
143 שם, בעמ' 108.
144 ס' 30 לחוק איסור הלבנת הון; ראו בן אוליאל וחיים, לעיל ה"ש 100, בעמ' 109. החוק קבע מי הגופים שיכולים לקבל מידע מהמאגר.

nevo.co.il

מוסמכת ליזום בקשות מידע לגופים מדווחים לצורך השלמת דיווח;[145] רביעית, הרשות מוסמכת לבקש ולהעביר מידע לרשויות לאיסור הלבנת הון ומימון טרור בעולם לאור חשיבות שיתוף הפעולה הבין־לאומי בנוגע להלבנת הון.[146]

חוק איסור הלבנת הון בארץ מאמץ בעיקרו את המלצות ארגון ה־FATF[147] ונועד ליצור משטר של דיווח על פעולות כספיות אשר יאפשר להתחקות אחר פעולות הלבנת הון ומבצעיהן.[148] החוק הסמיך בסעיף 7(א) את נגיד בנק ישראל להטיל חובות על הבנקים, ונחקקה חקיקת משנה ליישום הוראותיו.[149] צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), התשס״א–2001, שהוצא מכוחו של סעיף זה, מטיל בסעיף 2 חובות על הבנקים לזהות את לקוחותיהם (חובת הכרת הלקוח),[150] לתעד את פרטיהם ואת הפעולות שהם מבקשים לבצע ולשמור את המידע.[151] הצו אף מחייב את התאגידים הבנקאיים לדווח לרשות המוסמכת (הרשות לאיסור הלבנת הון ומימון טרור) על התנועות המבוצעות בידי לקוחותיהם. חובות הדיווח נחלקות לשניים: חובת דיווח אובייקטיבית על עסקאות מעל לסכום מסוים (חובת דיווח אוטומטית),[152] וחובת דיווח סובייקטיבית על עסקאות בלתי רגילות ללקוח. לגבי חובת הדיווח הסובייקטיבית, נדרש הבנק להפעיל שיקול דעת ולהחליט באילו מקרים לדווח.[153] לשם מילוי חובת הדיווח הבנקים מחויבים לעקוב באופן שוטף אחר הפעילות בחשבון הלקוח כדי לאתר פעילות בלתי רגילה.[154] החוק אף מטיל חובה למינוי אחראי לעניין איסור הלבנת הון.[155] בצידן של חובות אלה קיימות

145 ס׳ 31(א)–31(ג) לחוק איסור הלבנת הון; בן אוליאל וחיים, לעיל ה״ש 100, שם.
146 ס׳ 30(1) לחוק איסור הלבנת הון; בן אוליאל וחיים, לעיל ה״ש 100, שם.
147 להרחבה על ה־FATF ראו ה״ש 100 והטקסט הצמוד אליה.
148 ראו באום, לעיל ה״ש 2, בעמ׳ 291.
149 ס׳ 7(א) לחוק איסור הלבנת הון.
150 להרחבה ראו פלאטו שנער, לעיל ה״ש 32, בעמ׳ 257–262, לפי ס׳ 6 לצו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), התשס״א–2001 על חובת הזיהוי להיות פנים אל פנים.
151 פלאטו שנער, לעיל ה״ש 32, בעמ׳ 265.
152 ראו ס׳ 8 ו־9 לצו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של תאגידים בנקאיים למניעת הלבנת הון ומימון טרור), התשס״א–2001, לגבי פרטי הדיווח. להרחבה על חובת הדיווח ראו רות פלאטו שנער ״הזכות לפרטיות פיננסית: עולם הולך ונעלם״ **משפט חברה ותרבות, מן הכלל אל הפרט, פרטיות וחברת המעקב** 199, 210 (2019); פלאטו שנער, לעיל ה״ש 32, בעמ׳ 262–265.
153 ראו ס׳ 9 לצו איסור הלבנת הון; פלאטו שנער, לעיל ה״ש 152, בעמ׳ 210; פלאטו שנער, לעיל ה״ש 32, בעמ׳ 263. לדוגמה, כמה פעולות משיכה לאחר ההפקדה בלא סיבה נראית לעין ושלא במהלך העסקים הרגיל; הפקדות מרובות בלי סיבה נראית לעין על ידי אדם שאינו בעל החשבון או מורשה חתימה בו ועוד. יצוין כי חובות הדיווח התרחבו למגזרים פיננסיים ועסקיים אחרים לפי הערכת הסיכון הנשקפת בעיני המחוקק לשימוש בגורמים אלה לצורך הלבנת הון (באום, לעיל ה״ש 2, בעמ׳ 298). אפשר לטעון כי הרחבת רשת הדיווח משקפת מגמה, עליה עמדנו, של העברת האחריות לשומרי הסף. ראו לעניין זה גם באום, שם, בעמ׳ 301.
154 להרחבה ראו פלאטו שנער, לעיל ה״ש 32, בעמ׳ 264.
155 ס׳ 8 לחוק איסור הלבנת הון.

nevo.co.il

סנקציות פליליות, אשר ממחישות את אחריותו הציבורית של הבנק.[156] החוק אף מאפשר לחלט כספים שמקורם בעבירה.[157]

לצד החובות החלות על הבנקים, המחוקק פטר אותם מאחריות בגין כל מעשה או מחדל לפי הוראות החוק, בתום לב, וקבע כי אין בהם הפרה של חובת סודיות ונאמנות או של חובה אחרת לפי כל דין או הסכם.[158] כך, אף שכאשר הבנק מדווח לרשות המוסמכת לפי חוק לאיסור הלבנת הון הוא פוגע בפרטיותו הפיננסית של אותו לקוח ובחובת הסודיות כלפיו,[159] זכויות אלה אינן מוחלטות. קיימים חריגים לזכות לפרטיות ולחובת הסודיות הבנקאית,[160] ודיווח הנעשה על פי הוראה כדין זוכה להגנה לפי החוק ואינו מטיל אחריות על הבנק.[161] הזכות היא בעלת תוקף חוקתי, אך מותר לפגוע בה למטרה ראויה, אף שהזכות לפרטיות מעוגנת בחוק־יסוד: כבוד האדם וחירותו,[162] לאור הצורך להילחם בתופעות של הלבנת הון ומימון טרור, מאחר שהאיזון ראוי והפגיעה עומדת בתנאי פסקת ההגבלה של חוק־יסוד: כבוד האדם וחירותו.[163]

החובות שמטיל החוק למעשה מאפשרות להתחקות אחר המשתמשים באמצעי התשלום. גישה זו מביאה לדה־אנונימיזציה של המשתמשים באמצעי תשלום כלפי המדינה והמערכת הפיננסית, בשונה משימוש בכסף מזומן שיכול להיעשות ללא רישום ובאופן בלתי אמצעי.[164] מגמת הדה־אנונימיזציה מתבטאת בחקיקה שמטרתה למזער את היכולת להשתמש באמצעי תשלום השוללים את היכולת לאתר את נותן התשלום ואת מקבלו ולעקוב אחריהם[165] וכן בדברי חקיקה שנועדו לאפשר לפקח על נותני שירותים שעלולים לשמש להלבנת כספים.[166]

156 בן אוליאל וחיים, לעיל ה״ש 100, שם; באום, לעיל ה״ש 2, בעמ׳ 291.

157 ס׳ 21 ו־22 לחוק איסור הלבנת הון; באום, לעיל ה״ש 2, שם.

158 ס׳ 24 לחוק איסור הלבנת הון; פלאטו שנער, לעיל ה״ש 32, עמ׳ 266.

159 להרחבה בסוגיה זו ראו פלאטו שנער, לעיל ה״ש 152, בעמ׳ 201.

160 ראו רות פלאטו שנער ״הסודיות הבנקאית לאור חוק־יסוד: כבוד האדם וחירותו, והשיח החוקתי החדש״ **קריית המשפט** ח 71, 83, 86 (2009).

161 ראו ס׳ 19 לחוק הגנת הפרטיות התשמ״א–1981; פלאטו שנער, לעיל ה״ש 152, בעמ׳ 205 (עמדה על החריגים לזכות זו); ראו גם פלאטו שנער, לעיל ה״ש 32, בעמ׳ 268.

162 ס׳ 7 לחוק־יסוד: כבוד האדם וחירותו המעגן את זכותו של אדם לפרטיות ולצנעת חייו.

163 ס׳ 8 לחוק היסוד קובע: ״אין פוגעים בזכויות שלפי חוק־יסוד זה אלא בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שאינה עולה על הנדרש, או לפי חוק כאמור מכוח הסמכה מפורשת בו״. ראו פלאטו שנער, לעיל ה״ש 32, בעמ׳ 268–269; פלאטו שנער, לעיל ה״ש 160, בעמ׳ 91; פלאטו שנער, לעיל ה״ש 152, בעמ׳ 201.
יצוין כי הרשות לאיסור הלבנת הון יכולה להעביר את המידע גם לרשויות המבקשות מידע זה לצורך חקירת עבירות אחרות. פרופסור רות פלאטו שנער מבקרת זחילה פונקציונלית זו ומסבירה כי היא בעייתית ויש ספק בשאלה האם תעמוד בפסקת ההגבלה לחוק היסוד, אולם נעשו ניסיונות להתמודד עימה. בתיקון לחוק איסור הלבנת הון בשנת 2016, הוסף סעיף 29(ב) הקובע כי ״השימוש בסמכות להעביר ולקבל מידע כאמור בסעיפים 30 ו־31, ייעשה באופן שאין בו כדי לפגוע, במידה העולה על הנדרש, בפרטיותו של אדם״. ראו פלאטו שנער, לעיל ה״ש 152, בעמ׳ 214.

164 באום, לעיל ה״ש 2, בעמ׳ 294.

165 שם, בעמ׳ 294; ראו לדוגמה ס׳ 2 לחוק לצמצום השימוש במזומן, התשע״ח–2018.

166 שם, בעמ׳ 294.

nevo.co.il

(ב) מוסדות פיננסיים והמאבק בטרור

רגולציה בתחום הלבנת הון וחובות החלות על מוסדות פיננסיים מכוחה, כמו זיהוי הלקוח, ניטור עסקאות וחובות דיווח על עסקאות חשודות, מסייעות מאוד לגדוע את מקורות המימון לטרור דרך המערכת הפיננסית ולהילחם בפשיעה.[167] נוסף על כך, התפתחו במקביל מסגרות משפטיות פרטיקולריות למאבק בטרור דרך גדיעת מקורות המימון המיועד לטרור. ניסיונות ליצור מסגרת משפטית בין־לאומית למאבק בטרור החלו לפחות מאז שנות השבעים.[168] כאמור, מאז שנת 1989 פועל גוף בין־לאומי המורכב ממדינות וארגונים חוץ ממשלתיים למאבק בכלכלת הטרור והפשע על ידי קביעת כללים וסטנדרטים שיאפשרו מיגור הלבנת כספים, ה־Financial Action Task Force (FATF). גוף זה מפרסם שורה של המלצות שנועדו למיגור הלבנת הון ומימון טרור.[169] המלצות אלה התקבלו אצל רוב המדינות בעולם ואומצו בחקיקה. מדינות שלא תיקנו את החוק בהתאם להמלצות הוכנסו לרשימה שחורה בכל הקשור להלבנת הון, ונקבע כי הן טריטוריות שאינן מצייתות ((non-compliant terretories) ועל כן נמצאות בסיכון גבוה להלבנת הון.[170] קביעה זו גוררת אחריה שורה של צעדים שמגבילים את הבנקים המרכזיים של טריטוריות מצייתות מלקיים יחסים עם בנקים מרכזיים שנמצאים במדינות שאינן מצייתות להמלצות. בנוסף, היכללות ברשימה מטילה שורה של מגבלות על אנשים הנושאים את הדרכונים של אותן טריטוריות.[171]

בשנת 1999 אומצה אמנה בין־לאומית לעצירת מימון טרור.[172] האמנה האמורה מיועדת להוביל ל״ייבוש״ המקורות הכספיים המזינים את הטרור, ובכך למנוע את התופעה.[173] לפי האמנה, מימון טרור כולל פעולות פיננסיות התומכות ב״כל מעשה המיועד לגרום למוות או לפציעה גופנית חמורה של אזרח או של כל אדם אחר שאינו נוטל חלק ישיר במעשי איבה במצב של עימות מזוין, כאשר מטרת המעשה — מטבעו או מהקשרו — היא לאיים על אוכלוסייה או לאלץ ממשלה או ארגון בין־לאומי לעשות פעולה מסוימת או להימנע מלעשותה״.[174] אמנה זו עוצבה כדי לחסום את כספי הטרור מבלי לפגוע בתפקודו של השוק הגלובלי. האמנה מסדירה את התנהלותם של גורמים לא־מדינתיים, ובפרט מוסדות פיננסיים, ומטילה חובה על המדינות החברות לשתף פעולה ולסייע זו לזו באיסוף מידע ובאכיפה כדי ליצור רשת הסדרה יעילה להתמודד עם הסוגיה.[175] לאחר מתקפות ה־11 בספטמבר 2001

167 ראו בהרחבה חלק 2(א) למאמר.
168 לוסטיג, לעיל ה״ש 100, בעמ׳ 885.
169 ראו לעיל ה״ש 99—103 והטקסט הצמוד אליהן.
170 Geslevich Packin & Jabotinsky, לעיל ה״ש 104; FATF, About the Non-Cooperative Countries and Territories (NCCT) Initiative (Nov. 22, 2021) https://bit.ly/3NULDJu.
171 Financial Action Task Force on Money-Laundering, Report on Non-Cooperative Countries and Territories 8 (2000).
172 International Convention for the Suppression of the Financing of Terrorism, 2178 U.N.T.S. 197(9.12.1999); לימון, לעיל ה״ש 28, בעמ׳ 18; לוסטיג, לעיל ה״ש 100, בעמ׳ 892.
173 לימון, לעיל ה״ש 28, שם.
174 שם, שם
175 ראו לוסטיג, לעיל ה״ש 100, בעמ׳ 892, מפנה לס׳ 18 לאמנה.

nevo.co.il

הפכה מועצת הביטחון של האו״ם את מרבית הוראות האמנה למחייבות ואף הקימה מנגנון לפיקוח על קיומן וניטורן.[176]

מסגרות לעצירת מימון טרור מרחיבות את מעגל האחריות אל מעבר למעורבים הישירים בטרור ומטילות חובות ואחריות על שותפים עקיפים שהיו מעורבים בהיבטים שונים של סיוע לפעילות הטרור והכנת ביצועה וכן על מי שלא היו מעורבים בביצוע מעשי טרור קונקרטיים, אך תרמו לעצם פעילותו של ארגון הטרור בדרך של חברות בארגון, אימונים, גיוס חברים, מימון ואף הסתה לביצוע פעילות טרור.[177] מדינות פועלות למניעת טרור במגוון רחב של אמצעים וערוצי פעולה. עם האמצעים המרכזיים נמנים הוצאתם של ארגונים המעורבים בטרור אל מחוץ לחוק והקפאת נכסים שבבעלותם, איסור מימון של פעילות טרור או סיוע לקבלת מימון זה.[178]

דוגמה בולטת היא החקיקה בארצות הברית נגד תמיכה מהותית בטרור.[179] חקיקה זו למעשה יוצרת קידוד של חוק הפטריוט[180] באיסור לספק תמיכה מהותית לטרור וחושפת מוסדות פיננסיים, שמאפשרים העברות כספים לארגוני טרור, לאחריות אזרחית ופלילית.[181] סעיף 2339A אוסר לספק תמיכה מהותית (material support) או משאבים ביודעין לארגוני טרור. הסעיף כולל איסור על העברת כספים בכוונה שישמשו להתכונן או לבצע עבירות מסוימות, כולל טרור.[182] סעיף 2339C מתייחס לאיסוף תרומות וכופה סנקציות נגד הרשאה לאיסוף ומימון תרומות בכוונה שאלה ישמשו, או בידיעה שאלה ישמשו בחלקן, או בכללותן, לטרור.[183] בשונה מסעיפים 2339A § ו־2339C, סעיף 2339B § לא כולל יסוד נפשי של ידיעה או כוונה, אלא איסור על הרשאה מרצון של כל הוספת ערך לארגון טרור ייעודי מוכרז ((ForeignTerrorist Organization (FTO)).[184] כך, אם בנק, או מוסד פיננסי אחר, יודע שארגון

176 שם, בעמ׳ 893.

177 לימון, לעיל ה״ש 28, בעמ׳ 38.

178 שם, בעמ׳ 43.

179 Anti-Terror, דבר החקיקה המרכזי הוא 18 U.S.C. §2339A שקובע אי־חוקיות של תמיכה מהותית לביצוע פעולות טרור ו*18 U.S.C. § 2339B*, שקובע אי־חוקיות לארגוני טרור מוכרזים ראו *See* Charles Doyle, *Terrorist Material Support: An Overview of 18 U.S.C. §2339A and §2339B*, Congressional Research Service (Dec. 8, 2016) fas.org/sgp/crs/natsec/R41333.pdf.

180 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, §810(c),(d), 115 Stat. 272, 380.

181 ראו Norman Abrams,*The Material Support Terrorism Offenses: Perspectives Derived from the (Early) Model Penal Code*, J. Nat'l Sec. L. & Pol'y 5 (2005).

182 18 U.S.C. § 2339A (2018) ("Providing material support to terrorists"); Ronbert H. Schwartz, *Laying the Foundation for Social Media Prosecutions Under 18 U.S.C. § 2339B*, 48 Loyola Chi L. J. 1181, 1186 (2017).

183 18 U.S.C. § 2339C(a).

184 Lavi, לעיל ה״ש 54, בעמ׳ 510; 18 U.S.C. § 2339B (2018) ארגון טרור מוכרז הוא ארגון שמזכירות המדינה הגדירה אותו בצורה זו. הרשימה של ארגוני הטרור המוכרזים שמורה בידי מחלקת המדינה (state department), סוכנות פדרלית אמריקאית שאחראית בעיקר על ענייני החוץ

nevo.co.il

הוכרז כארגון טרור, או שאותו ארגון מעורב בטרור, ומאפשר לו להמשיך לפעול, הוא יכול להימצא אחראי.[185] קשה להפריד בין פעילות אסורה כשלעצמה לפי דין כמו גיוס לארגון טרור ואימון מחבלים לבין פעילות לגיטימית לכאורה כמו תשלום משכורת ושירותים חברתיים, מאחר שפעילות לגיטימית מסייעת לטרוריסטים למסך פעילות שאינה לגיטימית.[186] לדוגמה, תשלום משכורות ושירותים חברתיים תורמים בעקיפין ליכולת של ארגון הטרור להסית לאלימות. אולם תחולת סעיף 2339B § רחבה, והוא חל על כל תמיכה שניתנת לארגון טרור.

בעניין *Holder v. Humanitarian Law Project* (*HLP*)[187] בית המשפט העליון בארצות הברית קבע כי סעיף 2339B § חוקתי ולממשלה יש סמכות לאסור על עבודה עם ארגוני טרור, אפילו כאשר המבצעים האלימים שהם מבצעים קשורים עם תפקודים בלתי מזיקים לכאורה כמו פעולות צדקה.[188] בשל הסכנה הנשקפת מארגוני טרור, בית המשפט העליון פירש את החקיקה בהרחבה וקבע כי עבודה בתיאום עם ארגון טרור ייעודי מוכרז מקדמת טרור, ולכן גם פעולות אלה הן בגדר תמיכה מהותית בטרור.[189] סעיפים 2339A ו־2339B לא יוצרים עילה לתביעה אזרחית כשלעצמם, אבל סעיף 2333 מאפשר לצדדים פרטיים בעלי אזרחות אמריקאית להגיש תביעות אזרחיות בבתי משפט פדרליים מחוזיים ולקבל פיצוי ושכר טרחת עורך דין אם נפגעו בנפש, ברכוש או בעסקים בשל טרור בין־לאומי.[190] זאת כאשר יש ישות שפעילותה תומכת בארגון טרור, ללא צורך להוכיח קידום פעולת טרור ספציפית.[191]

בעקבות התקפות טרור רבות, קורבנות התקפות טרור ומשפחותיהם עומדים בפני מציאות שאינה פשוטה, מאחר שהסיכוי לתבוע ולהיפרע מהאחראים ישירות בבתי המשפט הוא נמוך.[192] הטלת אחריות אזרחית על אלה שסיפקו תמיכה מהותית לארגוני טרור משרתת אפוא כמה מטרות. ראשית, היא מאפשרת לקורבנות ומשפחותיהם להחזיק כל מי שבשרשרת הסיבתית של מעשה הטרור אחראי; שנית, אחריות זו יכולה לאפשר פיצוי; שלישית, היא

של הממשל. רשימה זו מכילה למעלה מ־60 (Bureau of Counterterrorism, US Dep't of State, *Foreign Terrorist Organizations*).

185 ראו Rachel E. Van Landingham, *Jailing the Twitter Bird: Social Media, Material Support to Terrorism and Muzzling the Modern Press*, 39 CARDOZO L. REV. 1, 48 (2017).

186 DION-SCHWARZ, MANHEIM & JOHNSTON, לעיל ה״ש 3. מפנים ל־ELI BERMAN, RADICAL, RELIGIOUS, AND VIOLENT: THE NEW ECONOMICS OF TERRORISM (2009). יצוין כי הדבר נכון גם לפעילות עבריינית אחרת. קשה עד בלתי אפשרי להפריד בין הפעילות הפיננסית הלגיטימית לפעילות הלא לגיטימית.

187 Holder v. Humanitarian Law Project (HLP), 561 U.S. 1 (2010), ראו גם Olivia G. Chalos, *Bank Liability Under the Antiterrorism Act: The Mental State Requirement Under § 2333(a)*, 85 FORDHAM L. REV. 303, 326 (2016).

188 Lavi, לעיל ה״ש 54, בעמ׳ 510; עניין *Holder*, לעיל ה״ש 187, בעמ׳ 7–8.

189 עניין *Holder*, שם, בעמ׳ 30–31; Lavi, לעיל ה״ש 54, בעמ׳ 511.

190 Chalos, לעיל ה״ש 187, בעמ׳ 315 (“The provision is designed to criminalize all financial supporters of terrorists, including those who fund terrorism in the guise of philanthropic and charitable activities. It is the most frequently charged of the terrorist financing statutes”). ראו גם Lavi, לעיל ה״ש 54, בעמ׳ 511; הרפון, לעיל ה״ש 26, בעמ׳ 223.

191 Chalos, לעיל ה״ש 187, בעמ׳ 307.

192 שם.

nevo.co.il

מעודדת גופים כמו בנקים לגדוע את השרשרת שמאפשרת את הטרור.[193] אולם, למרות שאחריות יכולה להיות מוטלת על בנקים בשל תמיכה מהותית,[194] בתי משפט חלוקים בשאלה האם סעיף 2333 מאפשר אחריות משנית לפי התאוריה של סיוע או עזרה למעשים שהם טרור וחלוקים בשאלת רמת האשם הנדרשת לביסוס אחריות אזרחית תחת סעיף 2333 (a),[195] והפסיקה בנושא אינה עקיבה. יחד עם זאת, נציין כי נראה שפסק הדין של בית המשפט העליון שניתן לאחרונה בארצות הברית בעניין *Twitter, Inc. v. Taamneh* שעניינו משיק לענייננו, טרף את הקלפים. בפסק הדין פירש בית המשפט את החוק בצמצום ונדחתה אחריותה של פלטפורמה אינטרנטיות לסיוע לטרור. לפרשנות מצמצמת זו יכולות להיות השלכות גם לגבי הסיכוי לביסוס אחריות המערכת הבנקאית ונראה כי לאחר פסק הדין, קטן הסיכוי כי תוטל אחריות על המערכת הבנקאית לסיוע או עזרה לטרור.[196]

(1) איסור מימון טרור בישראל

יסודות המשפט הישראלי למאבק במימון טרור הם תקנות ההגנה (שעת־חירום), 1945 ופקודת מניעת טרור, התשע״ח–1948. מכוח מקורות אלה ניתן להכריז על ארגון כארגון טרור ולהחרים רכוש השייך לו.[197] בשנת 2000 נחקק כאמור חוק איסור הלבנת הון,[198] אשר קובע חובות פיקוח מוגבר על העברות כספים חשודות כדי להביא בין השאר לגדיעת מימון טרור. ב־2005 נחקק חוק איסור מימון טרור, התשס״ה–2005, ושמה של הרשות לאיסור הלבנת הון שונה לרשות לאיסור הלבנת הון ומימון טרור. החוק הוחלף בחוק המאבק בטרור, התשע״ו–2016, שאישרה הכנסת ביום 15 למאי 2016. חקיקה זו התפתחה מתוך הבנה ששיתוף פעולה בין־מדינתי הוא תנאי הכרחי למאבק בטרור,[199] ומוסדות פיננסיים נדרשו ליטול חלק במאבק בטרור וליטול חלק באכיפה,[200] לדוגמה, לסרב לתת שירות,[201] להקפיא חשבונות או לסגור אותם.[202]

193 שם, בעמ׳ 306.

