



בית המשפט העליון

עה"ס 82202-07-25

עה"ס 88783-07-25

לפני: כבוד השופט עופר גרוסקופף
כבוד השופט חאלד כבוב
כבוד השופט יחיאל כשר

המערער: אלכסנדר בן ולרי בלוק

נגד

המשיבה: מדינת ישראל

ערעורים על פסק דינו של בית המשפט המחוזי בירושלים
מיום 14.7.2025 בתה"ג 700-05-25 שניתנה על ידי כבוד
השופט אוהד גורדון

תאריך ישיבה: ד' שבט תשפ"ו (22.1.2026)

בשם המערער: עו"ד שרון נהרי; עו"ד יוסי חביב

בשם המשיבה: עו"ד אבי קרוננברג

פסק-דין

השופט עופר גרוסקופף:

לפנינו ערעור על פסק דינו של בית המשפט המחוזי בירושלים (כב' השופט אוהד גורדון) בתה"ג 700-05-25 מיום 14.7.2025, בו נקבע כי המערער הינו בר-הסגרה לארצות הברית, בהתאם לסעיף 3 לחוק ההסגרה, התשי"ד-1954 (להלן: חוק ההסגרה).

הערה מנהלתית: ככל הנראה מחמת שגגה נפתחו במקרה זה שני תיקי ערעור, שיש לראות בהם, הלכה למעשה, ערעור אחד.

רקע והשתלשלות העניינים

1. ביום 10.12.2024 הגישה ממשלת ארצות הברית בקשה להסגיר לידיה את המערער, מר אלכסנדר בלוק (גורביץ'), על מנת להעמיד אותו לדין פלילי (להלן: בקשת ההסגרה). כמפורט בבקשת ההסגרה, נגד המערער הוגש ביום 16.8.2023 כתב אישום לבית המשפט הפדראלי במחוז הצפוני של קליפורניה (להלן: כתב האישום האמריקני).

למערער יוחסו האישומים הבאים: ארבעה אישומים של מרמה ופעילות נוספת בקשר למחשבים (1030(a)(5)(A), 1030(c)(4)(B)(i) U.S.C. § 18 (להלן: מרמה במחשבים)); העברת טובין גנובים (18 U.S.C. § 2314. (להלן: העברת טובין גנובים)); ושלושה אישומים של הלבנת הון (18 U.S.C. § 1956). לבקשת ההסגרה צורפו, בין היתר, תצהירו של התובע הפדרלי, עו"ד אג'אי קרישנמורת'י (להלן: תצהיר התובע) וכן תצהירו של סוכן ה-FBI מייקל הילטון (להלן: תצהיר הסוכן הפדרלי). בבקשת ההסגרה נטען כי המערער ניצל פרצה במערכת ממחושבת בשם Nomad Bridge (להלן: נומאד), שבבעלות חברת Illusory Systems, Inc. על מנת לגנוב מטבעות דיגיטליים בשווי של למעלה מ-2.8 מיליון דולרים, ולאחר מכן ביצע פעולות שונות על מנת לטשטש את מקורם. להלן יפורטו בתמצית האישומים נגד המערער; אך תחילה, רקע קצר הדרוש להבנתם.

2. מטבעות דיגיטליים הם יחידה ממוחשבת המשמשת אמצעי תשלום. המטבעות הדיגיטליים מונפקים, נסחרים ו-"מוחזקים" ברשתות בלוקצ'יין (להגדרות שונות למונח מטבעות דיגיטליים, ראו: הוועדה לבחינת אסדרה של הנפקת מטבעות קריפטוגרפיים מבוזרים לציבור דוח ביניים 8 (2018); מורן אופיר ועידו שדה "האם ב-ICOs מונפקים ניירות ערך? על אסדרה של אסימונים דיגיטליים שמנפיקות חברות" משפטים נא 437, 444-446 (2021) (להלן: אופיר ושדה)). רשת בלוקצ'יין היא מאגר מידע מבוזר, המוחזק במקביל במחשבים רבים, וכולל תיעוד מלא של כל הפעולות הקודמות (כגון, עסקאות והעברות) שנעשו באותה רשת. עדכוננו של מאגר המידע נעשה במקביל בכלל המחשבים הפועלים ברשת, והוא אינו תלוי בהחלטה של ארגון מרכזי כזה או אחר, ומכאן אופייה המבוזר של הרשת (ראו: אופיר ושדה, בעמ' 441-442; יעקב אנוך "חוזים חכמים" טכנולוגיות מתפרצות: אתגרים בדין הישראלי 279, 281-282 (ליאור זמר ואח' עורכים (2022)). עסקאות ברשת הבלוקצ'יין גלויות לכל המשתמשים ברשת – אך הצדדים לכל עסקה כזו אינם מזוהים לפי שמם, אלא בהתאם לכתובת פומבית (המורכבת מרצף ספרות ואותיות), שאליה יכולים משתמשים אחרים ברשת להעביר מטבעות דיגיטליים (כתובת זו תכונה להלן: אדנק דיגיטלי. ראו: יונתן יובל "מטבעות קריפטוגרפיים: אתגרים מושגיים, משפטיים ורגולטיביים" דין ודברים טז 447, 475-476 (2023); מבקר המדינה מיסוי מטבעות דיגיטליים 5 (2024)). בנוסף, רשתות בלוקצ'יין רבות מאפשרות להגדיר באמצעותן חוזים חכמים. חוזים חכמים הם תוכנות, אשר בהתקיים תנאים מסוימים שנקבעו מראש, מוציאות לפועל, באופן עצמאי, הסכמות חוזיות שהוטמעו בקוד המגדיר את החוזה החכם (מעין "חוזה אחיד ללא מגע יד אדם". להרחבה, ראו: Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L. J. 101, 108 (2017)

פינקלשטיין "דיני חוזים 'חכמים' – בין התקדמות טכנולוגית לרגולציה" מעשי משפט יב 349, 355 (2021) (להלן: פינקלשטיין)).

