

פרק ג

התפישה הטריטוריאלית באשר לאיסוף ראיות בחקירה פלילית במרחב הסייבר

א. הקדמה

בפרק זה אבקש לעמוד על תפישה יסודית של המשפט בכלל ושל המשפט באשר למרחב הסייבר בפרט, ולפיה משפט המדינה הוא, ככלל, טריטוריאלי, וכל פעולה של הריבון מחוץ לטריטוריה מהווה חריג המאיים על ריבונותה של המדינה שבשטחה מבוצעת אותה פעולה. תפישה זו קנתה לה אחיזה במרחב הפיזי והועתקה גם אל המרחב הקיברנטי. העתקה זו ניצבת בבסיס קשיים רבים של המדינה באכיפת חוק פלילית במרחב הסייבר. בפרק זה אבקש לעמוד על טיבה של התפישה הטריטוריאלית בחקירה הפלילית, תחילה במרחב הפיזי ולאחריה במרחב הסייבר. אראה כיצד תפישה זו "מסנדלת" את רשויות החקירה בבואן לחקור עברות פליליות במרחב הסייבר, כיוון שאלה מטבען כוללות ראיות האגורות במחשבים במקומות שונים בעולם. כן אראה כיצד מדינות שונות ביצעו מהלכים הסכמיים ועצמאיים בניסיון להתמודד עם התפישה הטריטוריאלית. לבסוף אציג ביקורות מכיוונים תאורטיים שונים על התפישה הטריטוריאלית באשר לחקירה הפלילית במרחב הסייבר.

ב. התפישה הטריטוריאלית באשר לסמכות המדינה לאסוף ראיות במרחב הפיזי

כאמור, בשלב הראשוני של הדיון לא אתמקד בזירה המקוונת כי אם במרחב הפיזי בלבד. תמצית הטיעון בתת-פרק זה היא כדלקמן: עקרון היסוד בדבר סמכותה של המדינה הוא כי הסמכות, בהקשרים משפטיים, תחומה לטריטוריה של המדינה. עם זאת סמכויות התחיקה והשיפוט של המדינה פרצו את הגבולות הטריטוריאליים בהקשרים שונים, ולעומתן סמכות האכיפה נותרה באופן קפדני במסגרת טריטוריאלית. כפי שאטען בהמשך הפרק, פער זה שנפתח בין סמכות האכיפה לבין סמכויות התחיקה והשיפוט מעורר קשיים ניכרים ביותר בזירה המקוונת ומאיים על יכולות המדינה לאכוף באפקטיביות את הדין הפלילי ברשת. כאשר בוחנים את סמכותה המשפטית הפלילית של המדינה, מקובל להבחין בין שלושה: (א) Jurisdiction to prescribe – סמכות תחיקה: החלת הדין המהותי המדינתי על המקרה הנדון; (ב) Jurisdiction to adjudicate – סמכות שיפוט: סמכות לבית המשפט המדינתי לשיפוט את המקרה הנדון; (ג) Jurisdiction to enforce – סמכות אכיפה: סמכות לסוכניה של המדינה לאכוף

בפועל מקרה מסוים המקים סמכות שיפוט.¹ ייאמר מיד כי במוקד דיונו סמכות האכיפה הבין-לאומית, כיוון שהיא הנוגעת במישרין לאיסוף הראיות במסגרת חקירה פלילית. עם זאת תובנות מסוימות בנוגע לסמכות התחיקה והשיפוט מקרינות על הדיון בסמכות האכיפה, ולכן ארחיב במידת מה על שלוש הסמכויות בהקשר של משפט פלילי.

סמכות תחיקה בין-לאומית בהקשר של משפט פלילי: סמכות זו נוגעת לתחולת החוק הפלילי המדינתי על עברה מסוימת מבחינת מקום ביצועה. העיקרון היסודי הוא כי הנורמה הפלילית מוגבלת לתחום הטריטוריאלי של המדינה.² יש להבחין בין טריטוריאליות אובייקטיבית לסובייקטיבית. הטריטוריאליות הסובייקטיבית משמעה תחולה על כל הפרטים בטריטוריה הנתונה. הטריטוריאליות האובייקטיבית משמעה תחולה על כל המעשים המתבצעים בחלקם לפחות בשטח של הריבון, גם אם המבצע מצוי מחוץ לשטחו של הריבון.³ ניתן לראות בעיקרון הטריטוריאלי המצטבר – הן האובייקטיבית והן הסובייקטיבית – משום נקודת מוצא שממנה הורחבה תחולת דיני העונשין גם אל עברות מחוץ לטריטוריה של המדינה, בניסבות ובתנאים מסוימים. ההרחבה היא בשני ממדים: בממד של מתיחת העיקרון הטריטוריאלי עצמו ובמדד של פיתוח עקרונות שאינם טריטוריאליים.

בכל הנוגע לממד הראשון, של מתיחת העיקרון הטריטוריאלי עצמו, מוכרת הקביעה במשפט האמריקני למשל כי גם תכנון מעשה עברה שנועד להתבצע בשטח המדינה אך לא יצא לבסוף אל הפועל, כאשר התכנון עצמו היה מחוץ לשטח המדינה – ייחשב לכזה הנחלש על ידי משפט של המדינה.⁴ גם במשפט הישראלי חוק העונשין מחיל את ההרחבה האמורה. החוק

1 ראו RESTATEMENT OF THE LAW (3rd) OF FOREIGN RELATIONS LAW OF THE UNITED STATES (2009). בגרסתו הקודמת של ה-*Restatement* הופיעו רק שתי קטיגוריות: *Jurisdiction to Prescribe* או *Jurisdiction to Enforce*, או סמכות מהותית וסמכות אכיפתית-פרוצדורלית. כן ראו International Bar Association, Report of the Task Force on Extraterritorial Jurisdiction 7–8 (2009), available at Roger O'keefe, *Universal*, www.ibanet.org. להבחנה בין סמכות מהותית לסמכות אכיפתית, ראו Susan W. Brenner & Bert-Jaap Koops, *Cybercrime Jurisdiction – An Introduction*, in CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY 1–7 (Bert-Jaap Koops & Susan W. Brenner eds., 2008) עור: Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1 (2004).

2 ראו למשל Joseph H. Beale, *The Jurisdiction of a*; United States v. Bowman, 260 U.S. 94 (1922); State, 36 HARV. L. REV. 241, 245 (1923); MICHAEL AKEHURST, MODERN INTRODUCTION TO INTERNATIONAL LAW 110–111 (7th ed., 1997); ש"ז פלר "בחנינות אחדות של עקרון החוקיות בפלילים" משפטים א 19, 32 (1968); יורם דינשטיין "סמכות השיפוט הפלילית: גבולות והגבלות" עיוני משפט א 303, 306 (1971); בג"ץ 279/51 אמסטרדם נ' שר האוצר, פ"ד ו 945, 971 (1952); ע"פ 7230/96 פלוני נ' מדינת ישראל, פ"ד נא(3) 513, 513 (1997); רע"פ 1178/97 כהנא נ' מדינת ישראל, פ"ד נא(3) 266, 269 (1997).

3 ראו Rivard v. United States, 375 F.2d 882, 886 (5th Cir., 1967). וראו גם את סעיפים 7(א) ו-12 לחוק העונשין, התשל"ז-1977 (להלן – חוק העונשין), הקובעים כי "עבירת פנים" נחשבת גם לעבירה שמקצתה בלבד נעברה בישראל.

4 ראו Christopher L. Blakesley, *United States Jurisdiction over Extraterritorial Crime*, J. CRIM. L. & CRIMINOLOGY 1109, 1112 (1982); United States v. Ricardo, 619 F.2d 1124, 1128 (5th Cir.,

מגדיר כי די בתכנונה של העברה הנדונה להיעבר בישראל על מנת שדיני העונשין הישראליים יחולו עליה.⁵ הרחבה נוספת של העיקרון הטריטוריאלי כוללת קביעה כי גם מעשה שבוצע כל כולו פיזית בחו"ל, אך משפיע בפועל על הטריטוריה המדינתית או על תושבים בטריטוריה זו, ייחשב מעשה שהדין המדינתי חל עליו (לדוגמה, קרטל בין חברות זרות שנועד להשפיע על השוק המקומי בענף מסוים).⁶

בכל הנוגע לממד השני, של פיתוח עקרונות אקסטרה-טריטוריאליים לסמכות תחיקה, דיני העונשין הישראליים חלים על עברות שנעברו כולן מחוץ לשטחי ישראל, כשהדגש הוא על שתי חלופות: תחולת עברות-חוץ מטעמים לאומיים (עברות נגד המדינה, ביטחונה וכלכלתה או נגד העם היהודי ואזרחי ישראל באשר הם כאלה, עברות מסוימות נוספות נגד תושבי ישראל שנעברו בחו"ל ועברות מסוימות שביצעו תושבים ישראליים בחו"ל)⁷ ותחולה אוניברסלית על עברות (כגון פשעי השמדת עם).⁸ גם המשפט האמריקני הכיר בפריצת גבולות הטריטוריה בכל הנוגע

United States v. Mann, 615 F. 2d 668, 671 (5th Cir., 1980); United States v. Yousef, 327 F.3d 56, 91 (2nd Cir., 2003).

ראו סעיפים 7 (א) ו-12 לחוק העונשין.

United States v. Aluminum Co. of America, 148 F.2d 416 (2nd Cir., 1945); Rio Tinto Zinc Corp. v. Westinghouse Electric Corp., [1978] 1 All E.R. 434 (HL) (Eng.) כ-*The "Effects" Doctrine*, ראו למשל: Vaughan Lowe & Christopher Staker, *Jurisdiction, in* INTERNATIONAL LAW 313, 322–323 (Malcolm D. Evans ed., 3rd ed. 2010). על מיתון ההרחבה מטעמי כיבוד הריבונות של מדינות זרות אחרות שבהן התרחש המעשה מבחינה פיזית, ראו MALCOLM N. SHAW, INTERNATIONAL LAW 688–692 (6th ed., 2008).

ראו סעיפים 13–15 לחוק העונשין. עוד בקטגוריה זו גם החובה, שעונש בצד הפרתה, של תושבי ישראל לשלם מס הכנסה בישראל גם על הכנסותיו שנצמחו מחוץ לישראל (כקבוע בסעיף 2 לפקודת מס הכנסה [נוסח חדש], התשכ"א–1961), בכפוף לסייגים ולאמנות בדבר מניעת כפל מס. לביקורת על הרחבת התחולה של חוק העונשין לעברות חוץ, בדגש על תחולה לאומית של החוק מחוץ לטריטוריה, ראו יורם שחר "בגנות התחולה הנציגונית של דיני העונשין" פלילים ה' 5 (1996). לעמדה המצדיקה את ההרחבה האמורה, ראו ש"ז פלר ומרדכי קרמניצר "תגובה לחיבור 'בגנות התחולה הנציגונית של דיני העונשין' מפרי עטו של יורם שחר" פלילים ה' 65 (1996). כדוגמה ליישום הרחבת התחולה של עברות החוץ על עברות של גנבת רכבים מישראל לשטחי יהודה ושומרון, על בסיס התחולה של חוק העונשין על עברות-חוץ נגד כלכלתה של המדינה, ראו ע"פ 8831/08 מדינת ישראל נ' אלשחרה (פורסם בנבו, 30.6.2010). כדוגמה ליישום על עברות של פעילות וחברות בארגון טרור שנעברו בחו"ל, ראו בג"ץ 861/87 אבו שרח נ' בית המשפט הצבאי בלוד, פ"ד מב(1) 810 (1988). כדוגמה נוספת להרחבת תחולה חקיקתית מחוץ לטריטוריה על בסיס פרסונלי, ראו את הוראתו המיוחדת של סעיף 14 לחוק השיפוט הצבאי, התשט"ו–1955, ולפיה בית דין צבאי מוסמך לדון חייל על כל עברה שאינה עברה צבאית (דהיינו עברה מכוח דיני העונשין הכלליים), בין שעבר אותה במדינה ובין מחוצה לה. ראו עוד את גישתו של פרופ' מרדכי קרמניצר, שלפיה הוראה אקסטרה-טריטוריאלית זו, המבוססת על מיהותו של הנאשם, יכולה לחול גם על שיפוט של נאשם חייל בבית משפט אזרחי. ראו מרדכי קרמניצר "סמכות שיפוט או תחולת חוק או שניהם גם יחד?" – דעה אחרת" משפטים יג 415 (1984). מנגד, ראו ש"ז פלר "סמכות שיפוט או תחולת חוק או שניהם גם יחד?" משפטים יא 92 (1981).

ראו סעיף 16 לחוק העונשין, שכותרתו "עבירות נגד משפט העמים", ומכוחו מקובל למנות פשעי מלחמה חמורים, השמדת עם, שוד ים, סחר בעבדים ועינויים. כן ראו סעיפים 1 (א) ו-2 לחוק לעשיית דין בנאצים ובעוזריהם, התש"י–1950; סעיף 5 לחוק בדבר מניעתו וענישתו של הפשע השמדת עם, התש"י–1950. היישום המוכר ביותר של תחולה אוניברסלית אקסטרה-טריטוריאלית (וכן רטרואקטיבית) במשפט הישראלי הוא במשפט אייכמן, שבו נדון נאשם שאינו תושב מדינת ישראל על עברות שביצע מחוץ למדינת ישראל כלפי קרבנות שלא היו תושבי המדינה (שעוד לא קמה). ראו ע"פ

לסמכות תחיקה.⁹ מהלך של פריצת גבולות הטריטוריה במסגרת סמכות התחיקה הוכר גם במשפט הבין-לאומי.¹⁰

מבחינה עיונית ניתן לדבר על כמה עקרונות של סמכות תחיקה שאינה צמודה לטריטוריה:¹¹ סמכות פרסונלית אקטיבית במובן של פרישת סמכות התחיקה על אזרחי המדינה בכל מקום שבו הם פועלים; סמכות פרסונלית פסיבית שלפיה ניתן להחיל את החוק המדינתי ולשפוט אדם על מעשה שמשפיע על אזרחי המדינה, אפילו אם הוא אינו אזרח המדינה ואם הוא פעל מחו"ל; סמכות פרוטקטיבית שלפיה ניתן להחיל את החוק הפלילי על מעשים שבוצעו בחו"ל בידי כל אדם הפוגעים באינטרסים חיוניים של המדינה או מוסדותיה; סמכות אוניברסלית.¹²

336/61 אייכמן נ' היועץ המשפטי לממשלה, פ"ד טז 2033, 2066–2067 (1962). כמו כן ראו סעיף 38 לפקודת הסמים המסוכנים [נוסח חדש], התשל"ג–1973, הקובע תחולה אקסטרה-טריטוריאלית על עברות סמים בכל מקום בעולם, כאשר ככשמדובר בתושב ישראלי אין דרישת פליליות כפולה (Dual criminality), הן במדינת ישראל והן במדינה שבה בוצעה העברה, ואילו כאשר מדובר במי שאינו תושב ישראלי, מוחלת דרישת פליליות כפולה.

9 ראו 18 U.S.C. § 1119, 2332, 3261; Model Penal Code, 10 U.L.A. 433 (1974), § 1.03; United States v. King, 552 F.2d 833, 850 (9th Cir., 1976); Federal Trade Commission v. Compagnie de Saint-Gobain-Pont-a-Mousson, 636 F.2d 1300, 1323 (D.C. Cir., 1980); United States v. Yunis, 924 F.2d 1086, 1091 (D.C. Cir., 1991); United States v. Nippon Paper Industries Co. Ltd., 109 F.3d 1 (1st Cir., 1997). כן ראו 11th Cir., 1307 (11th Cir., 1998); United States v. MacAllister, 160 F.3d 1304, 1307 (11th Cir., 1998). שם נקבע כי על כוונה לתחולה חוץ-טריטוריאלית ניתן ללמוד מלשונו המפורשת של החוק, אך ניתן להסיק זאת גם מ"טבעו" של הדין. ראו גם את הסקירה אצל: Charles Doyle, *Extraterritorial Application of American Criminal Law*, CONGRESSIONAL RESEARCH SERVICE REPORT 12–19 (2010).

10 ראו 10 PCIJ Ser. A No. 10, S.S. Lotus (France v. Turkey), 1927. באותו מקרה דובר בהתנגשות בים הפתוח בין אנייה תורכית לאנייה צרפתית, ובהתנגשות נספר כמה אזרחים תורכים. האנייה הצרפתית הגיעה לאיסטנבול, והקצין הראשון שלה נעצר ונשפט בתורכיה. בשל התנגדות צרפת למהלך זה של תורכיה הגיע העניין לבית הדין הבין-לאומי בהאג, ובו נפסק, בין היתר, כי המשפט הבין-לאומי מתיר למדינה להפעיל את סמכות השיפוט שלה וכן להחיל את חוקיה על פעולות שבוצעו מחוץ לטריטוריה שלה, אם יש להן תוצאות בטריטוריה שלה (האנייה התורכית נתפשת כטריטוריה). עקרון הטריטוריאליות אינו יסוד יחיד לסמכות השיפוט הפלילית. לעניין הרחבתה של סמכות התחיקה של מדינות מעבר לטריטוריה שלהן והכרת המשפט הבין-לאומי בכך, ראו הסקירה אצל: SHAW, לעיל ה"ש 6, בעמ' 652–683. לעניין הרחבת השימוש בסמכות אוניברסלית בזירה הבין-לאומית, ראו למשל אמנון רייכמן "סמכות שיפוט אוניברסלית בבתי משפט מדינתיים – עקצוע הריבונות או יצירת סדר עולמי?" משפט וצבא 17, 49, 54–60 (2004).

11 ראו 29 AM. J. INT'L L. 435, 445 (1935). ראו עוד למשל את: SHAW, לעיל ה"ש 6, בעמ' 652–696 והפסיקה המובאת שם; דינשטיין "סמכות השיפוט הפלילית", לעיל ה"ש 2; יורם דינשטיין סמכויות המדינה כלפי פנים 94–104 (1972); ש"ז פלר "הסמכות התחיקתית/סמכות השיפוט" הפרקליט כז 179, 181 (1971); אסתר גוימן-כהן המשפט הפלילי הבינלאומי: העמדתם לדין של רודנים ופושעי מלחמה 189–221 (2009); ע"פ 163/82 דוד נ' מדינת ישראל, פ"ד לז(1) 622, 627–629 (1983); ע"פ 4596/05 רוזנשטיין נ' מדינת ישראל, פ"ד ס(3) 353, 380–390 (2005).

12 כאשר מוחלת סמכות אוניברסלית, הרי שקודם לפתיחה בהליכים לפי עיקרון זה, מוטלת על המדינה החובה לתת הזדמנות למדינת האזרחות להעמיד את הנאשם לדין. ראו ארנה בן נפתלי וקרן מיכאלי "סמכות השיפוט האוניברסלית והשיח המשפטי המדינתי" המשפט ט 141, 148–159 (2004). כן ראו רובי סיבל "המדינה" משפט בינלאומי 77, 100–101 (רובי סיבל עורך, מהדורה שנייה, 2010).

סמכות שיפוט בין-לאומית בהקשר של משפט פלילי: ככלל במסגרת המשפט הפלילי סמכות השיפוט כרוכה בסמכות התחיקה. על כן כמעט שאין הפרדה מעשית ביניהן. ככל שדיני העונשין המדינתיים חלים על סיטואציה בין-לאומית, ובהינתן שהנאשם הובא לדין ונאספו ראיות לצורך העמדתו לדין (דהיינו בהינתן שאין בעיה בתחום תחולת דיני העונשין ואין בעיה בתחום האכיפה הפלילית), ייטה בית המשפט להחיל את סמכותו על הנאשם.¹³ ניתן לציין בכל זאת שני עניינים הנפרדים במלואם מסמכות התחיקה והם מתחום סמכות השיפוט בלבד: בחינת טענות של זיכוי או הרשעה קודמים וסיכון כפול המביאים לבטלות ההליך השיפוטי, גם אם סמכות התחיקה חולשת על המקרה; קביעת סטנדרט של סבירות (Reasonableness) השיפוט של המקרה במדינה הנדונה. זהו סטנדרט שלפיו המדינה תשקול את סבירות השיפוט של המקרה, על פי נסיבותיו, בפניה, גם אם באופן דווקני קמה סמכות שיפוט בין-לאומית.¹⁴ מלבד האמור עד כה באשר לסמכות התחיקה וסמכות השיפוט הפלילית ברמה של משפט המדינות, ראוי לציין כאן התפתחות נוספת, הפעם מכיוון המשפט הבין-לאומי עצמו, בדמות פיתוחה של סמכות משפטית פלילית אל-מדינתית בדמות בית הדין הבין-לאומי בהג (ICC – International Criminal Court) ובדמות ערכאות שיפוטיות פליליות נוספות שהוקמו אד הוק.¹⁵ התפתחות זו מצרה את סמכותן של המדינות ומבטאת את הכפפת הריבונות לעקרונות-העל של המשפט הבין-לאומי.

סמכות אכיפה בין-לאומית בהקשר של משפט פלילי: בהכללה, הסמכות השיפוטית עוסקת בהוצאה לפועל של סמכות התחיקה, ואילו סמכות האכיפה עניינה בהוצאה לפועל של שתיהן – סמכות התחיקה וסמכות השיפוט. לפיכך ניתן לכלול כאן את סוגיית ההסגרה של חשודים ונאשמים ואת כלל פעולות החקירה (מעצר, תשאול, חיפוש, תפיסה וכיוצא בזה) ככל שאלה מיועדות להתבצע מחוץ לטריטוריה המדינתית. עיקר ענייני בפרק זה בסמכות האכיפה הבין-לאומית, ובתוך קטגוריה זו ענייני הוא בסמכות הנוגעת לאיסוף ראיות המצויות בחו"ל במסגרת החקירה הפלילית (סמכות איסוף בין-לאומית). הכלל הגדול הוא כי סמכות האכיפה במרחב הפיזי, ובכלל זה סמכות איסוף הראיות, מתוחמת לטריטוריה של המדינה החוקרת. כלל זה מצוי בעקרונות המשפט הבין-לאומי, כנגזר מעקרונות הטריטוריאלית¹⁶ וכנלמד מאמנות

13 גם פלר הצביע על החפיפה המעשית, גם אם לא עיונית, בין סוגיית סמכות התחיקה הבין-לאומית בפלילים לבין סמכות השפיטה הבין-לאומית. ראו ש"ז פלר יסודות דיני עונשין כרך א 236–237 (1984). ראו עוד את עניין רוזנשטיין, לעיל ה"ש 11, בעמ' 3892–3983, 3988.

14 ראו RESTATEMENT, לעיל ה"ש 1, §421. על פי ה- Restatement האמריקני, ניכר כי הכוונה לדרישה מחייבת, שאינה כוללת דרישת הדדיות בין מדינות, דהיינו שמדינה א תשקול סבירות העמדה לדין אצלה לעומת העמדה לדין במדינה ב רק אם מדינה ב תשקול את אותו השיקול במקרה הפוך, שבו היא תידרש לבחון את בררת השיפוט בינה לבין מדינה א. במילים אחרות, בחינת הסבירות תידרש גם במקרה של מדינה הצריכה לשקול את סמכות שיפוטה אל מול סמכות שיפוטה של מדינה אחרת שעמה אין לה יחסים דיפלומטיים מכל סוג.

15 ניתן לציין את בתי הדין הפליליים הבין-לאומיים ליוגוסלביה לשעבר ולרואנדה, אשר הוקמו באמצע שנות התשעים של המאה הקודמת בידי מועצת הביטחון של האו"ם, מכוח סמכותה על פי פרק VII למגילת האו"ם, ואשר כוחם מחייב את כל המדינות החברות באו"ם.

16 ראו *The Lotus Case*, לעיל ה"ש 10, בעמ' 18, שם נפסק:

“The first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its

שוונות העוסקות באכיפה פלילית בין-מדינתית,¹⁷ וכן מצוי הוא בעקרונות הפנימיים של המדינות,¹⁸ לרבות מדינת ישראל.¹⁹ ארחיב מעט על עקרון הטריטוריאליות בכל הנוגע לסמכות

powers in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from custom or from a convention”.

17 אמנות אלה מניחות מראש את עקרון הטריטוריאליות כעקרון היסוד המחייב אפוא שיתוף פעולה בין-מדינתי כאשר מדובר בפעולה חוצת-גבולות. ראו Schengen Convention (Vienna, 1956); Interpol (Vienna, 1956); Convention (Schengen, 1990), Title III Ch. 1, Title IV Ch. I-IV; EC Council Regulation no. 1468/81 on Mutual Assistance Between the Administrative Authorities of the Member States and Cooperation Between the Latter and the Commission to Ensure the Correct Application of the Law on Customs or Agricultural Matters (1981). עוד ראו את סעיף 4 לאמנת האו"ם נגד פשיעה בין-לאומית חוצת-גבולות: United Nations Convention against Transnational Organized Crime (2000), שעל פיו –

“Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law”.

כן ראו סיבל, לעיל ה"ש 12, בעמ' 98–99. ראו גם, בהקשר של המשפט הישראלי, את חוק עזרה משפטית בין מדינות, התשמ"ח–1988, ובעיקר סעיפים 4, 8, 14–21, 28–31, 46–47, 53. ודוק, חוק עזרה משפטית לא רק מחייב הגשת בקשה לעזרה משפטית כשמדובר באיסוף ראיות בטריטוריה זרה אלא גם קובע כי כאשר מדינה זרה מגישה בקשה לעזרה משפטית בישראל, ומוחלט להיעתר לבקשה, תתבצע פעולת איסוף הראיות על פי הדין הישראלי, על מגבלותיו השונות, ולא על פי דינה של המדינה המבקשת. ליישום ראו ח"ד (שלום ת"א) 10-10-11287 הרשות המוסמכת באיי הבתולה נ' הנהלת בתי המשפט (פורסם בנבו, 2.5.2011). ראו עוד, ANTONIO CASSESE, INTERNATIONAL LAW 50 (2nd ed., 2005); ROBERT CRAYER, HAKAN FRIMAN, DARRYL ROBINSON & ELIZABETH WILMSHURST, AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE 38–39 (2007); Staker, לעיל ה"ש 6, בעמ' 335–337.

18 במשפט האמריקני ראו ה־RESTATEMENT, לעיל ה"ש 1, §432 cmt. b.

“It is universally recognized, as a corollary of state sovereignty, that officials of one state may not exercise their functions in the territory of another state without the latter’s consent. Thus, while a state may take certain measures of nonjudicial enforcement against a person in another state, ... its law enforcement officers cannot arrest him in another state, and can engage in criminal investigation in that state only with that state’s consent”.

ראו עוד למשל את Doyle, לעיל ה"ש 9, בעמ' 20–25. Harold G. Maier, *Extraterritorial Jurisdiction at a Crossroads: An Intersection Between Public and Private International Law*, 76 A.J.I.L. 280, 293–296 (1982). במשפט האמריקני הכלל אף חלחל ליחסים בין המדינות השונות המרכיבות את הפדרציה של ארצות הברית. גם האכיפה הפלילית הבין-מדינתית בתוך ארצות הברית זוכה להתייחסות מתוך נקודת מוצא טריטוריאלי. קיימת כמובן הכרה באפשרות לבצע פעולות של איסוף ראיות מחוץ לטריטוריה של המדינה, אך ככלל הדבר יכול להיעשות בהסכמת המדינה האחרת בלבד. ראו למשל State of New Hampshire v. Windhurst, 2006 WL 2075119 (N.H. Super., 2006).

במשפט הקנדי ראו (Ca.) [2007] SCC 26, para. 94, R. v. Hape, שם נפסק מפי השופט לבל (LeBel):

“A criminal investigation in the territory of another state cannot be a matter within the authority of Parliament or the provincial legislatures, because they have no jurisdiction to authorize enforcement abroad. Criminal investigations, like political structures or judicial systems, are intrinsically linked to the organs of the state, and to its territorial integrity and internal affairs. Such matters are clearly within the authority of Parliament and the provincial legislatures when they are in Canadian territory; it is just

האכיפה הפלילית במשפט הישראלי. ניתן למצוא התייחסות מפורשת לסמכות האיסוף הבין-לאומית בפרשת אל מצרי.²⁰ באותו מקרה דובר בהאזנת סתר משטרתית שבוצעה בשטח רצועת עזה בשנת 1989 (כאשר הרצועה הייתה בשליטה צבאית מלאה של מדינת ישראל) במסגרת חקירה של עברות סמים. בית המשפט העליון קבע כי חוק האזנת סתר, התשל"ט-1979, שמכוחו רשאי בית משפט מחוזי להתיר למשטרה לבצע האזנת סתר, אינו חל בשטחים הכבושים אלא רק בתחולה פרסונלית על אזרחי מדינת ישראל המתגוררים בהם.²¹ תחת הוואקום החקיקתי

as clear that they lie outside the authority of those bodies when they are outside Canadian territory".

19 ראו בג"ץ 5128/94 פדרמן נ' שר המשטרה, פ"ד מח(5) 647, 655 (1995), שם נפסק מפי הנשיא שמגר:

"תפקידיה וסמכויותיה של משטרת ישראל נקבעו כאמור בפקודת המשטרה... ובחוקים נוספים. אין חולק כי סמכויותיה של משטרת ישראל, בתור מפעילת כוחותיה על פי החוקים הנ"ל, מוקנות לה רק בתחומים הנתונים לשליטת מדינת ישראל, ובמסגרת זו היא פועלת למטרות הקבועות בפקודה הנ"ל. בהתאם לכך, אין משטרת ישראל, ואין שוטר הנמנה על משטרת ישראל, מוסמכים להפעיל כל סמכות משטרתית שהוענקה להם בחוקים השונים, מחוץ לשטח הנתון לשליטתה של מדינת ישראל..."

בעניין פדרמן דן בג"ץ בשיגור משלחת של שוטרי משטרת ישראל כדי שיצטרפו לכוח הפיקוח הרב-לאומי שהופעל בהאיטי בעקבות החלטה של מועצת הביטחון של האו"ם וביזמת ממשלת ארצות הברית. העותר טען כי פעולתה זו של המשטרה אינה על פי סמכויותיה מכוח פקודת המשטרה [נוסח חדש], התשל"א-1971. בג"ץ אמנם הכשיר את פעולת משטרת ישראל בראותו בה פעולה מכוח סמכותה השירותית של הממשלה מכוח סעיף 29 לחוק-יסוד: הממשלה, ומכוח הסכמה בין-מדינית על שיגור המשלחת כאמור. הנשיא שמגר חזר והדגיש כי פעולות משטרת ישראל הן בתחום הטריטוריה הישראלית בלבד, והחריג הוא פעולה אל מחוץ לגבולות המדינה במסגרת הסכמתו של הריבון הזר בלבד.

כן ראו ת"פ (מחוזי י-01) 1071-01 מדינת ישראל נ' רבינוביץ' (פורסם בנבו, 19.9.2010). מקרה זה נודע כפרשת הפטריארכיה היוונית-אורתודקסית, שבה נוהלו הליכים פליליים בגין עברה של קבלת דבר במרמה בנסיבות מחמירות (ועברות נלוות נוספות) מהקרן הקיימת לישראל לצורך ביצוע, כביכול, של עסקאות חכירה של קרקעות בבעלות הפטריארכיה היוונית-אורתודקסית, אולם בפועל הנאשם לא התכוון לבצע בשם הפטריארכיה עסקאות אלה. בתום ההליכים הפליליים בפרשה ביקשה המדינה מבית המשפט להפעיל את סמכותו מכוח פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 (להלן – הפסד"פ) ולהורות כי כספים המצויים בשני חשבונות בנק בשווייץ, שהנאשם פתח, יועברו לרשות הקרן הקיימת לישראל (נפגעת העברה). ההגנה טענה כי בית משפט ישראלי אינו מוסמך להורות על ביצוע פעולה בנוגע לחשבונות בנק בשווייץ. הטענה נדחתה מבלי שנדונה לגופה, מהטעם שהמדינה הציגה הסכמה של שלטונות שווייץ להיעתר לצו בית-משפט ישראלי בנדון, במידה שזה יוצא. לנוכח הסכמת המדינה הזרה, הניח בית-המשפט למעשה כי אין כל מניעה, מבחינת סמכות בין-לאומית, להוצאת הצו, ואכן קיבל את בקשת המדינה בעניין.

