

# חקירה פלילית באינטרנט במגבלות הטריטוריה

חיים ויסמונסקי\*

מבוא

- א. התפישה הטריטוריאלית בנוגע לסמכות המדינה לאסוף ראיות במרחב הפיזי
- ב. איתור התפישה הטריטוריאלית בנוגע לאינטרנט
  1. סמכות תחקית ושיפוטית באינטרנט
  2. סמכות אכיפה
  3. הביטוי היישומי של התפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט
- ג. פריצת מעשיות של התפישה הטריטוריאלית בנוגע לדיני איסוף באינטרנט
  1. הסכמה בין-לאומית על חדירות אקסטרה טריטוריאליות לחומרים באינטרנט
  2. דין מדינתי המתיר חדירה אקסטרה טריטוריאלית במצבים מסוימים באינטרנט
  3. התפישה הטריטוריאלית ותזכיר הצעת חוק החיפוש
- ד. פריצת גבולות התפישה הטריטוריאלית בנוגע לאינטרנט – דיון נורמטיבי
  1. התפישה הטריטוריאלית ופגיעתה בחקירה הפלילית באינטרנט
  2. ביקורות על התפישה הטריטוריאלית ויישומה על דיני האיסוף במסגרת חקירה פלילית באינטרנט
- ה. סיכום ואחרית דבר

מבוא

האכיפה הפלילית באינטרנט לוקה בחסר. בעקבות זאת היו שהכריזו על כישלון

---

\* תלמיד מחקר לתואר שלישי במשפטים במרכז צבי מיתר באוניברסיטת תל-אביב בהנחייתו של פרופ' מיכאל בירנהק. הח"מ משמש כממונה על נושאי משפט וטכנולוגיה בפרקליטות המדינה, אולם הכתוב במאמר מבטא את עמדתו האישית בלבד. תודה לפרופ' מיכאל בירנהק, לד"ר אסף הרדוף ולעו"ד אביטל בגין על הערותיהם המחכימות והמועילות.

האכיפה הפלילית המקובלת באינטרנט.<sup>1</sup> אכיפה פלילית מקובלת, משמעה חקירה פלילית הנערכת על ידי המדינה ותוצאתה איסוף ראיות דיגיטליות בסמכות ובמימונות. עקב הכרזת הכישלון האמורה, היו שקראו לשינוי פרדיגמת האכיפה מחקירה פלילית לניסיונות מניעה מראש,<sup>2</sup> או שינויה מחקירה פלילית לתקיפת אתרים.<sup>3</sup> היו שחזו שבאינטרנט תוחצן האחריות לאכיפה מהמדינה לספקיות השירות הגדולות באינטרנט;<sup>4</sup> היו שטענו שרק אכיפה בין-מדינתית תצלח<sup>5</sup> והיו שטענו שהזירה האינטרנטית תופקר, כך שמשותמי האינטרנט יצטרכו לנקוט אמצעים של הגנה עצמית.<sup>6</sup>

במאמר זה אבקש לטעון שאין להכריז על כישלון האכיפה הפלילית המדינתית באינטרנט. במקום זאת, אני מציע לחשוף הנחת יסוד בסיסית החולשת על דיני החקירה הן במרחב הפיזי והן במרחב האינטרנטי. הנחת יסוד זאת, הסמויה מן העין במידה רבה, מורכבת מההיגדים הבאים: **הראשון**, משפט המדינה מוגבל לטריטוריה שלה. זו הנחת המוצא של כל שיטות המשפט המוכרות כמעט, בוודאי של שיטת המשפט הישראלית. **השני**, האינטרנט אינו חוץ-טריטוריאלי, והגבולות המדיניים מורכבים על האינטרנט על ידי המשפט. אף זו הנחת מוצא של כל שיטות המשפט המוכרות כמעט, לרבות של שיטת המשפט הישראלית. **השלישי**, חיבור שתי הנחות

- 
- <sup>1</sup> ראו למשל: Nimrod Kozlovski, A Paradigm Shift in Online Policing – Designing Accountable Policing 108 (paper as a part of a research towards J.S.D. dissertation, Yale Law School, 2005); Susan Brenner, *Distributed security: Moving away from reactive law enforcement*, 9 INT'L J. COMM. L. & POL'Y 11, 40–49 (2004)
- <sup>2</sup> ראו: Kozlovski, לעיל ה"ש 1, בפרק 2; ראו סקירה אצל אסף הרדוף **הפשע המקוון** 167–178 (2010).
- <sup>3</sup> ראו למשל: Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. TECH. J. 213, 228–229 (2004).
- <sup>4</sup> ראו למשל: Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 49–85 (2006); Jonathan L. Zittrain, *Internet Points of Control*, 44 B.C. L. R. 653 (2003).
- <sup>5</sup> ראו למשל: Henry H. Perritt, *Jurisdiction in Cyberspace: The Role of Intermediaries*, in **רואו למשל**: BORDERS IN CYBERSPACE 164 (Brian Kahin & Charles Nesson eds., 1998). פריט הציע מודל אכיפה בין-מדינתית באינטרנט, שלפיו המדינות תתפקדנה כאוכפות בתיווך או בתיאום של גורם בין-לאומי. כן ראו: Sean Selin, *Governing Cyberspace: The Need for an International Solution*, 32 GONZ. L. REV. 365 (1997); Ellen S. Podgor, *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. DAVIS L. REV. 267 (2002).
- <sup>6</sup> ראו למשל: Susan Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 2, 15–80 (2003).

מוצא אלו מביא למסקנה כי משפט המדינה, ולענייננו – דיני החקירה, מוגבל לחלק הטריטוריאלי שבו המדינה אוזרת באינטרנט. פעולת אכיפה מחוץ לטריטוריה אינטרנטית זו אינה בסמכותה של המדינה. כפי שאטען להלן, כאשר החקירה מתנהלת במרחב האינטרנטי, הופכת הנחת היסוד הזו לחסם מרכזי בחקירת עברות פליליות באינטרנט.

אכנה בקיצור את הנחת היסוד האמורה – "התפישה הטריטוריאלית". תפישה טריטוריאלית בדיני החקירה הייתה תמיד חסם בפני פעולתה של המדינה. החסם הוא בדמות האיסור לפגוע בריבונותן של מדינות זרות במסגרת פעולתה של המדינה לאכיפת משפטה הפנימי. עם זאת, בכל הנוגע לפשיעה במרחב הפיזי, חסם זה לא הפך את כלי החקירה של המדינה לכלי ריק, כפי שמאיים החסם לעשות בנוגע לחקירות פליליות באינטרנט.

במאמרי אבקש לעמוד על טיבה של התפישה הטריטוריאלית, תחילה במרחב הפיזי, ולאחריו באינטרנט. אראה כיצד התפישה קנתה לה אחיזה בדיני החקירה במרחב הפיזי ולאחר מכן במרחב האינטרנט. כן אבקר את ההצדקות לתפישה הטריטוריאלית, ואראה כי אין הצדקה לאחוז בה, ודאי שלא באדיקות הנוהגת כיום, בכל הנוגע לאיסוף ראיות במסגרת חקירה פלילית של המדינה באינטרנט.

בפרק הראשון אבחן את התפישה הטריטוריאלית בדיני איסוף הראיות במרחב הפיזי. אתמקד במושג הסמכות (Jurisdiction) שעניינו כוחה של המדינה להחיל את משפטה אל מחוץ לטריטוריה שלה, ואבחין בין סמכות תחיקה לבין סמכות שפיטה ולבין סמכות אכיפה. אמקד את הדיון בסמכות האכיפה, ולמען הדיוק, בנגזרת שלה הנוגעת לחקירה הפלילית והיא – סמכות לאיסוף ראיות. בפרק השני אבחן את התפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט. אראה כיצד העתקת החקירה הפלילית לאינטרנט לא שינתה את התפישה הבסיסית, שלפיה כוחה של המדינה מוגבל לחקירה פלילית בתוך הטריטוריה המדינתית. התפישה הטריטוריאלית בנוגע לאינטרנט מניחה שהראיות הדיגיטליות ניתנות למיקום, המקום שבו מצויות הראיות הדיגיטליות הוא השרת שבו הן אגורות, או המחשב שבו הן עוברות, וכל עוד אלה מצויים מחוץ לטריטוריה המדינתית, אין למדינה סמכות לאכוף איסוף של אותן ראיות. בפרק השלישי אציג חריגות שונות מהתפישה הטריטוריאלית שהוכרו במשפטן של מדינות שונות. חריגות אלה מעידות כולן על הקושי הממשי של המדינות להתנהל במשטר טריטוריאלי קשיח באינטרנט. כן אתייחס בפרק זה לחריגות המוצעות בפרק המחשבים של תזכיר הצעת חוק סדר הדין הפלילי.<sup>7</sup> בפרק הרביעי אערוך דיון נורמטיבי בהצדקות לתפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט. אציג שלוש ביקורות על התפישה:

<sup>7</sup> תזכיר הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפישה), התשע"א-2011 (להלן: "תזכיר חוק החיפוש" או "תזכיר הצעת חוק החיפוש").

האחת היא ביקורת מכיוון אפיסטמולוגי; השנייה היא ביקורת המתמקדת במבנה הארכיטקטוני-טכנולוגי של הרשת; השלישית היא הביקורת מכיוון תאוריות של ריבונות. לבסוף, בפרק החמישי אסכם את הדיון במסקנה בדבר הצורך בפיתוח מודל חלופי למודל הטריטוריאלי שאינו תקף עוד בחקירה פלילית באינטרנט.

## א. התפישה הטריטוריאליה בנוגע לסמכות המדינה לאסוף ראיות במרחב הפיזי

כאשר בוחנים את סמכותה המשפטית-פלילית של המדינה, מקובל להבחין בין שלושה: (א) *Jurisdiction to Prescribe* – **סמכות תחיקתית**: החלת הדין המהותי המדינתי על המקרה הנדון; (ב) *Jurisdiction to Adjudicate* – **סמכות שיפוט**: סמכות לבית המשפט המדינתי לשפוט את המקרה הנדון; (ג) *Jurisdiction to Enforce* – **סמכות אכיפה**: סמכות לסוכניה של המדינה לאכוף בפועל מקרה מסוים המקים סמכות שיפוט.<sup>8</sup> ייאמר מיד כי במוקד מאמרי סמכות האכיפה הבין-לאומית, כיוון שהיא הנוגעת במישרין לאיסוף הראיות במסגרת חקירה פלילית. עם זאת, תובנות מסוימות בנוגע לסמכות התחיקה והשיפוט יוכלו להקרין על הדיון בסמכות האכיפה, ולכן ארחיב במידת מה על שלוש הסמכויות בהקשר של המשפט הפלילי.

בשלב זה של הדיון איני מתמקד בזירת האינטרנט, כי אם במרחב הפיזי בלבד. תמצית הטיעון בפרק זה היא כדלקמן: עקרון היסוד בדבר סמכותה של המדינה הוא כי הסמכות, בהקשרים משפטיים, תחומה לטריטוריה של המדינה. **סמכויות התחיקה והשיפוט של המדינה פרצו את הגבולות הטריטוריאליים** בהקשרים שונים, ואילו **סמכות האכיפה נותרה במסגרת טריטוריאליה**. כפי שאטען בהמשך הפרק, פער זה, שנפתח בין סמכות האכיפה לבין סמכויות התחיקה והשיפוט, מעורר קשיים משמעותיים ביותר בזירת האינטרנט ומאיים על יכולות המדינה לאכוף באפקטיביות את הדין הפלילי ברשת.

<sup>8</sup> הבחנה זו מופיעה ב: Restatement לעניין המשפט הבין-לאומי האמריקני: RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS LAW OF THE UNITED STATES (2009). כן ראו: International Bar Association, Report of the Task Force on Extraterritorial Jurisdiction 7–8 (2009), available at: [www.ibanet.org](http://www.ibanet.org). עוד ראו, בהקשר של כתיבה על סמכות שיפוט באינטרנט, את ההבחנה בין סמכות תחיקתית, שיפוטית ואכיפתית, כפי שהיא מופיעה אצל ברנר וקופס: Susan W. Brenner & Bert-Jaap Koops, *Cybercrime Jurisdiction: An Introduction*, in CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY (Susan W. Brenner & Bert-Jaap Koops eds., 2008) 1–7. ראו עוד: Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1 (2004).

**אשר לסמכות התחקית הבין-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.<sup>9</sup> יש להבחין בין טריטוריאליות סובייקטיבית ובין טריטוריאליות אובייקטיבית. 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.<sup>10</sup> ניתן לראות בעיקרון הטריטוריאלי משום נקודת מוצא, שממנה הורחבה תחולת דיני העונשין גם אל עברות מחוץ לטריטוריה של המדינה, וזאת בנסיבות ובתנאים מסוימים. ההרחבה היא בשני ממדים: הראשון, בממד של מתיחת העיקרון הטריטוריאלי עצמו. השני, בממד של פיתוח עקרונות שאינם טריטוריאליים. בכל הנוגע למתיחת העיקרון הטריטוריאלי עצמו, מוכרת הקביעה במשפט האמריקני, למשל, כי עברה שלא התממשה ותוכננה להתבצע בשטחו של הריבון, תיחלש על ידי העיקרון הטריטוריאלי גם אם תוכננה מחוץ לשטחו.<sup>11</sup> גם במשפט הישראלי חוק העונשין מחיל את ההרחבה האמורה. החוק קובע כי די שהעברה הנדונה תוכננה להתבצע בישראל על מנת שדיני העונשין הישראליים יחולו עליה.<sup>12</sup> הרחבה נוספת של העיקרון הטריטוריאלי היא כי גם מעשה שבוצע כל כולו פיזית מחוץ לארץ, אך **משפיע בפועל** על הטריטוריה המדינתית או על תושבים בטריטוריה זו, ייחשב כמעשה שהדין המדינתי חל עליו (לדוגמה, קרטל בין חברות זרות שנועד להשפיע על השוק המקומי בענף מסוים).<sup>13</sup>

<sup>9</sup> Joseph H. Beale, *The Jurisdiction of a State*, 36 HARV. L. REV. 241, 245 (1923); MICHAEL AKEHURST, MODERN INTRODUCTION TO INTERNATIONAL LAW 110-111 (7<sup>th</sup> ed. 1997); ש"ד פלר "בחנינות אחדות של עיקרון החוקיות כפליליים" **משפטים** א 19, 32 (1968); יורם דינשטיין "סמכות השיפוט הפלילית: גבולות והגבלות" **עיוני משפט** א 303, 306 (1971); כג"ץ 279/51 **אמסטרדם נ' שר האוצר**, פ"ד ו(2) 945, 971 (1952); ע"פ 7230/96 **פלוגי נ' מדינת ישראל**, פ"ד נא(3) 513, 521-522 (1997); רע"פ 1178/97 **כנא נ' מדינת ישראל**, פ"ד נא(3) 266, 269 (1997); United States v. Bowman, 260 U.S. 94 (1922).

<sup>10</sup> ראו: Rivard v. United States, 375 F.2d 882, 886 (5<sup>th</sup> Cir. 1967); וראו גם את ס' 7(א) ו-12 לחוק העונשין, התשל"ז-1977 הקובעים כי "עברת פנים" נחשבת גם לעברה שמקצתה בלבד נעברה בישראל.

<sup>11</sup> 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 (5<sup>th</sup> Cir. 1980); United States v. Mann, 615 F. 2d 668, 671 (5<sup>th</sup> Cir. 1980); United States v. Yousef, 327 F.3d 56, 91 (2<sup>nd</sup> Cir. 2003).

<sup>12</sup> ראו ס' 7(א) ו-12 לחוק העונשין.  
<sup>13</sup> Rio Tinto Zinc Corp. v. Westinghouse Electric Corp. [1978] 1 All ER 434 (HL) (Eng.). הרחבה זו מוכרת גם כ-"Effects" Doctrine, ראו למשל: Vaughan Lowe & Christopher Staker, *Jurisdiction*, in INTERNATIONAL LAW 313, 322-323 (3<sup>rd</sup> ed.,

בכל הנוגע לפיתוח עקרונות אקסטרה-טריטוריאליים לסמכות תחקית, ניתן לראות שדיני 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 ישראלים בחו"ל)<sup>14</sup> ותחולה אוניברסלית על עברות.<sup>15</sup> גם המשפט האמריקני

Malcolm D. Evans eds., 2010). על מיתון ההרחבה מטעמי כיבוד ריבונות של מדינות זרות אחרות שבהן התרחש המעשה מבחינה פיזית, ראו: MALCOLM N. SHAW, INTERNATIONAL LAW 688–692 (6<sup>th</sup> ed., 2008); United States v. Aluminum Co. of America, 148 F.2d 416 (1945).

14 ראו ס' 13–15 לחוק העונשין. עוד בקטגוריה זו גם החובה, שעונש בצד הפרתה, של תושב ישראל לשלם מס הכנסה בישראל גם על הכנסותיו שנצמחו מחוץ לישראל (כקובע בס' 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 הנציגולית של דיני העונשין" פלילים ה 5 (1996). לעמדה המצדיקה את ההרחבה האמורה, ראו: ש"ז פלר ומרדכי קרמניצר "תגובה לחיבור 'בגנות התחולה הנציגולית של דיני העונשין' מפרי עטו של יורם שחר" פלילים ה 65 (1996). כדוגמה ליישום הרחבת התחולה של עברות-החוק 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, תק-על 4387 (2)10 (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 ס' 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 טריטוריאליית 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).

15 ראו ס' 16 לחוק העונשין, שכתרתו "עבירות נגד משפט העמים", ומכוחו מקובל למנות פשעי מלחמה חמורים, השמדת עם, שוד ים, סחר בעבדים ועינויים. כן ראו: ס' 1(א) ו-2 לחוק לעשיית דין בנאצים ובעוזריהם, התש"י-1950; ס' 5 לחוק בדבר מניעתו וענישתו של הפשע השמדת עם, התש"י-1950. היישום המוכר ביותר של תחולה אוניברסלית אקסטרה טריטוריאליית (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 336/61 אייכמן נ' היועץ המשפטי לממשלה, פ"ד טז(3) 2033, 2066–2067 (1962); כמו כן, ראו: ס' 38 לפקודת הסמים המסוכנים [נוסח חדש], התשל"ג-1973, הקובע תחולה אקסטרה טריטוריאליית על עברות סמים בכל מקום בעולם. כאשר מדובר 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.

הכיר ב"פריצת גבולות" הטריטוריה בכל הנוגע לסמכות תחיקתית.<sup>16</sup> מהלך של פריצת גבולות הטריטוריה במסגרת הסמכות התחיקתית הוכרה גם במשפט הבין-לאומי.<sup>17</sup>

מבחינה עיונית ישנם כמה עקרונות של סמכות תחיקתית שאינה צמודה לטריטוריה: סמכות פרסונלית אקטיבית במובן של פרישת סמכות התחיקה על אזרחי המדינה בכל מקום שבו הם פועלים; סמכות פרסונלית פסיבית שלפיה ניתן להחיל את חוק המדינה ולשפוט אדם על מעשה שמשפיע על אזרחי המדינה, אפילו אם הוא אינו אזרח המדינה ואם הוא פעל מחו"ל; סמכות הגנתית/פרוטקטיבית שלפיה ניתן להחיל את החוק הפלילי על מעשים שבוצעו בחו"ל על ידי כל אדם, הפוגעים באינטרסים חיוניים של המדינה או מוסדותיה; סמכות אוניברסלית.<sup>18</sup> ניתן לומר שכל הרחבת סמכות מחוץ לגבולות הטריטוריה משמעה הצרת סמכות של מדינה אחרת.

<sup>16</sup> 18 U.S.C. § 1119, 2332, 3261; United States v. King, 552 F.2d 833, 850 (1976); MODEL PENAL CODE, 10 U.L.A. 433 § 1.03 (1974); 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 (1<sup>st</sup> Cir. 1997); United States v. MacAllister, 160 F.3d 1304, 1307 (11<sup>th</sup> 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*, in CONGRESSIONAL RESEARCH SERVICE REPORT 12-19 (2010).

<sup>17</sup> ראו: S.S. Lotus (France v. Turkey), 1927 PCIJ (Ser. A) No. 10, p. 18. אותו מקרה עסק בהתנגשות בים הפתוח בין אנייה תורכית לאנייה צרפתית, שבעקבותיה נספו כמה אזרחים תורכים. האנייה הצרפתית הגיעה לאיסטנבול והקצין הראשון שלה נעצר ונשפט בתורכיה. נוכח 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 לגבי פעולות שבוצעו מחוץ לטריטוריה שלה, ככל שיש להן תוצאות בטריטוריה שלה (האנייה התורכית נתפשת כטריטוריה). עקרון הטריטוריאליות אינו מהווה יסוד יחיד לסמכות השיפוט הפלילית. לעניין הרחבת סמכות התחיקה של מדינות מעבר לטריטוריה שלהן והכרת המשפט הבין-לאומי בכך, ראו הסקירה אצל: SHAW, לעיל ה"ש 13, בעמ' 652-683. לעניין הרחבת השימוש בסמכות אוניברסלית בזירה הבין-לאומית, ראו למשל: אמנון רייכמן "סמכות שיפוט אוניברסלית בבתי משפט מדינתיים – קרקוע הריבונות או יצירת סדר עולמי?" **משפט וצבא** 17, 49, 54-60 (2004).

<sup>18</sup> קטגוריזציה זו נסמכת על: Harvard Research in International Law, *Jurisdiction with Respect to Crime*, 29 AM. J. INT'L L. 435, 445 (1935). ראו עוד למשל את: SHAW, לעיל ה"ש 13, בעמ' 652-696 והפסיקה המובאת שם; דינשטיין "סמכות השיפוט הפלילית", לעיל ה"ש 9; יורם דינשטיין **סמכויות המדינה כלפי פנים** 94-104 (1972); ש"ז פלר "הסמכות התחיקתית" ו"סמכות השיפוט" **הפרקליט** כז 179, 181 (1971); אסתר נוימן-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, 629-627 (1983); ע"פ 4596/05 רוזנשטיין נ' מדינת ישראל, תק-על(4) 05, 3955, 3967-3973 (2005).

פרט להתפתחויות אלה של העיקרון הטריטוריאלי בנוגע לסמכות התחיקה הפלילית של המדינות, ראוי לציין התפתחות בין-לאומית נוספת: פיתוחה של סמכות משפטית פלילית אל-מדינתית בדמות בית הדין הבין-לאומי בהאג (ה-International Criminal Court – ICC); והקמתן של ערכאות שיפוטיות פליליות בין-לאומיות נוספות שהוקמו אד-הוק. התפתחות זו מצרה את סמכותן של המדינות, ומבטאת את הכפפת הריבונות לעקרונות-העל של המשפט הבין-לאומי.

