פרק א

מבוא

א. הצגת הנושא

אין ספק כי מרחב הסייבר (Cyberspace),[1] המכונה גם המרחב הקיברנטי או המרחב המקוון, מביא עמו פריחה ושגשוג חסרי תקדים מבחינה אישית, חברתית וכלכלית. אולם נוסף על הטוב שהוא מביא עמו, מרחב הסייבר הוא גם זירה פעילה לביצוע מגוון רחב של עברות פליליות. במרחב המקוון התוודענו לתופעות פשיעה חדשות כמו פיתוח והחדרה של וירוס מחשב,[2] חדירות לא מורשות לחומר מחשב (האקינג – hacking),[3] החדרת סוסים טרויאניים,[4] תולעים,[5]

---

1 למרחב הקיברנטי אין הגדרה אחת אחידה, אולם אפשר להיזקק להגדרה של סוכנות ה־ITU (International Telecommunication Union) במסגרת מסמך הדוגמה לחקיקה בנוגע לפשיעה קיברנטית (Toolkit for Cybercrime Legislation) מפברואר 2010, שהגדיר את המרחב הקיברנטי כך: "The physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users". ראו International Telecommunication Union, Toolkit for Cybercrime Legislation (Feb. 2010), *available at* http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf. להגדרה דומה ראו גם KLAUS W. GREWLICH, GOVERNANCE IN "CYBERSPACE" – ACCESS AND PUBLIC INTEREST IN GLOBAL COMMUNICATIONS 1 (1999). ראו גם ההגדרה של "המרחב הקיברנטי" כפי שמופיעה בהחלטת ממשלה מס' 3611 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011), אשר זו נוסחה: "'המרחב הקיברנטי' – המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה". מטבע הדברים ההתמקדות בספרי זה תהיה בעיקר באינטרנט, על מופעיו השונים (דוא"ל, אתרי Web, צ'אטים, שרתי FTP – File Transfer Protocol, שירותי "מחשוב ענן", רשתות חברתיות, אתרי שיתוף קבצים ועוד), בשל תפוצתו הגלובלית ותדירות השימוש בו. עם זאת תיתכנה תופעות פשיעה גם במסגרת רשתות מחשב סגורות, שאינן מחוברות לרשת העולמית.

2 "וירוס מחשב" הוא תוכנה המוחדרת למחשב ומבצעת שינויים בפרוצדורות, בתוכנות או במידע האגור בו, על פי הגדרה נתונה. סעיף 6 לחוק המחשבים, התשנ"ה–1995 (להלן – חוק המחשבים), שכותרו "נגיף מחשב", קובע עברה פלילית של עריכה והשתלה של וירוס מחשב.

3 להרחבה על ההיסטוריה של ההאקינג, כמו גם על מניעי הפעולה השונים שלהם, ראו למשל WINN SCHWARTAU, CYBERSHOCK: SURVIVING HACKERS, PHREAKERS, IDENTITY THIEVES, INTERNET TERRORISTS AND WEAPONS OF MASS DISRUPTION 153–272 (2000); Paul Taylor, *Hacktivism: In Search of Lost Ethics?*, *in* CRIME AND THE INTERNET 59–73 (David S. Wall ed., 2001). לבחינת תופעת התקפות ה־DDoS, מניעיה והשלכותיה, ראו למשל SUSAN BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE 1-12, 32–34 (2009).

4 "סוס טרויאני" (Trojan Horse) הוא כינוי לתוכנה תמימה למראה, המוחדרת למחשב הקרבן ומפעילה בו קוד זדוני שיכול לכלול תוכנת וירוס, או יכול לאפשר לגורם המפעיל לחדור למחשב הקרבן ללא הרשאה ולבצע בו פעולות ללא ידיעתו.

nevo.co.il

ביצוע מתקפות של Distributed Denial of Service (DDoS)[6] ושאר מרעין בישין. כן נתוודענו לעברות פליליות "ישנות" שהופיעו בלבוש חדש ומשוכלל במרחב הסייבר, למשל גנבת זהות (Identity theft) כשיטת התחזות מקוונת,[7] דיוג (phishing) כשיטת מרמה מקוונת,[8] הימורים מקוונים,[9] עברת פרסומי התועבה באינטרנט,[10] עברות של הסתה לגזענות באינטרנט,[11] גנבת

---

5 "תולעת" (Worm) היא תוכנה בעלת יכולות הרסניות כשל "וירוס", אלא שתהליך התפשטותה אינו מצריך התערבות אנושית כבמקרה של תוכנת וירוס. התולעת יודעת לנצל את הארכיטקטורה של רשתות המחשבים על מנת לשכפל את עצמה ולהתפשט אל משתמשי מחשב אחרים. התפשטות ה"תולעת" מביאה להשתלטות על רוחב פס התקשורת או על משאבי הזיכרון והמעבד של המחשב. "תולעים" מפורסמות הן ILoveYou שהופץ בשנת 2000 ונתגלה לראשונה בהונג קונג, ו־Blaster, שתקף מחשבים בעלי מערכות הפעלה של Windows באוגוסט 2003. ראו www.en.wikipedia.org/wiki/ILOVEYOU; www.en.wikipedia.org/wiki/Blaster_%28computer_worm%29.

6 מתקפות DDoS (Distributer Denial of Service) הן מתקפות וירטואליות שמטרתן לגרום לשיתוק ול"נפילה" של שרתי מחשב או אתרים מסוימים השוכנים בשרת המחשב באופן שלא יאפשר התחברות אל אותו שרת מותקף וממנו. מתקפות ה־DDoS מתבצעות באמצעות כינון רשת Master ה"מגייסת" מחשבים תמימים לפקודתה (Botnet). ה"גיוס" נעשה באמצעות חדירה לא מורשה לאותם מחשבים תמימים והשתלת תוכנה בתוכם שמאפשרת שליטה בהם והפעלה שלהם במסגרת אותה רשת Master. מפעיל רשת ה־Master מפעיל לפי הוראה את כל המחשבים המגויסים, המתקשרים אל השרת המותקף בעת ובעונה אחת באופן שמציף אותו מעבר ליכולתו הטכנית או הפיזית לקלוט התקשרויות נכנסות, ולפיכך משתק אותו. התקפות DDoS יכולות להתבצע ממניעים של הוכחת מסוגלות טכנולוגית, נקמה אישית, סחיטה כלכלית של בעלי האתר המותקף, מניעים אידאולוגיים, טרור קיברנטי ועוד. בישראל המקרה הראשון שבו הועמדו לדין מבצעי התקפות DDoS נגע להצפת שרת מרכזי בשם DalNet המשמש לכינון שיחות (צ'טים) באינטרנט. הנאשמים הורשעו בביצוע עברות של שיבוש והפרעה למחשב או לחומר מחשב, עברה על סעיף 2 לחוק המחשבים, וכן בעברות נלוות אחרות. ראו ת"פ (שלום ת"א) 5476/03 **מדינת ישראל נ' שי** (פורסם בנבו, 30.9.2004).

7 ראו למשל אלעד אורג **זכות לזהות אינפורמטיבית: עקרון משפטי חדש להגנת קיומה של זהות אינפורמטיבית ויישומו בסביבת מידע מודרני** 65–79 (חיבור לשם קבלת תואר "דוקטור למשפטים", אוניברסיטת תל־אביב, 2008); Chris J. Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J. L. & TECH. 97 (2007); לדיון בסיבות לשכיחות התופעה באינטרנט, ראו Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L. J. 1277 (2003).

8 ראו למשל Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1363 (2005). לקשר בין גנבת זהויות לבין ביצוע מזימות דיוג, ראו למשל Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259 (2005).

9 ראו למשל Bruce P. Keller, *The Game's the Same: Why Gambling in Cyberspace Violates Federal Law*, 108 YALE L.J. 1569 (1999), שם המחבר טוען כי חוקי ההימורים הפדרליים של ארצות הברית חלים על ההימורים באינטרנט. לטיעון בדבר תחולת דיני ההימורים הישראליים על ההימורים המקוונים ולהצגת הקושי הבין־מדינתי באכיפת דיני ההימורים באינטרנט, ראו חיים ויסמונסקי "הימורים באינטרנט – דין ישן וחדש" **רשימות בנתיב קנייני הרוח – השנתון למשפט, תקשורת וטכנולוגיה** 1, 291 (2004). לטיעון נגד ההצדקות להפללה של הימורים מקוונים, ראו אסף הרדוף **הפשע המקוון** 297–334 (2010). להצגת מודלים אפשריים להתמודדות עם הימורים מקוונים, ראו Aaron Craig, *Gambling on the Internet*, 1998 COMP. L. REV. & TECH. J. 61 (1998). לניתוח כלכלי של האינטרסים המשתנים בזירת ההימורים המקוונים לעומת ההימורים במרחב הפיזי, ראו Frank Vandall, *Why Are We Outraged: An Economic Analysis of Internet Gambling*, 7 RICH. J. GLOBAL L. & BUS. 291 (2008).

10 לדיון בבעיית התחולה של עברת פרסומי התועבה (obscenity) במרחב האינטרנטי, ראו Yuval Karniel & Haim Wismonsky, *Pornography, Community and the Internet – Freedom of Speech and*

מידע ממוחשב באמצעות העתקתו בלבד,[12] הפרת צווי איסור פרסום והוראות צנזורה באינטרנט[13] ועוד.

דברי ימיה של עבריינות המחשבים, ובכללה עבריינות בזירה המקוונת, כמעט מקבילים לדברי ימיהם של המחשב והאינטרנט עצמם.[14] עם הפיכתו של האינטרנט לזמין לציבור הרחב, גם הפשיעה החלה להתפשט ברשת.[15] אותה פשיעה מותירה עקבות דיגיטליות. ספר זה דן בחקירה הפלילית בנוגע לאותן עקבות.

האם המשפט מספק כלים מתאימים ונכונים להתמודדות עם פשיעת הסייבר? אם שאלה זו תיענה בשלילה, יכולות להיות לכך כמה משמעויות: ראשית, אם הכלים המשפטיים יהיו צרים מדי, הרי שיכולת האכיפה הפלילית במרחב הסייבר תיפגע, וכתוצאה מכך הביטחון הלאומי,

---

Obscenity on the Internet, 30 RUTGERS COMP. & TECH. L. J. 105 (2004). העברה של פרסומי תועבה, על פי הדין האמריקני, כמו גם על פי הדין הישראלי, היא עברה תלוית־קהילה, במובן זה שהסטנדרט הקהילתי שבו מופץ הפרסום המיני הוא שקובע אם מדובר בביטוי מותר או בעברה פלילית של פרסומי תועבה. לפיכך אין דינו של פרסום מיני בקרב קהילה שמרנית כדינו של פרסום תועבה בקרב קהילה מתירנית. במרחב האינטרנטי, שבו הפרסום יכול להגיע לכל מקום בעולם, ולכמה גולשים בו־זמנית בכמה מקומות, מתעוררת השאלה על פי איזה סטנדרט ייבחן הפרסום המיני. ראו עוד Bret Boyce, *Obscenity and Community Standards*, 33 YALE J. INT'L L. 299 (2008).

11 להרחבה על פרסומי הסתה ו־Hate Speech שהועתקו ונפוצו במרחב האינטרנטי, ראו למשל RAPHAEL COHEN-ALMAGOR, THE SCOPE OF TOLERANCE 238–263 (2006); Audrey Guinchard, *Hate Crime in Cyberspace: The Challenges of Substantive Criminal Law*, 18 INFO. & COMM. TECH. L. 201 (2009); Alexander Tsesis, *Hate in Cyberspace: Regulating Hate Speech on the Internet*, 38 SAN DIEGO L. REV. 817 (2001).

12 ראו, למשל, חיים ויסמונסקי "חסר: איסור פלילי לריגול עסקי" http://www.law.co.il/articles/criminal-law/2006/08/04/263 (2006), שם דנתי בשאלת התחולה של עברת הגניבה כהגדרתה בסעיף 383 לחוק העונשין, התשל"ז–1977, על הסיטואציה של העתקת מידע ללא ידיעת בעליו או המחזיק בו. כן ראו DAVID S. WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE 69–102 (2007).

13 ראו בעניין זה את העיסוק בפרסומי ויקיליקס (Wikileaks), אתר אינטרנט ללא מטרת רווח, שעלה לאינטרנט ב־2006 ונוהל בידי ג'וליאן אסאנג' האוסטרלי. ויקיליקס נוהג לפרסם חומרים רגישים מבחינה מדינית וצבאית הנוגעים למדינות רבות בעולם. האתר הגיע לשיא בתודעה הבין־לאומית כאשר פרסם באוקטובר 2010 כ־400,000 מסמכים מסווגים של ארצות הברית. המסמכים נגעו לפעילות צבא ארצות הברית בעיראק. בכל הנוגע למקורות של פרסומי ויקיליקס, אלה מבצעים עברות על ביטחון מדינתם. כך היה בעניינו של החייל האמריקני בראדלי מאנינג, שהורשע בהדלפת 400,000 המסמכים עובר לאוקטובר 2010. בכל הנוגע לאתר ויקיליקס עצמו ולמנהלו אסאנג', הרי שמתעוררת שאלה של פליליות כפולה ובעברות של פגיעה בסודות מדינה (המקבילות לעברות של ריגול וריגול חמור לפי סעיפים 112 ו־113 לחוק העונשין, התשל"ז–1977, החלות גם על מקבל הידיעות ולא רק על מוסרן), ניתן לומר כי סודה של מדינה א אינו סודה של מדינה ב, ואם החשוד מצוי במדינה ב ומעלה לאינטרנט פרסומים הנוגעים למדינה א, הרי שאין מתקיים בעניינו תנאי הפליליות הכפולה (dual criminality), ולפיכך אין הוא בר הסגרה למדינה א. על ההשלכות של פרשת ויקיליקס על האכיפה הפלילית של עברות מתחום של גילוי סודות מדינה, ראו Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate*, 46 HARV. C.R. – C.L. L. REV. 311 (2011); כן ראו MICAH SIFRY, WIKILEAKS AND THE AGE OF TRANSPARENCY (2011); GREG MITCHELL, THE AGE OF WIKILEAKS (2011).