194 ראו לדוגמה, Linde v. Arab Bank PLC, No. 04-CV-02799 (E.D.N.Y. Sept. 22, 2014), בית משפט הטיל אחריות על בנק בשל תמיכה מהותית. הבנק סיפק כספים לחמאס וארגוני טרור ייעודיים מוכרים נוספים ששימשו להתקפות טרור בין השנים 2002–2004; ראו גם הרפון, לעיל ה״ש 26, בעמ׳ 216, 223.

195 Chalos, לעיל ה״ש 187, בעמ׳ 307.

196 שם, בעמ׳ 308. ראו פסק הדין של בית המשפט העליון בו נדחתה אחריות פלטפורמות לסיוע לטרור Twitter, Inc. v. Taamneh, No. 21–1496 (SCOTUS May 18, 2023), פסק הדין פירש את סעיף 2333 ל־ATA- Anti-Terrorism Act בצמצום וקבע כי לא הוכח שטויטר קשרה קשר עם ארגון המדינה האיסלמית כדי לבצע פיגוע או לפעול ביודעין כדי לגרום להצלחתו. כך, דחה בית המשפט את האחריות.

197 לוסטיג, לעיל ה״ש 100, בעמ׳ 901.

198 שם, בעמ׳ 902.

199 שם, בעמ׳ 902

200 שם, בעמ׳ 909–910 מסבירה כי מקור החוקים גלובלי והם בהתאם להנחיות ה־FTAF, וסוכן אכיפת החוק אינו גוף מדינתי קלסי.

nevo.co.il

חוק המאבק בטרור נותן בידי הרשויות כלים משפטיים להתמודד עם איומי הטרור, להעמיד את ישראל בשורה אחת עם המדינות הנאבקות בטרור ובמימון הטרור הבין־לאומי ולהבטיח כי החקיקה הישראלית עומדת בסטנדרטים הבין־לאומיים שנקבעו בהקשר זה.[203] החוק קובע הוראות שונות ורבות בקשר עם המאבק בטרור, שעיקרן במשפט הפלילי, הביטחוני והמנהלי, ומאמץ שורה של הוראות מחוק איסור מימון טרור. החוק מקנה סמכות לשר הביטחון להכריז על ארגון טרור או על פעיל טרור בשל הכרזה מחוץ לישראל.[204] בחוק נקבעו חובות דיווח על פעולות ברכוש טרור, השייך לארגון טרור או הקשור לעבירה שהיא עבירת טרור או עשויה לקדם פעילות טרור.[205] חובות דיווח אלה התקיימו גם במסגרת חוק איסור מימון טרור, שאותו החליף החוק, אולם החוק מרחיב את חובת הדיווח על מוסדות פיננסיים, לעומת חוק איסור מימון טרור, ומטיל גם חובת דיווח למשטרה, ולא רק לרשות לאיסור הלבנת הון ומימון טרור.[206] סעיף 33 מטיל חובת דיווח על מי שהתבקש ״לעשות פעולה ברכוש במהלך עסקיו או במילוי תפקידו, או בנסיבות שבהן היתה לו אפשרות של ממש לביצוע הפעולה״ כאשר היה לאותו אדם חשד סביר כי ״הרכוש הוא רכוש של ארגון טרור, או שהוא תמורתו הישירה, או הרווח הישיר של רכוש כאמור״ או ש״יש בפעולה כדי לקדם, או לממן ביצוע של עבירת טרור חמורה, לסייע לביצוע עבירת טרור חמורה, או לתגמל בעבור ביצוע של עבירה כאמור.״[207] חובת דיווח זו חלה גם אם החשד התעורר בתוך שישה חודשים מביצוע הפעולה.[208] החוק קובע עבירות פליליות שעניינן המאבק בטרור. העבירה המרכזית לענייננו היא הפרת חובת דיווח. עבירה זו נקבעה כעבירה שדינה מאסר או קנס גם כאשר התעורר חשד שהארגון הוא ארגון טרור והעושה פעולה ברכוש טרור נמנע מלברר חשד זה.[209]

201 לוסטיג, לעיל ה״ש 100, בעמ׳ 907, מפנה לרע״א 6582/15 **עמותת איעמאמר לפיתוח וצמיחה כלכלית נ׳ בנק הדואר** (נבו 1.11.2015) (שם בנק הדואר קיבל מידע שחשבונות העמותה נסגרו מחשש למימון טרור וסירב לתת לה שירות פיננסי. נקבע כי מטילות על הבנק תפקיד ציבורי, מנהלי ואכיפתי, בהיותו הגורם העומד בחזית המאבק בהלבנת הון ומימון טרור).

202 רע״א 2407/19 **ישראל זיו נ׳ בנק לאומי לישראל** (נבו 14.5.2019) שם בית משפט דחה בקשת רשות ערעור על דחיית בקשת המבקשים למתן סעד זמני המורה לבנק לאומי להימנע מהקפאת חשבונות הבנק שלהם לנוכח הכללת משרד האוצר האמריקאי את המבקשות ב״רשימה שחורה״ של גופים החשודים בהלבנת הון או במימון טרור.

203 ראו חוק המאבק בטרור; **הרשות לאיסור הלבנת הון ומימון טרור** https://bit.ly/3yrrQvw.

204 ס׳ 11(א)(1-2) לחוק המאבק בטרור; לוסטיג, לעיל ה״ש 100, בעמ׳ 913. לוסטיג מבקרת סעיפים אלה שבאמצעותם כאמור חייב המחוקק הישראלי את רשויות אכיפת החוק במדינה לשמש סוכני אכיפה של מנגנון קבלת החלטות גלובלי, מבלי שהם נדרשים לוודא בעצמם את תוקף הממצאים העומדים ביסוד החלטותיו ומשמעותם, שם, בעמ׳ 916. אולם נראה כי כדי להתמודד עם טרור גלובלי נדרש תיאום גלובלי, ומדינה אינה יכולה ללחום בטרור ביעילות אם תפעל אוטונומית.

205 ס׳ 32—34 לחוק המאבק בטרור.

206 שם, ס׳ 32—33.

207 שם, ס׳ 33(א)(1-2).

208 שם, ס׳ 33(א) לחוק ״...והיה לו במועד עשייתה או בתוך שישה חודשים מהמועד האמור, חשד סביר כאמור, ידווח על כך למשטרת ישראל״.

209 שם, ס׳ 36.

נבו nevo.co.il

חוק המאבק בטרור מפנה בסעיף 35 לסעיפי הפטור מאחריות בחוק איסור הלבנת הון ופוטר מאחריות "אי־עשיית פעולה ברכוש, מחדל אחר או מעשה שנעשו בתום לב כדי להימנע מעבירה לפי חוק זה, וכן דיווח, גילוי או אי־גילוי שנעשו בתום לב לצורך קיום הוראות חוק זה".[210] כמו כן החוק פוטר מאחריות אף לפעולה בהתאם להוראות משטרת ישראל וקובע כי אין בפעולות אלה הפרה של חובות סודיות ונאמנות, או של חובה אחרת לפי כל דין או הסכם. כך, מוסדות פיננסיים פטורים מאחריות שאחרת עלולה הייתה לנבוע ממילוי חובות הדיווח.

המלחמה בהלבנת הון ובמימון טרור היא מלחמה שאפשר לנצח בה רק אם יהיה קשה לעקוף את החקיקה והרגולציה באשר לאיסור הלבנת הון ומימון טרור. עקיפת מתווכים פיננסיים מסורתיים מאפשרת לעקוף את האכיפה של העברות לא חוקיות ואת השימוש בכסף למימון טרור. כפי שידגים המאמר, שימוש במטבעות אלקטרוניים עוקף את המתווכים המסורתיים ומאפשר זרימת כספים ותמיכה בפעילות טרור.

ב. מהם מטבעות אלקטרוניים? כיצד הם עובדים? וכיצד משתמשים בהם לקידום טרור?

1. מטבעות אלקטרוניים

מטבעות אלקטרוניים הם מטבעות שנוצרים באופן אלקטרוני ומאוחסנים על גבי מחשב. מטבעות אלה מהווים למעשה תצוגה דיגיטלית של ערך, שאינה מבוססת על הילך חוקי כלשהו. מטבעות אלה מאפשרים עשיית עסקאות בשוק החופשי,[211] שכן הם ניתנים להעברה ויכולים להיות מוחלפים בהתבסס על עקרונות סחר חליפין.[212] בשונה מכסף מזומן, השימוש במטבעות אלה אינו מצריך מפגש פיזי של נותן התשלום ומקבלו כדי להשלים את פעולת התשלום, וניתן לבצעה באופן וירטואלי, ולעיתים אף חוצה גבולות.[213]

ב־2008 הוצג לעולם המטבע האלקטרוני הראשון והידוע ביותר – ביטקוין, שנכנס לשימוש החל משנת 2009.[214] המטבע הוצג במסגרת מסמך בשם "White Paper", שכותרתו "מערכת אלקטרונית להחלפת מזומן ישירות בין משתמשים – ביטקוין". המטבע הופץ על ידי ישות אנונימית תחת השם "סאטושי נקאמוטו".[215] אותו מסמך חשף כי הביטקוין מועבר מיד ליד על ידי טכנולוגיה בשם בלוקצ׳יין, המהווה פרוטוקול לאחסון בטוח והעברה של מטבעות וירטואליים, וחשף את שם יחידת הערך במערכת. ב־White Paper הוסבר כי הביטקוין הוא מטבע דיגיטלי מוצפן שיכול להיות מועבר ממחשב של משתמש אחד למחשב של משתמש

210 שם, ס׳ 35.

211 ראו בן אוליאל וחיים, לעיל ה״ש 16, בעמ׳ 357; Jabotinsky, לעיל ה״ש 37.

212 שם, בעמ׳ 357–358.

213 באום, לעיל ה״ש 2, בעמ׳ 279.

214 שם, בעמ׳ 296.

215 Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) (hereinafter: White Paper), git.dhimmel.com/bitcoin-whitepaper.

nevo.co.il

אחר מבלי להיזקק לישות מרכזית או לרישום העסקה ומבלי להישלט על ידי ממשלות או גוף מוניטרי מרכזי המנפיק את המטבעות.[216] תחת זאת, עסקאות מתועדות בטכנולוגיה של שרשרת לוחות מבוזרת (distributed ledger technology (DLT)), שמאפשרת למשתמשים לעקוב אחר העסקאות הרשומות. מאחר שהטכנולוגיה מורכבת מבלוקים שמקושרים אחד לשני דרך חתימה דיגיטלית מוצפנת, היא נקראת הבלוקצ׳יין.[217]

הבלוקצ׳יין של הביטקוין הוא הזירה שבה המטבעות נסחרים ומאוחסנים. הבלוקצ׳יין נשמר על רשת עמית־לעמית (peer-to-peer), והמערכת המבוזרת עוקבת אחר העסקאות ומשמרת את ההיסטוריה השלמה של העסקאות שאושרו ואומתו.[218] בכל פעם שנוצר ונחתם בלוק נוסף, הרשת מתעדכנת אצל כל העמיתים, כך שכולם יכולים לצפות ברישום העסקאות. בהתאם לכך, ולאור טבעו של הבלוקצ׳יין הציבורי, כל משתמש במערכת יכול להשתתף בכל ההיבטים של התפעול, כולל כל העסקאות, אבל אין אף משתמש יחיד שיש לו שליטה במערכת. כדי לתמוך באנונימיות העסקאות בביטקוין, הארנקים האלקטרוניים של המשתתפים מזוהים על ידי מחרוזת של מספרים רנדומליים, במקום באמצעות שם או מידע אישי אחר.[219] כל מטבע ביטקוין הוא בעל מזהה ייחודי (מספר סידורי שמוענק לו עם יצירתו).[220] כדי לעשות שימוש בביטקוין, על כל משתמש להתקין תוכנת מחשב שיוצרת ארנק אלקטרוני שבו יישמרו מטבעותיו.[221] השימוש בארנק מבוסס על ידיעת המפתח הציבורי (המספר המזהה של

216 Nakamoto, שם; Roee Sarel, *Property Rights in Cryptocurrencies: A Law and Economics Perspective*, 22 N.C. J.L. & Tech. 389, 397 (2021); בן אוליאל וחיים, לעיל ה״ש 16, בעמ׳ 359; באום, לעיל ה״ש 2, בעמ׳ 279.

217 De Filippi, לעיל ה״ש 1; יצוין כי ה־Bitcoin White Paper המקורי (ה״ש 215) אינו משתמש במונח הספציפי ״בלוקצ׳יין״, ומונח זה התפתח מאוחר יותר. אותו מסמך מתייחס לשרשרת (“The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work”). להסבר מפורט על טכנולוגיית הבלוקצ׳יין ראו Lin William Cong & Zhiguo He, *Blockchain Disruption and Smart Contracts*. 32 Rev. Financ. Stud. 1754 (2019). לסקירה בנושא המטבע ביטקווין בפרט ראו Christian Rueckert, *Cryptocurrencies and Fundamental Rights,* 5 J. Cybersecurity 1 (2019).

218 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3; Robby Houben & Alexander Snyers, Cryptocurrencies and Blockchain, Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion (2018).

219 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 2. יצוין כי הביטקוין מספק רק אנונימיות לכאורה (פסאודו אנונימיות), ולא אנונימיות מוחלטת. ראו See Ermilov, Dmitry, Maxim Panov & Yury Yanovich, *Automatic Bitcoin Address Clustering*, 16th IEEE International Conference on Machine Learning and Applications, 461 (2017) (“Bitcoins owning and transferring (addresses and transactions) is available as a public ledger called blockchain. But real-world owners of addresses are not known in general. That’s why Bitcoin is called pseudo-anonymous. However, some addresses can be grouped by their ownership using behavior patterns and publicly available information from off-chain sources”).

220 ראו בן אוליאל וחיים, לעיל ה״ש 16, בעמ׳ 360

221 שם.

nevo.co.il

המשתמש בפני כלל המשתמשים) והמפתח הפרטי של המשתמש (סיסמה אישית הידועה רק לו ומאפשרת גישה מאובטחת למטבעות).[222] ביטקוין נוצר בהליך המכונה "כרייה", שבו המחשב הכורה מבצע פעולות חישוביות הדרושות לאבטחת מידע הנוגעת לשימוש בכלל מטבעות הביטקוין. הרשת חדה למחשבים חידה מתמטית, ובעליו של המחשב שמגיע ראשון לפתרון הבעיה מתוגמל בביטקוין.[223] פרט לכרייה, אפשר לרכוש ביטקוין גם ממשתמשים אחרים.[224] כאמור, הבלוקצ׳יין מאפשר את שמירת כל המידע על יצירת מטבעות ביטקוין, השימוש בהם והעסקאות שנעשו באמצעותם.[225] המידע בשרשרת נשמר בכל אחד ממחשבי משתמשי הביטקוין ומוגן מפני פלישה זדונית על ידי הכוח החישובי המיוצר בידי הכורים.[226]

גם המטבע את׳ר הנמצא בשימוש נרחב פועל בצורה דומה בבלוקצ׳יין של את׳ריום (Etheruem).[227] הבלוקצ׳יין של קרן את׳ריום מאפשר למשתמשים ליצור חוזים חכמים.[228] חוזים אלה הם פקודות מחשב שאומרות למחשב אם x מתרחש עשה y.[229] רשת בלוקצ׳יין זו מאפשרת לחברות אחרות להשתמש בה, כדי לפתח את מטבעותיהן ולהנפיקם בתהליך של הצעת מטבע ראשונית Initial Coin Offering (ICO). גם בבלוקצ׳יין של קרן את׳ריום נשמרת אנונימיות המשתמשים.[230]

222 שם.
223 שם.
224 שם, בעמ׳ 361
225 שם.
226 שם.
227 Shaanan Cohney & David A. Hoffman, *Transactional Scripts in Contract Stacks*, 105 MINN. L. REV. 319, 335–336 (2020) ("a programmer named Vitalik Buterin proposed and developed Ethereum, a blockchain based computing platform, with an associated cryptocurrency, Ether The protocol's explicit goal was to permit enhanced scripting—more complicated logical operations than recording ownership—on a blockchain"). ראו גם GAVIN WOOD ET AL., ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER 151 (2014); Ethereum Project Yellow Paper 1-32 (2014).
228 Smart Contracts: 10 Use Cases for Business, AMBISAFE, https://bit.ly/3ACKbrQ ("Smart contracts do not require any intermediaries. Hence, you pay *no fees*. As there's no bureaucracy involved, *transactions become fast and cheap*. Moreover, the transparency guaranteed by the blockchain reduces the possible risks of fraud"); Alexander Savelyev, *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COMMC'N. TECH. L. 116 (2017); *Ethereum Smart Contract Best Practices*, GitHub: ConsenSys: bit.ly/3oL4KJW; Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, First Monday (Dec. 5, 2016), https://bit.ly/3NJ3R0d ("[S]mart contracts are actually meant to replace legal contracts").
229 Jabotinsky, לעיל ה״ש 37, בעמ׳ 143.
230 Sergio Martins& Yang Yang, *Introduction to Bitcoins: A Pseudo-anonymous Electronic Currency System*, Proceeding of the 2011 Conference of the Center for Advanced Studies on Collaborative Research (2011).

nevo.co.il

אחד מהמטבעות האלקטרוניים היותר מדוברים, שגם חזו לו הצלחה מרובה, היה מטבע בשם דיאם (Diem) – פרי יוזמה של פייסבוק.[231] הדיאם היה אמור להיות מטבע גלובלי המעוצב להחליף חלק ממטבעות ההילך החוקי, כך שתתאפשר העברת כסף לאחרים או קניית טובין כמעט ללא עמלות.[232] על פי החזון, כדי להשתמש בדיאם, משתמשים יצטרכו לטעון אפליקציה של ארנק כמו Novi, האפליקציה שפייסבוק עיצבה לשימוש במטבע החדש. האפליקציה הייתה אמורה להיבנות כך שתותאם לוואטסאפ והמסנג׳ר של פייסבוק.[233] משתמשי האפליקציות הללו יצרו בעיני פייסבוק את בסיס המשתמשים הפוטנציאלי של המטבע.[234] מטבעות הדיאם היו אמורים להיות מוצמדים לסל של בנק מטבעות פיאט (מטבעות מדינתיים כגון יורו, דולר וכולי) כדי להפחית תנודות בערך שבדרך כלל מתקשרות לשימוש במטבעות אלקטרוניים.[235] בשונה ממטבעות אלקטרוניים אחרים, כמו ביטקוין, את׳ר ורוב המטבעות האלקטרוניים האחרים שבנויים על הבלוקצ׳יין של קרן את׳ריום, הדיאם אמור היה לפעול על גבי בלוקצ׳יין פרטי. על פי התוכנית, המשתתפים בבלוקצ׳יין היו אמורים להיות מזוהים לפני כניסתם לבלוקצ׳יין, כך שזהותם הייתה אמורה להיות ידועה לקרן הדיאם. הבלוקצ׳יין של דיאם אמור היה להיות מנוהל על ידי חברי הקרן של דיאם.[236] המשמעות היא ששרשרת העסקאות הייתה אמורה להיות נגישה רק למשתמשים אלה, ושהם יוכלו לשלוט במי מקבל גישה לעשיית עסקאות על גבי הבלוקצ׳יין. כך, מאחר שקרן הדיאם אמורה הייתה לשלוט בנקודת הכניסה למערכת של המטבע, הוא נחשב לפחות מבוזר לעומת מטבעות אלקטרוניים אחרים.[237] בתחילת פברואר 2022, לאור חששות רגולטורים בארצות הברית ובעולם, פייסבוק גנזה את התוכנית ומכרה את הטכנולוגיה לחברה אחרת,[238] ואף הארנק הדיגיטלי Novi צפוי להיסגר.[239]

הנפקת מטבע ראשונית (ICOs) של מטבעות אלקטרוניים היא התהליך שבו מגויס כסף מהציבור לשם פיתוח המטבע. הנפקות אלה הן אטרקטיביות ליזמים מסיבות שונות, חלקן לגיטימיות וחלקן פחות. סיבות לגיטימיות יכולות לכלול את העובדה שהנפקת מטבע, בשונה

231 Jabotinsky, לעיל ה״ש 37, בעמ׳ 146.

232 Jabotinsky & Sarel, לעיל ה״ש 14, בעמ׳ 24.

233 Josh Constine, *Facebook Announces Libra Cryptocurrency: All You Need to Know*, TECHCRUNCH (June 18, 2019), techcrunch.com/2019/06/18/facebook-libra; Jabotinsky, לעיל ה״ש 37, בעמ׳ 146.

234 John Taskinsoy, *This Time is Different: Facebook's Libra Can Improve Both Financial Inclusion and Global Financial Stability as a Viable Alternative Currency to the U.S. Dollar*, 5 FINANCE & AUDITING STUDIES 67,71 (2019).

235 Jabotinsky & Sarel, לעיל ה״ש 14, בעמ׳ 23.

236 האיגוד של דיאם (ליברה) הוא ארגון עצמאי שאחראי לממשל ברשתות ליברה והפיתוח של הפרויקט של ליברה. ראו DiemAssociationhttps://www.diem.com/en-us/, ראו גם Jabotinsky, לעיל ה״ש 37, בעמ׳ 146–147.

237 Jabotinsky & Sarel, לעיל ה״ש 14, בעמ׳ 24; Jabotinsky, לעיל ה״ש 37, בעמ׳ 146–147.

238 Romain Dillet, *Facebook Ditches Diem Stablecoin with Asset Sale to Silvergate*, TECHCRUNCH (Jan. 27, 2022), https://tcrn.ch/3OPJb8j.

239 Olga Kharif, *Meta to Shut Down Novi Service in September in Crypto Winter,* BLOOMBERG (July 3,2022) https://bloom.bg/3InFLas.

nevo.co.il

ממניות, מאפשרת ליזם לשמר את כל זכויותיו בתאגיד בלי דילול, ועדיין לגייס כסף, להגיע ליותר משקיעים ברחבי העולם ולהימנע מדרישות רגולטוריות יקרות.[240] מסיבות אלה, השוק להנפקות פרח בשנים 2016–2019 וגייס מעל לשלוש מאות מיליארדי דולרים ממשקיעים ברחבי העולם.[241] בשנים אלה חזינו בפלטפורמות שקמו על מנת לאפשר מסחר במטבעות אלקטרוניים בלבד וסיפקו לשוק נזילות. האפשרות להעביר את המטבעות בין המשתמשים יוצרת שוק שבו מוכרים וקונים של מטבעות יכולים לערוך ביניהם חילופין.[242] אולם לצד הסיבות הלגיטימיות להנפקה ושימוש במטבעות אלקטרוניים, ישנן גם סיבות שאינן לגיטימיות. בין היתר, ניצול תכונת האנונימיות של המטבע לצורך הלבנת הון,[243] התחמקות ממס,[244] הונאות פונזי[245] ותמיכה בארגוני טרור.[246]

2. מדוע וכיצד משתמשים ארגוני טרור ופשע במטבעות אלקטרוניים?

לשם הוצאה לפועל של פעולות טרור נדרש מימון משמעותי. מימון זה נדרש לצורכי תעמולה, גיוס, אימון, משכורות וניהול ארגון הטרור.[247] לדוגמה, ארגון המדינה האסלאמית (ISIS) אישר תקציב של שני מיליארד דולר לשנת 2015. עלויות של התקפות ספציפיות יכולות להתחיל מתקציב של 10,000 דולר עבור התקפות הטרור בפריז בשנת 2015 ועד ל־400,000–500,000 דולר להתקפות ה־9/11 בארצות הברית. כסף הוא המנוע לפעילות טרור.[248] ככל שיש לארגוני הטרור יותר כסף, היכולת שלהם לגייס חברים, לארגן ולבצע התקפות טרור גוברת.[249] גיוס מקורות ההכנסה והמימון של ארגוני טרור משלב שיטות מסורתיות ולא מסורתיות. ארגונים אלה תלויים במגוון מקורות כספיים המגיעים מעבירות פליליות ושימוש לרעה בפעילות לגיטימית. דוגמאות לפעילות פלילית שמייצרת הכנסות לארגון הטרור כוללות סחר בנשק וסמים, חטיפה ודרישות כופר, סחיטה ואיומים. נוסף על זה, ארגוני טרור והנלווים

240 Sarel, לעיל ה"ש 216, בעמ' 399–400.

241 שם, בעמ' 400.

242 שם.

243 Van Wegberg et al., *Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin*, 25 J. Fin. Crime 17 (2018). ראו לדוגמה מנחם שטאובר "פרשת טלגראס: כתב אישום נגד ארז שמואלי בגין הלבנת הון באמצעות מטבעות קריפטו" **גלובס** (12.6.2019) https://bit.ly/3nFvCMD.

244 Van Wegberg et al., שם; Thomas Slattery, *Taking a Bit out of Crime: Bitcoin and Cross-Border Tax Evasion*, 39 Brook. J. Int'l L. 829 (2014); עמיר קורץ "כתב אישום שני בגין העלמת הכנסות ממכירת ביטקוין – והקשר לפרשת טלגראס" **כלכליסט** (27.1.2021) https://bit.ly/3NQ6Cge.