20 ראו ע"פ 4211/91 מדינת ישראל נ' אל מצרי, פ"ד מז(5) 624, 639–640 (1993).

21 בהקשר רחב יותר מהקשרו של פסק הדין בעניין אל מצרי, ראו חוק להארכת תוקפן של תקנות שעת חירום (יהודה ושומרון וחבל עזה – שיפוט בעבירות ועזרה משפטית), התשל"ח-1978, בעיקר את סעיפים 2, 3, 5, 6, 11, 14. הוראות אלה מרחיבות את תחולת החקיקה, השפיטה והאכיפה מחוץ לטריטוריה של מדינת ישראל אל שטחי יהודה ושומרון, כאשר בסיס ההרחבה הוא פרסונלי ותחולתו הוא על ישראלים הנמצאים בשטחים או שביצעו שם את העברה. אשר למי שאינם ישראלים שביצעו עברות פליליות בשטחים, אלה יכול שיישפטו בבתי משפט צבאיים שהקים מפקד האזור, אלוף פיקוד המרכז. הוראות אלה מוסברות בבית המשפט העליון בכך שהכיבוש נתפש כמצב זמני וכך בכך שההתנגשות עם העיקרון של כיבוד ריבונות של מדינה זרה מעומעם, לפחות בדוגמה של שטחי יהודה ושומרון שנכבשו מירדן במלחמת ששת הימים. ראו למשל בג"ץ 390/79 דויקא נ' מדינת ישראל, פ"ד

הזה קבע בית המשפט כי מותר למשטרת ישראל לצותת לשיחות בשטחים ללא צו שיפוטי, אך יהיה עליה לפעול על פי חובות כלליות של המשפט המנהלי.²² חובות של הגינות, שוויוניות, הימנעות משיקולים זרים, פעולה למען הגשמת תכליתו של החוק וכיוצא בזה. לכאורה נובע מפסק דין זה שהאזנת סתר מחוץ לטריטוריה הישראלית מותרת לרשויות החקירה בלא צורך בהסמכה שיפוטית. אולם אני מציע לראות בפסק הדין הלכה המתייחסת להאזנת סתר בשטחים כבושים תחת "תפיסה לוחמתית" ולא הוראה גורפת המתירה האזנת סתר "מנהלית" בכל העולם. במקרה של האזנת סתר, או כל פעולת איסוף אחרת לצורך העניין, שתתבצע בטרטוריה של מדינה עצמאית אחרת, תידרש לכאורה בקשה לעזרה משפטית מהמדינה הזרה, או למצער הסכמתה של המדינה לביצוע ההאזנה באמצעות הרשויות הישראליות (מחוץ למסלול העזרה המשפטית הפורמלית). ושוב אזכיר, כוונתי כאן לפעולות איסוף ראיות במסגרת חקירה פלילית ולא לפעולות המתבצעות מכוח סמכויות הביטחון של המדינה. במקרה של שטח כבוש, כיוון שלא רלוונטי לפעול בדרך של עזרה משפטית, ואין צורך בשמירה על עיקרון של כיבוד ריבונות של מדינה זרה, תיתכן התוצאה של האזנת סתר מחוץ לטריטוריה הקבועה ובסמכות מנהלית בלבד. בחזרה אל תמצית ההלכה בעניין אל מצרי הצריכה לענייננו, בית המשפט העליון קבע הלכה למעשה כי תחולת החוק המסדיר סמכויות אכיפה של משטרת ישראל לביצוע האזנת סתר היא טריטוריאלית כל עוד לא נקבע במפורש אחרת.

אם לסכם עד כאן, הרי שבשונה מסמכות התחיקה הפלילית, שבה המשפט מייצר הרחבות רבות הן בדמות פיתוח העיקרון הטריטוריאלי והן בדמות פיתוח עקרונות אקסטרטריטוריאליים, בכל הנוגע לסמכות האכיפה הפלילית, הכללים הטריטוריאליים נשמרים בקפידה רבה יחסית. ההפרה המוכרת ביותר היא במקרים שבהם רשויות המדינה "חטפו" חשודים, ולימים נאשמים, ממדינות זרות. מקרים אלה הם מתחום של הבאה לדין (התגברות על דיני ההסגרה) ולא מתחום של איסוף ראיות לצורך העמדה לדין.²³ מחירה של הפרה יכול להיות

לד(1) 1, 12 (1979); בג"ץ 69/81 אבו עיטה נ' מפקד אזור יהודה ושומרון, פ"ד (2) 197, 228 (1981); בג"ץ 185/87 עפו נ' מפקד כוחות צה"ל בגדה המערבית, פ"ד מב(2) 1, 50 (1987); בג"ץ 2977/91 תג' נ' שר הביטחון, פ"ד מו(5) 467, 471 (1991); בג"ץ 2056/04 מועצת הכפר בית סוריק נ' ממשלת ישראל, פ"ד נח(5) 807, 826–827 (2004). על כל פנים, היוצא מן הכלל דווקא מעיד על הכלל, והוא שבהיעדר הוראה מפורשת אין סמכויות אכיפה פליליות מחוץ לטריטוריה של המדינה, אפילו לא במסגרת שטח כבוש, שעליו חולשות הוראות מהמשפט הבינ-לאומי הפומבי לעניין השלטת סדר ושמירה על הביטחון.

22 להבחנה זו, בדבר תחולתו של המשפט המנהלי במקום המשפט החוקתי בשטחי איו"ש, ראו גם יעל רונן "תחולתו של חוק יסוד: כבוד האדם וחירותו בגדה המערבית" שערי משפט ז 149, 153–154 (2014).

23 ראו למשל *United States v. Alvarez-Machain*, 504 U.S. 655; *Ker v. Illinois*, 119 U.S. 436 (1886); שם לא ביטל בית המשפט את ההליכים נגד הנאשם שנחטף ממקסיקו לארצות הברית, תוך יישום הדוקטרינה של "Male captus, bene detenus" ("Improperly captured, properly detained"). *R. v. Plymouth Justices (ex parte Driver)*, [1986] 1QB 95 (Eng.). לפסיקה הפוכה בבריטניה ראו *R. v. Horseferry Magistrate's Court (ex parte Bennet)*, [1994] 1 A.C. 42 (Eng.). כן מוכר עניינם של מרדכי וענונו, שנחטף – על פי הפרסומים – מאיטליה לישראל, ועניינו של אדולף אייכמן, שנחטף לישראל מארגנטינה. בעניינו של אייכמן קבע בית המשפט העליון מפי השופט אגרנט: "לא יחקור בית המשפט בנסיבות עצירתו והבאתו (של הנאשם) לתחום השיפוט" (פרשת אייכמן, לעיל ה"ש 8, בעמ' 2067). עם זאת ארגנטינה לא הסתפקה בהתנצלותה של מדינת

במישור היחסים הדיפלומטיים בין המדינה החוקרת לבין המדינה הטוענת לפגיעה בריבונותה בעקבות פעולת חוקרים בטריטוריה שלה, וכן יכולה הפעולה להגיע לכדי אישום פלילי נגד אותם חוקרים בטענה לביצוע עברות של תקיפה (במקרה של מעצר), התפרצות (במקרה של חיפוש) וכדומה.²⁴

ג. איתור התפישה הטריטוריאלית באשר למרחב הסייבר

עמדתי לעיל על שתי תופעות, שבהן אבקש להתמקד בחלק זה של הדיון: האחת, סמכות התחיקה הבין-לאומית (ובעקבותיה סמכות השיפוט הבין-לאומית) מורחבת ומוחלת כל אימת שחלק מן העברה נעבר בשטח המדינה; השנייה, סמכות האכיפה הבין-לאומית מוצרת ומחייבת כי כל מעשה האכיפה יתבצע בשטח המדינה. שתי תופעות אלה, אשר אובחנו באשר למרחב הפיזי, מתרחשות גם בכל הנוגע למרחב הסייבר. הן ההרחבה התחיקתית (והשיפוטית) והן ההצרה האכיפתית – שתיהן מניחות כנקודת מוצא את התפישה הטריטוריאלית באשר למעשה העברה במרחב הסייבר, כמו גם באשר לאיסוף הראיות במרחב הסייבר.

1. סמכות תחיקה ושיפוט

התפישה באשר לסמכות התחיקה והשיפוט על עברות במרחב הסייבר יוצאת מאותה נקודת מוצא טריטוריאלית הרלוונטית לסמכות התחיקה והשיפוט במרחב הפיזי. עם זאת הטריטוריאליות נמתחת באופן שמאפשר להרחיב באופן ניכר את סמכות התחיקה והשיפוט ביחס לעברות במרחב הסייבר. על סמך הכלל הדורש כי מקצת העברה (בישראל למשל)²⁵ או חלק לא מבוטל ממנה (בבריטניה למשל)²⁶ ייעברו במדינת הפורום, על מנת שזו תיחשב עברת פנים, בתי המשפט תופשים עברות מקוונות רבות כעברות פנים. מיקומו הפיזי של מבצע העברה מחוץ לטריטוריה, ואף מיקום מחשביו מחוץ לטריטוריה, אינו מחסן מפני הפללת ההתנהגות ככל שהיא כוללת התקשרות עם קרבן או חשיפה מודעת של מידע במחשבו של קרבן הנמצא

ישראל על הפגיעה בריבונותה ופנתה למועצת הביטחון של האו"ם, וזו גינתה את מדינת ישראל וקבעה כי עליה לשלם לארגנטינה פיצוי הולם. ראו, לעניין זה, את גנון המדינה "מאחורי הקלעים של פרשת מעצרו ומשפטו של אדולף אייכמן" (2011), <http://www.archives.gov.il/ArchiveGov/pirsumyginzach/>, HistoricalPublications/EichmanTrial/EichmanTrialMavo.htm. לתיקי חטיפה נוספים שבהם נדונה

שאלת הפרת הדין הבין-לאומי, ראו סקירה אצל: CASSESE, לעיל ה"ש 17, בעמ' 50–52. ראו למשל Doyle, לעיל ה"ש 9, בעמ' 20. כן ראו את המקרה המובא ב-RESTATEMENT, לעיל ה"ש 1, §432 cmt. c, שם מובא מקרה של שני חוקרים צרפתים שתחקרו בשווייץ עובד בנק שווייצרי כמה פעמים. אותו עובד בנק דיווח לשלטונות השווייצריים, ואלה עצרו את החוקרים הצרפתים בפעם הבאה שבה נכנסו לשווייץ לצורך המשך התחקור של אותו עובד בנק. החוקרים הצרפתים ביקשו לבסס עברות כלכליות שיוחסו לחשודים צרפתים. רשויות האכיפה בשווייץ העמידו לדין את החוקרים הצרפתים בגין עברות נגד הסודיות הבנקאית השווייצרית שמבצעת סוכנות זרה (מעין עברה של ריגול עסקי שמבצעת רשות מדינתית), והשניים נידונו לעונשי מאסר בפועל.

24 ראו לעיל ה"ש 5.

25 ראו R. v. Smith, [2004] Q.B. 1418 (Eng.) 26. בעבר הגישה האנגלית חייבה השלמה של כל היסוד העובדתי של העברה בטריטוריה האנגלית על מנת שתיחשב העברה "עבירת פנים" לפי הדין האנגלי. ראו R. v. Manning, [1998] 2 Cr. App. R. 461 (Eng.)

במדינה השופטת.²⁷ בשל כלל מרחיב זה לא התעורר הצורך בפיתוח עקרונות נוספים שאינם טריטוריאליים במיוחד בשביל עברות במרחב הסייבר. אציג להלן כמה מקרים מייצגים המלמדים על הרחבת סמכות התחיקה והשפיטה כאשר לעברות באינטרנט דרך הצינור הטריטוריאלי במובנו המקובל, המסתפק במקצת או בחלק מן העברה על מנת לקנות סמכות. המקרה המוכר ביותר במשפט הישראלי שבו נדונה סוגיית סמכות השיפוט (וכפועל יוצא מכך גם סמכות התחיקה) הביין-לאומית במרחב הסייבר הוא מקרהו של מייקל קרלטון. קרלטון הוא מבצע של אתר הימורים מצליח ששרתיו מוקמו בגיברלטר, שם מותרים כל סוגי ההימורים המוצעים באתר. האתר מציע את שירותיו למהמרים מכל העולם, לרבות מישראל, כאשר חלק מההימורים הם בעברית, וברי כי הם מכוונים, על פי תוכנם, לקהל דובר עברית. בעת שהגיע קרלטון לביקור בישראל, עוכב לחקירה בגין ביצוע לכאורה של עברת ארגון הימורים אסורים. אגב דיון בתנאי שחרורו בערובה, העלתה ההגנה את שאלת סמכות השיפוט הישראלית על העברה הנטענת, וזאת משום שאתר ההימורים ממוקם בחו"ל. בית המשפט קבע כי מעשה ההימור נתפש ככזה המתבצע במחשבו של כל אחד ואחד מהגולשים מישראל, ומשכך, מקום ביצוע העברה הוא גם בישראל, ויש לראות בעברה משום עברת פנים, המקימה סמכות שיפוט ישראלית.²⁸ מקרה נוסף שבו התעוררה שאלת סמכות השיפוט הביין-לאומית בנוגע לעברות אינטרנט הייתה בעניינו של משה הלוי, פעיל רשת ידוע המכונה "הלמו", שהואשם בכך שפרסם את תמונתו של מפכ"ל המשטרה לשעבר, רנ"צ משה קראדי, כשהוא לבוש כביכול במדים נאציים. התמונה נערכה כפוטו-מונטאז' והועלתה לפורום ששרתיו מצויים בארצות הברית. הלוי הואשם בעברה של העלבת עובד ציבור, ובמהלך משפטו העלה טענה מקדמית של חוסר סמכות ביין-לאומית לשפוט אותו על העברה היות שמקום הפרסום המיוחס לו הוא בחו"ל. בית המשפט דחה את הטענה, בנימוק שהנאשם העלה את התמונה, כך לכאורה על פי כתב האישום, מישראל, ולכן אם עובדה זו תוכח במשפט, אין לקבל את הטענה המקדמית. לפחות חלק מביצוע העברה הוא מישראל, ועל כן מדובר ב"עברת פנים" ישראלית.²⁹

בדין האמריקני מוכרת הפסיקה בעניין *W.I.G.C.*, שם דובר על הקמת אתר הימורים באינטרנט במדינת אנטיגואה המתירה הימורים בשטחה. אתר האינטרנט הוצע באנגלית, ועיקר הכנסותיו היו מתושבי ארצות הברית, ובהם תושבי מדינת ניו יורק, אשר נקטה הליכים פליליים

27 ברם אילו הייתה רווחת הגישה שבוטאה בפסק הדין האנגלי בעניין *Manning*, שם, היה ניתן לומר כי מיקום שרתי המחשב של מבצע העברה בחו"ל הופך את העברה מעברת פנים לעברת חוץ, ובמקרה כזה, אלמלא ינקוב חוק העונשין המדינתי במפורש בהוראה מרחיבת-תחולה טריטוריאלית, יהיה בלתי אפשרי להפיל את התנהגותו של מבצע העברה.

28 ראו ב"ש (מחוזי ת"א) 90861/07 קרלטון נ' היחידה הארצית לחקירות הונאה (פורסם בנבו, 17.6.2007). להתייחסות מוקדמת יותר (אם כי לאקונית יחסית), גם היא בהקשר של הימורים באינטרנט, ראו ב"ש (מחוזי חי') 3707/01 יגודייב נ' מדינת ישראל, בפס' 19–21 (פורסם בנבו, 8.8.2001). כן ראו ת"פ (מחוזי ב"ש) 6596-04-11 מדינת ישראל נ' גיאג' (פורסם בנבו, 21.1.2012).

29 ראו ת"פ (שלום חי') 1826/08 מדינת ישראל נ' הלוי (פורסם בנבו, 27.1.2009). לימים זוכה הלוי מן העברות שיוחסו לו, אם כי מטעמים אחרים שאינם צריכים לענייננו. ראו ת"פ (שלום חי') 1826/08 מדינת ישראל נ' הלוי (פורסם בנבו, 2.11.2011). למקרה נוסף שבו התעוררה שאלה דומה, ראו ת"פ (שלום ראשל"צ) 38070-06-12 מדינת ישראל נ' גודוביץ' (פורסם בנבו, 30.6.2013), שם שלח תושב ישראל הודעת דוא"ל בעלת תוכן מדאיג מישראל למשטרה ברוסיה, והוחלט שמעשהו מגלם עברת פנים בישראל (עברה של פרסום ידיעה כוזבת העלולה לגרום פחד ובהלה, לפי סעיף 159(א) לחוק העונשין).

נגד האתר ומנהליו. בית המשפט שם הכיר בסמכותו לדון בעברות כעברות פנים.³⁰ בנוסף ניתן למצוא פסיקה מרחיבת סמכות שיפוט בכל הנוגע לעברות של פרסומי תועבה באינטרנט. בעברות אלה התעוררה השאלה אם עברת הפרסום נעברת רק במקום העלאת התכנים (Upload), או שמא גם במקום שבו כל אחד ואחד מהגולשים מוריד את התכנים (Download). בעניין Thomas נקבע העיקרון של ביצוע עברת הפרסום כ"עברת פנים" בכל מקום שאליו מגיע התוכן ולא רק במקום הפצתו המקורי.³¹

בדין הצרפתי התנהל ההליך המפורסם ביותר בתחום סמכות החקיקה והשיפוט באינטרנט – פרשת Yahoo!. תחילתה של הפרשה בצרפת, שם עתרו שני ארגונים למלחמה באנטישמיות נגד אתר יאהו!, שבו הוצגו למכירה פומבית מזכרות נאציות, דבר המהווה עברה על הקוד הפלילי הצרפתי, האוסר על הצגת סמלים נאציים. בית המשפט הגבוה בפריז קבע כי יאהו! הפרה את הקוד הפלילי הצרפתי. נפסק כי אמנם מצד אחד לא דובר באתר אינטרנט שכוון מראש לקהל צרפתי, אלא באתר הנגיש לכלל הציבור והניתן לצפייה בין היתר על ידי קהל צרפתי, אולם מצד שני דובר באתר מסחרי (מכירות פומביות) ששאיפתו היא להגיע לקהל יעד רחב ככל הניתן מטעמים רווחיים, ולכן יש בפעולה זו של האתר משום הכפפה רצונית לסמכויות שיפוט של המדינות שבהן מצויים משתמשי האינטרנט הגולשים אל האתר. על כן מחובתה של יאהו! למנוע גישה של משתמשי אינטרנט צרפתים לדפי התוכן האסורים, לרבות באמצעות סינון גולשים מכתובות IP צרפתיות, דרישה מהגולש לציין את מדינת מוצאו כאשר כתובת ה-IP שלו מעורפלת באופן שאינו מאפשר זיהוי ארץ מוצאו בוודאות וכיוצא בזה. הפסיקה הוחלה לא רק על יאהו! בצרפת (Yahoo.fr) אלא גם על יאהו! האמריקנית (Yahoo.com).³² יאהו! האמריקנית בחרה לפנות לבית משפט אמריקני בבקשה לסעד הצהרתי שיכריז על אי-אכיפותו של פסק הדין הצרפתי בארצות הברית בשל פגיעתו בחופש הביטוי כפי שהוא מפורש על בסיס התיקון הראשון לחוקה האמריקנית. בערכאה הראשונה התקבלה עתירתה של יאהו!³³ בית המשפט לערעורים במחוז התשיעי הפך את פסיקת בית המשפט דלמטה על בסיס טענה של היעדר סמכות שיפוט. נמצא כי המערערים לא כיוונו את פעולתם, בפנייתם לבית המשפט בפריז, כלפי ארצות הברית, ועל כן הפעלת סמכות השיפוט במקרה כזה תהיה לא סבירה בנסיבות העניין.³⁴ ניסיונות לדיון בהרכב מורחב (en banc) ובקשת רשות ערעור לבית המשפט העליון – לא הביאו

30 People of New York v. World Interactive Gaming Corp., 714 N.Y.S. 2d 844 (N.Y. Sup. Ct. ראו 1999).

31 United States v. Thomas, 74 F.3d 701 (6th Cir., 1996), ראו ששסק בבררת סמכות השיפוט בין שתי מדינות בארצות הברית, ולא בין ארצות הברית למדינה זרה, אך בעניין זה סבורני כי אין הכדל בין המערכת הפדרלית בארצות הברית לבין המערכת הבין-לאומית, ונוסח פסק הדין כוון לקבוע עיקרון כללי בעניין דגן.

32 La Ligue Contre le Racisme et l'Antisemitisme (LICRA) v. Yahoo!, Inc., Tribunal de Grande Instance [T.G.I.] Paris, Ordonnance de Refere (2000) (Fr.), available at <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf> ראו

33 Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

34 La Ligue Contre le Racisme et l'Antisemitisme v. Yahoo!, Inc., 379 F.3d 1120 (9th Cir., ראו 2004).

להפיכת התוצאה.³⁵ פרשת *Yahoo!* מלמדת אפוא על האופן שבו הרחיבה הפסיקה הצרפתית את סמכות התחיקה הפלילית שלה, האוסרת על הצגת סמלים נאציים, גם על פעולות באינטרנט שמקורן הוא מחוץ לתחומי צרפת. לעומת זאת בארצות הברית לא הכיר בית המשפט בהרחבת סמכות זו.

גם במשפט האיחוד האירופי ניתן למצוא ביטוי לתפישה מרחיבה של סמכות התחיקה והשיפוט כאשר לעברות באינטרנט. בית הדין האירופי הגבוה לצדק (European Court of Justice) מתח את גבולות "עברת הפנים" בהימורים באינטרנט בדומה לפסיקה בעניין *W.I.G.C.* וקרלטון שנמנו לעיל.³⁶ בנוסף, ניתן לציין את החלטת האיחוד האירופי משנת 2005 בנוגע לעברות נגד מערכות מידע (EU Framework Decision on Attacks against Information Systems). החלטה זו מאפשרת למדינות האיחוד האירופי לקבוע בחוקיהן הפנימיים תחולה אקסטרטריטוריאלי של עברות מידע, בשני מובנים: במובן זה שמבצע העברה פוגע מחו"ל במערכות המידע שבמדינה, ובמובן זה שמבצע העברה מצוי בטריטוריה של המדינה, ומערכות המידע הנפגעות מצויות בכל מדינה אחרת שהיא.³⁷

להשלמת התמונה אציין כי בתחומי המשפט האזרחי קיימת פסיקה ענפה בכל הנוגע להכפפת גורם זר, המעלה תכנים בשרת זר, לסמכות השיפוט של מדינת הפורום במקרה שבו התובע (הנפגע) מצוי במדינת הפורום בפועל. הדיון המתעורר שם נוגע לשאלה אם העלאת תכנים בשרת זר מחייבת לפי דין מקום מושבם של כל מקבלי התכנים (Situs of recipient), לפי דין מקום מושבו של מעלה התכנים (Situs of Transmitter) או לפי מבחן ביניים תלוי נסיבות.³⁸

35 ראו (בהתאמה) 433 F.3d 1199 (9th Cir., 2006) *Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, cert. denied, 126 S. Ct. 2332 (2006).

36 ראו *Liga Portuguesa de Futebol Profissional v. Departamento de Jogos da Santa Casa da Misericórdia de Lisboa*, ECJ C-42/07 [2009].

37 ראו Council Framework Decision 2005/222/JHA on Attacks Against Information Systems, Art. 10, OJ L69/67 (16.3.2005).

38 ראו למשל את *Compuserve v. Patterson*, 89 F.3d 1257 (6th Cir., 1996), שם נפסק בעניין סכסוך חוזי בין-מדינתי בתוך ארצות הברית. התובעת הייתה חברת *Compuserve*, שמושבה באוהיו ושרתיה ממוקמים שם. הנתבע אזרח טקסס שפעל מטקסס. נקבע כי לאוהיו קמה סמכות שיפוט היות שהנתבע התקשר בפועל עם שרתיה המחשב של *Compuserve* באוהיו והעלה באמצעותם תכנים שונים לאינטרנט, ומכאן שלנתבע זיקה לאוהיו. בעניין *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295 (S.D.N.Y., 1996), נקבע כי עצם העובדה שאתר אינטרנט נצפה במדינות שונות, נוסף על המדינה שבה מצוי השרת שעליו "יושב" האתר, היא כשלעצמה אינה מספיקה לצורך הקמת סמכות שיפוט (בתביעת סימני מסחר) במדינות אחרות שבהן ניתן לצפות באתר. בעניין *Zippo Manufacturing Company v. Zippo Dot Com, Inc.*, 925 F. Supp. 1119 (W.D. Pa., 1997) נתבע זר במדינת הפורום: בקצה האחד של הסקאלה, כאשר הנתבע מבצע עסקאות באמצעות האינטרנט המשפיעות ישירות ובבירור על אזרחים במדינת הפורום – קמה סמכות למדינת הפורום. בקצה השני של הסקאלה, כאשר הנתבע מנהל אתר פסיבי באינטרנט, והמידע בפועל נגיש לאזרחים מכל העולם, אין די בכך כדי להקנות סמכות שיפוט למדינה שבה רק נצפה התוכן מאתר האינטרנט. ובין קצוות הסקאלה מצויים כל אותם מקרים שבהם הנתבע הזר מנהל אתר אינטרנט אינטראקטיבי, שדרכו אזרחים ממדינות זרות יכולים לפעול, יש לבחון את מידת האינטראקטיביות והאופי המסחרי של הפעילות האינטראקטיבי, ועל בסיסה יהיה ניתן לקבוע סמכות שיפוט למדינת הפורום. סקאלת *Zippo* אומצה בפסיקה מאוחרת יותר: *Soma Med. v. Cybersell, Inc.*, 130 F.3d 414 (9th Cir., 1997); *Int'l v. Std. Chtd. Bank*, 196 F.3d 1292 (10th Cir., 1999); *Mink v. AAAA Dev. LLC*, 190 F.3d 333

לא אתיימר להקיף את הפסיקה האמורה, וכשלעצמי איני סבור כי ניתן להסיק כלל אצבע ברור מן הפסיקה שניתן להקיש ממנו אל המשפט הפלילי.³⁹ עם זאת ניתן להבחין כי מקום מושבו של מעלה התכנים ומקום הימצאותו הפיזית של השרת או המחשב שממנו מועלים או משודרים התכנים אינם מחסנים מפני החלת הדין של מדינות אחרות שבהן נחשפו משתמשי אינטרנט לתכנים אלה. מכאן שסמכות השיפוט, גם במישור האזרחי, אינה כפופה להתקשרות אינטרנטית פנים-מדינתית בלבד אלא יכולה בהחלט להתפרש על פעולה אינטרנטית שרק חלקים ממנה מבוצעים במדינה השופטת או עוברים בה.

2. סמכות אכיפה

המצב המשפטי הנוהג (בוודאי במדינות המערב) הוא כי סמכות האכיפה באשר לאיסוף ראיות דיגיטליות במרחב הסייבר מוגבלת לטריטוריה המדינתית. הגבולות המדינתיים מורכבים על המרחב הקיברנטי, וראיה האגורה בשרתים מחוץ לטריטוריה המדינתית – אסורה, ככלל, באיסוף במסגרת חקירה פלילית, אלא אם קיימת הסכמה בין-מדינתית לפעולה אקסטרה-טריטוריאלית. זהו המצב החוקי שעל פיו פועלות רשויות אכיפת החוק במרבית מדינות

(5th Cir., 1999); *ALS Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707 (4th Cir., Amway Corp. כן ראו. 2002); *Toys “R” Us, Inc. v. Step Two, S.A.*, 318 F.3d 446 (3rd Cir., 2003) שם נפסק כי כוונה להשפיע באמצעות האינטרנט ממדינה אחת (שבה יושב הנתבע ושבה ממוקם מחשבו) על אדם המצוי במדינה שנייה מקימה סמכות שיפוט במדינה השנייה. לסקירה נוספת ראו למשל HENRIK SPANG-HANSEN, PUBLIC INTERNATIONAL COMPUTER NETWORK LAW ISSUES 175–257 (2006). כמו כן אציין את פסק הדין של בית המשפט העליון האוסטרלי בתביעת לשון הרע שהגיש איל ההון ג'וזף גוטניק נגד גרסה מקוונת של עיתון אמריקני, שרשומה וממוקמת בשרת בארצות הברית, שפרסם באתר שלו כתבה מכפישה נגדו. אתר האינטרנט "יושב" בשרתים אמריקניים. האתר נצפה בכל העולם, וחלק (קטן) מקוראיו הם אוסטרלים. בית המשפט העליון קבע כי בשל כוונתו של העיתון האינטרנטי להגיע לקהל קוראים רחב באמצעות האינטרנט, יש לראות בפרסום כמתבצע בכל מדינה שבה נצפה, במקרה זה באוסטרליה. ראו *Dow Jones & Co. Inc. v. Gutnick, HCA 56* (2002) (Austl.). פסיקה זו אינה מתיישבת עם הגישה האמריקנית בתיק לשון הרע בעניין *Young v. New Haven Advocate*, 315 F.3d 256 (4th Cir., 2002), שם נפסק כי מהדורה מקוונת של עיתון ממדינת קונטיקט שהועלה לאתר אינטרנט ש"יושב" בשרת בקונטיקט אך נצפה בפועל גם במדינת וירג'יניה, שבה התגורר התובע, אינה מקימה כשלעצמה סמכות שיפוט בוירג'יניה. העובדה שהפרסומות באתר האינטרנט כוונו לתושבי קונטיקט והכתבות בעיתון לא עסקו במכוון בענייני מדינת וירג'יניה – מלמדת שאין להעניק סמכות שיפוט למדינת וירג'יניה.

במשפט הישראלי, ראו ה"פ (מחוזי י-ם) 3137/04 *Ahava (USA) Inc.* נ' ג'. דבליו. ג'י. בע"מ (J.W.G. Ltd.), פ"מ תשס"ג(2) 337 (2004), שם הכריז בית המשפט המחוזי בירושלים על פסק דין אמריקני כאכיף בישראל, ובכך הכשיר למעשה את הקביעה השיפוטית שלפיה אתר אינטרנט ישראלי המציע לרוכשים מכל העולם, לרבות מארצות הברית, לרכוש מוצרי טיפוח של המותג "אהבה", מפר למעשה את זכויות המפיץ האמריקני של המותג. במילים אחרות, בית המשפט הישראלי הכיר בכך שאתר אינטרנט ישראלי הפועל גם אצל הקהל אמריקני מכפיף עצמו לסמכות השיפוט האמריקנית. אין דוקטרינה אחידה וכוללנית בנוגע לכינונה של סמכות שיפוט. קיימת שונות בין כללי סמכות השיפוט במדינות השונות, בין עילות התביעה השונות (סוג ההפרה או העוולה הנטענת) ובין הפרורם האינטרנטי שבו הוצעה ההפרה או העוולה: האם מדובר בפרורם "ציבורי" או "פרטי" ברשת? ראו לעניין זה למשל את *Julia Horne, The Jurisdictional Challenge of the Internet, in LAW AND THE INTERNET* 121 (Lilian Edwards & Charlotte Waelde eds., 2009).

העולם.⁴⁰ אדגים את מגבלת סמכות האכיפה האקסטרטריטוריאליה במרחב הסייבר באמצעות פרשה אמריקנית-רוסית אשר נודעה כפרשת *Gorshkov-Ivanov*. עניינה של פרשה זו בהאקרים

40 ראו: Henry H. Perritt, *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 35–36, 82–90, 114 (1996); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1216–1221 (1998); Jack L. Goldsmith, *Unilateral Regulation of the Internet: A Modest Defense*, 11 EJIL 135, 139–140 (2000); Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL. F. 35, 45–57 (2001); Susan W. Brenner & Joseph J. Schwerha, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMP. & INFO. L. 347, 354–366 (2002); International Bar Association, לעיל ה"ש 1, בעמ' 9–10. לפירוט על החריגה האקסטרטריטוריאליה המוסכמת, ראו פרק 3(ה)(1).