**אשר לסמכות שיפוט בין-לאומית בהקשר של המשפט הפלילי:** ככלל, במסגרת המשפט הפלילי, סמכות השיפוט כרוכה בסמכות התחיקה. על כן כמעט שאין הפרדה מעשית ביניהן. אם דיני העונשין המדינתיים חלים על מקרה בין-לאומי, והנאשם הובא לדין ונאספו ראיות לצורך העמדה לדין (דהיינו, אם אין בעיה בתחום תחולת דיני העונשין ואין בעיה בתחום האכיפה הפלילית), ייטה בית המשפט להחיל את סמכותו על הנאשם.<sup>19</sup> יתר על כן, ברמה העיונית, ניתן לומר כי עצם הקביעה שדיני העונשין המדינתיים חלים על המקרה הנדון הוא אקט שיפוטי, ולכן מדובר בהפעלת סמכות שיפוט ולא סמכות תחיקה.<sup>20</sup>

**אשר לסמכות אכיפה בין-לאומית בהקשר של משפט פלילי:** הכוונה היא למכלול פעולות החקירה (מעצר, תשאול, חיפוש, תפיסה וכיוצא באלה) אם הן מיועדות להתבצע מחוץ לטריטוריה המדינתית. הכוונה היא גם לסוגיית הסגרתם של חשודים ונאשמים. בהכללה ניתן לומר שהסמכות השיפוטית עוסקת בהוצאה לפועל של הסמכות התחיקתית, ואילו סמכות האכיפה עניינה בהוצאה לפועל של שתיהן – הסמכות התחיקתית וסמכות השיפוט. עיקר ענייני במאמר הוא בסמכות האכיפה הבין-לאומית, ובתוך קטגוריה זו ענייני בסמכות הנוגעת לאיסוף ראיות המצויות בחו"ל במסגרת החקירה הפלילית (סמכות איסוף בין-לאומית). הכלל הגדול הוא כי

<sup>19</sup> 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 בדיני עונשין** כרך א' 236–237 (1984). ראו עוד את פרשת **רוזנשטיין**, לעיל ה"ש 18, בעמ' 3983–3992, 3988.

<sup>20</sup> ניתן לציין בכל זאת שני עניינים הנפרדים באופן מלא מסמכות התחיקה והם מתחום סמכות השיפוט בלבד: האחד, בחינת טענות של זיכוי או הרשעה קודמים וסיכון כפול, המביאים לבטלות ההליך השיפוטי, גם אם סמכות התחיקה חולשת על המקרה. השני, 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. ראו: RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 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 שיפוט אל מול סמכות שיפוט של מדינה אחרת, שעמה אין לה יחסים דיפלומטיים מכל סוג.

**סמכות האכיפה במרחב הפיזי מתוחמת לטריטוריה של המדינה החוקרת.** כלל זה מצוי בעקרונות המשפט הבין-לאומי, כנגזר מעקרון הריבונות הטריטוריאלית וכנלמד מאמנות שונות העוסקות באכיפה פלילית בין-מדינתית.<sup>21</sup> הוא מצוי גם בעקרונות הפנימיים של המדינות,<sup>22</sup> לרבות מדינת ישראל.<sup>23</sup> ארחיב מעט על עקרון הטריטוריאליות

<sup>21</sup> אמנות אלה מניחות מראש את עקרון הטריטוריאליות כעיקרון היסודי המחייב, לפיכך, שיתוף פעולה בין-מדינתי כאשר מדובר בפעולה חוצת גבולות. ראו: Europol Convention (Brussels, 1995); Constitution of Interpol (Vienna, 1956); 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 art.4, Nov. 2000 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: רובי סיבל **משפט בינלאומי** פרק 4: המדינה 77, 98-99 (מהדורה שנייה, רובי סיבל עורך 2010). ראו גם, בהקשר של המשפט הישראלי, את חוק עזרה משפטית בין מדינות, התשמ"ח-1988, ובפרט סעיפים 4, 8, 14-21, 28-31, 46-47, 53. ראו עוד: ANTONIO CASSESE, INTERNATIONAL LAW 50 (2<sup>nd</sup> ed., 2005); ROBERT CRAYER, HAKAN FRIMAN, DARRYL ROBINSON & ELIZABETH WILMSHURST, AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE 38-39 (2007) *Lowe & Staker*; לעיל ה"ש 13, בעמ' 335-337.

<sup>22</sup> **במשפט האמריקני** ראו: RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS: LAW OF THE UNITED STATES § 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 non judicial 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 את: Doyle, לעיל ה"ש 16, 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 טריטוריאלית. קיימת כמובן הכרה באפשרות לבצע פעולות איסוף ראיות מחוץ לטריטוריה של המדינה, אך ככלל הדבר יכול להיעשות בהסכמת המדינה האחרת בלבד. ראו למשל: State of New Hampshire v. R. v. Hape, Windhurst, 2006 WL 2075119 (N.H. Super. 2006). במשפט הקנדי ראו: "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

בכל הנוגע לסמכות האכיפה הפלילית במשפט הישראלי. ניתן למצוא דיון מפורש בסמכות האיסוף הבין-לאומית בפרשת **אל מצרי**.<sup>24</sup> אותו מקרה עסק 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 המשפט המחוזי להתיר למשטרה לבצע האזנת סתר, אינו חל בשטחים הכבושים, אלא רק בתחולה פרסונלית על אזרחי מדינת ישראל המתגוררים בהם. בוואקום החקיקתי 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: 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 סבורני כי יש לראות בפסק הדין הלכה המתייחסת להאזנת סתר בשטחים כבושים תחת "תפיסה לוחמנית", ולא הוראה גורפת המתירה האזנת סתר "מנהלית" בכל העולם. במקרה של האזנת סתר, או כל פעולת איסוף אחרת לצורך העניין, שתבצע בטריטוריה של **מדינה** עצמאית אחרת, תידרש בקשה לעזרה משפטית מהמדינה הזרה, או למצער הסכמתה של המדינה לביצוע ההאזנה על ידי הרשויות הישראליות (מחוץ למסלול העזרה המשפטית הפורמלית).<sup>25</sup> במקרה של שטח כבוש, כיוון שלא רלוונטי לפעול בדרך של עזרה משפטית, ואין צורך לשמור על עקרון כיבוד הריבונות של מדינה זרה, תיתכן התוצאה של האזנת סתר מחוץ לטריטוריה הקבועה ובסמכות מנהלית בלבד. מההלכה בפרשת **אל מצרי** נמצאנו למדים כי בית המשפט העליון קבע כי תחולת

---

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

<sup>23</sup> ראו את בג"ץ 5128/94 **פדרמן נ' שר המשטרה**, תק-על 195(1) 272, 266 (1995), שם נפסק מפי הנשיא שמגר: "תפקידיה וסמכויותיה של משטרת ישראל נקבעו כאמור בפקודת המשטרה [...] ובחיקוקים 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 בחיקוקים השונים, מחוץ לשטח הנתון לשליטתה של מדינת ישראל". יצוין כי אם הריבון הזר מסכים להפעלת סמכות אכיפה ישראלית בחו"ל, ההנחה היא שלא קיימת מניעה, מבחינת בית המשפט הישראלי, להכיר בסמכות לביצוע אותה פעולת אכיפה, במגבלות הרגילות של הדין הישראלי; כן ראו: ת"פ (מחוזי י"ם) 1071/01 **מדינת ישראל נ' רבינוביץ'**, תק-מח 2010(3) 16430 (2010).  
<sup>24</sup> ראו ע"פ 4211/91 **מדינת ישראל נ' אל מצרי**, פ"ד מז(5) 624, 639-640 (1993).  
<sup>25</sup> אציין כי כוונתי כאן לפעולות איסוף ראיות במסגרת חקירה פלילית ולא לפעולות המתבצעות מכוח סמכויות הביטחון של המדינה.

החוק המסדיר סמכויות אכיפה של משטרת ישראל לביצוע האזנת סתר היא טריטוריאלית, כל עוד לא נקבע במפורש אחרת. בשונה מהסמכות התחקיתית, בה נמצאו הרחבות רבות הן בדמות פיתוח העיקרון הטריטוריאלי והן בדמות פיתוח עקרונות אקסטרה-טריטוריאליים, בכל הנוגע לסמכות האכיפה המדינות ממעטות להפר את עקרון הטריטוריאליות. ההפרה המוכרת ביותר היא במקרים שבהם רשויות המדינה חטפו חשודים, ולימים נאשמים, ממדינות זרות לצורך הבאתם לדין.<sup>26</sup>

## ב. איתור התפישה הטריטוריאלית בנוגע לאינטרנט

כפי שאציג בפרק זה, התפישה הטריטוריאלית, החולשת על סמכות האכיפה הפלילית הבין-לאומית במרחב הפיזי, מועתקת אל מרחב האינטרנט. מאחר שהעברות באינטרנט חוצות גבולות מדיניים ב"לחיצת כפתור", הופכת סוגיית הטריטוריאליות באינטרנט לסוגיה מרכזית ביותר בדיני האכיפה הפלילית. במישור הפלילי המהותי, הרחיבו המדינות בנדיבות את סמכותן לשפוט עברות המתרחשות בכמה "מקומות" באינטרנט בו-זמנית, ואילו במישור הפלילי הדיוני, הפך עניין מיקום הראיות הדיגיטליות למעין עקרון וטו להשבתת חקירות מדינתיות. כך או כך, הנחת המוצא בנוגע למעשה העברה באינטרנט היא טריטוריאלית, וכך אף היחס לאיסוף הראיות באינטרנט.

מרבית המחקר בתחום המשפט הפלילי באינטרנט, הנדרש לסוגיית הסמכות הבין-לאומית בנוגע לאינטרנט, בחן את סוגיית הסמכות הבין-לאומית המהותית (בעיקר התחקיתית), ולא סוגיות מתחום דיני האכיפה. גם הפסיקה מתמקדת בבחינת גבולות הסמכות הבין-לאומית המהותית. אשר לחסר בפסיקה בתחום זה, ניתן להסבירו בכך שמגבלת סמכות האכיפה היא כאמור מעין וטו המביא לריסון מראש של גופי אכיפת החוק, ועל כן הסוגיה אינה מרבה להתעורר באופן חזיתי.

<sup>26</sup> ראו למשל: United States v. Alvarez-Machain, 504 ;Ker v. Illinois, 119 U.S. 436 (1886) U.S. 655 (1992). שם בית המשפט לא ביטל את ההליכים נגד הנאשם שנחטף ממקסיקו לארצות-הברית, ויישם את הדוקטרינה של "Improperly captured, properly detained". כן ראו: פרשת **אייכמן**, לעיל ה"ש 15, בעמ' 2067. שם מוכר עניינו של אדולף אייכמן שנחטף על ידי המוסד מארגנטינה. בית המשפט העליון קבע מפי השופט אגרנט: "לא יחקור בית המשפט בנסיבות עצירתו והבאתו (של הנאשם) לתחום השיפוט". לתיקי חטיפה נוספים שבהם נדונה שאלת הפרת הדין הבין-לאומי, ראו סקירה אצל: Cassese, לעיל ה"ש 21, בעמ' 50-52.

## 1. סמכות תחיקתית ושיפוטית באינטרנט

הסמכות התחיקתית והשיפוטית בנוגע לעברות באינטרנט, יוצאת מאותה נקודת מוצא טריטוריאלית הרלוונטית לסמכות התחיקתית והשיפוטית במרחב הפיזי, אך הטריטוריאליות נמתחת באופן כזה, המאפשר להרחיב משמעותית את סמכות השיפוט בנוגע לעברות האינטרנט. לפי הכלל הדורש כי מקצת העברה (בישראל למשל)<sup>27</sup> או חלק בלתי-מבוטל ממנה (בבריטניה למשל)<sup>28</sup> ייעברו במדינת הפורום, על מנת שזו תיחשב עברת פנים, מיובאות עברות אינטרנט רבות כעברות פנים. מיקומו הפיזי של מבצע העברה מחוץ לטריטוריה, ואף מיקום מחשביו מחוץ לטריטוריה, אינו מחסן מפני הפללת מעשהו, אם יש בה התקשרות עם קרבן או חשיפה מודעת של מידע לקרבן הנמצא במדינה השופטת.<sup>29</sup> מכאן שלא התעורר הצורך בפיתוח עקרונות נוספים שאינם טריטוריאליים במיוחד עבור עברות באינטרנט. אציג להלן כמה מקרים מייצגים המלמדים על הרחבת סמכות התחיקה והשפיטה בנוגע לעברות אינטרנט דרך הצינור הטריטוריאלי במובנו המקובל, המסתפק במקצת או חלק מן העברה על מנת לקנות סמכות.

המקרה המוכר ביותר במשפט הישראלי שבו נדונה סוגיית סמכות השיפוט (וכפועל יוצא מכך גם סמכות התחיקה) הבין-לאומית באינטרנט הוא מקרהו של **מייקל קרלטון**. קרלטון הוא מבעליו של אתר ההימורים המצליח "ויקטור צ'נדלר", ששרתיו ממוקמים בגיברלטר, שם מותרים כל סוגי ההימורים המוצעים באתר. האתר מציע את שירותיו למהמרים מכל העולם, לרבות מישראל, וחלק 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, לנוכח העובדה 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

<sup>27</sup> ראו לעיל ה"ש 13.

<sup>28</sup> ראו: R. v. Smith (Wallace Duncan) (No. 4) [2004], QB 1418 (Eng.). בעבר הגישה האנגלית חייבה השלמה של כל היסוד העובדתי של העברה בטריטוריה האנגלית, על מנת שתחשב העברה כ"עברת פנים" לפי הדין האנגלי; ראו: R. v. Manning, [1998] 2 Cr. App. R. 461 (Eng.).

<sup>29</sup> ברם, אילו הייתה רווחת הגישה שבוטאה בפסק הדין האנגלי בפרשת *Manning*, לעיל, ניתן היה 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, לא ניתן יהיה להפיל את התנהגותו של מבצע העברה.

משום עברת פנים, המקימה סמכות שיפוט ישראלית.<sup>30</sup> מקרה נוסף שבו התעוררה שאלת סמכות השיפוט הבין-לאומית בנוגע לעברות אינטרנט, היה בפרשת **משה הלוי**, פעיל רשת ידוע המכונה "הלמו", שהואשם בכך שפרסם את תמונת מפכ"ל המשטרה לשעבר, רנ"צ משה קראדי, כשהוא לבוש כביכול במדים נאצים. התמונה נערכה כפוטו-מונטאז' והועלתה לפורום rotter.net, ששרתיו מצויים בארצות-הברית. הלמו הואשם בעברה של העלבת עובד ציבור, ובמהלך משפטו העלה טענה מקדמית של חוסר סמכות בין-לאומית לשיפוט אותו על העברה, נוכח העובדה 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.<sup>31</sup>

בדין האמריקני מוכרת הפסיקה בפרשת *W.I.G.C.*, שעסקה בהקמת 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. בית המשפט שם הכיר בסמכותו לדון בעברות כעברות פנים.<sup>32</sup> בנוסף, ניתן למצוא פסיקה מרחיבת סמכות שיפוט בכל הנוגע לעברות של פרסום 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). בפרשת *Thomas* נקבע העיקרון של ביצוע עברת הפרסום כעברת פנים בכל מקום שאליו מגיע התוכן, ולא רק במקום הפצתו המקורי.<sup>33</sup>

גם במשפט האיחוד האירופי ניתן למצוא ביטוי לתפישה מרחיבה של סמכות השיפוט התחיקתית והשיפוטית בנוגע לעברות באינטרנט. בית הדין האירופי לצדק

<sup>30</sup> ראו: ב"ש (מחוזי ת"א) 90861/07 קרלטון נ' היחידה הארצית לחקירות הונאה, תק-מח 07(2) 11247 (2007); להתייחסות מוקדמת יותר (אם כי לאקונית יחסית), גם כן בהקשר של הימורים באינטרנט, ראו: ב"ש (מחוזי חי') 3707/01 יגודייב נ' מדינת ישראל, תק-מח 01(3) 4750, 4753 (2001). ראו: ב"ש (מחוזי חי') 3707/01 יגודייב נ' מדינת ישראל, (פורסם בנבו, 08.08.2001).

<sup>31</sup> ראו: ת"פ (שלום עכו) 1826/08 מדינת ישראל לשכת תביעות גליל-משטרת ישראל נ' הלוי, תק-של 09(1) 13793 (2009). לימים זוכה הלוי מן העברות שיוחסו לו, אם כי מטעמים אחרים שאינם צריכים לענייננו. ראו: ת"פ (שלום עכו) 1826/08 מדינת ישראל נ' הלוי (פורסם בנבו, 2.11.2011).

<sup>32</sup> ראו: People of New York v. World Interactive Gaming Corp., 714 N.Y.S. 2d 844 (1999) (להלן: "פרשת *W.I.G.C.*").

<sup>33</sup> ראו: U.S. v. Thomas, 74 F.3d 701 (6<sup>th</sup> Cir. 1996). יצוין כי פרשת *Thomas* נוגע לבררת סמכות השיפוט בין שתי מדינות בארצות-הברית, ולא בין ארצות-הברית למדינה זרה, אך בעניין זה אין הבדל בין המערכת הפדרלית בארצות-הברית לבין המערכת הבין-לאומית, ונוסח פסק הדין כוון לקבוע עיקרון כללי בעניין דנן.

(European Court of Justice) מתח את גבולות עברת הפנים בהימורים באינטרנט בדומה לפסיקה בפרשות *W.I.G.C. וקרלטון* שנמנו לעיל.<sup>34</sup> 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.<sup>35</sup>

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.<sup>36</sup> לא אתיימר

<sup>34</sup> ראו: *Liga Portuguesa de Futebol Profissional v. Departamento de Jogos da Santa Casa da Misericórdia de Lisboa*, ECJ C-42/07 (2009).

<sup>35</sup> ראו: Council Framework Decision 2005/222/JHA on Attacks Against Information Systems, Art. 10, OJ L69/67 (16.3.2005).

<sup>36</sup> אתן מדגם של כמה פסקי דין מוכרים מהמשפט האמריקני: ראו למשל את: *Compuserve v. Patterson*, 89 F.3d 1257 (6<sup>th</sup> Cir. 1996), שם נפסק בעניין סכסוך חוזי בין-מדינתי בתוך ארצות-הברית. התובעת היא חברת *Compuserve* שמושבו באוהיו ושרתיה ממוקמים במדינה. הנתבע הוא אזרח טקסני שפעל מטקסס. נקבע כי לאוהיו קמה סמכות שיפוט, נוכח העובדה שהנתבע התקשר בפועל עם שרתי המחשב של *Compuserve* באוהיו והעלה באמצעותם תכנים שונים לאינטרנט, ומכאן שלנתבע זיקה לאוהיו; ראו: *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295 (S.D.N.Y. 1996), שם 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; ראו: *Zippo Manufacturing Company v. Zippo Dot Com, Inc.*, 925 F. Supp. 1119 (W.D. Pa. 1997), שם נקבעה סקאלה לקביעת סמכות שיפוט על נתבע זר במדינת הפורום: בקצה האחד של הסקאלה, כאשר הנתבע מבצע עסקאות באמצעות האינטרנט המשפיעות באופן ישיר וברור על אזרחים במדינת הפורום – קמה סמכות למדינת הפורום. בקצה השני של הסקאלה, כאשר הנתבע מנהל אתר פאסיבי 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 יכולים אזרחים ממדינות זרות לפעול, יש לבחון את מידת האינטראקטיביות והאופי המסחרי של הפעילות האינטראקטיבי, ועל בסיסה ניתן יהיה לקבוע סמכות שיפוט למדינת הפורום. סקאלת *Zippo* אומצה בפסיקה מאוחרת יותר; לסקירה ראו למשל: *HENRIK SPANG-HANSEN, PUBLIC INTERNATIONAL COMPUTER NETWORK LAW* (2006) ISSUES 175–257. כמו כן, אציין את פסק הדין של בית המשפט העליון האוסטרלי בתביעת לשון הרע שהגיש איל ההון יוסף 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 נוכח הכוונה של העיתון האינטרנטי להגיע לקהל

להקיף את הפסיקה האמורה. עם זאת, ניתן להבחין כי מקום מושבו של מעלה התכנים ומקום הימצאותו הפיזית של השרת או המחשב שממנו מועלים או משודרים התכנים אינו מחסן מפני החלת הדין של מדינות אחרות שבהן נחשפו משתמשי אינטרנט לתכנים אלה.<sup>37</sup>

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 (4<sup>th</sup> Cir. 2002), שם נפסק כי מהדורה מקוונת של עיתון ממדינת קונטיקט, שהועלה לאתר אינטרנט שנמצא בשרת בקונטיקט אך נצפה בפועל גם במדינת וירג'יניה, שבה מתגורר התובע, אינה מקימה כשלעצמה סמכות שיפוט בוירג'יניה. העובדה שהפרסומות באתר האינטרנט כוונו לתושבי קונטיקט והכתבות בעיתון לא עסקו באופן מכוון בענייני מדינת וירג'יניה – מלמדת שאין להעניק סמכות שיפוט למדינת וירג'יניה; במשפט הישראלי ניתן לציין את ה"פ" (מחוזי י"ם) *Ahava (USA) Inc. 3137/04 נ' ג'. דבליו. ג'י. בע"מ (J.W.G. Ltd.)*, תק-מח 404 (4) 128 (2004). באותו מקרה 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 בנוגע לקהל אמריקני מכפיף עצמו לסמכות השיפוט האמריקנית.

הפרשה אשר בוודאי היא המוכרת ביותר בתחום סמכות השיפוט בעניינים אזרחיים באינטרנט היא פרשת *Yahoo! v. L.I.C.R.A.* פרשת זו מלמדת על האופן שבו הרחיבה הפסיקה הצרפתית את סמכות התחיקה הפלילית שלה, האוסרת הצגת סמלים נאציים, גם על פעולות באינטרנט שמקורן הוא מחוץ לתחומי צרפת. 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, כאמור. בית המשפט הגבוה בפריז קבע כי יאהו! הפרה את הקוד הפלילי הצרפתי, ועל כן מחובתה למנוע גישה של משתמשי אינטרנט צרפתיים לדפי התוכן האסורים, לרבות על ידי סינון גולשים מכתובות IP צרפתיות, דרישה מהגולש לציין את מדינת מוצאו כאשר כתובת ה-IP שלו מעורפלת באופן שאינו מאפשר זיהוי ארץ מוצאו בוודאות וכיצא בזה. הפסיקה הוחלה לא רק על יאהו! בצרפת (*Yahoo.fr*), אלא גם על יאהו! האמריקנית (*Yahoo.com*). ראו: *La Ligue Contre le Racisme et l'Antisemitisme (LICRA) v. Yahoo!, Inc.*, Tribunal de Grande Instance [T.G.I.] Paris, Ordonnance de Refere (2000), available at [www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf](http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf). יאהו! האמריקנית בחרה לפנות לבית משפט אמריקני בבקשה לסעד הצהרתי שיכריז שפסק הדין הצרפתי לא ייאכף בארצות-הברית, בשל פגיעתו בחופש הביטוי כפי שהוא מפורש על בסיס התיקון הראשון לחוקה האמריקנית. בערכאה הראשונה התקבלה עתירתה של יאהו!. ראו: *Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal. (2001)). 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 בלתי-סבירה בנסיבות העניין. ראו: *La Ligue Contre le Racisme et l'Antisemitisme (en banc) v. Yahoo!, Inc.*, 379 F.3d 1120 (9<sup>th</sup> Cir. 2004).

