

## פרק ה

# הזכויות החוקתיות בחקירה פלילית במרחב הסייבר

## א. הקדמה

עד כה הצגתי את שתי התפישות החולשות על דיני איסוף הראיות בחקירה פלילית במרחב הסייבר: התפישה הטריטוריאלית והתפישה הפיזית. עמדתי על מקורותיהן של התפישות הללו במרחב הפיזי, איתרתי את העתקתן של התפישות מהמרחב הפיזי למרחב הקיברנטי וביקרתי את מהלך ההעתקה האמור מזוויות שונות. כן הראיתי כי החלתן של תפישות אלה על הזירה הקיברנטית משמעה פגיעה בסמכויות האיסוף של הרשות החוקרת.

בפרק זה אבקש להתמקד בהשלכתן של התפישות האמורות – הטריטוריאלית והפיזית – על הזכויות החוקתיות של הנחקרים ושל שאר מושפעי החקירה במרחב המקוון (קרי גורמים שאינם נחקרים במישרין אך מושפעים מפעולות איסוף הראיות בחקירה). כפי שאראה, התפישה הטריטוריאלית והתפישה הפיזית מביאות לפגיעות מוגברות בזכויות חוקתיות בהקשר של חקירה פלילית במרחב הסייבר. הניתוח בפרק זה משלים את ביקורתי על התפישה הטריטוריאלית ועל התפישה הפיזית בחקירה הפלילית במרחב הסייבר בהראותי כי החסר שהן מייצרות הוא דו-כיווני, הן במישור של סמכויות איסוף הראיות והן במישור של ההגנות החוקתיות מפני פעולתה של הרשות החוקרת.

הדיון החוקתי כולל כמה ממדים: האחד, זיהוי ה"שחקנים" נשאי הזכויות הנפגעים מפעולות איסוף הראיות במרחב הסייבר (מי נפגע?); השני, זיהוי היקף פרישתן של הזכויות החוקתיות מבחינה טריטוריאלית (איפה הפגיעה?); השלישי, עמידה על טיב הפגיעה בזכויות החוקתיות הנפגעות מאיסוף ראיות בחקירה פלילית, בדגש על המובנים הדיגיטליים של הפגיעה המבחינים אותה מהפגיעה המגולמת בחקירה במרחב הפיזי (מה הפגיעה?). מתווה הדיון בפרק זה יהיה על פי הממדים האלה: תחילה אצביע על ה"שחקנים" הרלוונטיים לסיטואציה החקירתית במרחב הסייבר. בשלב הבא אציג את השפעתה של התפישה הטריטוריאלית על אופן פרישתן של הזכויות החוקתיות בחקירה הפלילית במרחב הסייבר. בפרט אראה כיצד נטישת התפישה הטריטוריאלית באשר לחקירה הפלילית במרחב הסייבר יכולה וצריכה להשפיע על הדיון בדבר פרישתן הטריטוריאלית של הזכויות החוקתיות של הנחקר ושל שאר מושפעי החקירה. לאחר מכן אראה את השפעתה של התפישה הפיזית על הזכויות החוקתיות בחקירה הפלילית במרחב הסייבר. אראה כיצד יסודות התפישה הפיזית מביאים להזנחת היבטים שונים של ההגנות החוקתיות הרלוונטיות לחקירה הפלילית במרחב הסייבר, וכן אראה כיצד הרחבת סמכויות איסוף הראיות בשל נטישת התפישה הפיזית עלולה להחמיר את הפגיעה בזכויות החוקתיות המוגנות.

הדיון בפרק זה לא יכלול דיון בשאלת האיזון בין סמכויות האיסוף בחקירה הפלילית במרחב הסייבר לבין הזכויות החוקתיות הכולמות את הסמכות ומאזנות אותה. שאלת האיזון, הן העקרוני (בדבר עצם ההכרה בסמכות האיסוף ובתנאיה) והן הקונקרטי (בדבר עצם החלטתה

לאשר שימוש בסמכות בנסיבות קונקרטיות), תידון בפרק ו, במסגרת המודל שאציע תחת התפישה הטריטוריאלית והפיזית.

## ב. ה"שחקנים" הטוענים לזכויות חוקתיות בחקירה פלילית במרחב הסייבר

הסיטואציה החקירתית מגלמת התנגשות בין האינטרס הציבורי להתמודדות עם הפשיעה לבין זכויות החוקתיות המוגנות של החשוד.<sup>1</sup> עם זאת החקירה הפלילית עשויה לגלם פגיעה גם בזכויות של צדדים שלישיים. על פי רוב, הצדדים השלישיים אינם עדים לפעולת איסוף הראיות, ומכאן שמודעותם לעצם הפגיעה ויכולתם להתדיין על הפגיעה בזכויותיהם – פחותה. הדברים אמורים בעיקר על פגיעה בזכות לפרטיות, אשר מטבעה היא זכות לא מוחשית, ולא תמיד ירגיש בה הצד השלישי (למשל במצב שבו מתבצעת האזנת סתר לשיחה שבה משתתפים החשוד וצדדים שלישיים). כאשר מדובר בזכות מוחשית, כזכות הקניין, ירגיש הצד השלישי בפגיעה במוקדם או במאוחר, והוא יוכל להתייזב כטוען לזכות נגד התפיסה של החפצים במסגרת החקירה גם אם התפיסה לא בוצעה מרשותו אלא מרשותו של החשוד (לדוגמה, כאשר נערך חיפוש בבית החשוד ונתפס חפץ של אחד מבני הבית האחרים או שנתפס חפץ השייך לאדם שאינו מתגורר בבית והפקיד את החפץ בידי החשוד).<sup>2</sup>

טענתי היא שהחקירה במרחב הקיברנטי, להבדיל מהחקירה במרחב הפיזי, כוללת פגיעה מובנית ובהיקפים ניכרים בצדדים שלישיים, משלושה סוגים: (א) צדדים שלישיים הבאים במגע עם הנחקר; (ב) ספקי שירות שונים; (ג) ציבור משתמשי המחשב והאינטרנט בכלל. התפישה הפיזית החולשת על דיני החקירה במרחב הסייבר מביאה להזנחת הדיון החוקתי הרלוונטי בעניינם. הנחות המוצא של התפישה הפיזית, שמנתי בפרק ד, מתעלמות מן העובדה שהמידע הדיגיטלי, מושא החקירה הפלילית, מבוזר ומוחזק בידי ספקיות שירות שונות; המידע ניתן

1 זו התפישה הבסיסית של הרברט פקר (Packer), אשר תיאר בחיבוריו מאבק בין שתי הגישות למשפט הפלילי ולהנגדה בין האינטרס הציבורי לבין זכויות החשוד/הנאשם: גישת השליטה בפשיעה (Crime Control Model), שתדגיש את יעילות האכיפה הפלילית, וגישת ההליך ההוגן (Due Process Model), שתדגיש את ההליך הראוי נגד החשוד/הנאשם, גם אם במחיר של פגיעה ביעילותה של המלחמה בפשיעה. ראו 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). ההצגה הדיכוטומית האמורה של פקר בוקרה, אם כי לא לעניין ההצבה של החשוד / הנאשם, למול רשויות החקירה. ראו John Griffiths, *Ideology in Criminal Procedure or a Third "Model" of the Criminal Process*, 79 YALE L.J. 359 (1970). כן ראו יואב ספיר "הגנה ראויה על אנשים לא נחמדים" משפט וממשל 571, 576–579 (2007).

2 מעמדו של הטוען לזכות הוכר הן לשלבי החקירה והמשפט והן לשלב הסופי של המשפט, כאשר המדינה מבקשת לחלט את התפוס. אשר למעמדו של הטוען לזכות בשלב התפיסה (לפני תום המשפט), ראו סעיף 34 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969 (להלן – הפסד"פ). אשר למעמדו של הטוען לזכות בתום המשפט, כאשר המדינה מבקשת לחלט את התפוס, ראו סעיף 40 לפסד"פ; סעיף 21 לחוק איסור הלבנת הון, התש"ס–2000; סעיף 36א(ג) לפקודת הסמים המסוכנים [נוסח חדש], התשל"ג–1971; בש"פ 6817/07 מדינת ישראל נ' סיטבון (פורסם בנבו, 31.10.2007); עוד על מעמד הטוען לזכות למול האינטרס הציבורי בחילוט חפצים ששימשו לביצוע עברה, ראו שמואל דורנר "חילוט חפצים ששימשו לביצוע עבירה" הפרקליט מג 211 (1997).

להעתקה, ועל כן יכול להימצא בנפרד מיוצרו או מבעליו המקורי; המידע מצטבר ועל כן סביר להניח שיכלול מידע רב יותר על צדדים שלישיים. תכונות אלה משפיעות על ה"שחקנים" שמנתי, והזנת תכונות אלה במסגרת הדיון החוקתי הרלוונטי לדיני החקירה במרחב המקוון – פוגעת באופן שקלול זכויותיהם החוקתיות. גם פעולות איסוף ראיות במרחב הפיזי משפיעות, נוסף על הנחקר, על צדדים שלישיים הבאים עמו במגע, לרבות ספקי שירות שונים (לדוגמה בנקים, חברות אשראי וחברות למתן שירותי טלפוניה). ואולם, כפי שאראה במהלך הדיון בפרק זה, קיימים מאפיינים הייחודיים לחקירה בסביבה הדיגיטלית, השונים מהמוכנים המוכרים במרחב הפיזי, המשפיעים על אותם "שחקנים". אפרט להלן על ה"שחקנים":

### 1. צדדים שלישיים הבאים במגע עם בעל חומר המחשב

המידע האגור במחשב אינו שייך בהכרח לאדם אחד, מכמה טעמים: האחד, ה"מחשב אישי" (personal computer) יכול להשתייך לכמה משתמשים.<sup>3</sup> כך, למשל, מחשבים ביתיים רבים הם בשימוש של כמה בני משפחה, וכל אחד מהם עשוי להיחשב "מחזיק" במחשב או בעל הרשאה וגישה למידע שבו; השני, יכול שחומר מחשב מסוים יוחזק בספרייה שיתופית כלשהי ברשת ויהיו לו כמה מחזיקים או מורשי גישה בעלי זיקה למידע. כך הוא למשל במקרה של ספרייה שיתופית במשרד, שבה מצויים תכנים המשותפים או הנגישים לכמה אנשים; השלישי, כמעט כל מחשב, ודאי מחשב אישי, כולל תכנים אישיים שחוברו, שייכים או מתארים אנשים נוספים, ונמסרו בהסכמה למשתמש במחשב. לדוגמה, מחשב הכולל גיבוי של תכתובות דוא"ל עם צדדים שלישיים (תקשורת אגורה), תמונות של צדדים שלישיים, מסמכים שחיברו אחרים ושנשלחו למשתמש במחשב וכדומה. הגם שהמשתמש מחזיק תכנים אלה במחשבו ברשותם ובהסכמתם של אותם צדדים שלישיים, אין זאת אומרת שכאשר הרשות החוקרת חודרת לתכנים אלה, אין היא פוגעת בזכויותיהם של אותם צדדים שלישיים בנוגע למידע, מעבר לפגיעה בזכויותיו של הנחקר. לעתים התכנים של אותם צדדים שלישיים אף נהנים מחיסיון ראייתי,<sup>4</sup> או שהם מוחזקים במסגרת יחסי נאמנות מיוחדים.<sup>5</sup>

אמנם גם במרחב הפיזי יש מצבים של חיפושים אצל בעלי מקצוע הנהנים מחיסיון מקצועי, אולם בכל הנוגע לאיסוף ראיות ממוחשבות, קיים קושי אינהרנטי להפריד בין מידע חסוי לבין מידע שאינו נהנה מחיסיון, שכן שני סוגי המידע עשויים להיכלל באותו דיסק קשיח. בנוסף, בכל הנוגע לאיסוף ראיות ממוחשבות, פוטנציאל האגירה של מידע על אודות צדדים שלישיים רב יותר, ומכאן שבערכים מוחלטים עצמת הפגיעה העודפת בהם גבוהה יותר.

3 מערכות ההפעלה במחשב מאפשרות להגדיר פרופילים שונים למשתמשים שונים. המשמעות היא שבאותו מחשב יכולים להימצא תכנים שונים אשר יהיו גלויים אך ורק למי שנכנס בשם משתמש וססמה אישיים, וכך באותו מחשב תהיה הפרדה בין תכנים שונים, לפי זהות המשתמש בפועל במחשב.

4 לדוגמה, מחשב של רופא הכולל תכנים רפואיים של מטופליו; מחשב של עורך דין הכולל מסמכים ותיעוד דברים הנוגעים לשירות המקצועי שנתן ללקוחותיו; מחשב של פסיכולוג הכולל תוכני טיפול נפשי וכיוצא בזה.

5 כפי שניתן ללמוד בהשאלה מהמקרה שנדון ב"ש" (מחוזי ת"א) 92828/05 חברת ס' נ' מדינת ישראל, (פורסם בנבו, 11.9.2005). באותו מקרה הכיר בית המשפט בחיסיון על 33 מסמכי מחשב של חברת נאמנות שווייצרית שנגעו ללקוחותיה. החיסיון חל במסגרת הליך פלילי שעניינו חדירה למחשבי אותה חברת נאמנות וגנבת תכניה הממוחשבים.

קיים קושי אינהרנטי לזהות מראש (ex ante) וקונקרטי את כל הצדדים השלישיים הנוגעים בפעולת איסוף הראיות. עם זאת ברמה הקטגורית של אפיון טיפוסי הצדדים השלישיים שחומריהם עתידים להימצא בחומר המחשב – ניתן להגיע לרמת פירוט מסוימת. כך למשל במחשב ביתי של משפחה ניתן להניח שלצד חומריו של החשוד יימצאו במחשב גם חומרים אישיים של בני המשפחה האחרים. במחשב במקום העבודה ניתן להניח שיימצאו חומרים שקשורים למקום העבודה ולאנשים ממקום העבודה, במחשב של בעל מקצוע חסוי יימצאו תכנים חסויים של הלקוחות שלו וכדומה. יש מקום להביא בחשבון מראש את הפגיעות באותם צדדים שלישיים, אשר בהגדרה, וקטגורית, הפגיעה בהם היא עודפת (שכן הם אינם יעדי פעולת האיסוף).