אביא התייחסות פרטנית נוספת למדינות הבאות: בארצות הברית: מדריך משרד המשפטים האמריקני מנחה את גופי התביעה ורשויות החקירה להימנע מחדירה לחומרי מחשב האגורים בשרתים בחו"ל. ההיתר לחדירה מחוץ לטריטוריה יינתן רק במקרה של שיתוף פעולה והסכמה עם המדינה הזרה, או במקרה שהמדינה הזרה נוהגת לאפשר למדינות אחרות לערוך פעולות חדירה לחומרי מחשב שמצויים בשטחה. ראו DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 56–60 (2009), available at <http://www.cybercrime.gov/ssmanual/index.html> (להלן – DOJ Manual).

בבריטניה: סמכות החדירה לחומרי מחשב חלה גם על חירות מרחוק למחשבים, לאו דווקא על חדירה למחשבים התפוסים פיזית בידי המשטרה. כך קבוע ב- Police and Criminal Evidence Act 1984, s. 19(4) כפי שתוקן בתיקון עקיף על ידי ה- Criminal Justice and Police Act 2001, Sch. 2(2), para. 13(2)(a). לכאורה אין הגבלה בחוק זה על מיקומו של המחשב הנחדר מבחינה טריטוריאליה, אולם חלה בעניין זה המגבלה הכללית הקבועה ב- Police Act 1996, s. 30(1) "A member of a police force shall have all the powers and privileges of a constable throughout England and Wales and the adjacent United Kingdom waters". עוד על התפישה הטריטוריאליה ביחס לאיסוף ראיות דיגיטליות ראו במדריך רשויות האכיפה הבריטיות: ASSOCIATION OF CHIEF POLICE OFFICERS, GOOD PRACTICE GUIDE FOR COMPUTER-BASED ELECTRONIC EVIDENCE 13, available at http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf. בהולנד: החוק ההולנדי מתיר חדירה משטרתית לרשת בין מחשבים, שבכללה יותר לרשויות להגיע לכל המחשבים אליהם יש גישה דרך המחשב המקורי, שבעניינו הוצא צו החדירה. עם זאת, ההיתר כאמור מוגבל בתנאי שהמחשבים הנוספים ברשת לא ממוקמים מחוץ לגבולות הטריטוריה ההולנדית. ראו Bert-Jaap Koops, *Cybercrime Legislation in the Netherlands*, in CYBERCRIME AND SECURITY 1, 8 (Pauline C. Reich ed. 2005).

בדנמרק: דנמרק מפרשת את המשפט הבינ-לאומי, כמו גם את שיטת משפטה הפנימית, ככאלה האוסרים על אכיפה מחוץ לתחומי הטריטוריה המדינתית. לפיכך גם בהקשר אינטרנטי נאסר על חדירה או העתקה של חומר מחשב המצוי במחשבים מחוץ לטריטוריה הדנית. ראו SPANG-HANSEN, לעיל ה"ש 38, בעמ' 418–420.

באיטליה: דיני איסוף הראיות הדיגיטליות באיטליה מחייבים את הרשויות לעצור כשהן מגיעות לחומר מחשב המצוי מחוץ לטריטוריה ולפנות למנגנוני שיתוף הפעולה הבינ-מדינתיים, בין שמדובר במנגנון אמנת מועצת אירופה בדבר פשעי מחשב ובין שמדובר במנגנוני עזרה משפטית רגילים (אם הטריטוריה הזרה שבה מצוי חומר המחשב אינה שייכת למדינה שהיא צד לאמנה) ומנגנוני עזרה משפטית וולונטרית לא-פורמלית. ראו Giovanni Ziccardi, *Cybercrime and Jurisdiction in Italy*, in CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY 227, 233–234 (Bert-Jaap Koops & Susan W. Brenner eds., 2008).

בשוודיה: הדגש הוא על מיקומו של השרת, ומיקום מחוץ לטריטוריה השוודית פוסל מניה וביה כל אפשרות לאסוף את הראיה הדיגיטלית בפעולה של הרשות השוודית. ראו GRAHAM J. H. SMITH, INTERNET LAW AND REGULATION 339 (3rd ed., 2002).

בגרמניה: הדעה הרווחת היא שאסורה לרשויות החקירה הגישה לחומרי מחשב האגורים בחו"ל, כאשר בעבר הייתה מחלוקת על שאלת הגישה של החוקרים הגרמנים לחומרי מחשב הפתוחים לעיון כלל הציבור באינטרנט. ראו Nicolai Seitz, *Transborder Search: A New Perspective in Law*

רוסים שסחטו כספים מחברות אמריקניות תוך איום עליהן כי אם לא ישלמו להם, ישביתו את שירותיהם באמצעות מתקפות אינטרנטיות מתוזמנות. לצורך חקירת הפרשה נזקקו חוקרי ה-FBI לחומרי מחשב שנאגרו בשרתי מחשב רוסיים. חוקרי ה-FBI העתיקו בהעתקה סמויה, על דרך של התקשרות ממחשב בארצות הברית לשרת הרוסי, את חומר המחשב הרלוונטי. לאחר מכן ניגשו חוקרי ה-FBI לבית משפט אמריקני וביקשו צו לעיון בחומר שהועתק כאמור. בית המשפט האמריקני נעתר לבקשה. בכך התגברו חוקרי ה-FBI על בעיית איסוף הראיות הדיגיטליות האגורות מחוץ לטריטוריה האמריקנית. לאחר מכן פותו ההאקרים הרוסים לצאת מרוסיה לארצות הברית באמתלת שווא של כינוס בתחום המחשבים, ונעצרו בידי חוקרי ה-FBI.⁴¹

בפרשת *Gorshkov-Ivanov* נאספה הראיה בידי חוקרים אמריקנים משרת רוסי, שופט אמריקני הכשיר את העיון בראיה בשלב החקירה, ולאחר מכן שופט אמריקני הכשיר את השימוש בראיה ודחה טענות של ההגנה לפסלותה. לעומת זאת השלטונות ברוסיה ראו בפעולה האמריקנית משום פגיעה בריבונות הרוסית והוציאו צווי מעצר נגד חוקרי ה-FBI.⁴² פעולתן של הרשויות האמריקניות בפרשת *Gorshkov-Ivanov* הייתה חריגה,⁴³ ובמקרים אחרים של עברייני אינטרנט שפעלו מחו"ל כלפי תושבים ועסקים אמריקניים הייתה הפעולה על פי מגבלת סמכות האכיפה הטריטוריאלית, תוך הסתייעות במנגנוני עזרה משפטית בין-מדינות.⁴⁴

(2004) 7 YALE J. L. & TECH. 23, 34–35. *Enforcement?* מאז שנת 2009, עם הצטרפות גרמניה לאמנת מועצת אירופה בדבר פשעי מחשב, אימצה גרמניה את הכלל שבסעיף 32 לאמנה, שלפיו מותר לחדור לחומרי מחשב האגורים מחוץ לטריטוריה במקרה של חומרים הנגישים לכלל הציבור ובמקרה של הסכמה כדין של המחזיק בחומר המחשב.

בישראל: ראו את עמדת פרקליטות המדינה, כפי שהתקבלה בבית המשפט העליון, כי המדינה מוגבלת מבחינת דיני הסמכות (Jurisdiction) לאסוף חומר משרתי חברת פייסבוק, שכן אלה מצויים מחוץ לטריטוריה הישראלית: בש"פ 6926/12 אדטו נ' מדינת ישראל, פסקה 8 להחלטתו של השופט עמית (פורסם בנוב, 18.10.2012).

41 כך התאפשר לרשויות האמריקניות להתגבר על בעיה נוספת, שאיני דן בה כאן, והיא הבעיה של העמדה לדין של נאשמים שמקום מושבם בחו"ל. בעיה זו מוסדרת באמצעות דיני ההסגרה, ומדינות שונות, כבמקרה זה, משתמשות בכלים לפיתוי נאשמים לעבור ממדינה למדינה על מנת ללכוד אותם בשטחן ללא צורך בבקשת הסגרה.

42 ראו *United States v. Gorshkov*, 2001 WL 1024026 (W.D. Wash., 2001); *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn., 2001). לפרטים נוספים על אופן פעולת חוקרי ה-FBI והתגובה הרוסית, ראו את דיווח מחלקת עברות המחשב במשרד המשפטים האמריקני: <http://www.cybercrime.gov/gorshkovconvict.htm/>; Susan Brenner, "Our" Fourth Amendment..., CYB3RCRIM3 (11.3.2006), available at <http://cyb3rcrim3.blogspot.com/2006/03/our-fourth-amendment.html>; Jack Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. OF CHI. LEG. FORUM 103 (2001), לעיל ה"ש 40, בעמ' 23–28. מעניין לציין כי כאשר המדובר בחקירה המתנהלת במדינה אחת בארצות הברית, ונדרשת חידרה לחומר מחשב האגור בשרת במדינה אחרת בארצות הברית, הרי שהעמדה היא שעל החוקר לבקש את צו החידרה במדינה האחרת ולא במדינתו שלו. ראו את "מדריך השטח" של משרד המשפטים: U.S. DEPARTMENT OF JUSTICE, FIELD GUIDE ON THE NEW AUTHORITIES (REDACTED) ENACTED IN THE 2001 ANTI-TERRORISM LEGISLATION § 216A (2002).

43 כאמור לעיל בה"ש 40, הכלל הוא איסור על חריגה אקסטרה-טריטוריאלית.

44 אציין שני מקרים מוכרים יחסית: המקרה הראשון הוא של Oleg Zezev, שכונה גם "Alex", שפעל מקזחסטן באמצעות האינטרנט וסחט את שירות החדשות של Bloomberg, לאחר שפרץ למחשביה כמה פעמים, בתמורה להפסקת הפריצות. הלה הוזמן למשרדי Bloomberg בלונדון למטרת תשלום דמי הסחטה, נעצר בידי הרשויות הבריטיות והוסגר לארצות הברית. ראו United States Department of Justice Press Release, *U.S. Convicts Kazakhstan Hacker of Breaking Into Bloomberg L.P.'s*

פרשת *Gorshkov-Ivanov* היא בבחינת היוצא מן הכלל המעיד על הכלל, אשר לפיו התפישת הטריטוריאלית, החולשת על סמכות האכיפה הפלילית הבין-לאומית במרחב הפיזי, מועתקת אל המרחב הקיברנטי. ניתן להסביר את תהליך ההעתקה האמור כך: כיוון שבתי המשפט מצאו עצמם נאלצים להתמודד עם תיקים פליליים שנאספו לפתחם, וכיוון שבתי המשפט, בעיקר במדינות המשפט המקובל, הם מוסדות משפטיים שמרניים מטבעם, במובן זה שהם מחויבים להתקדם על דרך של פרשנות, לרבות היקש, תוך החלת תקדימי עבר מחייבים, אך טבעי הוא שהוחל הכלל האוסר על הפעלת סמכות אכיפה אקסטר-טריטוריאלית, מהמרחב הפיזי אל המרחב המקוון.⁴⁵

היות שהעברות במרחב המקוון מתאפיינות בחציית גבולות מדיניים ב"לחיצת כפתור", ואכן בפועל חלק ניכר מהפשעה המקוונת היא בין-מדינתית,⁴⁶ מחריפה בעיית האכיפה הפלילית המדינתית במרחב זה. במישור הפלילי המהותי הרחיבו המדינות בנדיבות את סמכותן לשפוט עברות המתרחשות בכמה "מקומות" באינטרנט ברו־זמנית, ואילו במישור הפלילי הדיוני, כפי שעוד אפרט בהמשך, הפך עניין מיקום הראיות הדיגיטליות למעין עקרון וטו להשבתת חקירות מדינתיות.

ד. מיקוד העדשה בתפישה הטריטוריאלית באשר לדיני איסוף ראיות במרחב הסייבר

1. פירוק התפישה הטריטוריאלית ליסודות

התפישה הטריטוריאלית, כפי שהוצגה ביחס לחקירה הפלילית במרחב הסייבר, ניתנת לפירוק, מבחינה עיונית, לשלושה יסודות: האחד, הראיה הדיגיטלית ניתנת למיקום בתוך המרחב הקיברנטי. הגם שהמידע מיוצג בביטים והוא חסר משקל וגודל, הוא משויך, תפשיתית, לאטומים פיזיים.⁴⁷ הדבר מוביל ללוקליזציה ולטריטוריאליוזציה של המרחב המקוון, שכן אטומים ניתנים למיקום והם מצויים בתוך מרחב טריטוריאלי; היסוד השני הוא כי המקום הוא

Computers and Attempting Extortion (26.2.2003), available at [http://www.justice.gov/usao/Michael Cooper, Bloomberg Tells Trial](http://www.justice.gov/usao/Michael%20Cooper,%20Bloomberg%20Tells%20Trial) .nys/pressreleases/February03/zezevconvict1.pdf כן ראו *Jury of his Part in Taped Sting*, N.Y. TIMES (12.2.2003), at B4 הבריטי Gary McKinnon, שהואשם בפריצה ובגרימת נזק ל-92 מחשבים בשנים 2001–2002, בין היתר למחשבים של הצבא האמריקני. מקינון הסביר כי פרץ למחשבים המסווגים כדי לנסות לחשוף מידע על עב"מים שהסתירו רשויות הביטחון האמריקניות מעין הציבור. הרשויות הבריטיות עצרו את מקינון, והוחל בהליך ממושך ביותר של הסגרה מבריטניה לארצות הברית. ההליך לא הסתיים עד היום. באותו מקרה אספו הרשויות הבריטיות את הראיות מן המחשבים בבריטניה במסגרת בקשה לעזרה משפטית בריטית. ראו: McKinnon v. Government of the United States of America, [2008] UKHL 59 (Eng.); McKinnon v. Secretary of State for Home Affairs, [2009] EWHC 2021 (Eng.)

45 עם זאת בהמשך אציג את הוראותיהן המיוחדות של כמה מדינות, אשר בכל זאת פותחו ביחס לזירה האינטרנטית, ונקבע בהן היתר מסוים לחדירה לחומרי מחשב האגורים מחוץ לטריטוריה המדינתית.

46 ראו למשל Ellen S. Podgor, *Cybercrime: National, Transnational, or International*, 50 WAYNE L. REV. 97, 102–106 (2004). כן ראו דברי ההסבר לאמנת מועצת אירופה בדבר פשעי מחשב: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

47 ההבחנה בין אטומים לביטים, כהגדרתו של ניקולאס נגרופונטי להיות דיגיטלי 17–25 (עמנואל לוטם מתרגם, 1996), מצויה בבסיס התפישה הפיזית של העידן הדיגיטלי בכלל ושל עידן הסייבר בפרט.

המחשב שבו מאוחסנת הראיה הדיגיטלית; היסוד השלישי הוא כי איסוף הראיה מתבצע במקום שבו מאוחסנת הראיה הדיגיטלית. נניח למשל כי איסוף הראיה באינטרנט מתבצע בידי שוטר המתקשר מרחוק אל השרת שבו אגורה הראיה ומעייין בה ממחשבו ומעתיק אותה אל מחשבו. ברי כי פעולת האיסוף בוצעה ממקום מושבו של השוטר, אולם לא זה המקום הקובע כאמור, כי אם המקום שבו אגורה הראיה הדיגיטלית.⁴⁸

שלושת היסודות הללו נלמדים מהפרקטיקה המשפטית, מהחוק החרות, מהפסיקה והבחירה בשימוש מטאפורי בדימוי של מרחב הסייבר כ"מקום", שעליו ארחיב מיד. חיבור שלוש היסודות הללו מבטא את התפישה הטריטוריאלית בהקשר המקוון. שלושם מכוננים את עקרון הווטו הטריטוריאלי באשר לסמכות האכיפה הפלילית במרחב הסייבר, ולפיו אם הראיה הדיגיטלית המבוקשת אגורה בשרת המצוי פיזית בחו"ל, אזי אין סמכות למדינה החוקרת לאסוף את הראיה האמורה בפעולה עצמית (אוניטרלית).

2. מרחב הסייבר כ"מקום"

כאמור לעיל, היסוד הראשון המכונן את התפישה הטריטוריאלית הוא שהמידע במרחב הסייבר ניתן למיקום. להתגבשות יסוד זה תורמת באופן משמעותי התפישה של מרחב הסייבר כ"מקום". תפישה זו, כפי שאראה, היא מטאפורית במידה רבה. כדי להבין מדוע בכוחה של מטאפורה זו להשפיע על התגבשות היסוד הראשון בתפישה הטריטוריאלית אסביר תחילה בקצרה על תפקידה של המטאפורה במשפט.

השימוש במטאפורות הוא, מצד אחד, תהליך קוגניטיבי בלתי נמנע של דפוס החשיבה האנושי, ומצד שני, זהו תהליך מודע של הבניית דפוס הניתוח של הסוגיה הנדונה ולעתים אף הכוונת תוצאת הניתוח. ג'ורג' לאקוף (Lakoff) ומרק ג'ונסון (Johnson) הדגישו שימוש במטאפורות שונות ואת השפעתן הפוליטית והסוציולוגית.⁴⁹ ניתוחים מאוחרים יותר הרחיבו את ההדגמה לחשיבה המשפטית ולהשפעת המטאפורות על התוצאה המשפטית.⁵⁰ בדומה לזה, אף כי ישיר יותר, ניתן להסביר את השימוש באנלוגיות, שבהן מושווית סוגיה משפטית מסוימת לסוגיה שכבר נדונה בעבר. הגם שהמטאפורה והאנלוגיה בשימוש המשפט מייצרות מעין פיקציה, שכן אין הן מתארות את המציאות העובדתית כהווייתה אלא מדמות אותה, אין זאת אומרת כי הן פסולות בשימוש.⁵¹ הפיקציה המשפטית היא כלי שיכול להיות מועיל מאוד

48 הקביעה כי המקום הקובע לעניין סמכות האכיפה האקסטרה-טריטוריאלית בחקירה פלילית באינטרנט הוא מקום אגירתה של הראיה הדיגיטלית המבוקשת נלמדת ממגוון המקורות המפורטים לעיל בה"ש 40.

49 ראו GEORGE LAKOFF & MARK JOHNSON, METAPHORS WE LIVE BY (2nd ed., 2003).

50 ראו את עבודותיו של סטיבן וינטר (Winter): Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 40 STAN. L. REV. 1371, 1832-94 (1988); Steven L. Winter, *Transcendental Nonsense, Metaphoric Reasoning, and the Cognitive Stakes for Law*, 137 U. PA. L. REV. 1105 (1989); Steven L. Winter, *The "Power" Thing*, 82 VA. L. REV. 721 (1996).

51 ראו (1967) 9 LON L. FULLER, LEGAL FICTIONS. כן ראו, בהקשר של מטאפורות לתיאור הפרטיות באינטרנט, את DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 27-28 (2004).

לצורך ניתוח משפטי של סוגיות חדשות ולצורך חיזוי וחיווי דעה משפטית המאפשרת לתכנן צעדים אישיים וכלכליים מראש.

עתה בחזרה אל תפישת המרחב הקיברנטי כ"מקום". המרחב הקיברנטי כתופעה משפטית הוא עניין רחב ומגוון הקשה ל"עיכול" משפטי. לפיכך נדמה כי השימוש במטאפורות בענייני רב במיוחד.⁵² המרחב המקוון תואר כמערב הפרוע,⁵³ אוטוסטרדת המידע,⁵⁴ Cyberspace⁵⁵ ואף כעולם פאודלי.⁵⁶ בין המטאפורות השונות מתקיימת תחרות מטאפורית. חוקרים שונים טענו כי

- 52 לשימוש כללי במטאפורות בהקשר של משפט וטכנולוגיה ראו, David R. Johnson & Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 VILL. L. REV. 487, 489–90 (1993); A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip and the Constitution*, 143 U. PA. L. REV. 709, 860–862 (1995); Dan Hunter, *Cyberspace as a Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 458–472 (2003); Mark Lemley, *Place and Cybespace*, 91 CAL. L. REV. 521 (2003); אברהם נ' טננבוים "על המטאפורות בדיני המחשבים והאינטרנט" *שערי משפט* ד 359, 375–374 (2006); ניבה אלקין-קורן ומיכאל בירנהק "שפת מחשב, שפת משפט" *רשת משפטית: משפט וטכנולוגיות מידע* (ניבה אלקין-קורן ומיכאל בירנהק עורכים) 65, 67–65 (2009). ראו גם ע"מ 3782/12 מפקד מחוז תל-אביב-יפו במשטרת ישראל נ' איגוד האינטרנט הישראלי 15–16 (פורסם בנבו, 24.3.2013).
- 53 ראו Shamoil Shipchandler, *The Wild Wild Web: Nonregulation as the Answer to the Regulatory Question*, 33 CORNELL INT'L L.J. 435, 436 (2000); STUART BIEGEL, *BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE* 4, 13–18 (2001); Alfred C. Yen, *Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1222–32 (2002).
- 54 ראו Clay Calvert, *Regulating Cyberspace: Metaphor, Rhetoric, Reality, and the Framing of Legal Options*, 20 HASTINGS COMM. & ENT. L.J. 541, 542–43, 547–49 (1998); HENRY H. PERRITT, *LAW AND THE INFORMATION SUPERHIGHWAY* (1996); Jonathan H. Blavin & I. Glenn Cohen, *Gore, Gibson; Infobahn או ה-Information superhighway and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary*, 16 HARV. J. L. & TECH. 265, 269–274 (2002).
- 55 מקובל לראות את מקורה של המטאפורה "Cyberspace" בספר מדע בדיוני של ויליאם גיבסון משנת 1984, ראו WILLIAM GIBSON, *NEUROMANCER* (1984). להחלה משפטית של המטאפורה, ראו למשל I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 994–95 (1994); David R. Johnson & David G. Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); David R. Johnson & David G. Post, *The Rise of Law on the Global Network*, in *BORDERS IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE* 3, 12–28 (Brian Kahin & Charles Nesson eds., 1997); Blavin & Cohen; בעמ' 280–275. ג'ולי כהן (Cohen) וברוס קלר (Keller) גרסו כי מטאפורת המרחב המקוון כ-"Cyberspace" היא שגויה. מטאפורת ה-Cyberspace מעודדת התייחסות שגויה, לטענתם, אל המרחב המקוון כמציאות נפרדת. ראו Bruce P. Keller, *The Game's The Same: Why Gambling in Cyberspace Violates Federal Law*, 108 YALE L.J. 1569, 1571 (1999); Julie E. Cohen, *Cyberspace Orin S. Kerr, Criminal Law in Virtual as/and Space*, 107 COLUM. L. REV. 210 (2007) (2008) *Worlds*, 2008 U. CHI. LEG. F. 415, 415–416. קר לא טען כי מטאפורת ה-Cyberspace אינה נכונה, אלא כי היא הפכה עם השנים ללא רלוונטית עוד, עם חדירתו המלאה של האינטרנט לחיי היום-יום, עם השתפרות הקישוריות (Connectivity) והעברת חלק ניכר מפעילות הפנאי והמסחר לאינטרנט. ראו Yen, *לעיל ה"ש* 53, בעמ' 1261–1236.

בריבוי השימוש במטאפורות יש כוח מאזן למניעת עיוותים בהתייחסות המשפטית לסוגיה מסוימת.⁵⁷

סבורני כי בכל הנוגע להקשרנו הנדון, של אכיפה פלילית במרחב הסייבר, תפישת המרחב הקיברנטי כמקום גברה על מרבית המטאפורות האחרות, והיא המוצאת ביטוי במשפט הנוהג ביחס לאכיפה פלילית במרחב הסייבר. מתפישת המרחב הקיברנטי כ"מקום" נגזרים תיאורים מטאפוריים משניים, המתארים פעולות שונות במרחב זה. כך, למשל, אנו נכנסים לאתר אינטרנט מסוים,⁵⁸ אנחנו מקלידים כתובת אינטרנטית, החדירה האסורה לחומר מחשב מתוארת כפריצה למקום, אתר האינטרנט אף נבחן כמקום הנגיש לאנשים עם מוגבלויות ועוד.⁵⁹ מלבד השימוש הלשוני במטאפורות המרחב הקיברנטי כמקום, על נגזרותיה, אדגים עתה כמה ביטויים מעשיים במשפט הישראלי לתפישת המרחב הקיברנטי כמקום בדין הפלילי – הן המהותי והן הפרוצדורלי:

ראשית, הוראת סעיף 23 לפסד"פ דנה בהסמכת הרשות החוקרת לחדור לחומר מחשב במסגרת חקירה פלילית. הסעיף מדבר ב"חדירה", וכפי שהשופט אברהם טננבוים ביאר במאמרו, החדירה היא ל"מקום".⁶⁰ בנוסף, הסעיף מחיל את הוראות פרק החיפוש במקום על הוראות החדירה לחומר מחשב, משמע שהחדירה לחומר מחשב נתפשת כמקרה פרטי של חיפוש במקום.⁶¹

שנית, סעיף 228 לחוק העונשין אוסר על החזקה או ניהול של "מקום משחקים אסורים, או מקום לעריכת הגרלות או הימורים". פרקליטות המדינה הגישה בשנת 2010 כתב אישום בעברות של הימורים באינטרנט, ובין סעיפי האישום יוחסה גם עברה לפי סעיף זה. במסגרת הסדר טיעון הודו הנאשמים בעברה של ניהול מקום משחקים אסורים כאמור.⁶²

57 ראו, בהקשר משפטי כללי (לא-אינטרנטי): MILNER S. BALL, LYING DOWN TOGETHER: LAW, METAPHOR AND THEOLOGY 22 (1985) ובהקשר אינטרנטי ראו Timothy Wu, *Application-Centered*, 85 VA. L. REV. 1163, 1163–1166 (1999), Yen; *Internet Analysis*, 85 VA. L. REV. 1163, 1163–1166 (1999), לעיל ה"ש 53, בעמ' 1209.

58 ראו עניין איגוד האינטרנט הישראלי, לעיל ה"ש 52, בעמ' 16, שם קושר השופט סולברג בין "אתר" אינטרנט לבין תפישת האינטרנט כ"מקום".

59 ראו National Federation of the Blind v. Target Corp., 452 F. Supp. 2d 946 (N.D. Cal., 2006), שם נדונה השאלה אם אתר אינטרנט של חברת שיווק סיטונאי הוא "מקום ציבורי" שיש להנגישו לאנשים עם מוגבלויות, בכלל זה לעיוורים.

60 טננבוים, לעיל ה"ש 52, בעמ' 374–375. כן ראו ת"פ (שלום י-ם) 3047/03 מדינת ישראל נ' מזרחי, פ"מ תשס"ג(3) 769, 786–787 (2004). באותו מקרה דובר באישום בעברה של ניסיון לחדור לחומר מחשב שלא כדין. מדובר בנאשם שהריץ בדיקות port scanning לגילוי פרצות אבטחה באתר האינטרנט לגיוס עובדים של המוסד למודיעין ותפקידים מיוחדים. בית משפט השלום זיכה את הנאשם בטענה כי הבדיקות שערך אינן מתפרשות בהכרח כהתחלה של פעולת חדירה לא מורשה. ערעור המדינה לבית המשפט המחוזי בעניין נדחה (ע"פ (מחוזי י-ם) 8333/04 מדינת ישראל נ' מזרחי (פורסם בנבו, 22.8.2004)). כן ראו מיכאל בירנהק "משפט המכונה: אבטחת מידע וחוק המחשבים" שערי משפט ד 315, 355–357 (2006). וראו עוד את ע"פ (מחוזי ת"א) 71227/01 מדינת ישראל נ' טננבאום, פ"מ תשס"א(2) 595, 604–606 (2002), שם השווה בית המשפט את מעשיו של הנאשם למעשיו של מי שפורץ לביתו של אדם.

61 להרחבה ראו להלן בפרק ד.ב.2.א).

62 ראו ת"פ (מחוזי ת"א) 14974-05-10 מדינת ישראל נ' עובד (פורסם בנבו, 8.9.2011). הנאשמים הודו, לאחר הליך גישור, בכתב אישום מתוקן במסגרת הסדר טיעון שכלל עברה של ניהול מקום לשם

שלישית, בפרשת איגוד האינטרנט הישראלי, במסגרת הדיון בסמכותה של משטרת ישראל להורות לספקיות הגישה לאינטרנט לחסום גישה לאתרי הימורים מקוונים, בחן בית המשפט העליון את השאלה אם אתרי הימורים יכולים להיחשב "מקום משחקים אסורים או מקום לעריכת הגרלות או הימורים", כלשון סעיף 229(א)(1) לחוק העונשין.⁶³ אף על פי שדעת הרוב בפסק הדין דחתה את עמדת המדינה, כי קמה הסמכות להורות לספקיות הגישה לאינטרנט לחסום גישה לאתרי הימורים, הן שופטי הרוב והן שופט המיעוט הסכימו כי אתרי הימורים הם בבחינת "מקום".⁶⁴

רביעית, בכמה החלטות שיפוטיות בעברות של חדירה לחומר מחשב שלא כדין, עברה על סעיף 4 לחוק המחשבים, התשנ"ה–1995 (או סעיף 5 לחוק, אם החדירה נעשתה כדי לעבור עברות אחרות), הושווה החודר לחומר המחשב למי שפורץ לביתו של אדם או שגונב את רכושו.⁶⁵

חמישית, בעניינו של משה הלוי שהוזכר לעיל (עברת העלבת עובד ציבור על דרך של פרסום תמונת המפכ"ל לשעבר עם מדים נאציים),⁶⁶ ביקשה התביעה, לאחר תחילת המשפט, לתקן את

הימורים אף שדובר באתר אינטרנט. היות שדובר בהרשעה במסגרת הסדר טיעון, לא נדונה שאלת האינטרנט כמקום בבית המשפט. גם בערעור הנאשם על חומרת עונשו לא נדונה סוגיית האינטרנט כ"מקום". הנאשם הגיש גם בקשה לדיון נוסף, שם העלה בכתבי טענותיו את הטענה כי הרשעתו הייתה למעשה פסולה, שכן יוחסה לו עברה תלוית-מקום, ואילו אתר האינטרנט איננו "מקום", אולם מטעמים פרוצדורליים, של עילות הכניסה לדיון נוסף, נדחו הטענות. ראו דנ"פ 4409/12 עובד נ' מדינת ישראל (פורסם בנבו, 10.6.2012).

63 ראו עניין איגוד האינטרנט הישראלי, לעיל ה"ש 52. דנתי בפסיקה זו גם לעיל בפרק 2(ד)(4), כאשר הצגתי את האכיפה המגננתית-הכופה כחלופה לאכיפה הפלילית המדינתית באינטרנט.

64 ראו לעיל, בעמ' 14–20 לפסק דינו של השופט סולברג, בדעת המיעוט, ובעמ' 31 לפסק דינו של השופט פוגלמן, כותב דעת הרוב. הנמקה מרכזית של השופט סולברג בקביעתו שאתרי הימורים הם בבחינת "מקום" היא כי דיני העברות משופעים במונחי "מקום". על כן מתחייב, לשיטתו, כצורך מעשי, לראות באינטרנט "מקום", שאם לא כן עברות רבות לא תוחלנה על הפלטפורמה האינטרנטית, והמשפט הפלילי יודר מן המרחב הווירטואלי. נאמן להנמקה זו השופט סולברג מסיק (בעמ' 15 לפסק הדין) כי הגם שהדיון לא עסק בשאלת האינטרנט כ"מקום" מחוץ לגבולות עברות הימורים האסורים, הרי ש"הכלל צריך להורות כי אינטרנט בא בגדרו של 'מקום'". מהתייחסותו הקצרה של השופט פוגלמן ניתן להסיק כי אינו מסתייג מההנמקה ומהמסקנה של השופט סולברג. להשלמת התמונה יצוין כי הטעם המרכזי לקביעה כי משטרת ישראל נעדרת סמכות להורות לספקיות השירות על חסימת גישה לאתרי הימורים, הוא כי הסעיף שעליו ביקשה המשטרה להסתמך אינו מדבר על האפשרות להטיל את משימת "סגירת המקום" על צד שלישי תמים כגון ספקיות הגישה לאינטרנט.