3. מכיוון שכל רשת בלוקצ'יין מהווה מאגר מידע מבוזר נפרד, לא ניתן להמיר ישירות בין מטבע דיגיטלי אחד לאחר, ועל כן, ככלל, כדי לבצע עסקה בין מטבעות דיגיטליים שונים יש צורך בשירותי גישור בין הרשתות הרלוונטיות (ראו פירוט בסעיפים 14-20 לתצהיר הסוכן הפדרלי). מערכת נומאד מספקת שירותי גישור כאלה, במתכונת המכונה "Lock-And-Mint". דרך הפעולה של המערכת היא שמשמש "נועל" מטבעות דיגיטליים ברשת בלוקצ'יין אחת, כך שלא ניתן יהיה להשתמש בהם לעסקאות אחרות. המטבעות הדיגיטליים הנעולים מוחזקים בארנק דיגיטלי בבעלות נומאד. בתמורה לנעילת המטבעות הדיגיטליים, מקבל המשתמש מטבעות דיגיטליים ברשת בלוקצ'יין אחרת, המכונים "אסימונים" (tokens), שערכם שווה למטבעות הדיגיטליים שננעלו (להלן: הטוקנים). הטוקנים ניתנים לשימוש ברשת הבלוקצ'יין האחרת וכן ניתן להחליפם בחזרה למטבעות דיגיטליים שננעלו (להרחבה באשר ליחס בין טוקנים כאלה ובין סוגים אחרים של נכסים המוחזקים ברשתות בלוקצ'יין, ראו: אופיר ושדה, בעמ' 448-446). שירותי גישור אלה ניתנו, בין היתר, באמצעות חוזים חכמים אותם יצרה נומאד (להלן: החוזים החכמים).

4. לפי בקשת ההסגרה, במהלך חודש יוני 2022 בוצע עדכון תוכנה במערכת נומאד, ובעקבותיו נוצרה פרצת אבטחה לא-מכוונת בחוזים החכמים. החוזים החכמים השתמשו בפקודה מסוימת על מנת לוודא כי המטבעות הדיגיטליים ברשת בלוקצ'יין אחת אכן "ננעלו", ואינם ניתנים לשימוש יותר, לפני שהחוזים החכמים העבירו למשתמש טוקנים שווי-ערך ברשת בלוקצ'יין אחרת (פקודה זו נקראת "proveAndProcess"). כתוצאה מהפגם בחוזים החכמים, למשתמשים הייתה אפשרות להעביר הודעה שגרמה לכך שהמערכת השתמשה בפקודה אחרת מזו המתוכננת (פקודה הנקראת "process"). להלן: פרצת האבטחה). פקודה זו אפשרה למשתמשים לקבל טוקנים ברשת בלוקצ'יין אחת, מבלי "לנעול" מטבעות דיגיטליים בשווי דומה ברשת אחרת. בבקשת ההסגרה נטען כי המערער, שפעל תחת השם "Bitliq.eth" (להלן: ביטליק), איתר את פרצת האבטחה הזו. תחילה הוא ביצע שש העברות ניסיוניות, במסגרתן הורה למערכת נומאד להנפיק עבורו טוקנים, מבלי "לנעול" תמורתם מטבעות דיגיטליים. במקביל לאותן העברות, הפקיד המערער את המטבעות הדיגיטליים בארנקה הדיגיטלי של נומאד, וזאת על מנת למנוע מפרצת האבטחה להתגלות. לאחר שראה כי טוב, בסמוך ליום 1.8.2022 ביצע המערער, באמצעות פרצת האבטחה, ארבע העברות מארנקה הדיגיטלי של נומאד ברשת

הבלוקצ'יין Ethereum לכתובת המשויכת למשתמש "ביטליק" מבלי "לנעול" תמורתם מטבעות דיגיטליים (העברות אלו יכוננו להלן: ההעברות העיקריות). בסך הכול, בהעברות אלו, הונפקו למערער טוקנים ששווים עלה על 2.8 מיליון דולרים. לאחר מכן, העביר המערער את הטוקנים שקיבל למספר ארנקים דיגיטליים והמיר אותם למטבעות דיגיטליים אחרים, וזאת, על פי הנטען, במטרה להסתיר את המקור של הטוקנים. מעשיו של המערער חשפו את פרצת האבטחה בפני משתמשים אחרים בנומאד, ואיפשרו לאותם גורמים לרוקן את ארנק דיגיטלי בבעלות נומאד, שבו היו מצויים מטבעות דיגיטליים שהיו שייכים למשתמשים אחרים בשווי של מעל 186 מיליון דולרים. מספר ימים לאחר מכן, החזיר המערער לנומאד חלק מהטוקנים שנלקחו, ופנה לבכיר בנומאד באמצעות הרשת החברתית "טלגרם" (תחת חשבון הנושא את השם "@alvagar"). המערער הציע להחזיר לנומאד את יתר הטוקנים שלקח, וזאת בתמורה לכך שיקבל תשלום על כך שהוא הביא את פרצת האבטחה לידיעתה של נומאד. הצדדים החלו לנהל משא ומתן, אך בשלב מסוים ניתק המערער את הקשר עם נומאד, והחברה פנתה לרשויות אכיפת החוק בארצות הברית. במסגרת החקירה שביצעו הרשויות זוהה המערער כבעלים של הארנק הדיגיטלי המשויך למשתמש "ביטליק".

5. ביום 2.5.2025 הגישה המשיבה (להלן: המדינה) עתירה, ובה ביקשה להכריז על המערער כבר-הסגרה. המדינה טענה כי המעשים המתוארים בבקשת ההסגרה מהווים עבירות הסגרה לפי הדין הישראלי. בפרט, נטען כי המעשים המיוחסים למערער מקימים עבירות של שיבוש או הפרעה לחומר מחשב וחדירה לחומר מחשב כדי לעבור עבירה אחרת (לפי סעיפים 2 ו-5 לחוק המחשבים, התשנ"ה-1995 (להלן: חוק המחשבים)); עבירות של קבלת דבר במרמה בנסיבות מחמירות וגניבה בנסיבות מחמירות (לפי סעיפים 415 סיפא ו-384א(ב) לחוק העונשין, התשל"ז-1977); וכן עבירות לפי סעיפים 3(א) ו-4 לחוק איסור הלבנת הון, התש"ס-2000 (להלן: חוק הלבנת הון).