יכולה להישמע טענה בנוגע לצדדים שלישיים שמסרו תכנים למשתמש המחשב (בהתכתבויות בדוא"ל, בצ'אט, באתרים חברתיים וכדומה), כי ככל שמידע אישי של צדדים שלישיים מצוי במחשבו של הנחקר, והימצאות זו היא על דעתם של אותם צדדים שלישיים, הרי שיש לראות במצב דברים זה כאילו ויתרו על פרטיותם באשר לאותו מידע.<sup>6</sup> טענה זו מניחה, ככלל, כי ויתור על זכות (לפרטיות ולסוד מסחרי) כלפי אדם אחד זהה לויתור עליה כלפי כולי עלמא. נראה כי דוקטרינת ההסכמה מדעת<sup>7</sup> לויתור על הפרטיות, כמו גם הדוקטרינה של "צמידות המטרה" בנוגע להגנת מידע אישי<sup>8</sup> סותרות טענה זו, ולפיהן הסגרת מידע יכולה להיעשות לצורך מסוים בלבד, ולגורם מסוים בלבד, ואין להרחיבה, בלא הסכמה מדעת, לצרכים או לגורמים אחרים.

## 2. ספקיות השירות

אחד ממאפייניו של המרחב הקיברנטי הוא כי המידע שבו מבוזר ומתווך בידי ספקיות שירות שונות. המונח "ספקיות שירות" רחב מאוד, ולמעשה כולל כמה קבוצות שונות של שחקנים המספקים שירותים במרחב הסייבר. המונח מאגד בתוכו את כל אלה ואחרים: (1) ספקיות גישה לאינטרנט (הן ספקיות גישה ישירה והן ספקיות Wi-Fi המאפשרות גלישה משותפת דרך נתב (Router) פתוח); (2) ספקיות תשתית פיזית לחיבור אינטרנט; (3) שרתי Proxy המאפשרים

6 במשפט האמריקני טענה זו מוכרת כ-Third party doctrine. הטענה היא סייג לתחולת ההגנה החוקתית של התיקון הרביעי לחוקה. לביקורת על הטענה ראו למשל Susan Freiwald, *First Principles Of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007); Andrew J. DeFilippis, *Note, Securing Informationships: Recognizing A Right To Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086 (2006). לתמיכה בדוקטרינה בהקשר של הזכות לפרטיות במרחב הקיברנטי, ראו Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) וכן ראו Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229 (2010).

7 ראו סעיף 1 ביחד עם סעיף 3 (הגדרת "הסכמה") לחוק הגנת הפרטיות, התשמ"א-1981 (להלן – חוק הגנת הפרטיות).

8 ראו סעיף 9(2) לחוק הגנת הפרטיות; מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" משפט וממשל יא 9, 54-57 (2007); מיכאל בירנהק מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה 106-108 (2010); ע"א 439/88 רשם מאגרי המידע נ' ונטורה, פ"ד מח(3) 808, 824 (1994); עת"מ (מחוזי ת"א) 24867-02-11 איי. די. איי חברה לביטוח בע"מ נ' רשם מאגרי המידע, הרשות למשפט טכנולוגיה ומידע במשרד המשפטים, בפס' 8 (פורסם בנבו, 1.8.2012).

גלישה באינטרנט דרכם, תוך רכישת קבוצת ההרשאות של שרת ה-Proxy;<sup>9</sup> (4) ספקיות שירותי אחסון מידע ואירוח אתרים; (5) מנועי חיפוש; (6) מנהלי אתרי האינטרנט. גם מונח זה – "אתר אינטרנט" – מתפרק לסוגים אלה ואחרים: אתרי תוכן מסוג יחיד-אל-רבים (One-to-Many), אתרים חברתיים ואתרי שיתוף מסוג רבים-אל-רבים (Many-to-Many) וכיוצא בזה.<sup>10</sup> כל אחד מאלה עשוי לאצור בקרבו מידע שיכול לקדם חקירה פלילית במרחב המקוון. בפרק בדנתי בסוגיית ההעברה של חובות האכיפה הפלילית מהמדינה לספקיות השירות. טענתי כי ראוי לשמר את אחריותה של המדינה כאוכפת החוק הפלילית גם אם אין מנוס מלהרבות בשימוש בספקיות השירות כזרועותיה לצורך איסוף המידע בפועל. למרות זאת יש לזכור כי ספקיות השירות הן גורם עצמאי נשא זכויות משל עצמו, בנפרד מהנחקר עצמו. התערבות המדינה בפעולת ספקיות השירות, באמצעות חיובן לאסוף ראיות עבור המדינה, פוגעת בחופש העיסוק שלהן, משיתה עליהן עלויות כלכליות שאינן קשורות בתפעול השוטף שלהן<sup>11</sup>

9 כן, למשל, שרתי אוניברסיטאות רבות מאפשרים לאנשי הסגל ולסטודנטים להתקשר אליהם מרחוק, ולגלוש דרכם אל האינטרנט, כאשר שרתים אלה יישמו כ-Proxy. הגלישה לאינטרנט דרך שרתי האוניברסיטה מאפשרת כניסה לאתרי אינטרנט מסוימים (כדוגמת Lexis) בחינם, במקום בתשלום, נוכח העובדה שלשרתים אלה הוענקו הרשאות גישה לאותם אתרים.

10 השוו להצעת חוק מסחר אלקטרוני, התשס"ח-2008, ה"ח הממשלה 356. ההצעה נדונה במושב הכנסת ה-17 והוגשה מחדש בידי ח"כ מאיר שטרית בתאריך 25.7.2011 (במושב הכנסת ה-18), בה מוגדר "ספק שירותי אינטרנט" כאחד משלושת אלה: ספק שירותי אחסון זמני, ספק שירותי אירוח וספק שירותי גישה. כך מגדירה הצעת החוק את שלושת סוגי "ספק שירותי אינטרנט":

"שירותי אחסון זמני" (Caching) – שירות שמהותו היא אחסון זמני של מידע, אשר נעשה באופן אוטומטי לשם הקלה על העברת המידע ברשת תקשורת אלקטרונית (הכוונה לאינטרנט או כל רשת ציבורית מוכרזת אחרת – הערה שלי, ח.נ.ו.) והגברת מהירות ההעברה;

"שירותי אירוח" (Hosting) – שירות שמהותו היא אחד מאלה: אחסון, דרך קבע, ברשת המחשב של ספק השירות, של מידע שנמסר לו לשם העלאתו לרשת תקשורת אלקטרונית;

הצגה, באתר אינטרנט של נותן השירות, של מידע שנמסר לו לשם העלאתו לרשת תקשורת אלקטרונית;

מתן אפשרות לאתר באופן אלקטרוני מידע המצוי ברשת תקשורת אלקטרונית; "שירות גישה" (Mere Conduit) – שירות שמהותו היא מתן גישה לאדם לרשת תקשורת אלקטרונית".

הגדרה זוהי, להוציא השמטה של החלופה השלישית של הגדרת "שירותי אירוח" (החלופה הכוללת מנועי חיפוש בגדר ספקי שירותי אירוח), הועתקה גם לתזכיר חוק חשיפת פרטי מידע של משתמש ברשת תקשורת אלקטרונית, התשע"א-2011 (תזכיר העוסק בחשיפת תגובנים (טוקבקיסטים) שפרסמו הודעות מכפישות ובחשיפת משתמשי אינטרנט שהפרו זכויות יוצרים).

11 ניתן להבחין בין הסגרת מידע האגור ברשותה של ספקית השירות לבין איסוף מידע העובר ברשות ספקית השירות אך אינו נאגר אצלה, ואיסופו מחייב את ספקית השירות בפעולה מיוחדת שלה. דוגמה להסגרת מידע קיים – מסירת תוכן תיבת הדוא"ל. דוגמה לאיסוף המידע בגלל דרישת הרשות החוקרת בלבד – בקשה לספקית שירותי גישה שתמסור את רשימת האתרים שאליהם גלש מנוי מסוים שלה. הספקית אינה שומרת את נתוני הגלישה של משתמשיה, ולצורך מענה לשאלה זו יהיה עליה לשנות את התשתית שלה, על מנת שיתאפשר לה לתעד את הנתון האמור. קיימת גם סיטואציה ברמת הביניים, שבה ספקית השירות אחוזר מידע האגור ברשותה, כאשר פעולת האחזור עצמה גוזלת משאבי זמן וכסף ואינה נדרשת לספקית השירות אלא לצורך הוצאה אל הפועל של דרישת הרשות החוקרת. לדוגמה: מסירת נתוני התקשורת נכנסות למנוי סלולרי מסוים (כאשר הנתונים אגורים לפי שיחות יוצאות,

ומתערכת בחופש ההתקשרות שלהן בהסכם עם לקוחותיהן, התקשרות שיש בה כדי להקים חובה כלפי הלקוחות שלא להסגיר את המידע של הלקוחות לידי איש, בכלל זה הרשויות.<sup>12</sup> חובה זו מקבלת הכרה מפורשת בחוק הגנת הפרטיות.<sup>13</sup> כמו כן לספקיות השירות אפשר שתעמוד טענה עצמאית לפגיעה בזכות הקניין, משני סוגים: האחד, פגיעה בזכות של ספקית השירות לנהל את עסקה כרצונה;<sup>14</sup> השני, קניינית, ככל שהסגרת המידע שהן מבקשות תחשוף סוד מסחרי מוגן שלהן או זכות יוצרים באופן אגירת המידע, סיווגו ותיוגו.<sup>15</sup> להבחנה בין ספקיות השירות השונות עשויה להיות חשיבות ניכרת ביחס לעצמת הצורך של רשויות החקירה להתערב בפעולתן למשקל הטענה האפשרית שלהן לפגיעה בחופש העיסוק. ככל שמדובר בספקיות שירות "פרטיות" יותר (למשל מנהלות אתרים של חברות מסחריות) או מצומצמות יותר מבחינת טיבו והיקפו של המידע הנאגר על לקוחותיהן (למשל מנהל אתר חדשות לעומת ספק שירותי דוא"ל), כך נראה כי למדינה יהיה צורך מופחת לחייב אותן להסגיר מידע. לעומת זאת ככל שמדובר בספקיות גישה "ציבוריות" יותר (למשל ספקיות הגישה או התשתית לאינטרנט, אשר אף מקבלות רישיון מכוח חוק התקשורת (בזק ושידורים), התשמ"ב—1982),<sup>16</sup> היושבות על צומת שליטה רחבה יותר במרחב הסייבר, כך יגבר הצורך של המדינה להטיל חובות ולדרוש איסוף מידע מאותן ספקיות. מנגד, הפגיעה באותן ספקיות, כגופים פרטיים, תעמוד בתוקפה, ובאותה עצמה.<sup>17</sup>

- ומכאן שאחזור השיחות הנכנסות יצריך כוח מחשוב מסוים משרתי חברות הסלולר); איתור כל התכנים שמופיעה בהם מילה מסוימת בקבצים האגורים אצל ספק שירותי אחסון (המענה מצריך מיון של הקבצים וחיפוש בהם לצורך מענה ממוקד).
- 12 סוגיית הנאמנות של ספקית השירות ללקוחותיה תלויה בסוג ספקית השירות שבה מדובר: הנאמנות ללקוח של מנוע חיפוש אינה כמידת הנאמנות של ספק שירותי אחסון מידע.
- 13 ראו סעיף 8(2) לחוק הגנת הפרטיות, וכן ראו את סעיף 16 לחוק, המקים חובת סודיות, על מנהל, מחזיק או עובד המתפעל מאגר מידע. הוראות אלה כוללות סנקצייה פלילית ונוזיקית בצדן.
- 14 מדובר למעשה בהמשגה קניינית של חופש העיסוק. המשגה זו מאפשרת לראות באוטונומיה של ספקית השירות לנהל את ענייניה כרצונה, לא רק כחירות שלילית, כפי שמנוסח חופש העיסוק, אלא כזכות על דרך החיוב. המשגה זו מופיעה בפסיקה הישראלית, וראו למשל את בג"ץ 726/94 כלל חברה לביטוח בע"מ נ' שר האוצר, פ"ד מח(5) 467-466, 441 (1994); בג"ץ 6218/93 ד"ר שלמה כהן, עו"ד נ' לשכת עורכי הדין, פ"ד מט(2) 529, 548, 552 (1995); בג"ץ 1715/97 לשכת מנהלי ההשקעות בישראל נ' שר האוצר, פ"ד נא(4) 367, 398, 406 (1997).
- 15 על קיומה של זכות יוצרים בגין אופן בניית מאגר המידע, ראו רע"א 2516/05 מעריב הוצאת מודיעין בע"מ נ' חברת אול יו ניד בע"מ (פורסם בנבו, 7.5.2006); רע"א 8304/09 בזק החברה הישראלית לתקשורת בע"מ נ' דפי זהב בע"מ (פורסם בנבו, 1.12.2009); ת"א (מחוזי ב"ש) 5310/08 קווי מידע ופרסום בע"מ נ' בל תקשורת פרסום ויחסי ציבור (פורסם בנבו, 5.1.2012).
- 16 כוונתי בספקיות שירות "ציבוריות" לחברות פרטיות המשתמשות במשאב ציבורי מוגבל, אשר במקרה שלפנינו הוא המשאב של גישה לאינטרנט או תשתית החיבור לאינטרנט. אמנם ספקיות אלה חופשיות לפעול באופן פרטי, אולם היות שהן פועלות מכוח רישיון בזק כ-Common carrier, הרי שהן כפופות לחובות שונות מן המשפט המנהלי. במילים אחרות, יש לראות בספקיות השירות הציבוריות משום גופים דו-מהותיים. ראו גם אמל ג' בארין "הזכות לאנונימיות, זכות הגישה לערכאות, סמכות טבעוה ומה שביניהן" מחקרי משפט כט 309, 325-326 (2013).
- 17 ראוי לציין כי אין התאמה בין מידת השליטה של ספקיות השירות ה"ציבוריות" במידע לבין אחריותן לתכנים האסורים ולפעולות האסורות המתבצעות באמצעותן. וכך, הגם שספקיות הגישה או ספקיות התשתית חולשות על תעבורת מידע ניכרת וכוללנית יחסית, ותנאי רישיון הבזק שלהן מפרטים חובות ונטלים שונים, הרי שככלל הן נתפשות כמשוחררות מאחריות לפעילותן או לתכנים מזיקים המועברים