65 כך היה בפרשת ה"אנגליזר", עניינו של האקדמי אהוד טננבאום שהתפרסם בכך שחדר שלא כדין בין היתר למחשבי נאס"א בארצות הברית, לאתר הכנסת ולחשבון דוא"ל של צעירה. השופטת ברלינר, בדונה בערעורה של המדינה על קולת עונשו של טננבאום, כתבה: "...חדירה למחשב היא פריצה לכל דבר ועניין. אין הבדל בין מי שמטפס כדי לפרוץ לבניין, לבין מי שמוצא את הדרך לפרוץ למחשב"; כן כתבה: "המשיב, אשר פעל, כאמור, בעצמו והפעיל גם אחרים, הן בארץ והן בעולם, איננו שונה ממי שעומד בראש כנופיה הפורצת לבתייהם של אנשים". ראו ע"פ (מחוזי ת"א) 71227/01 טננבאום, לעיל ה"ש 60, בעמ' 605 ו-612. בקשת רשות ערעור של טננבאום לבית המשפט העליון נדחתה: רע"פ 5147/02 טננבאום נ' מדינת ישראל (פורסם בנבו, 17.6.2002). לחזרה על אנלוגיית הפריצה לבית, ראו גם ת"פ (מחוזי ת"א) 40250/99 מדינת ישראל נ' בדר, בפס' 6 (פורסם בנבו, 13.11.2001); ת"פ (שלום ת"א) 5476/03 מדינת ישראל נ' יוסף (פורסם בנבו, 2.3.2004).

66 ראו לעיל טקסט לה"ש 29–30.

כתב האישום על דרך של ציון כתובת אינטרנט נוספת שבה פרסם הנאשם את התמונה. הנאשם התנגד לתיקון האמור בטענה כי מדובר בשינוי המקום של ביצוע העברה, וכי שינוי שכזה משפיע על אופן ניהול הגנתו, כיוון שניהל את הגנתו בהסתמך על ייחוס מקום עברה מסוים ולא אחר, וכיוון שכיום אין באפשרותו להפיק ראיות לתועלת הגנתו מה"מקום" החדש בשל חלוף הזמן והתנדפות הראיות או השתנותן. בית המשפט קיבל את טענת הנאשם ודחה את בקשת התיקון האמור.⁶⁷

שישית, נאום אבו סלים, אימאם במסגד בנצרת, הורשע בין השאר בעברה של תמיכה בארגון טרוריסטי, בין היתר באמצעות האינטרנט, כאשר עברה זו מחייבת אקט של "פרסום". הגדרת ה"פרסום" מחייבת כי הדברים יופצו ב"מקום ציבורי", ונפסק כי אתרי האינטרנט שבהם הופצו הפרסומים מושאי האישומים הם "מקום ציבורי".⁶⁸

אם לסכם עד כאן, תפישת המרחב הקיברנטי כ"מקום" רווחת, בוודאי בדין הפלילי שבו עסקינן. האם תפישת מרחב הסייבר כ"מקום" היא מטאפורית או שמא היא אינה אלא תיאור מציאות מדויק? מרבית החוקרים שדנו בתפישת המרחב המקוון כמקום הסכימו כי מדובר בתיאור מטאפורי של המרחב המקוון, במובן זה שהוא אינו "מקום" במובנו הפיזי.⁶⁹ כנגדם, ג'ולי כהן חלקה על עצם הקביעה שתפישת המרחב המקוון כ"מקום" היא מטאפורית. לטענתה, המרחב המקוון אינו "מקום" שונה מן העולם הפיזי מבחינה פרקטית. בפועל כמעט תמיד קיימת זיקה בין העולם המקוון לבין העולם הממשי, ולכן בפועל המרחב המקוון הוא מקום ואינו מקום נפרד מהמרחב הפיזי.⁷⁰ כשלעצמי, אני סבור כי גם אם נקבל את טענותיה של כהן בדבר הזיקה בין המרחב הקיברנטי למרחב הפיזי כנכונות, עדיין אין בהן כדי לשנות את העובדה שהמרחב הקיברנטי עצמו אינו "מקום" במובנו הפיזי.⁷¹ המידע הוא נזיל, נמצא בתנועה, מתפרק ל"חבילות" (packets) ומחובר מחדש,⁷² מבוזר על פני מחשבים שונים וספקיות שירות שונות, נמצא ב"ענן" באופן שמיקומו לא ידוע, משוכפל לכמה אתרים או שרתים באופן כזה שלעתים קרובות הוא אינו בשליטה של "בעלי" המידע. מטעמים אלה ואחרים, שתלויים בארכיטקטורת המרחב המקוון, נראה כי אי אפשר לראות במרחב המקוון "מקום" במובנו הפיזי המקובל. לפיכך זיקות בין המרחב המקוון למרחב הפיזי אין בהן כדי להפוך את הרשת למקום. ניתן להוסיף ולטעון מכיוון אחר כי התפתחות העולמות הווירטואליים (Virtual worlds), כדוגמת Second Life, המתיימרת לדמות מציאות תלת־ממדית מלאה,⁷³ מחזקת מכיוון אחר את העמדה

67 ראו ת"פ (שלום חי') 1826/08 מדינת ישראל נ' הלוי (פורסם בנבו, 13.10.2010).
 68 ראו ת"פ (שלום נצ') 12629-11-10 מדינת ישראל נ' אבו סלים, בפס' 29–56 (פורסם בנבו, 1.4.2012).
 69 ראו למשל Hunter, לעיל ה"ש 52; Lemley, לעיל ה"ש 52; טננבוים, לעיל ה"ש 52.
 70 ראו Cohen, לעיל ה"ש 55.
 71 לסיג העלה טענה כי המונח "מקום" אינו חייב להיות תלוי בממד פיזי ויכול להיות תלוי בממד חווייתי. על פי טענה זו, כשאנשים חווים חוויות באינטרנט על בסיס קבוע וחוזר, הם נכנסים, כל אימת שהם מתחברים לאינטרנט, ל"מקום". ראו Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. (1996) 1403.
 72 ראו התייחסותי לעיל בפרק ב טקסט לה"ש 56–57, וכן ראו להלן בנספח א (רקע על ארכיטקטורת האינטרנט).
 73 העולמות הווירטואליים אף מפעפעים לתוך העולם האמתי. כך, למשל, ניתן להפיק רווחים כלכליים ממשיים במסגרת פעילויות שונות בעולמות הווירטואליים. לסקירה רחבה על הנושא ראו GREG LATOWSKA, *VIRTUAL JUSTICE: THE NEW LAWS OF ONLINE WORLDS* (2010).

שהמרחב המקוון הוא אכן מקום, ולא רק ברמה המטאפורית. גם טענה זו ראויה להידחות, שכן אחרי הכול העולם הווירטואלי אינו בעל מאפיינים שווים לאלה של העולם האמתי, ודי לציין כאן את הנימוק של אורין קר (Kerr) בהקשרנו, כי העולם הווירטואלי חוקיו מעוצבים ונשלטים בידי האדמיניסטרטור, שלא כמו בעולם האמתי.⁷⁴

בהנחה שהמרחב המקוון אינו באמת "מקום", מתבקשת השאלה אם השימוש במטאפורת ה"מקום" הוא עניין דטרמיניסטי, או שמא הוא ניתן לשינוי. השימוש במטאפורות ובאנלוגיות כמתודת חשיבה וניתוח הוא כנראה עניין יסודי, טבעי ואינו ניתן לשינוי.⁷⁵ מגבלות השפה, כמו גם מגבלות המחשבה, מחייבות התבססות על הקיים על מנת להבין את החדש. דפוס החשיבה האנושית הם אינקרימנטליים, ולפיכך עליהם להתבסס על תקדימים, בדומה להתקדמות המשפט המקובל. אם כך, ברי כי החשיבה המשפטית על סוגיות חדשות תרבה במטאפורות. עם זאת אין זאת אומרת כי המטאפורה המסוימת שנבחרת לייצג נושא מסוים היא עצמה אינה ניתנת לבחינה, לערעור ולשינוי. מרק למלי (Lemley) טען ככלל כי אין לקבל את המטאפורות השכיחות בנוגע למרחב הסייבר כעניין דטרמיניסטי. בין היתר דן למלי במטאפורת המרחב הקיברנטי כמקום. לשיטתו, ניתן לפתח חשיבה ביקורתית על המטאפורות השגורות בנוגע למרחב הקיברנטי, להאיר את מגבלותיהן ולהיטיב בכך את הפרספקטיבה המשפטית על המרחב.⁷⁶ דפוס החשיבה הביקורתי על מטאפורות במרחב הקיברנטי ניתן לשיטתו לתיאור כדלקמן: איתור המטאפורה בשלב ראשון, הצבעה על השגיאה שבמטאפורה בשלב השני, ניתוח השלכות השגיאה בשלב השלישי וחיפוש חלופה בשלב האחרון. מלבד זאת, על פי קו הטיעון של למלי, יש לראות בשימוש במטאפורות משום תהליך דינמי: מטאפורה יכולה להחליף מטאפורה אחרת. החלפת מטאפורות יכולה לבטא שינויים בתפישה המשפטית של המרחב הקיברנטי.

עד כאן הראיתי שלמעשה תפישת המרחב המקוון כ"מקום" היא מטאפורית, וכי ההיזקקות למטאפורות כדי לנתח את המרחב הקיברנטי מבחינה משפטית – אינה דטרמיניסטית, וניתן בהחלט לבקר את השימוש במטאפורה זו, ובמידת הצורך – להציע להחליף את המטאפורה בתפישות אחרות. מכאן מתבקשת השאלה הבאה: האם מטאפורת המרחב הקיברנטי כמקום ראויה או שמא יש לזנוח אותה? דן האנטר (Hunter) טען כי תפישת המרחב המקוון כ"מקום" מובילה לתפישה של המידע כ"מקום" עם "בעלות" של מחזיק המידע, ובעקבות תפישה זו תיווצר מגמה של סגירת האינטרנט ומניעת זרימה חופשית של מידע.⁷⁷ כך עלול להיווצר אפקט מצנן על התפתחות האינטרנט כמקור חופשי של זרימת מידע, תקשורת הדדית ושיתוף. האנטר

74 Kerr, לעיל ה"ש 55, בעמ' 417.

75 איבור ריצ'רדס (Richards) טען כי איננו מסוגלים לנהל שיחה בת יותר משלושה משפטים אשר לא תכלול שימוש במטאפורות. ראו IVOR A. RICHARDS, THE PHILOSOPHY OF RHETORIC 92 (1936).

76 ראו Lemley, לעיל ה"ש 52. למלי הציג סיטואציות שבהן הצליחו בתי המשפט להתנתק ממגבלות מטאפורת ה"מקום" וגילו גישה מחשבתית פרגמטית מעט יותר, המתאימה למאפייניו של המרחב הקיברנטי. ראו גם: Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561 (2001). מאמר זה היה בין הראשונים לבחון את היחס בין מטאפורות ואנלוגיות שגויות לבין דיני האינטרנט, עוד קודם לעבודותיהם של למלי והאנטר (שאת עבודתו אסקור בהמשך). אורורק בחנה את האנלוגיות – אתר אינטרנט כספר ואתר אינטרנט כקניין מוחשי – בהקשר של דיני המסחר האלקטרוני. גם היא התייחסה אל אנלוגיות אלה כעניין ברישיוני ולא כעניין נתון.

77 ראו Hunter, לעיל ה"ש 52.

ניתח בין היתר בהרחבה גם פסיקה במישור הפלילי מהמשפט האמריקני הדנה בעברה של חדירה לחומר מחשב שלא כדין, ולטענתו עולה כי במישור הפלילי יש נטייה לראות באתר האינטרנט, בתיבת הדוא"ל וכד' "מקומות" באינטרנט.⁷⁸ מן הניתוח של האנטר ניתן להסיק בבירור שגם בכל הנוגע לסמכויות האיסוף של הרשות החוקרת, התפישה היא כי הרשות נכנסת ל"מקומות" שונים במרחב המקוון במסגרת חקירתה. דניאל בן-אוליאל (Benoliel) טען שראוי נורמטיבית לשמר את מטאפורת ה"מקום" במרחב הסייבר, אם כי יש לערוך הבחנה בין מקומות שונים במרחב זה – מקומות פרטיים מחד גיסא ומקומות ציבוריים מאידך גיסא.⁷⁹ להבחנה זו יכול שתהיה השלכה ניכרת על דיני איסוף הראיות במרחב הסייבר מבחינת עצמת ההגנה החוקתית שתוענק לחשוד ולצדדים שלישיים נגד האינטרס של הרשות החוקרת. כנגד האנטר ובן-אוליאל טענתי בפרק זה היא בדבר השלכה נוספת של מטאפורת המרחב הקיברנטי כמקום, והיא כי המטאפורה הובילה להשלטת התפישה הטריטוריאלית באשר לאכיפה הפלילית במרחב הקיברנטי, תפישה אשר חוסמת את דרכן של המדינות לאכיפה יעילה של הדין הפלילי במרחב.

3. על איזה "מקום" מדובר?

הראיתי לעיל כי מטאפורת המרחב הקיברנטי כ"מקום" רווחת בדיני המחשבים. ממסקנה זו מתבקשת השאלה הנגזרת הזאת – על איזה "מקום" מדובר: האם מדובר ב"מקום" אחד, היינו האם כל פעולה במרחב הסייבר או כל מידע במרחב זה ניתן לשייך למקום אחד קונקרטי? לחלופין, האם נכון לדבר על כמה מקומות בו-זמנית? כאשר למשל מתרחשת התקשרות בין שני משתמשי אינטרנט – האם נכון לשייך את ההתקשרות לשני מקומות, לפי מיקומם של שני משתמשי האינטרנט? האם נכון לשייך את ההתקשרות לכל המקומות שבהם עבר המידע (למשל באחסון זמני או קבוע בשרת מסוים)? כאשר מדובר על פרסום ברבים באינטרנט: האם נכון לשייך את הפעולה לכל העולם, או לכל המקומות שבהם נצפה הפרסום? השימוש במטאפורת האינטרנט כ"מקום" הוא הקשרי: בהקשרים שונים מתקבלות מסקנות שונות בדבר סוג ה"מקום" המיוחס. הראיתי לעיל כי בכל הנוגע לדיני הסמכות המהותית (תחיקה ושיפוט), התפישה היא שמרחב הסייבר הוא רב-מקומי וכולל הן את מקום יציאת המידע, המגלם את העברה, והן את כל המקומות שאליהם הגיע המידע האמור.⁸⁰ בכל הנוגע לדיני סמכות השיפוט המקומית בתביעות אזרחיות הציגה הפסיקה בישראל עמדה שלפיה

78 ראו שם, בעמ' 475–483.

79 ראו Daniel Benoliel, *Law, Geography and Cyberspace: The Case of On-Line Territorial Privacy*, 23 CARDOZO ART & ENT. L.J. 125 (2005).

80 ראו למשל, בהקשר של הימורים באינטרנט, את עניין *W.I.G.C.*, לעיל ה"ש 30; עניין קרלטון, לעיל ה"ש 28. בהקשר של עברת פרסומי תועבה, ראו Yuval Karniel & Haim Wismonsky, *Pornography, Community and the Internet*, 30 RUTGERS COMP. & TECH. L.J. 105, 146–151 (2004); עניין *Thomas*, לעיל ה"ש 31. בהקשר של עברות איסור על הכחשת השואה והסתה לגזענות, ראו עניין *Yahoo!*, לעיל ה"ש 32, בהקשר של עברות מרמה באמצעות האינטרנט, ראו ב"ש (מחוזי ים-9037/09 היועץ המשפטי לממשלה נ' עייש (פורסם בנבו, 16.6.2010). בהקשר של דיני זכויות יוצרים באינטרנט ומידע האגור בזיכרון מטמון של ספקי גישה לאינטרנט, ראו Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers, [2004] 2 S.C.R. 427 (Ca.).

ההתנהגות ביסוד התביעה מתבצעת בכל מקום בארץ, או לפחות בכל המקומות שבהם נצפה המידע הרלוונטי המקים את ההתנהגות האמורה.⁸¹ לעומת זאת בכל הנוגע לסמכות לאיסוף ראיות דיגיטליות בחקירה פלילית, כפי שהראיתי לעיל בפרק 3(ג), ה"מקום" הקובע הוא מקום הימצא הראיה ולא מקום ביצוע העברה או מקום מעברו של המידע מושא החקירה. במילים אחרות, ה"מקום" הקובע הוא מקום אחד בלבד. ה"מקום" נתפש ככזה המצוי בריבונותה של מדינה מסוימת, ועל כן גישה אל ה"מקום" האמור מחוץ לגבולותיה של אותה מדינה, ללא הסכמתה, תהיה פעולה אקסטר-טריטוריאלית אסורה.

כאמור, השימוש במטאפורת האינטרנט כ"מקום" הוא הקשרי. כפועל יוצא מכך, ניתן לגזור כמה מסקנות הרלוונטיות להמשך הדרך: האחת, מטאפורת ה"מקום" היא גמישה, ועל כן ניתן להציע מובנים שונים ואף חדשניים למונח "מקום". כך למשל דייוויד ג'ונסון ודייוויד פוסט הציעו לתפוש את האינטרנט כ"מקום" אחד נפרד מהמרחב הפיזי.⁸² אנה מריה בלסנו (Balsano), קתרין היבן (Heaven) ואחרים הציעו לתפוש את האינטרנט כ"מקום" שהוא נחלת הכלל, בדומה לחלל החיצון, הים הפתוח או אנטארקטיקה;⁸³ השנייה, בביקורת על התפישה הטריטוריאלית

81 ראו למשל רע"א 530/12 יעקובוביץ' נ' זיאס (פורסם בנבו, 28.3.2012); בש"א 2267/12 פרל נ' קבוצת אייזנברג נדל"ן (פורסם בנבו, 4.4.2012); בש"א (שלום ק"ג) 884/02 לנדאו נ' חסון (פורסם בנבו, 1.5.2002); בש"א (מחוזי י-ם) 2841/03 רעות אלקטרוניקה ורכיבים בע"מ נ' מראות אימאג' בע"מ (פורסם בנבו, 14.12.2003); ת"א (שלום ת"א) 32786/06 לבבי נ' דראי (פורסם בנבו, 5.10.2006); ת"א (מחוזי חי') 27608-04-11 הטכניון – מכון טכנולוגי לישראל נ' Google Inc (פורסם בנבו, 28.4.2011); ת"א (מחוזי נצ') 27593-09-12 קידי-קיט י.ד.ע בע"מ נ' שטרומן (פורסם בנבו, 29.11.2012). ראו גם ב"ש (שלום י-ם) 8033/06 שטיינברג נ' לוי (פורסם בנבו, 10.4.2007), שם העיר בית המשפט כי האינטרנט הוא חסר מקום, אך הסיק אופרטיבית כי סמכות השיפוט באשר לפעולות המתבצעות בו היא כלל-מדינתית, בכפוף למקרים שבהם מנוצל לרעה עניין הסמכות הכלל-ארצית בידי תובע, ונוצר מצב קיצוני של פורום לא נאות. מנגד, ראו בש"א 6659/05 (שלום י-ם) המכרז של המדינה בע"מ נ' אבו הצירה (פורסם בנבו, 30.11.2005), ניסה בית המשפט לייחד את מקום ביצוע המעשה מושא התביעה למקום שבו נרשם התובע, משתמש האינטרנט, לשירותי הנתבעת, בעלת אתר האינטרנט שאליו גלש התובע. ראו עוד לעניין זה את אסף טבקה "על הדבש ועל העוקץ": סמכות השיפוט המקומית בתביעות אינטרנט" הפרקליט נב 365 (2013).

82 Johnson & Post, לעיל ה"ש 55.

83 המאפיין את אנטארקטיקה, הים הפתוח או החלל החיצון הוא שהם חופשיים מריבונותן של המדינות. הם אינם נתונים לסמכותה הבלעדית של שום מדינה (Terra nullius). ראו United Nations Convention on the Law of the Sea, art. 87, 89–90 (1982). אמנת דיני הים מעגנת את עקרון אי-הריבונות בים הפתוח ומדגישה עקרונות של חופש השימוש בים הפתוח, חופש המעבר בו, הנחת כבלים תת-מימיים, דיג בו ומעבר באוויר שמעליו. ראו עוד קודם לכן באשר לים הפתוח: Convention on the High Seas, art. 2 (Geneva 1958). ראו באשר לחלל החיצון: Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, art. 2 (1967). ראו, בדומה, גם ביחס לאנטארקטיקה, שם ישנן מדינות בעלות אינטרסים ביבשת, אולם מוסכם כי אין היא בריבונות אף מדינה: Antarctic Treaty, art. 4 (Washington, 1959). כן ראו Richard B. Bilder, *Criminal Conduct in Antarctica*, 52 VIRGINIA L. REV. 231 (1966). להצעות להמשגת האינטרנט כמקום שהוא בבחינת נחלת הכלל, ראו Anna Maria Balsano, *An International Legal Instrument for Cyberspace? A Comparative Analysis with the Law of Outer Space*, THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 127 (UNESCO Pub. 2000); Catherine Heaven, *Note, A Proposal for Removing Road Blocks from the Information Superhighway by Using Integrated International Approach to Internet Jurisdiction*, 10 MINN. J. GLOBAL TRADE 373, 390–400 (2001). בלסאנו הציעה להחיל את העקרונות שבאמנה הבין-לאומית

בנוגע לחקירה הפלילית במרחב הסייבר, אין הכרח לתקוף את עצם השימוש במטאפורה של האינטרנט כ"מקום" אלא ניתן להצביע על השגיאה באופן יישום המטאפורה בסיטואציה החקירתית.⁸⁴ מכאן שאין הכרח להכריע בשאלות שהצגתי לעיל: האם מטאפורת האינטרנט כ"מקום" היא מטאפורית או שמא היא בבחינת תיאור מציאות? האם השימוש במטאפורה הוא דטרמיניסטי או לא? השאלה הרלוונטית יותר היא בדבר אופן יישום המטאפורה או אופן בחירת סוג המקום בהקשר של חקירה פלילית במרחב הסייבר.

4. מבחן מקום הימצא הראיה ככלל וטו בחקירות פליליות במרחב הסייבר

כפי שניתן לראות מפירוק התפישה הטריטוריאלית ליסודותיה, הרי שמבחן מקום הימצא של הראיה גוזר כיום את שאלת סמכותה של המדינה החוקרת לאסוף את הראיה הדיגיטלית במסגרת חקירה פלילית. כיוון שהפעילות המקוונת כוללת ביצוע פעולות ואגירת מידע במחשבים המצויים פיזית במדינות זרות, וכיוון שמשמעות הדבר היא שאין סמכות אכיפה בין-לאומית כלפי המידע המצוי במחשבים במדינות זרות, הרי שסוגיית היעדר סמכות האכיפה הבין-לאומית הופכת בפועל לכלל וטו של המשפט הבין-לאומי, המסכל חקירות פליליות מדינתיות במרחב הסייבר.⁸⁵ נוצר אפוא צורך פרקטי מוגבר של רשויות אכיפת החוק לערער על כלל הווטו האמור.

מדוע, מבחינה משפטית-דיונית, הפך עניין סמכות האכיפה הבין-לאומית לכלל וטו המנטרל חקירות פליליות? התשובה לכך נעוצה במשמעות הפנימית של היעדר סמכות בין-לאומית, ולא דווקא במשמעות הבין-מדינתית של הטענה. מנקודת מבט של המדינה כלפי חוץ, משמעות הפרתם של כללי סמכות האכיפה היא עימות דיפלומטי עם המדינה הזרה הטוענת לפגיעה בריבונותה ואף העמדה לדין של החוקרים מהמדינה הפוגעת, אך בכך כשלעצמו אין כדי לנטרל את הליך החקירה הפלילית. ברם נוסף על האמור, מנקודת מבטה של המדינה כלפי פנים, טענת היעדר סמכות אכיפה בין-לאומית, ככל טענת היעדר סמכות עניינית, יכולה להוביל לבטלות ההליך כולו. הטענה אף זוכה במשפט הפנימי למעמד מיוחד: היא יכולה לעלות בכל שלב של הדיון המשפטי, אפילו בערעור בלבד ואפילו ביזמת בית המשפט עצמו (גם אם מדובר בשיטת

העוסקת בחלל החיצון לדיני האינטרנט. היבן הציע ליישם את העקרונות של האמנות המסדירות את הפעילות בחלל החיצון, אנטארקטיקה והים הפתוח לאינטרנט. כן ראו Darrel C. Menche, *Jurisdiction in Cyberspace: A Theory of International Law*, 4 MICH. TELECOMM. TECH. L. REV. 69 (1997); Kevin A. Meehan, *Note, The Continuing Conundrum of International Internet Jurisdiction*, 31 B.C. INT'L & COMP. L. REV. 345, 355-365 (2008); Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 749-759 (2003), אשר הציע להחיל את דין אנטארקטיקה, הים הפתוח והחלל החיצון גם על תחום שמות המתחם ברשת. תפישת האינטרנט כמקום שהוא בבחינת נחלת הכלל לא הוכרה בפועל, והיא נותרה בבחינת רעיון עיוני המבטא גישה מהפכנית ליחס שבין המשפט לאינטרנט. על כן אין הכרח להכריע בשאלות שהצגתי לעיל בפרק ג.ד.2: האם מטאפורת האינטרנט כ"מקום" היא מטאפורית או שמא היא בבחינת תיאור מציאות? האם השימוש במטאפורה הוא דטרמיניסטי או לא? השאלה הרלוונטית יותר היא בדבר אופן יישום המטאפורה, או אופן בחירת סוג המקום, בהקשר של חקירה פלילית באינטרנט.

כפי שהצגתי בפרק ב, הביקורת המעשית הזאת עומדת גם בבסיס הטיעון – שאותו דחיתי – שלפיו שיטת האכיפה של עברות פליליות במרחב הסייבר צריכה להשתנות, בין בשינוי שיטת האכיפה ובין בשינוי זהות הגורם האוכף.

משפט אדוורסרית).⁸⁶ טענת היעדר סמכות אכיפה בין-לאומית היא אפוא בעלת מעמד גבוה ביותר במשפטה הפנימי של המדינה.⁸⁷

כיצד אפוא יכולה המדינה לפעול כיום כאשר מתעורר צורך חקירתי באיסוף ראיה האגורה בשרתים מחוץ לטריטוריה המדינתית? הדרך האחת תהיה פנייה למנגנון של עזרה משפטית. קיימים מנגנונים מיוחדים לעזרה משפטית המתייחסים במפורש לראיות דיגיטליות, ובראשם אמנת מועצת אירופה בדבר פשעי מחשב (Convention on Cybercrime) שנחתמה בכודפשט בשנת 2001⁸⁸ ומנגנון העזרה המשפטית של מדינות ה-G8.⁸⁹ אמנם מנגנונים אלה נועדו לטפל באופי הטרנס-מדינתי של העברות הפליליות במרחב הסייבר, אולם בה בעת הנחת העבודה, שהיא חלק אינהרנטי של פעולה במישור המשפט הביין-לאומי ההסכמי, היא שהאכיפה הפלילית היא עניין למדינה, וכי נקודת המוצא היא שמירה על השוויון הריבוני (Sovereign equality) של המדינות.⁹⁰ מכאן שהפעולה במישור ההסכמי הביין-לאומי משעתקת את התפישה הטריטוריאלית ביחס לאכיפה הפלילית במרחב הסייבר.

דרך שנייה שבה יכולה המדינה להתמודד עם מגבלת סמכות האכיפה הביין-לאומית היא פנייה בבקשה לפתיחה בחקירה מקומית במדינה הזרה, בתנאי שמדובר בעברה גם על פי דיניה של אותה מדינה שבה אגורה הראיה הדיגיטלית. תיתכנה שתי תוצאות חלופיות לפתיחה בחקירה כאמור: (א) המדינה הזרה תפעל להעמדה לדין בגין המקרה הנחקר; (ב) המדינה הזרה תחליט לסגור את תיק החקירה ותשקול להעביר את ממצאי החקירה למדינה שבה נפתחה החקירה המקורית. וכך, מתוך שלא לשמה בא לשמה, והמדינה שפתחה ראשונה בחקירה תקבל את הראיה הדיגיטלית שנדרשה לה מחו"ל.

דרך שלישית להתמודדות המדינה עם מגבלת סמכות האכיפה הביין-לאומית היא פנייה לעזרה משפטית שלא על פי מנגנון פורמלי אלא על סמך רצונה הטוב של המדינה הזרה. יש לזכור כי מנגנוני העזרה המשפטית הפורמליים אינם שוללים עזרה משפטית לא-פורמלית. זו תמיד אפשרית במסגרת יחסים בין מדינות.⁹¹

לטעמי, הדרכים האלה רחוקות מלספק מענה הולם לבעיית האקסטרטריטוריאליות המובנה בחקירות פליליות במרחב הסייבר. כל המסלולים שמנתי לעיל מניחים כי המדינה הזרה תיאותר פעולה עם פנייתה של המדינה החוקרת. בפועל שיתוף הפעולה לא יתקיים בין מדינות שאינן ביחסי שלום, לרוב המדינה הזרה לא תשתף פעולה אם המעשה אינו נחשב לעברה פלילית על פי דיניה, או כאשר עצמת החשד המצדיק פתיחה בחקירה אינו על פי הסטנדרט

86 ראו, למשל, Alex Lees, *The Jurisdictional Label: Use and Misuse*, 58 STAN. L. REV. 1457, 1458–1460 (2006).

87 הטענה עשויה לעלות במסגרת ההליך המשפטי, ככל שהרשות החוקרת תבקש צו שיפוטי אשר יסמך אותה לביצוע פעולת איסוף מסוימת. הדיון בטענה יכול שייבחן בבית המשפט בדיון במעמד צד אחד בנוכחות נציג הרשות החוקרת, במסגרת השגה (עיון חוזר או ערר) של הנמען לצו השיפוטי על ההוראה המסמיכה, ואולי אף במסגרת שלב הגשתה של הראיה במסגרת התיק העיקרי.

88 לנוסח האמנה המלא ולפירוט המדינות החתומות על האמנה, ראו ההפניות לעיל בפרק ב בה"ש 216.

89 ראו לעיל בפרק ב טקסט לה"ש 229.

90 סעיף 22(4) לאמנה, שכותרתו "Jurisdiction", קובע כי האמנה אינה מתנה על גישתן של המדינות כלפי סמכות התחיקה, השפיטה והאכיפה שלהן.

91 ראו Perritt, לעיל ה"ש 40; Brenner & Schwerha, לעיל ה"ש 40.

המקובל בדיניה הפנימיים. רוב המנגנונים שמנתי לעיל גוזלים זמן יקר, שעלול להביא לאבדן הראיות דיגיטליות, למחיקתן או לשינויין. אמנם מנגנוני העזרה המשפטית המהירים והמיוחדים לראיות דיגיטליות שנקבעו באמנת מועצת אירופה בדבר פשעי מחשב משפרים את האכיפה הפלילית האקסטרטריטוריאלית באופן ניכר, אולם מנגנונים אלה פועלים אצל המדינות שהן צד לאמנה בלבד, ובעניינן של עברות שאסורות על פי דיניהן של שתי המדינות הנוגעות בדבר, המדינה המבקשת והמדינה שבה שמורה הראיה. האמנה דורשת, כדרישת חובה, הסכמה על בסיס צר למדי של עברות פליליות בלבד, ומכאן שהשונות בסטנדרט הפלילי בין המדינות השונות יכול להיות גבוה למדי. כפי שהסברתי בפרק ב.ה.2. לעיל, אמנם האמנה היא הניסיון המעשי הבולט ביותר לאכיפה בין-לאומית, אולם פתרון זה, כפתרון כולל שנועד לבוא בנעלי האכיפה הפלילית המדינתית במרחב הסייבר, אינו צליל.