## 2. סמכות אכיפה

הכלל הנוהג הוא שסמכות האכיפה בנוגע לאיסוף ראיות דיגיטליות באינטרנט מוגבלת לטריטוריה המדינתית. הגבולות המדינתיים מורכבים על האינטרנט וראיה האגורה בשרתים מחוץ לטריטוריה המדינתית – אסורה, ככלל, באיסוף במסגרת חקירה פלילית.<sup>38</sup> במקרה כזה, יכולה המדינה לפעול באחת הדרכים הבאות: **האחת**, פנייה למנגנון של עזרה משפטית. ישנם מנגנונים מיוחדים לעזרה משפטית המתייחסים במפורש לראיות דיגיטליות, בראשם אמנת מועצת אירופה בדבר פשעי מחשב (Convention on Cybercrime) שנחתמה בבודפשט בשנת 2001.<sup>39</sup> אמנה זו נועדה לטפל באופי הטרנס-מדינתי של העברות הפליליות באינטרנט. אולם בה בעת, הנחת המוצא של האמנה היא שהאכיפה הפלילית היא עניין למדינה, וכי נקודת המוצא היא שמירה על השוויון הריבוני של המדינות.<sup>40</sup> מכאן שהאמנה, כיצירת המשפט הבינ-לאומי ההסכמי, משעתקת את התפישה הטריטוריאלית בנוגע לאכיפה הפלילית באינטרנט. **השנייה**, פנייה בבקשה לפתוח בחקירה מקומית במדינה הזרה, בתנאי שמדובר בעברה גם על פי דינה 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

הפסיקה נותרה על כנה. ראו: Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 433 F.3d 1199 (9<sup>th</sup> Cir. 2006). הארגונים הצרפתיים למלחמה באנטישמיות הגישו בקשת רשות ערעור לבית המשפט העליון והבקשה נדחתה. ראו: La Ligue Contre le Racisme et l'Antisemitisme v. Yahoo!, Inc., cert. denied, 126 S. Ct. 2332 (2006).

<sup>38</sup> Henry H. Perritt, *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 82–90 (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. International Bar Association ; MARSHALL J. COMP. & INFO. L. 347 (2002), לעיל ה"ש 8, בעמ' 9–10.

<sup>39</sup> האמנה פתוחה להצטרפות של מדינות מחוץ למועצת אירופה. עד כה 46 מדינות, כולל כמה מדינות מחוץ לאירופה, כגון ארצות-הברית, קנדה ויפן, חתמו על האמנה, ו-26 מתוכן אשררו אותה. לנוסח האמנה המלא, ראו: Convention on Cybercrime, Nov. 23 2001, [conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm](http://conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm); לפירוט המדינות החתומות על האמנה, ראו: [conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG](http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG).

<sup>40</sup> לפי Convention on Cybercrime, Art. 22(4), האמנה אינה מתנה על גישתן של המדינות בנוגע לסמכות התחיקה, השפיטה והאכיפה שלהן.

המקורית. וכך, מתוך שלא לשמה בא לשמה, והמדינה שפתחה ראשונה בחקירה תקבל את הראיה הדיגיטלית שנדרשה לה מחו"ל. **השלישית**, 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.<sup>41</sup>

מרבית המדינות המערביות מגבילות את עצמן מלאסוף ראיות דיגיטליות באינטרנט האגורות פיזית בחומרי מחשב בחו"ל.<sup>42</sup> ניתן להסביר זאת כהמשך טבעי

<sup>41</sup> ראו: Perritt, לעיל ה"ש 38, בעמ' 35-36, 83-89, 114; כן ראו: Brenner & Schwerha, לעיל ה"ש 38, בעמ' 354-366.

<sup>42</sup> ראו את המקורות שפורטו לעיל בה"ש 38; ראו התייחסות פרטנית נוספת למדינות הבאות: בארצות-הברית: מדרין משרד המשפטים האמריקני מנחה את גופי התביעה ורשויות החקירה בארצות-הברית 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 (2009) 56-60, available at: [www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf](http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf). סמכות החדירה לחומרי מחשב חלה גם על חדירות מרחוק למחשבים, לאו דווקא על חדירה למחשבים התפוסים פיזית בידי המשטרה. כך קבוע ב- 19(4) Police and Criminal Evidence Act, s. 19(4) (1984) כפי שתוקן בתקון עקיף על ידי ה- Criminal Justice and Police Act, Sch. 2(2), para. 13(2)(a) (2001). לכאורה אין הגבלה בחוק זה על מיקומו של המחשב שאליו חדרו מבחינה טריטוריאלית, אולם חלה בעניין זה המגבלה הכללית הקבועה ב- Police Act 1996, s. 30(1) (1996) לפיו: "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 הטריטוריאלית בנוגע לאיסוף ראיות דיגיטליות ראו במדרין רשויות האכיפה הבריטיות: ASSOCIATION OF CHIEF POLICE OFFICERS, GOOD PRACTICE GUIDE FOR COMPUTER-BASED ELECTRONIC EVIDENCE 13, available at: [www.7safe.com/electronic\\_evidence/ACPO\\_guidelines\\_computer\\_evidence.pdf](http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf). בהולנד: החוק ההולנדי מתיר חדירה משטרתית לרשת בין מחשבים, בגדרה יותר לרשויות להגיע לכל המחשבים אליהם יש גישה דרך המחשב המקורי, שביחס אליו 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) דנמרק: דנמרק מפרשת את המשפט הבין-לאומי ואת שיטת משפטה הפנימית, ככאלה האוסרים אכיפה מחוץ לתחומי הטריטוריה המדינתית. לפיכך, גם בהקשר אינטרנטי, נאסרו חדירה או העתקה של חומר מחשב המצוי במחשבים מחוץ לטריטוריה הדנית. ראו: Spang-Hanssen, לעיל ה"ש 36, בעמ' 418-420. באיטליה: דיני איסוף הראיות הדיגיטליות באיטליה מחייבים את הרשויות לעצור ככל שהם מגיעים לחומר מחשב המצוי מחוץ לטריטוריה, ולפנות למנגנוני שיתוף הפעולה הבין-מדינתיים, בין שמדובר במנגנון האמנה האירופית למניעת פשעי מחשב, מנגנוני 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,

וישיר של האיסור המקביל הקיים בנוגע לחקירות פליליות במרחב הפיזי. כיוון שבתו המשפט נאלצו להתמודד עם תיקים פליליים שנאספו לפתחם, וכיוון שבתו המשפט, בפרט במדינות המשפט המקובל, הם מוסדות משפטיים שמרניים מטבעם, המתקדמים על דרך של פרשנות, לרבות היקש,<sup>43</sup> ומחילים תקדימי עבר מחייבים, אך טבעי הוא שהוחל הכלל, האוסר על הפעלת סמכות אכיפה אקסטרה טריטוריאלית, מהמרחב הפיזי אל האינטרנט.<sup>44</sup>

### 3. הביטוי היישומי של התפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט

כיצד מיושמת התפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט? מהלך החשיבה הטריטוריאלית ניתן לתיאור על פי הפירוק שלושה גורמים, כדלקמן: ראשית, הראיה הדיגיטלית ניתנת למיקום באינטרנט. שנית, המקום הוא המחשב שבו מאוחסנת הראיה הדיגיטלית. שלישית, איסוף הראיה מתבצע במקום שבו מאוחסנת הראיה הדיגיטלית. שלושת היסודות הללו מבטאים את התפישה הטריטוריאלית. שלושתם מכוננים את עקרון הווטו הטריטוריאלית בנוגע לסמכות האכיפה הפלילית באינטרנט, ולפיו אם הראיה הדיגיטלית המבוקשת אגורה בשרת המצוי פיזית בחו"ל, אזי אין סמכות למדינה החוקרת לאסוף את הראיה האמורה בפעולה עצמית (אונילטרלית).

הנחת המוצא, הנלמדת מהפרקטיקה המשפטית, היא שהמידע באינטרנט, אשר בענייננו מרכיב ראיות דיגיטליות הדרושות לחקירה פלילית, ניתן למיקום. הגם

---

*Cybercrime and Jurisdiction in Italy, in CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY 227, 233–234 (Bert-Jaap Koops & Susan W. Brenner eds., 2008)*; שבכדיה: הדגש הוא על מיקומו של השרת, ומיקום מחוץ לטריטוריה השבדית פוסל מיניה וביה כל אפשרות לאסוף את הראיה הדיגיטלית בפעולה של הרשות השוודית. ראו: GRAHAM J. H. SMITH, INTERNET LAW AND REGULATION 339 (3<sup>rd</sup> ed., 2002). בגרמניה: הדעה הרווחת היא שאסורה לרשויות החקירה הגישה לחומרי מחשב האגורים בחו"ל. בעבר התגלעה מחלוקת בנוגע לשאלת הגישה של החוקרים הגרמנים לחומרי מחשב הפתוחים לעיון כלל הציבור באינטרנט. ראו: Nicolai Seitz, *Transborder Search: A New Perspective in Law Enforcement?*, 7 YALE J. LAW & TECH. 23, 34–35 (2004). מאז שנת 2009, עם הצטרפות גרמניה לאמנה האירופית למניעת פשעי מחשב, אימצה גרמניה את הכלל הנקוט בסעיף 32 לאמנה, שלפיו מותר לחדור לחומרי מחשב האגורים מחוץ לטריטוריה במקרה של חומרים הנגישים לכלל הציבור ובמקרה של הסכמה כדין של המחזיק בחומר המחשב.

<sup>43</sup> יש לזכור כי הליך היקש הפרשני אף מתומרך על ידי המחוקק. ראו ס' 1 לחוק יסודות המשפט, התש"ם-1980, שבו נקבע כי אחת מדרכי ההכרעה השיפוטיות היא "בדרך של היקש".

<sup>44</sup> בהמשך המאמר אציג את הוראותיהן המיוחדות של כמה מדינות, אשר בכל זאת פתחו בנוגע לזירת האינטרנט, ונקבע בהן היתר מסוים לחידרה לחומרי מחשב האגורים מחוץ לטריטוריה המדינתית.

שהמידע מיוצג בביטים והוא חסר משקל וגודל, הוא משויך לאטומים פיזיים. הדברים מובילים ללוקליזציה וטריטוריאליזציה של האינטרנט, שכן אטומים ניתנים למיקום, והם מצויים בתוך מרחב טריטוריאלי. ההנחה שהראיה הדיגיטלית ניתנת למיקום באינטרנט מושפעת מהתיאור המטאפורי,<sup>45</sup> השגור בפי משפטנים הבוחנים את האינטרנט, של האינטרנט כמקום.<sup>46</sup> מטאפורת האינטרנט כמקום, על אף שכיחותה,

<sup>45</sup> השימוש במטאפורות במסגרת החשיבה המשפטית הוא, מצד אחד, תהליך בלתי נמנע של דפוס החשיבה האנושי, ומצד שני, תהליך מודע של הבניית דפוס הניתוח המשפטי ולעתים אף הכוונת התוצאה המשפטית. הגם שהמטאפורה בשימוש המשפט מייצרת מעין פיקציה, שכן אין היא מתארת את המציאות העובדתית כהווייתה, אלא מדמה אותה, אין זאת אומרת כי מיניה וביה היא פסולה בשימוש. להרחבה על תפקידה של המטאפורה בחשיבה המשפטית ראו למשל את עבודותיו של סטיבן וינטר: Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 40 STAN. L. REV. 1371 (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) 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, 489–490 (1993); 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); אברהם נ' טננבוים "על המטאפורות בדיני המחשבים והאינטרנט" **שערי משפט** ד 359 (2006).

<sup>46</sup> האינטרנט כתופעה משפטית הוא עניין רחב ומגוון הקשה ל"עיכול" משפטי. לפיכך, נדמה כי השימוש במטאפורות בנוגע אליו רב במיוחד. האינטרנט תואר כ**מערב פרוע**. ראו: Shamoi 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, 1222–1232 (2002); Clay Calvert, *Comment, Regulating Cyberspace: Aotostordet המידע*, ראו: *Metaphor, Rhetoric, Reality, and the Framing of Legal Options*, 20 HASTINGS COMM. & ENT. L.J. 541, 542–543, 547–549 (1998); HENRY H. PERRITT, *LAW AND THE INFORMATION SUPERHIGHWAY* (1996), שם מציג פריט בהקדמה לספרו את מטאפורת ה-Cyberspace; Infobahn או Information superhighway – מקובל לראות את מקורה של המטאפורה בספר מדע בדיוני של ויליאם גיבסון משנת 1984. ראו: WILIAM Hardy I. Gibson, *Neuromancer* (1984). להחלה משפטית של המטאפורה, ראו למשל: Trotter, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 994–995 (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 &

אינה עניין דטרמיניסטי, ויש לפתח כלפיה יחס ביקורתי,<sup>47</sup> כפי שאני מבקש לעשות

Charles Nesson eds., 1997). ג'ולי כהן (Cohen) וברוס קלר (Keller) גרסו כי מטאפורת האינטרנט כ-"Cyberspace" היא שגויה. מטאפורת ה-Cyberspace מעורדת התייחסות שגויה, לטענתם, אל האינטרנט 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 as/and Space*, 107 COLUM. L. REV. 210 (2007). ראו גם: Orin S. Kerr, *Criminal Law in Virtual Worlds*, 2008 U. CHI. LEG. F. 415, 415-416 (2008). קר לא טען כי מטאפורת ה-Cyberspace אינה נכונה, אלא כי היא הפכה עם השנים לבלתי-רלוונטית עוד, עם חדירת האינטרנט לחיי היומיום באופן מלא, עם השתפרות הקישוריות (Connectivity) והעברת חלק ניכר מפעילות הפנאי והמסחר לאינטרנט. ואף **כעולם פיאודלי**. ראו: Alfred C. Yen, *Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1236-1261 (2002). המטאפורות השונות מתקיימת תחרות מטאפורית. חוקרים שונים טענו כי ריבוי השימוש במטאפורות יש בו כוח מאזן למניעת עיוותים בהתייחסות המשפטית לסוגיה מסוימת. ראו, בהקשר משפטי כללי (לא אינטרנטי): MILNER S. BALL, LYING DOWN TOGETHER: LAW, METAPHOR AND THEOLOGY 22 (1985) Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1163-1166 (1999); ראו: Yen, שם, בעמ' 1209. בכל הנוגע להקשרו הנדון, של אכיפה פלילית באינטרנט, מטאפורת האינטרנט כמקום גברה על מרבית המטאפורות האחרות, והיא זו המוצאת ביטוי במשפט הנוהג בנוגע לאכיפה פלילית באינטרנט. ממתאפורת האינטרנט כ"מקום" נגזרים תיאורים מטאפוריים משניים, המתארים פעולות שונות במרחב האינטרנטי. כך, למשל, אנו נכנסים לאתר אינטרנט מסוים, אנחנו מקלידים **כתובת** אינטרנטית, החדירה האסורה לחומר מחשב מתוארת כ**כריצה** למקום או **כהשגת גבול**, אתר האינטרנט אף נבחן כ**כזה הנגיש לאנשים עם מוגבלויות** ועוד. ראו: Dan L. Burk, *The Trouble With Trespass*, 3 J. SMALL & EMERGING BUS. L. 1 (1999); Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421 (2002); Kathleen K. Olson, *Cyberspace as Place and the Limits of Metaphor*, 11 CONVERGENCE 10 (2005). ליישום פסיקתי של עוולת השגת גבול במיטלטלין בארצות-הברית, ראו למשל: eBay Inc. v. Bidder's Edge Inc., 100 F. Supp. 2d 1058 (2000); America Online v. National Health Care Discount, Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001); Oyster Software, Inc. v. Forms Processing, F.Supp.2d 2001 Intel Corp. v. Hamidi, 71 P.3d 296 (N.D. Cal. 2001). WL 1736382 (N.D. Cal. 2001) עם **אולם השוו, מנגד, עם** (2003), שם נדחתה האנלוגיה להשגת גבול במיטלטלין בנוגע לעובר לשעבר באינטל ששלח דוא"לים לעובדים בחברה, ובהם הכפיש את החברה.

ראו: Mark A Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003). למלי הציג סיטואציות שבהן בתי המשפט הצליחו להתנתק ממגבלות מטאפורת ה"מקום" וגילו גישה מחשבתית מעט פרגמטית יותר, המתאימה למאפייניה של רשת האינטרנט. 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 האינטרנט. ראו עוד: 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 שבחן את היחס בין מטאפורות ואנלוגיות שגויות לבין דיני האינטרנט. אורוק כחנה את האנלוגיות הבאות – אתר אינטרנט כספר ואתר אינטרנט כקניין מוחשי – בהקשר של

47

במאמר זה, בהקשר של השלכת המטאפורה על התפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית. על ההנחה כי הראיה הדיגיטלית ניתנת למיקום באינטרנט, מורכבת הנחה נפרדת ונוספת, שלפיה המקום הרלוונטי לראיה הדיגיטלית הוא המקום בכתובת האינטרנטית המסוימת, שאליה מבקשים החוקרים לחדור ואשר בה אגור המידע המבוקש. ואל שני אדנים אלה מתווספת ההנחה השלישית, שלפיה המקום שלגביו מיוחסת פעולת איסוף הראיה הדיגיטלית הוא המקום שבו מאוחסנת אותה ראיה. נניח כי איסוף הראיה באינטרנט מתבצע על ידי שוטר המתקשר מרחוק אל השרת שבו אגורה הראיה, מעיין בה ממחשבו ומעתיק אותה אל מחשבו. ברי כי פעולת האיסוף בוצעה ממקום מושבו של השוטר, אולם לא זה המקום הקובע, כאמור לעיל, כי אם המקום שבו אגורה הראיה הדיגיטלית.

### ג. פריצות מעשיות של התפישה הטריטוריאלית בנוגע לדיני איסוף באינטרנט

התפישה הטריטוריאלית הנוקשה בנוגע לסמכות האכיפה הפלילית באינטרנט היא גזרה קשה עבור המדינות. עקב כך הסכימו חלק מהמדינות על פריצת גרדי התפישה הטריטוריאלית הנוקשה, וחלק מהמדינות אף ביצעו מהלכים אוניטריאליים לפריצתה. המהלכים ההסכמיים אינם מעוררים שאלות של פגיעה בריבונותן של מדינות אחרות, אולם המהלכים האוניטריאליים בהחלט מסכנים את המדינות הנוקטות אותן, שכן הן תיחשבנה כמי שמפרות ריבונות של מדינות אחרות, כל עוד הן מבצעות בפועל פעולות לאיסוף ראיות האגורות בטריטוריה של מדינות אחרות. להלן אסקור את המהלכים ההסכמיים והעצמיים של המדינות לפריצת גרדי החומה הטריטוריאלית בנוגע לאיסוף ראיות במסגרת חקירה פלילית באינטרנט. אלה גם אלה מעידים על

---

דיני המסחר האלקטרוני. גם היא התייחסה אל אנלוגיות אלה כעניין בר שינוי, ולא כעניין נתון. דן האנטר (Hunter) טען כי תפישת האינטרנט כ"מקום" מובילה לתפישה של המידע כ"מקום" ב"בעלות" מחזיק המידע, ועקב תפישה זו תיווצר מגמה של סגירת האינטרנט, מניעת זרימה חופשית של מידע, ובעצם תתרחש "טרגדיית המאגר המפוצל" (Anticommons tragedy). ראו: Hunter, לעיל ה"ש 45. טרגדיית ה-Anticommons הפוכה ל-Tragedy of the Commons המוכרת של גרט הארדין (Hardin). הארדין דיבר על תופעה של ניצול יתר של כר מרעה משותף, באופן שיביא לחיסולו, ובכך נמצאנו למדים שזיקת הנאה משותפת יכולה ליצור תמריץ אישי לניצול יתר לצורכי הפרט מבלי להתחשב כלל בצורך הכללי לשמור על הטובין הקולקטיביים. תופעת ה-Anticommons הוצגה על ידי מייקל הלר (Heller) וממנה עולה כי כאשר לכל אחד יש זכות למנוע מאחרים שימוש בטובין, הרי שכל אחד ייטה להשתמש בזכותו זו, באופן שיביא למצב של סטגנציה ואי-שימוש בטובין על ידי אף אחד מהפרטים. ראו: Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998).

הצורך המעשי בפריצת האיסור הנוקשה המגולם בתפישה הטריטוריאלית בנוגע לאיסוף ראיות דיגיטליות בחקירות פליליות באינטרנט.

### 1. הסכמה בין-לאומית על חדירות אקסטרה טריטוריאליות לחומרים באינטרנט

האמנה האירופית למניעת פשעי מחשב – המסמך המשפטי הבין-לאומי המרכזי בנוגע לאכיפה פלילית באינטרנט – כוללת הוראה בסעיף 32 המתייחסת לחריגות אקסטרה טריטוריאליות מוסכמות. על פי סעיף זה, מוכרת הסמכות לבצע חדירה לחומר מחשב מחוץ לתחום השיפוט בשני המצבים הבאים: הראשון, כאשר המחזיק בחומר המחשב מביע את הסכמתו (כדין ומרצון – "Lawfully and Voluntary") לכך;<sup>48</sup> השני, 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, ואינו מחייב מבחינת המשפט הבין-לאומי כמו אמנה.<sup>49</sup>

במבט ראשון ההסכמות האמורות מתנות על המגבלה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט, אולם במבט נוסף ניתן בהחלט לטעון כי ההתניה האמורה דווקא משעתקת את התפישה הטריטוריאלית: **ראשית**, היא מכירה בכך שהאינטרנט פרוש טריטוריאלית בהתאם למיקומו של השרת שבו אגורה הראיה הדיגיטלית המבוקשת. **שנית**, היא מכירה בכך שבנוגע לכל המדינות שאינן צד לאמנה האירופית או להסכמות ה-G8, לא ניתן לחדור לחומרי מחשב האגורים בשרתים בשטחן. **שלישית**, היא מכירה בכך שבכל שאר המצבים לא תותר חריגה אקסטרה טריטוריאלית. דווקא אותם מצבים הם 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" שאישר). סיטואציה חקירתית שכיחה נוספת היא כאשר מתבקש מראש חיפוש ברשת בין מחשבים, ולא במחשב בודד (Network search), ואחד המחשבים ברשת, שאליו יש לחשוד 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

48 ראו: 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.