### 3. ציבור משתמשי המחשב והאינטרנט

החקירה הפלילית אמנם מתוארת כמערכת של הפעלת כוח שלטוני כלפי נחקר מסוים, אולם להפעלת כוח זו משמעות כללית-הרתעתית. ההרתעה היא בשני מובנים: האחד, במובן שלפיו הציבור נחשף לפעולה השלטונית ולמד על סיכויי התפיסה ומחיר התפיסה (הן מחיר מידי, בדמות הפגיעות המגולמות בחקירה הפלילית, והן מחיר עתידי, של הסתברות להעמדה לדין, הרשעה ולבסוף ענישה); השני, במובן שלפיו מתגברת תחושת המעקב של הרשויות אחר פעולות משתמשי המחשב, ותחושה זו מייצרת אפקט מצנן על פעילותם הלגיטימית במרחב הממוחשב. פעולות איסוף מידע במרחב הסייבר, בפרט פעולות איסוף מידע סמויות (חדירה סמויה, האזנת סתר), גורפות (קבלה של מכלול נתוני הגלישה ביחס לאתר מסוים) או כאלה שאינן תלויות בחשד (שימור מידע דרך קבע), פוגעות בחירות הבסיסית של ציבור משתמשי המחשב והאינטרנט ומייצרות סיכון להרתעת יתר של ציבור משתמשי האינטרנט הנורמטיביים. נוסף על ציבור משתמשי המחשב והאינטרנט בכללותו, ניתן לסמן קבוצת ביניים, בין הפרט לבין הציבור הכללי, שיכולה לטעון לזכויות נפרדות במסגרת חקירה פלילית. זו הקהילה הווירטואלית, שעליה הרחבתי לעיל.<sup>18</sup> חקירה פלילית שתפנה דרישות להסגרת מידע כלפי הקהילה וירטואלית עלולה לסכן את עצם המשך קיומה של הקהילה כקבוצה סגורה וולונטרית שנוצרים בה יחסי אמון.

לסיכום עד כאן, הצגתי לעיל קבוצות של "שחקנים" נשאי זכויות המושפעים מהחקירה הפלילית במרחב המקוון. דיני איסוף הראיות, אשר פותחו עבור המרחב הפיזי, מזניחים את קיומם של ה"שחקנים" הנוספים, ועניינם אינו משוקלל כנגד צורכי החקירה. נוכח אופיין של הראיות הדיגיטליות במרחב הקיברנטי, הרי שבשונה מהחקירה הפלילית במרחב הפיזי, הפגיעה ב"שחקנים" שמנתי לעיל הופכת, ככלל, לחלק אינטגרלי יותר מן החקירה הפלילית, ועל כן מתחייב להתאים בעניין זה את הוראות הדין המסדירות את סמכויות האיסוף ואת אופן הפעלתן.

### ג. התפישה הטריטוריאלית ופרישת הזכויות החוקתיות בחקירה הפלילית במרחב הסייבר

האקסטרה-טריטוריאליות המובנה במרחב הסייבר מרבה מאוד מצבים שבהם מידע ממוחשב על אודות אדם מצוי במחשבים מחוץ לטריטוריה של המדינה החוקרת. המידע הממוחשב האמור מקים הגנות חוקתיות, ובראשן הזכות לפרטיות של מי שהמידע הוא על אודותיו, ולצדה מערך זכויות נוספות, הכול כפי שיפורט בהמשך. על פי איזה סטנדרט תימדדנה הזכויות החוקתיות המוגנות? האם על פי הסטנדרט של מקום מושבו של האדם? האם על פי הסטנדרט

באמצעותן. ראו, למשל Directive 2000/31/EC of the European Parliament and of the Council (8.6.2000) on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178.

7-8. השו עור עם: 47 U.S.C. § 230.

18 ראו פרק ב.ד.3..

של מקום הימצא הראיה? האם על פי הסטנדרט של המדינה החוקרת (בהנחה כמובן שמדובר בשלוש מדינות שונות)?

סוגיית הפרישה הטריטוריאלית של הגנות החוקה אינה ייחודית לחקירה הפלילית במרחב הסייבר, והיא התעוררה בעבר בהקשרים שונים במרחב הפיזי, לרבות במסגרת הפעלת סמכויות חקירה. אציג להלן את הדיונים בנושא בהקשרי המרחב הפיזי ולאחר מכן אבחן את הסוגיה בהקשר של חקירה פלילית במרחב הסייבר. אטען כי התפישה הטריטוריאלית מכתובה נקודת מוצא של פרישת הגנותיה של החוקה על הנוכחים בשטחה של המדינה בלבד, ותחת זאת אציע כי ככל שהחקירה הפלילית באינטרנט תהיה בעלת מובנים אקסטרה-טריטוריאליים (במשקפי התפישה הטריטוריאלית כמובן), הרי שיש מקום להחיל את הגנות החוקה בכל "מקום" שבו תפעל הרשות החוקרת כלפי מידע השייך לכל אדם שכלפיו היא תפעיל את סמכויות החקירה שלה.

## 1. התוויית השאלות בדבר פרישת הזכויות החוקתיות במסגרת חקירה פלילית

שאלת פרישת הזכויות החוקתיות מתחלקת למעשה לשתי שאלות נפרדות: האחת, באילו נסיבות יחיל בית משפט של מדינה מסוימת את דיני החוקה של אותה מדינה על סיטואציה אקסטרה-טריטוריאלית; השנייה, אם וכיצד יתחשב בית המשפט של מדינה מסוימת בדיני החוקה של מדינות אחרות היכולים לטעון לתחולה בסיטואציה אקסטרה-טריטוריאלית מסוימת. השאלה השנייה היא מעין שאלת מראה לשאלה הראשונה. בהקשר של חקירה פלילית השאלה הראשונה עניינה אפוא במודל תחולת משפטה החוקתי של המדינה החוקרת על סיטואציות של חקירה אקסטרה-טריטוריאלית, והשאלה השנייה עניינה במעין "בררת דינים חוקתית" במקרה של איסוף ראיות השייכות לתושבי חוץ.

תחילה ארחיב על השאלה הראשונה. קיימים כמה מודלים אפשריים באשר לאופן תחולתן של הזכויות החוקתיות: מודל טריטוריאלי, מודל פרסונלי, מודל פונקציונלי ומודל אוניברסלי.<sup>19</sup> אבהיר את משמעות המודלים האלה בהקשר של חקירה פלילית בשלב זה במרחב הפיזי בלבד. בהמשך אציג את יישום חלק מהמודלים הללו במשפטן של מדינות שונות. על פי המודל הטריטוריאלי, ההגנות החוקתיות מוחלות בנוגע לכל פעולה של הרשות החוקרת בתוך הטריטוריה המדינתית בלבד, בלי להתחשב באזרחותם או בתושבותם של מושאי החקירה.<sup>20</sup> במילים אחרות, על פי מודל טריטוריאלי מובהק, גם זרים (למשל תיירים), ואפילו מי שנכנסו

19 ראו ליאב אורגד "חוקה של מי ובעבור מי? על היקף תחולתם של חוקי היסוד" משפט וממשל יב 145 (2010).

20 ראו Sarah H. Cleveland, *Powers Inherent in Sovereignty: Indians, Aliens, Territories, and the Nineteenth Century Origins of Plenary Power over Foreign Affairs*, 81 TEX. L. REV. 1, 22–23 (2002); Sarah H. Cleveland, *Embedded International Law and the Constitution Abroad*, 110 COLUM. L. REV. 225, 231–244 (2010); Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 HARV. INT'L L.J. 121, 127 (2007).



למדינה שלא כחוק,<sup>21</sup> נהנים מהגנת המשפט החוקתי של המדינה שבה הם נמצאים, ומנגד, אזרח המדינה אינו נהנה עוד מהגנת המשפט החוקתי של מדינתו בצאתו מגבולות מדינתו.<sup>22</sup> שלושת המודלים האחרים הם בעלי תחולה אקסטר-טריטוריאלית: המודל הפרסונלי קובע כי סטטוס מסוים (אזרחות, תושבות וכדומה) מביא לכך שהנושא בסטטוס זכאי ליהנות מההגנה החוקתית של מדינתו בכל מקום שבו הוא נמצא, אם בתוך גבולות מדינתו ואם מחוצה לה. בהקשר של חקירה פלילית ניתן לומר כי הרשות החוקרת, ובית המשפט המסמיך אותה לפעול, מחויבים בכיבוד ההגנה החוקתית של מושאי החקירה שהם אזרחיה/תושביה בלבד, בכל מקום שבו תפעל הרשות החוקרת ובכל מקום שבו ימצאו אותם אזרחים/תושבים, לרבות מחוץ לטריטוריה המדינתית. המודל הפונקציונלי קובע כי הזכות החוקתית נפרשת באופן אקסטר-טריטוריאלית תלוי-נסיבות:<sup>23</sup> תלוי באיזו זכות מדובר,<sup>24</sup> מי נושא בזכות, אם מדובר בעתות שלום או מלחמה וכו'. בהקשר של חקירה פלילית ייבחנו נתונים כגון הסטטוס של הטוען לזכות (אזרח, תושב, תושב זר), באיזו זכות חוקתית הנוגעת לחקירה מדובר (למשל פרטיות, קניין, חופש עיסוק, זכות להליך הוגן, זכות היועצות בסנגור ואי-הפללה עצמית) ונסיבות נוספות כגון מקום פעולתה של הרשות החוקרת (בתוך הטריטוריה, במדינה זרה, או שמא במקום שבו יש למדינה זיקה מיוחדת, כגון שטח כבוש ובסיס צבאי של המדינה השוכן במדינה ידידותית וכיוצא בזה). המודל האוניברסלי קובע כי בכל מקום שבו המדינה פועלת, בין בתוך הטריטוריה

- 21 ליישום ההגנות החוקתיות על שוהים בלתי חוקיים בארצות הברית, ראו *Wong Wing v. United States*, 163 U.S. 228 (1896); *Plyler v. Doe*, 457 U.S. 202 (1982); *United States v. Mendoza-Lopez*, 481 U.S. 828 (1987). ובפסיקה הישראלית, ראו את פרשת החזקתם במשמורת של מסתננים לישראל שלא כחוק, שבו בג"ץ נדרש בשלוש הזדמנויות לבחינת חוקתיותן של הוראות החוק למניעת הסתננות, התשי"ד-1954, בעניין אופן ההחזקה של מסתננים המיועדים לגירוש, ובכל אחת מההזדמנויות הכריז על בטלות הוראות מסוימות בחוק בשל פגיעתן בזכויותיהם החוקתיות של המסתננים: בג"ץ 7146/12 נג' נ' הכנסת (פורסם בנבו, 16.9.2013), בג"ץ 8425/13 איתן מדיניות הגירה ישראלית נ' ממשלת ישראל (פורסם בנבו, 22.9.2014) ובג"ץ 8665/14 דסטה נ' הכנסת (פורסם בנבו, 11.8.2015).
- 22 לעניין זה ראו *Ross v. McIntyre*, 140 U.S. 453 (1891). באותו מקרה נשפט הנאשם בבית דין קונסולרי על עברת רצח שביצע על אנייה אמריקנית בתחומי המים הטריטוריאליים של יפן. רוס הלין על שמשפטו לא התנהל בפני חבר מושבעים, כקבוע בחוק הששי לחוקה האמריקנית. טענתו נדחתה בנימוק מפורש שהחוקה האמריקנית חלה אך ורק בתחומי שטחה של ארצות הברית, ומחוצה לו אינה חלה לא על אזרחים ולא על מי שאינם אזרחים (שם, בעמ' 464).
- 23 ראו *Gerlad L. Neuman, The Extraterritorial Constitution After Boumediene v. Bush*, 82 S. CAL. L. REV. 259 (2009).
- 24 מודל תחולה פונקציונלי אקסטר-טריטוריאלית של הגנות החוקה מעורר שאלה מכבידה בדבר אפליה בין זכויות שונות. אם חלק מהזכויות החוקתיות מוחלות אקסטר-טריטוריאלית וחלק אחר – לא, נובע שקיים פרמטר חדש ליצירת מדרג בין זכויות חוקתיות ולאפליה ביניהן. זכויות חוקתיות, שנחשבו כממוקמות במדרגה נורמטיבית אחת, עלולות להתפצל למדרגות שונות. על מיצובן של זכויות חוקתיות במדרגה נורמטיבית אחת, במסגרת מתודולוגיה של בית המשפט העליון להכרעה בין אינטרסים, זכויות וערכים, ראו מיכאל דן בירנהק "הנדסה חוקתית: המתודולוגיה של בית-המשפט העליון בהכרעות ערכיות" מחקרי משפט יט 591, 596–601 (2003). מנגד, ניתן להגן על המודל הפונקציונלי בטענה שחלק מהזכויות החוקתיות אינן רלוונטיות במצב שבו נשא הזכויות נמצא מחוץ לטריטוריה של מדינתו. כך למשל הזכות לחופש עיסוק נדמית, בהגדרתה, כזכות התחומה לטריטוריה של המדינה, או למצער שעצמתה של הזכות שונה בעת שאדם מהגר ממדינתו.

המדינתית ובין מחוצה לה, היא מחויבת על פי המשפט החוקתי שלה.<sup>25</sup> בהקשר של חקירה פלילית משמעות הדבר היא כי הרשות החוקרת, ובית המשפט המסמיך אותה לפעול, מחויבים בכיבוד ההגנה החוקתית של מושאי החקירה בכל מקום שבו תפעל הרשות החוקרת, ואין נפקא מינה אם מושאי החקירה אינם תושבי המדינה החוקרת, כפי שאין נפקות לשאלת מיקומם הטריטוריאלי של מושאי החקירה.