6. בפני בית המשפט המחוזי העלה המערער שלל טיעונים נגד הסגרתו. המערער גם הגיש חוות דעת שכתב עו"ד עמית לוי (להלן: חוות הדעת מטעם המערער). בחוות הדעת נטען כי הפעולות המיוחסות למערער היוו שימוש חוקי בחוזים החכמים, שכן לא נטען כי הוא ביצע מניפולציה אסורה בקוד העומד מאחורי החוזים החכמים. עוד נטען כי לא ניתן לייחס למערער עבירה של הלבנת הון, שכן כל ההעברות ברשתות בלוקצ'יין הן פומביות וגלויות לכל המשתמשים ברשת, ואף לא נטען כי המערער ביצע פעולות שונות להסוואת מקורם של הטוקנים שנלקחו. כפי שיפורט להלן, לאחר דיון בעל-פה שהתקיים לפנינו, הודיע המערער כי הוא ממקד את הערעור בשניים מבין התנאים

הקבועים בחוק ההסגרה – קיומה של "אחיזה לאישום" בבקשת ההסגרה, ופליגות המעשים המיוחסים לו לפי הדין הישראלי. משכך אתמקד במסקנותיו של בית המשפט קמא ביחס לתנאים אלה.

7. בפסק הדין של בית המשפט המחוזי, מיום 14.7.2025, התקבלה העתירה, ונקבע כי המערער הוא בר-הסגרה.

תחילה, מצא בית המשפט כי התצהירים שצורפו לבקשת ההסגרה מציגים "אחיזה לאישום" ביחס לכלל העבירות המיוחסות למערער. בית המשפט ציין כי המערער לא חלק על הטענה כי הוא עומד מאחורי המשתמש "ביטליק" גם לאחר שניתנה לו הזדמנות לעשות זאת, ומכל מקום גם לעניין זיהויו כ-"ביטליק" הובאו ראיות מספיקות לשלב זה. במישור פליליות המעשים, ציין בית המשפט כי המערער לא התייחס לקיומם של איסורים מקבילים בארצות הברית ובישראל על המעשים המיוחסים לו, אלא התמקד בטענה כי מדובר בפעולות לגיטימיות, וזאת בהסתמך על חוות הדעת שהגיש. אלא שבית המשפט קבע כי לא ניתן לאמץ את מסקנותיה. ראשית, צוין כי מדובר בעורך-דין ישראלי שחיווה את דעתו באשר לפליליות מעשי המערער – סוגיה שבמשפט, שאינה עניין לחוות דעת מומחה. מכל מקום הודגש שהמסקנות בחוות הדעת מטעם המערער אינן חד-משמעיות; שהן נסמכות על תשתית עובדתית השונה מהאמור בבקשת ההסגרה; ושהן נקבעו מבלי שהובאו אסמכתאות מספקות לביסוסן.

טענות הצדדים בערעור

8. על פסק דין זה הגיש המערער ערעור, באמצעות בא הכוח שייצג אותו בבית המשפט המחוזי (עו"ד יעקוב ג'בר), ובו העלה טענות שונות נגד כלל ההיבטים של פסק הדין. ביום 11.1.2026, זמן קצר לפני המועד שהיה קבוע לדיון בערעור, נמסרה הודעה על החלפת הייצוג, אשר לוותה בבקשה לדחייה קצרה של מועד הדיון לצורך לימוד התיק. בקשה זו נענתה, והדיון בתיק התקיים לפנינו ביום 22.1.2026. בפתח הדיון הודיע בא כוחו החדש של המערער, עו"ד שרון נהרי, כי הוא ימקד את טענותיו לשני נושאים: דרישת הפליליות הכפולה והתקיימות "אחיזה לאישום" במישור הראייתי (ראו: פרוטוקול הדיון מיום 22.1.2026, עמ' 1, ש' 3-6). סוגיות אלה הועלו אומנם בנימוקי הערעור שהוגשו, ואולם טיעונו של בא הכוח החדש לגביהן היה מרחיב ומפורט משמעותית מזה שהופיע בכתובים. לפיכך, ועל מנת שלא לקפח מי מהצדדים, אפשרנו להם, לאחר תום הדיון בעל פה, להגיש השלמות טיעון בכתב בסוגיות האמורות.

9. בהשלמת הטיעון מטעמו, שהוגשה ביום 29.1.2026, טוען המערער כי בית המשפט קמא שגה כשקבע כי ההעברות העיקריות הן פליליות. לדברי המערער, בבקשת ההסגרה לא נטען, אף לא במשמע, כי המערער "שינה קוד, חדר למערכת, עקף מנגנון אבטחה או פעל מחוץ למסגרת פעולתו הרגילה והאוטונומית של החוזה החכם" (שם, בסעיף 11). הפגם בחוזים החכמים נגרם עקב שגיאה של מתכנתי מערכת נומאד, משמע, מדובר בתקלה פנימית, ולא בכשל שנובע מפעולה חיצונית שביצע המערער. שגיאה זו בהבנת התשתית העובדתית לבקשת ההסגרה, כך נטען, הקרינה על מסקנותיו המשפטיות של בית המשפט.

10. בפרט, המערער סבור כי לא מתקיימת דרישת "הפליליות הכפולה" ביחס לעבירות בניגון מבוקשת ההסגרה. אשר לעבירת המרמה במחשבים – המערער טוען כי עניינה של עבירה זו, לפי הדין האמריקני, הוא בשידור ביודעין של קוד בכוונה לגרום נזק למחשב, מבלי לדרוש גישה בלתי-מורשית או חדירה אחרת למערכת המחשב. לעומת זאת, חוק המחשבים, עליו הסתמכה המדינה לעניין זה, אינו מכיר בעבירה דומה, והעבירות הרלוונטיות בחוק הישראלי מחייבות כי הנאשם יכנס ללא הרשאה למחשב, או ישבש באופן ממשי את פעילותו. בבקשת ההסגרה, לשיטת המערער, כלל לא מיוחסים לו מעשים עליהם אוסר הדין הישראלי, שהרי אין מחלוקת כי החוזים החכמים זמינים לכל משתמש, מבלי להגביל את ההרשאה למשתמשים מסוימים, ומכיוון שהמערער לא גרם לקריסת החוזים החכמים או לפגיעה בתפקודם. למעשה, המערער מוסיף כי גם לפי פסיקה אמריקנית שפירשה את עבירת המרמה במחשבים, המעשים המיוחסים לו אינם מספיקים לצורך הרשעה בעבירה זו.