14 ראו למשל את הסקירה אצל BRUCE STERLING, HACKER CRACKDOWN – LAW AND DISORDER ON THE ELECTRONIC FRONTIER (1992).

15 ראו למשל SUSAN BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 9–38 (2010).

הכלכלי והאישי במרחב הסייבר עלולים להיפגע אסטרטגית. **שנית**, אם הכלים המשפטיים יהיו רחבים מדי, משמעות הדברים היא שמערך ההגנות החוקתיות מפני פעולתה של הרשות החוקרת גם הוא עלול להיפגע פגיעה לא ראויה מאי־ההתאמה האמורה. עוד ייתכן, שהכלים המשפטיים הקיימים יימצאו רחבים מדי וצרים מדי בו־זמנית, כלומר דיני החקירה הקיימים יימצאו רחבים מדי בנקודות מסוימות וצרים מדי בנקודות אחרות, וכך החמצתו של האינטרס הציבורי בהגנה על הפעילות במרחב המקוון והחמצתו של מערך הזכויות החוקתיות הרלוונטיות לפעילות במרחב הסייבר – תתקיימנה בד בבד. לכך אתייחס בהמשך.

כפי שאראה, אכן קיימת אי־התאמה של הדינים המסדירים את החקירה הפלילית לזירה המקוונת. המחוקק הסדיר את איסוף הראיות הדיגיטליות בחקירה פלילית בשיטה תוֹסֶפתית, טלאי על טלאי, על יסוד הנחות המוצא הקיימות בדבר ראיות במרחב הפיזי. בבואי לנתח את אי־ההתאמה האמורה אחשוף שני **כשלים תפישתיים סמויים**, ולפיהם דיני החקירה מבטאים **תפישה טריטוריאלית** של סמכות המדינה לאסוף ראיות דיגיטליות בחקירה פלילית (דהיינו המדינה מוסמכת לאסוף ראיות דיגיטליות האגורות בשטחה בלבד) **ותפישה "פיזית"** של טבע הראיות הדיגיטליות (דהיינו הן נתפשות כחפצים במרחב הפיזי, בעוד בפועל היותן דיגיטליות והימצאותן במרחב הקיברנטי משנים את טבען ואת האופן שבו יש להתבונן עליהן). ארחיב מעט על שתי תפישות אלה.

1. התפישה הטריטוריאלית בדבר איסוף ראיות דיגיטליות במרחב הסייבר

כפי שאפרט בהרחבה בפרק 3, תפישה זו מורכבת משלוש הנחות מצטברות: **האחת**, כי הראיה הדיגיטלית ניתנת למיקום במרחב המקוון; **השנייה**, כי המקום של הראיה הדיגיטלית הוא בשרת המחשב שבו היא אגורה או עוברת; **השלישית**, כי אם שרת המחשב שבו אגורה הראיה הדיגיטלית מצוי פיזית מחוץ לתחומי המדינה החוקרת, הרי שאין למדינה סמכות המאפשרת לאסוף את הראיה בעצמה. כפי שאטען, ניתן לתקוף כל אחת משלוש הנחות אלו.

אשר לשתי ההנחות הראשונות אציע טיעוני־נגד **ארכיטקטוניים־טכנולוגיים** (שלפיהם מרחב הסייבר, ובייחוד האינטרנט, מבוסס על ביזוריות ועל ניידות של המידע המצוי בו, כתובת האינטרנט אינה קבועה, ולעתים יש העתקה של המידע ממקום למקום מטעמים של ויסות עומסי הרשת) **ואפיסטמולוגיים** (שלפיהם למיקומו של המידע לרוב אין משמעות מבחינת מי שמאחסן אותו, מציג אותו או צורך אותו). אשר להנחה השלישית, שעניינה במגבלת הסמכות האכיפתית (Jurisdiction to Enforce)[16] של המדינה כלפי ראיות האגורות מחוץ לשטחה הריבוני, אציע

16 כפי שאראה בפרק 3, מקובלת ההבחנה בין שלושה סוגים של סמכות של המדינה: (א) Jurisdiction to Prescribe – החלת הדין המהותי המדינתי על המקרה הנדון; (ב) Jurisdiction to Adjudicate – שיפוט בבית המשפט המדינתי של המקרה הנדון; (ג) Jurisdiction to Enforce – אכיפה של המקרה הנדון בידי המדינה וסוכניה. הבחנה זו מופיעה ב־RESTATEMENT OF THE LAW (3rd) OF FOREIGN RELATIONS LAW OF THE UNITED STATES (2009). כן ראו, בהקשר של כתיבה על סמכות שיפוט באינטרנט, את ההבחנה כפי שהיא מופיעה אצל ברנר וקופס: Susan W. Brenner & Bert-Jaap Koops, *Cybercrime Jurisdiction – An Introduction*, *in* CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY 1–7 (Bert-Jaap Koops & Susan W. Brenner eds., 2008). ראו עוד Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1 (2004). בדיון שאערוך אתמקד ב־Jurisdiction to Enforce. הסמכות האכיפתית כוללת כללים בנוגע למעצר חשודים בחו"ל, הסגרתם

בחינה ביקורתית של המונח ושל הכלל המגביל סמכות זו של המדינה. אבחן את שורשי המגבלה ואת ההצדקות לה ואראה כי הצדקותיה אינן חלות באותה עצמה במסגרת חקירה פלילית במרחב המקוון. אראה כי הסמכות האכיפתית במרחב הפיזי מקבילה לטריטוריה של המדינה, וריבונות המדינה אף היא מתוחמת לטריטוריה שלה. יש אפוא חפיפה בין המושגים של ריבונות, טריטוריה וסמכות (חקיקתית, שיפוטית וחקירתית), וחפיפה זו הועתקה גם לזירה המקוונת.[17] כפי שאראה, קירוב העדשה אל הסמכות החקירתית הבין־לאומית מלמדנו כי הגם שהכלל נתפס כחלק מהמשפט הבין־לאומי המנהגי, והגם שיש לו ביטויים בחוקים הפנימיים של המדינות, בפועל יש זליגות הולכות וגדלות מכלל זה הן בעולם הפיזי והן בעולם המקוון. זליגות אלה אינן נובעות משינוי בפרדיגמה הטריטוריאלית של הסמכות החקירתית, אבל הן מעידות על הצורך המעשי ההולך וגובר לסטות ממנה. הקול החלוצי שקרא במפורש, מטעמים מעשיים, לפרוץ את המחסום של הסמכות החקירתית הבין־לאומית באשר לראיות דיגיטליות במרחב המקוון היה קולו של ג׳ק גולדסמית׳ (Goldsmith).[18] בספרי אבקש להצטרף אל האמירה הזאת של גולדסמית׳, תוך מתן הצדקות נורמטיביות ומעשיות (הקשורות בארכיטקטורת המרחב המקוון) לדברים.

2. התפישה הפיזית בדבר איסוף ראיות דיגיטליות במרחב הסייבר

נוסף על התפישה הטריטוריאלית, הדין הקיים מגלם גם תפישה פיזית בדבר הראיות הדיגיטליות. התפישה הפיזית מגלמת כמה הנחות באשר לאופייה של הראיה הדיגיטלית: **האחת**, הראיה מיוצגת באופן פיזי־חפצי (באטומים); **השנייה**, תוכנה של הראיה ומשמעותה אינם

ממדינה למדינה, אכיפת סגר ימי ועוד כהנה וכהנה סוגיות אשר בהן לא אעסוק. בתוך קטגוריה זו אתמקד בסמכות אכיפתית שנוגעת לשלב החקירה הפלילית ואיסוף הראיות במסגרתה, ועל כן אגזור מתוך הסמכות האכיפתית עיקרון מצומצם יותר שאותו אכנה ״סמכות חקירתית״, כשהכוונה היא לסמכות חקירתית אקסטרה־טריטוריאלית.

17 ראו האמנה האירופית למניעת פשעי מחשב Council of Europe Convention on Cybercrime, (Budapest, 2001), שממנה נובע כי נדרש ככלל שיתוף פעולה בין מדינות לצורך ביצוע פעולות חקירה אקסטרה־טריטוריאליות. כן ניתן ללמוד על הנחת המוצא הטריטוריאלית באינטרנט במדינות המערב מעיון בסקירה המופיעה אצל: GRAHAM J. H. SMITH, INTERNET LAW AND REGULATION 241–366 (3rd ed., 2002). באותו ספר עולה כי מרבית מדינות המערב יוצאות מהנחה כי מותר להן להסדיר את הפעילות האינטרנטית המתקיימת פיזית בשטחן בלבד.

18 ראו Jack Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. OF CHI. LEG. FORUM 103 (2001). באותה עת פורסם מאמרה של פטריציה בליה (Bellia), שבחנה את האפשרות להכיר בחיפושים אקסטרה־טריטוריאליים במחשב ושללה זאת. ראו Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL. F. 35 (2001). שני המאמרים נכתבו בהשראת פרשת *Gorshkov-Ivano*. באותו מקרה דובר על חקירה פלילית אמריקנית נגד שני האקרים רוסים שפעלו מרוסיה. במסגרת החקירה העתיקו חוקרי ה־FBI בהעתקה סמויה חומר מחשב שהיה אגור בשרתי מחשב רוסיים, וזאת על דרך של התקשרות ממחשב בארצות הברית לשרת הרוסי. לאחר מכן ניגשו חוקרי ה־FBI לבית משפט אמריקני וביקשו צו לעיון בחומר שהועתק כאמור. לימים הורשעו שני ההאקרים בבית משפט אמריקני בביצוע עברות מחשב. במקביל העמידו הרשויות ברוסיה לדין את אחד מחוקרי ה־FBI ודרשו פעמיים את הסגרתו לרוסיה, אך האמריקנים לא כיבדו דרישתם זו. ראו United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001); United States v. Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001). ראו הרחבה להלן בפרק 3(ד)(4).

nevo.co.il

נפרדים מן החפץ הפיזי שבו הם מיוצגים; **השלישית**, הראיה אינה ניתנת להעתקה, ומכאן שהיא בת־תפיסה בלבד; **הרביעית**, השימוש בראיה תלוי בהחזקתו בפועל פיזית בתוספת שליטה אפקטיבית בו. הנחות אלה אינן מתקיימות כשמדובר בראיות הדיגיטליות במרחב המקוון: ראיות אלה מורכבת מסיביות (ביטים) ולא מאטומים;[19] הן ניתנות להעתקה באופן המייצר העתק הזהה למקור; המידע מנותק פיזית מאת המשתמש בו,[20] והוא מבוזר ומוחזק בידי ספקי שירות שונים; המידע ניתן לאחזור ולכרייה באמצעים ממוחשבים; הוא מצטבר וניתן לאגירה; עם זאת הוא נדיף ופגיע; המידע אף ניתן להצפנה ולהסוואה בנקל. התפישה הפיזית מביאה לכך שעיקר תשומת הלב החקיקתית והשיפוטית מוקדשת לפעולות החקירה הפיזיות כלפי הראיות – כניסה לחצרים, תפיסת המחשב והעתקת חומר המחשב – ופחות לשלבי העיון במידע, לכרייתו או לעיבודו. במילים אחרות, התפישה הפיזית מביאה להדגשת שלבי הלוואי של איסוף הראיות הדיגיטליות ולא של השלב המהותי.

3. על מטאפורות ואנלוגיות בשירות התפישה הטריטוריאלית והתפישה הפיזית

כפי שאראה בפירוט, ניתן ללמוד על התפישות הללו מקריאה מודרכת של לשון החוק, תוך בחינת ההיסטוריה החקיקתית, אשר הרכיבה על האדנים המשפטיים הקיימים את המאטריה המשפטית החדשה. יתרה מזאת, ניתן להבחין בשימוש תדיר **במטאפורות ובאנלוגיות מן העולם הפיזי** בבוא "עושי המשפט" (מחוקקים, שופטים, עורכי דין) לנתח את הסוגיות המשפטיות שמעורר עולם הסייבר. מטאפורות ואנלוגיות אלה משפיעות על האופן שבו מוּחל הדין על מרחב הסייבר ומביאות להחמצתה של מהות הראיות הדיגיטליות, ואפרט על אודותיהן במהלך הדיון. לעת הזאת אציין כי המטאפורה המוכרת מכולן, הצריכה לענייננו, היא מטאפורת המרחב הקיברנטי כ"מקום" (Cyberspace as a place). מטאפורה זו מבטאת תפישה פיזית וטריטוריאלית באשר לראיות הדיגיטליות, כי אם המרחב המקוון הוא מקום, אזי הראיות שבו ניתנות למיקום, וככאלה הן משולות לאטומים יותר מאשר לביטים. דן האנטר (Hunter) עמד על השימוש במטאפורה זו וגרס כי היא שגויה.[21] בהתייחסותו ניכרת תפישה דטרמיניסטית באשר לשימוש במטאפורה זו. לעומתו, מרק למלי (Lemley) הציע לפתח חשיבה ביקורתית על המטאפורה של האינטרנט כ"מקום", להאיר את מגבלותיה ובכך להיטיב את הפרספקטיבה המשפטית על המרחב המקוון.[22] גם למלי גרס כי המטאפורה של האינטרנט כ"מקום" היא שגויה ביסודה

---

19 ראו ניקולאס נגרופונטי **להיות דיגיטלי** 17–25 (עמנואל לוטם מתרגם, 1996).