245 Investor Alert, Ponzi schemes Using virtual Currencies, Sec Pub. No. 153 (7/13) https://www.sec.gov/files/ia_virtualcurrencies.pdf.

246 Dion-Schwarz, Manheim & Johnston, לעיל ה"ש 3.

247 FATF Report, Emerging Terrorist Financing Risks (2015) www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.

248 Goldman et al., לעיל ה"ש 13, בעמ' 10.

249 הרפון, לעיל ה"ש 26.

nevo.co.il

אליהם מקבלים מימון מתרומות, חסות ומקורות חוקיים כמו הלוואות אשראי ועסקים.[250] לאחר גיוס הכספים, ארגוני הטרור צריכים לנהל את כספיהם. אם הכסף אינו תחת השליטה הישירה של ארגון הטרור, או אם אי אפשר להעבירו בגלל חשש מבעיות אבטחה תפעוליות, הטרוריסטים יכולים לנסות להלבין את ההון כדי להעביר את הכסף בשביל לתמוך בצורך שלהם במזומן לארגון שלהם. ארגוני טרור מוציאים את הכסף שהם מקבלים על משכורות ושירותים, אולם משתמשים בו גם לפעילות כמו גיוס פעילי טרור, אימון שלהם, תעמולה, רכישת נשק, התקפות טרור והוצאות קשורות.[251] מאחר שחלק מהמטבעות האלקטרוניים נהנים מאנונימיות, ומאחר שלא ניתן לדעת מי עומד מאחורי הארנקים האלקטרוניים שמבצעים את ההעברות, הם מהווים כר פורה ונוח להעברת כספים שמיועדים לטרור.

גם ארגוני פשע נזקקים לצינורות של העברת כספים והלבנתם. כפי שכבר ציינו, הלבנת הון היא עשיית פעולה ברכוש אסור. ארגוני הפשע מנסים להסוות את מקור הכסף ולהחדירו למערכת הפיננסית ככסף לגיטימי. תכונת האנונימיות של חלק מהמטבעות האלקטרוניים מאפשרת לארגוני פשע להעביר כספים ברחבי העולם ולהמיר אותם בסוף לכסף פיאט שנכנס למערכת הפיננסית המסורתית ככסף לגיטימי. בכך עוקפים ארגוני הפשע את חוקי איסור הלבנת ההון ברחבי העולם.[252]

3. האנונימיות של חלק מן המטבעות האלקטרוניים וחשיבותה לפעילות טרור ופשיעה

מטבעות אלקטרוניים הם אטרקטיביים לטרוריסטים ופושעים, מאחר ששימוש במטבעות אנונימיים יכול לקדם את פעילותם, לסייע להם לבצע עסקאות ולאפשר להם לקבל מימון, לנהל כספים ולהשתמש בהם. מטבעות אלה מאפשרים העברת כספים מיידית ברחבי הגלובוס ללא מתווכים דוגמת בנקים, אשר דורשים יותר שקיפות ומחויבים לדווח על עסקאות חשודות בחשבונות לקוחותיהם. אנונימיות המטבעות האלקטרוניים מאפשרת להסתיר את זהות המשתמש. שעה שהרוכש המקורי של המטבע יכול להיות מזוהה, לדוגמה באמצעות המערכת הבנקאית, קשה לאתר את כל ההעברות שלאחר מכן.[253] יש להודות כי האנונימיות על גבי הבלוקצ׳יין אינה מוחלטת[254] ואינה מספקת לחלקם של המשתמשים,[255] מאחר שדרגת האנונימיות תלויה בגורמים תפעוליים וטכניים, ואפשר לעשות דה־אנונימיזציה ולחשוף את

250 Goldman et al., לעיל ה״ש 13, בעמ׳ 10.
251 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 13.
252 Alex Vet, *Italian Mafia Launders Money Through Crypto*, Coinatory (Apr. 6, 2019) bit.ly/2G0u1P8.
253 FATF Report, לעיל ה״ש 247.
254 Paul Carroll & James Windle, *Cyber as an Enabler of Terrorism Financing, Now and in the Future*, 13 J. Policing, Intelligence & Counter Terrorism 285 (2018).
255 Stephan Breu & Theodor G. Seitz, *Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on Economy and Society*, *in* Legal Impact on the Economy 4 (2018).

nevo.co.il

זהות המשתמשים במגוון שיטות.[256] אולם, דה־אנונימיזציה כרוכה בעלויות, וחשיפת הזהויות יכולה לקחת זמן. יתרה מזו, ארנקים דיגיטליים שמגבירים את דרגת האנונימיות על ידי ערפול עסקאות ביטקוין (dark wallets) מקשים מאוד על דה־אנונימיזציה בעסקאות במטבעות אלקטרוניים ומאפשרים עסקאות לא חוקיות.[257]

אנונימיות בעסקאות פיננסיות היא היבט חשוב בכל אחד מסוגי הפעילות הפיננסית של ארגוני טרור כפי שנסביר להלן: ראשית, אנונימיות חשובה לגיוס כספים.[258] מאחר שאין זה חוקי לספק תמיכה מהותית לארגון טרור, היעדר אנונימיות מרתיע את התורמים.[259] בדומה לזה, כדי לגייס כספים למבצעי טרור נדרשת אנונימיות, מאחר שמעורבות אקטיבית בגיוס כספים לארגוני טרור ו/או למבצעי טרור אינה חוקית, ואם תיחשף זהות הגורמים שאליהם עוברים הכספים, עסקאות אלה יסוכלו בידי הרשויות.[260] לפיכך, אם מטבעות אלקטרוניים ישארו אנונימיים, האנונימיות שהם מאפשרים תאפשר לעקוף את הרגולציה המערבית, אשר מגבילה תרומות לג׳יהאד דרך הגבלות על המערכת הבנקאית.[261] שנית, אנונימיות בעסאות פיננסיות היא קריטית עבור סחר לא חוקי בסמים וסחר בתחמושת ונשק. אנונימיות נדרשת לארגוני טרור ופשיעה כדי לא להתגלות על ידי הרשויות במהלך ולאחר העסקה.[262] לבסוף, אנונימיות חשובה למימון התקפות טרור, מאחר שחיוני לארגוני טרור שהתוקף שמקבל את הכספים לא יתגלה לפני מבצע התקפת הטרור.[263]

פעילי טרור יכולים להסוות את זהותם ולהפחית את הסיכון שהתקשורת והפעילות הפיננסית שלהם תתגלה. שעה שטרוריסטים היו אקטיביים במגוון פלטפורמות אינטרנטיות למעלה משני עשורים, רשת האינטרנט מציבה פעילי טרור המבקשים להישאר אנונימיים בסיכון, מאחר שאפשר לפקח על פעילותם, לאתר ולמצוא אותם.[264] אולם, חלקים נרחבים מהאינטרנט נמצאים מתחת ל״קו המים״ המטפורי, לא ניתן לחפש בהם והם אינם נגישים לציבור הרחב.[265] השכבה העמוקה ביותר של הרשת העמוקה ידועה כרשת האפלה. שכבה זו

256 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 25; Brenna Smith, *The Evolution of Bitcoin in Terrorist Financing*, Bellingcat (Aug. 9, 2019) www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/; Carroll & Windle, לעיל ה״ש 254 ("Cryptocurrencies provide increased, rather than complete, anonymity as they are added to blockchains which can be used to trace the originating electronic wallet from which the cryptocurrency was sent").

257 Goldman et al., לעיל ה״ש 13, בעמ׳ 15.

258 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 32.

259 להרחבה על החקיקה האמריקאית בנושא תמיכה בטרור ראו חלק א. 2(ב) למאמר זה.

260 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, בעמ׳ 32.

261 לרגולציה אשר מטילה חובות על המערכת הבנקאית כדי למנוע הלבנת הון ומימון טרור ראו חלק א.2.

262 Dion-Schwarz, Manheim & Johnston , לעיל ה״ש 3, בעמ׳ 32.

263 שם, בעמ׳ 33.

264 ראו Gabriel Weiman, Going Darker? The Challenge of Dark Net Terrorism 4 (2020).

265 Weiman בעמ׳ 8, מסביר כי כל משתמש אינטרנט יכול לפעול ברשת האפלה בשימוש בתוכנה מיוחדת כמו דפדפן TOR (The Onion Router), כלי המאפשר לתקשר באנונימיות באינטרנט.

nevo.co.il

מכילה תוכן שהוסתר במכוון, כולל פעילות לא חוקית ותוכן אנטי־חברתי.[266] שכבה זו מאפשרת העברות חבויות של כספים, בשימוש במטבעות אלקטרוניים שממלאים את הצורך של ארגוני הטרור באנונימיות ומבטיחים את זרם המימון לפעילותם.

המגמה החדשה היא השילוב המדאיג של טרור מאורגן ויכולות של הרשת האפלה.[267] בגלל שחלקם של המטבעות האלקטרוניים מספקים את אותה צורה של אנונימיות במיקום הפיננסי כמו שהרשת האפלה מספקת למערכות תקשורת, מטבעות אלקטרוניים הם רגישים לניצול לרעה על ידי טרוריסטים שיכולים להשתמש בהם וליהנות מניצול יתרונותיהם.[268] בשונה מהעברות בנקאיות רגילות בחשבונות בנק, ממשלות וגורמי אכיפת החוק מתקשים לשלוט בעסקאות, לעצור עסקאות, לעקוב אחר נכסים אלקטרוניים (קריפטוגרפיים) ולהקפיא נכסים אלה כדי לשבש מימון לא חוקי.[269] פרטים יכולים לשנן את מחרוזת המספרים שמרכיבה את המפתח הפרטי או לרשום אותה על נייר ולשמור אותו היטב ולקבל גישה למימון בבלוקצ׳יין. כך טרוריסטים יכולים לגייס מימון באמצעות תרומות מטבעות אלקטרוניים מכל אחד ובכל מקום בעולם על ידי פרסום המפתח הציבורי שלהם באתר אינטרנט, ולהימנע מהסתמכות על מתווכים פיננסיים.[270] פרסום המפתח הציבורי מאפשר לנצל מטבעות אלקטרוניים כמו ביטקוין לקמפיינים של מימון המונים לפעילות טרור.[271] קשה לשבש את פעילותן של מערכות לא חוקיות אלה.[272]

כאשר הטכנולוגיה מקילה את השימוש במטבעות אלקטרוניים וברשת האפלה, הם הופכים להיות היבט שגרתי של חיינו, ולטרוריסטים יש יותר הזדמנויות לגייס כספים, לפעול ולבצע התקפות לא חוקיות, מבלי שהרשויות יאתרו אותם.[273] כתוצאה מזה, גדל האיום לביטחון הלאומי.[274]

(א) הקושי בסיכול מימון טרור *Counter Terrorism Financing (CTF)* המתבצע במטבעות אלקטרוניים

בלוקצ׳יין ציבורי משתמש ברשתות עמית־לעמית (peer-to-peer) שמנוהלות באופן אוטונומי ונטול מתווכים. המידע על הבלוקצ׳יין מאובטח ומבוזר, ללא שרת מרכזי שאותו ניתן לתפוס

266 שם, בעמ׳ 7.

267 שם.

268 Goldman et al., לעיל ה״ש 13.

269 Armin Krishnan, *Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations*, 13 J. STRAT. SEC. 41, 44 (2020).

270 שם, בעמ׳ 45.

271 Brenna Smith, *The Evolution of Bitcoin in Terrorist Financing*, BELLINGCAT (Aug. 9, 2019) www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing.

272 Carroll & Windle, לעיל ה״ש 254.

273 WEIMAN, לעיל ה״ש 264, בעמ׳ 4.

274 Carroll & Windle, לעיל ה״ש 254.

nevo.co.il

במקרה של חשד לעבירות פליליות. כתוצאה מזה, קשה מאוד לגורמי אכיפת החוק והביטחון לזהות את המשתמשים על הבלוקצ׳יין.[275]

רגולטורים ומחוקקים שונים זיהו את הסיכון העצום הטמון בשימוש במטבעות אלקטרוניים ואת הפוטנציאל של שימוש זה לחתור תחת הצלחת סיכול מימון טרור ועצירת פשיעה. רגולטורים בעולם אף החלו להסדיר הנפקות ראשוניות של מטבעות אלקטרוניים Initial coin offering (ICO)) במטרה להגן על משקיעים ולמנוע שימוש לא חוקי במטבעות. חלקם הטילו חובות הכרת הלקוח על נותני שירותים במטבעות האלקטרוניים והכפיפו אותם לחוקי איסור הלבנת הון ומימון טרור. נרחיב על אודות יוזמות חקיקה אלה בחלק הבא. נוסף על כך, חלקן של המדינות נקטו בגישה קיצונית ומחמירה ואסרו את הנפקת המטבעות. כך, דרום קוריאה וסין נקטו גישה קיצונית ומחמירה ואסרו על הנפקות של מטבעות אלקטרוניים לחלוטין.[276] דרום קוריאה אסרה על כל הצורות של גיוס כספים במטבעות אלקטרוניים ונקטה צעדים שמטרתם לדחוק לשוליים את השימוש במטבעות אלקטרוניים.[277] בסין עוד בספטמבר 2017 רוב החלפנים ושירותי ההמרה הודיעו שהם יעצרו את פעילותם הנוגעת למטבעות אלקטרוניים באופן וולנטרי, עד שהממשל בסין יודיע על הצעדים הרגולטוריים שבכוונתו לנקוט. לאחרונה נקבע בסין כי הנפקות של מטבעות קריפטוגרפיים אינן חוקיות.[278] הרשות המפקחת על שווקים פיננסיים בשווייץ Swiss Financial Markets Supervisory Authority (FINMA) הודיעה ב־2017 שתחקור כמה מקרים ספציפיים של הנפקות בחשד להפרת ההוראות של חוקי איסור הלבנת הון, חוקי איסור מימון טרור וחוקים נוספים.[279]

בעת הזו, עדיין שולטת אי־בהירות בשוק המטבעות האלקטרוניים סביב הנושא, ורגולטורים ובתי משפט סביב העולם צריכים לפעול לגיבוש פתרון קוהרנטי שימנע הלבנת הון ומימון טרור באמצעות מטבעות אלקטרוניים. משימת מפתח של מתווי המדיניות, אכיפת החוק, גורמי הביון וקהילות של רגולציה פיננסית היא למנוע מקבוצות של טרוריסטים ופושעים שימוש נרחב במטבעות אלקטרוניים.[280]

275 Breu & Seitz, לעיל ה״ש 255, בעמ׳ 2.

276 Saman Adhami et al., *Why do businesses go crypto? An empirical analysis of initial coin offerings,* 100 J. Econ & Bus.64, 64–75 (2018); וכן Jabotinsky & Sarel, לעיל ה״ש 14, בעמ׳ 3.

277 Breu & Seitz, לעיל ה״ש 255.

278 Bloomberg News, *China Widens Ban on Crypto Transactions; Bitcoin Tumbles*, Bloomberg (Sept. 24,2021) https://bloom.bg/3yIPmFo.

279 Breu & Seitz, לעיל ה״ש 255, בעמ׳ 7, מתייחסים להודעה לעיתונות של FINMA ב־29 ספטמבר 2017 שלפיה רשות זו, המפקחת על שווקים פיננסיים, מצאה שיש עלייה בשוק בהנפקות מטבע בשווייץ. הרשות פרסמה מדריך בנושא זה, FINMA (Guidance 04/2017), אשר מתמקד בהוראות למלחמה בהלבנת הון ומימון טרור, הוראות חקיקה בנקאיות, הוראות בדבר סחר בניירות ערך והוראות באשר להשקעות קולקטיביות. FINMA אף ציינה כי היא חוקרת כמה מקרים של הנפקות כדי לקבוע האם הופרו הוראות הרגולטור. www.finma.ch/en/news/2017/09/20170929-mm-ico/ (last visited 4 Jan. 2021).

280 Goldman et al., לעיל ה״ש 13.

nevo.co.il

אולם אנו סבורות **שאין מקום לאסור איסור גורף על הנפקות של מטבע אלקטרוני**, כי בכך למעשה נשליך את התינוק עם המים ונוותר על ההטבות שבשימוש במטבעות אלקטרוניים. תחת זאת, **נציע להתמקד באיתור פעילות המתבצעת בניגוד לחוק ובעיצוב מנגנונים לזיהוי ולאימות שיכולים להיות מוטמעים בתוך הטכנולוגיה ולאפשר לחשוף את זהותם של השחקנים שמנצלים לרעה את המטבעות האלקטרוניים לפעילות לא חוקית**. גישה זו מציבה במרכז את ההבנה כי האנונימיות במטבעות אלקטרוניים רחבה מדי וכי התוויית דרכים לצמצם אותה היא סוגיית המפתח שיש להתייחס אליה במאבק נגד איסור הלבנת הון ומימון טרור בשימוש במטבעות אלקטרוניים.

(ב) מגבלות קיימות על אימוץ מטבעות אלקטרוניים בידי טרוריסטים

כפי שהוסבר, מטבעות אלקטרוניים יכולים להיות אטרקטיביים לטרוריסטים. אולם, יצוין שהשימוש במטבעות אלקטרוניים בידי טרוריסטים מתבצע עדיין בקנה מידה מוגבל. ראשית, בשל העובדה שערכם של המטבעות אינו יציב. בשימוש בהם, ארגוני טרור חשופים לאירודאות. שנית, השימוש במטבעות אלקטרוניים מצמצם את יכולתם של מנהיגי ארגוני טרור להפעיל שליטה על הכספים המצויים אצל סוכנים. שלישית, הקשיים בשלב המרת המטבעות לכסף מדינתי (fiat) נותרים ואף מתגברים ככל שיותר מדינות מכפיפות את שירותי ההמרה לחובת הכרת הלקוח.[281] רביעית, הדרגה היחסית נמוכה של חדירת כלי תקשורת טכנולוגיים לאזורים גאוגרפיים מסוימים, שבהם קיימת תשתית לארגוני הטרור, גם משפיעה על הדרגה של אימוץ הטכנולוגיה. אחרי הכול, אם קבוצה של טרוריסטים או ארגוני טרור אינם יכולים להמיר בקלות מטבעות אלקטרוניים בהיקף גדול למטבע מדינתי, או אינם יכולים להשתמש בהם בקלות כדי לרכוש נשק, או חומרים אחרים כמו אוכל, ולשלם בעבור מגורים באזורים שבהם הם פועלים, במקרים אלה תרומת המטבעות האלקטרוניים לפעילותם פחותה.[282]

אולם, בעתיד יעילות השימוש במטבעות אלקטרוניים בשירות גורמי טרור יכולה לגדול, מאחר שגם שיטות של גורמי טרור וגם המטבעות האלקטרוניים מתפתחים. התפתחויות אלה יכולות להקל את השימוש במטבעות האלקטרוניים לכל המשתמשים ולאפשר לקבוצות של טרור וארגוני טרור להיות מעורבים בגיוס כספים ולארגן מבצעי טרור והתקפות נרחבות. כך, אין להקל ראש בסיכון שהשימוש במטבעות אלקטרוניים בידי גורמי טרור מציב לביטחון הלאומי.

281 DION-SCHWARZ, MANHEIM & JOHNSTON, לעיל ה״ש 3, בעמ׳ 27.

282 Goldman et al., לעיל ה״ש 13, בעמ׳ 6 (“This is true, for example, of al Qaeda in the Islamic Maghreb (AQIM) in the Sahel, Al Qaeda in the Arabian Peninsula (AQAP) in Yemen, and, in some measure, ISIS in Iraq and Syria”). ראו גם FATF REPORT, EMERGING TERRORIST FINANCING RISKS 7 (2015) (“If the areas in which these groups operate lack the basic technical and telecommunications infrastructure for their ecosystems to support the use of Bitcoin, then there is no reason for terrorist groups to accept value from outside donors in that form”).

nevo.co.il

ג. מתווה לרגולציה גלובלית של אימות זהות משתמשי מטבעות אלקטרוניים אקס אנטה וחשיפתם אקס פוסט

1. הדין המצוי – צעדים רגולטוריים ראשונים לאכיפת חוקי איסור הלבנת הון ומימון טרור על מטבעות אלקטרוניים

הדירקטיבה האירופית החמישית לאיסור הלבנת הון, the 5th European Anti-Money Laundering Directive (hereinafter – 5AMLD),[283] נחקקה ב־9 ליולי 2018 ונכנסה לתוקף בינואר 2020. הדירקטיבה נחקקה לאחר שרשות הבנקאות האירופית הביעה דאגה באשר לשימוש במטבעות אלקטרוניים לצורכי פשיעה וטרור.[284] הדירקטיבה מכוונת להביא לשקיפות רבה יותר בעסקאות פיננסיות כדי למנוע הלבנת הון ומימון טרור. בפעם הראשונה, דירקטיבה חלה על עסקאות של מטבעות אלקטרוניים, מאחר שהיא חלה על ספקי שירותים של מטבעות אלקטרוניים, כמו שירותי המרה של מטבעות אלה למטבע מדינתי, ועל ספקי הארנקים.[285] גיליון המידע הפורס את המסגרת של הדירקטיבה (ה־5AMLD fact sheet) מציין כי "*The rules will now apply to entities which provide services that are in charge of holding, storing and transferring virtual currencies*".[286] גיליון זה מציין שהחקיקה תגביר את השקיפות ותספק לרשויות האירופיות מידע בעל ערך שיסייע להן להתמודד עם סיכונים הנובעים ממימון טרור והלבנת הון, כאשר המטרה היא לתת מענה לבעיות העולות משימוש במטבעות אלקטרוניים אנונימיים. למעשה, הדירקטיבה מכפיפה שירותי המרה של מטבעות

283 Directive (EU) 2018/843 (June 19, 2018).

284 Theodor, לעיל ה"ש 255, בעמ' 3 מתייחס לרשות הבנקאות האירופית EBA European Banking Authority אשר הפיצה את ה־"EBA Opinion on Virtual Currencies" עוד ביולי 2014, אשר מציינת כי "Criminals or terrorists use the VC remittance systems and accounts for financing purposes (C03). The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across the globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high". referring to EBA European Banking Authority "EBA Opinion on Virtual Currencies", published by EBA in July 2014 states on page 33 "Criminals or terrorists use the VC remittance systems and accounts for financing purposes (C03). The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across the globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high".

285 Directive (EU) 2018/843 (June 19, 2018) Article 2 (d) (19): "custodian wallet provider" means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies...".

286 5th Anti-Money Laundering Directive Fact Sheet 2 (July 9, 2018): https://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=48935.

nevo.co.il

אלקטרוניים וספקי ארנקים לאותן דרישות רגולטוריות שלהן כפופים גם המוסדות הפיננסיים המסורתיים. נציין כי כל המדינות החברות באיחוד האירופי נדרשו להטמיע את הדירקטיבה בחקיקה המדינתית עד ה־10 לינואר 2021.

נוסף על הדירקטיבה, ב־20 ליולי 2021 המועצה האירופית הציגה הצעות חוק שנועדו לחזק את החקיקה בנושא איסור הלבנת הון ומימון טרור. לפי הצעות אלה, ארנקים דיגיטליים המחזיקים נכסים אלקטרוניים אנונימיים (crypto asset wallets) יהיו אסורים לשימוש. הצעה זו משווה ארנקים אלה לחשבונות בנק אנונימיים שכבר נאסרו באיחוד האירופי, ומשתמשי ספקי הארנקים יצטרכו לזהות עצמם במספרי תעודת זהות לפי הנחיות ״הכר את הלקוח״. כך למעשה מוחלים החוקים בנושא איסור הלבנת הון ומימון טרור גם על שוק המטבעות האלקטרוניים.[287] בנוסף, קבע האיחוד כללים המחייבים נותני שירותים בנכסים קריפטוגרפים לאסוף מידע על השולחים והנהנים מהטרנזקציות.[288]

גם הקונגרס האמריקאי החל בסדרת צעדים שהרחיבו את חובותיהם של שירותי ההמרה למטבעות אלקטרוניים. בארצות הברית, החל ממאי 2017 תת־ועדה של הקונגרס דנה בנושא ובהמשך שקדה על הצעת חוק שלפיה על המשרד לביטחון פנים לבצע הערכה וניתוח של סיכוני השימוש במטבעות אלקטרוניים למימון טרור.[289] בינואר 2018 חקיקה נוספת הוצגה לקונגרס בנושא טכנולוגיה פיננסית, חדשנות והגנה, שמטרתה לבסס כוח משימה עצמאי

287 Beating Financial Crime: *Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism rules, European Commission*, Press Release (July 20,2021) https://bit.ly/3rzfT2E ("[I]n addition, anonymous crypto asset wallets will be prohibited, fully applying EU AML/CFT rules to the crypto sector"). לכללי האיחוד המחייבים נותני שירות בנכסים קריפטוגרפיים לאסוף מידע על השולחים והנהנים ראו Council of the EU Press Release, Anti-Money Laundering: Council Adopts Rules Which Will Make Crypto-Asset Transfers Traceable (May 16,2023) https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable.