49 ראו: G8 Justice and Interior Ministerial, Principles on Transborder Access to Stored Computer Data (Oct., 1999): [www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data\\_en.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf)

המחשב המקורי ברשת (בלי שהרשות החוקרת ידעה על כך מראש). לאור כל זאת, ניתן לראות באמנה או בהסכמות של מדינות ה-G8 ניסיונות שכשלו, כמעט באופן מלא, לפרוץ את המסגרת של התפישה הטריטוריאלית בנוגע לאיסוף ראיות במסגרת חקירה פלילית באינטרנט.<sup>50</sup>

פרט לניסיונות שמנתי לעיל, אזכיר עוד את ניסיונה הטרי יחסית של קבוצת מומחים של האו"ם לגיבוש הסכמות סביב אכיפה פלילית ברשת האינטרנט.<sup>51</sup> אחת ממטרותיה של קבוצת המומחים היא לבחון במשותף מה נחשב לעניין בין-מדינתי בכל הנוגע לאיסוף ראיות באינטרנט. תוצאת הפעולה המשותפת של המדינות יכולה להיות השגת הסכמה על פעולות מסוימות בין-מדינתיות שלא תיחשבנה אסורות, בין אם כיוון שלא תיחשבנה אקסטרה טריטוריאליות, ובין אם כיוון שיוסכם במשותף על כך שהן מותרות חרף משמעותן האקסטרה טריטוריאלית. במושגי המשפט הבין-לאומי, ניסיונה של קבוצת המומחים הוא לבחון ויתור מראש ובהסכמה הדדית על פן מסוים של סמכותן בטריטוריה שלהן, כפי שמיושמת הסמכות כיום. הקושי המרכזי בניסיון להגיע להסכמה מעין זו נעוץ בכך שיש צורך להשיג הסכמה כלל-מדינתית. היעדר הסכמה מוחלטת של כל המדינות לוותר על סמכותן בהקשר הנדון, משמעו יצירת סחרור שלילי, שלפיו המדינות שלא תסכמנה לוותר זה תהפוכנה למדינות מקלט, ועבריינים יעתיקו את פעילותם למדינות הסודרות הללו, ובכך יקשו על חקירת פעולתם העבריינית.<sup>52</sup>

<sup>50</sup> לעמדה מעין זו ראו: Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 433, 443-444 (2003). כפי שצינו מנסחי האמנה האירופית למניעת פשעי מחשב בדברי ההסבר שלהם לסעיף 32: "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" Convention available at: [conventions.coe.int/Treaty/EN/Reports/Html/185.htm](http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm). ראו: *Convention on Cybercrime*, Art. 32.

<sup>51</sup> ראו בפרט את: UNODC, Draft Collection of Topics for Consideration Within a Comprehensive Study on Impact and Response to Cybercrime, para. 31, 33(a) (Draft, [www.unodc.org/documents/treaties/organized\\_crime/EGM\\_21.1.2011](http://www.unodc.org/documents/treaties/organized_crime/EGM_21.1.2011)) available at: [www.unodc.org/documents/treaties/organized\\_crime/EGM\\_21.1.2011/Working\\_Papers/UNODCCPCJ\\_EG4\\_2011\\_2\\_rev1\\_-\\_amended\\_-\\_final.pdf](http://www.unodc.org/documents/treaties/organized_crime/EGM_21.1.2011/Working_Papers/UNODCCPCJ_EG4_2011_2_rev1_-_amended_-_final.pdf).

<sup>52</sup> לביקורת ברוח זו, המביעה ספקנות בנוגע ליכולת להגיע להסכמה גלובלית על אכיפה פלילית באינטרנט, ראו: Jack Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. OF CHI. LEG. FORUM 103, 107 (2001).

## 2. דין מדינת המתיר חדירה אקסטרה טריטוריאלית במצבים מסוימים באינטרנט

לא אתיימר להקיף כאן את מערך הדינים של כל המדינות. אציג להלן כמה קטגוריות של מקרים שבהם הוכרה האפשרות לבצע פעולות איסוף בעלות מובן אקסטרה טריטוריאלי, על פי התפישה הטריטוריאלית בנוגע לאינטרנט.<sup>53</sup> בכל קטגוריה כזאת אציג כדוגמה שיטת משפט, אחת או יותר, שאימצה את ההיתר האקסטרה טריטוריאלי. אל מול הדוגמות שיובאו להלן, אציין כבר עתה כי במשפט הישראלי הנוהג, אין כל היתר מוכר לפעולות חקירה אקסטרה טריטוריאליות בנוגע לחומרי מחשב באינטרנט. בהמשך אדון בהצעת חקיקה העוסקת לראשונה באפשרות להכיר בחדירה אקסטרה טריטוריאלית לחומר מחשב.<sup>54</sup>

### (א) גישה לחומר מחשב הנגיש לכלל הציבור

כל אחת מהמדינות שהן צד לאמנה האירופית למניעת פשעי מחשב או חברה ב-G8, מכירה באפשרות לגשת לחומר מחשב הנגיש לכלל הציבור באינטרנט, אף אם הוא אגור בשרתים בחו"ל. מדובר באיסוף חומר מחשב האגור מחוץ לטריטוריה המדינית, ובמובן זה מדובר בחריגה מהתפישה הטריטוריאלית. עם זאת, כיוון שמדובר בחומרים הפתוחים כלפי כולי עלמא, ניתן לטעון כי אין באיסופם משום הפעלת סמכות אמיתית, כיוון שאין בה משום פעולה כופה. על מנת להמחיש את הטענה אביא את הדוגמה הבאה: 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 על ידי העתקתו מאתר האינטרנט. על פי העמדה שהצגתי לעיל, לא תידרש הסמכה מפורשת ולא תוטל מגבלה משפטית על סמכותה של המדינה החוקרת להעתיק את המידע מאתר האינטרנט, אף אם הוא שוכן בחו"ל.

<sup>53</sup> איני מתייחס כאן להפעלת סמכויות ביטחון, אלא להפעלת סמכויות איסוף בלבד. סמכויות הביטחון יכולות להיות אקסטרה טריטוריאליות. כך, למשל, החקיקה האמריקנית העניקה במפורש סמכויות ביטחון אקסטרה טריטוריאליות. עוד אציין שעל פי הפסיקה, ראיות שהושגו באמצעות חוק ה-FISA האמריקני עשויות להיות קבילות בהליך פלילי "רגיל", אם המטרה המקורית לאיסוף הייתה ביטחונית על פי התכליות המוכרות בחוק. ראו, למשל, U.S. v. Pelton, 835 F.2d 1067 (4<sup>th</sup> Cir. 1987); U.S. v. Ning Wen, 477 F.3d 896, 898–899 (7<sup>th</sup> Cir. 2007).

<sup>54</sup> ראו להלן בפרק ג(3).

## (ב) גישה לחומר מחשב האגור בשרתים בחו"ל בהסכמה כדן של המחזיק בו

גם כאן, כל אחת מהמדינות שהן צד לאמנה האירופית למניעת פשעי מחשב או חברה ב-G8, מכירה באפשרות לגשת לחומר מחשב אשר הובעה לגבי הסכמה של בעל גישה והרשאה כדן כי הרשות החוקרת תחדור אליו.<sup>55</sup> שאלת הגישה וההרשאה כדן היא שאלה מורכבת למדי. כך, לדוגמה, לא ברור מאליו מעמדו של טכנאי מחשבים המחזיק ברשותו מחשב של לקוחו לצורך תיקון; מעמדו של מנהל רשת בנוגע למשתמשי הרשת; מעמדו של הורה בנוגע לילדו הקטין; מעמדו של שני משתמשים באותו מחשב זה כלפי זה, כאשר כל משתמש עובד על המחשב תחת פרופיל משתמש אחר; מעמדו של ספק שירות בנוגע למשתמש בשירות; מעמדו של מעביד בנוגע לעובדיו, וכיוצא בזה.<sup>56</sup>

<sup>55</sup> 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 מחייבת הסכמה של כולם. זאת, על בסיס הפסיקה המוחלת על דיני החיפוש בחצרים, ראו: Georgia v. Scott Fitz Randolph, 547 U.S. 103 (2006). כן ראו (בהתייחס במישרין להדירה לחומר מחשב): People of the State of Michigan v. Michael Aaron Dagwan, 711 N.W. 2d 386 (Mich. App. 2005). עם זאת, ראו את: U.S. v. Roy J. Hudspeth, 459 F. 3d 922 (8<sup>th</sup> Cir. 2006), שם נפסק כי ברגע שמחזיק אחד במקום סירב לביצוע החיפוש ותפיסת מחשבו, לא ניתן לפנות למחזיק אחר במשותף עימו ולקבל את הסכמתו.

<sup>56</sup> בארצות-הברית נקבע בחקיקה כי ספקי שירות שונים באינטרנט אינם רשאים למסור בהסכמה מידע על אודות לקוחותיהם לרשות החוקרת. ראו: 18 U.S.C. § 2510 (2002). כן נדונה השאלה אם טכנאי מחשבים שקיבל את המחשב לבדיקה רשאי למסור הסכמה לביצוע החדירה. ראו: U.S. v. Anderson, 2007 WL 1121319 (N.D. Ind. 2007), שם השיבו על השאלה בחיוב; מנגד ראו: U.S. v. Michael J. Barth, 26 F. Supp. 2d 929 (W.D. Tex. 1998), שם השיבו על השאלה בשלילה. כן נידונה השאלה אם הסכמה של משתמש אחד במחשב יכולה לחול על חדירה לקבצים מוצפנים או מוגני סיסמה של מחזיק אחר באותו מחשב. לעמדה המשיבה על השאלה בשלילה, ראו: Notra Trulock et al v. Freeh et al, 275 F. 3d 391 (4th Cir. 2001). לעמדה המשיבה על השאלה בחיוב, ראו: U.S. v. Andrus, 483 F. 3d 711 (10<sup>th</sup> Cir., 2007); People of the State of Michigan v. Brown, 755 N.W.2d 664 (116 Mich. App. 2008). בנוסף, התעוררה השאלה אם הורים יכולים למסור הסכמה להדירה למחשבים של ילדיהם. בפרשת Andrus, שם, נקבע כי להוריו של בגיר (בן 51), אשר התגורר בבית הוריו ולא שילם שכירות, ישנה הרשאה למסור הסכמה להדירה למחשבו, כאשר להורים הייתה גישה לחדרו וכאשר הם שילמו את חשבון האינטרנט בבית. אשר לשאלה אם מעביד רשאי להסכים להדירה הרשויות לחומרי מחשב של עובדיו, ראו למשל את: United States v. Ziegler, 474 F.3d (9<sup>th</sup> Cir. 2007), 1184, 1191, שם נפסק שמעביד יכול להסכים להדירה למחשב של עובד שלו, שהמעביד סיפק לו. 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.

בהקשר של שאלת טיב ההסכמה לחדירה אקסטרה טריטוריאליה לחומרים האגורים בחו"ל, מן הראוי לדון בקטגוריה מיוחדת של מצבים, שבהם מופעל סוכן וירטואלי ברשת, היוצר קשר עם חשוד ומקבל ממנו הסכמה תחת מצג שווא של התקשרות תמימה. למשל, נניח כי חשוד נחקר בגין ביצוע עברות מין, הטרדה מינית ופרסומי תועבה באמצעות האינטרנט. עוד נניח כי החשוד יוצר קשר עם קרבתו באתרים חברתיים כגון "פייסבוק" (ששרתיו מחוץ לישראל) ו"מקושרים" (ששרתיו בישראל). המשטרה מבקשת לטמון פח לחשוד. היא מטילה על שוטרת לפתוח כרטיס ולעדכן פרטים ותמונות ב"פייסבוק" וב"מקושרים", וליצור קשר עם החשוד, על ידי כך שתציע לו "חברות". עוד נניח שחשוד אינו חושף את כל פרטי ה"פרופיל" שלו, כולל תמונות, סרטונים, פרטי מידע אישיים שכתב על עצמו וכן "קיר" עם פוסטים שלו ושל חבריו, לכל משתמשי האתר, ורק מי שאישר כ"חבר" רשאי לראותם. סוכנת המשטרה הופכת ל"חברה" של החשוד, ויוצרת מצג שווא כלפיו. בזכות מצג שווא זה היא מקבלת את האפשרות לגשת ולעיין בחומרי המחשב שלו ולעקוב אחר פרסומיו הפתוחים רק לקהל חבריו. היא מקבלת גם את האפשרות לתקשר עמו בעצמה באותם אתרים חברתיים. מה דינה של הפעולה האמורה? האם דינה משתנה בין "פייסבוק" האמריקני לבין "מקושרים" הישראלי?

נראה לי, כי בדוגמה זו השאלה המכבידה היא שאלת טיב ההסכמה, ולא שאלת מיקומו של חומר המחשב הנצפה על ידי הסוכנת המשטרתית. אם יתגברו רשויות האכיפה על המשוכה המשפטית של בחינת כשרות ההסכמה במקרה כזה, תשווה השאלה, מבחינה אנליטית, לשאלת הסמכות לגשת לחומר מחשב בחו"ל בהסכמה של המחזיק בחומר, בה דנתי לעיל. במילים אחרות, שאלת כשרות ההסכמה בדוגמת סוכנת המשטרה אינה משתנה בין "פייסבוק" האמריקנית לבין "מקושרים" הישראלית. מכאן שלכאורה המשך הדיון בסוגיית סוכנת המשטרה אינו נוגע עוד במישורין לענייני במאמר. בסיכומי של דבר, סוגיית ההפעלה של סוכנים ועוקבים וירטואליים באתרי אינטרנט ה"יושבים" בחו"ל דומה למעשה לסוגיית הגישה בהסכמה לחומר מחשב האגור בחו"ל, בכל הנוגע לשאלת האקסטרה טריטוריאליה, והשוני המרכזי הוא אך ורק בנוגע לחקר טיב ההסכמה.

#### (ג) 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 לחזור לרשת מחשבים, ובמקרה כזה, ניתן להעתיק מידע הדרוש לחקירה שלא נמצא על המחשב המקורי שאליו כוון הצו השיפוטי מלכתחילה. החוק בבלגיה מכיר בסמכות "לתפוס" את המידע הממוחשב, כלומר למחקו מרשות מחזיקו (deleting) או לחסום את הגישה אליו על ידי מחזיקו (Blocking) וליטול את העתקו לרשות היחידה החוקרת. לחלופין, הרשות החוקרת

יכולה 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 למחוק, ויש לדווח מיד למשרד המשפטים הבלגי, אשר מחויב ליידע לאלתר את הרשויות במדינה הזרה על דבר ההעתקה כאמור.<sup>57</sup>

באסטוניה החקיקה דומה לזו שבבלגיה, והיא מתירה, במסגרת חיפוש ברשת מחשבים, העתקה של חומר מחשב האגור בשרתים מחוץ למדינה. לאחר ביצוע ההעתקה יש חובת יידוע של המדינה הזרה בדבר ביצוע פעולה זו.<sup>58</sup> גם בהונגריה החקיקה מתירה העתקה של מידע האגור בחו"ל במסגרת פעולת איסוף ראיות ברשת מחשבים.<sup>59</sup> מעניין לציין ששלוש המדינות – בלגיה, אסטוניה והונגריה – חתומות על האמנה האירופית למניעת פשעי מחשב, ושתיים מהן – אסטוניה והונגריה – אף אשררו אותה. מדינות אלה קבעו בסטנדרט החוקי הפנימי שלהן היתר לחריגה אקסטרה טריטוריאלית רחבה יותר מהמותר על פי האמנה. הדבר אפשרי כמובן מבחינת מערכת הדינים הפנימית של אותן מדינות, שכן האמנה קובעת רף מינימלי להסכמה בין-מדינית, ולא רף מקסימלי מותר. ברם, נראה לי כי מבחינת מערך הדינים של שאר המדינות, פעולה אקסטרה טריטוריאלית שכזו עלולה להיחשב פגיעה בריבונותן, בהנחה שאותן מדינות מחזיקות אף הן בתפישה טריטוריאלית בנוגע לסמכות האכיפה הפלילית ובהנחה שאיסוף הראיות הממוחשבות האגורות בשטחן לא נעשה בטעות, אלא בידיעה מראש שמדובר במידע האגור בשטחן. גם 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.

#### ד) צווים פרסונאליים אקסטרה טריטוריאליים בנוגע לאיסוף ראיות באינטרנט

אחד הקריטריונים לסיווג פעולות איסוף הוא לפי המבחן של הגורם המבצע בפועל

<sup>57</sup> ראו: Code d'Instruction Criminelle, 1808, Art. 88 § 3 (Bel.). הוראות הקוד הבלגי תורגמו והוזהרו עבורי על ידי מפקד יחידת עברות המחשב של משטרת בלגיה (Federal Computer Crime Unit – FCCU) (ראיון עם לוק ביירנס (Beirens), מפקד יחידת עברות המחשב של משטרת בלגיה (19.1.2011)). 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: [www.rand.org/content/dam/rand/pubs/technical\\_reports/2006/RAND\\_TR337.pdf](http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR337.pdf) (להלן: "EU Update"). ראו גם: SMITH, לעיל ה"ש 42, בעמ' 285.

<sup>58</sup> ראו: EU Update, לעיל, בעמ' 88.

<sup>59</sup> שם, בעמ' 133–134.

את הפעולה: ישנן פעולות המבוצעות על ידי הרשות החוקרת עצמה וישנן פעולות המבוצעות על ידי 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 האינטרנטי (בשונה, למשל, מצו חדירה לחומר מחשב, המופנה למחשב מסוים או למידע מסוים המאוחסן בו). כיוון שכך, ניתן – גם לפי תפישה הטריטוריאלית – לפתח גישה, שלפיה כל עוד האדם שאליו מופנה צו ההמצאה נמצא בישראל, הרי כלפיו 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, אם הוא בעל גישה חוקית, אינו פגיעה בריבונותה של המדינה הזרה שבה אגור פיזית חומר המחשב. מנגד, ניתן לטעון שכיוון שהנמען לצו ההמצאה פועל בכפייה, לנוכח הוצאת צו ההמצאה המלווה בסנקציה המשפטית של ביזיון בית המשפט במקרה של אי-ציות לצו, הרי שהנמען לצו מגויס לשמש כזרועה 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. הסמכות קבועה בסעיף 43 לפסד"פ. הסעיף לקוני למדי וזה נוסחו:

"ראה 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".

החוק הישראלי אינו מציין במפורש כי הסמכות להוצאת צווי המצאה היא אקסטרטריטוריאלית, אולם הסיווג של צווים אלה כצווים אישיים אפשר הרחבת תחולה בנקודה זו בפסיקת בית המשפט העליון בעניינו של גלעד שרון.<sup>60</sup> סעד נוסף, של

<sup>60</sup> כה נפסק מפי המשנה לנשיא אור בע"פ 1761/04 שרון נ' מדינת ישראל, פ"ד נח(4) 9, 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, בספרייה 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 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

ביצוע בעין, שלפיו המשטרה תתפוס את חומרי המחשב שמחוץ לתחום השיפוט, במקום הנמצא לצו, אינו מוכר במשפט הישראלי. וכך, בפרשת גלעד שרון אמנם הוצא צו המצאה לגבי חומרים המצויים מחוץ לתחום השיפוט, אולם הסנקציה על אי-ביצוע הצו הייתה יכולה להיות במישור של פקודת ביזיון בית המשפט ולא במישור של ביצוע פעולת האיסוף על ידי הרשות החוקרת במקום שרון, שאליו הופנה הצו. במשפט האמריקני יש אפשרות נוספת, במסגרת צו המצאה אישי, והיא – לכפות על שלוחה מקומית של חברה זרה לספק נתונים האגורים ברשות החברה הזרה מחוץ לשטחי ארצות-הברית.<sup>61</sup> בית המשפט העליון האמריקני אף הכיר באפשרות לכפות על מתדיין זר בערכאה אמריקנית להמציא נתונים המצויים בבנק מחוץ לארצות-הברית, וכי חובתו של המתדיין הזר במקרה כזה לנסות כמיטב יכולתו להמציא את הנתונים המבוקשים.<sup>62</sup> פסיקה דומה מצויה גם בקנדה.<sup>63</sup>

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 שבכוחו למסרם או להציגם". אציין עוד כי גם בתחום סדרי הדין האזרחיים הוכרה אפשרות להוצאת צווים אישיים בעלי תחולה אקסטרה טריטוריאלית. ראו תק' 383 לתקנות סדר הדין האזרחי, התשמ"ד-1984 שקבעה את הסמכות להוציא צו Mareva לאדם להימנע מלעשות דיס-פוזיציות בנכסים שברשותו. ברע"א 4556/03 בנק סטנדרט צ'רטר – תאגיד חוץ נ' קטב, פ"ד נז(6), 1, 7-6 (2003) 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: הפ"ב (מחוזי ת"א) 10-23485-02 ממיסטבלוב נ' Tchaturia, תק-מח 10(1) 11157 (2010). דוגמה נוספת מומחשת בפרשת רייפמן. באותו מקרה, ננקטו הליכי פשיטת רגל נגד רייפמן, והמנהל המיוחד שמונה לפי פקודת פשיטת הרגל הורה לו מכוח ס' 56(ב) לפקודה למסור את אחזקותיו במניות חברת אמבלייז אשר נסחרו בבורסה בלונדון. ראו: ס' 56(ב) לפקודת פשיטת הרגל (נוסח חדש), התש"ס-1980. כן ראו: רע"א 6067/09 רייפמן נ' CCM Master Qualified Fund LTD. (פורסם בנבו, 23.08.2009); ע"פ 7174/09 רייפמן נ' ארז, תק-על 09(3) 4320 (2009). לשורשים ישנים יותר של הסמכות להורות לתושבים ישראלים למסור מניות המוחזקות על ידם בבנקים בחו"ל ראו: פרשת אמסטרום, לעיל ה"ש 9.