ניתן לאבחן כי המודל הטריטוריאלי מדגיש את מקום הימצאו של מושא החקירה, המודל הפרסונלי מדגיש את זהותו של מושא החקירה, המודל הפונקציונלי מדגיש את נסיבות החקירה ואת סוג הזכות שבה מדובר, ואילו המודל האוניברסלי מפנה את הזרקור אל הרשות החוקרת. הצגתי את המודלים השונים כמודלים נפרדים זה מזה, אך מבחינה עיונית אין הכרח שמדינה תחזיק במודל אחד בלבד. יכולה מדינה לבחור בהחלה מצטברת של המודלים הללו, כולם או חלקם. כך למשל מדינה שתיישם עיקרון טריטוריאלי עם עיקרון פרסונלי יחד, תהיה מחויבת הן בכיבוד הזכויות החוקתיות של כל מי שנמצא בשטחה והן בכיבוד הזכויות החוקתיות של אזרחיה או תושביה בלבד גם בעת פעולתה בחו"ל.

עתה לסוגיית בררת הדינים החוקתית. לעתים סיטואציה חקירתית מסוימת יכולה להיות אקסטררה-טריטוריאלי מבחינתה של מדינה אחרת, ובמקרה כזה יוכל אדם לטעון כי משפט החוקתי של אותה מדינה אחרת הוא שצריך לחלוש על הפעולה החקירתית. אדגים את הסוגיה באמצעות הדוגמה הזאת: נניח כי ג'ון הוא אזרח אמריקני, הנוסע לתאילנד ושווה בה כתייר. ג'ון נעצר בתאילנד לחקירה פלילית בגין עברת סמים. שאלה אחת היא מה מידת זכאותו להגנה חוקתית על פי הסטנדרט התאילנדי. אם המודל החוקתי התאילנדי הוא טריטוריאלי או אוניברסלי, התשובה תהיה חיובית. אם המודל החוקתי התאילנדי הוא פרסונלי, ולפיו ההגנה החוקתית המקומית חלה על תושבי תאילנד בלבד, התשובה היא שלילית. אם המודל החוקתי התאילנדי הוא פונקציונלי, תיבחן השאלה לאיזו זכות טוען ג'ון ובאילו נסיבות. עד כאן דיון מסוג אחד. דיון מסוג שני, בבחינת דיון-מראָה כאמור, יכול להתפתח לנוכח טענה אפשרית כי ג'ון זכאי להגנת החוקה האמריקנית בשל אזרחותו האמריקנית. על פי טענה זו, יחויבו הרשויות בתאילנד בכיבוד המשפט החוקתי האמריקני באשר לג'ון. אף שסיטואציות מסוג הדוגמה האמורה שכיחות למדי, עיון בפסיקה מעלה כי על פי רוב אין מתעוררת בבתי המשפט שאלת בררת הדינים החוקתית. בכל זאת ניתן למצוא ביטויים מסוימים לשאלת בררת הדינים החוקתית, במקרים האלה: כאשר מבקשים להגיש במדינה א ראיות שהרשות החוקרת של מדינה ב אספה אותן במדינה ב;<sup>26</sup> בכל הנוגע למשפט הבין-מדינתי בארצות הברית, כאשר רשות חוקרת

25 GERLAD L. NEUMAN, STRANGERS TO THE CONSTITUTION: IMMIGRANTS, BORDERS AND  
FUNDAMENTAL LAW 5–6 (1996); Eric A. Posner, *Boumediene and the Uncertain March of  
Judicial Cosmopolitanism* 2–3 (Chi. Pub. Law & Legal Theory, Working Paper No. 228, 2008)  
26 *Stonehill v. United States*, 405 F.2d 738, 743 (9th Cir., 1969); *State v.*  
*Brown*, 940 P.2d 546, 576 (Wash., 1997); *State v. Minter*, 561 A.2d 570 (N.J., 1989);  
*Commonwealth v. Bennett*, 369 A.2d 493, 494–495 (Pa. Super. Ct., 1976); *Commonwealth v.*  
*Sanchez*, 716 A.2d 1221, 1222–1225 (Pa. Super. Ct., 1997). כן ראו במשפט הישראלי בקשר  
להאזנת סתר ורשות חקירה זרה ביצעה בחו"ל והיא מוגשת כראיה בישראל את ב"ש 82/83 מדינת  
ישראל נ' עליה, פ"ד לז(2), 738, 742–743 (1983); ע"פ 331/88 חלובה נ' מדינת ישראל, פ"ד מד(4)  
141, 144–145 (1990), שם נפסק כי אם רשות זרה ביצעה את האזנת הסתר במדינה הזרה, על פי דיני

ממדינה אחת פועלת פעולה אקסטר-טריטוריאלית במדינה אחרת בתוך ארצות הברית;<sup>27</sup> במסגרת שאלות של הסגרה ממדינה למדינה, כאשר המדינה המבקשת אוספת ראיות באופן הנחשב פוגעני על פי דיני המדינה המתבקשת להסגיר את הנאשם.<sup>28</sup> מדוע נושא בררת הדינים החוקתית אינו זוכה לדיון מפורט יותר? הנה הסבר אפשרי. הנורמות החוקתיות נמצאות במדרגה הנורמטיבית הגבוהה ביותר ומכפילות אליהן את שאר הדינים של המדינה. נורמות אלה מוצבות ככלמים לפעולת הרשות החוקרת, משמע שהן מתכתבות עם המשפט הפלילי המדינתי אשר גם הוא קשור בעבותות לסוגיית ריבונותה של המדינה. משמעות ייבואן של נורמות חוקתיות זרות בהקשר של דיני איסוף ראיות בחקירה פלילית היא הכפפת המשפט המקומי לנורמות ממערכת משפט זרה דווקא בעניינים "גרעיניים" שבליבת תפיסת הריבונות של המדינה.<sup>29</sup> עם זאת, בהמשך, אפתח מחדש את הדיון בשאלת בררת הדינים החוקתית היות שהחקירה הפלילית במרחב הסייבר יכולה להיות, לעתים מזומנות מאוד, אקסטר-טריטוריאלית במובן זה שהיא תכלול איסוף ראיות דיגיטליות האגורות במחשבים מחוץ לטריטוריה.

## 2. פרישת הזכויות החוקתיות כנגד הפעלת סמכות אקסטר-טריטוריאלית במרחב הפיזי

הצגתי ארבעה מודלים לתחולת החוקה של המדינה השופטת (מדינת הפורום). איזה מהמודלים נוהג במשפטן של מדינות שונות? נקודת המוצא המקובלת בעולם היא כי חל המודל הטריטוריאלי, קרי שחוקת המדינה חלה בטריטוריה של המדינה בלבד.<sup>30</sup> קביעה זו היא נקודת מוצא כאמור ולא נקודת סיום המגדירה את קצה גבול הפרישה של החוקה.<sup>31</sup> נקודת המוצא

אותה מדינה, ומבקשים להגיש את האזנת הסתר כראיה בבית משפט ישראלי, הרי שיחולו האיזונים והבלמים החוקתיים של דין מקום ביצוע ההאזנה ולא של המשפט הישראלי.  
 27 ראו *State of New Hampshire v. Windhurst*, 2006 WL 2075119 (N.H. Super., 2006).  
 28 ראו במשפט הישראלי את סעיף 12 לחוק ההסגרה, התשי"ד-1954, עם תקנה 15 (א) לתקנות ההסגרה (סדרי דין וכללי ראיות בעתירות), התשל"א-1970. סעיפים אלה דנים בייבואם של דיני קבילות ראיות זרים של המדינה המבקשת את ההסגרה מישראל אליה. לפסיקה שדנה בפרשנות סעיפים אלה ובטענות של ההגנה, כי סעיפים אלה מייבאים הגנות חוקתיות אחרות של שיטת משפט זרה לישראל, ראו ע"פ 6717/09 אוזיפה נ' היועץ המשפטי לממשלה, בפס' 11-15 (פורסם בנבו, 6.12.2010); ע"פ 10946/03 עיסא נ' מדינת ישראל, פ"ד ס(2) 33, 46 (2005); ע"פ 7303/02 הקש נ' מדינת ישראל, בפס' 26-27 (פורסם בנבו, 7.9.2003). בכל המקרים האלה לא התקבלו טענות ההגנה נגד ההסגרה.  
 29 להתבטאות בפסיקה הישראלית ברוח זו, ראו ע"פ 4596/05 רוזנשטיין נ' מדינת ישראל, פ"ד ס(3) 353, 411-412 (2005). כן ראו אביגדור לבונטין ברירת הדין – הצעה לחוק עם מבוא ודברי הסבר מקוצרים, פרק המבוא, עמ' ג (1987). כמו כן, ראו ברוח זו את הטיעון של אנופאם צ'אנדר (Anupam Chander, *The Electronic Silk Road: How the Web Binds the World in Commerce* 177 (2013)).  
 30 ראו *Neuman, Gerald L., Whose Constitution?*, 100 *YALE L.J.* 909 (1991); NEUMAN, לעיל ה"ש 25, בעמ' 3-5; אורגד, לעיל ה"ש 19, בעמ' 149-157; אהרן ברק כבוד האדם: הזכות החוקתית ובנותיה כרך א 401 (2014).  
 31 על רקע האמור מעניינת העובדה כי דווקא המבוא לחוקה האמריקנית פותח במילים "We the people..." דהיינו ברטוריקה שיכולה להתפרש כפרסונלית. עוד יצוין כי לפי הצ'רטר הקנדי בדבר זכויות וחירויות אזרח, הוא נועד לחייב את הפרלמנט ואת הרשות המבצעת הקנדית בכל פעולה שלהם.

הטריטוריאלי מוכרת גם במשפט הבין-לאומי.<sup>32</sup> עם זאת יש לציין כי המשפט הבין-לאומי מכונן משטר בין-מדינתי של זכויות אדם אשר מעצם טבעו חוצה גבולות מדינתיים וחל באופן המחייב את המדינות אף אם יפעלו אקסטרטריטוריאלי. משטר זכויות האדם הבין-מדינתי מורכב משלושה: זכויות אדם שהן חלק מהמשפט הבין-לאומי המנהגי, זכויות אדם המוסכמות בין מדינות במסגרת בין-לאומית כללית (אימוץ על ידי האו"ם) וזכויות אדם המוסכמות בין מדינות במסגרת אזורית.<sup>33</sup> הזכויות הנוגעות לחקירה פלילית אינן מנויות ככלל בין זכויות האדם המוכרות במסגרת הבין-לאומית, להוציא את הזכות להליך הוגן ואת הזכות לפרטיות המנויות בכמה מסמכים בין-מדינתיים, חלקם בעלי תוקף מחייב וחלקם נעדרי תוקף מחייב והם בבחינת קווים מנחים למדינות.<sup>34</sup>

אין הגבלה טריטוריאלי בהוראות הצ'רטר הקנדי. ראו The Canadian Charter of Rights and Freedoms, Art. 32 § 1. מכאן ששתי חוקות אלה פותחות פתח להחלת הגנות החוקה מעבר לגבולות הטריטוריה.

32 ראו (1933) 19 L.N.T.S 165, Montevideo Convention on Rights and Duties of States. סעיף 9 לאמנה קיובע:

“The jurisdiction of states within the limits of national territory applies to all the inhabitants. Nationals and foreigners are under the same protection of the law and the national authorities and the foreigners may not claim rights other or more extensive than those of the nationals”.

משתמעת מנוסח הסעיף ההכרה כי לא רק ההגנה החוקתית היא טריטוריאלי, אלא שגם סמכותה של המדינה היא טריטוריאלי.

33 במסגרת המשפט הבין-לאומי המנהגי הוכרו האיסורים על עינויים, על עבדות ועל השמדת עם, וכן הוכר העיקרון של איסור הפליה. ראו MALCOLM N. SHAW, INTERNATIONAL LAW 275 (6<sup>th</sup> ed., 2008) (והמקורות המצוטטים שם); LOUIS HENKIN, RICHARD C. PUGH, OSCAR SHACHTER & HANS SMIT, INTERNATIONAL LAW: CASES AND MATERIALS 615–617 (3<sup>rd</sup> ed., 1993) הכללית ניתן לציין למשל את האמנות האלה שאימצה העצרת הכללית של האו"ם: International Covenant on Civil and Political Rights (1966) (שבה הוכרו זכויות לאוטונומיה תרבותית למיעוטים, חופש דת וחופש התאגדות); International Covenant on Economic, Social and Cultural Rights (1966) (שבה זכות לחינוך, זכות לעבודה ולאגודי עובדים, זכות למזון, זכות לביטוח לאומי, זכות לבריאות וזכות לדיוור); Convention on the Elimination of All Forms of Discrimination against Women (1979); International Convention on the Elimination of All Forms of Racial Discrimination (1965); Convention on the Rights of the Child (1989); International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families (1990); Convention on the Rights of Persons with Disabilities (2006). ראו SHAW, לעיל ה"ש 33, בעמ' 276–343 (והמקורות המצוטטים שם). לאמנות בין-לאומיות נוספות המעגנות זכויות אדם, ראו HENKIN ET AL., שם, בעמ' 608–615. במסגרת האזורית ניתן לזהות הסכמים בין-לאומיים להגנה על זכויות אדם כמועצת אירופה, בין מדינות ברית המועצות לשעבר, בין מדינות יבשת אמריקה הצפונית והדרומית, בין מדינות אפריקה ובין מדינות ערב. אמנות אלה הקימו מנגנוני דיווח ובקרה על יישום הגנת הזכויות על ידי המדינות החתומות עליהן. ראו, בהתאמה, Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 1950); Convention on Human Rights and Fundamental Freedoms (Minsk, 1995); American Convention on Human Rights (San Jose, 1969); African Charter on Human and Peoples' Rights (Banjul, 1981); Arab Charter on Human Rights (1994). כן ראו SHAW, לעיל ה"ש 33, בעמ' 395–345 (והמקורות המצוטטים שם).