עוד טוען המערער כי אין מקבילה בדין הישראלי לעבירת העברת טובין גנובים, לא מבחינת יסודות העבירה ואף לא מבחינת הערכים המוגנים שבבסיסה. לדברי המערער, עבירת העברת הטובין הגנובים עוסקת בפעולות העברה בין מדינות שונות בארצות הברית לאחר שנגנב הרכוש, בעוד העבירות המקבילות לפי הדין הישראלי עניינן בפעולת הגניבה עצמה (עבירות גניבה בנסיבות מיוחדות וקבלת דבר במרמה בנסיבות מחמירות). המערער מוסיף כי בכתב האישום האמריקני לא הוצגו עובדות התואמות את היסודות המרכיבים עבירות אלה.

11. לבסוף טוען המערער כי אין בבקשת ההסגרה אחיזה ראייתית לאישום בהלבנת הון. זאת שכן כלל הפעולות המיוחסות לו בוצעו באמצעות רשתות בלוקצ'יין, שהנעשה בהן גלוי לכל המשתמשים ברשת, ומשכך לא ניתן לטעון כי המערער פעל להסוות או

להסתיר את מקור הטוקנים, כנדרש בעבירה של הלבנת הון לפי סעיף 3 לחוק זה. המערער מוסיף כי לא ניתן להקביל את המעשים המיוחסים לו לעבירה של עשיית פעולה ברכוש אסור, לפי סעיף 4 לחוק איסור הלבנת הון, שכן עבירה זו אינה קיימת בדין האמריקני. בהקשר זה מוסיף המערער כי בית המשפט קמא שגה כשלא ייחס משקל לחוות הדעת מטעמו, שהראתה כי המעשים שבכתב האישום האמריקני אינם מגבשים עבירה של הלבנת הון. ככל שיידחו טענותיו, מבקש המערער כי ימונה מומחה מטעם בית המשפט, על מנת להעמיד את ההכרעה בעתירה להסגרתו על תשתית מקצועית אובייקטיבית.

12. בהשלמת הטיעון מטעמה, שהוגשה ביום 5.2.2026, מדגישה המדינה כי דרישת הפליליות הכפולה מעוגנת במבחן מהותי, הבודק אם המעשים המיוחסים למבוקש מקימים עבירת הסגרה כלשהי בדין הישראלי, וזאת אף אם לא קיימת חפיפה מלאה בין רכיבי עבירה זו ובין העבירה בגינה מבוקשת ההסגרה. לשיטת המדינה, כתב האישום האמריקני עומד בדרישה זו. לשיטת המדינה, העברת פקודה שגויה ("process()") במקום ("proveAndProcess()") השפיעה על הקוד של החוזים החכמים, ומשכך עולה כדי שיבוש או הפרעה לפעילותה. מעשים אלה אף מהווים חדירה למערכת במטרה לבצע עבירה אחרת, בשים לב לפרשנות הרחבה שהוקנתה בפסיקה למונח "חדירה לחומר מחשב". העבירה האחרת, לשיטת המדינה, היא גניבה בנסיבות מחמירות, המתבטאת בנטילת הטוקנים בניגוד לכללי מערכת נומאד, וקבלת דבר במרמה בנסיבות מחמירות, המתבטאת בהצגת מצג מטעה למערכת, לפיו ניתן להנפיק לו טוקנים מבלי לוודא קודם לכן כי המערער "נעל" מטבעות דיגיטליים בשווי דומה.

המדינה סבורה כי קיימת מקבילה בדין הישראלי גם לעבירה שעניינה העברת טובין גנובים. העבירה המקבילה, לשיטתה, היא עבירת הלבנת הון (המדינה מוסיפה כי, בניגוד לטענת המערער, היא אינה מבקשת להקביל בין עבירת העברת הטובין הגנובים לעבירות הישראליות של גניבה בנסיבות מחמירות וקבלת דבר במרמה, והיא הסתמכה על עבירות אלה רק ביחס לעבירה לפי סעיף 5 לחוק המחשבים). לפי כתב האישום האמריקני, לאחר שנטל את הטוקנים (המונפקים על ידי מערכת נומאד, ולפיכך, מזוהים עימה) המיר אותם המערער לכמה סוגים של מטבעות דיגיטליים, העבירם בין חשבונות שונים (תוך חציית גבול מדינתי בארצות הברית), ופיצל אותם מספר פעמים. מעשים אלה, על פי הנטען, מעידים על ניסיון להסתיר את מקור הטוקנים ולטשטש את זהותו של המערער כנהנה מהם, כנדרש בעבירות לפי חוק הלבנת הון.

13. בתגובה להשלמת הטיעון מטעם המדינה, שהוגשה ביום 13.2.2026 על פי רשות שניתנה, טוען המערער כי המדינה מתבססת על עבירות לפי הדין הישראלי הכוללות רכיב של חדירה לאזור אסור במחשב או עקיפת מנגנון הרשאה – אך כתב האישום האמריקני אינו מייחס מעשה מסוג זה למערער. עמדת המדינה, כך נטען, מניחה כי שליחת הפקודה לחוזים החכמים ("process()") מהווה עקיפה של מנגנון ההרשאה שקבעה נומאד, אך בפועל מדובר בשימוש תקין בחוזים החכמים, שתואם את ההגדרות של מתכנתי המערכת. אשר ליתר העבירות – המערער טוען כי המדינה אינה חולקת על כך שאין עבירה מקבילה, מבחינה נורמטיבית, בדין הישראלי לעבירת העברת טובין גנובים, וכי לא ניתן לגשר על הפער באמצעות ייחוס עבירות אחרות למערער.

דיון והכרעה

14. לאחר שעיינתי בטענות הצדדים ושמעתי את טענותיהם, באתי לידי מסקנה כי דין טענות המערער להידחות. מצאתי כי דרישת "הפליליות הכפולה" מתקיימת הן ביחס לעבירת מרמה במחשבים, והן ביחס לעבירה של העברת טובין גנובים, וכי קיימת אחיזה לאישום בעבירת הלבנת הון.