פעולות האיסוף הנחסרות בשל התפישה הטריטוריאלית

אילו פעולות איסוף נחסרות בשל התפישה הטריטוריאלית, כפי שפירטתי את מרכיביה היישומיים לעיל? על מנת להשיב על שאלה זו, אשוב אל הטקסונומיה שהצגתי בפרק המבוא, שבו מנתי חמישה פרמטרים ממיינים לפעולות האיסוף השונות: האחד, הבחנה בין פעולות איסוף שמבצעת הרשות החוקרת בעצמה לעומת פעולות איסוף שמבצע אדם אחר; השני, הבחנה בין פעולות איסוף בעלות אופי כללי, שאינן תלויות בחקירה פלילית ספציפית, לבין פעולות איסוף בעלות אופי פרטיקולרי המתבצעות אד הוק עם התעוררות צורך חקירתי וחד קונקרטי במקרה נתון; השלישי, הבחנה בין פעולות איסוף המבוצעות בידיעת החשוד לבין פעולות איסוף סמויות; הרביעי, הבחנה בין תפיסה של ראיה קיימת, תפיסה של ראיה העתידה להיאגר במקום איסופה המיועד ויצירת תיעוד; החמישי, הבחנה בין פעולות איסוף כלפי חומרים המצויים בטריטוריה של המדינה החוקרת לבין פעולות כלפי חומרים המצויים מחוץ לטריטוריה.

הפרמטר האחרון המבחין בין פעולות איסוף בחו"ל לבין פעולות איסוף בארץ, הוא הנוגע לענייננו. כאשר מדובר באיסוף ראיות במרחב הפיזי, נדרשים החוקרים, ככל שהפעולה מבוצעת על ידיהם, או האדם המצווה לכך על-ידי רשויות האכיפה, ככל שהפעולה מבוצעת על-ידו, לנסוע פיזית לחו"ל או לנתב את הראיה המבוקשת לטריטוריה של המדינה החוקרת. אולם בכל הנוגע לחקירה במרחב האינטרנטי, כפי שטענתי לעיל, עצם הימצאות הראיות בחו"ל אינה מעלה ואינה מורידה מבחינת טיב הפעולה המבוצעת. הפעולה יכולה להתבצע ממקום מושבו של החוקר, או האדם הנמען לצו, במדינה החוקרת. מבחינה טכנית אין כל הבדל, בדמות "גבול", עם התקשרות החוקר לחומר מחשב המצוי במחשבים מחוץ לטריטוריה. על כן בכל הנוגע לאיסוף ראיות דיגיטליות באינטרנט, ניתן למעשה לזנוח את הפרמטר של מקום הימצאות הראיה המבוקשת – בארץ או בחו"ל – כפרמטר הממייין את פעולות האיסוף השונות מבחינת טיב הפעולה. אולם מבחינת הסמכות לביצוע הפעולה, הרי שנוכח התפישה הטריטוריאלית במרחב הסייבר, קיים איסור נוקשה על איסוף הראיות כשהן מצויות במחשבים מחוץ לטריטוריה. במילים אחרות, כל פעולות האיסוף, בין שהרשות החוקרת מבצעת אותן ובין שהאדם המצווה לכך מבצען, בין שהן מבוצעות בידיעת מושא הפעולה או בחשאיות, בין שמדובר בפעולה פרטיקולרית או כללית, ובין שמדובר בפעולה של תפיסת חומר קיים או בתפיסת חומר העתיד

להיאגר או ביצירת תיעוד של החומר האמור – ככל שהן מבוצעות כלפי חומרי מחשב המצויים במחשבים בחו"ל, הן אסורות.

הקריאה לאכיפה פלילית אקסטרה-טריטוריאלית במרחב הסייבר

המבקר החריף ביותר של כלל הווטו החקירתי הזה הוא ג'ק גולדסמית' (Goldsmith). גולדסמית' צידד בהמשך תפקודה של המדינה כגורם האוכף את הדין הפלילי במרחב הסייבר.⁹² לדעתו, המדינה צריכה לשמר את הלגיטימציה שלה כגורם אוכף הדין הפלילי במרחב. מטעמים מעשיים של יעילות והיתכנות לביצוע חקירות פליליות במרחב הסייבר, יש לטענתו לאפשר למדינה לשמר את הלגיטימציה כאמור באמצעות הכשרת פעולות איסוף של מידע משרתי מחשב המצויים מחוץ לתחום השיפוט.⁹³ אם תוסר מגבלת סמכות איסוף הראיות הבין-לאומית, לכאורה עלולה להתעורר במלוא חריפותה הבעיה שעליה הצביעו דייוויד ג'ונסון ודייוויד פוסט, ולפיה כל פעילות מקוונת, בפרט פעילות אינטרנטית, תהא כפופה לדיני כל המדינות.⁹⁴ זאת על בסיס ההנחה שכל פעילות ברשת, בפרט פעילות הכרוכה באלמנט של פרסום תוכן ברבים, או פנייה להצעת שירותים לציבור, היא בעלת השפעה על משתמשי מחשב מכל המדינות, ועל כן סמכות התחיקה של כל מדינה ומדינה יכולה להתפרש עליה. במקרה כזה עלולה להיווצר תופעה של "סחרור דינים שלילי", שלפיו המדינה השמרנית ביותר תכפה למעשה את דיניה על כלל משתמשי הרשת. גולדסמית' השיב לחשש זה באמרו כי תופעת סחרור הדינים השלילי תתרחש רק כשמדובר בספקיות שירות אשר יש להן שלוחה מקומית, שנגדה ניתן להוציא לפועל את פעולת האכיפה, או כשמדובר בספקיות שירות שניתן להסגיר אותן למדינה האוכפת. הלכה למעשה, טען גולדסמית', קבוצה זו של ספקיות שירות אינה כה גדולה, ומכאן שבעיית סחרור הדינים השלילי הנובעת מהסרת המגבלה של סמכות איסוף הראיות הבין-לאומית במרחב המקוון – אינה כה אקוטית.⁹⁵

לקריאה המעשית לביטול כלל הווטו במישור סמכות האכיפה הבין-לאומית קמו מתנגדים. פטרישיה בליה (Belia) טענה כי הגם שכיום כללי סמכות האכיפה הבין-לאומית מעוגנים במשפט הבין-לאומי ההסכמי, למעשה מקורות הכללים הללו במשפט הבין-לאומי המנהגי. על כן צורך פרקטי לגבור על מגבלות סמכות האכיפה הבין-לאומית במרחב הסייבר, חזק ככל שיהיה, אינו יכול להגמיש כללים של המשפט הבין-לאומי המנהגי.⁹⁶ ניקולאי סייטץ (Seitz) הביע עמדה עקרונית המתנגדת לאפשר לרשות החוקרת לחדור לחומר מחשב האגור בשרתים מחוץ לטריטוריה, למעט במקרים שבהם המידע הממוחשב פתוח לעיון כלל הציבור או במקרים של הסכמה מאת המחזיק במידע.⁹⁷ עמדתו של סייטץ נסמכת על עיקרון של מעין הדדיות: אם כל מדינה תתיר חדירה של חוקריה לחומרי מחשב האגורים בשרתי מדינות זרות, משמע שכל

92 ראו Goldsmith, *Unilateral Regulation of the Internet*, לעיל ה"ש 40. כן ראו Jack L. Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI. KENT L. REV. 1119 (1998).

93 ראו Goldsmith, לעיל ה"ש 42, בעמ' 107.

94 Johnson & Post, לעיל ה"ש 55, בעמ' 1374.

95 ראו Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 483-485 (1998).

96 ראו Goldsmith, *Unilateral Regulation of the Internet*, לעיל ה"ש 40, בעמ' 139-140.

97 ראו Bellia, לעיל ה"ש 40, בעמ' 61-65, 70-80.

98 Seitz, לעיל ה"ש 40.

מדינה תיפגע בעצמה מפעולה של הרשויות החוקרות של המדינות האחרות. למעשה סייטץ מניח במידה מסוימת את המבוקש בקבעו אוטומטית שאכן יש פגיעה יסודית בריבונותה של המדינה ברגע שרשות חוקרת של מדינה אחרת אוספת, באמצעות התקשרות מרחוק, ראיות דיגיטליות המצויות במחשבה של אותה מדינה. על כל פנים, גולדסמית' לא השיב, לפי שעה, לביקורות אלה.

לסיכום, התפישה הטריטוריאלית מתורגמת, הלכה למעשה, לכלל וטו שלפיו אם הראיה הדיגיטלית אגורה במחשב מחוץ לטריטוריה של המדינה החוקרת, הרי שאין למדינה החוקרת סמכות לאסוף את אותה ראיה. על פי גישה זו, במרחב הסייבר חקירות רבות תהפוכנה לאקסטרה-טריטוריאליות. גולדסמית' טען כי בעקבות זאת תיווצר בעיה קשה של אכיפה פלילית מדינתית במרחב הסייבר, ועל כן קיים הצורך הפרקטי בפריצת גבולותיה של התפישה הטריטוריאלית. הטענה של גולדסמית' נעדרת הצדקה נורמטיבית עצמאית לחריגה מהתפישה הטריטוריאלית, לבד מההצבעה על הקושי שמייצרת התפישה הטריטוריאלית במרחב הסייבר. בהמשך הדיון, בפרק ג.ו. להלן, אציע הצדקות נורמטיביות לפריצת גבולותיה של התפישה הטריטוריאלית באשר לדיני איסוף ראיות בחקירה פלילית במרחב הסייבר. ככל שייפרצו גבולותיה של התפישה הפיזית, ייפתח דיון נוסף בסוגיית ההגנות החוקתיות שתיפרשנה על החשודים ועל צדדים שלישיים נוספים, המושפעים מן החקירה, במקרה של פעולה אקסטרה-טריטוריאלית שכזאת: האם יחולו דיני החוקה של המדינה החוקרת? של המדינה שבה אגורה הראיה? או של מדינת תושבותו של החשוד (בהנחה שזו מדינה שונה)? אדון בנושא זה להלן בפרק ה.ג..

אעבור עתה להציג דוגמאות לפריצות של התפישה הטריטוריאלית כפי שניסחתי אותה לעיל. חלקן הוכרו במשפט הבינ-לאומי ההסכמי וחלקן במשפטן הפנימי של מדינות שונות. פריצות אלה הן בבחינת היוצא מן הכלל המעיד על הכלל. לאחר מכן אציג את התפישה הטריטוריאלית ואת הפריצות הבודדות שלה כפי שהוצעו בהצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד–2014 (להלן – הצעת חוק החיפוש או הצעת החוק).⁹⁸ בהמשך הפרק אציג ביקורות שונות לתפישה הטריטוריאלית, הן במישור הארכיטקטוני-טכנולוגי, הן במישור האפיסטמולוגי והן במישור המעשי, ואבקש לערער למעשה על שלושת היסודות הללו המרכיבים, מבחינה יישומית, את התפישה.

ה. פריצות מעשיות של התפישה הטריטוריאלית באשר לדיני איסוף ראיות במרחב הסייבר

קיים צורך משטרתי מעשי הולך וגובר לפרוץ את גדר החומה הטריטוריאלית בנוגע לאיסוף ראיות במסגרת חקירה פלילית במרחב הסייבר. בחלק זה אציג כמה מהלכים משפטיים בין-לאומיים להכרה בפעולות אקסטרה-טריטוריאליות במסגרת חקירה פלילית במרחב הסייבר.

98 ה"ח הממשלה 867. הצעת החוק מבוססת על דין וחשבון הוועדה לסדר דין פלילי (אמצעים משטרתיים) (חיפוש, הצגה, תפיסה וחילוט) משנת 1996 (המכונה – "ועדת לויין"). בתוספת עבודה ממושכת במשרד המשפטים, שבמסגרתה הוסף פרק העוסק באיסוף ראיות דיגיטליות אשר לא הפיע בעבודתה של ועדת לויין. על הצעת החוק אפרט עוד להלן, פרק ד.ב.2. ופרק ד.ד..

לאחר מכן אציג כמה מהלכים אונילטרליים שנקטו מדינות שונות באשר לפעולות איסוף שונות במרחב הסייבר. בכל הנוגע לפריצות של התפישה הטריטוריאלית במסגרת מהלכים במשפט הבינלאומי ההסכמי, ברי כי הם עדיפים, שכן הם מונעים טענות בדבר פגיעה בריבונות בעקבות פעולה אקסטרה-טריטוריאלית. המהלכים האונילטרליים שאותם אמנם מותרים על פי משפטן הפנימי של המדינות המקיימות אותם, אולם בשל תפישת הריבונות הטריטוריאלית ובשל תפישת הטריטוריאליות באשר למרחב הסייבר, אותן מדינות עלולות להיחשב למי שמפרות ריבונות של מדינות אחרות.

1. הסכמה בין-לאומית על חדירות אקסטרה-טריטוריאליות

אמנת מועצת אירופה בדבר פשעי מחשב כוללת הוראה בסעיף 32 המתייחסת לחריגות אקסטרה-טריטוריאליות מוסכמות. על פי סעיף זה, מוכרת הסמכות לבצע חדירה לחומר מחשב מחוץ לתחום השיפוט בשני המצבים האלה: כאשר המחזיק בחומר המחשב מביע את הסכמתו (כדין ומרצון – "Lawfully and Voluntary")⁹⁹; לכך, כאשר מדובר בחומרים הנגישים לכלל הציבור. שנתיים קודם לכן השיגו מדינות ה-G8 הסכמה דומה על התרת גישה אקסטרה-טריטוריאלית של רשויות חקירה לחומרי מחשב באותם תנאים. מסמך ה-G8 הוא מסמך עקרונות, והוא אינו מחייב מבחינת המשפט הבינלאומי כמו אמנה (גם אמנה מחייבת כמובן רק את המדינות שחתמו ואשררו אותה).¹⁰⁰

במבט ראשון ההסכמות האמורות מתנות על המגבלה הטריטוריאלית באשר לאיסוף ראיות בחקירה פלילית במרחב הסייבר. אולם במבט נוסף ניתן לומר כי ההתניה האמורה דווקא משעתקת את התפישה הטריטוריאלית: ראשית, היא מכירה בהיותו של המרחב המקוון פרוש טריטוריאלית בהתאם למיקומו של השרת שבו אגורה הראיה הדיגיטלית המבוקשת; שנית, היא מכירה במשתמע בהיעדר האפשרות לחדור לחומרי מחשב האגורים בשרתים שבשטחי כל המדינות שאינן צד לאמנת מועצת אירופה או להסכמות ה-G8; שלישית, היא מכירה בכך שבכל שאר הסיטואציות החקירתיות לא תותר חריגה אקסטרה-טריטוריאלית. אותם שאר המצבים הם דווקא השכיחים יותר במהלך חקירה פלילית: לדוגמה, חדירה לחומר מחשב ללא הסכמת המחזיק או חדירה לחומרי מחשב הפתוחים רק לקהל מסוים (למשל, תוכני פייסבוק של חשוד מסוים שאינו משתף בהם את כל הציבור אלא רק את ה"חברים" שאותם אישר). סיטואציה חקירתית שכיחה נוספת היא כאשר מתבקש מראש חיפוש ברשת בין-מחשבים ולא במחשב בודד (Network search), ואחד המחשבים ברשת, שאליו יש לחשוף גישה, מצוי פיזית בחו"ל. דוגמה דומה היא כאשר הרשות החוקרת מחפשת אחר ראיות במחשבו של חשוד, והמחשב כולל קישורית לחומרי מחשב נוספים במחשב אחר, המחובר אל המחשב המקורי ברשת (בלי שהרשות החוקרת ידעה על כך מראש). לאור כל זאת ניתן לראות באמנה או בהסכמות של

99 האמנה קובעת כי מי שנותן את ההסכמה לחדירה למחשבו, לרבות לחדירה מחוץ לתחום שיפוט, צריך להיות מוסמך על פי דיני אותה מדינה ("Lawfully Authorized") למסור את ההסכמה לגבי חומר המחשב המדובר.

100 ראו לעיל בפרק ב טקסט לה"ש 229.

מדינות ה-G8 ניסיונות חסרים ביותר לפרוץ את המסגרת של התפישה הטריטוריאלית באשר לאיסוף ראיות במסגרת חקירה פלילית במרחב הסייבר.¹⁰¹

2. דין מדינתי המתיר חדירה אקסטרה-טריטוריאלית במצבים מסוימים

לא אתימר להקיף כאן את מערך הדינים של כל המדינות. אציג כמה קטגוריות של מקרים שבהם הוכרה האפשרות לבצע פעולות איסוף ראיות אקסטרה-טריטוריאליות, על פי התפישה הטריטוריאלית באשר למרחב המקוון.¹⁰² בכל קטגוריה כזאת אציג כדוגמה שיטת משפט אחת או יותר שאימצה את ההיתר האקסטרה-טריטוריאלית. אל מול הדוגמאות שיובאו להלן אציין כבר עתה כי במשפט ישראלי הנוהג אין היתר לחדירה אקסטרה-טריטוריאלית לחומר מחשב האגור או העובר בתקשורת בין מחשבים בחו"ל; קיים היתר, פרי פסיקה, להוצאת צו המצאת מסמכים (ובכלל זה חומר מחשב) המצויים בחו"ל, ואשר לנמען לצו, המצוי בישראל, יש גישה כדין אליהם. בהמשך אתייחס להצעת חקיקה המתייחסת לראשונה לאפשרות להכיר, בתנאים מצומצמים, בחדירה אקסטרה-טריטוריאלית לחומר מחשב.¹⁰³

א) גישה לחומר מחשב הנגיש לכלל הציבור

הכוונה בחומר מחשב הנגיש לכלל הציבור היא לאתר אינטרנט שאין כל הגבלה יזומה של מנהלו על הגישה אליו. על מנת להמחיש את הסיטואציה הנדונה כאן אביא את הדוגמה הזאת: נניח שנפתחת בישראל חקירה בגין עברת הסתה לגזענות. העברה הנחקרת בוצעה על דרך של פרסום תכנים מסיתים לכאורה באתר אינטרנט אמריקני. מטרתו של הפרסום המסית להגיע לקהל יעד רחב יחסית, ולכן הוא מוצב באתר אינטרנט הפתוח לכלל הציבור ואינו דורש הרשמה מיוחדת, תשלום או כדומה. משטרת ישראל מעוניינת לחקור את העברה. צעד ראשון בחקירה יהיה לאסוף את הפרסום המסית לכאורה באמצעות העתקתו מאתר האינטרנט. מה דינה של פעולה זו? האם קמה סמכות למשטרת ישראל להעתיק את התכנים המסיתים מהאתר הזר? האם יש לראות בכך משום פעולה אקסטרה-טריטוריאלית?

101 לעמדה ברוח זו ראו Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 Berkeley Tech. L.J. 433, 443–444 (2003). כפי שציינו מנסחי האמנה בדברי ההסבר שלהם לסעיף 32 לאמנת מועצת אירופה בדבר פשעי מחשב (לעיל ה"ש 46):

“There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area”.

102 איני מתייחס כאן להפעלת סמכויות ביטחון אלא להפעלת סמכויות איסוף בלבד. סמכויות הביטחון, שעליהן עמדת בפרק המבוא, טקסט לה"ש 25–31, יכולות להיות אקסטרה-טריטוריאליות. כך למשל ציינתי שהחקיקה האמריקנית העניקה במפורש סמכויות ביטחון אקסטרה-טריטוריאליות. עוד אציין שעל פי הפסיקה, ראיות שהושגו באמצעות חוק ה-Foreign Intelligence Surveillance Act האמריקני עשויות להיות קבילות בהליך פלילי "רגיל", אם המטרה המקורית לאיסופן הייתה ביטחונית על פי התכליות המוכרות בחוק. ראו, למשל, *United States v. Pelton*, 835 F.2d 1067 (4th Cir., 1987); *United States v. Ning Wen*, 477 F.3d 896, 898–899 (7th Cir., 2007).

103 ראו להלן בפרק ג.ו.

כל אחת מהמדינות שהן צד לאמנת מועצת אירופה בדבר פשעי מחשב או חברה ב-G8, מכירה באפשרות לגשת לחומר מחשב הנגיש לכלל הציבור באינטרנט אף אם הוא אגור בשרתים בחו"ל. הדין הקיים במדינת ישראל שותק לעניין זה.¹⁰⁴ על פי התפישה הטריטוריאלית הטהורה, הסיטואציה הנדונה כאן היא של ביצוע פעולת איסוף אקסטרה-טריטוריאלית. עם זאת כיוון שמדובר בפעולת איסוף מרשות הרבים, והפעולה היא בבחינה המותר לכל תושב במדינה החוקרת, סביר להניח שברמה המעשית המדינה הזרה שבה מצוי חומר המחשב, לא תראה בפעולת הרשות החוקרת משום פגיעה ממשית בריבונותה, הגם שפורמלית מדובר כאן בחריגה מסמכות אכיפה טריטוריאלית מובהקת, כפי שהיא מתפרשת כיום.

ב) גישה לחומר מחשב האגור בשרתים בחו"ל בהסכמה כדין של המחזיק בו

גם כאן כל אחת מהמדינות שהן צד לאמנת מועצת אירופה בדבר פשעי מחשב או חברה ב-G8, מכירה באפשרות לגשת לחומר מחשב אשר הובעה בעניינו הסכמה של בעל גישה והרשאה כדין כי הרשות החוקרת תחדור אליו.¹⁰⁵ החוק הישראלי שותק, ככלל, באשר לסמכות החדירה לחומר מחשב בהסכמה, ובכלל זה הוא שותק גם לגבי סמכות החדירה האקסטרה-טריטוריאלית בהסכמה.¹⁰⁶ שאלת הגישה וההרשאה כדין היא שאלה מורכבת למדי, בשני

104 דיון בגישה לחומר באינטרנט הנגיש לכלל הציבור והמצוי בשרתים מחוץ לטריטוריה המדינתית מורכב למעשה משניים: האחד, דיון בשאלת מקור הסמכות של הרשות החוקרת לגשת לחומרים הנגישים לכלל הציבור, גם אם חומרים אלה מצויים בשרתים במדינה החוקרת; השני, בהינתן שקיימת סמכות לגשת לחומרים האמורים, יש לבחון מה מקור הסמכות לחדירה לחומרים פומביים שכאלה כשהם אגורים מחוץ לטריטוריה של המדינה החוקרת, ומה ההשלכות של פעולה אקסטרה-טריטוריאלית שכזאת מבחינתה של המדינה שבה מצויים החומרים המדוברים. עניינו, בהקשר של פעולה אקסטרה-טריטוריאלית באינטרנט, הוא למעשה בשאלה השנייה.

105 ראו למשל בארצות הברית את ה-DOJ Manual, לעיל ה"ש 40, בעמ' 139–140. בארצות הברית הפסיקה מכירה באפשרות של המחזיק בחומר המחשב לוותר על זכותו החוקתית לפרטיות לפי התיקון הרביעי לחוקה. די בהסכמה של אחד מן המחזיקים ולא מחויבת הסכמה של כולם. זאת על בסיס הפסיקה המוחלטת על דיני החיפוש בחצרים, ראו Georgia v. Randolph, 547 U.S. 103 (2006). כן ראו (בהתייחס במישרין לחדירה לחומר מחשב): People v. Dagwan, 711 N.W. 2d 386 (Mich. App. 2005). עם זאת ראו את United States v. Hudspeth, 459 F. 3d 922 (8th Cir., 2006), שם נפסק כי ברגע שמחזיק אחד במקום סירב לביצוע החיפוש ולתפיסת מחשבו, אי אפשר לפנות למחזיק אחר במשותף עמו ולקבל את הסכמתו.

106 שאלת הסמכות החוקתית לחודור לחומר מחשב בלא צו, בהסכמה כדין המחזיק/המשתמש/בעל ההרשאה/הגישה, אינה מוכרעת בדין הישראלי הקיים גם כאשר ההקשר הוא פנימי ולא אקסטרה-טריטוריאלית. אמנם בעניין בן חיים הכיר בית המשפט העליון בסמכות לערוך חיפושים במקום ועל הגוף בהסכמה, ללא צו שיפוטי ואף ללא עילה מכוח הפסד"פ (ראו רע"פ 10141/09 בן חיים נ' מדינת ישראל (פורסם בנבו, 6.3.2012)), אולם לשונו של סעיף 23 לפסד"פ נוקטת ניסוח קוגנטי, ולפיו לא תתבצע חדירה לחומר מחשב אלא בצו בית משפט המפרט את המטרות והתנאים לביצועה. מיגל דויטש, שהיה לו חלק מרכזי בניסוח הצעת חוק המחשבים, אשר תיקנה את סעיף 23 לפסד"פ הדין בחדירה לחומר מחשב, טען כי כוונת המחוקק הייתה לחייב ביצוע חדירה לחומר מחשב בצו בית משפט בלבד. ראו מיגל דויטש "חקיקת מחשבים בישראל" עיוני משפט כב 455–456 (1999). עם זאת בכמה מקרים הכירו בתי המשפט באפשרות העקרונית להתיר חדירה לחומר מחשב בהסכמה בהיעדר צו שיפוטי מסמך. ראו למשל ע"פ (מחוזי ת"א) 61187-06-14 קורס נ' מדינת ישראל (פורסם בנבו, 30.3.2015). כן ראו כמה החלטות מערכאות צבאיות, לדוגמה ח"א (מחוזי) 81/08 התצ"ר נ' רבן

ממדים: האחד, בממד היקפו של חומר המחשב הכלול במסגרת ההסכמה. כך לדוגמה תישאלנה שאלות אם וכיצד תיפרש ההסכמה על חומר מחשב מחוק, על לוגים שהמחשב מייצר לצורך ניטור עצמי של הפעילות בו; הממד השני נוגע לשאלת זהותו של המחזיק בחומר המחשב הרשאי להסכים לחדירה אל החומר. כך לדוגמה לא ברור מעמדו של טכנאי מחשבים המחזיק ברשותו מחשב של לקוחו לצורך תיקון; מעמדו של מנהל רשת; מעמדו של הורה ביחס לילדו הקטין; מעמדו של אדם המשתמש במחשב ביחס לזולתו, המשתמש באותו מחשב אך בפרופיל משתמש אחר; מעמדו של מעביד ביחס לעובדיו, וכיצא בזה.¹⁰⁷

ג) הפעלת סוכנים וירטואליים באתרים ה"יושבים" בשרתים בחו"ל

נניח כי חשוד נחקר בגין ביצוע עברות מין, הטרדה מינית ופרסומי תועבה באמצעות האינטרנט. עוד נניח כי החשוד יוצר קשר עם קרבתיו באתרים חברתיים כגון "פייסבוק" (שרתיו מחוץ לישראל) ו"מקושרים" (שרתיו בישראל). המשטרה מבקשת לטמון פח לחשוד. מוחלט על פעולה בכיסוי של שוטר, שתפתח כרטיס ותעדכן פרטים ותמונות ב"פייסבוק" וב"מקושרים" ותיצור קשר עם החשוד בכך שתציע לו "חברות". עוד נניח שהחשוד אינו חושף את כל ה"פרופיל" שלו, הכולל תמונות, סרטונים שלו, פרטי מידע אישיים שכתב על עצמו וכן "קיר" עם פוסטים שלו ושל חבריו לכל משתמשי האתר אלא רק למי שהוא אישר אותו מראש כ"חבר". הסוכנת המשטרתית הופכת ל"חברה" של החשוד תוך יצירת מצג שווה כלפיו. בזכות מצג השווה היא מקבלת את האפשרות לגשת ולעייין בחומרי המחשב שלו ולעקוב אחר פרסומיו הפתוחים רק לקהל "חבריו". כן היא מקבלת את האפשרות לתקשר עמו בעצמה באותם

(לא פורסם, 27.7.2009); ז"י (מחוזי) 120/14 התובע הצבאי נ' שניר פלה (פורסם בנוב, 25.6.2014). זו גם עמדתו של נמרוד קזולובסקי המחשב וההליך המשפטי 63–64 (2000).
107 ראו למשל הדיון בארצות הברית בשאלה אם טכנאי מחשבים שקיבל את המחשב לבדיקה רשאי למסור הסכמה לביצוע החדירה. ראו *United States v. Anderson*, 2007 WL 1121319 (N.D. Ind., 2007), שם השיבו על השאלה בחיוב; מנגד ראו *United States v. Barth*, 26 F. Supp. 2d 929 (W.D. Tex., 1998), שם השיבו על השאלה בשלילה. כן נדונה השאלה אם הסכמה של משתמש אחד במחשב יכולה לחול על חדירה לקבצים מוצפנים או מוגני-ססמה של מחזיק אחר באותו מחשב. לעמדה שלפיה התשובה לשאלה זו היא שלילית, ראו *Trulock et al v. Freeh et al*, 275 F. 3d 391 (4th Cir., 2002). לעמדה שלפיה התשובה חיובית, ראו *United States v. Andrus*, 483 F. 3d 711 (10th Cir., 2007); *People v. Brown*, 279 Mich. App. 116; 755 NW2d 664 (Mich. App., 2008). בנוסף, התעוררה השאלה אם הורים יכולים למסור הסכמה לחדירה למחשבים של ילדיהם. בעניין *Andrus* הנ"ל נקבע כי להוריו של בגיר (בן 51) אשר התגורר בבית הוריו ולא שילם שכירות יש הרשאה למסור הסכמה לחדירה למחשבו, זאת כאשר להורים הייתה גישה לחדרו וכאשר הם שילמו את חשבון האינטרנט בבית. כן ראו DOJ Manual, לעיל ה"ש 40, בעמ' 23–24, שם נקבע כי במקרה שבו הילד משלם שכירות להוריו בגין מגוריו בביתם, או כאשר הילד נוקט אמצעים מפורשים למנוע גישה של ההורים למחשב או לחלקים מדירתם, וכן בשים לב לגילו של הילד שבו מדובר, הרי שאי אפשר לראות בהורים בעלי סמכות להסכים לחדירה למחשב של ילדם. אשר לשאלה אם מעביד רשאי להסכים לחדירת הרשויות לחומרי מחשב של עובדיו, ראו למשל את *United States v. Ziegler*, 474 F.3d 1184, 1191 (9th Cir., 2007), שם נפסק שמעביד יכול להסכים לחדירה למחשב של עובד שלו, שהוא (המעביד) סיפק לו אותו. באותו מקרה המעביד אף פרסם מראש בקרב העובדים את מדיניותו שלפיה הוא נוהג לסרוק את מחשבי העובדים. מדיניות מוצהרת זו העניקה למעביד, כך נפסק, סמכות גם "להסגיר" את המחשבים לרשויות החקירה.

אתרים חברתיים. מה דינה של הפעולה האמורה? האם דינה משתנה בין "פייסבוק" האמריקני לבין "מקושרים" הישראלי?

מדינות שונות, ובהן מדינת ישראל, מפעילות סוכנים וירטואליים באינטרנט.¹⁰⁸ שאלת כשרות פעולתו של הסוכן הסמוי ברשת יכולה להיבחן דרך הפריזמה של הסכמה המושגת בתחבולה מותרת לאיסוף הראיות, אך סביר להניח שקונסטרוקציית ההסכמה לא תעמוד במבחן בית המשפט, שכן הסכמה בתחבולה משטרית לא תיחשב להסכמה מדעת הדרושה כדי לאיין פגיעה בפרטיות.¹⁰⁹ ואולם, פעולת הסוכנים הסמויים ברשת תיחפש, לדעתי, ככורה כל יגונה העשוי להיות מוכשר דרך הפריזמה של פטור מאחריות לפי חוק הגנת הפרטיות לאנשי רשות ביטחון (בכלל זה המשטרה) הפועלים באורח סביר במסגרת תפקידם.¹¹⁰ האם סעיף הפטור

108 לעניין זה (בהקשר של לכידת פדופילים באינטרנט), ראו למשל חיים ויסמונסקי "סוכנים וירטואליים לחשיפת פדופילים באינטרנט – בעקבות פרשת ערוץ 10" הסניגור 160, 5 (2010). כן ראו, באשר למשטרת אנגליה, את: Jamie Barlett et. al, *Policing in an Information Age*, THE CENTRE FOR THE ANALYSIS OF SOCIAL MEDIA (CASM) 13–17 (2013) http://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365. המחברים דיברו על פיתוח תחום מודיעין משטרתי חדש, שאותו הם כינו "Soemint", קיצור של Social media intelligence (על משקל מודיעין אנושי Human intelligence – "Humint", מודיעין של אותות דיגיטליים Signal intelligence – "Sigint", מודיעין המבוסס על איסוף ממקורות גלויים Open source intelligence – "Osint" ועוד).