288 לכללי האיחוד המחייבים נותני שירות בנכסים קריפטוגרפיים לאסוף מידע על השולחים והנהנים ראו Council of the EU Press Release, Anti-Money Laundering: Council Adopts Rules Which Will Make Crypto-Asset Transfers Traceable (May 16,2023) https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable.

289 Breu & Seitz, לעיל ה״ש 255; Homeland Security Assessment of Terrorists Use of Virtual Currencies Act, H.R. 428, 116th Cong(2019) https://www.congress.gov/bill/116th-congress/house-bill/428; Shane Kelly, Money *Laundering Through Virtual Words of Video Games: Recommendations for a New Approach to AML Regulation*, 71 SYRACUSE L REV. 1487,1510 (2021) ("The Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act calls for a threat assessment of 'individuals using virtual currency to carry out activities in furtherance of an act of terrorism…'"); JAY B. SYKES & NICOLE VANATKO, CONG. RSCH. SERV., R45664, VIRTUAL CURRENCIES AND MONEY LAUNDERING: LEGAL BACKGROUND, ENFORCEMENT ACTIONS, AND LEGISLATIVE PROPOSALS 12 (2019).

nevo.co.il

לטכנולוגיה פיננסית ולתעדף חקירות של שימוש לרעה בטכנולוגיה פיננסית, כולל מטבעות אלקטרוניים, אולם החוק לא התקבל על ידי הסנט.[290]

נוסף על זה, הרשות לאיסור הלבנת הון האמריקאית במשרד האוצר (FinCEN) ניסחה הנחיות בנושא.[291] הרשות הצהירה כי היא מתייחסת למפתחים ונותני שירותי המרה של מטבעות אלקטרוניים כמעבירי כספים, "money transmitters", למטרות חוק הסודיות הבנקאית.[292] הרשות להלבנת הון היא האחראית למלחמה בהלבנת הון ומימון טרור במערכת הפיננסית המסורתית. מטרתה לשמור על המערכת הפיננסית משימושים לא חוקיים, להילחם בהלבנת הון ולקדם את הביטחון הלאומי דרך שימוש אסטרטגי בסמכויות ואיסוף, ניתוח והפצה של מודיעין פיננסי.[293] היא עושה כן דרך הטמעה ואכיפה של ציות לחוקים כמו חוק הסודיות הבנקאית, אשר משלים את ההוראות ביחס לרישום וניהול חשבונות.[294] בין השאר, הרשות דורשת לוודא שלגופים שמאפשרים העברות כספים יהיה נוהל של "הכר את הלקוח" (KYC) ותוכנית לאיסור הלבנת הון ושהם ידווחו על עסקאות חשודות.[295] במכתב מ־2018 הרשות הבהירה שחלפני מטבעות אלקטרוניים הם עסקים לשירותים פיננסיים ולכן כפופים לדרישות אלה.[296] בהמשך, נחקק החוק החדש לאיסור הלבנת הון, Anti-Money Laundering Act of 2020,[297] שעבר בקונגרס בראשית 2021. החוק מרחיב את ההגדרות של חוק הסודיות הבנקאית, Bank Secrecy Act (BSA), של מוסדות פיננסיים, כך שיחולו על עסקים שממירים מטבעות אלקטרוניים. לפי החוק, שירותי ההמרה צריכים לאמת את הזהות של הלקוחות שלהם, לפתח פרופילים של סיכון ולפקח אחר העסקאות כדי להגיש לרשויות דיווחים על פעילות חשודה.[298] אולם, רגולציה חדשה זו מתמקדת רק בשירותי המרה. נוסף על זה,

290 Financial Technology Protection Act, H.R. 56, 116th Cong. § 3(a)-(b) (2019).

291 Dion-Schwarz, Manheim & Johnston, לעיל ה"ש 3, בעמ' 3 הפנו ל- US House of Representatives, Financial Innovation and Defense Act, H.R. 4752, January 20, 2018.

292 "regards developers as well as exchanges of [virtual currency] as 'money transmitters' for the purposes of the US Bank Secrecy Act" ראו Blake Hamil, *EU Cryptocurrency Regulation: Creating a Heaven for Businesses or Criminals?,* 48 GA. J. INT'L & COMP. L 833, 837–838 (2020).

293 Mission, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/about/mission (Oct. 25, 2019) ("The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence").

294 FinCEN's Legal Authorities, Fincen https://www.fincen.gov/fincens-legal-authorities "This Treasury Order describes FinCEN's responsibilities to implement, administer, and enforce compliance with the authorities contained in what is commonly known as the Bank Secrecy Act"; ראו גם Hamil, לעיל ה"ש 292, בעמ' 838.

295 Hamil, שם עמ' 838.

296 BSA Requirements for MSBs, Fin. Crimes Enf't Network, https://bit.ly/3NJ4E1b.

297 Anti- Money Laundering Act of 2020 H.R. 6395.

298 31 C.F.R. 1010 Bank Secrecy Act (BSA), להרחבה ראו King & Spalding, לעיל ה"ש 45.

nevo.co.il

לאחרונה נשיא ארצות הברית ג׳ו ביידן חתם על ה־Infrastructure Investment and Jobs Act.[299] לפי חוק זה, שירותי ההמרה של נכסים אלקטרוניים וספקי הארנקים (custody providers) יצטרכו לאסוף מידע מלקוחותיהם ולעקוב אחר תקופות ההחזקה והמחירים של המכירה והקנייה של הנכסים האלקטרוניים בחשבון של הלקוח בשירותיהם.[300] חברות שמקבלות, או עשויות לקבל בעתיד, תשלומים במטבעות אלקטרוניים מעל ל־10,000 דולר יצטרכו להגיש טופס למס הכנסה עם קבלת המטבעות האלקטרוניים.[301] חובות אלה טרם נכנסו לתוקף.[302]

למשרד לשליטה על נכסים זרים, Office of Foreign Assets Control (“OFAC”), במשרד האוצר בארצות הברית, ישנה סמכות לנהל ולאכוף סנקציות כלכליות וסנקציות על המסחר על מנת לממש מטרות של ביטחון לאומי, באמצעות קביעת תוכניות סנקציות שונות.[303] ב־15 לאוקטובר 2021, פרסם המשרד את המדריך לסנקציות שנועדו כדי לסייע לתעשיית המטבעות האלקטרוניים לנהל את הסיכונים הנובעים מהמטבעות.[304] המדריך של OFAC מציין חובות מכוח צווים שונים, אשר חלות בשוויוניות על עסקאות המערבות מטבעות אלקטרוניים ואלה המערבות מטבע מדינתי רגיל. חברי תעשיית המטבעות האלקטרוניים אחראים להבטיח שהם לא יהיו מעורבים, במישרין או בעקיפין, בעסקאות שנאסרו על ידי ה־OFAC כמו מעורבות במסחר אסור.[305] לפי המדריך, כל החברות בתעשיית המטבעות האלקטרוניים, כולל חברות הטכנולוגיה, שירותי ההמרה, אדמיניסטרטורים, כורים וספקי ארנקים, כמו גם מוסדות פיננסיים מסורתיים שעשויים להיחשף למטבעות אלקטרוניים בזמן מתן השירות, מתומרצים לפתח, להטמיע ולעדכן כעניין שבשגרה תוכנית מותאמת לציות המבוססת על סיכון לאי־חוקיות.[306] המדריך מספק את ״הפרקטיקות הטובות״, כמו מחויבות ההנהלה להכנת תוכנית ציות של החברה (sanctions compliance program),[307] הערכת סיכונים לחשיפה

299 Infrastructure Investment and Jobs Act. H.R. 3684, 117th Cong. (2021).

300 Timothy L. Jacobs, Jason Feingertz, Tim Strother, *New Cryptocurrency Information Reporting Regime New Cryptocurrency Information Reporting Regime Required on Form 1099 and Form 8300*, The National Law Rev. (Dec 29, 2021) https://bit.ly/3Rpah7Y0.

301 שם.

302 Jeff Waldeck, *Digital Asset Information Reporting,* GBQ (Dec.21, 2021) https://gbq.com/digital-asset-information-reporting (“The two provisions of the IIJA mentioned above become effective on December 31, 2023, which gives the Treasury Department time to collect input from the public and write appropriate rules and regulations”).

303 Office of Foreign Assets Control – Sanctions Programs and Information https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.

304 Sanctions Compliance Guidelines for the Virtual Currency Industry, Office of Foreign Asset Control (Oct.2021) https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

305 שם, בעמ׳ 5.

306 בעמ׳ 1.

307 בעמ׳ 11.

nevo.co.il

לסנקציות של OFAC ומדריך כיצד לנקוט צעדים כדי למזער את סיכוניהם[308] וכיצד להטמיע בקרה פנימית, לרבות השגת מידע על לקוחותיהם בהליך הכרת הלקוח בתחילת ההתקשרות ודרך מחזור החיים של היחסים עם הלקוח וכיצד להשתמש במידע כדי לצמצם את הסיכון לסנקציות.[309] שעה שהרבה חברות של מטבעות אלקטרוניים יוכלו לבנות תוכנית ציות מספקת תחת המסגרת שהתווה המדריך, היבטים במדריך מצריכים יותר בהירות באשר לאופן שבו יוחל על מטבעות אלקטרוניים הפועלים ללא מנגנון ריכוזי (*Decentralized Autonomous Organizations* DAOs).[310]

בנוסף, מתכוון ממשלביידן להעמיק את הדרישות הרגולטוריות לגבי נכסי קריפטו ולאחרונה חתם על צו נשיאותי, אשר מתייחס לחלק מהאתגרים שנכסי קריפטו מציגים במישור הרגולטורי, במישור הכלכלי ובמישור הביטחון הלאומי.[311] צו זה מתייחס באופן ספציפי לסכנות הקשורות להלבנת הון דרך מטבעות אלקטרוניים.

מחוץ לאיחוד האירופי ולארצות הברית התוו מדינות נוספות בעולם רגולציה של מטבעות אלקטרוניים. בסינגפור הנפקת מטבע אלקטרוני צריכה לעמוד ברגולציה של איסור הלבנת הון ולמלא אחר דרישות של הכרת הלקוח של כל האנשים שקונים את המטבע מהחברה המנפיקה.[312] החובות מוטלות גם על בורסות וחלות גם בשלב ההמרה.[313] בקנדה, מתוך חשש

308 בעמ׳ 12.

309 בעמ׳ 18.

310 OFAC Releases New Detailed Guidance for the Digital Currency Industry, JD Supra (Oct. 20, 2021) https://bit.ly/3AubowZ.

311 Exec. Order No. 14067 Fed. Reg. 05471 (Mar. 14, 2022); Hadar Y. Jabotinsky, Roee Sarel, *When Biden Met Crypto: Thoughts on the President's Executive Order*, THE CLS BLUE SKY BLOG (Apr. 1, 222) https://bit.ly/3IimYgt; *US Executive Order on Crypto: What does it Mean?* THE ECON. TIMES https://bit.ly/3ONb157 (Mar. 22, 2022).

312 The Payment Services Act 2019 (Sing.) https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220 ("An Act to provide for the licensing and regulation of payment service providers, the oversight of payment systems, and connected matters, to repeal the Money-changing and Remittance Businesses Act (Chapter 187 of the 2008 Revised Edition) and the Payment Systems (Oversight) Act (Chapter 222A of the 2007 Revised Edition), and to make consequential and related amendments to certain other Acts"); Hadar Y. Jabotinsky & Michal Lavi, *Speak Out: Verifying and Unmasking Cryptocurrency User Identity,* 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 518, 560(2021) ("requiring that anyone issuing a cryptocurrency adhere to Anti-Money Laundering regulation and fill in a KYC on all people buying the token from the issuing firm").

313 Ishan Singh, *Are you anonymous on blockchain? Here's how S'pore's crypto regulations keep track of investors,* Vulcan Post (Jan 6, 2022) https://vulcanpost.com/774173/anonymous-on-blockchain-crypto-regulations-singapore "The primary way to buy cryptocurrency using fiat money or convert cryptocurrency to fiat money is through a centralised exchange (CEX). In Singapore, this includes companies such as DBS Vickers and Independent Reserve. Such licensed exchanges are regulated under the Monetary Authority of Singapore (MAS)'s Payment Services Act. Following are the points laid out in the act which the exchanges must comply with: *a. customer due diligence by verifying their*

nevo.co.il

להלבנת הון ועסקאות אסורות, הפעילו חקיקת חירום שמכוונת לנותני שירות של ספק תשלום ופלטפורמות למימון המונים. על פי החוק, חברות אלה צריכות עכשיו להירשם אצל הרגולטור הקנדי FINTRAC.[314] בישראל נכנס לתוקף צו איסור הלבנת הון חובות זיהוי, דיווח וניהול רישומים של נותני שירותי אשראי למניעת הלבנת הון ומימון טרור.[315] הצו מכניס תחת משטר איסור הלבנת הון גם נותני שירותים במטבעות אלקטרוניים[316] ומטיל חובת הכר את הלקוח על כל נותני השירותים במטבעות אלקטרוניים כמו חלפני מטבע, מי שמאפשר העברות בין חשבונות בארץ ובחו״ל, באשר לכל פעולה מעל 5,000 ש״ח.[317] לפי הצו, על נותן שירות לשמור את פרטיה של כל פעולה כספית שבוצעה במסגרת מתן אשראי או שירות בנכס הפיננסי באופן שיכלול את תאריך ביצוע הפעולה, סוגה, סוג הנכס הפיננסי שבו נעשתה הפעולה והמטבע שבו בוצעה, לעניין פעולה במטבע וירטואלי גם סוג המטבע הווירטואלי,[318] ואת פרטי המעביר והנעבר במסמכי ההעברה.[319] נותן השירות ישמור באופן נגיש את כתובות הארנקים של המטבעות האלקטרוניים המעורבים בפעולה[320] ואת כתובות ה־IP ומזהי ה־IMEI[321] וכן את מסמך ההוראה לביצוע פעולה והתכתבות עסקית הנלווית לה בין נותן השירות למקבלו למשך חמש שנים לפחות ממועד מתן השירות בנכס הפיננסי. על שמירת המסמכים לאפשר גם שחזור עסקה בודדת.[322] על נותני השירות לדווח לרשות לאיסור הלבנת הון ומימון טרור על פעולות כספיות מעל 50,000 ש״ח[323] וכן על פעולות חשודות. הרגולציה שמתווה הצו בתחום הכרת הלקוח רחבה, ונהלים אף משלימים אותה וקובעים חובות ניהול סיכונים.

חשוב להדגיש כי ככלל בנקים אינם יכולים לסרב סירוב גורף לספק שירות בנקאי לחברות שעוסקות במסחר במטבעות אלקטרוניים. בעניין **ביטס אוף גולד**,[324] בורסה למטבעות אלקטרוניים הייתה לקוחה של בנק לאומי, והבנק סירב לתת לה שירות ורצה להפסיק את פעילותה. בית המשפט העליון נתן צו זמני האוסר על בנק לאומי להפסיק באופן גורף את

identities and businesses; b. monitoring of customers' transactions for signs of money laundering and terrorism financing; c. screening of customers against relevant international sanctions list by the United Nations; and d. maintain detailed records of customers activities and put in place a process to report suspicious transactions to MAS".

314 Sebastian Sinclair *Crypto Payment Systems Face New Restrictions Under Canada's Blockade Crackdown*, BLOCKWORKS (Feb. 14, 2022, 8:05 PM), https://bit.ly/3RdhdES.

315 צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של נותני שירותי אשראי למניעת הלבנת הון ומימון טרור) (תיקון), התשפ״א–2021.

316 ראו ס׳ 11 לצו אשר מוסיף את סעיף 7א לצו העיקרי. ״נותן שירות לא יבצע פעולה באמצעות שירות העברה אלקטרונית אל מחוץ לישראל בסכום העולה על 5,000 שקלים חדשים, בלא שירשום בכל אחד ממסמכי ההעברה את פרטי המעביר...״.

317 שם

318 ראו ס׳ 11(7).

319 ראו ס׳ 11 ב(1).

320 ראו ס׳ 20 (2) אשר מוסיף את ס׳ 16 ב לצו העיקרי.

321 שם

322 שם

323 ראו ס׳ 15 המתקן את ס׳ 11 לצו העיקרי.

324 ע״א 6389/17 **ביטס אוף גולד נ׳ בנק לאומי לישראל** (נבו 25.2.2018).

nevo.co.il

פעילות ביטס אוף גולד, העוסקת במסחר במטבעות אלקטרוניים. נוסף על זה, לאחרונה, פרסם הפיקוח על הבנקים תוספת חדשה לנוהל בנקאי תקין (נב"ת) 411, אשר הפכה לחלק מחייב מהנוהל, שכוללת תיקון להוראת ניהולי סיכוני איסור הלבנת הון ואיסור מימון טרור, שלפיה בנקים יבחנו כל מקרה של מסחר במטבעות אלקטרוניים בנפרד, מאחר שתשלומים במטבעות אלקטרוניים הם פעילות בסיכון גבוה.[325] אולם בנקים לא יוכלו למנוע שירות תשלום אגב פעילות במטבע אלקטרוני באופן גורף רק בשל העובדה שהשירות קשור במטבעות אלקטרוניים. התאגיד הבנקאי יצטרך לבצע הליך הערכת סיכונים שבו יברר את מקור הכספים ששימשו לרכישת המטבע האלקטרוני ואת הנתיב שעברו ממועד רכישתו ועד להפקדת כספים שמקורם במימושו בחשבון הלקוח בתאגיד הבנקאי.[326] יצוין שגם לפני הנחיות אלה היו בנקים שסירבו להפקיד רווחים ממטבעות אלקטרוניים שנרכשו במזומן בשל החשש לעקיפת איסורי מימון טרור והלבנת הון.[327]

נסכם כי עיקר הרגולציה במדינות רבות מוגבלת ומתמקדת בחובות "הכרת הלקוח", שמפחיתות את האנונימיות במטבעות האלקטרוניים חלקית בכך שהן מקשות על היכולת להשיג אנונימיות בשלב ההמרה ובכמה שירותים אחרים כפי שפורט לעיל.[328] כפי שצוין, הסיבות לחובות הכרת הלקוח היו במקור כדי שמתווכים פיננסיים יזהו עסקאות חשודות בחשבונות לקוחותיהם וידווחו עליהן לרשות להלבנת הון ומימון טרור ולמשטרה.[329] דרישת חובת הכר את הלקוח מאנשים שמקבלים מטבעות אלקטרוניים בשלב ההמרה היא צעד ראשון, אולם צעד זה אינו מספק, מאחר שאינו מאפשר לחסום עסקאות לא חוקיות.[330] פרטים המשתמשים בשירותי המרה לעיתים עושים רק פעולה אחת בשלב זה, ושירותי ההמרה אינם מכירים את דפוסי המסחר שלהם בנכסים הווירטואליים ואינם יכולים לאתר פעילות חשודה במטבעות האלקטרוניים.

325 יניב הלפרין "בנק ישראל: תשלומים במטבעות וירטואליים הם פעילות בסיכון גבוה" **אנשים ומחשבים** (30.12.2021) https://bit.ly/3RehuHO.

326 ראו **ניהול סיכוני איסור הלבנת הון ואיסור מימון טרור** (5/2022) (עמ' 21) https://www.boi.org.il/roles/supervisionregulation/3455/18098; אתי אפללו "לא יוכלו לסרב לפעול בענייני קריפטו: בנק ישראל בטיוטת הוראות לבנקים" **גלובס** (30.12.2021) https://bit.ly/3R89MyZ.

327 ראו לאחרונה: ליטל דוברוביצקי "פנסיונרית הרוויחה מיליון שקל מביטקוין, הבנק מסרב להפקיד: "סיכון להלבנת הון"" **Ynet, כלכלה וצרכנות** (18.11.2021) https://www.ynet.co.il/economy/article/r1gvn9z00t.

328 *Guidance FIN-2013-G001*, U.S. Dept. Of Treasury, Fin. Crimes Enf't Network, (Mar. 18, 2013), www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (at 3); Shahla Hazratjee, *Bitcoin: The Trade of Digital Signatures*, 41 T. MARSHALL L. REV. 55, 75 (2016).

329 ראו ס' 32–33 לחוק לחוק המאבק בטרור, התשע"ו–2016.

330 Scott D. Hughes, *Cryptocurrency Regulations and Enforcement in the U.S*, 45 W. ST. L. REV. 1 (2017) ("Bitcoin transactions are not facilitated within a consumer protection framework and measures, such as anti-money laundering (AML) or know-your-customer (KYC) policies, are not inherent to the system. Once a transaction is sent, there is no way to perform a chargeback").

nevo.co.il

בישראל, כאמור, הטיל המחוקק חובות רחבות על המערכת הבנקאית ונותני שירותים במטבע בצו לאיסור הלבנת הון הכוללות שמירת כתובות הארנקים והותוו הנחיות החלות על מוסדות פיננסיים לניהול בנקאי תקין לביצוע הערכות סיכונים והתחקות אחר נתיב העברות הכספים עד להפקדה בחשבון הלקוח בתאגיד בנקאי ובגופים הפיננסים האחרים הפועלים בשוק. אולם אין די ברגולציה האמורה כדי להתמודד עם השימוש במטבעות אלקטרוניים לעקיפת איסורים על הלבנת הון ומימון טרור מן הסיבות הבאות: ראשית, דרישות לחובת הכרת הלקוח בשלב ההמרה לא ימנעו מימון בשלב ההנפקה, משום שבשלב זה, אנשים אינם רוכשים את המטבע דרך שירותי המרה, אלא משלמים לחברה המנפיקה ישירות בכרטיס אשראי. כך, גורמי טרור ועבריינים יכולים להלבין את הכספים ישירות ברכישת המטבע בשלב ההנפקה ושימוש בו ברשת האפלה במטרה לרכוש נשק וציוד הנדרשים להתארגנות טרור, התקפות טרור ועבירות פליליות אחרות. המסקנה היא שהפיקוח הרגולטורי מוגבל, וקשה לעקוב אחר עסקאות רכישת מטבע אלקטרוני דוגמת ביטקוין המתאפשרות מכל מקום בעולם.[331] כמו כן, רגולציה המתמקדת בשלב ההמרה יכולה להתרחש גם שלא בידי ישות מוסדרת, לדוגמה תשלום עבור מטבעות אלקטרוניים במטבעות אלקטרוניים מסוג שונה.[332]

שנית, מטבעות אלקטרוניים אינם מוגבלים לאזור גאוגרפי. ככל שרגולציה בארצות הברית או באירופה מטילה חובות הכר את הלקוח בשלב ההמרה, גורמי טרור ועבריינים יכולים להשתמש בשירותי המרה בשיטת משפט אחרת שאינה מתווה הנחיות לעקוב אחר נתיב מעבר הכספים ואף אינה דורשת את חובת הכרת הלקוח.[333]

2. הדין הרצוי – הצעה לרגולציה גלובלית של אימות זהות משתמשי מטבעות אלקטרוניים אקס אנטה וחשיפה אקס פוסט

צומת זה, כאשר גורמי טרור מתחילים לגלות את ההטבות שהם מפיקים ממטבעות קריפטוגרפיים המאפשרים מימון לפעילתם, ובו גורמי פשיעה כבר משתמשים בנכסים קריפטוגרפיים, כולל מטבעות אלקטרוניים, לצורך הלבנת הון, הוא בדיוק הזמן לשאול אם

331 ראו לדוגמה LocalBitcoins.Com, *Buy and Sell Bitcoin Everywhere*, localbitcoins.com.

332 Dion-Schwarz, Manheim & Johnston, לעיל ה״ש 3, עמ׳ 49, ראה נאום של ראש רשות ניירות ערך האמריקאית בנוגע לשימוש בסטייבל קוינז על מנת להמיר מטבעות אלקטרוניים אחרים לצורך ביצוע הלבנת הון ועבירות אחרות: "...stablecoins raise issues on how they potentially can be used for illicit activity. Stablecoins primarily are used for crypto-to-crypto transactions, thus potentially facilitating platforms and users avoiding or deferring an on-ramp or off-ramp with the fiat banking system. Thus, the use of stablecoins on platforms may facilitate those seeking to sidestep a host of public policy goals connected to our traditional banking and financial system: anti-money laundering, tax compliance, sanctions, and the like…." (Gary Gensler, *Prepared Remarks of Gary Gensler On Crypto Markets Penn Law Capital Markets Association Annual Conference* (4 April, 2022) https://bit.ly/3IlCM1W.

333 Olly Jackson, *Cryptocurrency Exchanges Avoiding the US Due to Confusing Regulation*, Int'l Fin. L. Rev. (Mar. 26, 2018).

nevo.co.il

אנונימיות המטבעות האלקטרוניים היא הכרח המציאות[334] וכיצד להביא לרגולציה יעילה שתאפשר לפעול נגד הלבנת הון ומימון טרור באמצעות מטבעות אלקטרוניים. חלק זה מבקש לענות לשאלות אלה ולהתמודד עם הבעיות ברגולציה הקיימת שהעלינו בפסקה הקודמת ומציע שינוי בשלושה רבדים: א) אימות זהות המשתמשים הפועלים על גבי הבלוקצ׳יין; ב) דרישת צו שיפוטי לחשיפת המשתמשים כשיש חשש ממשי שהם משתמשים במטבעות למימון טרור או הלבנת הון; ג) שיתוף פעולה בין מדינות וסטנדרטים להסדרה גלובלית בין־לאומית שתאפשר להתמודד עם השימוש חוצה הגבולות במטבעות האלקטרוניים.