ראו: Todd Jones, *Compulsion Over Comity: The United States' Assault on Foreign Bank Secrecy*, 12 N.W. J. INT'L L. & BUS. 454 (1992), שם סוקר המחבר את התפתחות הפסיקה האמריקנית, 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 עוד: Gary E. Davidson, *Congressional Extraterritorial Investigative Powers: Real or Illusory?*, 8 EMORY INT'L L. REV. 99, 106-120 (1994).

ראו: Societe Internationale pour Participations Industrielles et Commerciales v. Rogers, 357 U.S. 197 (78 S.Ct., 1958). אותו מקרה עסק בתביעה של חברה שוויצרית נגד ממשלת ארצות-הברית בפני ערכאה אמריקנית. ממשלת ארצות-הברית עתרה בפני בית

### 3. התפישה הטריטוריאלית ותזכיר הצעת חוק החיפוש

בשנת 2010 פורסם תזכיר הצעת חוק החיפוש.<sup>64</sup> התזכיר נועד להסדיר באופן מפורט את דיני החיפוש, התפיסה, הכניסה וההמצאה, הן במרחב הפיזי והן במרחב הממוחשב. כפי שאראה להלן, בתזכיר מוזכרת לראשונה בדין הישראלי, גם אם באופן חלקי ביותר, סוגיית הטריטוריאליות בדיני החקירה באינטרנט. בתזכיר אין הוראה מפורשת הקובעת את מגבלת הטריטוריאליות. כיוון שכך, חל, כנקודת מוצא, הדין הכללי בנושא זה, אשר מניח הנחת טריטוריאליות, בהתאם למקובל גם במשפטן של מדינות נוספות ובמשפט הבינ-לאומי. פרט לכך, ברמה הקונקרטית של הוראות החוק עצמו, לשונו של תזכיר חוק החיפוש משופעת במילים המבטאות תפישה טריטוריאלית בנוגע לראיות הדיגיטליות. התזכיר מציין, בכמה הזדמנויות, את ה"מקום" שבו מצוי חומר המחשב, ומכאן ניתן ללמוד שהתזכיר מניח כי הראיה הדיגיטלית ניתנת למיקום, ואף כי המקום הוא השרת שבו מצוי חומר המחשב.<sup>65</sup>

התזכיר מונה ארבעה חריגים שבהם מוכרת אקסטרה טריטוריאליות בפעולת הרשות החוקרת. הראשון, צו המצאה בעל נפקות אקסטרה טריטוריאלית. סעיף 68(א) לתזכיר קובע כי "בית המשפט רשאי לצוות על מחזיק בחומר מחשב הקשור

המשפט להורות לתובעת להמציא נתונים בנקאיים שוויצרים. 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 האמריקני, כי מאחר שהתובעת השווייצרית לא המציאה את הנתונים שנצטוותה להמציא, התביעה האזרחית שהגישה תימחק. בבית המשפט העליון הפכו את התוצאה האופרטיבית של הערכאה הדיונית, אם כי קבעו את העיקרון של חובת מילוי הוראת ההמצאה 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 טריטוריאלית של בית המשפט האמריקני.

63 ראו: eBay Canada Ltd. v. M.N.R., [2010] 1 F.C.R. 145 (Ca.).

64 נכון למועד כתיבת שורות אלה, טרם פורסמה הצעת החוק הממשלתית בחוברת הצעות החוק, ומתקיימים דיונים במשרד המשפטים בנוגע להערות השונות שהתקבלו לתזכיר.

65 המקום הבולט ביותר הוא בסעיף 64, סעיף ההגדרות לפרק ז' של תזכיר חוק החיפוש, הן בפעולות בחומר מחשב. בסעיף זה מוגדר "מחזיק בחומר מחשב" כדלקמן:

"(1) מחזיק במקום בו מצוי חומר המחשב;

(2) מי שהוא בעל הרשאה או גישה לחומר המחשב, בכל מקום בו מצוי חומר המחשב – בין בארץ ובין בחו"ל, והכל לרבות ספק שירות" (הדגשות שלי – ח.ו.).

עינינו הוראות כי המחזיק בחומר המחשב יכול להיות מי שמחזיק במקום הפיזי שבו אגור חומר המחשב, פרט לבעלי הרשאה או הגישה לחומר. הוראה זו בהחלט מדגישה את ההתייחסות הפיזית, ואף הטריטוריאליסטית, אל חומר המחשב.

לעברה, להמציא את חומר המחשב כאמור במועד, במקום ובתנאים שיקבע". סעיף זה שותק לעניין תחולתו האקסטרה טריטוריאלית, אלא שהגדרת "מחזיק בחומר מחשב", בסעיף 64 לתזכיר חוק החיפוש קובעת כי "מחזיק בחומר מחשב" יכול להיות "מי שהוא בעל הרשאה או גישה לחומר המחשב, בכל מקום בו מצוי חומר המחשב – בין בארץ ובין בחו"ל, והכל לרבות ספק שירות" (הדגשות שלי – ח.ו.). קריאת שני הסעיפים יחדיו מלמדת כי ניתן למסור צו המצאה למחזיק בחומר מחשב, שיחייבו למסור חומר מחשב האגור בחו"ל, אם יש לו הרשאה או גישה לאותו חומר מחשב. המונחים "הרשאה" ו"גישה", וקביעת היחס החלופי ביניהם, מרחיבים באופן משמעותי את מעגל הגורמים שיכולים להידרש, בצו המצאה, למסור חומר מצוי האגור בטריטוריה מחוץ לישראל. בפרשת גלעד שרון דיבר בית המשפט העליון במושגים של נגישות, זמינות המידע ושליטה עליו ללא החזקה פיזית של המחשב שבו מצוי המידע. הדוגמה שהביא בית המשפט העליון נגעה לשירותי בנקאות באמצעות האינטרנט ולשירותי דואר אלקטרוני על ידי ספק שירות המצוי בחו"ל. בשתי דוגמות אלה, כיוון בית המשפט העליון את דבריו ללקוחות המנויים על שירותים אלה, ולא אל ספקי השירות עצמם. תזכיר חוק החיפוש צועד צעד נוסף במשעול זה וקובע כי גם ספק שירות, גם מנהל רשת כגון אדמיניסטרטור וגם מעביד המחזיק בשליטה על חומרי המחשב של עובדיו – כל אלה יכולים להידרש להמציא חומרים של אחר, האגורים בחו"ל, ובלבד שהחומרים האלה בני הרשאה או גישה מבחינתם. יתרה מזאת, ההמצאה על ידי אותם צדדים שלישיים יכול שתיעשה בלא ידיעת החשוד (שהוא, אינטואיטיבית, מי שנכנה "בעל החומרים").<sup>66</sup>

**השני**, צו שמירת מידע (Preservation)<sup>67</sup> אקסטרה טריטוריאלית. בדומה להוראות בנוגע לצווי המצאה, קובע תזכיר חוק החיפוש שגם צווי שמירה יכולים להימסר לגורם בישראל ולחול גם על חומרי מחשב של אותו גורם האגורים בחו"ל, ובלבד שלנמען לצו הייתה הרשאה או גישה אל החומרים האלה.<sup>68</sup>

<sup>66</sup> ס' 9(ב) לתזכיר חוק החיפוש קובע, בנוגע לצווי המצאה של מוצגים חפציים, כלל שלפיו הנמען לצו ההמצאה לא יגלה את תוכנו של הצו או את דבר ביצועו. החריג, כך על פי הסעיף, הוא "אם התיר זאת בית המשפט בצו". סעיף זה מוחל, מכוח הוראת ס' 73 לתזכיר, גם על צווי המצאה של חומר מחשב. ס' 71(2) קובע: "אם צו [...] ההמצאה של חומר מחשב מתייחס לחומר מחשב האגור אצל ספק שירות, שאינו החשוד, ישקול בית המשפט בין יתר השיקולים את אפשרות יידוע החשוד בדבר ביצוע הצו". במילים אחרות, בררת המחל על פי התזכיר, הוא אי-גילוי, אם כי בית המשפט נדרש להתייחס לנושא של צו המצאה שמופנה לספק שירות בנוגע ללקוחו, ולשקול את גילוי דבר ביצוע הצו לחשוד, אשר בנוגע למידע שלו הוצא הצו.

<sup>67</sup> הכוונה בשמירת מידע (Preservation) היא לסמכות להורות למחזיק בחומר מחשב לשמור את המידע אצלו לפרק זמן הנקוב בהוראת השמירה, וזאת, על מנת למנוע את מחיקתו של המידע או את שינויו.

<sup>68</sup> ראו ס' 67(א) לתזכיר חוק החיפוש המתייחס לצו שמירה המופנה ל"מחזיק בחומר מחשב", כאשר הגדרת ה"מחזיק בחומר מחשב" לעניין זה זהה להגדרת המחזיק בנוגע להמצאת חומר

**השלישי**, חדירה בהסכמה של בעל הרשאה וגישה לחומר המחשב, בכל מקום שבו הוא אגור.<sup>69</sup> חדירה לחומר מחשב בהסכמה, ללא צו שיפוטי, כוללת הגבלות והסתיוגויות שונות בנוגע לטיב ההסכמה ומגבלותיה. כך, למשל, נדרש כי המסכים יהיה "בעל הרשאה וגישה", ולא "בעל הרשאה או גישה", כפי שנקבע לעיל בנוגע לנמענים לצווי המצאה או שמירה. ועוד, סעיף 83(ב) לתזכיר מונה שורה של מגבלות נוספות, שלפיהן: ספק שירות אינו רשאי לתת הסכמה לחדירה בלא צו לגבי חומר מחשב של לקוחו; מעביד ככלל לא יוכל לתת הסכמה לגבי חומר מחשב פרטי של עובדו, אלא אם כן הוסכם הדבר בין המעביד לעובד מראש; ההסכמה יכולה להיות מסויגת רק לחומרי מחשב מסוימים במחשב; נותן ההסכמה יכול לסגת מהסכמתו, אם לא התייחס במפורש לחומרי מחשב מסוימים. למרות הוראות מגבילות אלה, בנקודה אחת החדירה בהסכמה לחומר מחשב מרחיבה דווקא לעומת החדירה לחומר מחשב שלא בהסכמה, וזאת בכל הנוגע למקום האגירה של חומר המחשב שבו מדובר. על פי הרציונל של תזכיר חוק החיפוש, ההסכמה של המחזיק בחומר המחשב, שהוא בעל הרשאה וגישה לחומר, יכולה להתפרש אל חומרי מחשב האגורים מחוץ למדינת ישראל, ואילו צו שיפוטי לחדירה לחומר מחשב אינו יכול להתפרש אל חומרים אלה.<sup>70</sup> רציונל זה אינו ייחודי לתזכיר חוק החיפוש, וכפי שהראיתי לעיל חדירה אקסטרה טריטוריאלית לחומר מחשב בהסכמה כדין של המחזיק בו – מותרת גם על פי האמנה האירופית למניעת פשעי מחשב ובמשפטן של מדינות נוספות.

**הרביעי**, חדירה לחומר מחשב הפתוח לכלל הציבור, כדוגמת דף באתר חדשות, "קיר" ב"פייסבוק", "פוסט" בבלוג פתוח וכיוצא בזה. סעיף 76(ב) לתזכיר חוק החיפוש קובע כי "חומר מחשב הפתוח לעיון הציבור או חלק בלתי מסוים ממנו בין בתשלום ובין שלא בתשלום" – לא ייחשב כמחייב צו חדירה לצורך עיון בו על ידי הרשות החוקרת. להבדיל משלושת ההיתרים הקודמים, כאן לשון התזכיר אינה מפורשת, אבל משתמע מדברי ההסבר שבתזכיר לסעיף זה, כי הכוונה הייתה להתיר חדירה לחומר הפתוח לכלל הציבור, גם כאשר החומר אגור על מחשבים בחו"ל, וזאת, לנוכח ההפניה בדברי ההסבר לסעיף 32 לאמנה האירופית למניעת פשעי מחשב, המתיר חריגה אקסטרה טריטוריאלית במקרה של חומר הפתוח לעיון הציבור ולשימוש.

מחשב. אציין עוד כי בדומה לצווי המצאה, גם בנוגע לצווי שמירה, נדרש ככלל הנמען לצו, לרבות ספק שירות, לשמור על סודיות הצו. ראו ס' 71(2), עם ס' 73 וס' 9(ב) לתזכיר.

69

ראו ס' 83(א) לתזכיר חוק החיפוש.

70

ודוק, צו חדירה לחומר מחשב לא יכול להיות אקסטרה טריטוריאלי, ואילו צו המצאה, שבו הרשות דורשת מאדם אחר להמציא לה את המידע המבוקש (במקום שהיא תאסוף אותו בעצמה) יכול, על פי החריג הראשון שציינתי בהקשר של תזכיר חוק החיפוש, לחול גם באורח אקסטרה טריטוריאלי.

## ד. פריצת גבולות התפישה הטריטוריאלית בנוגע לאינטרנט – דיון נורמטיבי

### 1. התפישה הטריטוריאלית ופגיעתה בחקירה הפלילית באינטרנט

פגיעתה של התפישה הטריטוריאלית בחקירה הפלילית באינטרנט ניתנת להמחשה באמצעות דוגמה מוכרת למדי מארצות-הברית (פרשת *Gorshkov-Ivanov*), שבה רשויות החקירה פרצו את המגבלה על מנת להמשיך ולקדם את החקירה הפלילית. עניינה של פרשה זו בהאקרים רוסים שסחטו כספים מחברות אמריקניות ואיימו עליהן, כי אם לא ישלמו להם, ישביתו את שירותיהן באמצעות מתקפות אינטרנטיות מתוזמנות. לצורך חקירת הפרשה נזקקו חוקרי ה-FBI לחומרי מחשב שנאגרו בשרתי מחשב רוסיים. חוקרי ה-FBI העתיקו באופן סמוי את חומר המחשב הרלוונטי בדרך של התקשרות ממחשב בארצות-הברית לשרת הרוסי. לאחר מכן ניגשו חוקרי ה-FBI לבית משפט אמריקני וביקשו צו לעיון בחומר שהועתק כאמור. בית המשפט האמריקני התיר לחוקרים לעיין בחומרים. ההאקרים הרוסים פתו לצאת מרוסיה לארצות-הברית באמתלת שווא של כנס בתחום המחשבים, ונעצרו על ידי חוקרי ה-FBI. כך התאפשר לחוקרים האמריקנים להתגבר על שתי בעיות שעמדו בדרכן: הראשונה, בעיית איסוף הראיות האגורות מחוץ לטריטוריה האמריקנית. השנייה, בעיית תפיסתם בפועל של החשודים והבאתם לדיון. בבעיה השנייה, של העמדה לדיון של נאשמים שמקום מושבם בחו"ל, איני דן במסגרת מחקר זה. בעיה זו מוסדרת באמצעות דיני ההסגרה, ומדינות שונות, כבמקרה זה, משתמשות בכלים לפיתוי נאשמים לעבור ממדינה למדינה על מנת ללכוד אותם ברשתה. הבעיה הראשונה היא במוקד פרק זה של המחקר. בפרשת *Gorshkov-Ivanov* הראיה נאספה על ידי חוקרים אמריקנים משרת רוסי, שופט אמריקני הכשיר את העיון בראיה בשלב החקירה, ולאחר מכן שופט אמריקני הכשיר את השימוש בראיה ודחה את טענות ההגנה לפסלותה. לעומת זאת, השלטונות ברוסיה ראו בפעולה האמריקנית משום פגיעה בריבונות הרוסית והוציאו צווי מעצר נגד חוקרי ה-FBI.<sup>71</sup> יצוין כי פעולתן של

<sup>71</sup> ראו: U.S. v. Ivanov, 175 F. Supp. ;U.S. v. Gorshkov, 2001 WL 1024026 (W.D. Wash.) 2d 367 (D. Connecticut 2001). מעניין לציין כי כאשר מדובר בחקירה המתנהלת במדינה אחת בארצות-הברית, ונדרשת חידה לחומר מחשב האגור בשרת במדינה אחרת בארצות-הברית, הרי העמדה היא שעל החוקר לבקש את צו החידה במדינה האחרת ולא במדינתו שלו. ראו, לעניין זה, את מדריך השטח של משרד המשפטים: DEPARTMENT OF JUSTICE, FIELD GUIDE ON THE NEW AUTHORITIES (REDACTED) ENACTED IN THE 2001 ANTI-TERRORISM LEGISLATION § 216A (2002), available at: [www.epic.org/privacy/terrorism/DOJ\\_guidance.pdf](http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf). כן ראו: Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J. L. & TECH. 257, 264 (2002).

הרשויות האמריקניות בפרשת *Gorshkov-Ivanov* הייתה חריגה, ובמקרים אחרים של עברייני אינטרנט שפעלו מחו"ל כלפי תושבים ועסקים אמריקניים, הן פעלו על פי מגבלת סמכות האכיפה הטריטוריאלית, והסתייעו במנגנוני עזרה משפטית בין מדינות.<sup>72</sup>

דוגמה זו מלמדת על **הקושי המעשי** של רשויות החקירה באיסוף ראיות האגורות מחוץ לתחום הטריטוריה המדינתית. מנגנוני העזרה המשפטית, המניחים את עקרון הטריטוריאליות ואף משעתקים אותו, אינם יכולים לספק תמיד מענה לצורכי החקירה, מבחינת קצב התפתחות החקירה והחשש מפני התנדפות הראיות. יתר על כן, לא בכל מקרה ומקרה אפשר להשיג שיתוף פעולה מן המדינה הזרה בדמות עזרה משפטית. כך הוא במקרה שאין הסכם עזרה משפטית בין שתי המדינות (המדינה החוקרת והמדינה שבה אגורה הראיה), או שעל פי דיניה של המדינה שבה אגורה הראיה המעשה אינו נחשב עברה (היעדר פליליות כפולה). אמנם מנגנוני העזרה המשפטית המהירים והמיוחדים לראיות דיגיטליות שנקבעו באמנה האירופית למניעת פשעי מחשב משפרים את האכיפה הפלילית האקסטרטריטוריאלית באופן משמעותי, אולם מנגנונים אלה פועלים אצל המדינות שהן צד לאמנה בלבד, ולגבי 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 שהפער בין הסטנדרטים הפליליים של המדינות השונות יכול להיות גדול למדי. האמנה האירופית למניעת פשעי מחשב היא אמנם הניסיון המעשי הבולט ביותר לאכיפה בין-לאומית, אולם פתרון זה, כפתרון כולל שנועד לבוא בנעלי האכיפה הפלילית המדינתית באינטרנט, אינו צלית.

<sup>72</sup> 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 למחשביהם כמה פעמים, בתמורה להפסקת הפריצות. הלה הוזמן למשרדי Bloomberg בלונדון, למטרת תשלום דמי הסחיטה, נעצר על ידי 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 Computers and Attempting Extortion* (2003), available at: [www.justice.gov/usao/nys/pressreleases/February03/zezevconvict1.pdf](http://www.justice.gov/usao/nys/pressreleases/February03/zezevconvict1.pdf) כן ראו: Michael Cooper, *Bloomberg Tells Trial Jury of his Part in Taped Sting*, N.Y. TIMES (12.2.2003), at B4. שהואשם בפריצה ובגרימת נזק ל-92 מחשבים בין השנים 2001–2002, בין היתר למחשבים של הצבא האמריקני. מקינון הסביר כי פרץ למחשבים המסווגים כדי לנסות לחשוף מידע על עב"מים שהוסתר על ידי רשויות הביטחון האמריקניות מעין הציבור. הרשויות הבריטיות עצרו את מקינון, והחל בהליך ממושך ביותר של הסגרה מבריטניה לארצות-הברית, הליך שלא הסתיים עד היום. באותו מקרה, הרשויות הבריטיות אספו 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.).

כיום מבחן מקום הימצא הראיה גוזר את שאלת סמכותה של המדינה החוקרת לאסוף את הראיה הדיגיטלית במסגרת חקירה פלילית באינטרנט. משתמשי האינטרנט, ובכלל זה חשודים בפוטנציה, יכולים למקם מידע ולבצע פעולות באינטרנט במחשבים המצויים פיזית במדינות זרות. לפיכך סוגיית היעדר סמכות האכיפה הבין-לאומית הופכת בפועל לכלל וטו, המסכל חקירות פליליות מדינתיות באינטרנט. מנקודת מבט של המדינה כלפי חוץ, משמעות הפרת כללי סמכות האכיפה היא עימות דיפלומטי עם המדינה הזרה הטוענת לפגיעה בריבונותה, ואף העמדה לדין של החוקרים מהמדינה הפוגעת. מנקודת מבט של המדינה כלפי פנים, טענת היעדר סמכות אכיפה בין-לאומית, ככל טענת היעדר סמכות עניינית, יכולה להוביל לבטלות ההליך כולו.<sup>73</sup> נוצר אפוא צורך פרקטי מוגבר לערער על כלל הווטו האמור.

המבקר החריף ביותר של כלל הווטו החקירתי הזה הוא ג'ק גולדסמית' (Goldsmith). גולדסמית' צידד בהמשך תפקודה של המדינה כגורם האוכף את הדין הפלילי באינטרנט.<sup>74</sup> לדעתו, המדינה צריכה לשמר את הלגיטימציה שלה כגורם אוכף הדין הפלילי באינטרנט. מטעמים של יעילות והיתכנות לביצוע חקירות פליליות באינטרנט, יש לטענתו להכשיר פעולות של איסוף מידע מרשתי מחשב המצויים מחוץ לתחום השיפוט.<sup>75</sup> אם תוסר מגבלת סמכות איסוף הראיות הבין-לאומית, לכאורה עלולה להתעורר במלוא חריפותה בעיה של הכפפת כל פעילות באינטרנט לדיניהן של כל המדינות. על בעיה זו הצביעו דייוויד ג'ונסון (Johnson) ודייוויד פוסט (Post) כחמש שנים קודם לכן.<sup>76</sup> כל פעילות ברשת, בפרט פעילות הכרוכה באלמנט של פרסום תוכן ברבים, כדוגמת פרסום תכנים מיניים, או פנייה להצעת שירותים לציבור, כדוגמת העלאת אתר הימורים מקוונים, היא בעלת השפעה על משתמשי אינטרנט מכל המדינות שיכולים להיחשף לאתרים אלה. עקב כך, לכאורה סמכות התחיקה של כל מדינה ומדינה יכולה להתפרש על האתרים הללו. ההחלה של סמכות התחיקה של כל המדינות על הסיטואציה, משמעה "סחרור דינים" שלילי, שלפיו המדינה השמרנית ביותר תכפה למעשה את דיניה על כלל משתמשי הרשת. כיצד

<sup>73</sup> טענת חוסר סמכות עניינית זוכה למעמד מיוחד: היא יכולה לעלות בכל שלב של הדיון המשפטי, אפילו בערעור בלבד ואפילו ביזמת בית המשפט עצמו (גם אם מדובר בשיטת משפט אדברסרית). ראו למשל: Alex Lees, *The Jurisdictional Label: Use and Misuse*, 58 STAN. L. REV. 1457, 1458-1460 (2006).