20 ראו FRANCIS CAIRNCROSS, THE DEATH OF DISTANCE – HOW THE COMMUNICATIONS REVOLUTION IS CHANGING OUR LIVES 75–98 (2001); Daniel E. Geer, *The Physics of Digital Law: Searching for Counterintuitive Analogies*, *in* Cybercrime – Digital Cops and Laws in a Networked Environment 13 (Jack M. Balkin et al. eds., 2007).

21 ראו Dan Hunter, *Cyberspace as a Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003). לטענת האנטר, מטאפורת ה"מקום" באינטרנט שגויה, כיוון שהיא תביא לכך שכל אחד ימנע מאחרים את השימוש ב"מקום" שלו באינטרנט, וכך למעשה יימנע כל שימוש באינטרנט כמשאב ציבורי. עוד על מטאפורת ה"מקום" באינטרנט, ראו אברהם נ' טננבוים "על המטאפורות בדיני המחשבים והאינטרנט" **שערי משפט** ד 359, 362–375 (2006).

22 ראו Mark Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003).

ומביאה להחמצת ההתייחסות המשפטית הראויה לאינטרנט (הגם שכמו האנטר לא התייחס מפורשות לחקירה פלילית במרחב המקוון). ג'ולי כהן (Cohen) ביקשה להצדיק את תפישת המרחב הקיברנטי כ"מקום". לטענתה, המרחב הקיברנטי אינו "מקום" שונה מן העולם הפיזי, ומכאן שהכתרתו כ"מקום" אינה שגויה. לדידה, המטאפורה השגויה היא מטאפורת המרחב המקוון כ־"Cyberspace".[23] מטאפורת ה־cyberspace מעודדת התייחסות, שגויה לטענתה, אל העולם המקוון כמציאות נפרדת.[24] כעולה מטיעונה של כהן באשר ליחס שבין מטאפורת ה"מקום" לבין מטאפורת "cyberspace", לעתים כמה מטאפורות "מתחרות" ביניהן על התיאור ההולם יותר את השאלה המשפטית או את התופעה החברתית־טכנולוגית החדשה.[25]

לצד מטאפורת האינטרנט כ"מקום" אצביע על אנלוגיות ספציפיות לדיני האיסוף של ראיות דיגיטליות, כגון אנלוגיית ה"חיפוש" במחשב ו"תפיסה" (seizure) של חומר המחשב, ואטען כי אנלוגיות אלה משעתקות את הקונספצייה הטריטוריאלית והפיזית אל הסביבה המקוונת. אם כך הוא, הרי שהמטאפורות, שנועדו לשרת את התודעה ולגשר בינה לבין המציאות, מסבות נזק לאופן שבו המשפט מתמודד עם הטכנולוגיה.

4. ההחמצה הדו־כיוונית הנובעת מהתפישה הטריטוריאלית ומהתפישה הפיזית

התפישה הטריטוריאלית והתפישה הפיזית באשר לאיסוף הראיות בחקירה פלילית במרחב הסייבר מביאות לכך שדיני איסוף הראיות הדיגיטליות מחטיאים את מטרתם המרכזית, שהיא יצירת מנגנון אפקטיבי לחשיפת עברות פליליות ועבריינים, תוך הקפדה על הזכויות החוקתיות של הנוגעים בדבר: הן משתמש המחשב הפרטי, הן התאגידים הפועלים במרחב הסייבר, שהם מה שאכנה "שחקני הציר" של המרחב, והן כלל ציבור משתמשי המחשב והאינטרנט. ההחמצה הקונספטואלית באשר לדיני איסוף ראיות במרחב הסייבר היא דו־כיוונית: מן העבר האחד נפגעת האפשרות להכיר בסמכויות הנדרשות לאיסוף ראיות בזירה המקוונת. כך, לשם המחשה בשלב זה בלבד, האינטרנט עשוי לעורר צורך חקירתי להכיר בסמכות לביצוע פעולות של חדירה לחומר מחשב באמצעות התקשרות מרחוק, לרבות חדירה לחומר מחשב האגור מחוץ

---

23 ראו Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007).

24 מטאפורת ה־"cyberspace" הובילה לניסיון להקביל את דיני האינטרנט לדיני החלל החיצון ולהחיל את העקרונות שבאמנות הבין־לאומיות העוסקות בחלל החיצון על דיני האינטרנט. ראו Anna Maria Balsano, *An International Legal Instrument for Cybersapce? A Comparative Analysis With the Law of Outer Space*, *in* THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 127 (2000).

25 עוד על התחרות האמורה, ראו Alfred C. Yen, *Western Frontier on Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207 (2002). דוגמה נוספת ל"תחרות" מושגית שכזו מביא מייקל פרומקין (Froomkin) באשר להצפנת חומרי מחשב. מצד אחד, לא אחת מושווית הסיטואציה של שליחת מסרים מוצפנים ל"רכב" או ל"שפה", ואילו עריכת הקובץ המוצפן ואחסנתו במחשב משולה ל"בית" או ל"כספת". בחירת המטאפורה משליכה רבות, הסביר פרומקין, על מידת ההגנה שתינתן לחומרי מחשב מוצפנים: השוואה לרכב תביא להענקת הגנה במידה פחותה, ואילו השוואה לבית תביא להענקת הגנה חוקתית ברמה גבוהה למידע המוצפן. ראו A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 859–882 (1995).

לטריטוריה של המדינה. כן עשוי להתעורר, כדוגמה נוספת, צורך להכיר בפעולות שונות של שימור או הקפאת מידע בשל תכונת הנדיפות של הראיה הדיגיטלית.

מן העבר השני, הדיון החוקתי המתחייב כנגד פעולת הרשות החוקרת במרחב הסייבר מוחמץ אף הוא בשל הכשלים הקונספטואליים האמורים. בהקשר זה ניתן להצביע על שלושה ממדים של החמצה:

1) ממד השחקנים הזכאים ליהנות מן ההגנות החוקתיות באשר לפעולות האיסוף שבהן מדובר. בשל תכונת הקישוריות (connectivity)[26] ופוטנציאל האגירה של המידע הדיגיטלי[27] ובשל ארכיטקטורת המרחב המקוון המבוססת על ספקי שירות שונים (תוכן, גישה, פלטפורמות לפרסום תכנים ושיתוף קבצים ועוד), נראה כי פעולות איסוף ראיות דיגיטליות בידי הרשות החוקרת עשויות להשפיע על קבוצה מגוונת של "שחקנים", מעבר ליעד פעולת האיסוף עצמו: צדדים שלישיים הבאים במגע עם החשוד (והאינטראקציות שלהם אגורות במחשב); ספקי השירות לסוגיהם השונים; ציבור משתמשי המחשב והאינטרנט בכללותו (או חלקים ממנו, כגון קהילות וירטואליות). יש לבחון את מידת ההגנה החוקתית שיש להעניק לכל אחד מה"שחקנים" האמורים.

2) ממד הפריסה הטריטוריאלית של הזכויות החוקתיות. היות שהמידע במרחב הסייבר אינו צמוד לגבולות מדיניים ברורים, הרי שפעולות איסוף ראיות במרחב זה יכולות להיות בעלות השפעה על מי שאינם תושבי המדינה החוקרת. במקרה כזה, בד בבד עם שאלת מקור הסמכות של הרשות החוקרת לאסוף ראיות באופן חוצה־גבולות מדיניים, מתעוררת שאלה מורכבת בדבר מודל התחולה של הזכויות החוקתיות: האם המדינה החוקרת צריכה להחיל את משפטה החוקתי על כל מושאי החקירה והמושפעים ממנה, או שמא רק על המצויים בשטחה? לחלופין, האם היא צריכה לייבא את המשפט החוקתי של המדינות הזרות שבהן מצויים כל מושאי החקירה והמושפעים ממנה? לחלופי חלופין, האם יש לקבוע מודל חוקתי גלובלי לפעולות בעלות אופי חוצה־גבולות?

---

26 הקישוריות ברשת נמצאת במצב מתמיד של התפשטות בשל הנגשת האינטרנט לעוד מקומות בעולם, הנגשת האינטרנט למכשירים ניידים שונים (מחשבי Laptop, טלפונים סלולריים ועוד), הוזלת מחירי המחשב ומחירי הגלישה באינטרנט ועוד. רוברט מטקאלף (Metcalf), ממציא טכנולוגיית ה־ethernet לתקשורת נתונים ברשתות מחשבים מקומיות (LAN), הראה באמצעות נוסחה מתמטית פשוטה את הכדאיות הכלכלית שבהתפשטות הקישוריות. על פי החוק של מטקאלף, שווייה של הרשת פרופורציונלי למספר המקושרים ברשת על פי הנוסחה הפשוטה: n X (n-1), כאשר n מייצג את מספר המקושרים ברשת. לחוק של מטקאלף ראו למשל CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 184 (1999).

27 אגירת המידע הממוחשב הלכה והוזלה עם השנים. ידוע בתחום המדע הפופולרי ה"חוק" שניסח גורדון מוּר (Moore), ממייסדי חברת אינטל, ולפיו כל שנתיים ניתן להכפיל את מספר הטרנזיסטורים על גבי מעגל אלקטרוני נתון, משמע שכל שנתיים עלויות הייצור של מעבד של מחשב מוזלת בחצי, או שכל שנתיים מואצת פי שניים מהירות העיבוד של המחשב בלא שמתייקרת העלות הכספית. ראו Gordon E. Moore, *Cramming More Components Onto Integrated Circuits*, 4 ELECTRONICS MAGAZINE 1 (1965).

3) ממד טיב הזכויות החוקתיות הנוגעות בסיטואציה החקירתית. התפישה הפיזית הביאה למיקוד הדיון במובנים מסוימים בלבד של הזכות לפרטיות של החשוד,[28] ובמובנים מסוימים גם בזכות הקניין שלו או של צדדים שלישיים הנפגעת אם הרשות החוקרת תופסת ראיה חפצית בעלת ערך.[29] כפי שאטען, איסוף ראיות דיגיטליות בידי הרשות החוקרת מחייב עיון מחדש במערך הזכויות הניצבות כנגד האינטרס החקירתי, על טיבן והיקפן. בכל הנוגע לזכות לפרטיות, אראה כי ההשתחררות מן התפישה הפיזית מאפשרת התחשבות במלוא מובניה של הזכות לפרטיות בהקשר של איסוף ראיות בחקירה פלילית במרחב הסייבר. כן אראה כיצד בשל התפתחויות טכנולוגיות ביכולות איסוף הראיות הדיגיטליות במרחב הסייבר, עצמת הפגיעה בפרטיות משתנה לעומת המרחב הפיזי, הן במובן של היקפי המידע שהרשות החוקרת יכולה לאסוף, הן במובן של איכות המיצוי של המידע הרלוונטי לחקירה והן במובן של מספר הנפגעים בפוטנצייה מהפעולה החקירתית (בשל תכונת הקישוריות של האינטרנט). בכל הנוגע לזכות הקניין, גם כאן יש לפתח את ההגנה החוקתית באופן שתתמודד עם מאפייני הראיה הדיגיטלית בשונה מההתמודדות עם מאפייני הראיה הפיזית. נוסף על הזכות לפרטיות ועל זכות הקניין אראה כי יש מקום להתחשב באגד של עוד זכויות חוקתיות: חופש העיסוק, הזכות לאנונימיות / פסידונימיות, זכות להליך הוגן וחובת תיעוד הנגזרת ממנה.

על רקע האמור, שאלת היסוד של הספר היא זו: **מהו המודל הראוי לדיני איסוף הראיות במסגרת חקירה פלילית בזירת הסייבר?** לפי המודל הנוהג כיום בדבר איסוף ראיות דיגיטליות בחקירה פלילית במרחב הסייבר, המבוסס כאמור על הנחות מוצא שגויות של טריטוריאליות ופיזיות, אציע את המודל הפרסונלי: מודל חלופי באשר לאופן שבו יהיה על המדינה לאסוף ראיות דיגיטליות בחקירה פלילית, וממודל זה יהיה ניתן לגזור הסדרים דוקטרינריים מפורטים. על פי הצעתי, הדגש יוסט מהראיה הדיגיטלית, כציר המארגן של דיני איסוף הראיות, אל הפרטים הנוגעים לחקירה (החשוד, צדדים שלישיים שבאו עמו במגע, הציבור הרחב). כך, שאלת "מיקומה" הטריטוריאלי של הראיה הדיגיטלית וזיהוי המחשב שבו היא אגורה יאבדו מחשיבותם המכרעת. השאלות המהותיות יותר, של סוגם ועצמתם של האינטרסים והזכויות של החשוד ושל צדדים שלישיים המגולמים בראיה הדיגיטלית, תיטולנה את הבכורה.