(א) אימות זהות המשתמשים הפועלים על גבי הבלוקצ׳יין

ראשית, נציע לחייב ספקי ארנקים, שירותי המרה ואף חברות שמנפיקות מטבעות אלקטרוניים לזהות את המשתמשים הפועלים על גבי הבלוקצ׳יין אצל הבורסות, החברות המנפיקות, שירותי ההמרה וספקי הארנקים. זיהוי זה יעבור התממה (אנונימיזציה), ולא יהיה נגיש לכלל הציבור. אולם, גורמי אכיפת החוק יוכלו לבקש מספקי ארנקים, שירותי המרה והחברות המנפיקות את המטבעות לחשוף את זהויות משתמשי המטבעות כאשר יש חשש של ממש להלבנת הון או מימון טרור בפעילותם בכפוף לצו שיינתן בידי בתי משפט. כאמור, על פי המוצע, עסקאות על גבי הבלוקצ׳יין לא יהיו מזוהות לכולם, אלא ספקי הארנקים, שירותי ההמרה והחברות המנפיקות יידרשו לזהות את לקוחותיהם ולערוך הליך הכר את הלקוח באותו אופן שבו מוסדות פיננסים מסורתיים נדרשים לעשותו. בדרך זו, אם מתעורר חשד שמתבצעת פעילות של הלבנת הון או מימון טרור במטבע, הרשויות יכולות לבקש מאותם תאגידים (הבורסות, החברות המנפיקות, שירותי ההמרה וספקי הארנקים) לחשוף את האנשים שעומדים מאחורי הארנקים.

נציין כי רעיון זה אמור היה להיות מיושם במטבע של Diem (לשעבר Libra) וכן במטבע הלא אנונימי שתוכנן להיות מונפק על ידי Saga.[335] שני המטבעות עוצבו מתוך מחשבה על כך שברצון הקרנות שהנפיקו אותם ליצור מטבע בין־לאומי שיוכל להחליף מטבע מדינתי (fiat) במקרים רבים, ולאפשר עסקאות גלובליות. בהתאם, התוכנית הייתה שכל מי שייכנס לבלוקצ׳יין כדי לרכוש מטבעות אלה, יידרש לזהות את עצמו בפני הקרן שהנפיקה את המטבע.[336] המשמעות היא שבכל נקודת זמן נתונה, לחברה המנפיקה יהיה מרשם של כל

334 Houben & Snyers, לעיל ה״ש 218, בעמ׳ 11 (“mandatory registration and a pre-set date as of which it applies would be a better approach to unveil the anonymity of cryptocurrency users”).

335 Saga הייתה קרן שהנפיקה מטבע דיגיטלי שאינו אנונימי שאמור היה להיות צמוד לסל של מטבעות פיאט. להרחבה ראו /https://www.saga.org. על אודות Diem (ליברה) ראו לעיל ה״ש 236 והטקסט הצמוד אליה.

336 הזיהוי יכול להיות על ידי ועידת וידאו של הכרת הלקוח המשתמש שבמהלכה הוא יחזיק את מסמכי הזיהוי שלו כמו תעודת זהות או דרכון. שיטה אחרת שבשימוש בידי Saga היא שימוש בתמונת סלפי שצילם הלקוח שעה שהוא מחזיק בידו דף עם משפט כתוב שמסופק אקסקלוסיבית בידיו על ידי Saga יחד עם מסמכי זיהוי. Saga מזהה לקוחות שמוכרים או קונים מטבעות ישירות ממנה, אבל מאשרת את המדיניות של איסור הלבנת הון בהמרה בה המטבע של Saga נסחר.

nevo.co.il

משתמשי הבלוקצ׳יין, והחברה תוכל לסייע לרשויות לפעול נגד הלבנת הון ומימון טרור. מאמר זה מבקש אפוא לקחת את רעיון הזיהוי על גבי הבלוקצ׳יין צעד אחד קדימה ולאפשר לחשוף את זהות המשתמשים כשיש חשש של ממש שמשתמשים במטבעות למימון טרור או הלבנת הון.[337]

(ב) חשיפת שמות המשתמשים כשמתעורר חשש ממשי למימון טרור או הלבנת הון תהיה כפופה לצו שיפוטי

המערכת הפיננסית המסורתית פועלת כסוכנת אכיפת החוק ומוטלות עליה חובות שוטפות לקיים בקרה לאתר ולדווח על פעולות החשודות בהלבנת הון או סיוע לטרור, תוך ניצול מאגרי המידע הקיימים בגופים הפיננסיים.[338] דיווח של בנק או מוסד פיננסי מסורתי אחר מתבצע ללא צו שיפוטי, אלא בהתאם לחקיקה ולצווים שהוצאו מכוחה. הסיבה שלא נדרש צו שיפוטי לפני כל דיווח של מוסד פיננסי לרשות לאיסור הלבנת הון היא משום שחשבונות הבנק לכתחילה אינם מתנהלים באנונימיות. המקרה שונה בענייננו, כאשר הפעילות הפיננסית מתבצעת במערכת מבוזרת המתאפיינת בדרגה גבוהה של אנונימיות, מאחר שחלק מהפרטים משתמשים במטבעות אלקטרוניים לצרכים לגיטימיים בדיוק בגלל האנונימיות שהם מאפשרים. כך, למשל, אדם שאינו רוצה להיות מזוהה עם מטרה פוליטית כזו או אחרת (הפלות בארצות הברית כדוגמה)[339] יכול לתמוך בפעילות הפוליטית שאיתה הוא מזוהה בצורה אנונימית. באותו אופן, כשמדובר על שימוש במטבעות אלקטרוניים אנונימיים לצריכה (ולא כנכס להשקעה), יש אנשים שמעדיפים לצרוך את המוצר הלגיטימי (למשל: רכישה של קלפי טארוט) בצורה אנונימית על מנת שלא להיות מתויגים חברתית בצורה זו או אחרת. בהיעדר פיקוח חוקתי ודרישה לצו לחשיפת הזהות, יהיה אפקט מצנן על שימוש במטבעות אלקטרוניים ויישמט הבסיס לשימוש בהם. כך נאבד את היתרונות שמטבעות אלה מאפשרים למבקשים לבצע באמצעותם פעולות פיננסיות לגיטימיות.

כפי שציינו קודם, במטבעות אלקטרוניים כל נושא זיהוי הלקוחות ודיווח על פעולות לא רגילות נמצא בחיתוליו. מאחר שהעסקאות גלויות על הבלוקצ׳יין, אין זה רצוי שהמידע על זהות המשתמשים יהיה גלוי וחשוף לכל, אלא אנו מציעות שהוא יותמם ויוצפן וחשיפתו תתאפשר רק לפי צו שיפוטי. האנונימיות תהא למעשה אנונימיות מותנית, כלפי הכלל היא אנונימיות שאפשר להסירה בדיעבד. נציע כי הליך החשיפה אף יעוגן בחקיקה בנושא איסור

337 נציין כי אפשר היה להגיע לאותה תוצאה אם היינו מחייבים כל מקבל מטבע אלקטרוני לוודא שהפרט שהעביר לו את המטבע זיהה את עצמו. אולם מודל זה מטיל את נטל הזיהוי על המשתמשים ומכביד על השימוש במטבעות, ולכן אנו סבורות כי המודל המוצע במאמר זה, שלפיו הטלת הנטל לזהות את המשתמשים תהיה על החברות המנפיקות, ספקי הארנקים ושירותי ההמרה, הוא יעיל יותר, והם מונעי הנזק היעילים בשונה מאדם פרטי.

338 ראו בהרחבה על הרגולציה החלה על מוסדות פיננסיים חלק א.2. (א)–(ב).

339 נציין כי נושא זה מצוי במחלוקת בארצות הברית, והמחלוקת מתגברת היום יותר מתמיד, לאחר קביעת בית המשפט העליון כי אין זכות חוקתית להפלה, פסיקה שהעבירה את הכוח להסדיר את נושא ההפלות לרמה המדינתית, ולכן לזכות לאנונימיות חשיבות רבה בהקשר זה. ראו Dobbs v. Jackson Women’s Health Organization, No. 19-1392, 597 U.S (2022)

nevo.co.il

הלבנת הון ומאבק בטרור. החובה לצו שיפוטי תוביל להחלטות טובות יותר באשר למסירת מידע על זהות משתמשים, מאחר שרשויות האכיפה יצטרכו למסור הנמקה משכנעת לבקשת החשיפה, וההחלטה לחשוף את המשתמש תתקבל תוך מודעות לתוצאות החשיפה.[340] כמו כן היעדר צו יפגע בחדשנות מאחר שמשתמשים שיודעים שזהותם עלולה להיחשף ללא צו שיפוטי יצמצמו את השימוש במטבעות אלה למטרות לגיטימיות והתפתחותם תיעצר, וכך נאבד את ההטבות שהם יוצרים לחברה ולכלכלה.[341]

אנו ערות לעובדה שהליך החשיפה מעורר שאלות חוקתיות ועלול לפגוע בזכותו של אדם לכבודו וחירותו, המוגנת בחוק היסוד. אולם נדגיש כי הצו לא יינתן כעניין כשבשגרה, אלא רק כאשר מתעורר חשש של ממש כי נעשה שימוש במטבעות האלקטרוניים למימון טרור או להלבנת הון. תפקיד בית המשפט יהיה לשמור על איזון כוחות בין המדינה למשתמשי המטבעות ובין הביטחון הלאומי לזכויות הפרט ולהוות איזון, בלם ובקרה כנגד שימוש יתר בכוחה של המדינה. צו שיפוטי ימנע מצב שבו בשל שינוי טכנולוגי יבוטלו למעשה זכויות הפרט לאנונימיות כנגזרת של הזכות לפרטיות וחופש הביטוי,[342] במקרה בו גורמי אכיפת החוק ינצלו כוחם לרעה. לדוגמה, בתחקיר שפורסם בעיתון "כלכליסט" נחשף כי חטיבת הסייבר של המשטרה מעסיקה האקרים חיצוניים בתשלום לצורך איסוף מידע מודיעיני.[343] לעניות דעתנו, פעולת רשויות האכיפה ללא צו שיפוטי, או בחריגה מסמכות ובהיעדר שקיפות, מדאיגה ואינה מאפשרת פיקוח משמעותי על התנהלות גופי החקירה. נציין כי שחיקת היסודות הדמוקרטיים אינה עוצרת במרחב הדיגיטלי וזוחלת גם לתחום החיפוש הפיזי.[344] מגמה זו מאפשרת שימוש לרעה בכוח של רשויות אכיפת החוק ועלולה לערער את היסודות הדמוקרטיים ואלה של שלטון החוק.

כדי לצמצם ניצול לרעה של כוח והתדרדרות במדרון חלקלק שתפגע פגיעה אנושה בדמוקרטיה, ולאזן בין זכויות יסוד, אנו סבורות כי נדרש צו שיפוטי שיינתן רק בהתקיים חשד ממשי לעבירות של איסור הלבנת הון ומימון טרור. הסדר שלפיו הליך החשיפה יותנה בצו שיפוטי אינו שונה מהסדרים דומים בדין שבהם רשויות האכיפה מקבלות לידיהן מידע, וקבלת מידע זה מותנית בצו שיפוטי. בדומה להצעה לחשיפת משתמשי מטבעות אלקטרוניים, נדרש צו שיפוטי בהקשרים משיקים בדין הפלילי, ומקובל כי צו זה מהווה נקודת איזון ראויה בין זכויות יסוד לפגיעת העבירה שיש חשד לביצועה. דוגמה ראשונה היא חוק האזנת סתר,

340 ראו בהרחבה על חשיבותם של צווים שיפוטיים בהקשר משיק של מעקב וחיפוש Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1642 (2012).

341 DANIEL J. SOLOVE, NOTHING TO HIDE, THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 109 (2011), מרחיב על חשיבותם של צווים שיפוטיים.

342 נדון בזכויות יסוד אלה בחלק הבא.

343 ראו תומר גנון "לא רק NSO: המשטרה שוכרת האקרים לבצע פריצות ולאסוף מידע על אזרחים" **כלכליסט** (19.1.2022) https://bit.ly/3IyerXb.

344 לאחרונה אישרה מליאת הכנסת בקריאה ראשונה הצעת חוק לתיקון פקודת סדר הדין הפלילי (מעצר וחיפוש) (עילות חיפוש במקום ללא צו בית משפט), התשפ"ב–2021 שמטרתה לתקן את סעיף 25 לפקודת סדר הדין הפלילי (מעצר וחיפוש) ולהרחיב את העילות שיאפשרו למשטרה לבצע חיפוש בביתו של אדם ללא צו בית משפט.

nevo.co.il

התשל״ט–1979 המתייחס להאזנה לשיחה וקובע בסעיף 6 שהאזנת סתר תותר רק בכפוף לצו שיפוטי של נשיא בית משפט מחוזי כשהדבר דרוש לגילוי לחקירה, או למניעה של עבירות מסוג פשע, או לתפיסה של עבריינים שעברו עבירות כאמור, או לחקירה לצורכי חילוט רכוש הקשור בעבירה שהיא פשע.[345] דוגמה שנייה היא סעיף 23א לפקודת סדר הדין הפלילי (מעצר וחיפוש), שלפיו חדירה לחומר מחשב על ידי רשויות החקירה וביצוע חיפוש בחומר שנשמר במחשב או מכשיר חכם שלא בהסכמה היא פעולה המחייבת צו שיפוטי, גם במקרים דחופים, ויש לפרט את מטרות החיפוש ותנאיו, שייקבעו באופן שלא יפגע בפרטיותו של אדם מעבר לנדרש.[346] דוגמה שלישית היא ההסדר בחוק נתוני תקשורת, אשר מאפשר לרשויות האכיפה לקבל מידע על נתוני מיקום ונתוני מנוי, אשר כוללים גם שם, כתובת ומספר זיהוי של המנוי ונתוני תעבורה.[347] מידע זה יתקבל בכפוף לצו בית משפט.[348] בדומה לדוגמאות שנזכרו, אנו סבורות כי על הליך חשיפת משתמשים במטבעות אלקטרוניים להיות מותנה בצו.

נציין כי הכפפת הליך החשיפה לצו שיפוטי אינה מובנת מאליה, אולם הצורך בצו מתחזק ומתחדד ככל שהטכנולוגיה מתפתחת ומאפשרת זרימת מידע מגופים פרטיים למדינות. ההבנה כי יש להתאים את ההגנה לטכנולוגיה משתנה כבר מחלחלת, כפי שמצטייר מהתפתחות הדין בנושא בארצות הברית שיתואר להלן: התיקון הרביעי לחוקה האמריקאית מגן על אזרחים נגד כוחו של הממשל וקובע כי מעקב וחיפוש של מידע על ידי הממשל יתאפשרו רק בצו בית

345 ראו ס׳ 6 לחוק האזנת סתר, התשל״ט–1979.

346 ראו ס׳ 23 א.(ב) לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ״ט–1969 ״על אף הוראות פרק זה, לא ייערך חיפוש כאמור בסעיף קטן (א), אלא על־פי צו של שופט לפי סעיף 23, המציין במפורש את ההיתר לחדור לחומר מחשב או להפיק פלט, לפי הענין, והמפרט את מטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש״. לעניין זה נציין בשולי הדברים, בעקבות פרשת NSOכי נראה כי מעקב המשטרה בעזרת תוכנת NSO בצו מכוח חוק האזנת סתר הוא בעייתי, מאחר שהמעקב משתרע מעבר להאזנת סתר ומהווה חדירה לחומר מחשב שלגביו נדרש צו שיפוטי גם במקרים דחופים. ראו עמרי רחום־טוויג ״חיפושים ממוחשבים – על סמכויות חקירה בגישה מרחוק למחשבים ומידע דיגיטלי״ **פורום עיוני משפט (תגוביות משפט)** מו 6, 7 (30.1.2022) https://bit.ly/3usu1xF (״חוק האזנת סתר, בלשונו ותכליתו, לא נועד לאפשר גישה רחבה כל כך למידע של הנחקר, אלא להאזין לשיחות מסוימות ומוגדרות של אותו נחקר בשים לב לחשדות הנחקרים ולצורכי החקירה הרלוונטיים. לכן, גם מבחינה מהותית וגם מבחינה דוקטרינרית, האכסניה הנכונה לצו שיאפשר גישה לחומר מחשב של הנחקר, גם מרחוק וללא תפיסה של המחשב עצמו, היא בסעיף 23א לפקודה המאפשר צו חיפוש בחומר מחשב״).

347 ראו ס׳ 1 (סעיף ההגדרות) לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס״ח–2007.

348 ראו ס׳ 3(א) לחוק ״בית המשפט רשאי, על פי בקשה של קצין משטרה שהסמיך לעניין זה המפקח הכללי או של נציג רשות חוקרת אחרת (בסעיף זה – הבקשה), להתיר, בצו, למשטרה או לרשות החוקרת האחרת, קבלת נתוני תקשורת ממאגר מידע של בעל רישיון בזק, בדרך שיקבע בצו, אם שוכנע שהדבר נדרש למטרה מהמטרות המפורטות להלן, ובלבד שאין בקבלת נתוני התקשורת כאמור כדי לפגוע, במידה העולה על הנדרש, בפרטיותו של אדם. (1)הצלת חיי אדם או הגנה עליהם (2)גילוי עבירות, חקירתן או מניעתן; (3) גילוי עבריינים או העמדתם לדין (4)חילוט רכוש על פי דין״.

nevo.co.il

המשפט.[349] החובה לצו משתרעת מעבר לחיפוש במקום פיזי מאחר שנקבע בעניין *Katz v. United States*[350] שתיקון מגן על פרטים אינדיווידואליים, ולא על מקומות, וחל כאשר יש ציפייה אובייקטיבית לפרטיות שהחברה מזהה אותה כציפייה סבירה.[351]

אולם לציפייה הסבירה לפרטיות יש חריג בולט: דוקטרינת הצד השלישי (the Third-Party Doctrine), כלל חוקתי שמאפשר גישה למשתמש לתיעוד של רישומים עסקיים ומידע על עסקאות של לקוחות בלי שהדבר ייחשב חיפוש.[352] לפי הדוקטרינה, אם המידע מוחזק, או ידוע לצדדים שלישיים, אזי מבחינת התיקון הרביעי, לפרט אין ציפייה סבירה לפרטיות באשר למידע והוא אינו מוגן בתיקון הרביעי.[353] דוקטרינה זו עוצבה בבית המשפט העליון בארצות הברית בשנות ה־70 בעניין *United States v. Miller*,[354] שם, גורמי אכיפת החוק ביקשו להשיג תיעוד של פעולות פיננסיות של לקוח של בנק בשם מילר וביקשו את התיעוד בכל חשבונותיו. הבנק מסר את המידע המפליל. מר מילר טען שתחת התיקון הראשון גורמי אכיפת החוק היו צריכים לקבל צו שיפוטי כדי לקבל את המסמכים. אולם בית המשפט העליון קבע כי למילר אין ציפייה סבירה לפרטיות ביחס למסמכי הבנק, מאחר שהוא העביר את המידע לבנק וולונטרית והמידע נחשף לעובדי הבנק במהלך העסקים. שלוש שנים אחר כך הדוקטרינה הורחבה בעניין *Smith v. Maryland.*,[355] שם קבע בית המשפט העליון כי התיקון הרביעי לא חל לגבי מכשיר המתעד את כל מספרי הטלפון שחויגו מטלפון מסוים (pen register), מאחר שאנשים חושפים את מספר הטלפון שלהם לחברת הטלפונים שיש לה יכולת לתעד את המידע, לכן הם לוקחים על עצמם סיכון שהמספרים שחויגו יעברו למשטרה והתיקון הרביעי לא מגן עליהם.

מלומדים ביקרו את הדוקטרינה שמתעלמת מעקרונות של סודיות וחיסיון,[356] ולפני כמה שנים בעניין *Carpenter v. United States* צמצם בית המשפט העליון את הדוקטרינה במידה ניכרת.[357] נקבע כי גורמי אכיפת החוק לא יוכלו לאסוף היסטוריה של מיקום, cell site location information (CSLI), מטלפונים ניידים בלי צו שמראה עילה מסתברת שתתמוך בבקשה לאיסוף המידע.[358] דעת הרוב לא החילה את דוקטרינת הצד השלישי לאיסוף היסטוריית מיקום של

349 Travis Panneck, *Incognito Mode Is in the Constitution*, Minn. L. Rev. 511, 537 (2019); Neil Richards & Woodrow Hartzog, *Privacy's Constitutional Moment and the Limits* of *Data Protection*, 61 B.C. L. Rev. 1687 (2020); Solove, Nothing to Hide, The False Tradeoff Between Privacy And Security 93 (2011).

350 ראו עניין Katz v. United States, 389 U.S. 347 (1967).

351 Daniel J. Solove, Understanding Privacy 71 (2008).

352 להרחבה על הדוקטרינה ראו Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 567–570 (2009); Jane Bambauer, *Other People's Papers, 94* Tex. L. Rev.205, 206 (2015).

353 Kerr, שם, בעמ' 567–570.

354 United States v. Miller, 425 U.S. 435, 437 (1976).

355 Smith v. Maryland, 442 U.S. 735 (1979).

356 Neil Richards, Intellectual Privacy – Rethinking Digital Liberties in The Digital Age 136–139 (2015).

357 Carpenter v. United States, 138 S. Ct. 2206 (2018).

358 Carpenter v. United States, 138 S. Ct. 2206, 2223; Paul Ohm, *The Many Revolutions of Carpenter*, 32 Harv. J. L. & Tech 357, 361 (2019).

nevo.co.il

שבעה ימים מטלפון נייד על ידי ה־FBI[359] וצמצמה אותה.[360] ההשלכות רחבות מהסוגיה הצרה של מידע על מיקום, וניכר כי דעת הרוב מתייחסת למידע שרשויות אכיפת החוק יכולות להשתמש בו כדי לאתר פרטים באופן כללי, מעבר למידע על מיקום.[361] למרות שבית המשפט בעניין קרפנטר לא דחה את שנקבע בפסקי הדין מילר וסמית׳,[362] ניתן למצוא רמזים בפסק הדין לכך שבעתיד קביעות פסקי דין אלה יצומצמו לעובדותיהם.[363]

פסק דין *Carpenter* פתח את הדלת להגנה על כל סוגי המידע הדיגיטלי.[364] עניין *Carpenter* מסמל את תחילת ההיפרדות מהתקדימים בעניין דוקטרינת הצד השלישי. אולם דוקטרינת הצד השלישי לא נמחקה,[365] ובתי המשפט חלוקים באשר להיקף תחולת פסק הדין.[366] כך, לפחות פסק דין אחד החיל את דוקטרינת הצד השלישי באשר לתיעוד של עסקאות בביטקוין וקבע שלא נדרש צו לעניין זה.[367] אולם לאור פסק הדין, בעתיד יידרשו בתי המשפט לערוך איזון עדין בין דוקטרינת הצד השלישי במתכונתה המצומצמת להגנת התיקון הרביעי.[368] נראה כי פסק הדין יוביל להרחבת הגנת התיקון הרביעי מעבר לקביעה בפסק הדין בנוגע לאיסוף מתמשך של נתוני מיקום, מאחר שהמגמה בערכאות נמוכות להרחיב את תחולת פסק הדין גוברת עם הזמן ועולה על המגמה ההפוכה לצמצמו.[369] ההבנה בדבר חשיבות צו שיפוטי בעידן של טכנולוגיות משתנות, שלא הייתה מובנת מאליה, מחלחלת. נראה שהמסגרת המוצעת

359 Carpenter v. United States, 138 S. Ct. at, 2217.

360 Ohm, לעיל ה״ש 358, עמ׳ 358.

361 שם, בעמ׳ 369.

362 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (“We do not disturb the application of *Smith* and *Miller*...”); Ohm, לעיל ה״ש 358, בעמ׳ 369, 359.

363 Ohm, לעיל ה״ש 358, בעמ׳ 369, 385.

364 Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law 2018-2021*, 135 Harv. L Rev. 1791, 1800 (2022).

365 Neil Richards, Why Privacy Matters 59 (2021).

366 Tokson, לעיל ה״ש 364, בעמ׳ 13; Jeff Kosseff, The United States of Anonymous 161 (2022) (“Even after Carpenter, the Fourth Amendment provides only limited protection at best for anonymity”).