15. כידוע, אחד מעקרונות היסוד בהליכי ההסגרה הוא עיקרון "הפליליות הכפולה", ולפיו ניתן להסגיר מבוקש רק בגין מעשה שהוא בר-עונשין, הן לפי דיני המדינה המבקשת והן לפי דיני המדינה המתבקשת (בענייננו – מדינת ישראל). עיגונו הפורמלי של עיקרון זה מצוי בסעיף 2(א) לחוק ההסגרה, הקובע כי "עבירת הסגרה", היא "כל עבירה שאילו נעברה בישראל דינה מאטר שנה או עונש חמור מזה" (סעיף 2(א) לחוק ההסגרה (ההדגשה נוספה)). במישור הבינלאומי, לעיקרון זה תפקיד בהבטחת ההדדיות ביחסי ההסגרה בין המדינה המבקשת והמדינה המתבקשת (ראו: ע"פ 6717/09 אוזיפה נ' היועץ המשפטי לממשלה, פסקה 25 (6.12.2010) (להלן: עניין אוזיפה); ע"פ 7742/15 פלוני נ' היועץ המשפטי לממשלה, פסקה 8 (28.8.2016) (בקשה לדיון נוסף נדחתה בדנ"פ 7108/16)). לא פחות חשוב מכך, לעיקרון הפליליות הכפולה חשיבות בהגנה על זכותו החוקתית של המבוקש לחירות, ובשמירה על עקרונותיה וערכיה של המדינה המתבקשת. עיקרון זה מבטיח כי לא יוסגר מבוקש בגין מעשה שבעיני המדינה המתבקשת אינו נתפס כראוי לענישה משמעותית (ש"ז פלר דיני הסגרה 176 (1980); עה"ס 8013/21 היועץ המשפטי לממשלה נ' כהן, פסקה 26 (27.4.2022) (בקשה לדיון נוסף נדחתה בדנ"פ 3009/22)). להרחבה באשר לאיזון בין שתי תכליות אלה בדיני ההסגרה, ראו: ע"פ 2612/23 גבר נ' מדינת ישראל, פסקאות 19-21 (11.11.2024).

מנגד, דרישת הפליליות הכפולה אינה מחייבת חפיפה מלאה בין כל רכיבי העבירות המקבילות בשתי המדינות. אין כל פסול בכך שמערכות משפט מגדירות באופן שונה עבירות פליליות דומות, והעובדה כי ישנם הבדלים מסוימים בין הגדרת העבירה במדינה המתבקשת להגדרתה במדינה המבקשת אינה פוגמת בתכליות עיקרון הפליליות הכפולה שתוארו לעיל. לפיכך, נפסק כי אין לפרש את דרישת הפליליות הכפולה באופן צר ודוקני, וכי על ההשוואה בין העבירות השונות להיעשות "באופן גמיש וליברלי" (ע"פ 459/12 אמארה נ' מדינת ישראל, פסקה 32 (13.3.2013). כן ראו: ע"פ 205/73 רוס נ' מדינת ישראל, פ"ד כז(2) 365, 373 (1973); עה"ס 6974/20 לייפר נ' היועץ המשפטי לממשלה, פסקה 13 (15.12.2020)).

16. עבירת מרמה במחשבים: עיקר טענות המערער כוונו כלפי קיומה של מקבילת ישראלית לעבירה זו. למען הנוחות, אציג את העבירות עליהן נסמכת המדינה בחוק המחשבים, בליווי ההגדרות הרלוונטיות:

הגדרות

1. בחוק זה –

"חומר מחשב" – תוכנה או מידע;

"מידע" – נתונים, סימנים, מושגים או הוראות, למעט תוכנה, המובעים בשפה קריאת מחשב, והמאוחסנים במחשב או באמצעי אחסון אחר [...]

"תוכנה" – קבוצת הוראות המובעות בשפה קריאת מחשב, המסוגלת לגרום לתיפקוד של מחשב או לביצוע פעולה על ידי מחשב [...] או שהיא טבועה או אחודה עם המחשב באופן כלשהו או שהיא נפרדת ממנו [...]

שיבוש או הפרעה למחשב או לחומר מחשב

2. העושה שלא כדין אחת מאלה, דינו – מאסר שלוש שנים: [...]

(2) מוחק חומר מחשב, גורם לשינוי בו, משבשו בכל דרך אחרת או מפריע לשימוש בו.

חדירה לחומר מחשב שלא כדין

4. החודר שלא כדין לחומר מחשב הנמצא במחשב, דינו – מאסר שלוש שנים; לענין זה, "חדירה לחומר מחשב" – חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר, התשל"ט-1979.

חדירה לחומר מחשב כדי לעבור עבירה אחרת

5. העושה מעשה האסור לפי סעיף 4 כדי לעבור עבירה על פי כל דין, למעט על פי חוק זה, דינו – מאסר חמש שנים.

17. המערער טוען כי המעשים המיוחסים לו אינם מהווים עבירה לפי חוק המחשבים מכיוון שהפעולות שעשה נעשו "בהתאם ללוגיקה הפנימית של החוזה החכם", ולא כלל כניסה ללא הרשאה או השבתה של מערכת נומאד. סבורני כי טענה זו שגויה. ההסבר לכך עובר הן במישור המשפטי, והן במישור הטכנולוגי-מעשי.

18. תחילה – למישור המשפטי. בבית משפט זה טרם נערך דיון מקיף באשר לפרשנות עבירת השיבוש או ההפרעה לחומר מחשב, אך בעניין רע"פ 8464/14 מדינת ישראל נ' עזרא (15.12.2015) (להלן: עניין עזרא) נדונה בהרחבה פרשנותה של העבירה הנוספת אליה מבקשת המדינה להקביל את המעשים המיוחסים למערער – חדירה לחומר מחשב כדי לעבור עבירה אחרת. בפסק הדין הבהיר המשנה לנשיאה אליקים רובינשטיין כי יש לפרש בהרחבה את שני הרכיבים המגדירים את תחולת העבירה – "חדירה לחומר מחשב" שנעשית "שלא כדין" – וזאת בכדי למנוע מקרים שבהם שינויים טכנולוגיים ישללו את תחולת העבירה אף שהערכים המוגנים על ידה עדיין נפגעים:

דומני שיש לקבל את הדעה הרווחת בקרב המלומדים, לפיה יש לפרש את המונח "חדירה" פרשנות מרחיבה. פרשנות נאמנה לתכלית החוק, ובמיוחד במבט צופה פני עתיד, מחייבת הגדרה כללית ל"חדירה", כך שכל מידע "הנכנס" למחשב – בין שנוצר על-ידי מחשב אחר ובין שנוצר כתוצאה מפעילות המשתמש במחשב – מקים את הדרישה ההתנהגותית בעבירה. דומה שהדבר תואם גם את השכל הישר, המבקש לטעמי לצמצם "דרכי מילוט". אם נעניק למונח "חדירה" פרשנות הקשורה לטכנולוגיה ספציפית שהנמצאת היום לנגד עינינו, ניאלץ להשתתף בעל כורחנו במשחק מתמיד של "חתול ועכבר", וכידוע הטכנולוגיה דהאידינא בטבעה מהירה עשרות מונים מן החוק. באשר לפרשנות המונח "שלא כדין" דומה, כי הפרשנות הראויה למונח היא שימוש במחשב בהיעדר הסכמת בעליו.