---

28 ראו למשל Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 560–561 (2005); הרדוף, לעיל ה"ש 9, בעמ' 275–288. הזכות לפרטיות מפני התערבות רשויות החקירה מעוגנת בתיקון הרביעי לחוקה האמריקנית, אשר נוסחו הוא "פיזי": התיקון עוסק בביתו של אדם, בדרישה לתאר את המקום שבו מחפשים, בהכרח לפרט את הפריטים שמבקשים לתפסם וכד'. הפסיקה האמריקנית, בקצב אטי, מתחה את גבולות הגנת הפרטיות החפצית־הפיזית לסיטואציות טכנולוגיות חדשות. בפרשת Olmstead v. United States, 277 U.S. 438 (1928) קבע בית המשפט העליון כי התיקון הרביעי אינו חל על האזנת סתר. רק כעבור כמעט 40 שנה נהפכה ההלכה. ראו Katz v. United States, 389 U.S. 347 (1967). בשנת 2001 הוחל התיקון הרביעי לחוקה על הסיטואציה שבה הרשות החוקרת הפעילה ציוד שיקוף תרמי מן הרחוב אל עבר ביתו של חשוד בגידול מריחואנה (החום הנפלט מהבית היה יכול להעיד אם מדובר במקום שמצויות בו חממות לגידול הסם). ראו Kyllo v. United States, 533 U.S. 27 (2001).

29 ראו Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2 (2008).

ב. הגדרתה של סמכות איסוף ראיות במסגרת חקירה פלילית במרחב הסייבר

כאמור, עניינו כאן בתחום האיסוף של ראיות דיגיטליות במרחב הסייבר. ההתמקדות היא בפעולותיה של הרשות החוקרת – המשטרה או גופי חקירה אחרים. לצורך חידודה והבהרתה של משמעות המונח "סמכויות האיסוף" אציע הבחנה בין שלוש סמכויות נפרדות מבחינה עיונית: (א) **סמכויות חקירה**; (ב) **סמכויות איסוף**; (ג) **סמכויות ביטחון**.

בקטגוריית סמכויות החקירה נכללות התשאול, גביית ההודעות מחשודים לאחר אזהרה, קבלת תלונות ממתלוננים, גביית הודעות מעדים, עריכת עימותים, מסדרי זיהוי, שחזורים, הובלות והצבעות, מעצר, עיכוב ותיעוד החקירה במצלמה. המשותף לכל אלה הוא כי מדובר בפעולות הנוגעות לקבלת מידע מעדים ומחשודים ולאופן ההתנהלות בעניינם. סמכויות החקירה נוגעות לשלב הגלוי של החקירה, רובן מתבצעות פנים אל פנים, ועיקר העיסוק של המשפט הוא בהן ובתוצאותיהן.[30]

קטגוריית סמכויות האיסוף, אשר בה מתמקד הדיון בספר זה, מתייחסת לכל אמצעי החקירה המגלמים פגיעה בזכויות מוגנות, המוקנים לרשות החוקרת, מלבד ההתמודדות הפרונטלית עם החשודים ועם העדים. סמכויות האיסוף מכוונות כלפי מסמכים, מידע, מוצגים וכיוצא באלה פריטים ונתונים דוממים. סמכויות האיסוף מופעלות לרוב בשלב הסמוי של החקירה או מיד עם פתיחתה של החקירה הגלויה. ניתן ליצור טקסונומיה של סמכויות האיסוף על פי חמישה פרמטרים כדלקמן: **הראשון**, הבחנה בין פעולות איסוף שמבצעת **הרשות החוקרת** בעצמה לעומת פעולות איסוף שמבצע **אדם אחר** המצווה למסור את הראיה שבחזקתו אל הרשות החוקרת; **השני**, הבחנה בין פעולות איסוף בעלות אופי **כללי**, שאינן תלויות בחקירה פלילית ספציפית, ומכאן שאינן תלויות בקיומו של חשד,[31] לבין פעולות איסוף בעלות אופי **פרטיקולרי** המתבצעות אד הוק עם התעוררות צורך חקירתי וחשד קונקרטי במקרה נתון; **השלישי**, הבחנה בין פעולות איסוף המבוצעות **בידיעת החשוד** לבין פעולות איסוף **הסמויות** מפניו; **הרביעי**, הבחנה בין פעולות איסוף בנוגע לחומרים **המצויים בטריטוריה** של המדינה החוקרת לבין פעולות בנוגע לחומרים המצויים מחוץ **לטריטוריה**. **החמישי**, הבחנה בין שלושה: בין **תפיסה (seizure) של ראיה קיימת** (בין שהתפיסה היא בידי הרשות החוקרת עצמה ובין שהיא מתבצעת לאחר המצאה מידי המחזיק לרשות החוקרת) ל**תפיסה של ראיה העתידה להיאגר** במקום

---

30 ראו בעניין זה יורם שחר "סדר דין פלילי" **ספר השנה של המשפט בישראל** 375 (אריאל רוזן־צבי עורך, 1993).

31 הכוונה בפעולות איסוף כלליות היא לאיסוף ראיות קולקטיבי, הנועד להכין עתודה של נתוני מידע חשובים שמהם תוכל הרשות החוקרת לדלות בבוא העת את הדרוש לה לצורך הוכחת ביצוע עברה מסוימת והוכחת זהותו של מבצע העברה. פעולות האיסוף שבקבוצה זו תזכינה לביקורת מוגברת היות שהן מחריפות במיוחד את תחושת המעקב השלטוני אחרי האזרחים הנורמטיביים ויוצרות אפקט פן־אופטיקוני מצנן על פעילות משתמשי המחשב והאינטרנט. על הפן־אופטיקון כתב במקור ג'רמי בנת'האם (Bentham) JEREMY BENTHAM, THE PANOPTICON WRITINGS 29–95 (Miran Bozovic ed., 1995). ראו גם MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (1975), שם חוזר פוקו אל המודל הארכיטקטוני של הפן־אופקטיקון ומתאר כיצד פוטנציאל הצפייה של הסוהרים בהתנהלות האסירים (גם אם בפועל מגדל השמירה אינו מאוכלס כל העת בסוהרים) מחזקת את ה־Discipline של האסירים.

איסופה המיועד ליצירת **תיעוד** של פעולה מסוימת, אשר ברגיל לא הייתה מותירה עקבות. מכפלת כל הפרמטרים האמורים מייצרת 48 פעולות איסוף טיפוסיות.

יש לציין כי הפרמטרים הללו מגדירים את פעולות האיסוף השונות ומבחינים ביניהן בהתייחס לטיב הפעולה שהרשות החוקרת מבקשת, ולא בהתייחס לטיב השיקולים הרלוונטיים לצורך איזון חוקתי טרם מתן ההסמכה לביצוע הפעולה החקירתית. כמו כן אין התחשבות בשיקול מאזן נוסף של כיבוד ריבונותן של מדינות זרות. במילים אחרות, הטקסונומיה הזאת אינה מתיימרת למצות את מכלול השיקולים הצריכים לעניין בבוא המחוקק או השופט לבחון את פעולת האיסוף המבוקשת (בין ברמה העקרונית, של עצם ההכרה בסמכות האיסוף האמורה, ובין ברמה הקונקרטית, של אישור השימוש בסמכות במקרה נתון). היא ממפה את מכלול פעולות איסוף הראיות הקיימות בארסנל הרעיוני לצדה של הרשות החוקרת.

הקטגוריה השלישית שמניתי לעיל היא הקטגוריה של **סמכויות ביטחון**, דהיינו סמכויותיה של המדינה לבצע פעולות של איסוף מידע במסגרת הגנה על ביטחון המדינה. להבדיל משתי הקטגוריות הקודמות שמניתי – חקירה ואיסוף – שעניינן בהעמדה לדין פלילי ובאיסוף ראיות קבילות להגשה בבית המשפט, מטרת־העל של הפעלת סמכויות הביטחון היא סיכול פעילות העלולה לפגוע בביטחון המדינה.[32] במדינת ישראל חלק ניכר מסמכויות הביטחון אינו מוסדר עלי חוק, וחלקן נלמדות מהסמכות השיורית של הממשלה, המעוגנת בסעיף 32 לחוק־יסוד: הממשלה,[33] או מהוראת הפטור של חוק הגנת הפרטיות.[34] גם החקיקה המסדירה את פעולת שירות הביטחון הכללי נותרה כללית למדי באופייה בכל הנוגע לסמכויות המוענקות לעובדיו.[35] בארצות הברית למשל יש הסדרה חוקית מפורטת יותר של סמכויות האיסוף למטרות ביטחוניות של מניעת ריגול וטרור.[36] כך או כך, פעילות ביטחונית מטבעה אינה תחומה לגבולות המדינה,[37] וממילא גלומה בה פגיעה אפשרית בריבונותן של מדינות זרות.[38] פגיעה זו היא לשם הגנה על אינטרסים של המדינה עצמה אל מול איומים הנתפסים כמסכנים את ריבונותה.

---

32 אם בעקבות הפעלת סמכויות הביטחון ייתפס מבצע עברה והמדינה תבקש להעמידו לדין, יהיה עליה להפעיל סמכויות חקירה ואיסוף, שאם לא כן, לא יהיו ברשותה ראיות קבילות הניתנות לחשיפה בפני ההגנה ובפני בית המשפט. הפעלת סמכויות הביטחון תיחסה על פי רוב מטעמי ביטחון המדינה, לפי סעיף 44 לפקודת הראיות.

33 זו לשונו של סעיף 32: "הממשלה מוסמכת לעשות בשם המדינה, בכפוף לכל דין, כל פעולה שעשייתה אינה מוטלת בדין על רשות אחרת".

34 זו לשונו של סעיף 19(ב) לחוק הגנת הפרטיות, התשמ"א–1981: "רשות בטחון, או מי שנמנה עם עובדיה או פועל מטעמה, לא ישאו באחריות לפי חוק זה על פגיעה שנעשתה באופן סביר במסגרת תפקידם ולשם מילויו". "רשות בטחון", על פי סעיף 19(ג) לחוק הגנת הפרטיות, כוללת גם את אגף המודיעין בצה"ל, שירות הביטחון הכללי והמוסד למודיעין ולתפקידים מיוחדים.

35 ראו למשל את סעיף 8(א)(1) לחוק שירות הביטחון הכללי, התשס"ב–2002, המסמיך את השירות "לקבל ולאסוף מידע".

36 ראו למשל את ה־Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801–1885.

37 ראו למשל את הגדרת תפקידיו של המוסד למודיעין ותפקידים מיוחדים מחוץ לגבולות המדינה כמפורט באתר הבית של המוסד: http://www.mossad.gov.il/AboutTheMossad.aspx.

38 דומה כי ניתן לומר שאחת מהתכונות המגדירות את סמכויות הביטחון של המדינה היא תכונת האקסטרה־טריטוריאליות, במובן של פעולה מעשית או השפעה אפקטיבית גם מחוץ לטריטוריה של המדינה. גם הכתיבה הביקורתית על סמכויות הביטחון של המדינה, לרבות על הפעלת סמכויות אלה במרחב האינטרנטי, מניחה כמובן מאליו שהסמכויות תופעלנה או תשפענה גם מחוץ לטריטוריה

לא כך הוא בכל הנוגע לחקירה פלילית. החקירה הפלילית תחומה, כפי שראה בהרחבה, במגבלות של טריטוריאליות, ופעולת חקירה מחוץ לגבולות המדינה מחייבת עזרה משפטית בין מדינות או הסכמה של המדינה הזרה לביצועה הפעולה בידי המדינה החוקרת. הפעולות הביטחוניות מחוץ לגבולות המדינה הן בבחינת היוצא מן הכלל המעיד על הכלל, שלפיו המדינה תפעיל את סמכויותיה, לרבות סמכויות החקירה והאיסוף שלה, בתוך גבולותיה בלבד. כאשר אבקש, בהמשך הדיון, לערער על התפישה הטריטוריאלית, כפי שהיא חולשת כיום על החקירה הפלילית במרחב הסייבר, הרי שאעשה זאת תוך הישענות על מאפיינים ייחודיים של החקירה במרחב הסייבר, ולא מתוך ערעור על המוסכמה כי ככלל על מדינות לערוך חקירות פליליות בתוך שטחן שלהן בלבד. במילים אחרות, איני מבקש להשוות או לקרב את סמכויות האיסוף לסמכויות הביטחון של המדינה, אלא להציע התבוננות על החקירה הפלילית במרחב הסייבר כחקירה שאינה תמיד אקסטרה־טריטוריאלית במהותה, ומכאן שאין הצדקה להגבילה לראיות האגורות בשטחה של המדינה החוקרת בלבד.

לסיכום נקודה זו, ענייני אפוא הוא בסמכויות **האיסוף** של ראיות דיגיטליות במסגרת חקירה פלילית, כאשר זו מתבצעת לצורך איתור עברות או עבריינים הפועלים במרחב הסייבר.

ג. סיווג עברות פליליות במרחב הסייבר

התעכבתי לעיל על המונח "סמכויות איסוף", ועתה יש להתעכב מעט על מושא החקירה הפלילית, קרי על העברות הפליליות במרחב הסייבר. מהן העברות הפליליות שייכללו במסגרת הדיון? מקובל לסווג את העברות הפליליות במרחב הסייבר לעברות **נגד** המחשב וחומר המחשב (התוכנות או המידע שבמחשב) ולעברות **באמצעות** המחשב.[39] על פי סיווג זה, עברות נגד

המדינתית, והביקורת מתרכזת באי־התאמה של החקיקה המסמיכה, אם זו קיימת, לצרכים וליכולות המתאפשרות במרחב הסייבר. ראו, למשל, את Kim A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH. 128 (2007); Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2008).