34 ראו את אמנת מועצת אירופה The European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 1950), שבה נקובה הזכות להליך הוגן (Art. 6) והזכות לפרטיות (Art. 8). הזכות להליך הוגן המוגדרת באמנה עיקרה בשלבי המשפט הפלילי עצמו ולא בשלבי החקירה

מלבד נקודת המוצא בדבר תחולה טריטוריאלית של הגנת החוקה יש קבוצת מצבים שבהם מופעלת סמכות של המדינה, בכלל זה סמכות איסוף ראיות בחקירה פלילית, בשטחים בשליטה אפקטיבית של המדינה. הדוגמה המובהקת ביותר, המוכרת בישראל, באשר לשטחים מעין אלה היא דוגמת השטחים המוחזקים מכוח "תפיסה לוחמתית" או כיבוש. בית המשפט העליון פסק בבג"ץ ההתנתקות כי בכל הנוגע לישראלים המתיישבים בשטחי יהודה ושומרון (ולשעבר עזה) – הם זכאים ליהנות מתחולת חוקי היסוד הישראליים עליהם, גם בשבתם בשטחים.<sup>35</sup> בכל הנוגע לתושבי השטחים שאינם ישראלים הותיר בג"ץ באותה פרשה את הסוגיה בצריך עיון ולא הכריע בה.<sup>36</sup> בכמה הזדמנויות אחרות ניתן למצוא התבטאויות המכירות בזכויות חוקתיות של תושבי השטחים שאינם ישראלים.<sup>37</sup> לעומת כל האמור הקביעה הרווחת היא שאיש הרשות הישראלית נושא בצקלונו את המשפט המנהלי של מדינת ישראל בכל מקום שבו הוא פועל, לרבות בשטחי יהודה, ושומרון ועזה (לפני ההתנתקות), אף אם מדובר בהפעלת הסמכות כלפי מי שאינם תושבי ישראל.<sup>38</sup> קביעה כזו קיימת גם בהקשר של חקירה פלילית, בפרשת אל מצרי, העוסקת בהאזנת

הפלילית, ולכן הזכות אינה נוגעת לנושא דיונונו. הזכות לפרטיות מוגדרת הגדרה צרה, בהתייחס לביתו, לחיי משפחתו ולתכתובותיו של אדם, ונקבע ככלל, ללא תנאים, כי ניתן לסייג את הזכות לפרטיות לצורכי שמירה על הסדר הציבורי ומניעת פשיעה, בכפוף לתנאי "פסקת הגבלה". על כן הסדר כללי זה בוודאי אינו יכול לספק מטריית הגנה מספקת ומפורטת דייה להקשרים של חקירה פלילית. להגדרה דומה של הזכות לפרטיות בהקשר של פרטיות בסקטור התקשורת, ראו גם את Directive 2002/58/EC of the European Parliament and the Council (12.7.2012), concerning the processing of personal .data and the protection of privacy in the electronic communications sector, OJ L 201, Art. 1 § 3 נוסף על כך ניתן לציין את הקווים המנחים של ה-OECD להגנת מידע אישי, אשר ציות להם מחולל משטר אזורי של הגנת מידע אישי. ראו OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). קווים מנחים אלה מטילים מגבלות על איסוף מידע אישי בידי החברות בארגון, אך גם הם מסויגים על פי אינטרסים של שמירה על ריבונות המדינה, על ביטחונה ועל הסדר הציבורי שבה (ראו בפס' 4 לקווים המנחים).

35 ראו בג"ץ 1661/05 המועצה האזורית חוף עזה נ' ראש הממשלה, פ"ד נט(2) 481, 559–560 (2005), שם נפסק מפי הנשיא ברק:

"לדעתנו, מעניקים חוקי היסוד זכויות לכל מתיישב ישראלי בשטח המפונה. תחולה זו היא אישית. היא נגזרת משליטתה של מדינת ישראל על השטח המפונה. היא פרי התפיסה כי על ישראלים המצויים מחוץ למדינה אך באזור הנתון לשליטתה בדרך של תפיסה לוחמתית חלים חוקי היסוד של המדינה באשר לזכויות האדם".

כן ראו ברק, לעיל ה"ש 30, בעמ' 402.

36 בית המשפט העליון ציין כי מדובר בשאלה מכבידה, אך בהזדמנויות שונות, כשהתאפשר לו להכריע במקרה שלפניו בלי להידרש לה לגופה, בחר לעשות כן. ראו למשל בג"ץ 3278/02 המוקד להגנת הפרט נ' מפקד כוחות צה"ל באזור הגדה המערבית, פ"ד נז(1) 385, 396–397 (2002); בג"ץ 7052/03 עדאלה – המרכז המשפטי לזכויות המיעוט הערבי בישראל נ' שר הפנים, פ"ד סא(2) 202, 280–281, 412 (2006); בג"ץ 8276/05 עדאלה – המרכז המשפטי לזכויות המיעוט הערבי בישראל נ' שר הביטחון, פ"ד סב(1) 1, 19–20 (2006); רע"א 993/06 מדינת ישראל נ' דיראני, בפס' 55 לפסק דינה של השופטת פרוקצ'יה (פורסם בנבו, 18.7.2011).

37 ראו למשל בג"ץ 1890/03 עיריית בית לחם נ' מדינת ישראל, בעמ' 755–756 (פורסם בנבו, 30.2.2005); בג"ץ 10356/02 הס נ' מפקד כוחות צה"ל בגדה המערבית, פ"ד נח(3) 443, 460–464 (2004). כן ראו אורגד, לעיל ה"ש 19, בעמ' 171–173. ראו עוד אצל יעל רונן "תחולתו של חוק יסוד: כבוד האדם וחירותו בגדה המערבית" שערי משפט ז 149 (2014).

38 ראו בג"ץ 390/79 דויקאת נ' ממשלת ישראל, פ"ד לד(1) 13, 14 (1979); בג"ץ 69/81 אבו עיטה נ' מפקד אזור יהודה והשומרון, פ"ד לז(2) 197, 227–226 (1983); בג"ץ 393/82 אסכאן נ' מפקד כוחות

סתר בשטח רצועת עזה.<sup>39</sup> מן הרטוריקה של בית המשפט העליון הישראלי נראה כי החלת חובות מן המשפט המנהלי הישראלי אינה זהה, לדידו, להחלת חובות לכבוד זכויות חוקתיות. במשפט האיחוד האירופי, כמו גם במשפט האנגלי, ניתן למצוא גישה שלפיה המשפט החוקתי של המדינה מחייב אותה בכל מקום שבו יש לה שליטה אפקטיבית (Effective control), אף הוא מחוץ לטריטוריה המוכרת שלה (למשל, במקרה של כיבוש צבאי) וכלפי כל מי שתפעל ביחס אליו באותם המקומות.<sup>40</sup> בפסיקה האמריקנית נדונה שאלת הזכות של עצורים שאינם אזרחים ליהנות מהגנות חוקתיות בהיותם במתקן מעצר אמריקני במפרץ גואנטנמו בקובה, שהוא שטח שחכרה ארצות הברית מקובה לפני יותר ממאה שנה. בפרשת *Boumediene* ניתן למצוא התייחסות מרחיבה לתחולת החוקה, למצער הזכות להביאם קורפוס לעצורים במפרץ גואנטנמו. בית המשפט העליון האמריקני קבע כי הזכות להביאם קורפוס, זכות המוגנת בחוקה האמריקנית, חלה בנסיבות העניין על עצורי בית הסוהר האמריקני הגם שמדובר בטריטוריה שאינה אמריקנית.<sup>41</sup> ניתן למצוא כמה מסלולי הנמקה בפסק הדין: האחד, כי אפקטיבית שלטה ארצות הברית בשטח זה, גם אם "טכנית", כך כהגדרת בית המשפט, מדובר בטריטוריה זרה. במילים אחרות, מדובר בריבונות אמריקנית דה פקטו, גם אם לא דה יורה; השני, ראוי כי מבחינה פונקציונלית הזכות החוקתית להביאם קורפוס תוחל בכל מקום שבו פועלות הרשויות האמריקניות, אף מחוץ לטריטוריה, כיוון שמדובר בדרישת סף חוקתית מינימלית.<sup>42</sup>

צה"ל באזור יהודה ושומרון, פ"ד לז(4) 785, 790–791 (1982); עניין המוקד להגנת הפרט, לעיל; בג"ץ 10104/04 שלום עכשיו – שעל מפעלים חינוכיים נ' יוסף, פ"ד סא(2) 93 (2006).

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

40 לעמדה באנגליה ראו [2007] UKHL 26 (Eng.) *Al-Skeini v. Secretary of State of Defence*. לעמדת בית המשפט האירופי לזכויות אדם ראו *Ilascu v. Moldova*, App. No. 48787/99 Eur. Ct. H.R. (2004); *Loizidou v. Turkey*, 310 Eur. Ct. H.R. 2216 (1995); *Medvedyev v. Turkey*, App. No 3394/03 Eur. Ct. H.R. (2010). מנגד, ראו העמדה בעניין *Bankovic' v. Belgium*, 11 Eur. Ct. H.R. 435 (2001).

41 ראו *Boumediene v. Bush*, 553 U.S. 723, 762–764 (2008). בכך דחה בית המשפט העליון את החלת הפסיקה משנת 1950 שלפיה החוקה האמריקנית אינה חלה על זרים השוהים במתקני מעצר אמריקניים על אדמת גרמניה. ראו *Johnson v. Eisentrager*, 338 U.S. 763 (1950).

42 ההנמקה הראשונה אינה נפרדת מהמודל החוקתי הטריטוריאלי אלא מגמישה אותו גם אל עבר שטחים שארצות הברית שולטת בהם דה פקטו. ההנמקה השנייה מציעה הבנה של פסק הדין כמציע תחולה אקסטרטריטוריאלי של החוקה האמריקנית על לא-אזרחים לפי מודל פונקציונלי. ההבנה ה"פונקציונלית" היא המקובלת, וראו למשל Neuman, לעיל ה"ש 23; *Christina Duffy Burnett, A Convenient Constitution? Extraterritoriality after Boumediene*, 109 COLUM. L. REV. 973 (2009); *Chimene I. Keitner, Rights Beyond Borders*, 36 YALE J. INT'L L. 55, 72, 78–79 (2011). מעניין כי דווקא הקריאה ה"טריטוריאליסטית" של פסק הדין, שאינה נפרדת מהפרדיגמה הטריטוריאלי בדבר היקף הפרישה של החוקה האמריקנית ונדמית ממבט ראשון כ"שמרנית", מביאה בפועל לתוצאה מרחיבה באשר לעצורי גואנטנמו, שכן משמעותה היא כי כל החוקה האמריקנית חלה במתקני המעצר במפרץ גואנטנמו, ואילו הקריאה של פסק הדין במשקפי הגישה הפונקציונלית משמעה, לעניין מתקני המעצר במפרץ גואנטנמו עצמו, כי לא כל החוקה חלה, וכי לגבי כל זכות חוקתית שתיטען יהיה מקום לבחון את תחולתה בפועל. במילים אחרות, הגם שמבחינה עיונית הקריאה ה"פונקציונלית" של פסק הדין בעניין *Boumediene* מהפכנית יותר, הרי שמבחינה יישומית קריאתה שמרנית מהקריאה ה"טריטוריאליסטית" של פסק הדין.

אם לסכם עד כאן, התפישה היסודית המקובלת בעולם, שהיא בבחינת נקודת מוצא ולא נקודת סיום, היא כי ההגנה החוקתית נפרשת בגבולות הטריטוריה על כל מי שנמצא בה ואשר כלפיו פועלת הרשות. שאלת פרישתה של החוקה אל שטחים מחוץ לגבולות הטריטוריה המדינתית המקיימים זיקה למדינה, כגון שטחים כבושים צבאית או שטחים המוחזקים בידי המדינה מכוח הסכם חכירה עם מדינה אחרת, אינה טריוויאלית, ואין בעניינה עמדה אחידה. מלבד הדיון בנוגע לשטחים ב"שליטה אפקטיבית" אצביע להלן על הרחבות נוספות של הפרישה החוקתית אל מעבר לטריטוריה. מקרה אמריקני חשוב, שעניינו בזכויות דינויות במהלך משפט פלילי, הוא מקרה *Reid v. Covert*, שנדון בבית המשפט העליון האמריקני בשנת 1956. באותה פרשה הועמדה אזרחית אמריקנית לדין בגין רצח בן זוגה האמריקני בפני בית דין אמריקני צבאי שמושבו בבריטניה. הרצח התבצע על אדמת בריטניה. השיפוט בבית דין צבאי אמריקני התקיים על בסיס הסכם בי-לטרלי בין ארצות הברית לבריטניה, ולפיו בתי דין צבאיים אמריקניים יוכלו לשפוט עברות שיבוצעו בבריטניה בידי אנשי צבא ארצות הברית או בני ביתם. בעקבות שפיטתה בערכאה צבאית טענה הנאשמת להפרת זכותה החוקתית לשיפוט בפני חבר מושבעים, לפי התיקון השישי לחוקה האמריקנית, כמו גם להפרת זכותה לשימוע בפני Grand Jury לפני כתב אישום על פי הקבוע בתיקון החמישי לחוקה האמריקנית. בית המשפט העליון קבע כי ההסכם הבינ-לאומי שעליו חתמה ארצות הברית עם בריטניה אינו יכול לגבור על הגנת החוקה האמריקנית, ובמילים אחרות לחוקה מעמד נורמטיבי מחייב גבוה מזה של התחייבויות הסכמיות של ארצות הברית בזירה הבינ-לאומית: חוקה גוברת על אמנה. עוד קובע בית המשפט כי החוקה אינה נפרדת מאזרחיה בחו"ל.<sup>43</sup>

אל מול פרשת *Reid* ניצבת פרשת *Verdugo-Urquidez*, שנדונה בבית המשפט העליון האמריקני בשנת 1990.<sup>44</sup> באותו מקרה נעצר אזרח מקסיקני והועבר לארצות הברית לצורך משפטו על עברות סמים ובגין חשד לרצח סוכן DEA (Drug Enforcement Agency) אמריקני. חוקרי ה-DEA קיבלו את הסכמת שלטונות מקסיקו לעריכת חיפוש בביתו. הם ערכו את החיפוש ללא צו שיפוטי. הנאשם התנגד להגשת ממצאי החיפוש לבית המשפט בארצות הברית בטענה

43 ראו *Reid v. Covert*, 354 U.S. 1 (1956). בפסק הדין נקבעה תחולתה של החוקה על אזרחית בחו"ל בנוגע לאישום בעברת רצח, שהיא *Capital crime*. בפסיקה מאוחרת יותר הוחל הכלל גם על עברות קלות יותר, וראו *Kinsella v. United States*, 361 U.S. 234 (1960). יצוין עוד כי לכאורה היה ניתן לפרש את פסק דין *Reid* כממשיך קו של הרחבת המודל הטריטוריאלי באמצעות הגמשה נוספת של גבולות הטריטוריה והשטחים שבהם יש "שליטה אפקטיבית" למדינה. על פי קו זה, גם בית דין צבאי אמריקני על אדמה זרה יכול להיחשב חלק מהשטחים שבהם יש לארצות הברית שליטה אפקטיבית. בפועל הרטוריקה של פסק הדין הייתה שונה. כך נפסק מפני השופט בלאק (Black), שם בעמ' 5-6:

"... we reject the idea that when the United States acts against citizens abroad it can do so free of the Bill of Rights. The United States is entirely a creature of the Constitution. Its power and authority have no other source. It can only act in accordance with all the limitations imposed by the Constitution. When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provide to protect his life and liberty should not be stripped away just because he happens to be in another land".