109 סעיף 3 לחוק הגנת הפרטיות, התשמ"א–1981, דורש כתנאי לכשרות ההסכמה כי ההסכמה תהיה "מדעת, במפורש או מכללא". על פי נתיב זה, יש לשאול אם השגת הסכמה, תוך התחזות של הסוכנת המשטרית באמצעות שימוש בזהות "תמימה", פוגמת בעצם ההסכמה. בהמשך לדוגמת הסוכנת הסמויה החוברת לחשוד ב"פייסבוק" וב"מקושרים", החשוד נותן הסכמה מודעת לצרף את הסוכנת כחברה שלו ולחשוף בפניה את נתוני הפרופיל האישיים שלו. אמנם הסוכנת אינה מרמה אותו לעניין עצם המעשה (צירוף חבר לדרך שלו ב"פייסבוק" או ב"מקושרים"), אולם הוא בהחלט מרמה לעניין זהות העושה. עוד ראו את מיכאל בירנהק מרחב פרטי: הזכות לפרטיות בין משפט טכנולוגיה 99–100 (2010); מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" משפט וממשל יא 9, 49–51 (2007). בירנהק הביע שם את עמדתו (העקרונית), לא בהקשר הנדון של פעולת סוכן משטרתי סמוי כי ניתן להרכיב עקרונות של דיני חוזים על דרישת ה"הסכמה מדעת" לפגיעה בפרטיות, ומכאן שהסכמה שהושגה ברמייה או בהטעיה אינה הסכמה מדעת ואינה הסכמה כלל. מנגד, מעניין כי בארצות הברית הכירה הפסיקה בהשגת הסכמה במרמה בידי סוכן משטרתי כהסכמה כשרה לצורך התנאה על הזכות לפרטיות כפי שהיא נקובה בתיקון הרביעי לחוקה האמריקנית. ראו *Lewis v. United States*, 385 U.S. 293, 302 (1966); *Hoffa v. United States*, 385 U.S. 206, 210 (1966).

110 סעיף 19(ב) לחוק הגנת הפרטיות קובע כדלקמן: "רשות בטחון, או מי שנמנה עם עובדיה או פועל מטעמה, לא ישאו באחריות לפי חוק זה על פגיעה שנעשתה באופן סביר במסגרת תפקידם ולשם מילוי". על פי נתיב זה, תישאל השאלה אם חרף הנחת המוצא שפעולתה של הסוכנת המשטרית פוגעת בפרטיות היא מזכה בכל זאת את המשטרה בפטור מאחריות לפי חוק זה. אשר לדרישת הסבירות המנויה בסעיף 19 לחוק הגנת הפרטיות, נראה כי זו תיבחן על פי השאלה אם יש במעשהו של הסוכן הסמוי משום הדחה פסולה (Entrapment) לדבר עברה. ראו למשל ע"פ 15/78 ביבס נ' מדינת ישראל, פ"ד לב(3) 64, 70–74 (1979); ע"פ 360/80 מדינת ישראל נ' אפנדי, פ"ד לה(1) 228, 232 (1980); ע"פ 470/83 מורי נ' מדינת ישראל, פ"ד לט(1) 1, 5 (1985); ע"פ 1224/07 בלדב נ' מדינת ישראל, בפס' 60–75 (פורסם בנבו, 10.2.2010); ישגב נקדימון הגנה מן הצדק 223–229 (מהדורה שנייה, 2009); עמנואל גרוס "סוכן מדיח – כטענת הגנה במשפט הפלילי" הפרקליט לז 107 (1987); גדי אשד "החקירה המשטרית והמודיעין האנושי" משפט וצבא 18, 223 (2005). בהקשר של הפעלת סוכנים סמויים לחשיפת פדופילים הפועלים באינטרנט, ראו הטענות אצל אסף הרדוף "הקלות המטרדיה של הפיתוי: בעקבות פרשת ערוץ 10" הסניגור 160, 11 (2010). כן ראו את פסק דינו של בית המשפט העליון מהעת האחרונה בפרשת "ערוץ 10" ברע"פ 1201/12 קטיעי נ' מדינת ישראל (פורסם בנבו,

בחוק הגנת הפרטיות יכשיר את פעולת הסוכן הווירטואלי בהיבט האקסטרה-טריטוריאלי, אם יאסוף ראיות האגורות בשרתים מחוץ לטריטוריה של המדינה החוקרת? במקרה כזה, קשה לצפות כיצד מדינה זרה, האמונה על התפישה הטריטוריאלית, שתדע על הפעלת סוכן שאוסף ראיות האגורות במחשבים בשטחה, תתפוש את הפעולה מבחינת אפשרות הפגיעה בריבונותה.

ד) חדירה למחשבים בחו"ל במסגרת חיפוש ברשת (Network search)

בבלגיה קובע סעיף 388(3) ל-Criminal Instruction Code (CIC) כי בית המשפט יכול להסמיך את הרשות החוקרת לחדור לרשת מחשבים, ובמקרה כזה ניתן להעתיק מידע הדרוש לחקירה שלא נמצא במחשב המקורי שאליו כוון הצו השיפוטי מלכתחילה. הדין הבלגי מכיר בסמכות "לתפוס" את המידע הממוחשב, במובן זה של מחיקתו מרשות מחזיקו (Deleting) או חסימת הגישה אליו בידי מחזיקו (Blocking) ונטילת העתקו לרשות היחידה החוקרת. לחלופין יכולה הרשות החוקרת רק להעתיק את המידע הממוחשב, בלי לשלול אותו מידי מחזיקו. על כל פנים, במסגרת חדירה לרשת מחשבים רשאית המשטרה הבלגית לחדור לחומרי מחשב מחוץ לטריטוריה הבלגית. במקרה כזה יותר לה להעתיק את המידע הממוחשב בלבד ולא למחקו, ויש לדווח מיד למשרד המשפטים הבלגי אשר מחויב ליידע לאלתר את הרשויות במדינה הזרה על דבר ההעתקה כאמור.¹¹¹

באסטוניה קיימת חקיקה דומה לזו שבבלגיה, המתירה, במסגרת חיפוש ברשת מחשבים, העתקה של חומר מחשב האגור בשרתים מחוץ למדינה. לאחר ביצוע ההעתקה קיימת חובת יידוע של המדינה הזרה בדבר ביצוע פעולה זו.¹¹² בהונגריה קיימת חקיקה המתירה העתקה של מידע האגור בחו"ל במסגרתה של פעולת איסוף ראיות ברשת מחשבים.¹¹³ באוסטרליה מתיר החוק, במסגרת חיפוש ברשת מחשבים (Network search), להגיע אל כל המחשבים המחוברים ברשת היכן שהם נמצאים, לרבות מחשבים המצויים בחו"ל. ככל שמיקומו של כל מחשב ומחשב בחו"ל ידוע, קמה חובה ליידע את הרשויות הזרות בדבר ביצוע החדירה לאותם המחשבים, לאחר מעשה.

ראוי לציין שכל ארבע המדינות האלה – בלגיה, אסטוניה, הונגריה ואוסטרליה – חתמו על אמנת מועצת אירופה בדבר פשעי מחשב, ואף אשררו אותה. מדינות אלה קבעו בסטנדרט החוקי הפנימי שלהן היתר לחריגה אקסטרה-טריטוריאלית רחבה מהמותר על פי האמנה. הדבר אפשרי כמובן מבחינת מערכת הדינים הפנימית של אותן מדינות, שכן האמנה קובעת רף מינימלי

9.1.2014). אשר לארצות הברית, אציין רק כמה פסקי דין "קלאסיים" שניתנו בה בנושא, המתמקדים כאמור בשאלת עצמת ההדחה של הנאשם בידי הסוכן והגינות פעולתה של הרשות במקרה כזה: Sorrells v. United States, 287 U.S. 435 (1932); Sherman v. United States, 356 U.S. 369 (1958); United States v. Russell, 411 U.S. 423 (1973); Hampton v. United States, 425 U.S. 484 (1975); Jacobson v. United States, 503 U.S. 540 (1992).

111 ראו Code d'Instruction Criminelle, 1808, Art. 88 § 3 (Bel.). ראו גם EU Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs 39 (2005), available at http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR337.pdf (להלן – EU Update). ראו גם Smith, לעיל ה"ש 40, בעמ' 285.

112 ראו EU Update, לעיל, בעמ' 88.

113 שם, בעמ' 133.

להסכמה בין-מדינתית ולא רף מקסימלי מותר. על כל פנים, בין שמדינות אלה חתומות על אמנת מועצת אירופה ובין שלא, נראה לי כי מבחינת מערך הדינים של שאר המדינות, פעולה אקסטרה-טריטוריאלית במסגרת Network search עלולה להיחשב פגיעה בריבונותן של המדינות האחרות, בהנחה שאותן מדינות מחזיקות אף הן בתפישה טריטוריאלית באשר לסמכות האכיפה הפלילית ובהנחה נוספת שאיסוף הראיות הממוחשבות האגורות בשטחן נעשה שלא בטעות בתום לב אלא בידיעה מראש שמדובר במידע האגור בשטחן.

ה) צווים פרסונליים אקסטרה-טריטוריאליים

כפי שצינתי בפרק המבוא,¹¹⁴ אחד הקריטריונים לסיווג פעולות איסוף הוא המבחן של הגורם המבצע בפועל את הפעולה: יש פעולות שהרשות החוקרת עצמה מבצעת, ויש פעולות אחרות המבוצעות בידי אדם או גורם אחר המצווה לכך. הצווים מן הסוג השני הם אישיים (in personam) ואינם מופנים כלפי חומר המחשב עצמו או כלפי אתר או "מקום" מסוים במרחב המקוון (בשונה, למשל, מצו חדירה לחומר מחשב, המופנה למחשב מסוים או למידע מסוים המאוחסן בו). כיוון שכך, ניתן – גם לפי תפישה טריטוריאלית – לפתח גישה שלפיה כל עוד האדם שאליו מופנה צו ההמצאה נמצא בישראל, הרי שכלפיו אין כל חריגה מסמכות האכיפה הטריטוריאלית. בהמשך לאותה גישה ניתן לומר שעצם הגישה של האדם עצמו (שאליו מופנה צו ההמצאה) אל חומר המחשב האגור בחו"ל, ככל שהוא בעל גישה חוקית, אינה בבחינת פגיעה בריבונותה של המדינה הזרה שבה אגור פיזית חומר המחשב. מנגד, ניתן לטעון שכיוון שהנמען לצו ההמצאה פועל בכפייה, לנוכח הוצאת צו ההמצאה עם השוט המשפטי של ביזיון בית המשפט במקרה של אי-ציות לצו, הרי שהנמען לצו מגויס לשמש זרועה הארוכה של הרשות החוקרת המושטת אל מחוץ לטריטוריה שלה. זאת על בסיס התפישה של ההמצאה כתחליף לחיפוש בחצרים או לחדירה על ידי הרשות החוקרת עצמה.

במשפט הישראלי הוכרה הסמכות להוצאת צווי המצאת מסמכים, לרבות חומר מחשב, האגורים מחוץ לטריטוריה הישראלית. העוגן לסמכות קבוע בסעיף 43 לפסד"פ. הסעיף לאקוני למדי ונוסחו אינו מתייחס לשאלת מיקום החומרים שיומצאו מכוחו.¹¹⁵ אולם הסיווג של צווים אלה כצווים אישיים אפשר הרחבת תחולה בפסיקת בית המשפט העליון, וכך, בעניין שרון נקבע כי צו המצאה לפי סעיף 43 לפסד"פ יכול לחול על חומרים המצויים פיזית בחו"ל.¹¹⁶ סעד נוסף

114 ראו פרק א.ב..

115 זו לשון הסעיף: "ראו שופט שהצגת חפץ נחוצה או רצויה לצרכי חקירה או משפט, רשאי הוא להזמין כל אדם, שלפי ההנחה החפץ נמצא בהחזקתו או ברשותו, להתייצב ולהציג את החפץ, או להמציאו, בשעה ובמקום הנקובים בהזמנה".

116 כה נפסק מפי המשנה לנשיא אור בע"פ 1761/04 שרון נ' מדינת ישראל, פ"ד נח(4) 9, 17–18 (2004): "בחיים המודרניים של זמננו הנגישות אל חפץ מסוים, אינה כרוכה בהכרח בהחזקתו הפיזית. לעיתים, יכול אדם להגיע 'בלחיצת כפתור', אל מידע המצוי בשליטתו, אך לא בהחזקתו הפיזית. את המסמכים שהחזיקו בעבר בני אדם במגירה, בספריה או בארכיון, מחליפים כיום, במקרים רבים, מאגרי מידע ברשת האינטרנט. כך למשל, מקבלים לקוחות הבנקים מידע שוטף על פעולות בחשבונותיהם, דרך האינטרנט ובאמצעות שימוש בסיסמא מזהה שמאפשרת להם ולהם בלבד, נגישות מיידית אל המידע וכן את הנפקתו המיידית בצורה של מסמך. בצורה דומה, מנויים בני אדם על חשבונות דואר אלקטרוני שניתן להגיע

של ביצוע בעין על דרך של תפיסת חומרי המחשב שמחוץ לתחום השיפוט בידי המשטרה במקומו של הנמען לצו אינו מוכר במשפט הישראלי. וכך, בעניין שרון אמנם הוצא צו המצאה באשר לחומרים המצויים מחוץ לתחום השיפוט, אולם הסנקציה כנגד אי-ביצוע הצו הייתה יכולה להיות במישור של פקודת בזיון בית-המשפט ולא במישור של ביצוע פעולת האיסוף בידי הרשות החוקרת במקומו של שרון, שאליו הופנה הצו. נוסף על האמור, לאחרונה נפסק בעתירה למתן צו מניעה על פי דיני התעמולה בבחירות לכנסת כי במקרה של סרט תעמולה פסול, על המפלגה שהפיקה את הסרטון לפעול כלפי אתרי האינטרנט שפרסמו את הסרטון, לרבות אתרי האינטרנט הזרים כ-Youtube, על מנת שהסרטון יוסר.¹¹⁷ בכך ביקשה למעשה ועדת הבחירות המרכזית לממש את הצו שהעניקה באורח אקסטר-טריטוריאלי כלפי המפלגה הנתונה תחת סמכות השיפוט שלה.

במשפט האמריקני קיימת אפשרות נוספת, במסגרת צו המצאה אישי בהליך פלילי (כמו גם בהליך אזרחי), לכפות על שלוחה מקומית של חברה זרה לספק נתונים האגורים ברשות החברה הזרה מחוץ לשטחי ארצות הברית.¹¹⁸ כן ניתן לציין בהקשר זה כי בית המשפט העליון

אליהם, באמצעות סיסמא, דרך כל מחשב המחובר לאינטרנט, בכל מקום ברחבי העולם, להדפיסם ולקבל את המידע בדרך של מסמך. התפתחויות אלה מחלישות במידה רבה את הקשר בין הנגישות או הזמינות של חפץ לבין החזקתו הפיזית. הן מלמדות כי מהעדר החזקתו הפיזית של החפץ, אין לגזור בהכרח את היעדר הנגישות אל אותו חפץ. בנסיבות אלה, כדי לקיים את תכליתו של סעיף 43 בנסיבות חיינו כיום, תכלית שהיא קידום החקירה או המשפט, מן הראוי לפרש את סעיף 43 כך שצו על פיו יוכל להשתרע גם על חפצים אשר למי שהצו מופנה אליו שליטה עליהם במובן זה שבכווח למסרם או להציגם.

גם בתחום סדרי הדין האזרחיים הוכרה אפשרות להוצאת צווים אישיים בעלי תחולה אקסטר-טריטוריאלית. תקנה 383 לתקנות סדר הדין האזרחי, התשמ"ד-1984 קבעה את הסמכות להוציא צו Mareva לאדם להימנע מלעשות דיספוזיציות בנכסים שברשותו. הסמכות להוציא צו Mareva הוכנסה לתקנות סדר הדין האזרחי בשנת 2001. סמכות זו הוכרה לראשונה בפסק הדין האנגלי המפורסם: *Mareva Compania Naviera SA v. International Bulkcarriers SA*, [1980] 1 All E.R. 213 (Eng. C.A.). בעניין בנק סטנדרט צ'רטר הכיר השופט ריבלין בתחולה הבין-לאומית של צו ה-Mareva על פי תקנות סדר הדין האזרחי, וזאת על בסיס נוסחו ה"אישי", בניגוד לנוסח "קנייני". ראו רע"א 4556/03 בנק סטנדרט צ'רטר – תאגיד חוף נ' קטב, פ"ד נו(6) 1, 6-7 (2003). במילים אחרות, הנמען לצו הוא העיקר ולא הנכס מושא הצו, ועל כן ניתן להכיר בתחולתו האקסטר-טריטוריאלית של הצו. אם הנמען לצו ה-Mareva אינו מצוי לצו, הסנקציה היא בזיון בית המשפט. דוגמה נוספת מומחשת בפרשת רייפמן. באותו מקרה ננקטו הליכי פשיטת רגל נגד רייפמן, והמנהל המיוחד שמונה לפי פקודת פשיטת הרגל הורה לו מכוח סעיף 56(ב) לפקודה למסור את החזקותיו במניות חברת אמבלייז אשר נסחרו בבורסה בלונדון. ראו סעיף 56(ב) לפקודת פשיטת הרגל [נוסח חדש], התש"ם-1980; רע"א 6067/09 רייפמן נ' CCM Master Qualified Fund LTD (פורסם בנבו, 23.8.2009); ע"פ 7174/09 רייפמן נ' ארז (פורסם בנבו, 21.9.2009). ליישום נוסף של צו Mareva בזיקה בין-לאומית, ראו הפ"ב (מחזית ת"א) 23485-02-10 ממסטבלוב נ' Tchaturia (פורסם בנבו, 16.3.2010). לשורשים ישנים יותר של הסמכות להורות לתושבים ישראלים למסור מניות שהם מחזיקים בבנקים בחו"ל ראו עניין אמסטרדם, לעיל ה"ש 2. עם זאת גם בסדרי הדין האזרחיים הנחת המוצא היא שאין סמכות להעניק סעד על פעילות מחוץ לגבולות המדינה. ראו למשל רע"א 8831/05 הרר נ' דיאליט בע"מ (פורסם בנבו, 29.8.2006); אורי גורן סוגיות בסדר דין אזרחי 536 (מהדורה אחת עשרה, 2013).

117 תב"כ 5/20 התנועה לאיכות השלטון בישראל נ' חבר הכנסת בנימין נתניהו, ראש הממשלה, בפס' 30 (פורסם בנבו, 20.1.2015).

118 ראו Todd Jones, *Compulsion Over Comity: The United States' Assault on Foreign Bank Secrecy*, 12 N.W. J. INTL. L. & BUS. 454 (1992), שם סוקר המחבר את התפתחות הפסיקה האמריקנית,

האמריקני הכיר באפשרות לכפות על מתדיין זר בערכאה אמריקנית להמציא נתונים המצויים בבנק מחוץ לארצות הברית, וכי חובתו של המתדיין הזר במקרה כזה לפעול על פי מיטב יכולתו לנסות ולהמציא את הנתונים המבוקשים.¹¹⁹ פסיקה דומה מצויה גם בקנדה.¹²⁰ עוד במשפט האמריקני, לאחרונה התפתח מאבק משפטי סביב דרישתו של בית משפט אמריקני מחברת מיקרוסופט (חברה אמריקנית) להמציא תכנים מחשבון דוא"ל של לקוחה לצורך קידום חקירה פלילית, כאשר תכנים אלה אגורים בשרתי החברה באירלנד.¹²¹ מיקרוסופט התנגדה לבקשה בטענה שלמעשה מדובר בצו אקסטרה-טריטוריאלי, המחיל את סטנדרט הפרטיות האמריקני כלפי אירלנד ופוגע למעשה בריבונות הארית. נכון לעת הזאת קנו לעצמם בתי המשפט האמריקנים סמכות בסיטואציה זו.¹²² פרשה מעניינת נוספת, הדומה במידת מה לפרשת מיקרוסופט האמריקנית, היא הפרשה הנוגעת למאבק המשפטי שניהלה Yahoo! עם הרשויות בבלגיה. בפרשה זו ציווה התובע הבלגי על נציגות יאהו! בבלגיה להסגיר תכנים של תיבות דוא"ל של יאהו!, אשר על פי החשד שימשו לביצוע עברות מרמה.¹²³ יאהו! סירבה לציית להוראה בטענה שמדובר בתיבות דוא"ל המנוהלות בידי שרתי החברה מחוץ לטריטוריה הבלגית, ועל כן הדרך לקבל את תוכן היא

האזרחית כמו גם הפלילית, בנוגע לצווי המצאה לבנקים זרים, בעלי שלוחה אמריקנית. מצד אחד טענו הבנקים הזרים לפגיעה בחיסיון הבנקאי כפי נוסחו במדינה הזרה, ומצד שני, עמד על הפרק האינטרס האמריקני לחקר האמת ולקיום הליך שיפוטי הוגן שבו ייחשף החומר הרלוונטי לשני בעלי הדין. ראו Gary E. Davidson, *Congressional Extraterritorial Investigative Powers: Real or Illusory?*, 8 EMORY INT'L L. REV. 99, 106-120 (1994).

ראו 119 Societe Internationale pour Participations Industrielles et Commerciales v. Rogers, 357 U.S. 197 (1958). באותו מקרה דובר בתביעה של חברה שווייצרית נגד ממשלת ארצות הברית בפני ערכאה אמריקנית. ממשלת ארצות הברית עתרה להורות לתובעת להמציא נתונים בנקאיים שווייצריים. התובעת טענה כי לא תוכל להמציא את הנתונים האמורים, כיוון שיהיה בכך משום הפרה של דיני הסודיות הבנקאית השווייצרית, כמו גם עברה של ריגול (בשל הסגרת הנתונים למדינה זרה). בערכאה הראשונה קבע בית המשפט כי היות שהתובעת השווייצרית לא המציאה את הנתונים שנצטוותה להמציא, תימחק התביעה האזרחית שהגישה. בבית המשפט העליון הפכו את התוצאה האופרטיבית של הערכאה הדיונית, אם כי קבעו את העיקרון של חובת מילוייה של הוראת המצאה של בית המשפט האמריקני. נקבע כי ברמה העקרונית דיני החיסיון הבנקאי הזר, ואף החשש שהמצאת הנתונים תהווה עברת ריגול, אינם יכולים לחסן מראש מפני מילוי הוראות בית המשפט האמריקני. עם זאת ברי כי אין ביכולתו של המתדיין הזר לכפות על הבנק בשווייץ למלא את בקשותיו, וכאן למעשה נעצרת השליטה האקסטרה-טריטוריאלי של בית המשפט האמריקני.

ראו 120 eBay Canada Ltd. v. M.N.R., [2010] 1 F.C.R. 145 (Ca.). ייתכן בהחלט שאילו הייתה מיקרוסופט נדרשת להמציא מידע עסקי שלה, האגור בשרת בחו"ל, לא היה המאבק המשפטי מתחולל, היות שמדובר במידע של הנמען לצו ישירות. בענייננו, הצו השיפוטי מתייחס למידע של לקוח של מיקרוסופט, כאשר מידע זה אגור מחוץ לטריטוריה האמריקנית.

ראו 122 In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y., 2014). מיקרוסופט ביקשה להתנגד לצו, ובקשתה נדחתה בבית המשפט הפדרלי המחוזי. כעת הוגש ערעור לבית המשפט הפדרלי לערעורים. לקראת דיון זה הוגשו כמה עמדות של "ידידי בית המשפט", ובהם ממשלת אירלנד, ארגוני זכויות אדם וכן ספקיות שירות שונות ברשת שאינן צד להתדיינות הקונקרטי. למעקב אחר ההליכים ראו <http://digitalconstitution.com/about-the-case>.

123 על פי הדין הבלגי, קבלת תוכן של תיבת דוא"ל יכולה להתבצע על פי הוראה הניתנת כשורה בידי תובע מוסמך, ואין דרישה להסמכה בצו שיפוטי.

באמצעות בקשה לעזרה משפטית מארצות הברית, שם מוחזקים השרתים. בית המשפט הבלגי לערעורים קבע כי יאהו! בבלגיה מחויבת לציית להוראה שנתן התובע הבלגי. זאת על בסיס תפישה מקסימליסטית,¹²⁴ הגורסת שכל עוד יאהו! לא פעלה לחסימת משתמשים מבלגיה, על פי כתובת ה-IP שלהם, הרי שיאהו! מוחזקת כמי שהסכימה להיכפף לסמכות השיפוט והאכיפה הבלגית. על כן עליה לציית להוראות שניתנו כשורה על-ידי רשויות אכיפת החוק בבלגיה, אף אם המידע המבוקש אגור בשרתי החברה מחוץ לטריטוריה הבלגית.¹²⁵

3. התפישה הטריטוריאלית והצעת חוק החיפוש

הצעת חוק החיפוש, אשר פורסמה כאמור בשנת 2014,¹²⁶ מגלמת תפישה טריטוריאלית באשר לדיני איסוף הראיות, בתוספת ניסיון מעשי להגמיש את האיסור על אכיפה פלילית אקסטרה-טריטוריאלית בכמה נקודות. אציג תחילה את ביטויי התפישה הטריטוריאלית שבהצעת חוק החיפוש ולאחר מכן את החריגות שהותרו לפיה.

א) איתור התפישה הטריטוריאלית בהצעת חוק החיפוש

בדומה לחוקים אחרים במשפט הישראלי הנוגעים לסמכויות אכיפה של המדינה, אין בהצעת חוק החיפוש הוראה מפורשת הקובעת את מגבלת הטריטוריאליות. המגבלה צרובה בדנ"א של הצעת החוק, והיא נתפשת כמובנת מאליה. כיצד בכל זאת ניתן ללמוד על התפישה הטריטוריאלית החולשת על הצעת חוק החיפוש? ראשית, כיוון שהצעת החוק שותקת לעניין השאלה העקרונית של תחולת דיני האכיפה של מדינת ישראל אל מעבר לטריטוריה שלה, חל הדין הכללי בנושא זה, אשר כפי שהראיתי לעיל, מניח הנחת טריטוריאליות, על פי המקובל גם במשפטן של מדינות אחרות ובמשפט הבין-לאומי. מלבד זאת, ברמה הקונקרטית ניתן להבחין כי לשונה של הצעת החוק משופעת במילים המבטאות תפישה טריטוריאלית באשר לראיות הדיגיטליות. ההצעה מדברת, בכמה הזדמנויות, על ה"מקום" שבו מצוי חומר המחשב, ומכאן שההצעה מבטאת את הגישה שלפיה הראיה הדיגיטלית ניתנת למיקום, וכי המקום הוא השרת שבו מצוי חומר המחשב.

החריגות האקסטרה-טריטוריאליות, שיפורטו מיד בהמשך, אף הן למעשה משתקות את התפישה הטריטוריאלית, בבחינת יוצא מן הכלל המעיד על הכלל: מעצם העובדה שהצעת החוק נוקבת בכמה מקומות במפורש שמותר איסוף של חומר מחשב בכל מקום שבו הוא נמצא, לרבות בחו"ל, נובע שלשיטת מנסחי הצעת החוק, במקום שלא צוין הדבר – אסור לעשות כן. יתרה מזאת, גם עצם ההכרה בחריגה אקסטרה-טריטוריאלית מבטאת, ברמה התפשטית, הכרה בכך שמיקום אגירת הראיה הוא הקובע.

124 תפישה זו מתיישבת עם גישתה מרחיבת-הסמכות של בלגיה, הניכרת גם בכל הנוגע לסמכות המוכרת בדין הפנימי הבלגי, ואשר נסקרה לעיל, לעריכת חיפושים בחומרי מחשב האגורים מחוץ לטריטוריה הבלגית. ראו לעיל בעמ' 144.

125 הכרעתו המתורגמת של בית המשפט לערעורים בבלגיה (Yahoo! Inc.) (2012/CO/1054) מיום 20.11.2013 מצויה בכתובת: <http://journals.sas.ac.uk/deeslr/article/view/2138/2068>.

126 ראו לעיל ה"ש 98.

ב) החריגות שהותרו בהצעת חוק החיפוש

כאמור, על פי המשפט הישראלי אין היתר לפעולות אוניטרליות לאיסוף ראיות אקסטרנה-טריטוריאליות, בחריג אחד, שנפסק בעניין שרון, של צו המצאה אישי המופנה לאדם המצוי בישראל בדבר חומרים שיש לו גישה אליהם, המצויים מחוץ לטריטוריה הישראלית (וייתכן שנוסף על זה חל גם החריג של גישה למידע ממוחשב הנגיש לכלל הציבור). במסגרת הצעת חוק החיפוש נעשה ניסיון ראשון לעגן בחקיקה היתרים לפעולות בעלות השלכה אקסטרנה-טריטוריאליה בארבע נקודות:

הראשונה, צו המצאה בעל נפקות אקסטרנה-טריטוריאליה. סעיף 73(א) להצעת חוק החיפוש קובע כי אם שוכנע בית המשפט בדבר קיומן של עילות למתן צו המצאה "בנוגע לחומר מחשב הקשור לעבירה, רשאי הוא לצוות על בעל הגישה לחומר המחשב להמציאו במועד, במקום ובתנאים שיקבע". סעיף זה שותק לעניין תחולתו האקסטרנה-טריטוריאליה, אלא שהגדרת "בעל גישה" לחומר מחשב, בסעיף 72 להצעת החוק, קובעת כי הלה ייחשב "מי שהוא בעל גישה לחומר המחשב, בין שחומר המחשב מצוי בישראל ובין שהוא מצוי מחוץ לישראל, ובכל זה ספק שירות" (ההדגשות שלי – ח'ו). קריאת שני הסעיפים יחדיו מלמדת כי מוצע שיהיה אפשר למסור צו המצאה לבעל גישה לחומר מחשב, שיחייבו למסור גם חומר מחשב האגור בחו"ל, אם הוא בעל גישה אליו. אם נשוב אל עניין שרון, באותו מקרה דיבר בית המשפט העליון במושגים של נגישות, זמינות המידע ושליטה עליו ללא החזקה פיזית של המחשב שבו מצוי המידע. הדוגמה שהביא בית המשפט נגעה לשירותי בנקאות באמצעות האינטרנט ולשירותי דוא"ל על ידי ספק שירות המצוי בחו"ל. בשתי דוגמאות אלה כיוון בית המשפט את דבריו ללקוחות המנויים על שירותים אלה ולא אל ספקיות השירות עצמן. הצעת החוק צועדת צעד נוסף במשעול זה וקובעת כי גם ספק שירות, גם מנהל רשת, גם מעביד המחזיק בשליטה על חומרי המחשב של עובדיו – כל אלה יכולים להידרש להמציא חומרים של אחר האגורים בחו"ל, ובלבד שהחומרים האלה בני גישה מבחינתם. יתרה מזאת ההמצאה בידי אותם צדדים שלישיים יכול שתיעשה בלא ידיעת החשוד (שהוא, אינטואיטיבית, מי שנכנה "בעל החומרים")¹²⁷.

השנייה, הצעת חוק החיפוש מציעה להכיר בסמכות שמירת מידע (preservation). על הצורך בהכרה בסמכות זו ארחיב בפרק הבא, שבו אנתח את התפישה הפיזית באשר לראיות הדיגיטליות ואת פעולות איסוף הראיות המוחמצות בעקבות תפישה זו. בהקשרו הנדון עתה, הרי שבדומה להוראות בנוגע לצווי המצאה, מצוין בהצעת החוק שגם צווי שמירה יכולים לחול

127 סעיף 8(ב) להצעת חוק החיפוש קובע באשר לצווי המצאה של מוצגים חפציים כלל שלפיו הנמען לצו ההמצאה לא יגלה את תוכנו של הצו או את דבר ביצועו. החריג, כך על פי סעיף, הוא "אם התיר זאת בית המשפט בצו". סעיף זה יוחל, לפי סעיף 80 להצעת החוק, גם על צווי המצאה של חומר מחשב. סעיף 76 מורה כי "בהחלטה למתן צו כאמור המופנה לספק שירות שאינו החשוד בעבירה, י שקול בית המשפט את האפשרות להורות למשטרה ליידע את החשוד על ביצוע הצו". במילים אחרות, בררת המחל, על פי הצעת החוק, היא אי-גילוי, אם כי בית המשפט נדרש להתייחס לנושא של צו המצאה שמופנה לספק שירות בנוגע ללקוחו ולשקול את גילוי דבר ביצוע הצו לחשוד שבנוגע למידע שלו הוצא הצו.