39 ראו מיגל דויטש "חקיקת מחשבים בישראל" **עיוני משפט** כב 427, 435–443 (1999). יוער כי פרופ' דויטש ניסח את הצעת חוק המחשבים בשביל משרד המשפטים בשנת 1994. על הבחנה זו, בין עברות באמצעות מחשב לבין עברות נגד מחשב, חזר דויטש במאמר שהוקדש לבחינת חוק המחשבים בחלוף כעשור לחקיקתו. ראו מיגל דויטש "חוק המחשבים במבחן העתים – זווית המבט של מציע החוק" **שערי משפט** ד 257, 271 (2006). להבחנה זו ראו עוד למשל Yoram Bar-Sela, *Computer Legislation in Israel: A Proposal Being Developed by the Ministry of Justice*, ISRAEL L. REV. 58, 61 (1986); אליעזר לדרמן "פעילות פסולה המסתייעת במחשבים, ודיני העונשין בישראל" **עיוני משפט** יג 499 (1988); בועז גוטמן "חקיקת מחשבים ויישומה" **משפט וצבא** 13, 175, 177–178 (1999); MICHAEL D. ROSTOKER & ROBERT H. RINES, COMPUTER JURISPRUDENCE: LEGAL RESPONSES TO THE INFORMATION REVOLUTION 334 (1986); NEIL BARRETT, DIGITAL CRIME: POLICING THE CYBERNATION 64–65, 100–101 (1997); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1013–1020 (2001). ליישום הבחנה זו בפסיקה הישראלית, ראו ת"פ (מחוזי ת"א) 40250/99 **מדינת ישראל נ' בדיר**, בפס' 5 (פורסם בנבו, 13.11.2001). באותו מקרה, היות שדובר בעברות מרמה שונות באמצעות מחשב, כאשר התכלית המרכזית של ביצוע העברות הייתה השגת רווח כספי באמצעים פליליים, הוחלט להחמיר בענישת הנאשמים (הנאשם המרכזי נידון בבית המשפט

המחשב וחומר המחשב הן העברות שבהן המחשב, המידע או התוכנות שבמחשב הם היעדים לביצוע העברה, ואילו העברות שבאמצעות המחשב הן אלה שבהן המחשב הוא האמצעי או ה"מכשיר" לביצוע העברות. תחת הסיווג האמור אציע סיווג מעט מפורט יותר, המתאים בעיקר לעידן האינטרנט, כמפורט להלן:[40]

(1) עברות נגד המחשב וחומר המחשב. אלה הן העברות החדשות שנולדו עם המצאת המחשב, ואין להן קיום ללא המחשב. בעידן האינטרנט ניתן לדבר בהתאמה גם על עברות אינטרנט שנולדו עם תחילת שימושו של הכלל ברשת, ואין לעברות אלו קיום עצמאי ללא הרשת. כדוגמה לעברות בקטגוריה זו ניתן למנות את עברת החדירה לחומר מחשב, המנויה בסעיף 4 לחוק המחשבים. אלמלא המחשב אי אפשר לבצע עברה של חדירה למחשב. דוגמה נוספת היא העברות של עריכה או העברה של נגיף מחשב, לפי סעיפים 6(א) ו־6(ב) לחוק המחשבים. ללא מחשב אין נגיף מחשב, ועל כן זו במובהק עברה נגד מחשב.[41] עברה נוספת הנחשבת לעברה נגד מחשב היא זו של שיבוש או הפרעה לפעולתו התקינה של מחשב, לפי סעיף 2 לחוק המחשבים. בעידן האינטרנט העברות שמניתי לעיל מקבלות פנים חדשות כי החדירה למחשב יכולה להתבצע ממחשב מרוחק באמצעות האינטרנט. כך גם באשר להעברת נגיף המחשב או ההפרעה לפעולתו התקינה של מחשב.

(2) עברות באמצעות מחשב שהועתקו במלואן אל המרחב הממוחשב. הכוונה כאן לעברות מן "העולם הישן" אשר זירת ביצוען עברה מן המרחב הפיזי למרחב הממוחשב. כאלו הן, למשל, עברות של הימורים מקוונים וכן עברות הביטוי השונות באינטרנט: פרסומי תועבה, החזקה והפצה של פרסומים פדופיליים,[42] הוצאת לשון הרע, פגיעה בפרטיות, הסתה לאלימות

המחוזי לחמש שנות מאסר, ולאחר מכן, בערעורו לעליון, קוצר העונש לשלוש שנים ותשעה חודשי מאסר בפועל, בשל הסכמת המדינה לזיכויו מחלק מהעברות שבהן הורשע).

40 מלבד ההבחנה בין עברות נגד המחשב לבין עברות באמצעות המחשב התפתחה הבחנה נוספת, בין שלושה סוגי עברות: (א) עברות נגד מהימנות המחשב והמידע הממוחשב (עברות האקינג, הפצת וירוס, השבתת פעילות של מחשבים ועוד); (ב) עברות מסתייעות־מחשב (כולל עברות מרמה וגנבה באמצעות מחשב); (ג) עברות ביטוי אינטרנטיות (הסתה לגזענות, פרסומי תועבה, הטרדה מינית באמצעות האינטרנט ועוד). **ראו** DAVID S. WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE 52–129 (2007). **ראו עוד** CHRIS REED & JOHN ANGEL (EDS.), COMPUTER LAW (6th ed., 2007) 554–578. הבחנה אחרת מציעה לסווג את עברות המחשב לעברות שבהן המחשב שימש מטרה (target), אמצעי אחסון (storage device) או אמצעי התקשרות (communication tool). **ראו** YEE FEN LIM, CYBERSPACE LAW: COMMENTARIES AND MATERIALS 247–251 (2003). ההבחנות השונות בין עברות המחשב נועדו לשרת מטרות מסוימות, או במילים אחרות, ההבחנות השונות הן מכשיריות ולא מוחלטות. ההבחנה שתפורט להלן מתאימה, לטעמי, לפרספקטיבה של דיני החקירה באינטרנט, כפי שאבהיר להלן.

41 לסקירה של עברות נגד מחשב **ראו**, למשל, JOHN AYCOCK, COMPUTER VIRUSES AND MALWARE 11–52, 143–176 (2006). כן **ראו עוד**, למשל, את הדוח של ה־IC3, גוף שנוסד בארצות הברית כשותפות בין ה־FBI ל־National White Collar Crime Center ועניינו בטיפול בתלונות הנוגעות לפשעי אינטרנט ברמה המדינתית והפדרלית. התלונות מוגשות ישירות ל־IC3, דרך אתר האינטרנט של הארגון. התלונות נאספות ויוצרות את בנק המידע של הארגון. לדוח האחרון של הארגון, המונה מגמות בתחום עברות נגד המחשב, **ראו** Internet Crime Complaint Center, 2013 Internet Crime Report (2014), https://www.ic3.gov/media/annualreport/2013_IC3Report.pdf.

42 **ראו** Marty Rimm, *Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories*, 83 GEO. L.J. 1849 (1995). באותו מחקר סקר רים את תת־רשת ה־Usenet שבאינטרנט, ובעזרת מודל סטטיסטי ובפיתוח של מומחי תוכנה אפיין את כלל התכנים שבאותה תת־רשת. רים מצא שרוב הפרסומים בתת־הרשת הם

ולגזענות, פגיעה ברגשי דת ועוד.[43] בשונה מעברות נגד המחשב, הרי מדובר בעברות שהיה להן, ועדיין יש להן, קיום גם בעולם הפיזי, אך ניתן, מבחינת יסודותיהן, לבצען כל כולן במרחב הממוחשב. עוד יש לציין, כי היות שניתן להעתיק את העברות הללו למרחב הממוחשב במלואן, הרי שלא אחת נמצאנו למדים שהעברות הללו עלו בתפוצתן עלייה תלולה. כך הוא בעניין פרסומי תועבה, ובייחוד פרסומים פדופיליים ברשת, עברות ההימורים המקוונים ועוד.[44]

עברות מסתייעות־מחשב שהושלמו מחוץ למרחב הממוחשב. קטגוריה זו של עברות הוזנחה בחלוקה המקובלת בין עברות נגד מחשב וחומר המחשב לבין עברות באמצעות מחשב. הכוונה כאן היא לעברות שהושלמו מחוץ למרחב הממוחשב, אולם חלק מתהליך ביצוען עבר במחשב או בתקשורת בין מחשבים, ועל כן ראיות להתרחשות העברה עשויות להימצא במחשב. השלב ה"ממוחשב" בביצועה של עברה מסתייעת־מחשב אינו חייב להשלים יסוד מיסודותיה של העברה, אלא הוא יכול להיות חלק משלבי ההכנה של העברה. הנפקות של העברה מסתייעת־המחשב לענייננו היא שגם עברה מסוג זה יכול שתותיר עקבות דיגיטליות אשר יניעו את הרשות החוקרת לאסוף ראיות בזירה זו. כדוגמאות מוכרות יחסית לעברות מסתייעות־מחשב ניתן לציין את מקרה הרצח של הנער אופיר רחום ז"ל בידי מחבלים פלסטינים.[45] תחילתו של המעשה בצ'אט אינטרנטי בין אמנה מונא לרחום. השיחות בצ'אט הפכו לבעלות תוכן מיני. מונא פיתתה את רחום להגיע למפגש עמה באזור רמאללה, שם נחטף ונרצח. דוגמה נוספת היא המקרה המוכר כפרשת החשיפה של פדופילים בידי כתב ערוץ 10 של הטלוויזיה דב גילהר.[46] גילהר ערך סדרת תכניות שבהן התחזו תחקירניות הערוץ הבגירות לקטינות הגולשות באתרי צ'אט באינטרנט. בגירים רבים יצרו קשר עמן בצ'אט וניהלו עמן שיחות שהן בבחינת ניסיון הטרדה מינית.[47] חלק מהבגירים קבעו מפגש עם ה"קטינות" ב"דירתן", נעצרו לאחר שנכנסו לדירה והחלו לשוחח עם ה"קטינות", ואף הועמדו לדין בעברות של ניסיון אינוס או ניסיון לביצוע מעשה מגונה בקטינה.[48] במקרים אלה עברת הניסיון להטרדה המינית, ככל שבוצעה במסגרת ניהול הצ'אט, היא עברה באמצעות מחשב אשר הועתקה במלואה אל המרחב הממוחשב. דהיינו, ניתן לבצע עברה של הטרדה מינית גם במסגרת העולם הפיזי, במפגש פנים

פרסומים מיניים, וכי מספר הפרסומים המיניים הסוטים, ובכלל זה פרסומים פדופיליים, גדול יחסית למרחב הפיזי. כיום יקשה לערוך סקר דומה על האינטרנט בשל התרחבותה העצומה של הרשת משנת 1995.

43 להרחבה נוספת על עברות באמצעות מחשב שהועתקו אל המרחב הממוחשב, ראו Katyal, לעיל ה"ש 39, בעמ' 1028–1038.

44 ראו למשל Rimm, לעיל ה"ש 42, לעניין פרסומי תועבה ופרסומים פדופיליים. ראו גם, למשל, את UNITED STATES GENERAL ACCOUNTING OFFICE (GAO), INTERNET GAMBLING – AN OVERVIEW OF THE ISSUES 1–2, 51–55 (Dec. 2002), *availble at* http://www.gao.gov/new.items/d0389.pdf. לעניין הימורים באינטרנט. כן ראו חיים ויסמונסקי "על עניינה בעבירות מחשב" **מחקרי משפט** כד 81, 87–93 (2008) (וההפניות המובאות שם).

45 לדיווח על המקרה ראו, למשל, פליקס פריש ועלי ואקד "הם הצליחו להרוג את אופיר בגלל האינטרנט" **Ynet** (20.1.2001) http://www.ynet.co.il/articles/1,7340,L-445948,00.html.

46 לסקירת הפרשה והשאלות המשפטיות שעוררה ראו רע"פ 1201/12 **קטיעי נ' מדינת ישראל** (פורסם בנבו, 9.1.2014).

47 עברת ההטרדה המינית היא לפי סעיף 3(א)(6)(א) לחוק למניעת הטרדה מינית, התשנ"ח–1998. עברה זו הוספה בתיקון לחוק מיום 8.8.2007. מדובר בניסיון ולא בעברה מוגמרת, היות שמן הצד השני לא נמצאה קטינה אמתית כי אם תחקירנית המתחזה לקטינה.

48 במקרהו של אחד הנאשמים, אשר הגיע ל"דירתה" של התחקירנית כשקונדום בכיסו, מצא בית המשפט את מעשהו עולה כדי ניסיון אינוס של קטינה. ראו ת"פ (מחוזי ת"א) 1137/07 **מדינת ישראל נ' אלדד** (פורסם בנבו, 21.10.2009).

אל פנים או בשיחת טלפון או כדומה, אולם הדבר בוצע באמצעות האינטרנט. למעשה עברות ניסיון האינוס או ניסיון המעשה המגונה נועדו להתבצע בעולם הפיזי (הרי אי אפשר להשלים מעשה אינוס באינטרנט, כפי שאי אפשר לרצוח באינטרנט), אך החתירה אל העברה נעשתה באמצעות האינטרנט, ומשכך, תידרש חקירת העברה גם לזירה הווירטואלית.