<sup>74</sup> ראו: Goldsmith "Unilateral Regulation of the Internet", לעיל ה"ש 38. כן ראו: Jack L. Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI. KENT L. REV. 1119 (1998). למען הדיוק, גולדסמית' יוצא מנקודת מוצא אקסיומטית שהמדינה צריכה לאכוף את הדין הפלילי באינטרנט, ואינו מבצע בחינה אמיתית של החלופות לשיטת האכיפה ולזהות הגורם האוכף. עם זאת, בחירתו של גולדסמית' בנקודת מוצא זו מבטאת לטעמי בחירה נורמטיבית, גם אם לא מנומקת.

<sup>75</sup> ראו: Goldsmith, לעיל ה"ש 52.

<sup>76</sup> Johnson & Post "Law & Borders", לעיל ה"ש 46, בעמ' 1374.

ניתן להתמודד עם תופעה זו? על כך השיב גולדסמית' כי תופעת סחרור הדינים השלילי תתרחש רק בנוגע לספקי שירותים באינטרנט אשר יש להם שלוחה מקומית, שנגדה ניתן להוציא לפועל את פעולת האכיפה, או בנוגע לספקי שירותים שניתן להסגיר למדינה האוכפת. הלכה למעשה, טען גולדסמית', קבוצה זו של ספקי שירותים אינה כה גדולה, ומכאן שבעיית סחרור הדינים השלילי הנובעת מהסרת מגבלת סמכות איסוף הראיות הבין-לאומית באינטרנט – אינה כה חמורה.<sup>77</sup>

לקריאה המעשית לביטול כלל הווטו במישור סמכות האכיפה הבין-לאומית קמו מתנגדים. פטרישיה בליה (Belia) טענה כי אף 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 באינטרנט, חזק ככל שיהיה, אינו יכול להגמיש כללים של המשפט הבין-לאומי המנהגי.<sup>78</sup> ניקולאי סייטץ (Seitz) הביע עמדה עקרונית המתנגדת לאפשר לרשות החוקרת לחדור לחומר מחשב האגור בשרתים מחוץ לתחום השיפוט, למעט במקרים שבהם המידע הממוחשב פתוח לעיון כלל הציבור או במקרים של הסכמה מאת המחזיק במידע.<sup>79</sup> עמדתו של סייטץ נסמכת על עיקרון של מעין הדדיות: אם כל מדינה תתיר חדירה של חוקריה לחומרי מחשב האגורים בשרתי מדינות זרות, משמע שכל מדינה תיפגע בעצמה על ידי פעולה של הרשויות החוקרות של המדינות האחרות. למעשה סייטץ מניח במידה מסוימת את המבוקש, בכך שלדירו אכן יש פגיעה יסודית בריבונותה של המדינה, ברגע שרשות חוקרת של מדינה אחרת אוספת, באמצעות התקשרות מרחוק, ראיות דיגיטליות המצויות במחשבה של אותה מדינה.

גולדסמית' לא השיב במחקריו לביקורות אלה. מענה אפשרי יכול להימצא לכאורה במישור של תורת ההפרה היעילה (Efficient breach theory), שלפיה בהינתן התפישה הטריטוריאלית, ובפרט בהינתן קיומו של כלל וטו האוסר לאסוף ראיות דיגיטליות האגורות במחשבים מחוץ לטריטוריה המדינתית, עדיין "משתלם" למדינות להפר כלל וטו זה בשיקול פשוט של עלות מול תועלת. תורת ההפרה היעילה מקובלת בקרב אסכולת הניתוח הכלכלי של המשפט, והיא פותחה לראשונה בהקשר של דיני חוזים, אולם יובאה לסוגיות נוספות, בהן סוגיות של הפעלת סמכות אכיפה, גם אם לא סמכות איסוף ראיות, מחוץ לטריטוריה המדינתית. כך נעשה למשל, בהקשרים של חטיפת חשודים הנמצאים מחוץ לטריטוריה של המדינה

<sup>77</sup> ראו: Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial* Sovereignty, 5 IND. J. GLOBAL LEGAL STUD. 475, 483–485 (1998). כן ראו: Goldsmith, "Unilateral Regulation", לעיל ה"ש 38, בעמ' 139–140.

<sup>78</sup> ראו: Bellia, לעיל ה"ש 38, בעמ' 61–65, 70–80.

<sup>79</sup> Seitz, לעיל ה"ש 42.

האוכפת והתנקשות בשודים הנמצאים מחוץ לטריטוריה.<sup>80</sup> באותו אופן ניתן להציע לנתח את סוגייתנו במשקפי תורת ההפרה היעילה: החלופות לאכיפה הפלילית המדינתית נכשלו. בפרט נכשלה החלופה של אכיפה פלילית בין-לאומית, הנשענת על שיתוף פעולה יעיל ומהיר בין המדינה החוקרת לבין מדינה זרה שבה מצויות הראיות הדיגיטליות הנדרשות לחקירה הפלילית. נוכח כישלון זה עולה משמעותית הכדאיות של הפגיעה בריבונותה של אותה מדינה זרה. ברגע שנחצית הנקודה הקריטית, של עלות מול תועלת, ובהיעדר פערי מידע, המדינה החוקרת תפעל באורח אקסטרה טריטוריאלי ותאסוף ראיות המצויות בשטח המדינה הזרה.

המענה במישור תורת ההפרה היעילה הוא חלקי במידה רבה, וזאת משני הטעמים הבאים: **האחד**, בענייננו מדובר בהחלה של התורה על סוגיות מתחום המשפט הבין-לאומי. כל חיותו של המשפט הבין-לאומי מבוססת על נכונותן של המדינות לכבד מערכת של כללים ביניהן, גם בעתות משבר וגם בהינתן קשיי אכיפה מסוימים.<sup>81</sup> על כן תורת ההפרה היעילה חותרת למעשה תחת כל גרעין קיומו של המשפט הבין-לאומי. **האחר**, תורת ההפרה היעילה מתבססת על כך שאין פערי מידע בין השחקנים, וכי הערכת הנזק היא מדויקת. בפועל, בזירה הבין-לאומית, הערכה של מדינה א' על אודות התגובה האפשרית של מדינה ב' בעקבות פעולה הפוגעת בריבונותה – נותרת הערכה בלבד. הזירה הבין-לאומית אינה ניתנת לחיזוי מדויק, ומכאן שיכולת חישוב העלויות מול התועלות מוגבלת. עוד יש להעיר, בהקשר של החלת תורת ההפרה היעילה על ענייננו, כי ניתן להעריך כי כשמדינה א' פוגעת בריבונותה של מדינה ב' פעם אחת בלבד, התגובה תהיה מתונה יחסית למקרה שבו מדינה א' תשוב ותפגע פעם אחר פעם בריבונותה של מדינה ב'. במילים אחרות, אם המשחק הוא רב-סיבובי ולא חד-סיבובי, צפוי שמחיר התגובה של מדינה ב' יגבה בסיבובים הבאים. ככל שעסקינן בעברות באינטרנט, שמטבען הן

<sup>80</sup> ראו למשל: Gregory S. McNeal & Brian J. Field, *Snatch-and-Grab Ops: Justifying Extraterritorial Abduction*, 16 Trans. L. & Contemporary Problems 491, 519–522 (2007); Andrew J. Calica, *Self-Help is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists*, 37 CORNELL INT'L L.J. 389, 414–419 (2004); Michael N. Schmitt, *State Sponsored Assassination in International and Domestic Law*, 17 YALE J. INT'L L. 609 (1992). במאמרים אלה סוקרים המחברים מקרים שבהם הפעילו מדינות כוח על טריטוריה זרה, באופן הנראה, קטגורית, כפוגעני יותר מאשר איסוף ראיות נגד חשוד. על פי הטענה, ה"מחיר" ששילמו אותן מדינות היה גיבוי במוסדות האו"ם, הצהרות דיפלומטיות שליליות מצד המדינה הנפגעת, איומים בסנקציות, אך בחישוב הכולל, "מחירו" של נזק זה לא השתווה לערך של לכידתו או חיסולו של אדם שנחשד בעברות חמורות נגד התושבים או האינטרסים של המדינה המפרה.

<sup>81</sup> לטעון זה ראו למשל: Harold Hongju Koh, *The Spirit of the Laws*, 43 HARV. INT'L L.J. 23 (2002). המאמר נכתב בהתייחס לתגובותיה האפשריות של ארצות-הברית למתקפת הטורוד של ה-11.9.2001.

חוצות גבולות טריטוריאליים, ניתן להניח שהמשחק יהיה רב-סיבובי. לסיכום, כפי שניתן לראות לעיל, הטענה הפרקטית של גולדסמית' אינה עומדת על רגליים איתנות כהצדקה נורמטיבית עצמאית לחריגה מהתפישה הטריטוריאלית, וערכה הממשי הוא בהצבעה ממוקדת על בעיית האכיפה הפלילית המדינתית באינטרנט והצבעה על הדרך אל פתרונה. עתה אעבור להציג ביקורות עיוניות על התפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט. ביקורות אלה, כפי שאטען, משמשות הצדקה לחריגה מטריטוריאליזם נוקשה בנוגע לחקירות פליליות באינטרנט.

## 2. ביקורות על התפישה הטריטוריאלית ויישומה על דיני האיסוף במסגרת חקירה פלילית באינטרנט

הביקורת הראשונה תתמקד במשמעות המיקום של המידע והיישומים בתוך האינטרנט לצורך קביעת כללי סמכות אכיפה בין-לאומית. הביקורת השנייה תתמקד בפעולות איסוף הראיות באינטרנט עצמן ועמידה על מאפייניהן של הפעולות מבחינה טכנולוגית, והתמקדות בארכיטקטורת הרשת ואופן השימוש בה. הביקורת השלישית תציג שיקולים מעשיים המצדיקים סטייה מהתפישה הטריטוריאלית כפי שהיא חולשת כיום על דיני איסוף הראיות באינטרנט. אבקש להקדים ולהדגיש כי מטרתי בהצגת הביקורות הללו אינה להצדיק באופן גורף פעולה של הרשות החוקרת המדינתית כלפי כל סוגי הראיות הדיגיטליות באינטרנט בכל מקום שבו הן מצויות (או נחשבות כמצויות) בתוככי האינטרנט. במילים אחרות, הביקורות הללו אינן מאיינות את משמעות המיקום, או משמעות הטריטוריאליזם, בנוגע לאינטרנט, אלא הן מבקשות לערער את יסודות התפישה הטריטוריאלית באינטרנט כפי שהיא מעוצבת כיום.

### (א) ביקורת אפיסטמולוגית

כפי שהראיתי לעיל, 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 שאציג להלן מתמקדת ביסוד הראשון, שלפיו הראיה הדיגיטלית ניתנת למיקום. הביקורת האפיסטמולוגית נשענת על נקודת מוצא שלפיה ההתבוננות על האינטרנט במונחים של מקום היא מטאפורית.<sup>82</sup> הביקורת מתמקדת פחות בשאלה אם האינטרנט, כמכלול, הוא מקום נפרד או שונה מהמקום הפיזי, אלא היא מתמקדת

<sup>82</sup> דנתי במטאפורת האינטרנט כ"מקום", לעיל בפרק ב(3).

בתוככי המרחב המקוון, וגורסת כי למיקום המידע והיישומים שבו אין משמעות דומה לזו המוענקת למיקומם של חפצים במרחב הפיזי.<sup>83</sup> גם אם ניתן לשייך בנקודת זמן נתונה את המידע הדיגיטלי המבוקש כראיה למחשב מסוים ברשת, וגם אם ניתן לדעת את מיקומו של המחשב המסוים האמור מראש, כנדרש מבחינתה של הרשות החוקרת לצורך בחינת סמכותה הבין-לאומית, עדיין המשמעות של מיקום זה והפונקציות שמיקום זה משרת אינן אותן המשמעויות והפונקציות המוענקות ל"מיקום" במרחב הפיזי. לכן, לצד הקליפה הטכנית של אפשרות ההצבעה על מיקום הראיה, לא יהיה לה פרט לכך גרעין מהותי, ועל כן ניתן לומר שלא יהיה מדובר למעשה במיקום של ממש, על כל משמעויותיו ונפקויותיו המשפטיות.<sup>84</sup> במרחב הפיזי ל"מיקום" חפצים בתוך "מקום" יש משמעות. כך, למשל, המיקום במרחב הפיזי הוא אחד, ולא ניתן לשכפול או לביזור. המיקום נותר סטטי לאחר בחירתו. עקב כך, בעל השליטה בחפץ הבוחר את המיקום של החפץ, מבצע פעולה בעלת משמעות פיזית, אך גם משפטית. הוא מניח את החפץ במרחב פיזי ובמרחב משפטי כהחלטה מודעת. באינטרנט אין למיקום המידע והיישומים שבתוכו משמעות בעלת ערך כפי שמתקיים במרחב הפיזי. עקב כך ניתן לטעון כי לא צריכה להיות למיקום המידע (הראיתי בפוטנציה) באינטרנט משמעות משפטית. על מנת להמחיש את הטעון אציג להלן שלוש דוגמות:

1) ראובן ושמעון מחליטים לפתוח חשבון דואר אלקטרוני הניתן לגישה מכל מחשב המחובר לאינטרנט (Webmail). ראובן מחליט לפתוח את החשבון בשירות הדואר האלקטרוני של חברת וואלה הישראלית, ואילו שמעון מחליט לפתוח את החשבון בשירות Gmail של גוגל האמריקנית. סביר להניח שהפרמטרים שיעניינו את ראובן ושמעון בהחליטם לפתוח את החשבונות הדואר האלקטרוני הם אמינות השירות, יכולות סינון דואר הזבל, נפח האחסון של הדואר האלקטרוני בתיבה וכדומה. עוד סביר להניח שהפרמטר של מיקום

<sup>83</sup> על כן הביקורת יכולה לדור בכפיפה אחת הן עם התפישה שלפיה האינטרנט הוא מקום אחד, נפרד מהמרחב הפיזי, והן עם התפישה שלפיה האינטרנט אינו צריך להיתפש כלל כ"מקום", אלא כמדיום לביצוע התקשוריות, כאמצעי או כמכשיר, ולא כמרחב שאליו המשתמש נכנס. לתפישת האינטרנט כמקום אחד נפרד, ראו למשל: "Law and Borders" Johnson & Post, לעיל ה"ש 46. וליישום פסיקתי של גישה זו ראו: *Voyeur Dorm, L.C. v. City of Tampa*, 265 F. 3d 1232, 1236 (11<sup>th</sup> Cir. 2001). ANDREW L. SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 710-712 (1999).

<sup>84</sup> טיעון אפיסטמולוגי כללי זה נתמך על ידי תאוריות 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).

שרתי הדואר האלקטרוני של החברות לא יעניין במיוחד את ראובן ושמעון. יתר על כן, ייתכן בהחלט שמיקום שרתי הדואר האלקטרוני כלל לא יהיה ידוע לראובן ושמעון. לא זו אף זו, אלא שגם מבחינת ספקיות שירותי הדואר האלקטרוני, לא יהיה זה חשוב כלל מהיכן נרשם משתמש האינטרנט לשירותי הדואר האלקטרוני האמורים. גם מבחינת המדינות שבהן פועלות ספקיות שירותי הדואר האלקטרוני אין כל פיקוח, לא מראש ולא בדיעבד, על הנרשמים לשירות. עוד סביר להניח כי גם מבחינת האנשים המתכתבים בדואר האלקטרוני עם ראובן ושמעון, אין כל משמעות לבחירה שלהם בשירותי הדואר האלקטרוני של וואלה או של Gmail. במילים אחרות, כל הצדדים הנוגעים, במישרין או בעקיפין, לעולם הדואר האלקטרוני אינם מעניקים משמעות לסוגיית המיקום של שרתי הדואר האלקטרוני או של משתמשי השירות.

(2) שירותי מחשוב הענן (Cloud Computing) מבקשים לשנות את האופן שבו משתמשי האינטרנט צורכים שירותי מחשוב כגון הפעלת יישומים ואגירת מידע. שני אלה יתבצעו מתוך הענן, שהוא בבחינת "קופסה שחורה" עבור משתמש האינטרנט, שמטרתה לספק שירותים מוזלים, יעילים ואמינים. לא בכדי המטאפורה שנבחרה לשירותים אלה היא מטאפורת ה"ענן", שהוא מקום מעורפל, בלתי-גלוי לאדם המצוי על הקרקע, שאינו מאפשר למקם דברים בתוכו. עבור משתמש האינטרנט, ה"מקום" שבו נאגר המידע שלו או שממנו מסופקים לו השירותים היישומיים – אינו בעל משמעות, ולרוב גם אינו ידוע. משתמש האינטרנט לא עובר כל תהליך של הכרה במיקומו של ה"ענן", לא כל שכן במיקומם של הדברים בתוך הענן, וכן אין הוא עובר את התהליך ההופכי, של עצימת עיניים במודע בנוגע למיקומו של ה"ענן" ומיקומי המשנה בתוכו.

(3) משתמש האינטרנט מישראל מחליט לגלוש לאתר אינטרנט מסוים. אתר האינטרנט, לצורך הדוגמה, אגור בשרתים בארצות-הברית. נוכח ריבוי הגולשים מישראל לאותו אתר אינטרנט, מחליט ספק הגישה לאינטרנט להעתיק את תוכן האתר אל שרתיו בישראל, וכך יספק את תכניו למנוייו במהירות, ויוזיל את עלויות הגלישה בכל פעם מחדש דרך כבלים תת-ימיים של האינטרנט אל השרת בחו"ל (פעולת Caching). 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, פעולת ה-Caching נעשית בלי ידיעתו.<sup>85</sup> דוגמה נוספת היא כאשר אתר האינטרנט עצמו, ולא ספק הגישה לאינטרנט, מחליט לבצע פעולת ניתוב מחדש (redirection) לכל משתמש אינטרנט המגיע אל האתר שלו. פעולה זו יכול

<sup>85</sup> ראו: Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy* 85  
*Rules through Technology*, 76 TEX. L. REV. 553, 564 (1998).

שתיעשה לצורכי תחזוקת השרת שבו נמצא אתר האינטרנט, או מטעמים של החלפת שרת אחסון של האתר, או מטעמים של ויסות עומסים על השרת (נוכח ריבוי משתמשי אינטרנט המבקשים להיכנס לאתר, יחסית לכמות משתמשי האינטרנט שיכולים להיכנס אליו בו-זמנית). פעולת ה-redirection עשויה להעביר 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.

דוגמות אלה מלמדות כי משתמש האינטרנט אינו מייחס חשיבות למיקומם של חלק ניכר ממופעי האינטרנט. נוסף על משתמש האינטרנט עצמו, הדוגמה הראשונה מלמדת כי במידה רבה גם המדינות השונות, שבהן מצויים השרתים המאחסנים את המידע, אינן מייחסות משמעות רבה למיקום מידע בשרתים אלה. מדינות רבות, להוציא מדינות המטילות צנזורה על האינטרנט כסין, איראן וכדומה, אינן מטילות פיקוח או הליך של רישוי מוקדם בנוגע לתכנים הנאגרים בשרתים הממוקמים פיזית בשטחן. במילים אחרות, המדינות מעניקות כר פעולה חופשי למדי למשתמשי אינטרנט זרים לאגור מידע בשרתים שבשטחן. גם ספקיות השירות השונות (בדוגמה השנייה – ספקית שירותי מחשוב הענן; בדוגמה השלישית – ספקיות הגישה לאינטרנט) אינן מייחסות משמעות יתרה לשאלת המיקום של המידע הדיגיטלי.

ראינו אפוא כי למיקום המידע והיישומים באינטרנט אין משמעות בעיני משתמש האינטרנט, המדינות השונות וספקיות השירות השונות. מנגד, אם נחיל בדווקנות את המבחן שקובע סמכות אכיפה של המדינה לפי מקום הימצא הראיה הדיגיטלית, הרי שבדוגמות שהבאתי לעיל, בפרט בדוגמה האחרונה של שימוש בפעולת caching ו-redirecting, עשויות מדינות שונות לאחוז בסמכות בלעדית, בשל פרמטר טכני וזמני בנסיבות המקרה, ולא בשל זיקות מהותיות הנוגעות לטיב הפעולה או השירות האינטרנטי שבו מדובר. האחיזה בסמכות זו אינה רק בבחינת פריבילגיה למדינה, אלא היא גם גוררת – כך על פי חלק מהתאוריות המבארות את מושג הריבונות<sup>86</sup> – חובות על המדינות הללו. במילים אחרות, למדינות עשוי להיות אינטרס שלא לאחוז בסמכות זו, על מנת שלא תחויבנה בשיטור בנוגע למידע דיגיטלי האגור בשטחן.

בסיכומי של דבר, ההנחה היא שהראיה הדיגיטלית ניתנת למיקום בתוך המרחב האינטרנטי, עומדת בבסיס התפישה הטריטוריאלית בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט. הנחה זו אינה תואמת את האופן שבו נתפש האינטרנט בעיני משתמשי ואף בעיני המדינות השונות והתאגידים הפועלים באינטרנט. הביקורת האפיסטמולוגית גורסת כי אין ערך למיקום בתוככי האינטרנט כפי שניתן לו במסגרת

<sup>86</sup> ראו הדיון להלן בפרק ד(2)(ג), במסגרת הדיון בביקורות במישור התיאוריות של ריבונות על התפישה הטריטוריאלית ביחס לחקירה הפלילית באינטרנט.

החלת התפישה החפצית על סמכויות האיסוף של המדינה באינטרנט. ביקורת זו סוללת את הדרך לטיעון העקרוני כי אין להעניק לפיכך גם משמעות משפטית למיקום המידע (כראיה) בתוך המרחב האינטרנטי.

## (ב) ביקורת ארכיטקטונית וטכנולוגית

הביקורת הארכיטקטונית והטכנולוגית מתמקדת ביסוד השני והשלישי של התפישה הטריטוריאלית, ולפיה גם אם הראיה הדיגיטלית ניתנת למיקום, הרי לא ניתן להניח כי המקום הוא המחשב שבו מאוחסנת הראיה, וכן אין לראות במקום הימצא הראיה משום המקום הקובע לעניין בחינת סמכותה הבין-לאומית של הרשות החוקרת המבקשת לאסוף את אותה ראיה.