על חומרי מחשב האגורים בחו"ל, ובלבד שלנמען לצו הייתה הרשאה או גישה אל החומרים האלה.¹²⁸

השלישית, בהצעת החוק נקבע כי חדירה בהסכמה של "בעל הרשאת גישה" לחומר המחשב תוכל להתבצע בכל מקום שבו אגור חומר המחשב. סעיף 90(א) להצעת החוק מורה כי שוטר ראשי לבצע חדירה לחומר מחשב בלא צו בית משפט אם "בעל הרשאת הגישה" לחומר המחשב הסכים לכך ובהתקיים אחת מהעילות למתן צו חדירה למחשב.¹²⁹ "בעל הרשאת גישה" לחומר מחשב מוגדר, בסעיף 72 להצעת חוק החיפוש: "בגיר שיש לו הרשאת גישה לחומר מחשב, בין שחומר המחשב מצוי בישראל ובין שהוא מצוי מחוץ לישראל" (ההדגשות שלי – ח' ו').

על פי הרציונל של הצעת חוק החיפוש, הסכמתו של בעל הרשאת הגישה לחומר המחשב יכולה להתפרש אל חומרי מחשב האגורים מחוץ למדינת ישראל, אולם צו שיפוטי המסמך את הרשות החוקרת לחדור לחומר מחשב (בלא הסכמת בעל הרשאת הגישה) אינו יכול להתפרש אל חומרים אלה. רציונל זה אינו ייחודי להצעת החוק. גם אמנת מועצת אירופה בדבר פשעי מחשב, בסעיף 32, מתירה חדירה אקסטרה-טריטוריאלית לחומר מחשב רק במקרה של הסכמה כדין של המחזיק בחומר המחשב ולא במקרה של צו שיפוטי כופה המתיר חדירה.

הרביעית, חדירה לחומר מחשב הפתוח לכלל הציבור. סעיף 97(ב) להצעת החוק קובע כי "חומר מחשב הפתוח לעיון הציבור בין שחומר המחשב מצוי בישראל ובין שהוא מצוי מחוץ לישראל, בין בתשלום ובין שלא בתשלום" (ההדגשות שלי – ח' ו') – לא ייחשב ככזה המחייב צו חדירה לצורך עיון בו על ידי הרשות החוקרת, והרשות החוקרת לא תוגבל טריטוריאלית לפי מקום אגירתו של חומר המחשב. בדברי ההסבר לסעיף זה מפנה הצעת החוק לאמנת מועצת אירופה בדבר פשעי מחשב, המתירה, בסעיף 32, חריגה אקסטרה-טריטוריאלית במקרה של חומר הפתוח לעיון הציבור ולשימוש.

4. סיכום

התפישה הטריטוריאלית באשר לאיסוף ראיות דיגיטליות במסגרת חקירה פלילית במרחב הסייבר מתבטאת בפגיעה ממשית ביכולת החקירה המדינתית במרחב. היא מייצרת מעין כלל וטו שלפיו כל אימת שהראיה הדיגיטלית אגורה במחשב מחוץ לטריטוריה, הרי שאיסוף הראיה הוא פעולה אקסטרה-טריטוריאלית החורגת מכללי סמכות האכיפה הבין-לאומית. מדינות שונות ניסו להגיע להסכמה מולטי-טריטוריאלית באשר לסיטואציות חקירתיות שבהן תותר פעולה בעלת מאפיינים אקסטרה-טריטוריאליים. כמו כן מדינות שונות פרצו בכמה סוגיות את גדריו הנוקשים

128 ראו סעיף 74(א) להצעת החוק, המתייחס לצו שמירה המופנה ל"בעל הגישה לחומר המחשב", כאשר הגדרת "בעל הגישה לחומר המחשב" לעניין זה זהה להגדרת "בעל הגישה" באשר להמצאת חומר מחשב. אציין עוד כי בדומה לצווי המצאה, גם בנוגע לצווי שמירה נדרש ככלל הנמען לצו, לרבות ספק שירות, לשמור על סודיות הצו. ראו סעיף 80 ועמו את סעיף 8(ב) וסעיף 76.

129 חדירה לחומר מחשב בהסכמה, ללא צו שיפוטי, כוללת הגבלות והסתייגויות שונות בנוגע לטיב ההסכמה ומגבלותיה. כך, למשל, נדרש כי המסכים יהיה "בעל הרשאת גישה" ולא "בעל גישה", כפי שנקבע לעיל בנוגע לנמענים לצווי המצאה או שמירה. ועוד, סעיף 90(ב) להצעת החוק מונה שורה של מגבלות נוספות, ולפיהן: ספק שירות אינו ראוי לתת הסכמה לחדירה בלא צו כשמדובר בחומר מחשב של לקוחו; מעביד ככלל לא יוכל לתת הסכמה כשמדובר בחומר מחשב פרטי של עובדו; ההסכמה יכולה להיות מסויגת כשמדובר בחומרי מחשב מסוימים בלבד מתוך המחשב.

של כלל הווטו הטריטוריאלי בנוגע לסמכות איסוף ראיות המצויות במחשבים שמחוץ לטריטוריה. לאור זאת בחנתי את הוראות הצעת חוק החיפוש, המבקשות גם הן להתיר בדין הישראלי כמה חריגות אקסטרה-טריטוריאליות בחקירה הפלילית במרחב הסייבר (חלק מההוראות מעגנות פסיקה או פרקטיקה נוהגת וחלקן מחדשות).

חריגות אלה מעידות על הקושי המעשי הממשי בניהול חקירה פלילית במרחב הסייבר בהתאם למגבלות הטריטוריאליות של המרחב הפיזי. לצד הצורך המעשי כאמור, אציג בהמשך ביקורות המבקשות לתקוף את עצם ההצדקה לקיומה של התפישה הטריטוריאלית באשר לחקירה הפלילית במרחב הסייבר.

1. פריצת גבולות התפישה הטריטוריאלית באשר למרחב הסייבר – דיון נורמטיבי

אציג שלוש ביקורות שונות נגד יישומה של התפישה הטריטוריאלית על החקירה הפלילית במרחב הסייבר. הביקורת הראשונה תתמקד במשמעות המיקום של המידע והיישומים בתוך מרחב הסייבר לצורך קביעת כללי סמכות אכיפה בין-לאומית. הביקורת השנייה תתמקד בפעולות איסוף הראיות עצמן תוך עמידה על ארכיטקטורת הרשת, אופן השימוש בה ומאפייניהן של פעולות האיסוף בתוכה מבחינה טכנולוגית. הביקורת השלישית תבחן כיצד תאוריות על מושג ה"ריבונות" יכולות להצדיק סטייה מהתפישה הטריטוריאלית כפי שהיא חולשת כיום על דיני איסוף הראיות במרחב הסייבר. אבקש להקדים ולהדגיש כי מטרת ההצגת הביקורות הללו אינה להצדיק הצדקה גורפת פעולה של הרשות החוקרת המדינית כלפי כל סוגי הראיות הדיגיטליות במרחב הסייבר בכל מקום שבו הן מצויות (או נחשבות כמצויות). במילים אחרות, הביקורות הללו אינן מאיינות את משמעות המיקום, או את משמעות הטריטוריאליזם, ביחס למרחב הסייבר, אלא הן מבקשות לערער את יסודות התפישה הטריטוריאלית במרחב כפי שהיא התעצבה כיום.

1.1. ביקורת אפיסטמולוגית

כפי שהראיתי, התפישה הטריטוריאלית מתבטאת בשלושה עיקרים: הראיה הדיגיטלית ניתנת למיקום; מיקומה הוא המחשב שבו היא מאוחסנת; מקום איסוף הראיה נחשב למקום שבו מאוחסנת הראיה הדיגיטלית. הביקורת האפיסטמולוגית מתמקדת ביסוד הראשון, כי הראיה הדיגיטלית ניתנת למיקום. על פי ביקורת זו, היסוד הראשון קורס בכל הנוגע לזירה הקיברנטית. הביקורת האפיסטמולוגית נשענת על נקודת מוצא שלפיה ההתבוננות על מרחב הסייבר במונחים של מקום היא מטאפורית. הביקורת מתמקדת פחות בשאלה אם המרחב הקיברנטי, כמכלול, הוא מקום נפרד או שונה מהמקום הפיזי ויותר בתוככי המרחב המקוון, וגורסת כי למיקום המידע והיישומים בו אין משמעות דומה לזו המוענקת למיקומם של חפצים במרחב הפיזי.¹³⁰ גם אם ניתן לשייך בנקודת זמן נתונה את המידע הדיגיטלי המבוקש כראיה למחשב

130 על כן הביקורת יכולה לדור בכפיפה אחת הן עם התפישה שלפיה המרחב הקיברנטי הוא מקום אחד, נפרד מהמרחב הפיזי, והן עם התפישה שלפיה המרחב הקיברנטי אינו צריך להיתפש כלל כ"מקום" אלא

מסוים ברשת, וגם אם ניתן לדעת את מיקומו של המחשב המסוים האמור מראש, כנדרש מבחינתה של הרשות החוקרת לצורך בחינת סמכותה הבין-לאומית, עדיין המשמעויות של מיקום זה והפונקציות שהוא משרת אינן אותן המשמעויות והפונקציות המוענקות ל"מיקום" במרחב הפיזי. לכן לצד הקליפה הטכנית של אפשרות ההצבעה על מיקום הראיה לא יהיה לה מלבד זאת גרעין מהותי, ועל כן ניתן לומר שלא יהיה מדובר למעשה במיקום של ממש, על כל משמעויותיו ונפקויותיו המשפטיות.¹³¹

במרחב הפיזי ל"מיקום" חפצים בתוך "מקום" יש משמעות. כך למשל המיקום במרחב הפיזי הוא אחד, ואינו ניתן לשכפול או לביזור. המיקום נותר סטטי לאחר בחירתו. לפיכך בעל השליטה בחפץ הבוחר את מיקומו של החפץ מבצע פעולה בעלת משמעות פיזית, אך גם משפטית. הוא מניח את החפץ במרחב פיזי ובמרחב משפטי כהחלטה מודעת. במרחב הסייבר אין למיקום המידע והיישומים שבתוכו משמעות בעלת ערך כפי שמתקיים במרחב הפיזי. לכן ניתן לטעון כי לא צריכה להיות למיקום המידע (הראייתי בפוטנציה) במרחב הסייבר משמעות משפטית. על מנת להמחיש את הטיעון אציג שלוש דוגמאות:

1. ראובן ושמעון מחליטים לפתוח חשבון דוא"ל הניתן לגישה מכל מחשב המחובר לאינטרנט (Webmail). ראובן מחליט לפתוח את החשבון בשירות הדוא"ל של חברת וואלה הישראלית, ואילו שמעון מחליט לפתוח את החשבון בשירות Gmail של גוגל האמריקנית. סביר להניח שהפרמטרים שיעניינו את ראובן ואת שמעון בהחליטם לפתוח את חשבונות הדוא"ל הם אמניות השירות, יכולות סינון דואר הזבל, נפח האחסון של הדוא"ל בתיבה וכדומה. עוד סביר להניח שהפרמטר של מיקום שרתי הדוא"ל של החברות לא יעניין במיוחד את ראובן ושמעון. יתר על כן, ייתכן בהחלט שמיקום שרתי הדוא"ל לא יהיה ידוע כלל לראובן ולשמעון. לא זו אף זו, אלא שגם מבחינת ספקיות שירותי הדוא"ל לא יהיה חשוב כלל מהיכן נרשם משתמש האינטרנט לשירותי הדוא"ל האמורים. גם מבחינת המדינות שבהן פועלות ספקיות שירותי הדוא"ל אין כל פיקוח, לא מראש ולא בדיעבד, על הנרשמים לשירות. עוד סביר להניח כי גם מבחינת האנשים המתכתבים בדוא"ל עם ראובן ועם שמעון אין כל משמעות לבחירתם בשירות הדוא"ל של וואלה או של Gmail. במילים אחרות, כל הצדדים הנוגעים, במישרין או בעקיפין, לעולם הדוא"ל אינם מעניקים משמעות לסוגיית המיקום של שרתי הדוא"ל או של משתמשי השירות.

2. שירותי מחשוב ענן (Cloud Computing) מבקשים לשנות את האופן שבו משתמשי האינטרנט צורכים שירותי מחשוב כגון הפעלת יישומים ואגירת מידע. שירותים אלה מתבצעים

כמדיום לביצוע התקשרויות, כאמצעי או כמכשיר, ולא כמרחב שאליו המשתמש נכנס. לתפישת המרחב הקיברנטי כמקום אחד, נפרד, ראו למשל Johnson & Post, *Law and Borders*, לעיל ה"ש 55. וליישום פסיקתי של גישה זו ראו Voyer Dorm, L.C. v. City of Tampa, 265 F. 3d 1232, 1236 (11th Cir., 2001). לתפישת המרחב הקיברנטי כמדיום ולא כמקום ראו למשל ANDREW L. SHAPIRO, *THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW* 710-712 (1999).

131 טיעון אפיסטמולוגי כללי זה נתמך בתאוריות מודרניות של גאוגרפיה פוליטית (Political Geography). ראו למשל Eric Fischer, *On Boundaries*, 1 WORLD POLITICS 196 (1949); Julian V. Minghi, *Boundary Studies in Political Geography*, in THE STRUCTURE OF POLITICAL GEOGRAPHY 140, 146 (Roger E. Kasperson & Julian V. Minghi eds., 1969).

מתוך ה"ענן", שהוא בבחינת "קופסה שחורה" מבחינתו של משתמש האינטרנט, שמטרתה לספק שירותים מוזלים, יעילים ואמינים.¹³² לא בכדי המטאפורה שנבחרה לשירותים אלה היא מטאפורת ה"ענן", שהוא מקום מעורפל, הנמצא בתנועה ובשינוי ואינו מאפשר למקם דברים בתוכו. בעיני משתמש האינטרנט אין ל"מקום" שבו נאגר המידע שלו או שממנו מסופקים לו השירותים היישומיים משמעות, ולרוב הוא גם אינו ידוע לו.¹³³ משתמש האינטרנט אינו עובר כל תהליך של הכרה במיקומו של ה"ענן", לא כל שכן במיקומם של הדברים בתוך הענן, וכך אין הוא עובר את התהליך ההופכי, של עצימת עיניים במודע באשר למיקומו של ה"ענן" ומיקומי המשנה בתוכו.

3. משתמש האינטרנט מישאל מחליט לגלוש לאתר אינטרנט מסוים. אתר האינטרנט, לצורך הדוגמה, אגור בשרתים בארצות הברית. בשל ריבוי הגולשים מישראל לאותו אתר אינטרנט מחליט ספק הגישה לאינטרנט לבצע פעולת caching, קרי העתקה של תוכן האתר אל שרתיו בישראל והספקת תכניו למנוייו במהירות ותוך הוצלת העלויות של הגלישה בכל פעם מחדש דרך הכבלים התת־ימיים של האינטרנט אל השרת בחו"ל. מבחינת משתמש האינטרנט, אין כל משמעות לכך שהוא גולש למעשה אל שרתי ספק הגישה לאינטרנט ולא אל אתר האינטרנט האמריקני עצמו. מבחינת אתר האינטרנט האמריקני, תהליך ה־caching נעשה בלי ידיעתו.¹³⁴ דוגמה נוספת היא כאשר אתר האינטרנט עצמו, ולא ספק הגישה לאינטרנט, מחליט לבצע פעולת redirection לכל משתמש אינטרנט המגיע אל האתר שלו. ה־redirection יכול שייעשה לצורכי תחזוקת השרת שבו נמצא אתר האינטרנט, או מטעמים של החלפת שרת אחסון של האתר, או מטעמים של ויסות עומסים על השרת (בשל ריבוי משתמשי אינטרנט המבקשים להיכנס לאתר, יחסית למספר משתמשי האינטרנט שיכולים להיכנס אליו בזמנית). פעולת ה־redirection יכול שתעביר את משתמש האינטרנט משרת אחסון של האתר המצוי במדינה א לשרת אחר המצוי במדינה ב. מבחינת משתמש האינטרנט, וייתכן גם שלעתים מבחינת מנהל השרת, אין משמעות למעבר זה.

דוגמאות אלה ממחישות כי קיימות סיטואציות טיפוסיות שונות של שימוש במרחב הסייבר שבהן המשתמש אינו מייחס חשיבות למיקומם של חלק ניכר מן המופעים במרחב.¹³⁵ גם מבחינת כל שאר הצדדים הנוגעים בדבר, החל מספקית השירות, דרך המדינה שבה מצוי השרת ועד לצדדים שלישיים שעמם בא משתמש המחשב במגע – לעתים מזומנות אין משמעות לשאלת המיקום. לבד מאי־משמעות המיקום של המידע והיישומים במרחב הסייבר ושל אופן מיקומם בעיני המשתמש ושאר הנוגעים בדבר, ניתן לטעון מנגד כי אם נחיל בדיוקנות מבחן

132 ראו גם בפרק ב לעיל, בה"ש 58.

133 ראו United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime 140–141 (Draft – February 2013) http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

134 דוגמה זו הביא כבר בשנת 1998 ג'ואל ריידנברג (Reidenberg), ראו Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553, 564 (1998).

135 לטיעון ברוח זו, בדבר ניליות המידע במרחב הסייבר, המביאה לאבדן משמעות המיקום של המידע, ראו Jennifer Daskal, *The Un-Territoriality of Data*, YALE L.J. 26–28 (Forthcoming 2016), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2578229.

שקובע סמכות אכיפה של המדינה לפי מקום הימצא הראיה הדיגיטלית, ובה בעת שולל סמכות אכיפה כזאת מכל שאר מדינות העולם, הרי שבדוגמאות אלה, בעיקר בדוגמה האחרונה של שימוש ב־*redirecting* ו־*caching*, עשויות מדינות שונות לאחוז בסמכות בלעדית, בשל פרמטר שולי יחסית בנסיבות המקרה – שעשוי לנבוע מסיבות טכניות ולהיות זמני במהותו – ולא בשל זיקות מהותיות הנוגעות לטיב הפעולה או השירות המקוון שבהם מדובר.

בסיכומו של דבר, ההנחה שבבסיס התפישה הטריטוריאלית באשר לאיסוף ראיות בחקירה פלילית במרחב הסייבר, שלפיה הראיה הדיגיטלית ניתנת למיקום בתוך המרחב הקיברנטי, אינה תואמת את האופן שבו נתפש המרחב הקיברנטי, בנסיבות מסוימות, בעיני משתמשיו כמו גם בעיני המדינות הרלוונטיות השונות. הביקורת האפיסטמולוגית גורסת כי אין ערך למיקום בתוככי המרחב הקיברנטי כפי שניתן לו במסגרת החלת התפישה הפיזית על סמכויות האיסוף של המדינה במרחב הקיברנטי. ביקורת זו סוללת את הדרך לטיעון העקרוני כי פעמים רבות אין להעניק אפוא גם משמעות משפטית למיקום המידע (כראיה) בתוך המרחב הקיברנטי.¹³⁶

2. ביקורת ארכיטקטונית וטכנולוגית

הביקורת הארכיטקטונית-טכנולוגית מכוונת כלפי שני היסודות האלה של התפישה הטריטוריאלית: היסוד שלפיו הראיה הדיגיטלית ניתנת לשיוך (ולפיכך למיקום) למחשב מסוים שבו היא מאוחסנת, והיסוד שלפיו אבן הבוחן לקביעת סמכות אכיפה בין-לאומית של המדינה החוקרת הוא מקום אחסונה של הראיה הדיגיטלית. ביקורת זו גורסת כי יסודות אלה קורסים בזירה הקיברנטית.

אציג תחילה את הביקורת על היסוד הראשון מבין השניים. על פי הביקורת, יסוד זה מציב "דרישת מסוימות", שלפיה יהיה ניתן להצביע על מקום מסוים מובהק בתוך המרחב המקוון שבו מצויה הראיה הדיגיטלית. ברם קשה לבודד, לבדל ולמקם מידע במרחב המקוון באופן שיוחס לכל פרט מידע מיקום מסוים וייחודי ברשת. ארכיטקטורת המרחב המקוון, בעיקר האינטרנט, היא מבוזרת מעצם טבעה. התקשורת בה מועברת בשיטה של פירוק ל־*packets* ושליחתן בנפרד ליעד, דרך מסלולים נפרדים. חלק מתופעות הפשיעה באינטרנט מנצלות את משאבי הרשת ואת אלמנט הביזוריות שלה. כך למשל התקפות של DDoS מגייסות מספר גדול של מחשבים תמימים המחוברים לרשת במקומות שונים בעולם, מקומות שאינם ידועים למפעיל המתקפה או לקרבנה. בדומה לזה, הפצת דואר זבל (SPAM) מבוססת על גיוס מחשבים רבים (Zombies) ממקומות שונים שאינם ידועים למפיץ.¹³⁷ מכאן שעלול להיווצר קושי לשייך כל מידע וכל פעולה ברשת למיקום פיזי אחד מסוים. יש לזכור כי כשעוסקים בדיני איסוף הראיות, ובעיקר בסמכות האיסוף של הרשות החוקרת מבחינה בין-לאומית, על רשויות החקירה לדעת מראש את מיקומן של הראיות הדיגיטליות שהן מבקשות לאסוף בטרם הן מבצעות את פעולת

136 מובן שביקורת זו מוגבלת לזווית ההתבוננות האפיסטמולוגית, המדגישה את ההכרה והענקת המשמעות למקום. ברי כי יכולה להישמע טענה כי שאלת המשמעות של המקום אינה צריכה להיות מכרעת. על פי טענה זו, המשפט יכווין את התנהגות הפרטים מבלי להתחשב במשמעות ההכוונה עבורם או עבור המדינות השונות.

137 ראו למשל אצל Nimrod Kozlovski, *A Paradigm Shift in Online Policing – Designing Accountable Policing* 63–66 (J.S.D. Dissertation, 2005).

האיסוף, על מנת שלא תימצאנה בדיעבד כמי שפועלות בחוסר סמכות. כיוון שבחינת מיקומה של הראיה הדיגיטלית נדרשת *ex ante*, הקושי באיתור המיקום מחריף עוד יותר. שתי התפתחויות מן העשור האחרון בדבר אופן השימוש באינטרנט תורמות להפיכת המקום באינטרנט לעניין נזיל עוד יותר. ההתפתחות הראשונה היא בדמות המעבר לאינטרנט 2.0, שבו משתמשי האינטרנט יוצרים ועורכים תכנים בעצמם. נניח אתר אינטרנט שמבוסס על שיתוף תוכני גולשים (לדוגמה רשת חברתית, אתר פורומים וכדומה). המידע והפעילות באתר מעוצבים ברובם בידי משתמשי האינטרנט, שבוחרים מתי ומהיכן להתחבר, איזה מידע להעלות ואיזה מידע להעתיק לרשותם. המידע שבאתר יכול להימצא בכמה מקומות בו־זמנית (בשרתי האתר ובמחשביהם האישיים של משתמשי האתר). אם המשתמשים יכולים גם למחוק את התכנים באתר, לפחות את אלה שהם העלו אליו, הרי שהמקום עשוי להיות נזיל: בפרק זמן מסוים הוא יכול להימצא בשרתים של האתר וברגע אחר ייעלם משם ויימצא רק במחשבים של המשתמשים שהורידו אותו עד למחיקתו. ההתפתחות השנייה היא בדמות המעבר לאינטרנט 3.0, המתאפיין בהנגשת האינטרנט למכשירים ניידים (סמארטפונים וטאבלטים) ואף לחפצים אחרים בשימוש יום־יומי והגברת הנגישות לאינטרנט ממקומות ציבוריים (Wireless networks).¹³⁸ אם בעבר נתפש משתמש האינטרנט כמצוי בנקודה קבועה, ואתרי האינטרנט שאליהם גלש היו המשתנה הדינמי בפעילותו באינטרנט, הרי שכיום גם משתמש האינטרנט דינמי, במובן זה שהוא יכול להשתמש באינטרנט מכל מקום. במילים אחרות, צריכת האינטרנט אינה עוד "מנקודה קבועה לכל מקום", אלא "מכל מקום לכל מקום".

עד כאן באשר לביקורת על שהראיה הדיגיטלית לא תמיד ניתנת לשיוך (ולפיכך למיקום) למחשב מסוים שבו היא מאוחסנת. עתה אציג את הביקורת על היסוד השלישי של התפישה הטריטוריאלית, שעל פיו אבן הבוחן לקביעת סמכות אכיפה בין־לאומית של המדינה החוקרת הוא מקום אחסונה של הראיה הדיגיטלית. כאמור, סמכות האכיפה נשמרת בקפידה יחסית כסמכות הצמודה לטריטוריה של המדינה. כך הוא במקרה של אכיפה במרחב הפיזי, וכך הוא במקרה של אכיפה במרחב האינטרנטי. אולם במרחב הפיזי המקרה הטיפוסי הוא שמושאי הפעולה, מבצעי הפעולה, הפעולה עצמה והראיה המבוקשת – מצויים ומתרחשים כולם באותו מקום.¹³⁹ כך למשל חיפוש בביתו של חשוד מתבצע כאשר הן השוטרים והן החשוד באותו מקום, החיפוש עצמו נערך במקום, וגם הראיה המבוקשת מצויה באותו המקום, קרי בבית החשוד. לפנינו "אחדות מרובעת" באשר לאיסוף ראיות בחקירה פלילית במרחב הפיזי. עם זאת המקרה הטיפוסי של איסוף ראיות במרחב המקוון שובר את האחדות המרובעת האמורה, ולפיו החוקר, החשוד, פעולת האיסוף והראיה המבוקשת לא חייבים להשתייך לאותו המקום ולאותה המדינה.

לפיתוח הטענה אפנה לעולם האזנות הסתר לתקשורת טלפונית, שבו פותחו תוכנות מסוימות הנוגעות לענייננו עוד טרם עידן הסייבר. עולם האזנות הסתר הטלפונית אפשר לערוך חלוקה

138 הצבעה על עלייה בהנגשת האינטרנט באמצעות מכשירים ניידים, ראו למשל את הנתונים של OECD בנושא המצביעים על גידול של 18% בשנת 2012 בהנגשת האינטרנט למכשירים ניידים ("mobile"). מספר חיבורי האינטרנט ה"ניידים" עבר באופן ניכר את מספר חיבורי האינטרנט ה"ניידים". ראו <http://www.oecd.org/internet/broadband/oecdbroadbandportal.htm>.

139 לטיעון ברוח דומה ראו Daskal, לעיל ה"ש 135, בעמ' 29–33.

משולשת בין מיקומים של כמה גורמים: החוקרת, רכיב ההאזנה (שם מואזנת השיחה בפועל, קרי מתבצעת פעולת האיסוף בפועל), משוחח א ומשוחח ב. נניח כי נעברה עברה המקימה סמכות שיפוט ישראלית, והעברה נחקרת במשטרת ישראל. כל אחד מארבעת הגורמים האלה יכול להיות בישראל או מחוצה לה, אם כי ברי כי החוקרת תפעל מישראל, שאם לא כן תימצא כמי שמפעילה סמכות שלטונית בטריטוריה זרה, ובכך יש כדי לפגוע בריבונותה של מדינה זרה. נוצרת קשת של אפשרויות כמפורט להלן (טבלה 3.1):

טבלה 3.1 – ספקטרום הסיטואציות האקסטרה-טריטוריאליות בהאזנת סתר

מס'	מיקומה של החוקרת	מיקום רכיב ההאזנה	משוחח א	משוחח ב
1	ישראל	ישראל	ישראל	ישראל
2		ישראל	חו"ל	ישראל
3		ישראל	ישראל	חו"ל
4		ישראל	חו"ל	חו"ל
5		חו"ל	ישראל	ישראל
6		חו"ל	חו"ל	ישראל
7		חו"ל	ישראל	חו"ל
8		חו"ל	חו"ל	חו"ל

כעולה מטבלה זו, כשמדובר בהאזנת סתר לתקשורת בין שני משוחחים – או ליתר דיוק שני טלפונים – בלבד, הרי שיכול שייווצרו שמונה סיטואציות עובדתיות שונות בכל הנוגע לשאלת המיקום הטריטוריאלי של הטלפונים המואזנים ושל רכיב ההאזנה (בישראל או בחו"ל). זאת, שוב, בהנחה שהשוטרת המבצעת את פעולת האיסוף נמצאת בישראל. ברי כי הסיטואציה שבשורה 1 לטבלה אינה מעוררת כל שאלה משפטית הקשורה לביצוע פעולת אכיפה אקסטרה-טריטוריאלית. עם זאת כל אחת מהסיטואציות האחרות מעוררת לכאורה סוגיה אקסטרה-טריטוריאלית במידה משתנה. הגישה הרווחת בישראל,¹⁴⁰ כמו גם בארצות הברית¹⁴¹

140 הדבר עולה מפרשת אל מצרי, לעיל ה"ש 20. לעמדה המבכרת את מיקומו של החשוד על פני מיקומו של רכיב ההאזנה, עמדה אשר לא התקבלה בעניין אל מצרי, ראו אלי וילצ'ק "קבילות ראיות שהושגו בחו"ל בהאזנת סתר" משפטים טז 462 (1986).

141 ראו United States v. Rodriguez, 968 F.2d 130 (2nd Cir., 1992); United States v. Tavaréz, 40 F.3d 1136 (10th Cir., 1994); United States v. Denman, 100 F.3d 399 (5th Cir., 1996); United States v. Ramirez, 112 F.3d 849 (7th Cir., 1997); United States v. Jackson, 471 F.3d 910 (7th Cir., 2000); State of New Hampshire v. Windhurst; United States v. Luong, 471 F.3d 1107 (9th Cir., 2006). לעיל ה"ש 18.

ובקנדה,¹⁴² היא שהמיקום הקובע לעניין עצם הסמכות לבצע את הפעולה הוא של רכיב ההאזנה ולא של יעד ההאזנה (או המשוחחים עמו).¹⁴³

דוגמת האזנות הסתר הטלפונית מעלה כי מקום ביצוע פעולת האיסוף עצמה קובע את ה"מקום" הרלוונטי לעניין בחינת סמכות האכיפה האקסטרה-טריטוריאלית. בדוגמת האזנת הסתר לא התעוררה ההבחנה בין מקום הביצוע של פעולת האיסוף לבין מקום הימצא הראיה המבוקשת, הבחנה רבת-חשיבות בכל הנוגע לחקירה פלילית באינטרנט. מבחינה מעשית,¹⁴⁴ אכן הבוחן לקביעת המקום המיוחס לחקירה הפלילית באינטרנט היא מיקומה של הראיה הדיגיטלית הנאספת, בעת איסופה. במילים אחרות, לא מקום ביצוע פעולת האיסוף קובע לעניין השאלה אם מדובר בפעולת איסוף אקסטרה-טריטוריאלית במסגרת חקירה פלילית באינטרנט אלא מקום הימצא הראיה הנאספת.

במבחן מקום ביצוע הפעולה ובמבחן מקום הימצא הראיה יש כדי להוביל לתוצאות שונות בנוגע לשאלת האקסטרה-טריטוריאליות של פעולת האיסוף. נניח שחוקרת משטרה ישראלית מבקשת להעתיק חומר מחשב המצוי בחו"ל או לשתול רכיב האזנה למחשב המצוי בחו"ל באמצעות התחברות מרחוק דרך האינטרנט. בשתי דוגמאות אלה החוקרת נמצאת בישראל ומבקשת לבצע את הפעולות הללו באמצעות הפעלת מחשבה מישראל.¹⁴⁵ על פי מבחן מקום הימצא הראיה המבוקשת, החוקרת הישראלית מבצעת פעולת איסוף אקסטרה-טריטוריאלית. על פי מבחן מקום ביצוע הפעולה, נראה שהפעולה מתבצעת ממדינת ישראל ואינה נחשבת אקסטרה-טריטוריאלית.