את היחס בין שלוש הקטגוריות המוצעות הללו למיונן של עברות מחשב ניתן לתאר מבחינה גרפית כפירמידה, כאשר הבסיס הצר שבראש הפירמידה מתאר גם את רוחב היריעה שעליה נפרסת הסוגיה, הן מבחינה רעיונית והן (ככל הנראה) מבחינה כמותית (תרשים 1.1):

תרשים 1.1 – סיווג עברות פליליות במרחב הסייבר

כאמור, הסיווג המוצע כאן של עברות המחשב השונות רלוונטי לצורכינו לצורך הבהרת הסוגיה של סמכויות האיסוף במרחב הסייבר. סמכויות האיסוף במרחב זה אינן נוגעות רק לעברות נגד המחשב וחומר המחשב, אלא נוגעות בהחלט גם לעברות באמצעות מחשב שהועתקו במלואן למרחב הממוחשב, ולעברות מסתייעות־מחשב שהושלמו מחוץ למרחב הממוחשב והותירו עקבות דיגיטליות. למעשה, ניתן לנסח את הדברים הפוך ולומר כי נפקותן של סמכויות האיסוף במרחב הסייבר אינה רק לעברות מחשב כי אם לכל עברה פלילית שהיא, ובלבד שיש הסתברות שראיה דיגיטלית תימצא רלוונטית לצורך חקירתה או מניעתה.[49]

ד. שיבוץ הדיון במסגרת הפרדיגמה המחקרית המתהווה של משפט וטכנולוגיות מידע

הדיון שאערוך כאן, המתמקד בחקירה הפלילית, נגזר מתחום העיסוק של משפט וטכנולוגיות מידע. תחום זה הניב גישה מחקרית עולה ומתפתחת, הדנה בקשר שבין המשפט

---

49 השוו לגישת משרד המשפטים האמריקני שלפיה עברות מחשב כוללות: "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution". ראו U.S. DEPARTMENT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989). לפי גישה זו, כל עברה פלילית שהיא שבמהלך חקירתה מתעוררות שאלות של ראיות דיגיטליות במרחב הווירטואלי, נכנסת בגדר המונח עברת מחשב.

לטכנולוגיות מידע, ובראשן האינטרנט. מהם יסודותיה התאורטיים של הגישה המחקרית האמורה?

ג׳ואל ריידנברג (Reidenberg) ויוחאי בנקלר (Benkler) תיארו את יחסי הגומלין בין המשפט לאינטרנט כיחסים דינמיים של השפעה הדדית משתנה בין שני הכוחות, בדומה לטיב היחסים שבין המשפט לבין כל טכנולוגיה חדשה.[50] לעתים נדרשת הטכנולוגיה להתאים את עצמה אל הכללים המשפטיים שהשתנו, ולעתים (קרובות יותר) נדרש המשפט להתגמש ולהשתנות כדי להתמודד ביתר הצלחה עם מציאות טכנולוגית חדשה. לורנס לסיג (Lessig) הציע העשרה של ההתבוננות בהציגו את המשפט כגורם משתנה בסביבה של מקבילית כוחות רבת־משתנים, המונה את המשפט, את הנורמות החברתיות, את כוחות השוק ואת הארכיטקטורה של האינטרנט (המעוצבת באמצעות הקוד). כל אלה יחדיו מסדירים את התנהגות הפרט ואת פעילותו במרחב המקוון, אולם באפשרותם להשפיע הדדית אלה על אלה.[51] כל אחד מארבעת מוקדי הכוח הללו אינו סטטי; הוא מתפתח ומשתנה ובכך משפיע על האחרים, כמו גם על הפרטים מושאי ההסדרה.

המשפט הוא הכוח המסדיר הברור מאליו, הכולל הוראות המגובות באיום של סנקצייה בגין הפרתן. האיום נועד להרתיע, ומכאן שהוא, ולאו דווקא הסנקצייה, מסדיר את התנהגותם של מרבית הפרטים. הערכים החברתיים מסדירים את התנהגות הפרט באמצעות סנקצייה חברתית של הוקעה מהקהילה במקרה של התנהגות הסוטה מן המקובל. מחד גיסא הסנקצייה החברתית בוטה פחות מהסנקצייה הפלילית, ומאידך גיסא היא אינה מוסתת באמצעות מערכת של איזונים ובלמים חוקתיים, כפי שמתרחש כשמדובר בכללים המשפטיים כגורם המסדיר את התנהגות הפרט. אשר לכוחות השוק כגורם המסדיר את התנהגות הפרט, כאן ההסדרה היא באמצעות

---

50 ראו Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1998); Yochai Benkler, *Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1232–1261 (2000); Yochai Benkler, *Technology, Law, Freedom and Development*, 1 INDIAN J. L. & TECH. 1 (2005). לכתיבה יישומית ברוח גישה זו בנושאי הסדרה של פעילותם של מנועי חיפוש ברשת ראו ניבה אלקין־קורן ״כיצד מעצב המשפט את סביבת המידע ברשת״ **טכנולוגיות של צדק: משפט, מדע וחברה** 223 (שי לביא עורך, 2003); ובנושא של עיתונות מקוונת ראו מיכאל בירנהק ״אתיקה עיתונאית ברשת: על הסדרה פרטית, חופש העיתונות, כוח ותחרות״ **פתו״ח** 5, 173, 182–186 (2003).

51 ראו LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 85–99, 235–239 (1999). היסודות למודל הלסיגיאני הונחו במאמרו: Lawrence Lessig, *The New Chicago School*, 17 J. LEG. STUD. 661, 664 (1998), שם הציג את מודל ההסדרה, בלא להתייחס מפורשות לאינטרנט אלא לארכיטקטורה הכללית. בספרו זה התייחס לסיג פרטנית לסוגיית ההסדרה באינטרנט, ובכלל זה לארכיטקטורת האינטרנט. ראו גם Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507 (1999). ג׳וזף סומר (Sommer) הסתייג מהקביעה בדבר השפעה הדדית של ארבעת המוקדים במקבילית הכוחות הלסיגיאנית. לטענתו, אין השפעה ישירה בין הטכנולוגיה והמשפט. הקשרים בין שני מוקדים אלה מתווכים חברתית, במובן זה שהטכנולוגיה משפיעה על השוק או על הערכים החברתיים, ואלה משפיעים בתורם על המשפט. המשפט מגיב להם ולא לטכנולוגיה במישרין, וחוזר חלילה. ראו Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145, 1154–1161 (2000).

nevo.co.il

קביעת מחיר עלות להתנהגות מסוימת.[52] **הארכיטקטורה של האינטרנט** היא מגבלה טבעית שחלה באופן כללי ובקביעות (ואינה תלויה בשיקול דעת קונקרטי שמפעיל האדם שמחיל אותה). הכוונה למגבלות ולאפיונים טכנולוגיים הטבועים באינטרנט ומכוונים את התנהגות הפרטים.

נראה כי כל אחד מארבעת הכוחות יכול להסדיר על דרך השלילה התנהגות לא ראויה (סנקצייה משפטית, הוקעה חברתית, קביעת עלות גבוהה להתנהגות האסורה והגבלה טכנית). בכל הנוגע להסדרה על דרך החיוב, המשפט הפלילי, המבוסס על איסורים, אינו יכול ליצור תמריצים לעידוד התנהגות רצויה. הטכנולוגיה, הקהילה והשוק יכולים ליצור תמריצים חיוביים (יצירת יתרון טכנולוגי, פרגון חברתי וקביעת עלות נמוכה להתנהגות הרצויה). במילים אחרות, ההסדרה של שלושת הכוחות האלה היא דו־כיוונית, ואילו ההסדרה של המשפט, בהקשר הפלילי שבו עסקינן, היא בעיקר חד־כיוונית.[53]

את הכוחות במערך הלסיגיאני מייצגים "שחקנים" המפעילים אותם. וכך, את המשפט מייצגת המדינה; את כוחות השוק מייצגים תאגידים שונים הפועלים במרחב המקוון; את הערכים החברתיים מייצגות קבוצות של גולשים בקהילות וירטואליות, בפורומים שונים, בקבוצות ברשתות חברתיות כדוגמת פייסבוק ועוד. בכל הנוגע ל"שחקנים" המייצגים את הארכיטקטורה של המרחב המקוון, כיוון שהארכיטקטורה נתפשת כמגבלה טבעית,[54] הרי שהיא כביכול אינה מונעת בידי גורמים מזוהים. עם זאת, כיוון שהטכנולוגיה היא פרי פיתוח אנושי, הרי שניתן לומר שכל חברות הטכנולוגיה שפיתחו תשתית ותכניות יישומיות במרחב נכללות בקטגוריה זו.

ארחיב להלן מעט על מוקד הכוח של ארכיטקטורת המרחב המקוון ועל השפעתו על הפשיעה במרחב זה. עוד קודם לכן ראוי לעמוד על כך שהארכיטקטורה משמשת אלמנט המסדיר את התנהגות הפרט גם במרחב הפיזי, אשר בכוחו למנוע פשיעה. המשפט הפלילי כשלעצמו אינו מצליח למנוע פשיעה באופן מלא. הוא מתמקד במבצעי העברות ומאפייניהם הביו־פסיכו־חברתיים, אך גם למקום ולתנאים הסביבתיים לביצוע העברות נודעת חשיבות. כך למשל מקומות הנראים מבודדים מתמרצים ביצוע עברות. מקומות מגודרים היטב מקשים על התפרצות אליהם.[55] לצד המשפט קיים כלי חשוב, של ארכיטקטורה, המווסתת את התנהגות הפרטים ועשויה למנוע מראש, בבחינת מגבלה פיזית־טכנית, את כדאיות ביצוע העברות.

הדברים יפים גם לארכיטקטורת המרחב המקוון ולהשפעתה על הפשיעה. נמרוד קוזלובסקי מנה מאפיינים שונים המבדילים בין המרחב המקוון לבין המרחב הפיזי: דיגיטיזציה (כולל מאפיין של נְתיקוּת הראיה מן המחזיק בה), אנונימיות, ביזוריות, מודולריות, בין־לאומיות,

---

52 יצוין כי כוחות השוק, כגורם עצמאי במקבילית הכוחות של לסיג, לא הופיעו בכתיבתו המוקדמת. ראו למשל את Lawrence Lessig, *Constitution and Code*, 27 CUMBERLAND L. REV. 1, 1–2 (1996). ראו עוד את מאמרו של בירנהק, לעיל ה"ש 50, בעמ' 183, אשר ניתח את המודל הלסיגיאני ובחר לתארו כמשולש כוחות של המשפט, הארכיטקטורה של הרשת וערכים חברתיים.

53 ראו הבחנה זו גם אצל הרדוף, לעיל ה"ש 9, בעמ' 69–70.

54 בגלגולים ראשונים של תורתו השתמש לסיג במושג "טבע" לתיאור הכוח שהוא הגדירו מאוחר יותר – ארכיטקטורה של המרחב המקוון. ראו Lessig, לעיל ה"ש 52, בעמ' 2.

55 ראו Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039, 1039–1071 (2002).

חשאיות, תיווכיות (על ידי ספקי שירות שונים), אוטומטיות וקישוריות.[56] על מאפיינים אלה שמנה קוזלובסקי ניתן להוסיף עוד מאפיינים, כגון פוטנציאל האגירה של הראיה הדיגיטלית מחד גיסא ונדיפותה מאידך גיסא (שני מאפיינים הנובעים ממאפיין הדיגיטציה שנזכר למעלה), וכן הקישוריות און־ליין בין נקודות הקצה באינטרנט. לסיג טען כי בשנות התשעים של המאה הקודמת שירתה ארכיטקטורת האינטרנט את החירות מפני התערבות מדינתית, ובעשור שלאחריו השתנתה הארכיטקטורה לכזו המאפשרת Traceability (יכולת מעקב).[57] במילים אחרות, מאפיינים מסוימים של הזירה האינטרנטית השתנו – לא עוד זירה שבה ראיות נדיפות אלא זירה שבה ראיות מתועדות,[58] הניתנות לאחזורים "חכמים" בדיעבד.[59] קטיאל הסביר כי יכולת המעקב היא בעלת משמעות מניעתית (מראש), ככוח המסדיר את התנהגות הפרטים, וחקירתית (בדיעבד).[60] המשמעות המניעתית מצויה בכך שגוברים סיכויי האיתור והתפיסה של מבצע העברה, ולפיכך נפגמת האטרקטיביות של ביצוע עברות באינטרנט. קטיאל טען בהקשר זה כי אם ביצוע הפשע יהפוך לנטל יקר יותר, הרי יהיה בכך כדי להרתיע את מבצעו לא פחות מהחמרת הענישה או מהעלאת סיכויי התפיסה, כפי שמקובל לטעון בנוגע למשוואת ההרתעה המוכרת.[61] עם זאת האינטרנט מאפשר יישום עצמאי־פרטי של טכנולוגיות מקדמות־פרטיות (Privacy Enhancing Technologies – PETs). ה־PETs מאפשרים למשתמשי האינטרנט לשמר את האנונימיות שלהם או את חסיון התקשורת שלהם. כדוגמאות ל־PETs ניתן למנות שירותי אנונימיזציה המסווים את כתובת ה־IP של גולש האינטרנט, שירותי הצפנה ועוד.[62] עם זאת ה־

---

56 ראו Nimrod Kozlovski, *A Paradigm Shift in Online Policing – Designing Accountable Policing* (J.S.D. Dissertation, 2005) 48–102.

57 ראו Lawrence Lessig, *Law Regulating Code Regulating Law*, 35 LOYOLA L.J. 1 (2004). טיעון ברוח זו נשמע עוד קודם לכן מפי פרומקין: A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468–1501 (2000). טיעון זה מתחבר לטיעונם של בירנהק ואלקין־קורן במאמרם: 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). על פי טיעונם של בירנהק ואלקין־קורן, בעשור הראשון לעלייתו של האינטרנט בשימוש עולמי הייתה התחושה שהאינטרנט משוחרר מכבלי משפטן של המדינות. בעשור השני לקיומו של האינטרנט שב ועלה כוחה של המדינה, לאחר שהיא החלה להשתמש במידע שנאגר ברשותם של ספקי השירות השונים הפועלים במרחב האינטרנטי.