(שם, בפסקה י"ח. כן ראו: דנ"פ 1062/21 אור"ן מדינת ישראל, פסקה 30 לפסק דינה של הנשיאה אסתר חיות (11.1.2022))

מטעמים דומים, ומבלי לקבוע מסמרות, דומני כי ראוי להימנע מקביעת מגבלות קשיחות על טיב ההתנהגות המקימה את עבירת השיבוש או ההפרעה לחומר מחשב. כפי

ששינויים טכנולוגיים עשויים לשנות את הצורות בהן עבריינים מבקשים לחדור שלא כדין למחשבים, הם עשויים גם לשנות את האמצעים בהם משתמשים עבריינים על מנת לשבש או להפריע לפעולת מחשבים (ראו והשוו: ניבה אלקין-קורן, "כיצד המשפט מעצב את סביבת המידע ברשת" טכנולוגיות של צדק: משפט, מדע וחברה 223, 259 (שי לביא עורך 2003)).

19. עמדת המערער מוטעית גם במישור הטכנולוגי-מעשי. המערער מבקש למתוח קו גבול ברור בין מעשים המנצלים את ההרשאות הקיימות במערכת מחשב בכדי להשיג תוצאות אותן לא צפו מתכנתי המערכת, ובין מעשים המשיגים תוצאות מסוג זה תוך חדירה או שיבוש, ללא הרשאה, של אותה מערכת. אלא, שלמעשה, אין בנמצא קו גבול כזה. פרצות האבטחה נגדן נועד חוק המחשבים להגן הן, ככלל, מצבים שבהם נפלה טעות באופן בו הוגדרה מערכת מחשב בידי מתכנתיה, כך שפורץ חיצוני יכול לנצל את ההגדרות השגויות על מנת להשיג תוצאה בלתי-רצויה. מצב בו פרצת אבטחה בתוכנה נגרמה בשל שגיאה של בעלי התוכנה אינו חריג. למעשה – זהו מצב הדברים הרגיל (Derek E. Bambauer, *Ghost in the Network*, 162 U. PENN. L. REV. 1011, 1019-1025 (2014); Ian Williams, *The Secrets We Keep...: Encryption and the Struggle for Software Vulnerability Disclosure Reform*, 25 MICH. TECH. L. REV. 105, 105-106 (2018); 6 U.S.C. § 650(25); 105, 105-106 (2018)). לשם המחשה, קשה להניח כי לא נעברה עבירה לפי חוק המחשבים במצב שבו אדם מגלה כי עקב פגם באופן ייצורם של מכשירי כספומט ניתן להוציא מהם שטרות ללא הכנסת כרטיס אשראי (נניח, באמצעות הכנסת דף נייר למכשיר, במקום כרטיס אשראי). אכן, במצב כזה העבירה התאפשרה עקב שגיאה גסה של יצרן הכספומט, אך הדבר אינו גורע מהאופי הפלילי של ניצול הפרצה.

בעניין נדרא נדחתה במפורש האפשרות להגביל את עבירת החדירה למחשב רק למי שעקף מכשול טכנולוגי: "איני רואה סיבה מדוע יגן החוק על ראובן, שסיסמה נדרשת לשם שימוש במחשבו, אך לא על שמעון אשר לא השכיל להתקין במחשבו הגנה מסוג זה. בית ללא מנעול אינו הפקר – וכך הדין גם במחשב" (שם, בפסקה י"ח. כן ראו: שם, בפסקאות 2-4 לחוות דעתו של השופט מני מזוז ובפסקה 1 לחוות דעתו של השופט חנון מלצר). ברי כי אין להיענות להצעת המערער להגביל עוד יותר את העבירות לפי חוק המחשבים רק לסוג מסוים של עקיפת מכשולים טכנולוגיים – עקיפת מכשולים שמקורם אינו באופן בו הוגדר המחשב או חומר המחשב בידי בעליו. אף אין לקבל את הטענה העקרונית של המערער, ולפיה בשל אופיים האוטונומי של חוזים חכמים, אין כל פסול בניצול מודע של שגיאות באופן בו מומשו (ראו, לדוגמה, סעיפים 14-15 להשלמת הטיעון מטעמו).

הגדרת תוכנה כ- "חוזה חכם" אינה שוללת ממנה את ההגנות המשפטיות שהעניק המחוקק לתוכנות, וניצול פרצות אבטחה בה אינו שונה מניצול פרצות אבטחה בתוכנות אחרות (להרחבה באשר למדיניות המשפטית ביחס לפגמים בחוזים חכמים, ראו: דלית קן-דרור פלדמן ואור דונקלמן "טכנולוגיית הבלוקצ'יין – לא מה שחשבתם: שיקולים טכנולוגיים ומשפטיים" דין ודברים טז 511, 534-535 (2023); פינקלשטיין, בעמ' 362-360).