נניח דוגמה נוספת, שבה חוקרת המשטרה משתילה באופן סמוי את רכיב ההאזנה במחשבו של החשוד בעת שזה נמצא בישראל, וכעבור זמן החשוד נוסע לחו"ל עם מחשבו, ורכיב ההאזנה משדר ממנו אל החוקרת באמצעות האינטרנט. סיטואציה זו יכולה להתרחש בין בכוונה תחילה של החוקרת ובין שלא במתכוון. על פי מבחן מקום הימצא הראיה, פעולת ההאזנה נחשבת טריטוריאלית כל עוד המחשב נמצא בישראל, ואולם כאשר הוא יוצא לחו"ל, הפעולה הופכת לאקסטרה-טריטוריאלית ואסורה על פי דיני סמכות האכיפה הבין-לאומית. על פי מבחן מקום ביצוע הפעולה, גם השלב שבו המחשב מצוי בחו"ל עשוי להיחשב לשלב שאינו מעורר מגבלה אקסטרה-טריטוריאלית, והדבר תלוי באופן שבו נתפשים גבולות הפעולה: האם בשלב השתלת רכיב ההאזנה בלבד, או שמא בכל שלב שבו מתבצעת ההאזנה בפועל? ראינו אפוא כי מבחן מקום הימצא הראיה הוא דווקני מבחן מקום ביצוע פעולת האיסוף. על פי הביקורת הארכיטקטונית-הטכנולוגית על התפישה הטריטוריאלית בדיני איסוף הראיות במרחב הסייבר, ניתן לבסס טענות כדלקמן: ראשית, מרחב הסייבר עשוי ליצור הפרדה בין מקום

142 ראו למשל In re CSIS, [2010] 1 F.C.R. 460 (Ca.).

143 לעומת זאת לעניין ההגנה החוקתית שתחול על יעדי ההאזנה במקרה של האזנה אקסטרה-טריטוריאלית, ייתכן שתהיה חשיבות גם לעצם מיקומם של המשוחחים, תלוי במודל התחולה החוקתית של המדינה החוקרת. נושא זה יידון בהרחבה להלן בפרק ה.ג.

144 ראו לעיל בפרק ג.ד.1.

145 אציין שוב כי אילו הייתה החוקרת מבקשת להשתיל פיזית את רכיב ההאזנה במחשב המצוי בחו"ל, או לחדור אל המחשב עצמו במקום הימצאו, הרי שפעולתה הייתה מפרה את כללי סמכות האכיפה הבין-לאומית, ולמעשה לא היה בפעולתה כל הבדל לענייננו, לעומת פעולת איסוף אחרת במרחב הפיזי.

ביצוע הפעולה לבין מקום הימצא הראיה; שנית, מבחן מקום הימצא הראיה אינו חד דיו לקביעת אינטרס ריבוני של המדינה הזרה שבה אגורה הראיה המבוקשת; שלישית, כאשר הפעולה מתבצעת בידי שוטר במדינה החוקרת, מתקחה מאוד הטיעון בדבר פגיעה בריבונותה של המדינה הזרה.

ארחיב מעט על החלק השני של הטענה, מנקודת מבט של ארכיטקטורת המרחב הקיברנטי: מקום הימצאה של הראיה הדיגיטלית אינו תמיד ידוע מראש, שכן המרחב הקיברנטי אינו באמת "מקום" פיזי,¹⁴⁶ ולעומתו מקום ביצוע פעולת האיסוף הוא עניין ברור וידוע. כך למשל ייתכן שבידי רשויות החקירה תהיה בשלב ראשון כתובת IP שמייצגת אך ורק את שרת ה-proxy שדרכו בוצעה הפעילות הפלילית, והתחקות אחר החשוד לפי כתובתו של ה-proxy server שממנו פעל תוביל למסקנה כי הפעולה הייתה במדינה X בעוד בפועל הוא פעל ממדינה Y ורק התקשר דרך מדינה X. הידיעה בדבר המדינות שבהן "עבר" החשוד תוכל להיות בדיעבד בלבד. כמו כן חלק מפעולות האיסוף מתייחסות למידע העובר בתקשורת בין-מחשבים (לדוגמה בהאזנת סתר לתקשורת אינטרנטית), שאז עניין המיקום של המידע הוא מעצם טבעו נזיל ומשתנה. יתרה מזאת, חלק מהראיות הדיגיטליות חשובות וכבדות משקל דווקא כאשר הן מצויות בתקשורת בין מחשבים. כך הוא למשל כאשר מבקשים לאסוף ראיות על הפעלת נגיפי מחשב. עדיף לחוקרים לאתר את הפעלת נגיף המחשב בפועל מלאתר את עצם ההחזקה בנגיף, אשר אינה עברה כשלעצמה.¹⁴⁷ כשמקום הימצא הראיה הדיגיטלית אינו תמיד ידוע, הרי שהתבססות על נתון זה כאמת המידה לבחינת סמכות האכיפה הביין-לאומית – אינה ישימה.¹⁴⁸

אסכם עד כאן. לפי התפישה הטריטוריאלית בחקירה הפלילית במרחב הסייבר, מקום הימצא הראיה הדיגיטלית הוא המקום הקובע באשר לשאלת סמכות האכיפה הביין-לאומית. לעומת מבחן זה ניתן להציע את מבחן מקום ביצוע פעולת האיסוף. מרחב הסייבר מאפשר ביצוע פעולות איסוף ראיות מרחוק, תוך התחברות ממחשב אחד למחשב אחר, ככל ששניהם מחוברים לרשת. הפעולה מתבצעת בנוגע לראיה דיגיטלית שאמנם מצויה במחשב בחו"ל, אבל מתוך מחשב המצוי בטריטוריה של המדינה החוקרת. הראיה נאספת ונאגרת במחשב המצוי בטריטוריה של המדינה החוקרת. החוקר מושך את המידע אליו, והמחשב שבו אגור המידע המבוקש אינו "דוחף" אותו.¹⁴⁹

146 ראו הדיון בפרק ג.ד.2..

147 ראו סעיף 6 לחוק המחשבים, התשנ"ה-1995.

148 מטעם זה ביקש משרד המשפטים האמריקני לתקן את ה-FED. Federal Rules of Criminal Procedure (R. CRIM. P. 41) ולקבוע בו במפורש כי יותר להסמין את הרשות החוקרת לבצע פעולות של חדירה מרחוק לחומרי מחשב אשר מיקומם אינו ידוע, ואשר ייתכן כי בפועל הם אגורים בשרהים מחוץ לטריטוריה האמריקנית. זאת כל עוד הרשויות אכן אינן מסוגלות לאתר את מיקומו של חומר המחשב הדרוש לחקירה, בשל שימוש באמצעים להסוואת זהות המשתמש במחשב או להסוואת מיקומו של חומר המחשב. ראו Advisory Committee on Criminal Rules, Proposed Amendment to Rule 41 (2014), available at <http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014>, p. 165

149 על תקשורת push לעומת תקשורת pull ראו למשל Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. על תקשורת pull לעיל ה"ש 79, בעמ' 53-54. Benoliel; 1130, 1148 (2000).

יש לזכור כי בכל הנוגע לסמכות התחיקה והשיפוט של המדינה באשר למרחב הקיברנטי הונהג הכלל שלפיו המחשב שאליו מגיע התוכן המקים את העברה הפלילית מקים סמכות למדינה שבה מצוי המחשב, במובן זה שהמעשה נתפש כעברת פנים.¹⁵⁰ היקש מסמכות התחיקה והשיפוט אל סמכות האכיפה מוביל למסקנה כי פעולת האיסוף צריכה להיחשב כמתבצעת במחשבו של החוקר ולא דווקא במחשב היעד, שלגביו מתבצעת פעולת האיסוף.

3. ביקורת במישור תאוריות של ריבונות

שופט בית המשפט העליון האמריקני ג'וזף סטורי (Story) כתב בשנת 1834:

“[E]very nation possesses an exclusive sovereignty and jurisdiction within its own territory. The direct consequence of this rule is, that the laws of every state affect, and bind directly all property, whether real and personal, within its territory; and all persons, who are resident within it, whether natural born subjects, or aliens; and also all contracts made, and acts done within it... Another maxim, or proposition, is, that no state or nation can, by its laws, directly affect, or bind property out of its own territory, or bind persons not resident therein, whether they are natural born subjects, or others”.¹⁵¹

הריבונות מתאפיינת בטריטוריה, וטריטוריה מאפיינת את גבולות סמכותה המשפטית של המדינה, וכללי הסמכות המשפטית הם ביטוי של הריבונות. תפישת היסוד בדבר תפקידה של המדינה המודרנית גורסת כי על המדינה לשמש אמצעי הגנה על שלומו ורווחתו של הציבור החוסה תחת כנפיה, קרי בשטחה. בשם תפישה זו נמסרת לריבון מרות על הנעשה בשטחו הגאוגרפי. מבחינה היסטורית וכן מבחינה רעיונית, ניתן לזהות תפישה שורשית עמוקה של הצמדה בין ריבונות, סמכות וטריטוריה. תפישה זו היא נחלת המשפט הישראלי,¹⁵² כמו גם

150 ראו הסקירה לעיל בפרק ג.ג.1..

151 JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS, FOREIGN AND DOMESTIC, IN REGARD TO CONTRACTS, RIGHTS, AND REMEDIES, AND ESPECIALLY IN REGARD TO MARRIAGES, DIVORCES, WILLS, SUCCESSIONS, AND JUDGMENTS 19–22 (Reprinted ed., 1972). המהדורה הראשונה של ספר זה יצאה בשנת 1834. המיזוג בין ריבונות לסמכות ולטריטוריה פועל כלפי פנים (עליונות השלטון כלפי התושבים המצויים בטריטוריה) וכלפי חוץ (עצמאות מפני התערבות חיצונית בפעולת השלטון ביחס לטריטוריה שלו). על כפל מובנים זה, ראו גם H.L.A. HART, THE CONCEPT OF LAW 24–25 (2nd ed., 1994).

152 פרופ' פלר כתב בספרו יסודות דיני עונשין:

“התחולה הטריטוריאלית של הנורמה הפלילית היא גם ביטוי אלמנטרי של ריבונות המדינה; המדינה היא הכח המאורגן היחיד של החברה המתקיימת בתחום גבולותיה, המוסמך לקבוע את קו הגבול בין המותר לאסור מבחינה פלילית, לדרוש מכל אלה המצויים בתחום ריבונותה לכבד את דפוסי ההתנהגות הקובעים בה, ולטפל בכל אלה שהפרו דרישה זו... תחולתה הטריטוריאלית הבלתי מסוייגת של הנורמה הפלילית של המדינה היא היבט של ריבונותה כלפי פנים וכלפי חוץ כאחד” (פלר, לעיל ה”ש 13, בעמ’ 239).

נחלת המשפט האמריקני¹⁵³ ונחלתו של המשפט הביין-לאומי.¹⁵⁴ לעתים נדמה כי התפישה כה יסודית, עד שהחוק אינו צריך לנקוב במפורש כי המשפט חופף את הטריטוריה של המדינה, וכי זו הנחת היסוד. רק חריגה מהנחה זו צריכה להיאמר במפורש.¹⁵⁵ מכאן נובע שכאשר מדינה מבקשת להרחיב את סמכותה אל מחוץ לטריטוריה שלה, וכאשר ההרחבה נעשית אל עבר שטחה של מדינה אחרת ולא לעבר אזורים שאינם בבעלות מדינות אחרות, כגון הים הפתוח, הרי שנוצר משחק "סכום אפס", שלפיו הרחבת הסמכות של מדינה אחת אל מעבר לגבולות הטריטוריה שלה משמעה הצרת הסמכות של מדינה אחרת. זאת, אלא אם המדינות מחליטות לשתף פעולה ולהפוך את החריגות האקסטר-טריטוריאליות למוסכמות.¹⁵⁶

המונח "ריבונות" שנוי במחלוקת הן במסגרת המשפט הביין-לאומי והן בתחום מדע המדינה והיחסים הביין-לאומיים.¹⁵⁷ בשל עמימותו של מושג ה"ריבונות" היו שטענו כי אין הוא יכול להיות מונח משפטי, ויש למחקו ממגילת האו"ם, המחייבת שוויון ריבוני בין המדינות החברות בו.¹⁵⁸ עוד במסגרת עמדה זו, הטענה היא שהמונח "ריבונות" הוא מתחום היחסים הביין-לאומיים, וכי המונח הרלוונטי יותר לזירה המשפטית הביין-לאומית הוא "עצמאות", במובנו כאי-התערבות בענייניה הפנימיים של המדינה.¹⁵⁹ הרולד לאסקי (Laski) אף טען כי גם במסגרת השיח הפוליטי, לאו דווקא המשפטי, יש לזנוח את השימוש במונח "ריבונות" ולהתבונן על הזירה הביין-לאומית ועל היחסים בין המדינות במונחים של כוח / סמכות (Power).¹⁶⁰ בכל זאת המצב הנוהג הוא כי לריבונות יש נפקות משפטית. המדינות מחויבות בהתחשבות בריבונותן של מדינות אחרות. כיבוד הריבונות של מדינות זרות נתפש כמעין עקרון וטו, המאין פעולות

ראו גם ש"ז פלר ומרדכי קרמניצר "הצעת חלק מקדמי וחלק כללי לחוק עונשין חדש ודברי הסבר תמציתיים" משפטים יד 127, 201 (1984). אמירתו זו של פלר אומצה בפסיקת בית המשפט העליון. ראו ע"פ 4391/03 אבו ריא נ' מדינת ישראל, בפס' 11 (פורסם בנבו, 13.12.2005). ראו עוד, בהקשר של סמכות התחיקה הכללית של המדינה, לאו דווקא זו הפלילית: אהרן ברק פרשנות במשפט, כרך ב, פרשנות חקיקה 578 (1993).

153 ראו RESTATEMENT, לעיל ה"ש 1, § 206 cmt. B.

154 ראו למשל, SHAW, לעיל ה"ש 6, בעמ' 487-488. שואו כינה תפישה זו: האקסיומה הבסיסית של המשפט הביין-לאומי הקלאסי.

155 ראו בנימין רובין "תחום תחולת המשפט, שטח המדינה ומה שביניהם" משפטים כה 215, 216-219 (1995).

156 כך הוא למשל במקרה של הכרה בחסינות דיפלומטית לנציגים מוסמכים של מדינות זרות. נציגים אלה כפופים למשפט של מדינתם ולא לזה של מדינת שירותם.

157 ראו Winston P. Nagan & Craig Hammer, *The Changing Character of Sovereignty in International Law and International Relations*, 43 COLUM. J. TRANS. L. 141 (2004); LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE 66 (Arnold D. McNair ed., 4th ed. 1928).

158 ראו Charter of the United Nations (San Francisco, 1945), § 2(1). לעמדה המצדדת במחיקת הריבונות כמונח משפטי, ראו למשל יהושע ברקאי המשפט הבינלאומי 72-75 (1957) והמקורות המובאים שם. מנגד, לעמדה המצדדת בתפישת הריבונות כמונח משפטי, ראו למשל את WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, Vol. I, 46 (facsimile of the 1st ed. 1979); Alan James, *The Practice of Sovereign Statehood in Contemporary International Society*, 47 POLITICAL STUDIES 457 (1999).

159 ראו סיבל, לעיל ה"ש 12, בעמ' 80.

160 ראו HAROLD J. LASKI, A GRAMMAR OF POLITICS 44-45 (4th ed., 1938).

מדינתיות בעלות השלכה אקסטרטריטוריאליה. על כן יש מקום לעמוד על משמעותו של המונח.

סטפן קרייזנר (Krasner) עמד על ארבע קטגוריות של שימוש במונח "ריבונות":¹⁶¹ האחת, ריבונות פנימית (Domestic sovereignty), היינו סמכותו הסופית והעליונה של השלטון על הקבוצה הנתונה למרותו; השנייה, ריבונות בין-מדינתית (Interdependence sovereignty), היינו שליטה על התנועה אל המדינה ומחוצה לה; השלישית, ריבונות בין-לאומית (International legal sovereignty), היינו מעמדה של המדינה ביחס למדינות אחרות וההכרה בה בזירה הבין-לאומית; הרביעית, ריבונות וסטפליית (Westphalian sovereignty), או כפי שחוקרים אחרים כינו זאת: ריבונות במובן ראליסטי,¹⁶² היינו יצירת מוסד לארגון קבוצה פוליטית המתבסס על שני עיקרים: טריטוריאליה ומניעת התערבות חיצונית במנגנונים הפנימיים של המוסד הריבוני. כפי שניתן לראות, הטריטוריאליה מאפיין פן אחד של הריבונות במובן מוסדי, אך לא במובנים מהותיים של סמכות, שליטה והכרה הדדית. מעניין כי הקטגוריה הראשונה, של ריבונות במובן פנימי, אינה נזקקת לכאורה למדינה, ואילו שלוש הקטגוריות האחרות מדברות על המדינה עצמה.¹⁶³ במילים אחרות, קיימת זיקה ברורה בין ריבונות לבין המדינה, אך אין מדובר בחפיפה מלאה. המדינה כמוסד וכ"שחקן" בזירה הבין-לאומית מחייבת התייחסות במונחים טריטוריאליים, ואילו הריבונות, כמובנה הפנימי (שהוא גם המובן העתיק ביותר של המונח), אינה מדברת במדינה אלא ביחסים בין השלטון לבין נתיניו.

ברי כי הריבונות אין משמעה כוח מוחלט ובלתי ניתן לפיקוח של המדינות לנהוג בענייניהן הפנימיים והחיצוניים לפי ראות עיניהן וללא הגבלות. המשפט הבין-לאומי מטיל מגבלות על המדינות. מדינות הסוטות ממרותו של המשפט הבין-לאומי מנצלות לרעה את ריבונותן (Abuse of sovereignty).¹⁶⁴ הכללים המנהגיים ה"טבעיים" אינם דיספוזיטיביים, והם מחייבים את המדינות. יתרה מזאת, המשפט הבין-לאומי ההסכמי מחייב את המדינות החתומות על ההסכמים, לפחות כל עוד לא ביטלו את התחייבותן זו. אעיר כי עד כה הריבונות נתפשת, על פי גישה זו, כסכום הכוחות הנותרים למדינה לאחר הסדרתו של המשפט הבין-לאומי.¹⁶⁵

- 161 ראו STEPHEN D. KRASNER, SOVEREIGNTY – ORGANIZED HYPOCRISY 9–25 (1999).
- 162 ראו למשל: Anne-Marie Slaughter, *Interdisciplinary Approaches to International Economic Law: Liberal International Relations Theory and International Economic Law*, 10 AM. U. J. INT'L L. & POL'Y 717, 723–724 (1995); Anne-Marie Slaughter, *International Law in a World of Liberal States*, 6 EUR. J. INT'L L. 503, 507 (1995); David G. Post, *The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521, 523–524 (1997).
- 163 להרחבה על ההפרדה בין תפישת הריבונות לבין המדינה ראו JOHN HOFFMAN, SOVEREIGNTY 11–20 (1998).
- 164 ראו Nagan & Hammer, לעיל ה"ש 157, בעמ' 176–182; FRANCIS H. HINSLEY, SOVEREIGNTY 208–213 (2nd ed., 1986).
- 165 ראו *The Lotus Case*, לעיל ה"ש 10, בעמ' 18. כן ראו את עמדת השופט אנצ'לוטי בעניין: Customs Regime Between Germany and Austria, Advisory Opinion, 1931 PCIJ Series A/B No. 20, ICGJ Hans Kelsen, *The Principle of Sovereign Equality of States as a Basis of International Organization*, 53 YALE L. J. 207 (1944).

מונח ה"ריבונות" גמיש לאורך ציר הזמן. תפישת הריבונות עברה ועוברת שינויים לאורך ההיסטוריה.¹⁶⁶ קרייזנר הראה כיצד תפישת הריבונות השתנתה בתגובה להתפתחויות חברתיות ומדיניות.¹⁶⁷ אמנם, לדידו של קרייזנר, בליבת ההגדרה של ריבונות עדיין נותר העיקרון של הפעלת סמכות בטריטוריה נתונה,¹⁶⁸ אולם בשל הגמישות המושגית של הריבונות נראה שאין לראות במונח ה"ריבונות" משום חסם טבעי מפני ניתוח התפישה הטריטוריאלית הנוהגת באשר למרחב הסייבר. יצוין כי בעידן הגלובליזציה הכלכלית והתקשורתית, עוד טרום עידן האינטרנט, ובוודאי לאחר התפשטות האינטרנט בשימוש כלל-עולמי, רבו הקולות המדברים על פוסט-לאומיות (Post nationalism), על היחלשותה של המדינה ובעיקר על היחלשות מושג ה"ריבונות" של המדינות. הטענה המושמעת היא שבעידן של גלובליזציה מושגי הגבולות הפיזיים מיטשטשים, מדינות וגופים לא-מדינתיים משפיעים באופן ניכר על מדינות ופרטים בטריטוריות אחרות, הן ברמת המקור המדינתית והן ברמת המיקרו של הפרט במדינה הזרה, ובכך יש משום התערבות בענייני הפרטים הנתונים למרותן של מדינות זרות.¹⁶⁹ כנגד טענה זו נשמעו שני טיעוני תשובה, האחד של הנרי פריט (Peritt) והשני של ג'ואל טרכטמן (Trachtman). פריט טען כי הגם שיש בהתפתחויות הטכנולוגיות והתקשורתיות כדי לאיים על סוג מסוים של תפישת ריבונות לא-ליברלית, הרי שבכל הנוגע למשטרים ליברליים, המכירים בביזור הכוח בין השלטון לבין האזרחים, תפישת הריבונות ממילא שונה, והיא מפויסת יותר ביחס שבין הממשל לבין האזרחים. בשונה מהעמדה הראליסטית, אין התפישה הליברלית של ריבונות מבוססת על טריטוריאליות ועל ייחוד הסמכות בטריטוריה נתונה.¹⁷⁰ על פי תפישה זו, המדינה ומושג ה"ריבונות" נועדו לשרת אינטרסים משותפים של קבוצות פרטים.¹⁷¹ גם האינטרנט מקדם ערכים ואינטרסים של הפרט, ועל כן הוא אמצעי להגשמת ערכים ליברליים. הריבונות היא מכשירנית ולא מוחלטת, וכך גם האינטרנט הוא מכשירני, כשהערך שאותו שניהם – הריבונות והאינטרנט – נועדו לשרת הוא קידום תועלתו של הפרט. משכך, האינטרנט אינו סותר, ואינו יכול לסתור, את הריבונות. האינטרנט אף יכול לקדם ריבונות במובנה הליברלי.¹⁷² תפישת הריבונות שמציע

- 166 לבחינה היסטורית של התפתחות התפישה של המונח "ריבונות", מימי האימפריה הרומית ועד ימינו שלנו ראו למשל את הסקירה אצל: HINSLEY, לעיל ה"ש 164; CHARLES E. MERRIAM, HISTORY OF THE THEORY OF SOVEREIGNTY SINCE ROUSSEAU (1999).
- 167 ראו KRASNER, לעיל ה"ש 161.
- 168 ראו Stephen D. Krasner, *Sovereignty: An Institutional Perspective*, 21 COMP. POL. STUD. 66, 86 (1988).
- 169 ראו למשל את הסקירה בכרך כתב עת שהוקדש לנושא: Symposium, *The Decline of the Nation State and its Effects on Constitutional and International Economic Law*, 18 CARDOZO L. REV. 903 (1996); JEAN-MARIE GUEHENNO, THE END OF THE NATION-STATE (Victoria Elliott trans., 1995); John O. McGinnis, *The Decline of the Western*; 1376–1370 בעמ' 55, Johnson & Post *Nation State and the Rise of the Regime of International Federalism*, 18 CARDOZO L. REV. 903 (1996).
- 170 ראו Henry H. Peritt, *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 423 (1997).
- 171 ראו Anne-Marie Burley, ; 729–728 בעמ' 162, Slaughter, *Interdisciplinary Approaches Law Among the Liberal States: Liberal Internationalism and the Act of State Doctrine*, 92 COLUM. L. REV. 1907 (1992).
- 172 ראו Peritt, לעיל ה"ש 170, בעמ' 441–437.

פְּרִיט היא תלוית עמדה פוליטית-משטרית, ובמילים אחרות היא מתחום מדע המדינה יותר משהיא מתחומי המשפט. טרכטמן טען כי הקישור בין ההתקדמות הטכנולוגית להיחלשות מושג ה"ריבונות" נובע מתפישה שגויה של הריבונות כעניין מוחלט וקונגטי, בעוד שבפועל מעולם לא הייתה הריבונות אלא מושג גמיש שעובר שינויים תלויי-זמן, מקום והסכמה בין מדינות.¹⁷³ אם כך, אין לדבר על היחלשות מושג ה"ריבונות" בעקבות התפתחות המרחב המקוון אלא על היתכנות להגמשה נוספת של המושג.

הצגה מוכרת ומרכזית במשפט הבין-לאומי של מושג ה"ריבונות" מופיעה בבוררות בעניין האי Palmas משנת 1928.¹⁷⁴ באותו מקרה הוצע כי מושג ה"ריבונות" אינו צריך להיתפש רק כסמכות של המדינה כלפי פנים ואף לא כעצמאותה כלפי חוץ, אלא גם כחובתה כלפי חוץ.¹⁷⁵ בעניין האי פלמאס קבע הבורר הובר (Huber) כי אם לפעולה המתרחשת מתוך מדינה א יש השפעה ממשית על אוכלוסיית מדינה ב, ומדינה א אינה מונעת את המשכו של המצב האסור, הרי שמדינה א אינה מתפקדת כריבונית, ויש הצדקה להתערבות מדינה ב בנעשה בשטחה של מדינה א. ההצדקה של מדינה ב לפעול היא מילוי חובתה להגן על אנשיה (Responsibility to protect).¹⁷⁶ נראה כי הפרשנות הזאת למונח ריבונות מאפשרת לבחון מצבים שבהם המדינה תפעל באופן אקסטרטריטוריאלי לשם שמירה על ענייניה הפנימיים.

בהיקש מהאי פלמאס למרחב הסייבר: אם שרת מחשב מצוי פיזית במדינה א, אולם מתבצעת ממנו עברה בשטחה של מדינה ב, ומדינה א אינה חוקרת את העבירה בעצמה, בין מיזמתה ובין על פי פנייה ממדינה ב, הרי שיכולה לקום הצדקה למדינה ב לפתוח בחקירה עצמאית ולבצע את פעולות האיסוף מאותו שרת במדינה א, משני מקורות – פנימי וחיצוני. המקור הפנימי הוא אחריותה של מדינה ב להגן על אנשיה הנפגעים מפעילות פלילית במרחב הסייבר. המקור החיצוני הוא אי-עמידתה של מדינה א בחובתה במישור הבין-לאומי כלפי חוץ, קרי חובתה למנוע המשכו של מצב המשפיע על תושבי מדינה ב.

בסיכומו של עניין, התפישה הטריטוריאלית באשר לחקירה הפלילית במרחב הסייבר מניחה בפועל פער מושגי בין המונחים של "ריבונות", "סמכות" ו"טריטוריה". עם זאת, כפי שהראיתי לעיל, ניתן למצוא לפחות בחלק מהמונחים הגרעיניים של מושג ה"ריבונות" הפרדה רעיונית מהמונח "טריטוריה". יתרה מזאת, מושג ה"ריבונות" גמיש ובעל פוטנציאל להשתנות ולהתאים עצמו למציאות המשתנה. ועוד, כפי שהראיתי לעיל, גם בכל הנוגע למונחים שונים של מושג ה"סמכות", אין היצמדות לטריטוריה. על כן אין לקבל באופן דטרמיניסטי את הזיקה בין

173 ראו Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561, 563–565, 567 (1997).

174 ראו The Island of Palmas Case (Netherlands v. United States), 2 U.N. REP. INT'L ARB. AWARDS 829 (1928).

175 ראו לעיל, בעמ' 839. ראו גם SHAW, לעיל ה"ש 6, בעמ' 490.

176 עור על החובה של המדינה להגן על תושביה (Responsibility to protect) בעידן הגלובליזציה, ראו Tobias Stroll, *Responsibility, Sovereignty and Cooperation – Reflections on the "Responsibility to Protect"*, in INTERNATIONAL LAW TODAY: NEW CHALLENGES AND THE NEED TO REFORM I (Doris König ed., 2007); Markus Benzing, *Sovereignty and the Responsibility to Protect in International Criminal Law*, in INTERNATIONAL LAW TODAY: NEW CHALLENGES AND THE NEED TO REFORM 17 (Doris König ed., 2007).

שלושת המונחים הללו: ריבונות, סמכות וטריטוריה. פרימת הקשר בין שלושת המונחים הכרחית לצורך פיתוח ביקורת על התפישה הטריטוריאלית באשר לאיסוף ראיות במרחב הסייבר. ניתן להציע בסיס רעיוני למודל חקירתי בעל השלכות אקסטרה-טריטוריאליות דווקא מתוך ערכים יסודיים של ריבונות המדינה, ולא, כפי שניתן לשגות ממבט ראשון, מתוך הנחה בדבר היחלשות ריבונותה של המדינה.

ז. סיכום

התפישה הטריטוריאלית של דיני איסוף הראיות במרחב הסייבר מביאה להתנגשות בלתי נמנעת בין עקרונות מהמשפט הבין-לאומי לבין עקרונות מהמשפט הפלילי. המשפט הבין-לאומי הוא משפט של מדינות. מדינות הן יחידות הניתוח. גם כשעסקינן במשפט בין-לאומי פלילי, ההתייחסות היא להסכמות בין מדינות על כללי השיפוט של נאשם בביצוע עברות פליליות. כיוון שמשפט האינטרנט והמשפט הפלילי הם דיסציפלינות משפט המתייחסות לאנשים ולהסדרת היחסים בינם לבין המדינה, נוצר כאן עירוב תחומין: משפט של מדינות מקרין על משפט של אנשים.

דיני החקירה הפלילית מאזנים, על פי רוב, בין האינטרסים של רשויות אכיפת החוק לבין זכויות חשודים וצדדים שלישיים רלוונטיים. שיקול כיבוד ריבונותן של מדינות זרות אינו שיקול שמוכנס למשוואה באופן תדיר, הגם שהוא קיים במסגרת החקירה הפלילית במרחב הפיזי. עם זאת בזירה הקיברנטית הופכת כל עברה, ובעקבותיה כל חקירה, לבעלת פוטנציאל מידי להפוך לחקירה בין-מדינתית. כתוצאה מכך, שיקול שאינו בליבת דיני איסוף הראיות הופך לשיקול המושל בכיפה, בשל אופיו כשיקול המשול ל"כרטיס אדום" העוצר כיווני חקירה מסוימים במרחב הסייבר מלהתקיים.

בנוסף, כפי שהראיתי, ההגבלה הטריטוריאלית של סמכות האכיפה באשר לאיסוף ראיות בחקירה פלילית במרחב הסייבר – בעייתית מבחינה מעשית ואינה מוצדקת בהתחשב בארכיטקטורת המרחב ובמהותן של הראיות הדיגיטליות, וכן אינה מתאימה מבחינה אפיסטמולוגית. יש מקום אפוא לשינוי אמות המידה בנוגע לסמכות האכיפה במרחב הסייבר. ככל שתוכרנה סמכויות איסוף בעלות מובן אקסטרה-טריטוריאלי (על פי התפישה הטריטוריאלית דהיום באשר למרחב הסייבר), תתעורר שאלת הפרישה החוקתית במלוא עוזה ובתדירות תכופה מזו שבה היא מתעוררת כיום בדיני איסוף הראיות. על כך אפרט בפרק 5(ג) להלן, אך עוד קודם לכן אציג את התפישה הנוספת, החולשת על דיני איסוף הראיות הדיגיטליות במרחב הסייבר, שאותה אכנה "התפישה הפיזית".