58 התפתחות מן השנים האחרונות, המשפיעה על עיצוב הזירה האינטרנטית, היא הפיכת "נקודות הקצה" מנייחות לניידות: האינטרנט נצרך במחשבים ניידים עם גלישה אלחוטית, בטלפונים סלולריים "חכמים" (Smartphone), במכשירי iPad ועוד. הניידות הזאת של האינטרנט מנפקת יכולות מעקב משופרות על מיקומם של הגולשים. ארחיב על משמעותה של התפתחות זאת של הזירה האינטרנטית בהמשך הדיון.

59 ראו למשל Tal Z. Zarsky, "*Mine Your Own Business!*": *Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J. L. & TECH. 1, 35–43 (2002); מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 169–190 **(2010)**.

60 ראו Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261 (2003).

61 ראו Katyal, לעיל ה"ש 39.

62 להרחבה ראו בירנהק, לעיל ה"ש 59, בעמ' 388–395. כן ראו Kozlovski, לעיל ה"ש 56, בעמ' 52–62. לדוגמאות קונקרטיות ראו למשל www.torproject.org, אתר אינטרנט המאפשר התקשרות מאובטחת, בשיטת ה־onion routing, שבו מסר מועבר מהשולח אל הנמען דרך קבוצה של מחשבים מתווכים, באופן שגם המחשבים המתווכים אינם יודעים מי מקור ההתקשרות, וכך אם יידרשו בעתיד לחשוף את מקור ההתקשרות, לא יתאפשר להם לעשות כן. כן ראו www.no-ip.com, כדוגמה לשירות המספק

nevo.co.il

PETs אינם חלק אינהרנטי מהארכיטקטורה של האינטרנט, והשימוש הפרטני בהם הופך אותם לפתרון חלקי בלבד לשוחרי האנונימיות והחירות מפני התערבות מדינתית או תאגידית באינטרנט.[63] על מנת לתגבר עוד את ההגנה על חופש הפעולה של המשתמשים במרחב המקוון קיימת עמדה המצדדת בעיצוב הטכנולוגיה כמעודדת, ואף מחייבת, פרטיות (Privacy by Design).[64] כאן המטרה היא לשתול מראש את הפרטיות בדנ"א של היישומים הטכנולוגיים, ללא תלות בשימוש הפרטני של משתמש המחשב ב־PETs. הנה כי כן, ניתן להבחין כי קיימת מערכת יחסים דיאלקטית, דינמית, בין הארכיטקטורה של מרחב הסייבר לבין יכולתו של המשפט להתערב בנעשה בה.

כשדנים בארכיטקטורה של מרחב הסייבר, יש מקום להבחין בין שתי פרספקטיבות – התבוננות חיצונית על המרחב כולו כמכלול והתבוננות פנימית ברזולוציה של המופעים השונים של המרחב. אורין קֶר (Kerr) הציע לשמר את ההבחנה על מנת למנוע בלבול קונספטואלי, ולעומתו טען ברט פרישמן (Frischmann) כי ראוי לשלב את שתי הפרספקטיבות.[65] גם הניתוח של לסיג בסוגיית ההסדרה המשפטית של האינטרנט משלב בין שתי הרזולוציות, כאשר מצד אחד התאוריה הכללית שלו מתייחסת אל האינטרנט כאל מוקד אחד, ומצד שני, כאשר פיתח את טיעונו, הוא טען שמופעים שונים של האינטרנט מגלמים מידה שונה של "ריבונות" המעניקה להם אפשרות לבצע הסדרה עצמית.[66] התפישה הטריטוריאלית והתפישה הפיזית החולשות על דיני איסוף הראיות הדיגיטליות במרחב הסייבר חלות על זירה זו כמכלול, וחלק מכישלונן נעוץ לטעמי בגישה הפשטנית, הכוללנית, ביחס לזירה. בביקורתי נגד התפישה הטריטוריאלית והפיזית, ובהציעי את המודל הפרסונלי תחתן להסדרת דיני איסוף הראיות במרחב הסייבר, אבקש לבחון את תקפותו ואת יישומו של המודל לאורן של שתי הרזולוציות, הן הכוללנית והן הפרטיקולרית: מחד גיסא אציע תפישה כוללנית שונה, ומאידך גיסא אציע שהיא תיבחן לאורם של המופעים השונים של מרחב הסייבר, ולפי המידה שבה הם מניבים צורכי חקירה חדשים או מעצימים זכויות מוגנות מסוימות.

כיצד הדיון בספר זה נגזר מהפרדיגמה המחקרית של משפט וטכנולוגיות מידע, אשר פירטתי את עיקריה להלן? הדיון שאערוך יבחן את השפעת הטכנולוגיות החדשות והמתפתחות של מרחב הסייבר על מושכלות יסוד של המשפט, שלפיהן את החקירה הפלילית עורכת המדינה, על פי סֶט כלים חוקי מוגדר מראש, אשר נוסח במקורו להתמודדות עם ראיות פיזיות בתוך

כתובת IP דינמית ומטשטש עקבות IP כלפי שרתים ומחשבים אחרים שבהם גלש המשתמש. ראו גם את http://proxy.org, כדוגמה לאתר אינטרנט המספק מידע על שרתי proxy שונים אשר מהם ניתן "לגלוש" באופן שלא יסגיר את זהות הגולש, כיוון שהמידע בדבר מקור ההתקשרות לא יישמר בשרת ה־proxy.

63 ראו Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010). כן ראו Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 1301, 1334–1340 (2004).

64 לפירוט והרחבה ראו ANN CAVOUKIAN, PRIVACY BY DESIGN… TAKE THE CHALLENGE (2009). כן ראו Michael Birnhack, Eran Toch & Irit Hadar, *Privacy Mindset, Technological Mindset*, 55 JURIMETRICS 55 (2014).

65 ראו Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003); Brett M. Frischmann, *The Prospect of Reconciling Internet and Cyberspace*, 35 LOYOLA L.J. 205 (2001).

66 ראו LAWRENCE LESSIG, CODE VERSION 2.0 281–310 (2006).

הטריטוריה המדינתית. המשפט נדרש להגיב להתפתחויות הטכנולוגיות הניכרות הללו ולשכלל ולהתאים את כלי האיסוף החוקיים שלו לראיות הדיגיטליות במרחב המקוון. לתוך המשוואה נכנסים גם כוחות השוק, בדמות גורמים פרטיים עצמתיים, כגון ספקי גישה לאינטרנט, מנהלי אתרי web, מנועי חיפוש, מנהלי רשתות חברתיות ודומיהם, אשר מצד אחד הם אוגרים ברשותם מידע בעל פוטנציאל ראייתי רב, ומצד שני הם אינם מעוניינים להיכפף לסטנדרטים המדינתיים השונים שבהם הם פועלים. גם ערכים חברתיים, למשל בנוגע למידת החופש שיש להעניק לפעילות המקוונת ולמידת השחרור מכבליהן המשפטיים של המדינות השונות, נוצקים כאמור לתוך המשוואה. כפי שאטען, הרי שנכון לעת הזאת, בכל הנוגע לחקירות פליליות במרחב הסייבר, המשפט מאחר בתגובתו להתפתחותו של המרחב ולהשפעתו על המוקדים האחרים במקבילית הכוחות הלסיגיאנית (כוחות השוק ועיצוב הערכים החברתיים). לפיכך הסטטוס קוו באשר להסדרת התנהגות הפרט משתנה. על כן אציע עדכון ותיקון של מוקד הכוח המשפטי במקבילית הכוחות הלסיגיאנית, בכיוון של החזרת כוחו של משפט המדינה להסדרה יעילה, ובה בעת ערכית וראויה, של דיני החקירה הפלילית במרחב הסייבר.[67]

מלבד העובדה שהדיון שאערוך להלן יצא מתוך הגישה המחקרית של משפט וטכנולוגיות מידע, הדיון גם יבקש **לתרום לגישה המחקרית שממנו הוא יצא, של משפט וטכנולוגיות מידע.** כפי שתואר לעיל, המודל הלסיגיאני מתאר מקבילית כוחות של משפט, ארכיטקטורה של המרחב המקוון, ערכים וכוחות שוק. כוחות אלה מסדירים את התנהגות הפרט. מרבית הכתיבה של חוקרי המשפט והאינטרנט מתמקדת במרכיב הארכיטקטורה. המשפט זוכה להתייחסות מעט אמורפית, כיחידה אחת, והפרספקטיבה עליו, בהשאלה ממונחיהם של קר ופרישמן, היא חיצונית.[68] נראה כי הנחת המוצא היא שהמשפט מיוצג בידי המדינה כמחוקקת החוק וכאוכפת

---

67 אציין כי במסגרת הדיון שאערוך, הניסיון לעדכן ולתקן את מוקד הכוח המשפטי בהקשר של החקירה הפלילית במרחב המקוון יונק את חיותו מהפרדיגמה הנורמטיבית שלפיה המשפט יכול וצריך "לכבוש" את האתגרים שמציב מרחב זה. לכותבים בולטים ברוח עמדה זו ראו Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, U. CHI. LEGAL F. 207 (1996); Andrew L. Shapiro, *The Disappearance of cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703 (1998); Jack Sommer, לעיל ה"ש 51. ; L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) לגישה המתחרה, שלפיה מרחב הסייבר מחולל בפועל (וצריך לחולל) מהפך יסודי בתחולתו ובתפקידו של המשפט, ראו David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Jonathan Zittrain, *The Rise and Fall of Sysopdom*, 10 HARV. J. L & TECH. 495 (1997); Juliet M. Oberding & Terje Norderhaug, *A Separate Jurisdiction for Cyberspace*, 2 J. COMP. MEDIATED COMM. 1 (1996); Henry H. Perritt, *Cyberspace and State Sovereignty*, 3 J. INT'L LEGAL STUD. 155 (1997); David G. Post, *Against "Against Cyberanarchy"*, 17 BERKELEY TECH. L.J. 1365 (2002); John P. Barlow, *A Declaration of the Independence of Cyberspace* (9.2.1996) http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration. לכתיבה ישראלית ברוח הגישה המהפכנית האמורה, ראו אברהם טננבוים "השלכות רשת האינטרנט על המשפט המהותי" **שערי משפט** א 1 (1998). דומני כי ניתן לקבוע שכיום הגישה המהפכנית איבדה מחשיבותה המעשית והעיונית, והמוסכמה היא שהמשפט, על ענפיו השונים, יכול וצריך לחול במרחב המקוון.

68 ראו לעיל ה"ש 65.

nevo.co.il

אותו.[69] לטעמי בולטת בחסרונה ההתייחסות הנדרשת למשפט המדינה אל מול משפטן של מדינות אחרות ואל מול המשפט הבין־לאומי. הדיון שאערוך יבקש להשלים את החסר הזה.

ה. כתיבה מוקדמת על דיני החקירה הפלילית במרחב הסייבר

ככלל, החקירה הפלילית, שלא כמשפט הפלילי המהותי, זוכה להתייחסות מחקרית מועטה, הן באשר למרחב הפיזי והן באשר למרחב המקוון. החוקר הבולט ביותר שבחן את דיני החקירה במרחב המקוון הוא קֶר. קר הקדיש חלק ניכר מכתיבתו לאפיון דיני החקירה באינטרנט והפרוצדורה הפלילית בקשר לראיות דיגיטליות. קר טען כי עדיף פיתוח של דיני חקירה ייחודיים לראיות דיגיטליות מהאינטרנט על פני "תרגום" של דיני החקירה הקיימים לאינטרנט.[70] ענף משפטי זה, ברוח הגישה המחקרית של משפט וטכנולוגיה, יצטרך להיות תגובתי (responsive) להתפתחויות הטכנולוגיות, לשרת צרכים חקירתיים הולכים וגוברים באינטרנט, ומנגד לפתח את ההגנות החוקתיות הראויות. עיקר התמקדותו של קר היא בתחולת התיקון הרביעי (4th Amendment) לחוקה האמריקנית (המגן מפני Unreasonable search and seizure) כבלם מפני פעולתה של הרשות החוקרת בזירה המקוונת. קר טען כי יש מקום לשינוי תפישתי בכל הנוגע ליישומו של התיקון הרביעי לחוקה האמריקנית על איסוף ראיות דיגיטליות.[71] לטענתו, ניסוח התיקון הרביעי מותאם לחיפושים בחצרים ולתפיסת ראיות חפציות במרחב הפיזי, ומכאן שפרשנות לא גמישה של לשון התיקון עלולה להביא לתחולת יתר או לתחולת חסר של הגנת החוקה האמריקנית על החקירה בסביבה המקוונת.[72] קר הציע להגמיש את מבחן הציפייה הסבירה לפרטיות (reasonable expectation of privacy), שפותח בפסיקת בית המשפט העליון האמריקני מכוח התיקון הרביעי, באופן שיאפשר התאמה לסיטואציות העובדתיות המגוונות בחקירה הפלילית במרחב המקוון.[73] עוד צידד קר בסנקצייה של פסלות ראיות דיגיטליות שהושגו תוך פגיעה אסורה בפרטיות, וזאת בבחינת שיניים אכיפתיות להגנת התיקון הרביעי.[74] מנגד, התנגד קר לנטייה שזיהה אצל הערכאות הנמוכות בארצות הברית להגביל מראש, במסגרת צווי החדירה לחומר מחשב שהוציאו עבור הרשות החוקרת, את שיטת פעולת החוקרים ואת היקף החומר שבו יותר להם לעיין. קר טען כי מגבלה זו, שנועדה להגביר את ההגנה החוקתית על פרטיות הנחקרים, מטילה מגבלה לא רֵאלית על החוקרים, כיוון שטיבם

---

69 ראו LESSIG, לעיל ה"ש 66, בעמ' 340–341.