ניומן פירש את פסק הדין ככזה שחיסל סופית את הפרדיגמה הטריטוריאליה בדבר פרישת החוקה האמריקנית. ראו Neuman, לעיל ה"ש 30, בעמ' 965-976.

44 ראו *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

שהמסמכים הושגו בניגוד להוראות התיקון הרביעי לחוקה האמריקנית, המגן מפני חיפושם ותפיסה בלתי סבירים והמחייב הצטיידות מראש של רשויות החקירה בצו שיפוטי. בית המשפט העליון קבע, ברוב דעות, כי משטרת ארצות הברית, כאשר היא פועלת במקסימום, אינה כפופה לחובה החוקתית הקבועה בתיקון הרביעי לחוקה האמריקנית לקבל צו מבית משפט מבעוד מועד המסמך עריכת חיפוש. עוד על פי פסק הדין, אין נפקא מינה אם גם החוקה המקסיקנית מחייבת הצטיידות בצו חיפוש מבעוד מועד כאמור. לכאורה, פרשת *Verdugo-Urquidez* מייצגת חזרה אל הפרדיגמה הטריטוריאלית בעניין פרישת החוקה.<sup>45</sup>

פרשה אמריקנית נוספת היא פרשת *Wang* משנת 1996, שבה נדון עניינו של עד תביעה, אזרח ותושב סיני, שהרשויות בסין העבירו אותו לארצות הברית על מנת שיעיד שם במשפט פלילי בעברות סמים.<sup>46</sup> עדותו של ואנג נגבתה בידי הרשויות בסין באמצעים פסולים, שכללו איומים קשים, מניעת שינה ואוכל ועוד. במסגרת ההליך המשפטי בארצות הברית נטען לאי־קבילות ההודעות שנגבו מוואנג בסין, מחמת פגיעתן בזכות השתיקה שלו לפי התיקון החמישי לחוקה האמריקנית. בית המשפט הפדרלי לערעורים החיל את הגנת התיקון החמישי לחוקה על ואנג בנימוק שזכות זו חלה על כל אדם ולא דווקא על אזרחי ארצות הברית או תושביה. בכך ביקש בית המשפט ליישב את תוצאתו עם תוצאת ההליך השיפוטי בעניין *Verdugo-Urquidez*. במילים אחרות, בית המשפט החיל בעניין *Wang* את החוקה האמריקנית החלה אקס טריטוריאלית ופונקציונלית, תלוית־זכות.

במשפט הקנדי נודעת פרשת *R. v. Cook*, שדובר בה בחקירת רצח של נהג מונית קנדי בידי אזרח אמריקני ששב לארצות הברית. אותו אזרח נעצר בארצות הברית ולימים הוסגר לקנדה. בעודו עצור בארצות הברית נחקר באזהרה בידי חוקרים קנדים, בהסכמת הרשויות האמריקניות. כשהתנהל משפטו של הנאשם בקנדה, הוא התנגד להגשת הודעתו אשר נגבתה בידי החוקרים הקנדים על אדמת ארצות הברית בטענה שלא יודע כדבעי בדבר זכותו לעורך דין, על פי הדרישה שמעוגנת בסעיף 10(b) של הצ'רטר הקנדי. בית המשפט העליון הקנדי קבע כי המשפט החוקתי הקנדי מחייב את החוקרים הקנדים בכל מקום שבו הם פועלים מכוח אזרחותם הקנדית, ומכאן שאם לא מילאו את דרישות הצ'רטר הקנדי, דינה של ההודעה להיפסל ולא להיות מוגשת לבית המשפט.<sup>47</sup>

הלכת *Cook* נהפכה בפרשת *R. v. Hape*, שהוכרעה בבית המשפט העליון הקנדי בשנת 2007. באותו מקרה שלל בית המשפט העליון את אפשרותו של אזרח קנדי שהואשם בעברות של הלבנת הון לטעון לתחולת הצ'רטר הקנדי בדבר זכויות וחירויות אזרח, כנגד פעולת רשויות

45 אולם יש לשים לב לשני הבדלים בין פרשת *Verdugo-Urquidez* לבין פרשת *Reid*: האחד, בעניין *Verdugo-Urquidez* דובר בנאשם שאינו אזרח אמריקני, ואילו בעניין *Reid* דובר באזרחית אמריקנית; השני, בפרשת *Verdugo-Urquidez* דובר בתיקון הרביעי לחוקה האמריקנית, ואילו בעניין *Reid* דובר בתיקונים החמישי והשישי לחוקה. עם זאת בפרשת *Verdugo-Urquidez* לא צוין במפורש כי הכוונה היא להבחין בין הזכות לפי התיקון הרביעי לחוקה האמריקנית לבין הזכות לפי התיקון החמישי. לתמיכה בעמדה שהבחנה בין תוצאת פסק הדין בעניין *Reid* לבין תוצאת פסק הדין בעניין *Verdugo-Urquidez* נעוצה בשאלת האזרחות ולא בשאלת סוג הזכות החוקתית, ראו למשל Susan Freiwald, *Electronic Surveillance at the Virtual Border*, 78 Miss. L.J. 329, 349–350 (2008).

46 ראו *Wang v. Reno*, 81 F.3d 808 (9th Cir., 1996).

47 ראו *R. v. Cook*, [1998] 2 S.C.R. 597 (Ca.).



החקירה בקנדה לאיסוף ראיות נגדו באיי טורקס וקאיקוס שבקריביים, שאינם חלק מהטריטוריה הקנדית.<sup>48</sup> בית המשפט נימק את החלטתו בשני מסלולים שונים, מסלול פנימי ומסלול חיצוני. על פי המסלול הפנימי, התבונן בית המשפט העליון הקנדי על הצ'רטר הקנדי כשלעצמו, במנותק מהמדינות הזרות, וקבע כי אין לצ'רטר תחולה חוץ-טריטוריאלית. על פי המסלול החיצוני, התבונן בית המשפט על השלכות התחולה האקסטרה-טריטוריאלית של הצ'רטר וקבע כי החלה אקסטרה-טריטוריאלית כאמור יש בה כדי לפגוע בריבונותן של המדינות שבהן יוחל הצ'רטר בפועל. מעניין כי הרטוריקה בעניין *Cook* הייתה של הטלת חובות חוקתיות על אנשי הרשות החוקרת הקנדית, ואילו הרטוריקה בעניין *Hape* הייתה של בחינת הזכויות החוקתיות של הנאשם הקנדי. בית המשפט העליון ביקר בעניין *Hape* את הלכת *Cook* באמרו שבטעות נתפשה בה סוגיית התחולה האקסטרה-טריטוריאלית של הצ'רטר הקנדי כסוגיה מתחום סמכות התחיקה הבין-לאומית, ובפועל מדובר בסוגיה מתחום סמכות האכיפה הבין-לאומית. עוד על פי הביקורת בפסק דין *Hape*, כיוון שסמכות תחיקה יכולה לשאת אופי בין-לאומי, ואילו סמכות אכיפה היא טריטוריאלית באופן דווקני יותר, נבעה הטעות של פסק דין *Cook*. בפועל, נראה כי הטעות היא הפוכה: בפסק דין *Hape* שגו לראות בסוגיית תחולת הצ'רטר סוגיה מתחום סמכות האכיפה הבין-לאומית, ואילו בפועל מדובר בסוגיה מתחום סמכות התחיקה. זאת כיוון שהצ'רטר כשלעצמו, כדין חרות, לא נאכף מחוץ לקנדה, אלא רק נבחנת פרישתו על פעילות מחוץ לקנדה.<sup>49</sup>

פרשה קנדית נוספת שסייגה את הפרשנות הטריטוריאלית-הדווקנית שיכולה להילמד מעניין *Hape* היא פרשת *Khadr*. באותו מקרה דובר באזרח קנדי שנעצר באפגניסטן בהיותו קטין והושם במתקן המעצר שבמפרץ גואנטנמו שבקובה. הלה נחקר בידי חוקרים מהמודיעין הצבאי הקנדי, ותוצאות החקירה הועברו לידי הרשויות האמריקניות לצורך העמדתו לדין בגין עברות רצח. חקירתו לא התנהלה על פי הוראות הצ'רטר הקנדי לזכויות וחירויות אזרח, תוך הפרת זכותו לחירות והפרת זכותו לגילוי חומר חקירה. בית המשפט העליון הקנדי הכריז על פגיעה בזכויותיו החוקתיות של הנאשם על בסיס הקביעה שהפרות החוקרים הקנדים עולים כדי פגיעה בסטנדרטים של משפט זכויות האדם הבין-לאומי, וכאשר מדובר בפגיעה ברמה בסיסית זו של זכויות חוקתיות, הרי שיש לפרוש הגנה חוקתית על הנאשם גם אם מדובר בפעולת חקירה מחוץ לטריטוריה הקנדית. במילים אחרות, ניתן לראות בעניין *Khadr* משום החלה פונקציונלית של ההגנות החוקתיות הקנדיות על אזרחים מחוץ לטריטוריה.<sup>50</sup>

48 ראו R. v. Hape, [2007] SCC 26 (Ca.) מפסק הדין עולה כי השוטרים הקנדים פעלו על פי היתר ובליווי של קצין משטרה של איי טורקס וקאיקוס, ולכן מבחינת סמכות האכיפה הבין-לאומית לא התעוררה שאלה אלא רק מבחינת היקף פרישתה של הגנת המשפט החוקתי הקנדי. לחזרה על הלכה זו, ראו Amnesty Int'l Can. v. Canada (Chief of Def. Staff), [2008] F.C.R. 546 (Ca.).

49 ראו Pierre-Hugues Verdier, *International Decision: R. v. Hape*, 102 AM. J. INT'L L. 143, 147 (2008); John H. Currie, *Khadr's Twist on Hape: Tortured Determinations of the Extraterritorial Reach of the Canadian Charter*, 42 CAN. Y.B. INT'L L. 307, 317-318 (2008).

50 ראו Canada v. Khadr, [2008], 2 S.C.R. 125 (Ca.); Canada v. Khadr, [2010] 1 S.C.R. 44 (Ca.) (הפרת זכותו של הנאשם לחירות).

בסיכומו של דבר, ניתן לומר כי בצד התפישה הבסיסית הטריטוריאלית באשר להגנות החוקה המדינתית יש כמה "גלישות" בנוגע לטריטוריות שבהן המדינה מפעילה דה פקטו את סמכותה וכן כמה "גלישות" פונקציונליות המתרחשות במצבים מסוימים שבהם הותר למדינה החוקרת, בהסכמת המדינה הזרה, להפעיל סמכויות אכיפה מחוץ לטריטוריה.<sup>51</sup> קשה להצביע בשלב זה על כיוון מובהק של השינוי הפרדיגמתי בנוגע לתחולתו האקסטררה-טריטוריאלית של המשפט החוקתי המדינתי. כעת אבקש לעבור לסוגיית הפרישה החוקתית במסגרת חקירה פלילית במרחב הסייבר.

### 3. פרישת הזכויות החוקתיות כנגד הפעלת סמכות אקסטררה-טריטוריאלית במרחב הסייבר

החקירה הפלילית במרחב הסייבר מקימה באופן אינהרנטי צורך באיסוף ראיות האגורות במחשבים מחוץ לטריטוריה של המדינה החוקרת. התפישה הטריטוריאלית, התוחמת את גבולות החקירה הפלילית במרחב הסייבר לראיות האגורות בשטחה של המדינה החוקרת, מביאה לכך ששאלת הפרישה האקסטררה-טריטוריאלית של ההגנות החוקתיות אינה מתעוררת במלוא עוצה. עם זאת ביקרתי בפרק ג את ההצדקות להמשך קיומן של המגבלות הטריטוריאליות כפי שהוצבו על החקירה הפלילית במרחב הסייבר. אם תיפרץ התפישה הטריטוריאלית, והמדינות תבצענה מהלכים אקסטררה-טריטוריאליים באכיפה הפלילית במרחב הסייבר, הרי שתתעורר במלוא עוצה שאלת פרישתן האקסטררה-טריטוריאלית של הזכויות החוקתיות של הנחקר ושל יתר מושפעי החקירה כנגד פעולת הרשות החוקרת.