20. ומהתם להכא. לפי בקשת ההסגרה, המערער ניצל פרצת אבטחה במערכת נומאד, שאיפשרה לו לעקוף את מנגנון "הנעילה" החיוני לפעולת החוזים החכמים. באמצעות העברת הפקודה "process()" לחוזים החכמים, במקום הפקודה המתוכננת, "proveAndProcess()", קיבל המערער את התמורה שהציעו החוזים החכמים למשתמשים (טוקנים בשווי של למעלה מ-2.8 מיליון דולרים), מבלי שביצע כלל את חלקו בעסקה ("נעילת" מטבעות דיגיטליים שווי ערך). מעשיו של המערער חשפו את פרצת האבטחה בפני משתמשים אחרים במערכת נומאד, שניצלו אותה גם הם, ורוקנו את הארנק הדיגיטלי של נומאד ממטבעות דיגיטליים בשווי של כ-186 מיליון דולרים. לפי המיוחס לו, אם כן, המערער ניצל במודע פרצת אבטחה על מנת לקבל גישה בלתי-מוגבלת לחומר מחשב (ארנקה הדיגיטלי של נומאד), ולגנוב באמצעות גישה זו טוקנים בשווי גבוה, באופן שפגע בתפקוד התקין של מערכת נומאד (עד כדי ריקון ארנק דיגיטלי שבו נצברו סכומי כסף גדולים). הדבר נעשה ללא הסכמת מפעילי מערכת נומאד, ומכתב האישום האמריקני עולה כי המערער הבין זאת היטב. ולראיה, לאחר שביצע את ההעברות העיקריות פנה המערער לבכיר בנומאד וביקש תשלום בתמורה לכך שגילה "באג" בעיצוב החוזים החכמים – קרי, שגיאה בהגדרתם, בניגוד לכוונת מתכנתי מערכת נומאד (סעיף 51 לתצהיר הסוכן הפדרלי. כן ראו: פסקה 45 לפסק הדין קמא).

הערה: לצד עבירת שיבוש או הפרעה לחומר מחשב, מסתמכת המדינה על עבירת חדירה לחומר מחשב לצורך ביצוע עבירה אחרת (לפי סעיף 5 לחוק המחשבים), כאשר העבירה האחרת היא קבלת דבר במרמה בנסיבות מחמירות או גניבה בנסיבות מיוחדות (ראו: סעיף 17 להשלמת הטיעון מטעם המדינה). לעניין יסודות ה"קבלת דבר" או "הגניבה" שבעבירה האחרת, אציין כי די באמור בכתב האישום האמריקני, על מנת לייחס למערער ניסיון לשלול את הטוקנים שלילת קבע. זאת שכן לפי כתב האישום האמריקני ותצהיר הסוכן הפדרלי, המערער אומנם ניהל משא ומתן על החזרת הטוקנים בתמורה לתשלום, אך נמלך בדעתו וניתק את הקשר בינו ובין נציגי נומאד – אינדיקציה לכך שהחליט, לבסוף, לשמור את הטוקנים בידיו (סעיפים 51-54 לתצהיר הסוכן הפדרלי).

ראו והשוו: רע"פ 11066/03 מדינת ישראל נ' רום, פסקה ד' (28.5.2007); יעקב קדמי על הדין בפלילים חלק שני – על הפגיעות ברכוש 804-805 (2013).

21. אכן, קיימים הבדלים כאלה ואחרים בין העבירה האמריקנית של מרמה במחשבים, ובין העבירות לפי חוק המחשבים הישראלי, אך היסודות המהותיים של העבירות מקבילים זו לזו; הן נועדו להגן על אינטרסים זהים; והמעשים המיוחסים למערער מקיימים – באופן מובהק – את העבירות לפי החוק הישראלי. מטעמים דומים גם אין יסוד לטענת המערער לפיה בית המשפט קמא התעלם מכך שלא מיוחס לו מעשה אקטיבי של חדירה לחוזה החכם או שינוי הקוד שלו. אשר לטענת המערער כי לפי הפסיקה בארצות הברית מעשיו אינם באים בגדר עבירת מרמה במחשבים – טיעונו במישור זה ייבחנו במסגרת ההליך הפלילי בארצות הברית, וההליך דנן אינו המקום להידרש אליהם (ע"פ 9026/11 שוחט נ' היועץ המשפטי לממשלה, פסקה 29 (6.12.2012); ע"פ 6003/19 גרינס נ' היועץ המשפטי לממשלה, פסקה 18 (3.9.2020)).

22. עבירות הלבנת ההון והעברת הטובין הגנובים: באשר לעבירות אלו טוען המערער, ראשית, כי עבירת הלבנת ההון המיוחסת לו נעדרת אחיזה בחומר הראיות; ושנית, כי המדינה לא הציגה מקבילה ישראלית לעבירת העברת הטובין הגנובים, ומשכך לא מתקיימת בעניינה דרישת הפליליות הכפולה. אף בטענות אלה לא מצאתי ממש.

23. סעיף 9(א) לחוק ההסגרה קובע כי בית משפט יכריז על מבוקש כבד-הסגרה רק אם מצא כי "יש ראיות שהיו מספיקות כדי להעמידו לדין על עבירה כזאת בישראל". סעיף זה פורש בצמצום, ונקבע כי די בכך שקיימות ראיות, שאינן חסרות ערך על פניהן, המספיקות על מנת להמשיך לנהל, במדינה המבקשת, את ההליך הפלילי נגד המבוקש (ראו: ע"פ 2490/18 ג'ורנו נ' מדינת ישראל, פסקה 13 (8.1.2019); ע"פ 4416/20 פלוני נ' היועץ המשפטי לממשלה, פסקה 10 (8.12.2020)). במסגרת בירור זה אין לערוך בחינה מעמיקה של משקל הראיות שהוצגו ומהימנותן ואין צורך לקבוע כי הראיות שהוצגו מספיקות על מנת להביא להרשעת המבוקש (ע"פ 8304/17 למפל נ' היועץ המשפטי לממשלה, פסקה 22 (8.5.2018); ע"פ 2542/19 טוויל נ' היועץ המשפטי לממשלה, פסקה 9 (3.12.2019)).

24. התשתית הראייתית שהוצגה בתצהירי התובע והסוכן הפדרלי עומדת בתנאי זה. לפי הנטען בתצהירים, המערער המיר את הטוקנים אותם נטל מהארנק הדיגיטלי של נומאד למטבעות דיגיטליים מסוגים אחרים, ולאחר מכן שב והמיר חלק מהמטבעות