70 ראו Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 293–299 (2005). בכך מבקר קר את עמדתו של לסיג המצדד בשיטת ה"תרגום", ראו LESSIG, לעיל ה"ש 51, בעמ' 114–116. את עמדתו זו ניסח לסיג עוד קודם לכן בהקשר כללי, חוץ־אינטרנטי, במאמרו: Lawrence Lessig, *Fidelity in Translation*, 71 TEXAS L. REV. 1165 (1993).

71 Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85 (2005).

72 ראו Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE. L.J. 700 (2010), שם דן קר בשאלה אם המילה "seizure", שבפרשנות טבעית מתייחסת לתפיסה של חפצים במרחב הפיזי, יכולה לחול על סיטואציות של העתקת מידע פרטי השייך לנחקר בידי הרשות החוקרת. עוד ראו בעניין זה את Ohm, לעיל ה"ש 29.

73 Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007).

74 Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003).

של החדירה לחומר המחשב ושל העיון במידע שבו, שהם מתפתחים תוך כדי תנועה, והגבלתם מראש עלולה לסכל את החקירה.

פול אוֹם (Ohm), חוקר שעוסק אף הוא בתיקון הרביעי בנוגע לדיני החקירה, טען, מנגד, שהגבלה מראש (ex ante), בשלב הוצאת הצו השיפוטי המסמיך את הרשות החוקרת לבצע חדירה לחומר מחשב, יכולה לרוב להגביל את היקף הפגיעה בפרטיות מבלי לסכל את מטרות החקירה.[75]

ניכר כי נקודת המוצא במחקריהם של קר ושל אוֹם היא ההגנה החוקתית מפני פעולתה של הרשות החוקרת. סמכויות האיסוף של הרשות החוקרת אינה יחידת הניתוח המחקרית אלא התיקון הרביעי. כן נעדרת התייחסות לסוגיית הטריטוריאליזם במרחב הסייבר. בשונה ממחקרים אלה, אציע התבוננות רחבה יותר, בעלת שני חלקים נפרדים מבחינה מתודית. מן העבר האחד אבחן את צורכי החקירה הפלילית במרחב הסייבר. אטען כי התפכחות מהתפישות הטריטוריאלית והפיזית מאפשרת בחינה מחדש של קשת הפעולות של איסוף הראיות שבאפשרותה של הרשות החוקרת לבצע במרחב הסייבר. מן העבר השני אבחן את מכלול הזכויות החוקתיות החולשות על הסיטואציה החקירתית במרחב הסייבר, הן במובן של טיב הזכויות ועצמתן, הן במובן של זהות ה"שחקנים" האוחזים בזכויות אלה והן במובן היקף הפריסה של הזכויות מבחינה טריטוריאלית.

ו. מתווה הדיון

אפתח בבחינת החלופות לאכיפה הפלילית המדינתית, ואטען לכישלונן. אעבור לבחינת התפישות הסמויות באכיפה הפלילית המדינתית הקיימת כיום ביחס למרחב הסייבר, ואטען כי הן מכשילות את המדינה כאוכפת חוק פלילי במרחב. לאחר מכן אעבור להצגת המודל הפרסונלי, המשוחרר מהתפישות המכשילות האמורות. לפיכך בפרק השני של הספר אציג בפירוט את החלופות השונות לחקירה הפלילית המדינתית, הן מבחינת **שיטת האכיפה** והן מבחינת **זהות הגורם האוכף**: אי־אכיפה והותרת הרשת לכוחות השוק ולהתגוננות עצמית בלבד; אכיפה ברמת הקהילה הווירטואלית; חסימת גישה לאתרים פוגעניים; סינון תכנים אסורים; ביצוע פעולות אכיפה התקפיות (הפלת אתרים, תפיסת שמות מתחם וכדומה); אכיפה כלפי הנתיב הכספי של העברות במרחב הסייבר; סיכול הפעילות האסורה בעת התרחשותה; החצנת האכיפה לספקיות השירות באינטרנט; שיתופי פעולה בין־מדינתיים ליצירת מערכת אכיפה אחידה חוצת־גבולות. אבחן את ההצדקות העיוניות לחלופות אלה ואת ההיתכנות המעשית להחלתן. כפי שאראה, לחלק מהחלופות פוטנציאל חלקי בלבד מבחינת היקף תחולתן, וחלופות אחרות מוגבלות מבחינה טכנולוגית. החלופה בעלת הפוטנציאל הרב ביותר היא של אכיפה הסכמית בין־מדינתית, אשר במסגרתה נעשים ניסיונות מעשיים בולטים להתמודד עם הפשיעה בזירה האינטרנטית. כפי שאטען, חלופה זו מוגבלת מטעמים פוליטיים ומטעמים כלכליים, וארגון הפעולה המשותפת בין המדינות על בסיס הסכמי בכל הנוגע לאכיפה פלילית – לעולם

---

75 Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. 1 (2011).

nevo.co.il

יהיה מוגבל מבחינת סוג העברות הנכללות בהסכם, סוג פעולות החקירה שתאושרנה במסגרת שיתוף הפעולה הבין־מדינתי ומבחינת מספר המדינות שתהיינה פעילות במסגרת זו. על כן אבקש לשלול את החלופות הללו כתחליפים לחקירה הפלילית המדינתית ה"קלאסית". מכאן, כך אטען, יש לחזור אל מודל החקירה הפלילית המדינתית ולבחון אותו בהתייחס למרחב המקוון, כאשר המודלים האחרים יוכלו לשמש **מסגרות משלימות** לאכיפה המדינתית.

עם זאת קיימים קשיים ניכרים באכיפה הפלילית במרחב הסייבר. קשיים אלה נובעים מהארכיטקטורה הייחודית של המרחב, בעיקר בהתייחס לאינטרנט, כזירה לביצוע העברות וכזירה לאיסוף ראיות לביצוען של אותן עברות. ארכיטקטורה זו וניצולה לרעה בידי גורמים עבריינים, מייצרת קשיים משפטיים ממשיים לאכיפה פלילית. לפיכך עיקר השיח בנושא הפשיעה הקיברנטית עד כה הניח כי המדינה אינה אוכפת חוק יעילה או מתאימה למרחב זה. כנגד האמור, אערער על הנחה זו, ואערוך בחינה ישירה וכוללת של דיני איסוף הראיות בידי המדינה במרחב הסייבר ושל האפשרות להתאימם למציאות המקוונת.

כפי שאטען ואציג בהמשך הדיון, יש לזהות תחילה את הכשלים בהתמודדות עם מרחב הסייבר כזירה לאכיפה הפלילית בידי המדינה. לפיכך **בפרקים השלישי והרביעי** אציג (בהתאמה) את שתי הקונספציות הלטנטיות של חלק ניכר מעושי המשפט וחוקרי המשפט באשר לסוגיית החקירה הפלילית במרחב זה: קונספצייה של טריטוריאליות וקונספצייה של פיזיות. הדיון במסגרת פרקים אלה יכלול ניתוח פוזיטיבי ביקורתי של המשפט הישראלי. בנוסף, אזקק להשוואות למשפט האנגלו־אמריקני בעיקר, כמו גם המשפט הקונטיננטלי ומשפט האיחוד האירופי. כן אבחן נורמות מן המשפט הבין־לאומי המקרינות על הסוגיה.

כפי שאראה, הדין הישראלי (ולא רק הוא) המסדיר את דיני איסוף הראיות הדיגיטליות במרחב הסייבר מגלם את התפישה הטריטוריאלית והתפישה הפיזית במובהק. אשר לתפישה הטריטוריאלית, הנחת המוצא במשפט הישראלי היא של תחולה טריטוריאלית של דיני החקירה. אשר לתפישה הפיזית, אראה כי ההוראות הייחודיות, המעטות יחסית, המתייחסות לראיות דיגיטליות הותקנו בחוק הישראלי על דרך של תיקונים תוספתיים. אראה כי קיימים אך ורק הבדלים "קוסמטיים", הן ברמה החקיקתית והן ברמה המעשית, בין איסוף ראיות פיזיות לבין איסוף ראיות דיגיטליות במרחב המקוון, ומכאן שהתפישה הפיזית חולשת על דיני האיסוף במשפט הישראלי.

בפרק החמישי אראה כיצד התפישה הטריטוריאלית והתפישה הפיזית לא רק פוגעות בסמכויותיהן של רשויות החקירה, אלא גם מביאות להחמצה דו־כיוונית של השיח הנכון לטעמי לתחום דיני החקירה במרחב הסייבר: מן העבר האחד מוחמצות כאמור פעולות איסוף הרלוונטיות לאכיפת חוק יעילה במרחב זה, ומן העבר השני מוחמץ כאמור דיון באינטרסים ובזכויות החוקתיות של ה"שחקנים" השונים העלולים להיפגע מפתיחת אופקים חדשים למדינה במרחב המקוון. בחלק זה אעמוד על שלושת הממדים של הדיון החוקתי החסר, כפי שפירטתי לעיל: ממד זהות ה"שחקנים", ממד הפריסה האקסטרה־טריטוריאלית של הזכויות החוקתיות בחקירה וממד טיב הזכויות עצמן.

בפרק השישי אטען כי על מנת לשמֵר את כוחה של המדינה כאוכפת החוק הפלילית במרחב הסייבר, עליה **להשתחרר מכבלי התפישה הטריטוריאלית ומכבלי התפישה הפיזית** באשר לאיסוף הראיות הדיגיטליות. כן עליה לפתח תורת זכויות חוקתיות שאינה טריטוריאלית ואינה תופשת את הראיה הדיגיטלית כחפץ, ומתחשבת גם באינטרסים של כל ה"שחקנים" הנוגעים

בדבר ובזכויותיהם החוקתיות. תחת התפישות השגויות הללו אבקש להציע מודל חלופי לאיסוף ראיות דיגיטליות בחקירה פלילית. מבחינה תפישתית אטען כי המודל צריך להתמקד במשתנה הפרסונלי. נובע מכך שהעיקר בדיני האיסוף במרחב הסייבר הוא לא הראיה אלא מערכת היחסים שבין המדינה החוקרת לבין הפרט החשוד, כמו גם בינה לבין "שחקנים" אחרים בזירה המקוונת, כגון פרטים אחרים בעלי זיקה לראיה הדיגיטלית, ספקי שירותי אחסון / תוכן בעלי זיקה לראיה ומדינות אחרות בעלות זיקה שכזו.

מבחינה יישומית אבקש לערוך בחינה וביקורת של דיני האיסוף של ראיות דיגיטליות במשפט הישראלי. אבחן את סמכויות האיסוף הקיימות במשפט הישראלי הקיים ואסמן את מכלול פעולות האיסוף הנעדרות מן החקיקה הישראלית הקיימת והרלוונטיות לראיות דיגיטליות. מנגד, אצביע על האופן שבו עוצבו ההגנות החוקתיות בדין הישראלי הקיים, ואל מולן אנסח את האופן שבו ראוי לפתח את הדיון החוקתי הרלוונטי לדיני איסוף הראיות הדיגיטליות בחקירה פלילית במרחב הסייבר. עוד אבקש לטעון כי אם יש מקום לפריצת האיסורים על איסוף ראיות האגורות מחוץ לטריטוריה של המדינה במסגרת החקירה הפלילית במרחב הסייבר, הרי שיש להכיר במודל תחולה אוניברסלי של זכויות חוקתיות. על פי המודל האוניברסלי שאציע, המשפט החוקתי ייתפש כמשפט של חובות ולאו דווקא של זכויות,[76] ומכאן שהחובה היא על הרשות בכל מקום שבו היא פועלת.

את הבחינה היישומית האמורה אערוך גם אל מול הוראותיה של הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד–2014,[77] הכוללת פרק נרחב[78] המתייחס לסמכויות איסוף ראיות דיגיטליות בכלל ובמרחב האינטרנטי בפרט. הצעת החוק מבטאת את הכרתו של המחוקק הישראלי בצורך לחדש ולעדכן את הגדרת סמכויות איסוף הראיות. חלק מהרעיונות שיוצגו להלן באים לידי ביטוי מסוים בהצעת החוק, ואילו חלק אחר אינו זוכה להתייחסות בהצעה.

עוד במסגרת הדיון אציע עקרונות לעריכת איזון בין צורכי החקירה בזירה המקוונת לבין ההגנות החוקתיות הניצבות כבלם כנגד אותם צרכים. אציע עקרונות של ריבוי איזונים חוקתיים קונקרטיים (ולא עקרוניים), הסמכה שיפוטית לרשות החוקרת (ולא הסמכה מנהלית), בקרה פנים־מנהלית מקדימה במסגרת הרשות החוקרת, הבניית שיקול הדעת של השופט בבואו להידרש לבקשתה של הרשות החוקרת להסמכה לביצועה של פעולת איסוף ראיות דיגיטליות במרחב הסייבר, ניסוח חקיקה ניטרלית – ככל הניתן – לטכנולוגיה והטלת חובות תיעוד מוגברות על הרשות החוקרת.

---

76 זאת בפרפרזה על המודל שפיתח וסלי הופלד (Hohfeld), ולפיו זכותו של האחד היא חובתו של האחר. בעניינו הזכות החוקתית של התושב היא החובה החוקתית של הרשות לכבד זכות זו. ראו WESLEY NEWCOMB HOHFELD, FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING (1946).

77 ה"ח הממשלה 867.

78 פרק ו' הכולל את סעיפים 72–98.