367 U.S. v. Gratkowski, 964 F.3d 307 (5th Cir. 2020). במקרה זה סוכנים פדרליים השתמשו בשירות חיצוני לנתח את המידע הציבורי בבלוקצ׳יין וזיהו צבר כתובות ביטקוין שנשלטות על ידי אתרים של פורנוגרפיית ילדים. בית המשפט קבע שאין לאתרים אלה ציפייה סבירה לפרטיות במידע בשרשרת הבלוקצ׳יין כאשר טבע המידע על הבלוקצ׳ין והוולונטריות של החשיפה שוקלת נגד הטענה לאינטרס בפרטיות במידע של הפרט על הבלוקצ׳יין. תיעוד החילופין לא נהנה מהגנת התיקון הרביעי. ראו גם Daniel Penn, *The Fifth Circuit, Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court’s First Ruling on Bitcoin Privacy*, 24 SMU Sci. & Tech. L. Rev. 125,128 (2021).

368 Richards, לעיל ה״ש 365, שם; Kosseff, לעיל ה״ש 366, בעמ׳ 161 (“Post carpenter, courts must individually assess the privacy intrusion of a government search to determine whether the Fourth amendment applies”).

369 Tokson, לעיל ה״ש 364, בעמ׳ 5 (“the proportion of cases employing narrow interpretations of Carpenter has decreased over time, as familiarity with the Carpenter standard has likely increased”).

nevo.co.il

במאמר שלפיה חשיפת זהות משתמשי מטבעות אלקטרוניים תהיה כפופה לצו יכולה להתקבל גם בארצות הברית, מאחר שחשיפת זהות משתמשי מטבעות אלקטרוניים חושפת מידע נרחב באשר לפעילותם הפיננסית. כך אף שהכפפת המסגרת המוצעת לצו כאמור אינה מובנת מאליה, היא תוכל להשתלב בהסדרה גלובלית בין־לאומית. הכפפת הליך החשיפה לצו תביא לאיזון בין זכויות המשתמשים לביטחון לאומי בעידן של טכנולוגיות.

(ג) מודל הסדרה גלובלי: שיתוף בין מדינות ואמנות בין־לאומיות

המודל המוצע לאימות זהות משתמשי מטבעות אלקטרוניים וחשיפתם בכפוף לצו כאשר מתקיים חשש של ממש לעבירות מימון טרור ואיסור הלבנת הון יהיה יעיל באופן מוגבל אם יוחל רק ברמה המדינתית.[370] אכיפת אימות הזהות וחשיפת הזהות בכפוף לצו מעוררת קשיי אכיפה בשל השוני בין שיטות משפט שונות. גורמי טרור וגורמים העוברים על איסורי הלבנת הון משתמשים במטבעות אלקטרוניים באופן גלובלי, ופעילותם אינה מוגבלת לטריטוריה יחידה. כך, מאמצים מדינתיים לחקיקה מקומית ואכיפתה אינם צפויים להביא לשינוי.[371] אכיפה חוצת גבולות של הרגולציה המוצעת בשיטות משפט שונות מציבה אתגרים.

אכן, עבירות חוצות גבולות מצריכות הגברת שיתוף פעולה וסיוע מרשויות אכיפה במדינות אחרות.[372] כיום יש מגוון כלים לתיאום בין רגולטורים וסוכנויות אכיפת החוק.[373] סל הכלים נע בין אמנות מחייבות לכללים רכים. כך, לדוגמה, בהקשר של מלחמה בפורנוגרפיית ילדים ובהקשרים פליליים אחרים, מדינות נסמכות על עזרת מדינות אחרות לפי אמנות בנושא פשיעת סייבר, שדורשות מהמדינות לשתף פעולה כדי לקדם חקירות פליליות ופרוצדורות.[374]

כיום, משטרות בעולם הדמוקרטי רואות בטרור פשע המחייב שיתוף פעולה כדי להכריעו.[375] לדוגמה, היורופול של האיחוד האירופי נטל על עצמו את המלחמה בטרור ורואה בטרור את אחת מצורות הפשיעה המצריכות שיתוף פעולה בין־לאומי, אף ששיתוף הפעולה לעניין זה חלקי ואינו מושלם.[376]

בהקשר של רגולציה של הלבנת הון ומימון טרור, מסגרת מדיניות גלובלית שגובשה במועצת הביטחון של האו״ם, רגולצה מדינתית וסטנדרטים גלובליים הותוו לחסום גישה של גורמי טרור למערכת הפיננסית.[377] כמו כן ה־ Financial Action Task Force (on Money

370 Roee Sarel, Hadar Y. Jabotinsky, Israel Klein, *Globalize Me: Regulating Distributed Ledger Technology*, 56 VAND. J.TRANS. L. 435 (2023).

371 ראו באשר לצורך ברגולציה ושיתוף פעולה חוצה גבולות בהקשר של מעבר מידע בין גבולות CARISSA VELIZ, PRIVACY IS POWER : WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 188 (2020). להרחבה על היתרונות שברגולציה גלובלית: Hadar Y. Jabotinsky, *The Network Effects of International Crypto Regulation* (Working Paper).

372 ראו פלאטו שנער, לעיל ה״ש 152, בעמ׳ 216.

373 DION-SCHWARZ, MANHEIM & JOHNSTON, לעיל ה״ש 3, עמ׳ 55.

374 Convention on Cybercrime art. 14, Nov. 23, 2001, E.T.S. 185.

375 הרפז, לעיל ה״ש 29, בעמ׳ 202.

376 שם, בעמ׳ 202–203.

377 Goldman et al., לעיל ה״ש 13, בעמ׳ 4.

nevo.co.il

(FATF) Laundering), ארגון בין־ממשלתי שמטרתו לפתח מדיניות בנוגע למלחמה בהלבנת הון ובמימון טרור שעליו הרחבנו,[378] מנחה את המדינות והארגונים החברים בו בעיצוב חקיקה שמטרתה להצר את צעדי ארגוני הפשע והטרור ואף מפעיל סנקציות כדי לכפות את יישום המלצותיו, העיקרית שבהן היא פרסום ב״רשימה שחורה״.[379] כמו כן, האמנה הבין־לאומית לעצירת מימון טרור שאומצה בשנת 1999 מיועדת להביא לייבוש המקורות הכספיים המזינים את הפעילות הטרוריסטית ולהביא למניעה כוללת של התופעה.[380] בארצות הברית חשיבות שיתוף הפעולה לסיכול מימון טרור הודגשה לאחר אירועי ה־11 בספטמבר. כשבועיים לאחריהם הכריז הנשיא דאז על מצב חירום והצהיר כי יש צורך בשיתוף פעולה ומידע על ידי מוסדות פיננסיים בתוך ארצות הברית ומוסדות פיננסיים זרים.[381]

קידום שיתוף פעולה בין־לאומי בחקירות הלבנת הון, פשיעה כלכלית ומימון טרור משתקף אף בסעיף 330 לחוק הפטריוט האמריקאי.[382] החוק מסמיך את נשיא ארצות הברית להורות למזכיר המדינה או לאוצר, ובהתייעצות עם מערכת ה־Federal Reserve, להיכנס למשא ומתן עם רשויות פיקוח על הבנקים במדינות אחרות וגורמי חוץ נוספים כדי להבטיח שמוסדות פיננסיים זרים שעושים עסקים עם מוסדות פיננסיים בארצות הברית, או שעשויים להיות מנוצלים על ידי ארגון טרור זר, ישתפו פעולה ויקיימו מערכת של העברת מידע הדדית עם הרגולטורים בארצות הברית. כך, בין היתר, נועד החוק כדי להבטיח שבנקים זרים ומוסדות פיננסיים ישמרו תיעוד הולם של העסקאות ומידע על חשבונות של כל ארגון טרור זר, או כל אדם שהוא חבר בארגון, ויאפשרו גישה לתיעוד זה לגורמי אכיפת החוק בארצות הברית וגורמים המפקחים על המערכת הבנקאית.[383] סעיף 328 מבקש לעודד מדינות לחייב את הבנקים בתחומן לציין את שמו המלא של האדם שנתן את ההוראה להעביר את הכסף.[384] בדומה לזה, שיתוף פעולה בין־לאומי מתגבר גם בתחום של העלמת מס.[385]

378 ראו לעיל ה״ש 100, והטקסט הצמוד אליה.

379 באום, לעיל ה״ש 2, בעמ׳ 291 (״הסנקצייה העיקרית שמפעיל ה FATF - כדי לכפות את יישום המלצותיו היא הכללה ב״רשימה שחורה״ של מדינות שמפרסם ה FATF - ואשר היכללות בה משקפת בעיני הארגון רמה לא מספקת של ציות להמלצותיו מבלי להקל ראש ברצון של רשויות או סיכון גבוה להלבנת הון, או שניהם גם יחד״). כמו כן ראו Geslevich Packin & Jabotinsky, לעיל ה״ש 104.

380 International Convention for the Suppression of the Financing of Terrorism, 2178 U.N.T.S. 197; לימון, לעיל ה״ש 28, בעמ׳ 18.

381 Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001) "I also find that a need exists for further consultation and cooperation with, and sharing of information by, United States and foreign financial institutions as an additional tool to enable the United States to combat the financing of terrorism".

382 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Pub. L. No. 107-56, 115 Stat. 272 (2001); 18 U.S.C. § 330.

383 שם, ראו גם פלאטו שנער, לעיל ה״ש 32, בעמ׳ 283.

384 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Pub. L. No. 107-56, 115 Stat. 272 (2001); 18 U.S.C. § 328 "(1) in consultation with the Attorney General and the Secretary of State,

nevo.co.il

גורמי אכיפת החוק במדינות שונות צריכים לעבוד יחד כדי להתמודד בהצלחה עם הלבנת הון ומימון טרור, אשר מושפעים משינויים בשוק הפיננסי הגלובלי והתפתחות טכנולוגיות פיננסיות חדשות. הדבר אינו שונה בענייננו, גם כאן נדרשת מסגרת לשיתוף פעולה שתעגן את אכיפת חובותיהם של ספקי הארנקים, שירותי ההמרה והחברות המנפיקות.[386] זאת באמצעות הרחבת תחולתן של אמנות בין־לאומיות העוסקות בפשיעה כלכלית ומימון טרור[387] כך שיחולו גם על מטבעות אלקטרוניים ותיאום ושיתוף פעולה שוטף שיתאפשרו באמצעות גופים בין־מדינתיים דוגמת ה־FATF. גופים אלה יאפשרו להפעיל לחצים בין־לאומיים פוליטיים וכלכליים וסנקציות נגד מדינות שלא ישתפו פעולה. שיתוף פעולה בין־לאומי הכרחי כדי לעצב כללים ללחימה באיומים של הלבנת הון ומימון טרור, לאכוף אותם ולחזק את המאבק הבין־לאומי נגד עבירות חוצות גבולות.[388] הצורך לפתח מסגרת גלובלית כדי להתייחס לאתגר של שימוש במטבעות אלקטרוניים להלבנת הון ולמימון טרור הוא מחויב המציאות להצלחת המסגרת המוצעת במאמר זה. אכיפה ושיתוף פעולה בין־לאומיים יאפשרו החלה גלובלית של ההסדרה המוצעת ויאפשרו מילוי מטרותיה ביעילות.

ד. התייחסות למגבלות וביקורות על הרגולציה המוצעת

אימות וחשיפה של זהות משתמשי מטבעות אלקטרוניים אינם פתרון קסם ויש להם מגבלות וחסרונות. בחלק זה נתייחס לכמה טענות נגד המסגרת המוצעת המציגות את מגבלותיה וחולשותיה, ונתמודד עימן. קיימות שש מוטיבציות עיקריות לפעול באנונימיות.[389] ראשית, אנונימיות יכולה לצמצם חשיפה לאחריות פלילית, או אזרחית; שנית, אנונימיות מאפשרת הגנה מפני התקפות פיזיות על אדם בשל דעותיו; שלישית, אנונימיות יכולה לצמצם נזק כלכלי לעסקו של אדם בשל דעותיו; רביעית, אנונימיות מאפשרת פרטיות והימנעות מתשומת לב לא רצויה; חמישית, אנונימיות מאפשרת חופש ביטוי והתייחסות לתוכן הביטוי או המעשה לגופם, ולא לזהות האדם שעומד מאחוריהם; ושישית, האנונימיות מאפשרת כוח והשפעה שפעמים רבות לא הייתה מתאפשרת לאדם הפועל בזהותו. בחלק זה נתמקד במוטיבציות העיקריות לאנונימיות שיכולות להיפגע בשל החלת המסגרת המוצעת, למעט המוטיבציה לחמוק מאחריות, שלגביה המסגרת המוצעת היא הפתרון, ולא הבעיה. נתייחס אפוא לפגיעת המסגרת

take all reasonable steps to encourage foreign governments to require the inclusion of the name of the originator in wire transfer instructions sent to the United States and other countries, with the information to remain with the transfer from its origination until the point of disbursement". ראו גם פלאטו שנער, לעיל ה"ש 32, בעמ' 283.

385 להרחבה ראו פלאטו שנער, לעיל ה"ש 152, בעמ' 214–219.

386 Goldman et al., לעיל ה"ש 13, בעמ' 4.

387 ראו לדוגמה International Convention for the Suppression of the Financing of Terrorism, 2178 U.N.T.S. 197.

388 Houben & Snyers, לעיל ה"ש 218, בעמ' 10.

389 Kosseff, לעיל ה"ש 366, בעמ' 14.

nevo.co.il

בזכות לאנונימיות כנגזרת של פרטיות ולפגיעה בזכות לחופש ביטוי. נוסף על זה נתייחס לביקורות על הרגולציה המוצעת בפגיעתה ביתרון הביזוריות של מטבעות אלקטרוניים; ובעלויות המנהליות שיחולו אם יקבלו את הצעתינו, הן עלויות בהטמעת הפתרון והן לחשש מפריצה למידע על זהות משתמשים וגנבת זהות.

1. הזכות לפרטיות

הזכות לפרטיות מוגנת בחוק הגנת הפרטיות, התשמ״א–1981 והיא אף זכות חוקתית המעוגנת בחוק־יסוד: כבוד האדם וחירותו.[390] הזכות לפרטיות מקדמת ערכים חשובים. ראשית, פרטיות מקדמת יצירת זהות, מאחר שהיא עוזרת לנו להבין מי אנו ובמה אנו מאמינים. היא מבטיחה את החופש האינטלקטואלי,[391] שחשוב לפיתוח הזהות, מרחב או מעין בועה של הגנה, שמגן מפני ההתבוננות של החברה, הממשלה, או הקהילה.[392] במרחב זה יכולים פרטים ליהנות מחופש ממבטם של אחרים.[393] שנית, פרטיות מבטיחה את החופש הדמוקרטי, מאחר שהיא מצמצמת את הסיכון לסחיטה והפליה בהסתמך על מידע שהושג, והיא אף מגינה על יכולתם של האזרחים לתקשר ולקבל מידע בלי חשש.[394] כך, היא הכרחית לביסוס חופש פוליטי.[395] שלישית, פרטיות מאפשרת הגנה כצרכנים וכעובדים, וללא הזכות לפרטיות גורמים שונים יסיקו על הפרט מסקנות ואף ישפיעו על העדפותיו הצרכניות ועל בחירותיו.[396]

אפשר לטעון שחשיפת זכויות משתמשי מטבעות אלקטרוניים פוגעת בזכות המשתמשים לאנונימיות כנגזרת של הזכות לפרטיות.[397] הזכות לאנונימיות מאפשרות העצמה של הפרט, בכך שהיא מאפשרת לו את האוטונומיה לשלוט בפרטים על זהותו.[398] זכות זו מאפשרת לאדם ״להיעזב לנפשו״,[399] מונעת נעיצת מבט לצנעת חייו וחשיפת מידע אישי על אודותיו שאינו מעוניין שיימסר[400] ומאפשרת הגבלת הגישה של אחרים למרחבים פרטיים.[401] אנונימיות

390 ס׳ 7 לחוק־יסוד: כבוד האדם וחירותו המעגן את זכותו של אדם לפרטיות ולצנעת חייו.

391 Neil Richards, Intellectual Privacy- Rethinking Digital Liberties in the Digital Age 11(2015), מתייחס לחופש המחשבה, החופש לקרוא בחופשיות ולתקשר בפרטיות.

392 Richards, לעיל ה״ש 365, בעמ׳ 113, 119.

393 Veliz, לעיל ה״ש 371, בעמ׳ 130 (“privacy is important to build a robust private sphere, a bubble of protection from society in which individuals can enjoy times and places free from others’ gaze, judgements, questions, and intrusion”).

394 Kosseff, לעיל ה״ש 366, בעמ׳ 44.

395 Richards, לעיל ה״ש 365, בעמ׳ 131, 147.

396 שם, עמ׳ 164.

397 ראו עניין **מור נ׳ ברק אי.טי.סי**, לעיל ה״ש 53, פס׳ 13, 16 לפסק דינו של המשנה לנשיאה דאז ריבלין.

398 Kosseff, לעיל ה״ש 366, בעמ׳ 3.

399 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890); Solove, לעיל ה״ש 351, בעמ׳ 15.

400 עניין **מור**, לעיל ה״ש 53, פס׳ 13.

401 Ruth Gavison, *Privacy and the Limits of Law*, 89 Yale L.J. 421, 446–47 (1980); Solove, לעיל ה״ש 351, בעמ׳ 18.

nevo.co.il

השימוש במטבעות אלקטרוניים מאפשרת פרטיות צרכנית – מסחרית.[402] שימוש במטבעות אלקטרוניים מאפשר לבצע רכישה של שירות או מוצר ככלל, ללא תיעוד שקושר את מבצע העסקה עם השירות או המוצר שניתן בשל האנונימיות היחסית שהמטבעות מאפשרים. כך הוא יכול לרכוש מוצר או שירות שאינו בנורמות במגזר או בחוגים שאליהם הוא משתייך, לדוגמה רכישת קלפי טארוט, או התייעצות עם מיסטיקן. האפשרות לחשוף את זהותו של אותו אדם פוגעת בפרטיות הצרכנית שלו.

אימות זהות המשתמשים והאפשרות לחשוף אותה בדיעבד פוגעת בפרטיות המשתמשים. היא יוצרת לגביהם מעין מאגר מידע אישי, מאחר שזהותו של אדם היא מידע אישי, וקושרת בינו לבין העסקאות שביצע. מאחר שפרטיות נמצאת על הרצף בין מידע סודי לחלוטין למידע הידוע לכל, יש דרגות שונות של פרטיות. אימות הזהות והאפשרות לחשוף אותה למעשה מגבירים את הדרגה על הרצף שבה נמצא מידע ידוע על אנשים.[403] היעדר האפשרות לבצע עסקאות צרכניות ללא חשש מעין בוחנת, או מקישור הרוכש לעסקה בשלב מאוחר יותר, יפחית את דרגת הפרטיות שלה זוכים המשתמשים ויביא לפגיעה בפיתוח הזהות של המשתמשים המתגבשת גם באמצעות שירותים ומוצרים שהם רוכשים. זאת מאחר שאפשרות החשיפה עלולה ליצור אפקט מצנן על רכישות מחשש לסטיגמה שיכולה להציב אדם באור שלילי בשל רכישת מוצרים או שירותים שאינם מקובלים במגזר או בחוג שבו הוא פועל.[404] החשש מחשיפת הזהות עלול להוביל לוויתור על שימוש במטבעות אלקטרוניים ולקונפורמיות ברכישות.[405] כמו כן, חשיפת המשתמשים עצמה עלולה לפגוע בחופש הדמוקרטי, אם רכישת המוצר או השירות יכולה להביך אדם הממלא תפקיד ציבורי בחוג או במגזר שבו הוא פועל, וגילוי העובדה שרכש את המוצר או השירות יכול להביא לסחיטה והפליה ולפגיעה בביסוס כוח ציבורי. נוסף על זה, חשיפת שם המשתמש במטבע האלקטרוני וקשירתו לרכישה יכולות לפגוע בו כצרכן מאחר שאם המידע על זהות הרוכש יעבור לצדדים שלישיים, יהיה להם יותר קל לנתחו ולהשפיע על העדפותיו הצרכניות של הרוכש ועל בחירותיו בעתיד. לפיכך אפשר לטעון כי אימות הזהות והאפשרות לחשוף אותה אינם רצויים.

אכן, אנונימיות מטבעות אלקטרוניים חשובה, ובהיעדרה ייפגעו ערכים חשובים של יצירת זהות, חופש דמוקרטי והגנת הצרכן. אולם גם הזכות לפרטיות אינה מוחלטת והיא כפופה לחריגים המאפשרים לפגוע בפרטיותו של אדם.[406] המסגרת המוצעת מכירה בחשיבות הזכות לפרטיות והערכים שהיא מקדמת ויוצרת איזון ביניהם בכך שהמידע בדבר זהות המשתמשים

402 בירנהק, לעיל ה״ש 76, בעמ׳ 282.

403 ראו Richards, לעיל ה״ש 365, המגדיר פרטיות כרמה בה מידע על בני אנוש ידוע או שמשתמשים בו.

404 ראו Ari Ezra Waldman, Privacy as Trust- Information Privacy for and Information Age 159 (2018).

405 Jonathon W. Penney, *Understanding Chilling Effects,* 106 Minn. L. Rev. 1451, 1494 (2022), מרחיב על אפקט מצנן כתופעה רחבה יותר של קונפורמיות שהיא הנטייה של אנשים לשנות את אמונתם, גישתם, או התנהגותם כדי שיתאימו עם אלה של אחרים.

406 פלאטו שנער, לעיל ה״ש 32, בעמ׳ 268 מתייחסת לפגיעה בסודיות הבנקאית כאשר הבנק מדווח דיווחים לרשות לאיסור הלבנת הון ומימון טרור.

nevo.co.il

יותמם ויוצפן, והחשיפה תתאפשר רק בצו שיפוטי בהתקיים רף גבוה של חשש של ממש[407] שנעשה שימוש במטבעות האלקטרוניים למימון טרור או להלבנת הון. כמו כן, המסגרת המוצעת תעוגן בחקיקה בנושא הלבנת הון ומימון טרור.

צו שיפוטי שיינתן כאשר יש חשש של ממש לעבירות אלה הוא נקודת איזון ראויה נורמטיבית המפחיתה את החשש לצינון שימוש לגיטימי במטבעות האלקטרוניים ומאפשרת ללחום בעבירות פליליות. נדגיש כי על בקשת הצו להיות צרה ככל האפשר ולכלול בקשה לחשיפה של מעורבים בעסקה ספציפית, ולא חשיפה סיטונית גורפת. כמו כן, אם בית המשפט נתן צו לחשוף את זהות המשתמשים, על הרשות החוקרת להשתמש במידע רק למטרות החקירה.

במישור הפוזיטיבי, אימות שמות המשתמשים וחשיפתם לפי צו שיפוטי הם למעשה פעולה לפי דין אשר זוכה להגנה לפי סעיף 18(2)(ב) לחוק הגנת הפרטיות,[408] ולפיכך גם לא תהיה חבות באחריות לחברות המנפיקות, ספקי הארנקים ושירותי ההמרה שמסרו מידע על זהות משתמשי המטבעות האלקטרוניים לפי צו כאמור. המסגרת המוצעת עומדת באיזון לפי חוק־יסוד: כבוד האדם וחירותו, שבו מעוגנת הזכות לפרטיות בסעיף 7, זאת מאחר שהמסגרת עומדת בתנאי פסקת ההגבלה שבסעיף 8 לחוק.[409] ראשית, חשיפת שמות המשתמשים תהיה בהסמכה מפורשת בחקיקה; שנית, היא הולמת את ערכיה של המדינה ומסייעת לצמצם מימון טרור, אשר מבקש לחתור תחת קיומה; שלישית, המסגרת המוצעת נועדה לתכלית ראויה, התמודדות עם הסיכון לביטחון הלאומי הטמון בשימוש במטבעות אלקטרוניים למימון טרור; ורביעית, הפגיעה היא במידה שאינה עולה על הנדרש, מאחר שהחשיפה תתאפשר רק בצו, ברף הוכחה גבוה, כאשר הצו יינתן באשר לעסקאות מסוימות, ולא יינתן צו לחשיפה המונית וגורפת של המידע.

באיזון הכולל בין השיקולים ובבחינת מידת פגיעתה של המסגרת באנונימיות כנגזרת של הזכות לפרטיות אל מול קידום המטרה החשובה של צמצום שימוש לרעה במטבעות אלקטרוניים למימון טרור ולהלבנת הון, נראה כי הפגיעה בזכות לפרטיות במתכונת המוצעת מוצדקת. כפי שצוין, הדין מאפשר איזון דומה בין הגנה על הפרטיות לבין קידום חקירה

407 נציין כי זהו גם הרף שהוצע לחשיפת גולשים אנונימיים בהצעת חוק מסחר אלקטרוני, התשע״א–2011, ראו ס׳ 13 ב להצעה (״הוכח להנחת דעתו של בית משפט כי קיים חשש של ממש שתוכנו של מידע שהועלה לרשת תקשורת אלקטרונית או הפצתו ברשת כאמור, מהווים עוולה כלפי אדם או הפרת זכות קניין רוחני שלו, רשאי הוא, על פי בקשת אותו אדם, להורות לספק שירותי אינטרנט המספק שירות גישה או שירות אירוח, למסור למבקש פרטים שברשותו שיש בהם כדי לזהות את מפיץ המידע״). אף שמימון טרור והלבנת הון הם עניינים פליליים, אנו עדיין סבורות כי ראוי לאמץ סטנדרט זה, כדי למנוע מצב שבו צווים לא יינתנו כעניין שבשגרה ויפגעו בזכויות משתמשי המטבעות.