אציג תחילה את הביקורת כלפי היסוד שלפיו המידע הדיגיטלי באינטרנט ניתן למיקום לפי מחשב שבו הוא מאוחסן. על פי הביקורת, יסוד זה מציב "דרישת מסוימות", שלפיה ניתן יהיה לדבר על מקום מסוים מובהק בתוך האינטרנט שבו מצויה הראיה הדיגיטלית. ברם, קשה למקם, לבדוד ולבדל מידע באינטרנט, כך שייחס לכל פרט מידע מיקום מסוים וייחודי ברשת. גם פעולה המתרחשת ברשת, כגון התקשורת בין צדדים או פרסום תכנים – קשה לייחסה למקום אחד באינטרנט. ארכיטקטורת הרשת מבוזרת מעצם טבעה, התקשורת בה מועברת בשיטה של פירוק ל"חבילות" (packets) הנעות דרך מסלולים נפרדים אל היעד. חלק מתופעות הפשיעה באינטרנט מנצלות את משאבי הרשת ואת אלמנט הביזוריות שלה. כך, למשל, התקפות של DDOS מגייסות כמות גדולה של מחשבים תמימים המחוברים לרשת במקומות שונים בעולם, מקומות שאינם בהכרח ידועים למפעיל המתקפה או לקרבנה. באופן דומה, הפצה של דואר זבל (SPAM) מבוססת על גיוס מחשבים רבים (Zombies) ממקומות שונים שאינם ידועים למפיץ.<sup>87</sup> מכאן שנוצר לכול בנוגע לשאלה אם האינטרנט הוא מקום אחד, נפרד מהמרחב הפיזי, אם המידע שבו או הפעולה המתרחשת בתוכו מצויים בכמה מקומות בו-זמנית, או שמא אכן ניתן לשייך כל מידע וכל פעולה ברשת למקום פיזי אחד מסוים.<sup>88</sup> עוד מן הראוי לשוב ולהזכיר

<sup>87</sup> ראו למשל אצל: Koslovski, לעיל ה"ש 1, בעמ' 63–66.

<sup>88</sup> עיון בפסיקת בתי המשפט חושף את הקושי בשיוך פעולות או מידע מסוים באינטרנט למקום אחד הניתן לשיוך במרחב הפיזי. בכל הנוגע לפסיקה (ישראלית וזרה) הבהונת את מקום ביצוע העברה הפלילית, הראיתי לעיל (בהקשר של סמכות התחיקה) כי המקומות שבהם המידע נתפש כמצוי בהם הם כל המקומות שבהם המידע מצוי או נצפה בפועל, ולא אך ורק המקום שבו הועלה המידע לאינטרנט. ראו, למשל, בהקשר של הימורים באינטרנט את פרשת W.I.G.C., לעיל ה"ש 32; פרשת קרלטון, לעיל ה"ש 30. בהקשר של עברת פרסומי תועבה. ראו: Yuval Karniel & Haim Wismonskey, *Pornography, Community and the Internet – Freedom of Speech and Obscenity on the Internet*, 30 RUTGERS COMP. & TECH. L.J. 105, 146–151

כאן את הדוגמות של שירותי מחשוב ענן (Cloud Computing), פעולות Caching של ספקיות גישה לאינטרנט ופעולות redirection בין אתרי אינטרנט שונים, שמנתי לעיל, כדוגמות מסבכות לשאלת היכולת למקם את המידע הדיגיטלי באופן מפורש באינטרנט.<sup>89</sup> יש לזכור כי כשעוסקים בדיני איסוף הראיות, ובפרט בסמכות האיסוף של הרשות החוקרת מבחינה בין-לאומית, על רשויות החקירה לדעת מראש את המיקום של הראיות הדיגיטליות שהן מבקשת בטרם הן מבצעות את פעולת האיסוף. וזאת, על מנת שלא תימצאנה בדיעבד כמי שפועלות בחוסר סמכות. כיוון שבחינת המיקום של הראיה הדיגיטלית נדרשת מראש (ex ante), הקושי באיתור המיקום מחריף עוד יותר.

שתי התפתחויות מן העשור האחרון בעניין אופן השימוש באינטרנט תורמות להפיכת המקום באינטרנט לעניין נזיל. ההתפתחות הראשונה היא בדמות המעבר

---

(2004); פרשת *Thomas*, לעיל ה"ש 33. בהקשר של עברות איסור הכחשת השואה והסתה לגזענות, ראו פרשת *Yahoo*, לעיל ה"ש 37. בהקשר של עברות מרמה באמצעות האינטרנט, ראו: תה"ג (מחוזי י"ם) 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.). **הפסיקה הבוחנת סוגיות של סמכות שיפוט מקומית בתביעות אזרחיות הנוגעות לפעילות באינטרנט** מגלה כי יש אי-אחידות בנוגע לשייך הפעילות באינטרנט למקום מסוים. לפסיקה הקובעת כי הפעילות באינטרנט, הפרסום בו והמידע המופץ בו הם למעשה בכל מקום שבו נצפה המידע, ראו למשל: בש"א (שלום ק"ג) 884/02 **לנדאו נ' חסון**, תק-של (2)02 850 (2002); בש"א (מחוזי י"ם) 2841/03 **רעות אלקטרוניקה ורכיבים בע"מ נ' מראות אימאג' בע"מ**, תק-מח (4)03 1445 (2003); ת"א (שלום ת"א) 32786/06 **לבבי נ' דראי**, תק-של (4)06 1088 (2006); ת"א (מחוזי חי') 27608-04-11 **הטכניון – מכון טכנולוגי לישראל נ' Google Inc.**, תק-מח (2)11 4707 (2011). ראו גם: ב"ש (שלום י"ם) 8033/06 **שטיינברג נ' לוי**, תק-של (2)07 614 (2007). שם בית המשפט מעיר כי האינטרנט הוא חסר מקום, אך מסיק אופרטיבית כי סמכות השיפוט לגבי פעולות המתבצעות בו היא כלל-מדינתית, בכפוף למקרים שבהם מנוצל עניין הסמכות הכלל-ארצית על ידי תובע לרעה ונוצר מצב קיצוני של פורום לא נאות. בבש"א (שלום י"ם) **המכרז של המדינה בע"מ נ' אבו חצירה**, תק-של (4)05 9259 (2005), ניסה בית המשפט לייחד את מקום ביצוע המעשה נשוא התביעה למקום שבו נרשם התובע, משתמש האינטרנט, לשירותי הנתבעת, בעלת אתר האינטרנט שאליו גלש התובע. כן ראו בש"א 9598/10 **בר-יעקב נ' בית אבות עדנה בע"מ** (פורסם בנבו, 26.01.2011), שם נדונה בקשה של נתבע בתביעת לשון הרע להעתיק את מקום הדיון בתביעה שהוגשה נגדו. התובעים טענו כי לפרסומים באינטרנט אין מקום שיפוט ספציפי, כך שאין כל קושי, מבחינת דיני סמכות שיפוט מקומית, לדון בתביעה בכל מקום. הנשיאה ביניש בחרה בהחלטתה להזניח את סוגיית הפרסום באינטרנט, ולבחון את הבסיסים האחרים שעליהם ניתן להשתית את הסמכות המקומית. לטעמי, החלטה זו מבטאת במובהק את חוסר היכולת של בית המשפט להגדיר מקום מסוים בנוגע לפעולה המתבצעת באינטרנט.

89 ראו לעיל בפרק ד(2)(א), במסגרת הדיון בביקורת האפיסטמולוגית על התפישה הטריטוריאלית ביחס לחקירה הפלילית באינטרנט.

לאינטרנט 2.0, שבו משתמשי האינטרנט מעלים תכנים בעצמם ועורכים אותם. נניח אתר אינטרנט שמבוסס על שיתוף תוכני גולשים (לדוגמה רשת חברתית, אתר פורומים וכדומה). המידע והפעילות באתר מעוצבים ברובם על ידי משתמשי האינטרנט, שבוחרים מתי להתחבר ומהיכן, 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: בזמן מסוים הוא יכול להימצא בשרתי האתר ובזמן אחר, להיעלם משם ולהימצא רק במחשבי המשתמשים שהורידו אותו עד למחיקתו. **ההתפתחות השנייה** היא הנגשת האינטרנט למכשירים ניידים (סמארטפונים וטאבלטים) והגברת הנגישות לאינטרנט ממקומות ציבוריים (Wireless networks). אם בעבר נתפס משתמש האינטרנט כמצוי בנקודה קבועה, ואילו אתרי האינטרנט שאליהם גלש היו המשתנה הדינמי בפעילותו זו, הרי כיום גם משתמש האינטרנט דינמי, שהרי הוא 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 כך שלא תמיד ניתן לשייך את הראיה הדיגיטלית למחשב מסוים שבו היא מאוחסנת. עתה אציג את הביקורת על היסוד השלישי של התפישה הטריטוריאלית, ולפיו אבן הבוחן לקביעת סמכות אכיפה בין-לאומית של המדינה החוקרת היא מקום אחסונה של הראיה הדיגיטלית. ראינו לעיל שסמכות האכיפה נשמרת בקפידה יחסית כסמכות הצמודה לטריטוריה של המדינה. כך הוא במקרה של אכיפה במרחב הפיזי, וכך הוא במקרה של אכיפה במרחב האינטרנט. במרחב הפיזי מושאי הפעולה, מבצעי הפעולה, הפעולה עצמה והראיה המבוקשת – מצויים ומתרחשים כולם באותו מקום. 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**" בנוגע לאיסוף ראיות בחקירה פלילית במרחב הפיזי. איסוף ראיות באינטרנט שובר את האחדות המרובעת האמורה, ולפיו החוקר, החשוד, פעולת האיסוף והראיה המבוקשת לא חייבים להיות באותו המקום ובאותה המדינה.

בטרם אדון בשבירת האחדות המרובעת באינטרנט, אפנה תחילה לעולם **האזנות הסתר לתקשורת טלפונית**, שבו פותחו תובנות הנוגעות לענייננו עוד טרם עידן האינטרנט. עולם האזנות הסתר הטלפונית אפשר לערוך חלוקה משולשת בין מיקומים של כמה גורמים: החוקרת, רכיב ההאזנה (משם מאזינים לשיחה בפועל, קרי מתבצעת פעולת האיסוף בפועל), משוחח א' ומשוחח ב'. נניח כי נעברה עברה המקימה סמכות שיפוטית ישראלית, והעברה נחקרת על ידי משטרת ישראל. כל אחד מארבעת הגורמים האלה יכול להיות בישראל או מחוצה לה, אם כי מבחינת החוקרת ברי כי היא תפעל מישראל, שאחרת תימצא כמי שמפעילה סמכות שלטונית

בטריטוריה זרה ובכך יש כדי לפגוע בריבונות של מדינה זרה. נוצרת קשת של אפשרויות כמפורט להלן בטבלה הבאה:

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, יכולות להיווצר 8 סיטואציות עובדתיות שונות, בכל הנוגע לשאלת המיקום הטריטוריאלי של הטלפונים המואזנים ושל רכיב ההאזנה (בישראל או בחו"ל). זאת, 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 מסוימת. הגישה הרווחת בישראל,<sup>90</sup> כמו גם בארצות-הברית<sup>91</sup> ובקנדה,<sup>92</sup> היא שהמיקום הקובע הוא של רכיב ההאזנה ולא של יעד ההאזנה, לעניין עצם הסמכות לבצע את הפעולה.<sup>93</sup>

<sup>90</sup> הדבר עולה מפרשת אל מצרי, לעיל ה"ש 24. לעמדה המבכרת את מיקומו של החשוד על פני מיקומו של רכיב ההאזנה, עמדה אשר לא התקבלה בפרשת אל מצרי, ראו: אלי וילצ'ק "קבילות ראיות שהושגו בחו"ל בהאזנת סתר" משפטים טז 462 (1986).

<sup>91</sup> ראו: U.S. v. Tavarez, 40 F.3d 1136; U.S. v. Rodriguez, 968 F.2d 130 (2<sup>nd</sup> Cir. 1992); U.S. v. Denman, 100 F.3d 399 (5<sup>th</sup> Cir. 1996); U.S. v. Jackson, 471 (10<sup>th</sup> Cir. 1994) F.3d 910 (7<sup>th</sup> Cir. 2000); U.S. v. Ramirez, 112 F.3d 849 (7<sup>th</sup> Cir. 1997); U.S. v. Luong, 471 F.3d 1107 (9<sup>th</sup> Cir. 2006); Windhurst, פרשת Windhurst, לעיל ה"ש 22.

<sup>92</sup> ראו למשל: CSIS, [2010] 1 F.C.R. 460 (Ca.).

<sup>93</sup> לעומת זאת, לעניין ההגנה החוקתית שתחול על יעדי ההאזנה במקרה של האזנה אקסטרה טריטוריאלית, ייתכן שתהיה חשיבות גם לעצם המיקום שלהם. נושא הפרישה הטריטוריאלית או האקסטרה טריטוריאלית של ההגנות החוקתיות על מושאי החקירה הוא נושא מורכב, המתעורר בעקבות הכרה מהסמכות להפעיל סמכויות חקירה אקסטרה-טריטוריאליות. לא אפתח את הדיון בנושא זה במאמר.

דוגמת האזנות הסתר הטלפוניות מעלה כי מקום ביצוע פעולת האיסוף עצמה מכתוב את ה"מקום" הרלוונטי לעניין בחינת סמכות האכיפה האקסטרה טריטוריאלית. אולם הדוגמה אינה מגלמת היטב את ההבדל בין מקום ביצוע פעולת האיסוף לבין מקום הימצא הראיה המבוקשת, הבדל רב-חשיבות בכל הנוגע לחקירה פלילית באינטרנט. כאמור לעיל, אבן הבוחן לקביעת המקום המיוחס לחקירה הפלילית באינטרנט היא מיקומה של הראיה הדיגיטלית הנאספת, בעת איסופה. במילים אחרות, לא מקום ביצוע פעולת האיסוף, אלא מקום הימצא הראיה הנאספת, הוא הקובע לעניין השאלה אם מדובר בפעולת איסוף אקסטרה טריטוריאלית במסגרת חקירה פלילית באינטרנט.

**מבחן מקום ביצוע הפעולה ומבחן מקום הימצא הראיה עשויים 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 במחשב המצוי בחו"ל באמצעות התחברות מרחוק דרך האינטרנט. בשתי דוגמות אלה החוקרת נמצאת בישראל ומבקשת לבצע את הפעולות הנ"ל באמצעות הפעלת מחשבה מישראל.<sup>94</sup> על פי מבחן מקום הימצא הראיה המבוקשת, אין ספק כי החוקרת הישראלית ביצעה פעולת איסוף אקסטרה טריטוריאלית. על פי מבחן מקום ביצוע הפעולה, ניתן לטעון כי הפעולה בוצעה ממדינת ישראל ואינה נחשבת כאקסטרה טריטוריאלית. הטענה מעוררת דיון המשך מורכב בדבר המקום שבו מתבצעות התקשוריות באינטרנט: אם זהו מקום אחד, כמה מקומות בו-זמנית, או אולי כל מקום שבו נפרשת הרשת.

נניח שחוקרת משטרה משתילה באופן סמוי את רכיב ההאזנה במחשבו של החשוד, בעת שזה נמצא בישראל, ואילו כעבור זמן נוסע החשוד לחו"ל עם מחשבו ורכיב ההאזנה משדר ממנו אל החוקרת באמצעות האינטרנט. סיטואציה זו יכולה להתרחש בין שבמכוון (על ידי החוקרת) ובין שלא במכוון. 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: אם בשלב השתלת רכיב ההאזנה בלבד, או שמא בכל שלב שבו מתבצעת ההאזנה בפועל.

ראינו אפוא כי מבחן מקום הימצא הראיה הוא דווקני יותר ממבחן מקום ביצוע

<sup>94</sup> 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 בניגוד לכללי סמכות האכיפה הבין-לאומית, ולמעשה לא היה בפעולתה כל הבדל לענייננו, לעומת פעולת איסוף אחרת במרחב הפיזי.

פעולת האיסוף. לטעמי, מבחן מקום הימצא הראיה אינו משרת באופן מדויק את התכלית של כיבוד ריבונותן של מדינות זרות, ולמעשה מבחן מקום ביצוע פעולת האיסוף נכון ומדויק יותר. זאת, מכמה טעמים: הראשון, מקום הימצאותה של הראיה הדיגיטלית אינו תמיד ידוע מראש.<sup>95</sup> השני, חלק מפעולות האיסוף נוגעות למידע העובר בתקשורת בין מחשבים (לדוגמה, בהאזנת סתר לתקשורת אינטרנטית), שאז עניין המיקום של המידע הוא נזיל ומשתנה. יתרה מזאת, חלק מהראיות הדיגיטליות חשובות ומשמעותיות 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 מאשר לאתר את עצם ההחזקה בנגיף, אשר אינה מהווה עברה כשלעצמה.<sup>96</sup> במצב כזה, קשה עוד יותר לסמן מיקום של הראיות באינטרנט. השלישי, ניתן לטעון כי מבחינת משפטה הפנימי של המדינה החוקרת, החריגה האקסטרטריטוריאליית אינה כאשר הראיה המבוקשת מצויה בחו"ל, אלא כאשר המדינה החוקרת פועלת בחו"ל. יתר על כן, מדינות שונות מאפשרות לאזרחים זרים מן השורה גישה למידע האגור במחשבים בטריטוריה שלהן כל העת. מה שאין הן מתירות, הלכה למעשה, הוא גישה של רשויות של מדינות אחרות. על פי טענה זו, הפגיעה בריבונות של מדינות זרות, העשויה למנוע פעולה של המדינה החוקרת באינטרנט, נובעת מהפעולה של המדינה החוקרת, ולא דווקא ממקום הימצא הראיה המבוקשת. הרביעי, ניתן לציין בהקשר זה כי איסוף ראיות דרך התחברות מרחוק אינה יכולה לכלול הפעלת כוח פיזי, כפי שיכול להתרחש בעת שמבוצעת פעולת איסוף במרחב הפיזי, כדוגמת חיפוש בחצרים.<sup>97</sup> הפעלת כוח במקרים אלה היא הפעלת כוח שלטונית, המגלמת ביטוי מעשי של סמכות הריבון על נתיניו. כיוון שהפעלת הכוח הפיזי נעדרת מאיסוף ראיות באמצעות התקשורת מרחוק באינטרנט, הרי שחלק מהמובנים של פגיעה בריבונות של המדינה הזרה ממילא אינם מתקיימים במקרה של איסוף ראיה דיגיטלית האגורה במחשב בחו"ל. אין כוונתי שהמדינה

<sup>95</sup> ייתכן שברשות רשויות החקירה תהיה בשלב ראשון כתובת IP שמייצגת אך ורק את שרת ה-proxy שדרכו בוצעה הפעילות הפלילית, והתחקות אחרי החשוד לפי כתובתו של ה-proxy server שממנו פעל, תעיד כי הפעולה הייתה במדינה X אף שבפועל הוא פעל ממדינה Y, ורק התקשר דרך מדינה X. הידיעה בדבר המדינות שבהן "עבר" החשוד תוכל להיות בדיעבד בלבד.

<sup>96</sup> ראו ס' 6 לחוק המחשבים, התשנ"ה-1995.

<sup>97</sup> חיפוש בחצרים עלול לכלול הפעלת כוח, בין נגד מקומות נעולים בתוך החצרים, שבהם מבוצע החיפוש, ואף נגד נוכחים בחצרים המתנגדים לעצם החיפוש או החשודים בביצוע עברה פלילית שנעברה או שעתידיה להיעבר. ראו ס' 45, ס' 24(א) ו-ס' 19 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969, וכן ראו ס' 23 חוק הסדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו-1996, המעניק סמכות כללית למעצר בלא צו שיפוטי, בין היתר במקרים של חשש להעלמת ראיות או ביצוע עברת מעצר (ובכללה עברה של הפרעה לשוטר בעת מילוי תפקידו, תקיפת שוטר וכיוצא בזה סעיפים העשויים להיות רלוונטיים לסיטואציה של התנגדות לחיפוש).

החוקרת במצב כזה אינה מפעילה סמכות שלטונית, אבל במובן אחד של הפעלת סמכות שלטונית – מובן של הפעלת כוח פיזי – אין מופעלת סמכות שלטונית. לסיכום, מקובל לסבור כי מקום הימצא הראיה הדיגיטלית הוא המקום הקובע בנוגע לשאלת סמכות האכיפה הבין-לאומית. לעומת מבחן זה ניתן להציע את מבחן מקום ביצוע פעולת האיסוף. האינטרנט מאפשר ביצוע פעולות איסוף ראיות מרחוק, תוך התחברות ממחשב אחד למחשב אחר, אם שניהם מחוברים לרשת. הפעולה מתבצעת בנוגע לראיה דיגיטלית המצויה אמנם 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.<sup>98</sup>

יש לזכור בכל הנוגע לסמכות התחיקה של המדינה בנוגע לאינטרנט, הונהג הכלל, שלפיו המחשב שאליה מגיע התוכן המקים את העברה הפלילית, מקים סמכות למדינה שבה מצוי המחשב, במובן זה שהמעשה נתפס כעברת פנים.<sup>99</sup> היקף מסמכות התחיקה אל סמכות האכיפה מעלה כי **פעולת האיסוף צריכה להיחשב ככזו המתבצעת במחשבו של החוקר, ולא דווקא במחשב היעד,** אשר בנוגע אליו מתבצעת פעולת האיסוף.

### ג) ביקורת במישור תאוריות של ריבונות

הריבונות מתאפיינת בטריטוריה; טריטוריה היא גבולות סמכותה המשפטית של המדינה; וכללי הסמכות המשפטית מהווים ביטוי של הריבונות. לפי תפישת היסוד בדבר תפקידה של המדינה המודרנית, 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 ומבחינה רעיונית, ניתן לזהות פעפוע בין המושגים ריבונות, סמכות וטריטוריה. תפישה זו היא נחלת המשפט הישראלי,<sup>100</sup> כמו גם נחלת המשפט האמריקני<sup>101</sup> והמשפט הבין-לאומי.<sup>102</sup> לעתים

<sup>98</sup> על תקשורות push לעומת תקשורות pull ראו למשל: Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1130, 1148 (2000).

<sup>99</sup> ראו הסקירה לעיל בה"ש 88.