קשה לדלות מסקנה ברורה בנוגע למצב המשפטי הנוהג באשר לסוגייתנו בשל תחולתה של התפישה הטריטוריאלית על פעולתה של הרשות החוקרת במרחב הסייבר. בכל זאת ניתן לומר, באשר לפסיקה האמריקנית לפחות, כי נקודת המוצא היא שההגנה החוקתית חלה על פי הפרישה הטריטוריאלית של האינטרנט באופן שהיא חלה על פעולות איסוף של המדינה החוקרת המתייחסות לראיות המצויות בטריטוריה המדינתית, ומנגד היא אינה חלה על פעולות איסוף כלפי ראיות המצויות מחוץ לטריטוריה המדינתית.<sup>52</sup>

אם תוכרנה חריגות אקסטררה-טריטוריאליות בנוגע לחקירה הפלילית במרחב הסייבר, תרבינה השאלות באשר לפרישה אקסטררה-טריטוריאלית של הגנות החוקה על חקירה פלילית במרחב. הפסיקות השונות שהצגתי לעיל בנוגע להפעלת סמכות אכיפה אקסטררה-טריטוריאליות במרחב הפיזי אינן מלמדות על כלל ברור שניתן למצות מהן. בנוסף, הדיון בהקשר המקוון מורכב מזה שהתעורר עד כה בפסיקות בנוגע למרחב הפיזי. המקרה הטיפוסי שתואר בנוגע

51 זו גם המסקנה העולה מהניתוח של Keitner, לעיל ה"ש 42, ושל אורגד, לעיל ה"ש 19.

52 ראו United States v. Gorshkov, 2001 WL 1024026 (W.D. Wash., 2001), שם נקבע כי פעולה של חוקרי ה-FBI כלפי שרת רוסי לא תיבחן לפי הגנות החוקה האמריקנית, אולם ברגע שהמידע יגיע לארצות הברית, כל פעולה נוספת בנוגע למידע תיבחן לפי הגנות החוקה; Suzlon Energy Ltd. v. Electronic Communications Privacy Act (ECPA), 671 F.3d 726 (9th Cir., 2011), שם נפסק כי ה-ECPA אינה חלה על מידע של תושב זר האגור בשרתים אמריקניים. במילים אחרות, המבחן הוא טריטוריאלי ולא פרסונלי (שאז במקרה Suzlon לא הייתה מוחלת ההגנה החוקתית האמריקנית).

למרחב הפיזי נגע בפעולות חקירה פרונטליות של הרשות החוקרת כלפי חשודים, דהיינו פעולות של מעצר, חקירה כחשוד וכדומה, ולא בפעולות איסוף ראיות דוממות. ייתכן שניתן להסביר זאת בכך שבחקירה במרחב הפיזי המצב השכיח 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. היות שהופעלו סמכויות מעצר וחקירה פרונטלית, הדיון באיסוף הראיות נבלע בתוך הדיון בהפעלת הסמכויות הפרונטליות, ולא נדרשה הפרדה עיונית שלו. לעומת זאת הסיטואציות המקוונות האקסטר-טריטוריאליות הן מגוונות ומורכבות יותר. ספקטרום המצבים נוצר ממטריצה הכוללת את הפרמטרים האלה: מקום הימצא הראיה הדיגיטלית, מקום הימצא החוקר, מקום מושבו<sup>53</sup> של יעד פעולת האיסוף,<sup>54</sup> מקום מושבם של יתר מושפעי פעולת האיסוף (צדדים שלישיים כגון ספקי שירות או אנשים שמידע על אודותיהם מצוי ברשות יעד פעולת האיסוף). אציג את קשת המצבים בטבלה להלן (טבלה 5.1):<sup>55</sup>

טבלה 5.1 – ספקטרום הסיטואציות האקסטר-טריטוריאליות בחקירה פלילית במרחב הסייבר

הערכים				הפרמטרים	
				מדינה M	מיקומו של החוקר
			מדינה זרה N	מדינה M	מיקום הראיה המבוקשת
		מדינה זרה O	מדינה זרה N	מדינה M	מקום מושבו של יעד הפעולה
	מדינה זרה P	מדינה זרה O	מדינה זרה N	מדינה M	מקום מושבו של צד שלישי המושפע מהפעולה
מדינה זרה Q	מדינה זרה P	מדינה זרה O	מדינה זרה N	מדינה M	מקום מושבו של צד שלישי נוסף המושפע מהפעולה

53 למעשה ייתכן להרחיב כאן את האפשרויות לשתיים: מדינת אזרחות לחוד ומדינת תושבות לחוד, כיוון שהאזרחות והתושבות בפועל יכולות להיות שונות, ולכאורה התושבות יכולה להקנות הגנה חוקתית עצמאית מהאזרחות.

54 בדרך כלל יעד הפעולה הוא חשוד, אולם הוא יכול להיות גם עד שמופעלות כלפיו סמכויות איסוף ראיות לצורך חקירת עברה מסוימת.

55 כמה הבהרות לטבלה: ראשית, ההנחה היא שהחוקר פועל במדינתו שלו (מדינה M). אם הוא פועל פיזית מחוץ למדינתו, הרי שאנו בסיטואציה אקסטר-טריטוריאלית בהקשר פיזי ולא בהקשר מקוון, ואין זה ממין ענייננו בשלב זה של הדיון. שנית, הכוונה בערך "מדינה זרה N" לכל מדינה אחרת בעולם שאינה המדינה M. הכוונה בערך "מדינה זרה O" לכל אחת מהמדינות האחרות בעולם שאינן המדינה M או המדינה N, וכך הלאה. שלישיית, בחרתי כאן, שרירותית, לציין שני צדדים שלישיים הנפגעים מפעולת האיסוף במרחב הסייבר. בפועל יכולה להיות חקירה פלילית במרחב הסייבר שתפגע בצדדים שלישיים שונים רבים יותר, ואז הטבלה תישא פרמטרים רבים יותר וערכים שונים אפשריים רבים יותר. כן יכולה להיות לכאורה חקירה פלילית במרחב הסייבר שלא תכלול פגיעה ממשית בזכויות חוקתיות של צדדים שלישיים, שאז הטבלה תיראה מצומצמת יותר. רביעית, פעולות איסוף ראיות במרחב הסייבר, שהן גורפות באופיין, מגלמות, לצד הפגיעה ביעד פעולת האיסוף ובצדדים שלישיים שונים, גם פגיעה בכלל ציבור משתמשי המרחב המקוון. הדוגמה המובהקת ביותר לכך היא הטלת חובות שימור מידע דרך קבע (Retention) שהן גורפות ואינן תלויות בחשד קונקרטי.

על טבלה זו ניתן להרכיב את שני סוגי הדיונים בשאלת פרישת הזכויות החוקתיות: שאלת הפרישה האקסטרה-טריטוריאלית של דיני החוקה של המדינה השופטת ושאלת התחשבותה של המדינה השופטת בהגנות חוקתיות של מדינות זרות. אמחיש זאת בדוגמה להלן המבוססת על רצף ההנחות האלה: נניח שמדינה M היא המדינה החוקרת/השופטת. רשויות החקירה במדינה M חוקרות עברה של הפצת תכנים פדופיליים באינטרנט.<sup>56</sup> החוקר פועל מתוך מדינה M. מבחינת מדינה M העברה נחשבת גם עברת פנים מבחינת סמכות התחיקה והשפיטה שלה. החוקר מבקש לחדור, במסגרת החקירה, לחומרי מחשב האגורים במדינה אחרת (מדינה N), למשל לשרת אחסון שבו החשוד משתמש, שם מצופה כי ימצאו תכנים פדופיליים וראיות להפצתם של תכנים אלה. החשוד מתגורר דרך קבע במדינה שלישיית (מדינה O). בנוסף, שרת האחסון שבמדינה N מוחזק בידי ספק שירותי אירוח ממדינה P. הנה כי כן, ארבע מדינות שונות – מדינות M, O, N, P – נוגעות בסיטואציה החקירתית האמורה. מבחינת בית המשפט במדינה M שאלה אחת היא אם חל משפט החוקתי על הסיטואציה החקירתית האקסטרה-טריטוריאלית האמורה. השאלה השנייה היא אם משפט החוקתי של מי מהמדינות האחרות – P, O, N – כולן, חלקן או אחת מהן בלבד – חל על הסיטואציה החקירתית, ואם על בית המשפט של המדינה M להתחשב בהגנות החוקתיות של המדינות האחרות – P, O, N – נוסף על ההגנות החוקתיות של מדינה M עצמה או במקומן.

הדוגמה הזו היא של חקירה פלילית במרחב המקוון, הפורצת את חסמי התפישה הטריטוריאלית וכוללת איסוף חומר האגור במחשבים מחוץ לטריטוריה של המדינה החוקרת. פריצת התפישה הטריטוריאלית מביאה לריבוי מקרים של תחולה מקבילה של דיני החוקה של מדינות שונות על פעולת איסוף הראיות. אציין כי גם ללא פריצת התפישה הטריטוריאלית במרחב הסייבר, כאשר את פעולת האיסוף יבצע שוטר ממדינה M, שישנה פיזית במדינה M ויחדור לחומרי מחשב האגורים בשטחה של מדינה M, עדיין יכולות להתעורר שאלות של ברת דינים חוקתית (השאלה מן הסוג השני דלעיל), שכן החשוד יכול להיות במדינה N, וצדדים שלישיים המושפעים מפעולות האיסוף יכולים להיות במדינה O. ככל שהחשוד והצדדים השלישיים ייפגעו מפעולת האיסוף, אזי גם העובדה שהפעולה לא יצאה מגדר הטריטוריה של מדינה M אינה מחסנת מפני טענה לתחולה של הגנות דיני החוקה של מדינות N ו-O. עד כאן פרשתי את קשת הסיטואציות האפשריות במקרה של חקירה פלילית במרחב הסייבר. האם ראוי להצדיק את הפרישה האקסטרה-טריטוריאלית של ההגנות החוקתיות בסיטואציות אלה?

#### 4. הצדקות לפרישה אקסטרה-טריטוריאלית של ההגנות החוקתיות בחקירה הפלילית במרחב הסייבר

את שאלת ההצדקות לפרישה אקסטרה-טריטוריאלית<sup>57</sup> של ההגנות החוקתיות אפרק לשאלות משנה: האחת, אם ראוי להכיר בתחולה אקסטרה-טריטוריאלית של דיני החוקה של

56 במונחי הדין הישראלי תהיה זו עברה על סעיף 214(ב) לחוק העונשין, התשל"ז-1977 (להלן – חוק העונשין).

57 במונחי טבלה 5.1 לעיל, הכוונה בפעולה אקסטרה-טריטוריאלית לכל מקרה שבו אחד (או יותר) מהפרמטרים האלה – מיקום הראיה המבוקשת, מיקום יעד הפעולה ומיקומו של צד שלישי המושפע מהחקירה – נמצא במדינה זרה.

המדינה החוקרת כאשר הרשות החוקרת פועלת לאיסוף ראיות דיגיטליות האגורות מחוץ לטריטוריה המדינתית; השנייה, אם במסגרת חקירה פלילית במרחב הסייבר ראוי להכיר בתחולה של הגנות החוקה של מדינות אחרות הנוגעות בסיטואציה החקירתית, בין שהמדינה החוקרת פעלה לאיסוף ראיות דיגיטליות האגורות מחוץ לטריטוריה שלה ובין שפעלה לאיסוף ראיות האגורות בשטחה אך שייכות לתושב זר. על פי המודל הטריטוריאלי לפרישת ההגנות החוקתיות, שתי השאלות תיענינה בשלילה. אולם כפי שראינו ביחס למרחב הפיזי, כך גם לגבי המרחב המקוון יש לראות במודל הטריטוריאלי משום נקודת מוצא ולא נקודת סיום של הניתוח בדבר היקף הפרישה של הגנות החוקה.

### א) פרישת דיני החוקה של המדינה החוקרת בעת פעולתה לאיסוף ראיות האגורות מחוץ לטריטוריה

ראשית לכול, יש לשוב לדיון שערכתי בפרק ג בתפישה הטריטוריאלי באשר לדיני איסוף הראיות בחקירה פלילית במרחב הסייבר. כזכור, ההנחה כי איסוף הראיות ממחשבים המצויים מחוץ לטריטוריה המדינתית היא פעולה אקסטרה-טריטוריאלי אינה אלא הנחה התלויה באימוץ התפישה הטריטוריאלי. ככל שההתמקדות היא במקום הימצא הראיה, אכן מדובר בפעולה אקסטרה-טריטוריאלי. מנגד, ככל שההתמקדות היא ברשות החוקרת, אין מדובר בפעולה אקסטרה-טריטוריאלי, שכן החוקר פועל ממדינתו. לעומת זאת אם ההתמקדות היא בנחקר ובצדדים השלישיים המושפעים מפעולת האיסוף, הרי שאלה יכולים להימצא במדינה החוקרת גם אם המידע הנאסף על אודות הנחקר אגור מחוץ לטריטוריה: במקרה שכזה יהיה ניתן לטעון שהגם שהראיה אגורה מחוץ לטריטוריה, הרי שפעולת האיסוף משפיעה על מי שנמצא בטריטוריה של המדינה החוקרת בלבד.

כפי שניתחתי בפרק ג, המבחן הנוהג כיום הוא מבחן מקום הימצא הראיה, ולכן פעולות איסוף במרחב הסייבר ביחס לראיות האגורות מחוץ לטריטוריה של המדינה החוקרת תיחשבנה לפעולות אקסטרה-טריטוריאליות. כפי שאטען להלן, גם מתוך התבוננות זו יש מקום להכיר בפרישתן של ההגנות החוקתיות על פעולות האיסוף החלות כלפי ראיות דיגיטליות המצויות מחוץ לטריטוריה של המדינה החוקרת. זאת על בסיס ההצדקות האלה:

1. יש לראות בדיני החוקה לא רק מרסנים את פעולת הרשות אלא גם מכוונים את סמכותה ואת אופן פעולתה. רשויות המדינה יונקות את חיותן מדיני החוקה. המגבלות על סמכותן של רשויות המדינה הן חלק מהגדרת הסמכות עצמה, ומגבלות אלה מנויות בדיני החוקה. מכאן שדיני החוקה אינם מכוונים לאזרחים בלבד אלא גם לרשויות. עמדה זו רואה ברשויות המדינה מושאי הסדרה של דיני החוקה במקביל לפרטים שהם נשאי זכויות מכוח דיני החוקה. מעמדה זו נובע שהרחבת הסמכות לפעול אקסטרה-טריטוריאלי גוררת עמה, אוטומטית, את החובה הצמודה לפעול על פי ההגנות החוקתיות, וגם זאת באורח אקסטרה-טריטוריאלי.<sup>58</sup> על פי תפישה זו, יש לראות במשפט החוקתי משפט של חובות (המוטלות על הרשות) ולא רק של זכויות (של האזרחים).