408 ראו ס׳ 18 לחוק הגנת הפרטיות: ״במשפט פלילי או אזרחי בשל פגיעה בפרטיות תהא זו הגנה טובה אם נתקיימה אחת מאלה:...(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה״.

409 ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו: ״אין פוגעים בזכויות שלפי חוק־יסוד זה אלא בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שאינה עולה על הנדרש, או לפי חוק כאמור מכוח הסמכה מפורשת בו״.

nevo.co.il

למניעת פשיעה גם בהקשרים אחרים שנזכרו בחלק ג.2(ב): האזנת סתר,[410] חדירה לחומר מחשב[411] וחוק נתוני תקשורת.[412] ההתנגשות בין הזכות לפרטיות לקידום חקירה פלילית ומניעת פשיעה והאיזון שנערך באשר לחקיקה זו אינם שונים מהותית מזה שבענייננו ומובילים לתוצאה ראויה.

2. הזכות לחופש ביטוי

(א) חופש הביטוי של משתמשי מטבעות אלקטרוניים

הזכות לחופש ביטוי היא זכות יסוד. אף שזכות זו לא עוגנה מפורשות בחוק־יסוד: כבוד האדם, היא זכתה להכרה בפסיקה כחלק מהזכות לכבוד.[413] הזכות לאנונימיות אינה רק נגזרת של הזכות לפרטיות (עליה עמדנו בחלק הקודם), אלא שהאפשרות להתבטא באנונימיות היא חלק מחופש הביטוי.[414] למעשה, היכולת לשמור על אנונימיות היא לעיתים תנאי לעצם האפשרות או הנכונות להתבטא, ולעיתים האנונימיות היא חלק מהמסר עצמו.[415] "יש מצבים שבהם אדם שלא יוכל לדבוק באלמוניותו — לא יתבטא כלל. כך, למשל, בשל תחושות אישיות כמו בושה או מבוכה, או בשל לחצים חיצוניים וחששות מפני תגובת הסביבה".[416] האנונימיות מאפשרת לאדם לפעול ולהתבטא ומובילה להעצמת הפרט.[417] אפשר אפוא לטעון כי הטלת חובה על החברות המנפיקות, ספקי הארנקים ושירותי ההמרה לזהות את משתמשי המטבעות האלקטרוניים ולאפשר את חשיפתם פוגעת בחופש הביטוי של משתמשים אלה, מאחר שלהגבלת האנונימיות יהיה אפקט מצנן על הביטוי שלהם המשתקף בשימוש במטבעות האלקטרוניים. הידיעה כי זהותם עלולה להיחשף יכולה להביא לוויתור על רכישות לגיטימיות של מוצרים ושירותים, אף אם הרכישה לגיטימית, ולהביא לקונפורמיות ברכישות שלמעשה מהוות ביטוי של הצרכן.[418] לפיכך, אפשר לטעון כי הטלת חובות אלה אינה חוקתית.

זיהוי של אדם יכול לספק מידע על תוכניותיו לעתיד, אפילו בהיעדר מידע על תוכן התקשורת.[419] כך גם במשפט האמריקאי הוכרה הזכות לתקשר באנונימיות.[420] שורה של פסקי

410 ס' 6 לחוק האזנת סתר, התשל"ט–1979.

411 ס' 23א(ב) לפקודת סדר הדין הפלילי (מעצר וחיפוש).

412 ס' 1 (סעיף ההגדרות) לחוק סדר הדין הפלילי (סמכויות אכיפה — נתוני תקשורת).

413 ראו בג"ץ 4804/94 **חברת סטיישן פילם בע"מ נ' המועצה לביקורת סרטים ומחזות**, פ"ד נ(5) 661, 675 (1997) (הנשיא ברק); בג"ץ 2481/93 **דיין נ' וילק**, פ"ד מח(2) 456 (1994).

414 עניין **מור**, לעיל ה"ש 53, פס' 11 לפסק דינו של המשנה לנשיאה דאז ריבלין.

415 **שם**, בפס' 12.

416 **שם**, בפס' 11.

417 Kosseff, לעיל ה"ש 366, בעמ' 212.

418 ראו הדיון בנושא זה באשר לזכות לפרטיות ה"ש 404– 405 והטקסט הצמוד אליהן.

419 Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 Ariz. L. Rev. 95,99 (2017).

420 Kosseff, לעיל ה"ש 366, עמ' 3 ("Anonymity is deeply footed in the constitutional values and social norms of the United States"); Froomkin, לעיל ה"ש 419, בעמ' 149 ראו גם בהקשר משיק על מצלמות זיהוי משטרתיות ופגיעה בזכות לאנונימיות Julian R. Murphy, *Chilling: The*

nevo.co.il

דין בארצות הברית הבהירה שיש זכות חוקתית לביטוי אנונימי, בעיקר בנושאים פוליטיים ובנושאים הקשורים לדת.[421] יצוין כי בארץ בית המשפט העליון בעניין **מור**, בהקשר משיק של לשון הרע באינטרנט, הדגיש את החשיבות של הזכות לאנונימיות כנגזרת של פרטיות וביטוי ופסק כי לא קיימת כיום מסגרת דיונית הולמת למתן צו המורה לחשוף את זהותו של גולש אנונימי משמיץ באינטרנט ונמנע מלהורות על חשיפה.[422] האם ראוי להתוות מסגרת לחשיפת משתמשי מטבעות אלקטרוניים לכתחילה?

אפשר לטעון כי אימות זהות שמות המשתמשים וחשיפת זהותם פוגעים בחופש הביטוי של משתמשי המטבעות. מנגד, אפשר לטעון ששימוש במטבעות אלקטרוניים אינו ביטוי, והגבלות

Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests, 75 WASH. & LEE L. REV. ONLINE 1, 25–27 (2018).

421 KOSSEFF, לעיל ה״ש 366, **בעמ׳ 49—50**; Talley v. California, 362 U.S. 60 (1960) (בית המשפט העליון בארצות הברית ביטל צו של העיר לוס אנג׳לס שאסר על חלוקת עלונים בכל מקום ובכל נסיבות אם העלונים לא כללו את השם והכתובת של האדם שהם הוכנו עבורו), McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995) (בית המשפט העליון בארצות הברית ביטל חוק באוהיו שאסר על קמפיין אנונימי. בית המשפט קבע כי חוק כזה מפר את התיקון הראשון לחוקה האמריקנת ואינו חוקתי) ראו גם Buckley v. Am. Constitutional Law Found. Inc., 525 U.S. 182, 198–200, 204 (1999); Watchtower Bible & Tract Soc'y v. Vill. of Stratton, 536 U.S. 150, 160, 166–69 (2002).

422 ראו עניין **מור**, לעיל ה״ש 53, פס׳ 23. וראו גם בג״ץ 589/17 **פלונית נ׳ הכנסת** (נבו 26.1.2017); ת״א (שלום פ״ת) 40129-09-21 **כהן נ׳ google inc.** (נבו 26.4.2023) ״הלכת מור נותרה על מכונה, וכל עוד אין דבר חקיקה הקובע מסגרת דיונית הולמת למתן צו המורה לחשוף את זהותו של גולש אנונימי, אין ׳להמציא׳ מסגרת כזו ב׳חקיקה שיפוטית׳״. להרחבה ראו חאלד גנאים, מרדכי קרמניצר, בועז שנור **דיני לשון הרע, הדין הרצוי והמצוי** 257—259 (2019). לביקורת על העדפת מסגרת חקיקתית, ולא פסיקתית, ראו אמל ג׳בארין, יצחק כהן ״חשיפת זהותם של משתמשים אנונימיים באינטרנט – נקודת מבט מוסדית״ ***מחקרי משפט*** **כח** 7 (2012); לביקורת על התוצאה של מניעת גישה לערכאות ראו אמל ג׳בארין ״הזכות לאנונימיות זכות הגישה לערכאות סמכות טבועה ומה שביניהם״ ***מחקרי משפט*** **כט** 309, 324 (2013). יצוין כי לאחרונה בית משפט השלום למעשה החיל את הלכת מור מחוץ למרחב המקוון וקבע כי אין סמכות לחייב את חברת השכרת הקורקינטים ווינד לחשוף פרטי משתמשת בקורקינט שפגעה ברכב וצולמה במצלמת הרכב. אולם השופט קרא למחוקק להסדיר הליך המאפשר לבית משפט לחייב את מסירת פרטי צד שלישי במקרים כאלה. ראו ת״א (שלום ת״א) 61142-07-21 **כהן נ׳ ווינד תל-אביב (בייקי) בע״מ** (נבו 2.4.2022), אולם לאחרונה החלטה זו נהפכה בבית המשפט המחוזי, ע״א (מחוזי ת״א) 8720-06-22 **כהן נ׳ ווינד תל-אביב (בייקי) בע״מ**, פס׳ 11 (נבו 2.11.2022), ונקבע כי ״הסיטואציה שונה מהותית מן הסוגיה שעמדה לפני בית המשפט בעניין מור. שם, הגולש הביע בצורה ברורה ומובהקת את רצונו לשמור על אנונימיות. על כן, בעניין מור הקדיש בית המשפט כר נרחב לדיון בסוגית חופש הביטוי והזכות לפרטיות שנובעת מאותו רצון לאנונימיות שם, פסקאות 11-22.) ברם בענייננו, המזיק שזהותו אינה ידועה, לא הגדיר בעצם ההתקשרות עם המשיבה רצון לאנונימיות. נהפוך הוא. לפני שנשכר על ידו הקורקינט שעל פי הנטען הסב את הנזק לתובע, נמסרו למשיבה מלוא פרטיו של השוכר. לא נדרשה אנונימיות ולא פרטיות. וודאי שאין כאן עניין של חופש ביטוי. זאת ועוד, הובהר לשוכר על פי תנאי השימוש של המשיבה כי המשתמש בקורקינט עלול להיות חשוף לכך שהמידע שמסר יועבר או יעשה בו שימוש בעת תאונה (מוצג 7א לערעור). כמו כן, לא נדרשה כאן ביצוע פעולה אקטיבית וחודרנית, כדוגמת איתור כתובת IP של מי שהזדהה מראש באופן אנונימי, כפי שנדון בעניין מור. הפרטים נמסרו על ידי שוכר הקורקינט מראש ומרצונו החופשי״.

nevo.co.il

על אנונימיות המשתמשים אינן הגבלות על שוק הרעיונות, אלא על שוק המסחר.[423] אולם אפשר לטעון כי מטבעות אלקטרוניים הם לא רק תשלום דיגיטלי, אלא שלמטבעות יש ערך של תקשורת כאשר הם מאפשרים למשתמשיהם לתקשר בדרך שלא הייתה אפשרית קודם לכן, מאחר שעצם השימוש בהם הוא הבעת חוסר אמון בכלכלה המבוססת על מתווכים מרכזיים.[424] חשוב מכך, השימוש במטבעות האלקטרוניים מאפשר חופש ביטוי שמתבטא ברכישות. אימות זהותם של משתמשי המטבעות והאפשרות לחשוף את זהותם הם למעשה צנזורה על פעילות שיש לה ערך של ביטוי. כך, למשל, השימוש במטבעות אלקטרוניים אנונימיים יכול לאפשר לאדם שאינו רוצה להיות מזוהה פוליטית בפומבי לתרום למטרות פוליטיות לגיטימיות שהוא מזדהה עימן מבלי שיקשרו את התרומה ישירות אליו (למשל: רפובליקני שרוצה לתמוך בקליניקה להפלות בארצות הברית). אולם, אפשר לטעון כי למרות שאפשר לראות בשימוש במטבעות אלקטרוניים ביטוי, אפשר לטעון כי הם לא מייצגים את אותם אינטרסים שבליבת חופש הביטוי.[425] בדומה לזה, בפסק הדין בעניין **דהרי**[426] קבע בית משפט השלום כי אפשר לחשוף ספק אנונימי שהפיץ ביטוי מסחרי פרסומי (ספאם) לפי סעיף 30א(א) לחוק התקשורת, זאת מאחר שהזכות לשווק סחורה אינה חלק מחופש הביטוי במובנו הערכי.[427] עוד נקבע, כי הלכת **מור** לא חלה על ספאם.[428] גם באשר לשימוש במטבעות אלקטרוניים, הערך של הביטוי הוא מופחת[429] לעומת ביטוי שבליבת השיח דוגמת ביטוי פוליטי.

נוסף על זה, עניין רמי מור עסק בעוולה אזרחית, ונקבע שם מפורשות כי בעניינים פליליים לרשויות האכיפה סמכויות חקירה ובדיקה, והיעדר הליך בהקשר האזרחי אינו מסכל חקירה פלילית.[430] המסגרת המוצעת אף היא מתמקדת בהיבטים פליליים של פעילות פיננסית שמתאפשרים על ידי מטבעות אלקטרוניים. כך שהאיזון הוא בין הזכות לביטוי שאינו ביטוי פוליטי בליבת חופש הביטוי (אף שיכול לאפשר ביטוי זה במקרים מסוימים), לבין הערך של הגנה מפני עבירות חמורות והצורך להילחם בתופעות של הלבנת הון ומימון טרור בשימוש במטבעות אלקטרוניים. יתרה מזו, לפי המסגרת המוצעת חשיפת משתמשי המטבעות

423 Alexander Tsesis, *Marketplace of Ideas, Privacy, and Digital Audiences,* NOTRE DAME L. REV. 1585, 1588 (2019), מבחין בין התנהגות שוק לחופש הביטוי.

424 Justin S. Wales, *Bitcoin is Speech: Notes Toward Developing the Conceptual Contours of Its Protection Under the First Amendment*, 74 U. MIAMI L. REV. 204, 222 (2019).

425 להרחבה על פעילות שאינה בליבת חופש הביטוי, כמו למשל פרסום פרסונלי ממוקד, והיקף ההגנה המופחת על ביטויים אלה ראו RICHARDS, לעיל ה"ש 365, בעמ' 382.

426 ת"א (שלום טב') 16448-03-19 **דהרי נ' כושר פיננסי** (נבו 29.8.2019).

427 חוק התקשורת (בזק ושידורים), התשמ"ב–1982.

428 עניין **דהרי**, לעיל ה"ש 426, פס' 10: "הנה כי כן, להבדיל מהזכות להביע תחושה, דעה, ביקורת או עמדה, הזכות לפנות לקהל הרחב על מנת לשווק סחורה אינה מהווה חלק מחופש הביטוי במובנו הערכי – החוקתי אשר זכויות יסוד אחרות ניגפות מפניו. לשון אחר: הערך המוגן אשר לכבודו ולשם הגנה עליו דחה בית המשפט העליון את התביעה בפרשת **רמי מור** – אינו קיים במקרה של פרסום מסרונים בעלי מטרה שיווקית – מסחרית".

429 התנהגות השוק כביטוי שונה מביטוי פוליטי ונראה כי יש להקנות לו הגנה פחותה. ראו בהקשר משיק בנוגע לביטוי מסחרי אהרן ברק **כבוד האדם – הזכות החוקתית ובנותיה** 751 (2014).

430 עניין **מור**, לעיל ה"ש 53, פס' 36 לפסק דינו של המשנה לנשיאה דאז ריבלין, פס' יד' לפסק דינו של השופט רובינשטיין.

nevo.co.il

האלקטרוניים תהיה לפי צו שיפוטי שיעוגן בחקיקה, כאשר יש חשש של ממש לעבירה. כאשר חשיפת המשתמשים כפופה לצו שיפוטי, לא צפוי אפקט מצנן משמעותי על השימוש במטבעות אלקטרוניים, מאחר שמשתמשים ידעו שחשיפת זהותם כפופה לצו שיינתן רק כאשר יש חשש של ממש שנעשה שימוש לרעה במטבע האלקטרוני להעברה פיננסית של כספים, או עסקה לא חוקית. הצו השיפוטי יהיה בעצם הגורם המאזן שימנע פגיעה בשימוש לגיטימי במטבעות אלקטרוניים. כך נקודת איזון זו עומדת בתנאי פסקת ההגבלה בחוק־יסוד: כבוד האדם וחירותו.[431] מסגרת זו מאפשרת לכן איזון בין חופש ביטוי לצורך לצמצם נזק מעבירות פליליות ומטרור. כך המסגרת המוצעת מוצדקת במישור החוקתי.[432]

(ב) אימות זהות, חשיפת זהות וחופש הביטוי של החברות המנפיקות, ספקי הארנקים ושירותי ההמרה

היבט נוסף של חופש הביטוי נוגע לחופש הביטוי של החברות המנפיקות, ספקי הארנקים ושירותי ההמרה (להלן: חברות המטבעות). אפשר לטעון שהחובות המוצעות באשר לאימות זהות וחשיפתה מגבילות את החופש של חברות אלה לעצב את הקוד הטכנולוגי של המערכת שלהם. הקוד הטכנולוגי הוא מידע אשר הוכר כביטוי, ובארצות הברית אף הוקנתה לו הגנה רחבה.[433] בגלל ששפת מחשב וקוד הם ביטוי, חובה לעצב מערכת שמאפשרת אימות זהות משתמשים אקס אנטה ומאפשרת לחשוף אותם אקס פוסט יכולה לפגוע בזכות לחופש הביטוי של התאגידים שנדרשים לחשוף את המידע על המשתמשים במוצרים שלהם.[434] יצוין כי הטיעון שלפיו טכנולוגיות מוגנות קוד ללא ערך ביטויי מוגנות בחופש הביטוי זכה לביקורת מלומדים, מאחר שהכרה בזכות מדללת עקרונות של התיקון הראשון ומאיימת על חוזקו.[435] אולם, בתי משפט בארצות הברית הכירו באינטרסים של ביטוי בקוד הטכנולוגי.[436] כך, אפשר לטעון שהמסגרת המוצעת פוגעת בזכויות חופש ביטוי של החברות שיצטרכו לזהות את משתמשי המטבעות האלקטרוניים.

אולם, למרות שכלים טכנולוגיים באים בגדר ביטוי, הערך של ביטוי זה אינו אבסולוטי. עיצוב כלים שמנחים את הטכנולוגיה שמעצבת מערכות פיננסיות אינו השתתפות בשוק

431 ראו ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו.

432 Kosseff, לעיל ה״ש 366, בעמ׳ 227 (מרחיב על אנונימיות כחרב ועל המסגרת של התיקון הראשון לחוקה האמריקאית שמאפשר חשיפת זהות אנונימיות בהתקיים האיזונים המתאימים).

433 llen Nakashima& Mark Berman, *Apple Says FBI Seeks "Dangerous Power".Files Motion Opposing Court Order to Help Unlock iPhone*, Wash Post (Feb. 25, 2016); Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011); Bambauer, *Is Data Speech*?, 66 Stan. L Rev. 67 (2014), במבאוור סבורה כי גם מידע יכול ליהנות מהגנת התיקון הראשון כאשר הוא מקדם את הזכות ליצור ידע.

434 Kyle Langvardt, *The Doctrinal Toll of "Information as Speech"*, 47 Loy. U. Chi. L.J. 761, 770, 798 (2016).

435 Langvardt, שם

436 ראו לדוגמה Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996).

הרעיונות והדעה הציבורית, אלא מדובר בהתנהגות שוק שמשתמשת ב"ביטוי".[437] לאור העובדה שמדובר בביטוי של תאגיד ולנוכח הטבע המסחרי של הביטוי שמבנה את הקוד כחלק ממוצר, או כלי בשוק המסחר, החובה להטמיע בקוד הטכנולוגי מנגנונים לאימות זהות ויכולות לחשוף את המשתמשים נהנית מהגנה מופחתת של חופש הביטוי.[438] לאור חשיבות המלחמה בתופעות של הלבנת הון ומימון טרור בשימוש במטבעות אלקטרוניים וחשיבות המסגרת המוצעת בסיכול מבצעי טרור והגברת הביטחון הלאומי מול הערך (המופחת) של חופש הביטוי בקוד הטכנולוגי, נראה שהמסגרת המוצעת, שיישומה הוא בכפוף לצו שיפוטי, עומדת בתנאי פסקת ההתגברות ותקפה חוקתית.[439]

3. חשש מריכוזיות של כוח: מהקתדרלה לבזאר וחזרה לקתדרלה?

הקתדרלה והבזאר הם שני מודלים ידועים באשר להנדסת קוד תוכנה.[440] המודל של קתדרלה מגביל את הקוד המפותח לקבוצה ריכוזית של מפתחים. בשונה מזה, המודל של בזאר הוא ביזורי. הקוד שמפותח הוא קוד פתוח, וכל הציבור יכול להסתכל עליו ולעיתים גם לתרום לפיתוחו. למרות ששני המודלים מתייחסים לפיתוח תוכנה, המטפורות של קתדרלה ובזאר יכולות לתאר הקשרים חברתיים ומבנים רחבים יותר כמו המבנה של המערכת הפיננסית.

במודל מסורתי של "קתדרלה", המדיום של חילופי הילך חוקי דורש התערבות של מוסדות ריכוזיים. בשונה מזה, מטבעות אלקטרוניים פועלים באופן אוטונומי ומבוזר, עצמאית מרשות או מפעיל מרכזי. אין להם גיבוי ריבוני של מדינה והם חסרים הרבה מהתכונות של מטבע מדיני. אפשר לדמות מטבע אלקטרוני ל"בזאר".[441] האתוס הליברטריאני מעודד פרטים וישויות שמעורבים ביצירה והתרחבות של תנועה של מטבע אלקטרוני.[442] אולם הטלת חובות משפטיות על חברות המטבעות יכולה להוביל לריכוזיות ולמעשה לסמל את החזרה לאחור למודל של "קתדרלה", היכן שמתווך מרכזי מסדיר את השוק.

מהלך דומה לזה התרחש באינטרנט, אשר נחשב בעבר כמדיום סוברני ללא מתווכים שנשלט מלמטה למעלה בידי המשתמשים, ונוצרו בו מתווכים חדשים (המתווכים

437 ראו בהקשר משיק של ביטוי של אלגוריתם Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law In The Age of Predictive Analytics*, 79 MD. L. REV. 439, 502 (2020) ("they are forms of market behavior that use speech. Therefore, states may regulate the speech involved in them").

438 Nathan Cortez, William M. Sage, *The Disembodied First Amendment*, 100 WASH U. L REV. 707, 757 (2023) ("corporations should not have intrinsic constitutional rights as speakers").

439 ראו הדיון בחלק הקודם ה"ש 431 והטקסט הצמוד אליה.

440 את המטפורה של הקתדרלה והבאזר טבע אריק ראימונד שהשווה רישיון תוכנת מחשב ריכוזי וקוד פתוח דוגמת לינוקס. ראו: ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY (1999).

441 אריק ראימונד טבע את המטפורה הזו של קתדרלה ובזאר בהקשר משיק, כאשר השווה קוד מחשב מרכזי ברישיון לעומת לינוקס ראו: ERIC S. RAYMOND THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY (1999).

442 Goldman et al., לעיל ה"ש 13.

nevo.co.il

המקוונים).[443] מערכת הבלוקצ׳יין כבר היום הופכת למבוזרת פחות.[444] אפשר לטעון שהטלת חובות על חברות המטבעות לאימות זהות וחשיפת משתמשי מטבעות אלקטרוניים תגביר את המעורבות שלהם ברגולציה, תעוות את חלוקת הכוח בתשתית ותחתור תחת המודל המבוזר של המטבעות האלקטרוניים, אשר אין בו את החסרונות של מוסדות פיננסיים מסורתיים ושליטה של המדינה. החובות המוצעות עלולות לפגוע באמון המשתמשים במערכת ולעכב חדשנות. לפיכך, אפשר לטעון שזו טעות לדכא מודל חדשני מבוזר בגלל שחקנים גרועים, כמו גורמי טרור או פשיעה שעושים בו שימוש לרעה.[445]

אכן, הטלת חובות על חברות המטבעות אינה תרופת קסם. אולם, אימות זהות אקס אנטה וחשיפתה בכפוף לצו שיפוטי אקס פוסט אינן חובות המכוונות ישירות לעסקה הפיננסית עצמה, או לטכנולוגיה. כך, הן שונות ממודל שמירת סף מסורתי כמו עצירת תשלום, ופגיעתן במבנה המערכת פחותה.[446] בגלל שזהות המשתמשים מוצפנת ויכולה רק להיחשף בכפוף לצו היכן שיש חשש של ממש לעבירות של הלבנת הון או מימון טרור, רגולציה כזו מכוונת לשחקנים מפירי חוק שמשתמשים במערכת לקידום פעילויות פליליות.[447] לפיכך, השפעת חובות אלה על עסקה פיננסית לגיטימית של משתמשים תמימים והעברות כלליות של כסף תהיה מוגבלת, ולא צפויה להן השפעה מרחיקת לכת על המבנה המיוחד של המערכת ועל האמון של משתמשים תמימים בה. אומנם המסגרת המוצעת מקצה יותר כוח לחברות המטבעות, ולמרות שהיא מכוונת לשחקנים גרועים, היא עשויה לשבש במידת מה את המבנה המבוזר של המערכת. אולם, כאשר מאזנים את העלויות החברתיות של פגיעה זו כנגד התועלות לביטחון הלאומי ולסדר הציבורי, באיזון הכולל הטלת החובות המוצעות מוצדקת.