הדיגיטליים מחדש אל סוג הטוקנים שאותם נטל מנומאד מלכתחילה. בהמשך הוא אף פיצל את הטוקנים למספר חשבונות שונים. לפי התצהירים, פעולות אלה – שלחלקן אין תכלית כלכלית – הן טכניקות להלבנת הון, שמטרתן להסוות את מקורם של המטבעות הדיגיטליים (סעיפים 41-50 לתצהיר הסוכן הפדרלי וסעיף 28 תצהיר התובע). המערער טוען, בהסתמך על חוות הדעת שהגיש, כי המעשים המיוחסים לו אינם מקימים חשש להלבנת הון, מכיוון שכל ההעברות ברשתות בלוקצ'יין הן גלויות לכל, ומכיוון שלא נעשה במסגרת ההעברות המדוברות שימוש בטכניקות שונות לטשטוש מקורם של המטבעות הדיגיטליים. הטענה העקרונית של המערער לפיה לא ניתן להשתמש ברשתות בלוקצ'יין על מנת להלבין הון היא מפתיעה – שהרי היא מנוגדת לעמדתם של רגולטורים פיננסיים בישראל ובעולם, שמצאו כי פלטפורמות אלה דווקא מגדילות את הסיכון להלבנת הון (הודעה לציבור בדבר סיכונים אפשריים הטמונים במטבעות וירטואליים מבוזרים (הודעה משותפת לבנק ישראל, אגף שוק ההון, ביטוח וחיסכון, רשות המיסים, רשות ניירות ערך והרשות לאיסור הלבנת הון ומימון טרור, 2014); הדר ז'בוטינסקי ומיכל לביא "חשיפת זהות משתמשי מטבעות אלקטרוניים" מחקרי רגולציה ח 147, 188-184 (2025)). הטעם לכך הוא שאמנם פרטי הארנקים הדיגיטליים ברשתות בלוקצ'יין גלויים, אך זהויות המחזיקים בארנקים אלה מוסתרות, ורשתות בלוקצ'יין מקשות על חשיפתן. טענתו הפרטנית של המערער, לפיה לא נטען כי הוא השתמש בטכניקות המיועדות לטשטוש את מקור ההעברות, סותרת את טענתו הקודמת, לפיה ככלל לא ניתן להשתמש ברשתות בלוקצ'יין על מנת להלבין הון, וממילא, היא אינה מועילה לו. אין כל נפקות לעובדה שלפי בקשת ההסגרה, המערער השתמש רק בחלק מהשיטות להלבנת הון, ולא השתמש בשיטות אחרות. בכדי לקבוע שקיימת אחיזה לאישום, די בכך שבתצהירי התובע והסוכן הפדרלי הוצגו פעולות שעשה המערער ברכוש, ותכליתן "להסתיר או להסוות את מקורו" (סעיף 3(א) לחוק הלבנת הון. ראו והשוו: חוות דעתי בעה"ס 3463/24 מלכה נ' היועצת המשפטית לממשלה (6.3.2025) ועה"ס 1204-12-24 פאן נ' מדינת ישראל, פסקאות 50-53 לפסק דינו של השופט יוסף אלרון (29.6.2025) (בקשה לדיון נוסף נדחתה בדנ"פ 31931-07-25) (להלן: עניין פאן)).

25. טענתו האחרונה של המערער היא כי דרישת הפליליות הכפולה אינה מתקיימת ביחס לעבירה השלישית בכתב האישום האמריקני – העברת טובין גנובים. זאת שכן לא קיימת בדין הישראלי עבירה הכוללת רכיבים דומים, ובפרט רכיב של העברה בין מדינות בארצות הברית. כפי שמדגישה המדינה, המעשים המגבשים עבירה זו, לפי כתב האישום האמריקני, הם אותם המעשים בגינם מיוחסת לו עבירת הלבנת הון (לפי הדין האמריקני). משכך, סבורני כי דרישת הפליליות הכפולה מתקיימת גם ביחס לעבירה זו. המעשים

בגינם מיוחס למערער אישום של העברת טובין גנובים נופלים במובהק לגדרי עבירת הלבנת ההון (לפי הדין הישראלי), כפי שתואר לעיל. יתרה מזאת, קיים דמיון בין הערכים המוגנים על ידי העבירות. בשני המקרים נועדו העבירות למנוע ניצול של המערכת הכלכלית הלגיטימית לצרכים עברייניים, ולהפחית את התמריץ לפשיעה כלכלית באמצעות שלילת היכולת של עבריינים ליהנות או לסחור בפירות מעשיהם (ראו, בהתאמה: ע"פ 2333/07 תענך נ' מדינת ישראל, פסקה 233 (12.7.2010); עניין פאן, בפסקה 48 לפסק דינו של השופט אלרון. והשוו: *United States v. Sheridan*, 329 U.S. 379, 385 (1946); *Moskal v. United States*, 498 U.S. 103, 111 (1990); ביחס לחלופה אחרת של 18 U.S.C. § 2314).

אכן, בעבירה של העברת טובין גנובים קיים רכיב נוסף, שעניינו בהעברה בין מדינות בארצות הברית, אך לא מדובר באחד מהרכיבים המהותיים של העבירה (המצוי במוקד הבחינה במסגרת דרישת הפליליות הכפולה (ראו פסקה 15 לעיל)), אלא ברכיב שנועד להקנות לממשל הפדרלי סמכות שיפוט (ראו: *Luna Torres v. Lynch*, 578 U.S. 452, 456-457 (2016)). מכל מקום, אמנת ההסגרה בין ארצות הברית לישראל קובעת במפורש כי קיומם של רכיבים הנוגעים לסמכות שיפוט פדרלית בהגדרת העבירה האמריקנית (ובהם "הובלה בין מדינות") לא יהוו שיקול לעניין דרישת הפליליות הכפולה (סעיף 2(3) לאמנה, כנוסחו לפי הפרוטוקול המתקן לאמנת ההסגרה בין ממשלת מדינת ישראל לבין ממשלת ארצות הברית, כ"א 56(1511) 1, 3 (נחתמה ב-2005). כן ראו: עניין אוזיפה, בפסקה 58).

26. טו דבר: מהטעמים האמורים לעיל, דין טענותיו של המערער נגד פסק דינו של בית המשפט המחוזי להידחות. משכך, וכאמור בפסק הדין של בית המשפט המחוזי, נתמלאו התנאים להכרזה על המערער כבר-הסגרה לארצות הברית ביחס לעבירות שיוחסו לו בבקשת ההסגרה.



עופר גרוסקופף
שופט

השופט חאלד כבוב:

אני מסכים.



חאלד כבוב
שופט

השופט יחיאל כשר:

אני מסכים.



יחיאל כשר
שופט

הוחלט כאמור בפסק דינו של השופט עופר גרוסקופף.

ניתן היום, י"ט באדר התשפ"ו (8.3.2026).



יחיאל כשר
שופט



חאלד כבוב
שופט



עופר גרוסקופף
שופט