<sup>100</sup> פרופ' ש"ז פלר, בספרו הקלאסי "יסודות בדיני עונשין" כתב: "התחולה הטריטוריאלית של הנורמה הפלילית היא גם ביטוי אלמנטרי של ריבונות המדינה; המדינה היא הכוח 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 מסויגת של הנורמה הפלילית של המדינה היא היבט של ריבונותה כלפי פנים וכלפי חוץ כאחד". ראו:

נדמה כי התפישה כה יסודית, עד שהחוק אינו צריך לציין במפורש כי המשפט חופף את הטריטוריה של המדינה, וכי זו הנחת היסוד. רק חריגה מהנחה זו צריכה להיאמר במפורש.<sup>103</sup>

מכאן נובע, שכאשר מדינה מבקשת להרחיב את סמכותה אל מחוץ לטריטוריה שלה, וההרחבה נעשית אל עבר שטחה של מדינה אחרת, ולא לעבר אזורים שאינם בבעלות מדינות אחרות, כגון הים הפתוח, הרי נוצר משחק "סכום אפס", שלפיו הרחבת הסמכות של מדינה אחת אל מעבר לגבולות הטריטוריה שלה, משמעה הצרת הסמכות של מדינה אחרת. זאת, אלא אם כן מחליטות המדינות לשתף פעולה ולהפוך את החריגות האקסטרה טריטוריאליות למוסכמות.<sup>104</sup> פרט לפן ההסכמי, המשפט הבין-לאומי מחיל כללים מנהגיים, קוגנטיים, המחייבים את המדינות ומגבילים למעשה את ריבונותן, במובן של ניהול ענייניהן הפנימיים והחיצוניים לפי ראות עיניהן וללא הגבלות.<sup>105</sup>

כפי שאטען להלן, הפעפוע האמור בין המושגים ריבונות, סמכות וטריטוריה, אינו עניין דטרמיניסטי. תפישת הריבונות עברה שינויים לאורך ההיסטוריה.<sup>106</sup> סטפן קרייזנר (Krasner) הראה כיצד תפישת הריבונות השתנתה בתגובה להתפתחויות

פלר, לעיל ה"ש 19, בעמ' 239. ראו גם: ש"ז פלר ומרדכי קרמניצר "הצעת חלק מקדמי וחלק כללי לחוק עונשין חדש ודברי הסבר תמציתיים" **משפטים** יד 127, 200 (1984). אמירתו זו של פלר אומצה בפסיקת בית המשפט העליון. ראו: ע"פ 4391/03 **אבו ריא נ' מדינת ישראל**, תק-על 05 (4) 2821, 2828 (2005). ראו עוד, בהקשר לסמכות התחיקה הכללית של המדינה, לאו דווקא זו הפלילית: אהרן ברק **פרשנות במשפט** כרך ב: פרשנות חקיקה 578 (1993).

101 RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 206 cmt. b.

102 ראו למשל: SHAW, לעיל ה"ש 13, בעמ' 487-488. שאו כינה תפישה זו כאקסיומה הבסיסית של המשפט הבין-לאומי הקלאסי.

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

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

105 על פי האמור לעיל, הריבונות נתפשת כסך הכוחות הנותנים למדינה לאחר ההסדרה של המשפט הבין-לאומי. מדינות הסוטות ממרותו של המשפט הבין-לאומי מנצלות לרעה את ריבונותן (Abuse of Sovereignty). ראו: פרשת *Lotus*, לעיל ה"ש 17, בעמ' 18. כן ראו את עמדת השופט אנצ'לוטי בעניין: Custom Regime Between Austria and Germany, 1931. PCIJ (Vol. II) Advisory Opinion No. 20, p. 276. Hans Kelsen, *The Principle of Sovereign Equality of States as a Basis of International Organization*, 53 YALE L. J. 207 (1944).

106 לא אביא כאן בחינה היסטורית של התפתחות התפישה של המונח "ריבונות", מימי האימפריה הרומית ועד ימינו; CHARLES E. MERRIAM, HISTORY OF THE THEORY OF SOVEREIGNTY. SINCE ROUSSEAU (1999).

חברתיות ומדיניות.<sup>107</sup> אמנם, לדידו של קרייזנר, בליבת ההגדרה של ריבונות עדיין נותר העיקרון של הפעלת סמכות בטריטוריה נתונה,<sup>108</sup> אולם נוכח הגמישות המושגית של הריבונות, ניתן לטעון כי אין לראות במונח "ריבונות" משום חסם טבעי מפני ניתוח התפישה הטריטוריאלית הנוהגת בנוגע לאינטרנט. יצוין כי בעידן הגלובליזציה הכלכלית והתקשורתית, עד טרום עידן האינטרנט ובוודאי לאחר התפשטות האינטרנט בשימוש כלל-עולמי, רבו הקולות המדברים על פוסט לאומיות ( Post nationalism), על היחלשותה של המדינה ובפרט על היחלשות מושג הריבונות של המדינות. הטענה המושמעת היא שבעידן של גלובליזציה, מושגי הגבולות הפיזיים מיטשטשים, מדינות וגופים לא מדינתיים משפיעים באופן משמעותי על מדינות ופרטים בטריטוריות אחרות, הן ברמת המאקרו המדינתית והן ברמת המיקרו של הפרט במדינה הזרה, ובכך יש משום התערבות בענייני הפרטים הנתונים למרותן של מדינות זרות.<sup>109</sup> 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 בכל הנוגע למשטרים ליברליים, המכירים בביזור הכוח בין השלטון לבין האזרחים, תפישת הריבונות ממילא שונה והיא מפויסת יותר ביחס בין הממשל לבין האזרחים. בשונה מהעמדה הראליסטית, אין התפישה הליברלית של הריבונות מבוססת על טריטוריאליות ועל ייחוד הסמכות בטריטוריה נתונה.<sup>110</sup> על פי תפישה זו, המדינה ומושג ה"ריבונות" נועדו לשרת אינטרסים משותפים של קבוצות פרטים.<sup>111</sup> גם האינטרנט מקדם ערכים ואינטרסים של הפרט, ועל כן הוא אמצעי

<sup>107</sup> ראו: STEPHEN D. KRASNER, SOVEREIGNTY – ORGANIZED HYPOCRISY (1999).

<sup>108</sup> ראו: Stephen D. Krasner, *Sovereignty: An Institutional Perspective*, 21 COMP. POL. STUD. 66, 86 (1988).

<sup>109</sup> 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 JEAN-MARIE GUEHENNO, THE END OF THE NATION-STATE (Victoria Elliott trans., 1995); Johnson & Post "Law and Borders" לעיל ה"ש 46, בעמ' 1376-1370; John O. McGinnis, *The Decline of the Western Nation and the Rise of the Regime of International Federalism*, 18 CARDOZO L. REV. 903 (1997).

<sup>110</sup> 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 (1998).

<sup>111</sup> ראו: 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, 728-729 (1995); Anne-Marie Burley, *Law Among the Liberal States: Liberal Internationalism and the Act of State Doctrine*, 92 COLUM. L. REV. 1907 (1992).

להגשמת ערכים ליברליים. הריבונות היא אינסטרומנטלית ולא אבסולוטית, וכך גם האינטרנט הוא אינסטרומנטלי, והערך שנועדו לשרת שניהם – הריבונות והאינטרנט – הוא הערך של קידום תועלתו של הפרט. משכך, האינטרנט לא סותר, ולא יכול לסתור, את הריבונות. האינטרנט אף יכול לקדם ריבונות במובנה הליברלי.<sup>112</sup> תפישת הריבונות שמציע פריט היא תלויה עמדה פוליטית משטרית, ובמילים אחרות היא מתחום מדע המדינה יותר מאשר מתחומי המשפט. טרכטמן טען כי הקישור בין ההתקדמות הטכנולוגית ובין היחלשות המושג "ריבונות" נובע מתפישה שגויה של הריבונות כעניין מוחלט וקוגנטי, אלא שבפועל מעולם לא הייתה הריבונות אלא מושג גמיש שעובר שינויים תלויי זמן, מקום והסכמה בין מדינות.<sup>113</sup> אם כך הוא, אין לדבר על היחלשות מושג ה"ריבונות" בעקבות התפתחות האינטרנט, אלא על היתכנות להגמשה נוספת של המושג.

הצגה מוכרת ומרכזית במשפט הבין-לאומי של מושג הריבונות מופיעה בבוררות בפרשת **האי Palmas** משנת 1928.<sup>114</sup> באותו מקרה נטען כי מושג הריבונות אינו צריך להיתפש רק כסמכות של המדינה כלפי פנים, ואף לא כעצמאותה כלפי חוץ, אלא גם כחובתה כלפי חוץ.<sup>115</sup> בפרשת **האי Palmas** נקבע 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).<sup>116</sup> לטעמי, הפרשנות הזאת למונח ריבונות מאפשרת לבחון מצבים שבהם המדינה תפעל באופן אקסטרה טריטוריאלי לשם שמירה על ענייניה הפנימיים.

בהיקש מפרשת **האי Palmas** לאינטרנט: אם שרת מחשב מצוי פיזית במדינה א', אולם מתבצעת ממנו עברה בשטחה של מדינה ב', ומדינה א' אינה חוקרת את העברה 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

<sup>112</sup> ראו: Peritt, לעיל ה"ש 111, בעמ' 437–441.

<sup>113</sup> ראו: Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561, 563–565, 567 (1998).

<sup>114</sup> ראו פסיקת הבורר הובר (Huber) בעניין: Netherlands v. U.S., 2 RIAA 829 (1928).

<sup>115</sup> שם, בעמ' 839. ראו גם: SHAW, לעיל ה"ש 13, בעמ' 490.

<sup>116</sup> עוד 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 1 (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).

הנפגעים מפעילות פלילית באינטרנט. 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'.<sup>117</sup> בסיכומו של דבר, 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.

## ה. סיכום ואחרית דבר

התפישה הטריטוריאלית של דיני איסוף הראיות באינטרנט 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 עירוב תחומים: משפט של מדינות מקרין על משפט של אנשים. התפישה הטריטוריאלית הביאה להכפפת המשפט הפלילי באינטרנט, ובפרט דיני איסוף הראיות, לכללי המשפט הבין-לאומי בהסדרת יחסים בין מדינות. כללים אלה אינם אמורים להפוך לחלק אינטגרלי ממערכת האיזונים החוקתית שאמורה להישקל על בסיס יומיומי במסגרת הוצאה אל הפועל של חקירה פלילית. בזירת האינטרנט לכל עברה, ובעקבותיה לכל חקירה, פוטנציאל מידי להפוך לחקירה בין-לאומית. עקב כך, מערכת שיקולים שאינה בליבת דיני החקירה הופכת למערכת השיקולים המושלת בכיפה.

החקירה הפלילית צריכה לאזן בין שניים: מחד גיסא, אינטרס ציבורי לאתר עבריינים ולהעמידם לדין בגין עברות שביצעו, ומאידך גיסא, לשמור על הליך הוגן ועל זכויות היסוד של החשודים ושל צדדים שלישיים.<sup>118</sup> על כל פנים, אין החקירה

<sup>117</sup> ההצדקה העיונית לפעולה אקסטרה טריטוריאלית מתוך פסק הבוררות בפרשת **Palms** אינה עומדת לבדה. היא מצטרפת לתובנות נוספות, אותן מנית לעיל, בדבר מבנה רשת האינטרנט כרשת גלובאלית חוצת גבולות מדיניים, כמו גם לתובנות בדבר כלל הווטו החקירתי הקיים כיום באינטרנט, בדבר חוסר המשמעות של המקום באינטרנט וחוסר היכולת לאתר מראש (ex ante) את המקום באינטרנט. תובנות אלה מבדילות בין המרחב האינטרנטי לבין המרחב הפיזי כמרחב שבו יש מקום לפרוץ את גרדי התפישה הטריטוריאלית בנוגע לחקירות פליליות.

<sup>118</sup> ראו בהקשר זה את חיבוריו של הרברט פקר (Packer) על המאבק בין שתי הגישות למשפט הפלילי: גישת השליטה בפשיעה (Crime Control Model) וגישת ההליך ההוגן (Due Process Model): Herbert A. Packer, *Two Models of Criminal Process*, 113 U. PA. L. REV. 1 (1964); כן ראו: HERBERT A. PACKER, *THE LIMITS OF THE CRIMINAL SANCTION* (1968).

הפלילית מיועדת ככלל להתחשב במדינות זרות כ"שחקניות" רלוונטיות בזירת החקירה הפלילית. התפישה הטריטוריאלית של החקירה הפלילית באינטרנט הוסיפה את שיקול כיבוד ריבונותן של המדינות הזרות כמשתנה נוסף לתוך מערך השיקולים במהלך החקירה. לא זו אף זו, היא הפכה את שיקול כיבוד הריבונות של מדינות זרות למעין "כרטיס אדום" שמונע בעד חקירות פליליות באינטרנט להתקיים. בפועל, הצרת סמכות האכיפה בנוגע לאיסוף ראיות בחקירה פלילית באינטרנט, בעייתית מבחינה מעשית ואינה מוצדקת בהתחשב בארכיטקטורת האינטרנט ובמהותן של הראיות הדיגיטליות. כן אין היא מתאימה מבחינה אפיסטמולוגית ואף אין לראות בה כמבטאת במובהק את ריבונותן של המדינות.

מטרתי במאמר זה הייתה לחשוף את התפישה הטריטוריאלית החולשת על דיני החקירה, לבקר אותה ולהדגיש את הקשיים המיוחדים שהיא מציבה לחקירה הפלילית באינטרנט. מכאן סלולה הדרך להמשך הדיון בדבר המודל החלופי שיכול לבוא תחת המודל הטריטוריאלי בנוגע לסמכות האכיפה באינטרנט. במסגרת עבודת הדוקטורט אני בוחן את האפשרות לבסס מודל אכיפה המבוסס על קריטריונים פרסונליים, תחת הקריטריונים הטריטוריאליים. מיקומה הפיזי של הראיה הדיגיטלית אינו צריך עוד להיות הקריטריון לקביעת סמכות אכיפה או היעדרה של סמכות אכיפה. תחת זאת, אציע לבחון את מיקומו של האדם שמחזיק ומשתמש בראיה זו ואת משמעות מיקום הראיה הדיגיטלית מבחינת אותו אדם, וזאת על מנת לקבוע אם קיימת סמכות של המדינה החוקרת לאסוף את אותה ראיה דיגיטלית. מובן שיש הבדל משמעותי בין הרמה העיונית לבין הרמה המעשית. ברמה העיונית ניתן לבקר את התפישה הטריטוריאלית, כפי שעשיתי במאמר זה, וכן ניתן להציע מודל חלופי לתפישה זו בכל הנוגע לחקירה הפלילית באינטרנט, אולם ברמה המעשית, יצירת השינוי כאמור תחייב פעולה הסכמית, בין מפורשת ובין על דרך המחדל, של המדינות השונות.

ככל שהמגבלה הטריטוריאלית נפרצת בפועל על ידי המדינה החוקרת באינטרנט, ובוודאי ככל שתפותחנה הצדקות לפריצתה של המגבלה הטריטוריאלית, ייפתח שער אל דיון חשוב לא פחות בדבר גבולות הפרישה של ההגנה החוקתית שלה זכאים נחקרים וצדדים שלישיים החשופים לפגיעה בעקבות פעולת החקירה. ניתנת האמת להיאמר כי גם כיום בחקירות במרחב הפיזי מתעוררת לעתים שאלת הפרישה החוקתית,<sup>119</sup> אולם זאת בעיקר בנוגע להפעלת סמכויות חקירה פרונטאליות מול

<sup>119</sup> ראו למשל, את מאמרו של ליאב אורגר "חוקה של מי ובעבור מי? על היקף תחולתם של חוקי-היסוד" **משפט וממשל** יב 145 (2010). נקודת המוצא היא, שחוקת המדינה חלה בטריטוריה שלה בלבד. ראו: Gerald L. Neuman, *Whose Constitution?*, 100 YALE L.J. 909 (1991); GERLAD L. NEUMAN, STRANGERS TO THE CONSTITUTION: IMMIGRANTS, BORDERS U.S. AND FUNDAMENTAL LAW 3-5 (1996); אורגר, לעיל ה"ש 120, בעמ' 149-157. כן ראו: v. Verdugo-Urquidez, 494 U.S. 259 (1990). באותו מקרה אזרח מקסיקני נעצר והועבר

נחקר (מעצר, חקירה כחשוד) ולא בנוגע לסמכויות איסוף ראיות דוממות, כגון חפצים או מסמכים. ייתכן שניתן להסביר זאת בכך שבחקירה במרחב הפיזי הכלל הוא שהנחקר (החשוד או העד) והראיות החפציות הדרושות לחקירה יימצאו באותה מדינה, ואילו היוצא מן הכלל הוא שהראיות החפציות מצויות במדינה א' ואילו הנחקר מצוי במדינה ב'. נוכח כלל זה, הדיון בשאלת הפרישה של ההגנות החוקתיות

לארצות-הברית לצורך משפטו על עברות סמים, כמו גם בגין חשד לרצח סוכן DEA (Drug Enforcement Agency אמריקני. חוקרי ה-DEA קיבלו את הסכמת שלטונות מקסיקו לעריכת חיפוש בביתו. החיפוש נערך על ידם ללא צו שיפוטי. הנאשם התנגד להגשת ממצאי החיפוש לבית המשפט בארצות-הברית, בטענה שהמסמכים הושגו בניגוד להוראות התיקון הרביעי לחוקה האמריקנית, המגן מפני חיפושים ותפיסה בלתי-סבירים והמחייב הצטיידות של רשויות החקירה בצו שיפוטי. בית המשפט העליון קבע ברוב דעות, כי משטרת ארצות-הברית, כאשר היא פועלת במקסיקו, אינה כפופה לחובה החוקתית הקבועה בתיקון הרביעי לחוקה האמריקנית לקבל צו מבית משפט מבעוד מועד המסמין עריכת חיפוש. עוד על פי הפסיקה, אין נפקא מינה אם גם החוקה המקסיקנית מחייבת הצטיידות בצו חיפוש מבעוד מועד כאמור. במשפט הקנדי ראו את פרשת *Hape*, לעיל ה"ש 22. באותו מקרה שלל בית המשפט העליון הקנדי את אפשרותו של אזרח קנדי, שהואשם בעברות של הלכנת הון, לטעון לתחולת הצ'רטר הקנדי בדבר זכויות וחירויות אזרח, נגד פעולת רשויות החקירה בקנדה לאיסוף ראיות נגדו באי טורקס וקאיקוס שבקריביים, שאינם חלק מהטריטוריה הקנדית. בית המשפט נימק את ההחלטה בשני מסלולים שונים, הראשון – מסלול פנימי, והשני – מסלול חיצוני. המסלול הפנימי מתבונן על הצ'רטר הקנדי ועל קנדה עצמה, במנותק מהמדינות הזרות, וקובע כי אין לצ'רטר תחולה חוץ-טריטוריאלית. המסלול החיצוני מתבונן על השלכות תוצאה אחרת על מדינות אחרות, ומכתיב תוצאה שלפיה החלה אקסטרה טריטוריאלית של הצ'רטר יש בה כדי לפגוע בריבונותן של המדינות שבהן יוחל הצ'רטר בפועל. לחזרה על הלכה זו, ראו: *Amnesty Int'l v. Canada* (Chief of Def. Staff), [2008] F.C.R. 546 (Ca.) רבה את הלכת *Cook*, שבה נקבע כי אזרח אמריקני שנחקר על ידי חוקרים קנדים על אדמת ארצות-הברית, זכאי להגנות הצ'רטר הקנדי, אם לימים יישפט בקנדה בגין ביצוע עברה פלילית. ראו: *R. v. Cook*, [1998] 2 S.C.R. 597 (Ca.). ראו עוד: ס' 9 לאמנת מונטבידאו: *Montevideo Convention on Rights and Duties of States*, 165 L.N.T.S 19 (1933). פרט לנקודת המוצא הטריטוריאלית ניתן למצוא במשפט האמריקני כמה דוגמות להרחבות נוספות של הפרישה החוקתית אל מעבר לטריטוריה על פי מודל פונקציונלי. ראו: *Reid v. Covert*, 354 U.S. 1 (1957), שם נקבעה התחולה של החוקה האמריקנית על אזרחית מהוץ לארצות-הברית בנוגע לאישום בעברת רצח. בפסיקה מאוחרת יותר, הוחל הכלל גם על עברות קלות יותר, וראו: *Wang v. Reno*, 81 F.3d 808 (9<sup>th</sup> Cir. 1996), שם הוחלה ההגנה של התיקון החמישי לחוקה האמריקנית על אזרח ותושב סיני, שנחקר על ידי הרשויות הסיניות, והתביעה ביקשה להשמיע את עדותו בהליך משפטי אמריקני. בקנדה ראו: *Khadr v. Canada*, [2008] 2 S.C.R. 125 (2008) (הפרת זכותו של נאשם קנדי קטין, שנעצר באפגניסטן ונחקר על ידי המודיעין הקנדי במתקן המעצר במפרץ גואנטנמו בקובה, לגילוי חומר חקירה); [2010] 1 S.C.R. 44 (2010) *Khadr v. Canada*, (הפרת זכותו של אותו נאשם לחירות). חרף הרחבות אלה, קשה להצביע על כיוון ברור של שינוי פרדיגמתי ממודל טריטורינלי למודל אחר אקסטרה טריטורינלי. זו גם מסקנתו של אורגד, לעיל ה"ש 120; כן ראו: *Chimene I. Keitner, Rights Beyond Borders*, 36 YALE J. Int'l L. 55 (2011).

התמקד בנחקר עצמו, אשר מטבע הדברים נפגע באופן ישיר יותר כאשר מופעלות כלפיו סמכויות חקירה, מאשר כאשר מופעלות כלפיו סמכויות איסוף. בחקירה במרחב האינטרנטי היוצא מן הכלל הזה עשוי להפוך לכלל, ולפיו באופן טריוויאלי ביותר יכול שתתקיים הפרדה בין-מדינתית בין הנחקר לבין מקום הימצא הראיות הדיגיטליות הדרושות לחקירה. מכאן שתרכיבה הסיטואציות שבהן יעלה הצורך לבצע פעולת איסוף אקסטרה טריטוריאלית כשהיא עומדת לעצמה, ולא כפעולה נלווית לפעולות חקירה אקסטרה טריטוריאליות כלפי נחקר המצוי מחוץ לטריטוריה המדינתית.<sup>120</sup>

---

<sup>120</sup> נקודת המוצא היא שההגנה החוקתית חלה על פי הפרישה הטריטוריאלית של האינטרנט, באופן שההגנה החוקתית חלה על פעולות איסוף של המדינה החוקרת המתייחסות לראיות המצויות בטריטוריה המדינתית בלבד. ראו פרשת *Gorshkov*, לעיל ה"ש 72; *Suzlon Energy Ltd. v. Microsoft Corp.*, 2011 U.S. App. LEXIS 20018 (9<sup>th</sup> Cir. 2011).