4. עלויות מנהליות של אימות זהות אקס אנטה וחשיפתה אקס פוסט

ביקורות נוספת על הרגולציה המוצעת נוגעות לעלויות מנהליות של אימות זהות משתמשי המטבעות האלקטרוניים, עלויות אחסון ואבטחה של המידע ועלויות הטיפול בהליכים של חשיפת המשתמשים. כל משטר רגולטורי חדש מייקר עלויות,[448] ואפשר לטעון כי הטלת

443 ראו חלק א׳ למאמר זה אשר מרחיב על תפקיד המתווכים כשומרי סף. ראו גם Julie E. Cohen, Between Truth and Power: The Legal Constructions of Information Capitalism 75 (2019), מסבירה כי חלק מההיבטים של התפיסה של ״טכנולוגיה של חופש״ השתנו מעבר להכרה והתשתית הדיגיטלית כיום היא בעלת יכולות השפעה מורכבות הרבה יותר.

444 ראו De Filippi, לעיל ה״ש 1, (“Over the years, the governance of the most popular blockchain networks has become highly centralized, and only a few large corporations (such as the main blockchain exchanges and wallet providers) are responsible for making blockchain technology accessible to the wider public”).

445 לטיעון זה ראו Houben & Snyers, לעיל ה״ש 218, בעמ׳ 85.

446 על עצירת תשלום ראו חלק ראשון ובפרט Anne Marie Bridy, *Internet Payment Blockades*, 67 Fla. L. Rev. 1523 (2016).

447 Houben & Snyers, לעיל ה״ש 218, בעמ׳ 56.

448 Breu & Seitz, לעיל ה״ש 255.

חובות על חברות המטבעות מרחיקת לכת ותגרום לחלק מהחברות לצאת מהשוק.[449] יתרה מזו, משקיעים חדשים עלולים להימנע מהשקעה במערכות כאלה ולהימנע מלפתח מערכות חדשניות יותר של מטבעות אלקטרוניים. אפשר אפוא לטעון כי רגולציה כזו תוביל לאי־יעילות בשוק.

לרגולציה המוצעת יש אכן עלויות, אולם אפשר לטעון שההטבות של הפתרון המוצע בקטיעת הספקת החמצן לפעילות גורמי טרור, הגברת הביטחון הלאומי והצבת קשיים בפני הלבנת הון עולות על העלויות של הטמעת מסגרת של אימות זהות, ובסופו של דבר המסגרת המוצעת ממקסמת את הרווחה בכללותה.[450] חובות אימות זהות כבר קיימות בהקשרים אחרים, וכפי שהראינו בחלק א.2 גם במערכת הבנקאית המסורתית קיימת חובה להכיר את הלקוח. המגמה להטיל חובה זו אומצה גם בתחומים אחרים. לדוגמה, הצעת חקיקה באירופה באשר לשירותים דיגיטליים – Digital Services Act (DSA)[451] מבקשת להטיל חובות על שווקים מקוונים לזהות סוחרים שמציעים מוצרים ושירותים ולאסוף מידע מפורט על זהותם של הסוחרים.[452] לפי ההצעה, על הפלטפורמות הדיגיטליות להשקיע מאמץ סביר להבטיח שהמידע שמסופק הוא מדויק ומלא. לחובה חדשה זו עלויות מנהליות. אולם, בגלל שחובה זו תסייע לאתר סוחרים נוכלים ולהגן על קונים בשווקים האלקטרוניים מקניית מוצרים מזויפים, או ממוצרים מסוכנים, בכך שהזיהוי יקל את אכיפת הפרות הדין, היא מוצדקת.[453] הצעת חוק דומה להטלת חובות הכרת הלקוח על שווקים מקוונים הוצעה לאחרונה גם בארצות הברית.[454]

449 תהליך זה כבר מתרחש בעקבות הטמעת הדירקטיבה החמישית האירופית לאיסור הלבנת הון (5th European Anti-Money Laundering Directive), לדוגמה, חברת ארנקים בשם Bottle Pay, המבוססת בבריטניה, הודיעה על החלטתה להפסיק פעילות בסוף 2019, ולפי הפוסט שהחברה פרסמה ב־13 לדצמבר 2019 היא נימקה את הפסקת הפעילות בקושי לציית ולעמוד בתנאי הוראות הדירקטיבה לאיסור הלבנת הון. "As we are a UK based custodial Bitcoin wallet provider, we will have to comply with the 5AMLD EU regulation coming into effect on January 10, 2020. The amount and type of extra personal information we would be required to collect from our users would alter the current user experience so radically, and so negatively, that we are not willing to force this onto our community" (Rachel Wolfson, *What the 5th Anti-Money Laundering Directive Means for Crypto Businesses*, COINTELEGRAPH (Jan.10, 2020)).

450 על תפקיד כללים בקידום מקסום הרווחה ראו John R. Hicks, *The Foundations of Welfare Economics*, 49 ECON. J. 696, 708 (1939).

451 European Commission, 15 December 2020, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Document COM(2020) 825 final 2020/0361.

452 Digital Services (Digital Services Act), Art 22.

453 ראו בהרחבה Miriam C. Buiten, *The Digital Services Act: From Intermediary Liability to Platform Regulation* (Working paper, June, 2021) (at 21).

454 INFORM Act HB 5502. נציין כי החוק עבר בקונגרס לאחרונה ונכנס לתוקף ב־27.6.2021 ראו Lesley Fair, INFORM Consumers Act takes effect on June 27th. Is Your Business Ready?Federal Trade Commission Business Blog (June 8, 2023) https://www.ftc.gov/business-guidance/blog/2023/06/inform-consumers-act-takes-effect-june-27th-your-business-ready.

nevo.co.il

באשר לחשיפת משתמשים, בארצות הברית מתקיימים הליכים של חשיפת משתמשים מפירי דין מול ספקי תוכן המאחסנים מידע על משתמשים, כמו כתובות ה־IP שלהם, למרות הנטל שהליכים אלה כופים. לדוגמה בבתי משפט בארצות הברית ניתנים צווי זימון לבית משפט מסוג John Doe subpoenas לחשיפת זהות הגולשים האנונימיים מספק שירותי האינטרנט (ISP) או מהאתר שבו פרסמו תכנים מפירי דין.[455] הליכים מעין אלה התקיימו בעבר בארץ,[456] לפני פסיקת בית המשפט העליון בעניין מור שהגבילה את האפשרות לחשיפת גולשים משמיצים בהיעדר מסגרת דיונית הולמת.[457] כמו כן, גם לאחר פרשת מור התאפשרה לעיתים חשיפה בסוגי ביטויים אחרים שאינם לשון הרע.[458] הטלת חובות על מתווכים מסורתיים לספק מידע בהליכים של חשיפת גולשים אנונימיים מוצדקת מנקודת מבט כלכלית, מאחר שספקי התוכן והאתרים הם בעמדה הטובה ביותר לאסוף, לאחסן ולספק את המידע בהליכים משפטיים. בדומה לזה, הרגולציה המוצעת מוצדקת על בסיס אותם טיעונים. נוסף על זה, אימות זהות של משתמשי מטבעות אלקטרוניים אינה מהפכנית. הליכי אימות דומים היו אמורים להיערך וולונטרית בבלוקצ׳יינים הפרטיים של המטבעות – Diem (לשעבר ״ליברה״) ו־Saga, אשר התכוונו לאמת את זהות כל משתמשיהם.[459] לאור העובדה שפרקטיקה זו כבר הוצעה על ידי התעשייה בעבר, אפשר לטעון כי עלויות אימות הזהות והכנת התשתית לחשיפתה אינן בלתי סבירות. לאור חשיבות אימות וחשיפת הזהות לביטחון הלאומי ומניעת פשיעה, ראוי וגם יעיל כי תוטל חובת אימות כזו על חברות המטבעות למרות עלויות מנהליות הכרוכות בחובות אלה.

5. חשש מפריצה למידע וגנבת זהות

ביקורת נוספת על הרגולציה המוצעת מתמקדת בחשש מפריצה למידע. הטלת חובה על החברות המנפיקות, ספקי הארנקים ושירותי ההמרה לאמת את זהות משתמשיהם כוללת מידע אישי הנוגע לזהות. מידע זה יכול לשמש לרעה מפירי חוק, אם תהיה פריצה למידע.[460] פריצה

455 Nathaniel Gleicher, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 344 (2008), מרחיב על השיקולים והסטנדרטים שבתי המשפט בארצות הברית שוקלים כאשר הם בוחנים האם לצוות על החשיפה. ראו גם Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn From John, Doe*? B.C L. REV. 1373, 1375 (2009).

456 ראו לדוגמה גישות שונות לעניין זה בש״א 4995/05 **פלונית (קטינה) נ׳ בזק בינלאומי בע״מ** (נבו 28.2.2006); ה״פ (מחוזי ת״א) 1244/07 **מזמור הפקות נ׳ מעריב הוצאת מודיעין בע״מ** (נבו 20.3.2008).

457 ראו עניין **מור**, לעיל ה״ש 53.

458 ראו לדוגמה עניין **דהרי**, לעיל ה״ש 426 (חשיפת זהות שולח מסרים פרסומיים (ספאם).

459 Diem White Paper, *available at* https://bit.ly/3ONwued, *The Radical Idea Hiding Inside Facebook's Digital Currency Proposal,* MIT TECH. REV. (2019).

460 לדאגה זו בהקשר משיק ראו Fennie Wang & Primavera De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, FRONTIERS IN BLOCKCHAIN (Jan 2020).

nevo.co.il

כאמור יכולה להוביל לנזק אדיר, מאחר שהמידע יכול לשמש לגנבת זהות והונאות,[461] נזק כלכלי ונזקי חרדה.[462] איסוף מידע אישי מעלה שאלות של אבטחת מידע ופרטיות.

אכן, מידע אישי על זהות משתמשי מטבעות אלקטרוניים הוא בסיכון לפריצה למידע ושימוש לרעה בו בידי שחקנים מפירי חוק. פריצה למידע היא בעיה כבדת משקל בעידן הדיגיטלי בכללותו. אולם, הסיכון לפריצה למידע כשלעצמו אינו סיבה מספקת להימנע מאיסוף ואחסון מידע אישי באופן גורף. כדי להתמודד עם סיכון זה, ראוי כי רגולטורים יתוו כללים סטנדרטים ראויים לאבטחת מידע, נהלים לשיפור אבטחת התשתית אשר יקשו את הפריצה למידע ויגבירו את הסיכוי לזיהוי מקרים שבהם כבר אירעה פריצה, כמו גם חקיקה בנושא הודעה על פריצה למידע ותגובה לאירוע הסייבר.[463] כמו כן, יש לשפר את האכיפה והפיקוח באשר ליישום סטנדרטים אלה.[464] נוסף על זה, ראוי כי יותוו נהלים לשיפור הגנת הפרטיות ויאומצו הפרקטיקות הטובות (best practices) בנושאים אלה.

אולם, מעבר להגנת התשתית וחידוד נהלים, קיימת חשיבות מכרעת להגבלת עיצוב אשר פוגע בבטיחות המידע ויוצר סיכוני פרטיות לא סבירים.[465] שתי תכונות של עיצוב יכולות להפחית את נזקי הפריצה למידע. ראשית, הצפנת המידע האישי תאפשר דרגה גבוהה של סודיות, והיא כלי יעיל לאזרחים ועסקים להגן על עצמם מפני שימוש לרעה בטכנולוגיות כמו פריצה למידע, גנבת זהות, גנבת מידע, הונאה וגילוי המידע ללא הרשאה.[466] הצפנה היא כלי

461 Dion-Schwarz, Manheim & Johnston, לעיל ה"ש 3; Wang & De Filippi, לעיל ה"ש 460; Veliz, לעיל ה"ש 371, בעמ' 107, 110 (“[E]very day of every week hackers break into networks and steal data about people. Sometimes they use that data to commit fraud. Other times they use it for shaming, extortion or coercion”); Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. Irvine L. Rev. 107 (2019); Sara S. Greene, *Stealing Identity from the Poor*, Duke Law School Public Law& Legal Theory Series NO. 2021-17.

462 על הנזק האדיר שנגרם מפריצה למידע ראו Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737, 768 (2018).

463 חקיקה מעין זו כבר אומצה במדינות רבות. להרחבה ראו Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021, 810 Ill. L. Rev. 803, 809–812 (2020).

464 יצוין כי בישראל כבר עתה ננקטים חלק מצעדים אלה וחלקם מתוכננים בחקיקה עתידית. ראו לדוגמה תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז–2017 אשר מגדירות את רמת אבטחת המידע הנדרשת מכל גורם במשק המנהל או מעבד מידע אישי דיגיטלי על אודות אנשים וקובעות מנגנונים שנועדו לשיפור אבטחת מידע. ראו גם הצעת חוק הגנת הפרטיות (תיקון 14), התשפ"ב–2021, אשר אושרה בוועדת השרים לחקיקה בנובמבר, 2021. הצעת החוק אושרה בקריאה ראשונה במליאת הכנסת ב־24 לינואר 2022. ההצעה מתוכננת לעדכן את דיני הפרטיות לעידן הדיגיטלי כדי לאפשר לעסקים ולחברות ישראליות לפעול במרחב הגלובלי.

465 להמלצה זו ראו Daniel J. Solove, *The Myth of the Privacy Paradox*89 Geo. Wash. L. Rev. 1, 50 (2021).

466 Rocio de la Cruz, *Privacy Laws in the Blockchain Environment*, 3 Annals of Emerging Technologies in Computing (AETiC) 34, 39 (2019) (“encrypting the data by choosing an encryption option that ensures a high level of confidentiality….[T]he solution I recommend here to minimise risks of breaching the law and/or facing a data breach incident, is anonymizing the personal data to the maximum extent that still allows the Blockchain achieve its purpose”).

nevo.co.il

חשוב מאחר שהיא מגבירה את דרגת הפרטיות ומקדמת את הטכנולוגיה עבור המשתמשים מאחר שרק לשולח ולמקבל יש מפתחות פרטיים והם יכולים ולראות את התקשורת. המידע אינו נגיש לקריאה ולהבנה לכל אחד אחר.[467] כך, כמה משטרים משפטיים החולשים על פריצה למידע פוטרים מידע מוצפן מדרישות בחקיקה לספק הודעה על פריצה למידע.[468] שנית, הצפנה יכולה להיות משולבת עם שיטות של התממה (אנונימיזציה).[469] המזהה הפרטי של המשתמש יכול לעבור התממה ולהיות מזוהה רק כאשר צו בית משפט דורש לחשוף את המשתמש. יצוין כי עיצוב זה אינו מעניק הגנה אבסולוטית מפני נזקי פריצה למידע, מאחר שההאקר יכול לערוך דה־אנונימיזציה של המידע המותמם.[470] אולם, התממה מייקרת משמעותית את עלויותיו של ההאקר, מפחיתה את התועלת עבורו מפריצה למידע וכך מפחיתה את הסיכון לגנבת זהות.[471]

יצוין שמעבר להפחתת הסיכון לשימוש לרעה במידע, התממה והצפנה יקלו את ההטמעה של הרפורמה המוצעת גלובלית,[472] מאחר שנקיטת אמצעים אלה יכולה לאפשר התאמה עם החקיקה האירופית להגנת מידע, General Data Protection Regulation (GDPR).[473] התממה והצפנה של זהות משתמשי המטבעות האלקטרוניים שלהם מאפשרות לחברות המנפיקות, ספקי הארנקים ושירותי ההמרה להימנע מהפרה של הרגולציה האירופית. יצוין כי מטרת הרגולציה האירופית להגן על הזכות לפרטיות של תושבי האיחוד האירופי באשר למידע אישי

467 Snyers, לעיל ה"ש 218, בעמ' 55; Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 Wash. L Rev.101, 145–147 (2020); *A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?*, ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE GUIDE (Nov. 19, 2018), https://bit.ly/3Pbh830; Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption and the CFAA the Case of WhatsApp V. NSO Group*, 101 Berkeley Tech. L.J 101,132(2021) ("for the Financial Industry Regulatory Authority (FINRA), encryption is a 'critically important' tool in a firm's cybersecurity arsenal").

468 Verstraete & Zarsky, לעיל ה"ש 463, שם.

469 Rocio de la Cruz, לעיל ה"ש 466, בעמ' 304 מציע לשלב הצפנה עם שיטות של התממה.

470 על מגבלות ההתממה ראו Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 Ucla L. Rev. 1701 (2010).

471 Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703 (2016) מאמצים גישה מבוססת סיכון וטוענים כי התממה צריכה להתמקד בהליך של הפחתת הסיכון לזיהוי מחדש, ולא במניעה מוחלטת של נזק. על מדיניות אבטחת מידע כמבוססת סיכון ועל הצורך לאזן בין נוחות, פונקציונליות ואבטחת מידע ראו Daniel J. Solove, Woodrow Hartzog, Breached 71–75 (2022).

472 Alexandra Giannopoulou, *Putting Data Protection by Design on the Blockchain*, 7 European Data Protection L Rev. 388 (2021) ("The use of encryption techniques as central features to the design of blockchains, would make the appear in compliance with part of the data protection by design obligations, since encryption is particularly underlined in article 25(1) GDPR").

473 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119).

nevo.co.il

שנשמר על אודותיהם בגופים עסקיים וממשלתיים, אולם היא משתרעת גם על חברות שאינן אירופיות, אם הן מציעות טובין או שירותים ללקוחות באיחוד האירופי. כך, היא משפיעה על הגנת מידע ברחבי העולם. GDPR כוללת מבחן סף להעברות בין־לאומיות של מידע אישי למדינות שאינן חברות באיחוד ויכולה להביא למעשה לחסימה משפטית של העברות מידע למדינות שאינן עומדות בסטנדרט התאימות ברגולציה (“adequacy” standard).[474] ה־GDPRמציבה מגבלות על עיבוד מידע ושמירת מידע ומכוונת לשמור את האוטונומיה האישית של מושא המידע ואת כבודו.[475] ההגבלות שמציבה הרגולציה האירופית חלות על מידע אישי (“personal data”), שהוא כל מידע שקשור לאדם טבעי שהוא מזוהה או בר זיהוי.[476] אולם, אם התממה מושגת במלואה, המידע אינו מקושר לאדם מזוהה.[477] יודגש כי על שיטת ההתממה להביא לאנונימיזציה מלאה,[478] ולא להסתפק בפסיידונים.[479] אם לא מושגת התממה מלאה, החברה שאוספת מידע מוגדרת כשולטת במידע, ולפי הרגולציה האירופית נדרשת להטמיע אמצעים טכניים וארגוניים כדי להבטיח שעיבוד המידע מתבצע בהתאם לרגולציה.[480] אולם, גם אם התממה לא תהיה מלאה, החברות המנפיקות, ספקיות הארנקים ושירותי ההמרה עדיין יוכלו ליהנות מסטנדרטים מקילים תחת הרגולציה האירופית,[481] והצפנת המידע תסייע להם לעמוד בהם.[482] במקרה זה הם יצטרכו לשאת בעלויות ציות לסטנדרטים של הרגולציה האירופית כשולטים במידע על זהות משתמשי המטבעות האלקטרוניים. אולם, אם המטרה של התממה מלאה מושגת, ומושא המידע לא ניתן לזיהוי, אותן חברות לא יוכפפו לחובות נוספות של הרגולציה האירופית להגנת מידע.[483]

474 “Art 45 titled Transfers on the basis of an adequacy decision”, Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2019).

475 ראו Alexander Tsesis, *Data Subjects’ Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 594 (2019).

476 GDPR Art 4(1) “any information relating to an identified or identifiable natural person”.

477 GDPR Recital 26.

478 המידע מוגדר כמותמם אם כאשר מביאים בחשבון אמצעים שעשויים להשתמש בהם, כולל טכנולוגיה שזמינה בזמן עיבוד המידע, והתפתחויות טכנולוגיות, המידע לא יוכל להיות מקושר עם אדם טבעי. ראו GDPR Recital 46.

479 GDPR Article 4(5) מגדיר פסיידונימיזציה כעיבוד של מידע אישי באופן כזה שהמידע האישי לא יהיה מקושר עוד למושא מידע ספציפי בלי שימוש במידע נוסף, בשים לב לכך שמידע נוסף כזה נשמר בנפרד והוא כפוף לאמצעים טכניים וארגוניים להבטיח שהמידע האישי הוא לא מיוחס לאדם טבעי מזוהה, או בר זיהוי.

480 GDPR Art 5.

481 ראו לדוגמה GDPR Art.6(4)(e), אשר מתייחס לעיבוד למטרות מותאמות אחרות שיכולות להיות מורשות עבור מידע פסיידונימי.

482 GDPR Article 25(1); Giannopoulou, לעיל ה״ש 472, בעמ׳ 399. הצפנה מאפשרת הגנת מידע שתעמוד בתנאי ART 25 לחקיקה זו, אשר מתייחס להגנת מידע על ידי עיצוב, לפיו בזמן פיתוח המערכת ובזמן עיבוד המידע על השולטים במידע להטמיע אמצעים טכניים וארגוניים כדי להגן על זכויות מושאי המידע.

483 Waltraut Kotschy, *The New General Data Protection Regulation - Is there Sufficient pay-off for Taking the Trouble to Anonymize or Pseudonymize Data?* (Nov. 2016) https://bit.ly/3afrkbT

nevo.co.il

סיכום

התפתחויות טכנולוגיות מאפשרות את הרחבת הטרור הגלובלי והפשיעה הבין־לאומית ומגבירות את הסכנות שמהווים ארגוני פשע וגורמי טרור ואת קטלניות התקפותיהם.[484] טכנולוגיות חדשות מעלות שאלות חדשות ובעיות שמחוקקים ומתווי מדיניות צריכים להתייחס אליהם כדי לשמור על הביטחון הלאומי. המאמר התמקד בבעיה של מטבעות אלקטרוניים אשר מאפשרים זרימת מימון לגורמי טרור ומאפשרים הלבנת הון. ביקשנו לטעון כי על המשפט להתייחס לאתגרים העולים משימוש במטבעות אלקטרוניים ובעיקר לאיום שהם מציבים לביטחון הלאומי ואף לביטחון הפנים. מאחר שמטבעות אלקטרוניים בנויים במערכת מעמית־לעמית שמאפשרת למשתמשים לסחור במטבעות מבלי להסתמך על מוסדות פיננסיים כמתווכים, פתרונות מסורתיים כנגד מימון טרור ופשיעה, שמכוונים לעצירת זרם המימון, אינם ישימים. לפיכך, נדרשת מסגרת חדשה שתוכל להתמודד עם שימוש במטבעות אלקטרוניים למימון טרור, הלבנת הון ופשיעה כלכלית.

מאמר זה הציע להטיל חובות חדשות גלובליות שיחולו בזירה הבין־לאומית לאימות זהות משתמשים על חברות שמנפיקות מטבעות אלקטרוניים, ספקי הארנקים ושירותי ההמרה של מטבעות אלקטרוניים. על פי ההצעה, זהות המשתמשים לא תהיה זמינה לכול, אלא תוכל להיחשף רק לפי צו בית משפט כאשר יש חשש של ממש שמשתמש היה מעורב בהעברה כספית למטרות לא חוקיות של מימון טרור או הלבנת הון. דרישה של צו שיפוטי תוביל לאיזון בין שיקולים של ביטחון לאומי לבין זכויות של פרטיות וחופש ביטוי. המאמר אף התייחס למגבלות וביקורות על המסגרת המוצעת והגיב להן.

נסכם כי הרגולציה הגלובלית המוצעת מגלמת פוטנציאל רחב להתמודדות עם האתגרים שבשימוש לרעה במטבעות אלקטרוניים למימון טרור והלבנת הון ובכוחה אף להקטין סיכונים לביטחון הלאומי וביטחון הציבור. לאור השימוש הגובר במטבעות אלקטרוניים למימון לא חוקי, המשפט אינו יכול להתעלם מתופעה זו. אולם, לא יהיה זה יעיל לאסור את השימוש במטבעות אלקטרוניים לחלוטין, מאחר שהם משמשים גם לצרכים לגיטימיים ומקדמים ערכים של חדשנות, פרטיות וחופש ביטוי. הרגולציה המוצעת מאפשרת, מחד גיסא, לצמצם את הסיכונים שבשימוש לרעה במטבעות, ומאידך גיסא, מקדמת שימוש בהם למטרות לגיטימיות ויעילות. לפיכך, נסיים בקריאה למתווי מדיניות ומחוקקים לפעול לשיתוף פעולה בין־מדינתי ולהרחבת אמנות קיימות ולהביא לאימוץ הרגולציה המוצעת ברמה הגלובלית.

484 Lavi, לעיל ה״ש 54, בעמ׳ 489.

נבו nevo.co.il