58 ראו NEUMAN, לעיל ה"ש 25, בעמ' 6; Gerald L. Neuman, *Extraterritorial Rights and Constitutional Methodology after Rasul v. Bush*, 153 U. PA. L. REV. 2073, 2077 (2005).

לכאורה, על פי הסיווג המוכר של הופלד (Hohfeld) למושגי הזכות, החובה, הכוח והחסינות,<sup>59</sup> הזכות (Right) עומדת בקורלציה מלאה לחובה (Duty), ומכאן שאין כל הבחנה בין התבוננות על הזכות לבין התבוננות על החובה. ההבחנה היא רק מבחינת נקודת המבט. זכותו של א היא חובתו של ב לכבד את זכותו של א. וכך, בהקשרנו, הזכות החוקתית של אדם מסוים היא החובה של המדינה לכבד את אותה זכות חוקתית. הופלד לא התייחס בכתיבתו לממד האקסטרה-טריטוריאלי המסבך את התיאור הקורלטיבי הישיר ה"נקי" שלו. כשמדינה א מפעילה סמכות פוגענית בטריטוריה של מדינה ב (כאשר כל סמכות אכיפה, ובכללה סמכות איסוף ראיות, תיחשב סמכות הפוגעת בזכויות חוקתיות), לא ברור אם חובתה של מדינה א היא לכבד את זכויותיו החוקתיות של נפגעי הפעלת הסמכות לפי הנורמות החוקתיות של מדינה א או של מדינה ב. למעשה, על בסיס הקורלציה ההופלדיאנית, לא ברור אם זכותו החוקתית של אזרח מדינה א היא כלפי מדינה א בלבד, או אולי כלפי כל מדינה כאשר היא פועלת מחוץ לטריטוריה שלה ומשפיעה על אזרח מדינה א, או אולי גם כאשר היא פועלת בטריטוריה שלה אך משפיעה על אותו אזרח של מדינה א. במילים אחרות, בבואנו לבחון סיטואציות אקסטרה-טריטוריאליות, יש מקום להתבונן בנפרד על הטוענים לזכויות חוקתיות ועל המחויבים בכיבוד הזכויות החוקתיות, שכן הקורלציה ההופלדיאנית אינה מייצרת חפיפה אוטומטית בין החובה החוקתית לבין הזכות החוקתית.

2. ההחלה האקסטרה-טריטוריאלית של הגנות החוקה, כל אימת שהמדינה פועלת מחוץ לגבולות הטריטוריה שלה, אינה בעלת ערך מגביל בלבד מבחינתה של המדינה, אלא גם בעלת ערך מסייע למדינה: החוקה "מסייעת" להגביר את הלגיטימציה – הן הפנים-מדינתית והן הבין-לאומית – לפעולה השלטונית. בנוסף, ככל שבית משפט מבצע את האיזון החוקתי, הביקורת השיפוטית החוקתית מפחיתה את האפשרות לטעויות בהפעלת שיקול הדעת המנהלי בעת הפעולה האקסטרה-טריטוריאלית. הסבר זה מציג, לכאורה, אינטרס של המדינה עצמה בהחלת דיני החוקה שלה באורח אקסטרה-טריטוריאלי.<sup>60</sup> טענה ברוח דומה נטענה בעבר באשר להחלת ביקורת בג"ץ על פעילות צה"ל בשטחי יהודה, שומרון ועזה. על פי טענה זו, הביקורת הבג"צית מייצרת בסיס לגיטימציה משפטי לכיבוש הצבאי, הן בעיני תושבי מדינת ישראל והן בזירה הבין-לאומית.<sup>61</sup>

59 ראו Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16 (1913) WESLEY NEWCOMB HOHFELD, FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING (1946).

60 לטעון זה ראו Galia Rivlin, *Constitutions Beyond Borders: The Overlooked Practical Aspects of the Extraterritorial Question*, 30 BOSTON U. INT'L L.J. 135 (2012) STEPHEN HOLMES, PASSIONS AND "Constraints can be enabling": CONCONSTRAINTS: ON THE THEORY OF LIBERAL DEMOCRACY 11 (1995). הולמס ניתח חוקות במדינות ליברליות וטען כי חוקות לא רק מגבילות כוח של הריבון אלא גם מבססות את סמכותו ומעניקות לו חוסן ותמיכה. גליה ריבלין הציגה יישום מפורט של תובנה יסודית זו בהקשר של פעולה מדינתית אקסטרה-טריטוריאלית.

61 ראו Ronen Shamir, "Landmark Cases" and the Reproduction of Legitimacy: The Case of Israel's High Court of Justice, 24 LAW AND SOCIETY REV. 781 (1990) DAVID KRETZMER, THE OCCUPATION OF JUSTICE: THE SUPREME COURT OF ISRAEL AND THE OCCUPIED TERRITORIES 190 (2002).

אם לסכם עד כאן, קיימות הצדקות לחייב את המדינה החוקרת להחיל חובות חוקתיות בעת שהיא מפעילה סמכויות איסוף ראיות במסגרת חקירה פלילית במרחב הסייבר. מקום הימצא הראיה, פרמטר שהפך לאבן הבוחן לקביעה אם מדובר בפעולה אקסטרה-טריטוריאלית, אינו צריך להשפיע על חיוב בכיבוד הזכויות החוקתיות המחייבות במדינה החוקרת. נובע מן האמור שיש מקום להחיל מודל אוניברסלי מבחינת פרישת הזכויות החוקתיות בחקירה הפלילית במרחב הסייבר. מקובל לראות במודל האוניברסלי מודל הנשען על תאוריות בדבר זכויות טבעיות במשפט או בדבר צדק גלובלי.<sup>62</sup> עם זאת ההצדקות שמניתי לעיל נשענות על הנחות הפוכות, כי הסטנדרט החוקתי במדינות השונות אינו אחיד, ובשל האינצידנטליות של מקום הימצא הראיה, פעמים רבות, הרי שיש להמשיך ולהחיל את ההגנות החוקתיות של המדינה החוקרת באשר לכל מידע במרחב הסייבר שאותו היא אוספת.

### ב) פרישת דיני החוקה של מדינות אחרות על פעולתה של המדינה החוקרת במרחב הסייבר

למעשה, יש לחלק כאן את הדיון לשניים: מקרה שבו המדינה החוקרת אוספת ראיות דיגיטליות האגורות מחוץ לטריטוריה שלה, קרי כאשר המדינה החוקרת פועלת אקסטרה-טריטוריאלית, במונחי התפישה הטריטוריאלית, ומקרה שבו המדינה החוקרת אוספת ראיות דיגיטליות האגורות בטריטוריה שלה, אך אלה קשורות לתושבי חוץ הטוענים לתחולת משפט חוקתי זר על הסיטואציה החקירתית.

אשר למקרה שבו הרשות החוקרת תפעל באורח אקסטרה-טריטוריאלית (במשקפי התפישה הטריטוריאלית) במרחב הסייבר: במקרה זה אפשר שיתרחש מתקל דינים חוקתי, שלפיו כמה שיטות משפט, על דיני החוקה שלהן, תאחזנה בסיטואציה. תנאי מקדמי להתרחשות מתקל דינים חוקתי במקרה הנדון הוא שהמדינה הזרה, שבנוגע אליה פועלת המדינה החוקרת, תבקש להחיל את הגנות החוקה שלה אקסטרה-טריטוריאלית כלפי המדינה החוקרת. ציינתי לעיל כי בפועל בררת דינים חוקתית אינה עניין שבית המשפט שוקל בהקשר של אכיפה פלילית. עם זאת העיקרון שלפיו מדינה יכולה להכיר בנורמות ממשפטן של מדינות אחרות אינו זר במשפט הבין-לאומי, והוא יכול לנבוע מעיקרון של הדדיות (Comity). עיקרון זה אומץ למשל במשפט האמריקני,<sup>63</sup> ובמובנים מסוימים שלו גם במשפט הישראלי.<sup>65</sup> עקרון ה-Comity יכול

62 ראו NEUMAN, לעיל ה"ש 25, בעמ' 5-6; Posner, לעיל ה"ש 25, בעמ' 33-34.

63 ראו Hilton v. Guyot, 159 U.S. 113, 164 (1895), שם הוגדר עיקרון ה-Comity כ-

"The recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws."

כן ראו Société Nationale Industrielle Aérospatiale v. United States Dist. Court., 482 U.S. 522, 555 (1987); In re French v. Liebmann, 440 F.3d 145, 151-152 (4th Cir., 2006).

64 ראו לדוגמה את פסק הדין בעניין Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers, [2004] 2 S.C.R. 427 (Ca.) הדין, בהקשר של אחריות ספקיות שירות באינטרנט להפרת זכויות יוצרים. עם זאת כעולה מפסק הדין, עקרון ה-Comity, המדבר בהדדיות, נושא פן פנימי ופן חיצוני: בפן הפנימי – יישום העיקרון הוא על דרך של הכרה בדין זר

לכאורה להיות הצינור לכיבוד ולהחלה בפועל של דיני החוקה של שיטות משפט זרות במשפט המקומי. עיקרון זה נולד כעיקרון "רך" למדי, המקובל בעיקר במשפט האזרחי. הוא נקלט תחילה כעיקרון של נימוסין מתחום היחסים הבין-לאומיים,<sup>66</sup> אך עם עיגונו במשפט הפנימי של המדינות הפכה הפסיקה המאמצת אותו למחייבת התחשבות מצד בתי המשפט מכוח עקרון התקדים המחייב.<sup>67</sup>

הערך המרכזי ביישום עקרון ה-Comity הוא בהרחבת בסיס הלגיטימציה הבין-לאומית של המדינה המחילה אותו במשפט הפנימי. במילים אחרות, ככל שמדינה מחילה על עצמה את עקרון ה-Comity, כך פעולתה האקסטרטריטוריאלי מרוככת, שכן האינטרסים של המדינות הזרות מבוטאים ומשוקללים בפעולתה גם אם הגורם המשקלל אותם אינו המדינות הזרות. גמישותו של סטנדרט ה-Comity, שהחלתו היא פרי שיקול דעת ואינה מחויבת על פי כלל אצבע קשיח,<sup>68</sup> יכולה לכאורה לאפשר ייבוא זהיר של הגנות חוקתיות זרות במסגרת פעולת איסוף אקסטרטריטוריאלי במרחב הקיברנטי. הייבוא כאמור יכול להיות מותנה בנסיבות האלה:

1. עצמת הפגיעה בזכות החוקתית הזרה.
2. השאלה אם מדובר בזכות חוקתית תלוית-סטטוס משפטי, כאשר הסטטוס המשפטי מוגבל בתחולה טריטוריאלי. כך למשל חסינות דיונית של חבר כנסת מתקיימת רק במדינת ישראל ולא במדינה זרה. עם זאת במדינות זרות מוכרת חסינות דיונית של חבר פרלמנט, אלא

במסגרת הדין המקומי, ובפן החיצוני – יישום העיקרון הוא על דרך של בחינת מידת הריסון של הדין המקומי מלחול ולהתפרש אל מעבר לטריטוריה המדינתית. ניתן לקשור בין שני הפנים ולומר כי ריסונו של הדין הפנימי מפני תחולה אקסטרטריטוריאלי נובע מכך שהדין הזר מיושם, וההוראות הנקובות בו מונעות את החלת הדין הפנימי במקרה הנדון.

65 ראו, בהקשר של אכיפת פסקי חוץ, את ע"א 970/93 היועץ המשפטי לממשלה נ' אגם, פ"ד מט(1) 561, 571–572 (1995); ה"פ (מחוזי ת"א) 820/08 Intrinsyc Software International Inc. נ' זטה טכנולוגיות תוכנה בע"מ, בעמ' 11–12 (פורסם בנבו, 31.1.2010); בש"א (מחוזי י-ם) 7333/04 Steen נ' הרפובליקה האיסלמית של אירן, בפס' 46 (פורסם בנבו, 4.12.2008). כן ראו בהקשר של בקשה להוצאת צו חוסם מפני ניהול תביעה מקבילה בניו יורק לזו המתנהלת בישראל, ראו רע"א 778/03 אינטר-לאב בע"מ נ' Engineering Project Israel Bio, פ"ד נו(5) 769 (2003); ת"א (מחוזי חי') 292/03 וייס נ' זומריס (פורסם בנבו, 31.3.2004). עוד ראו בהקשר של זכות שתיקה בישראל על דברים של נאשם תושב שווייץ, שעצם אמירתם היא עברה פלילית לפי הדין בשווייץ: ע"פ 196/85 זילברברג נ' מדינת ישראל, פ"ד מד(4) 485, 528–529 (1990) (דעת המיעוט של השופט בך).

66 JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS, FOREIGN AND DOMESTIC, IN REGARD TO CONTRACTS, RIGHTS, AND REMEDIES, AND ESPECIALLY IN REGARD TO MARRIAGES, DIVORCES, WILLS, SUCCESSIONS, AND JUDGMENTS 33 (Reprinted ed. 1972); Joel R. Paul, *Comity* 32 HARV. INT'L L.J. 1, 4 (1991) (Paul) *ציין כי עקרון ה-Comity* אופיין, ברבות השנים, שלא בעקיבות, לעתים כדוקטרינה מתחום המשפט הבין-לאומי הפרטי, לעתים כדוקטרינה מתחום המשפט הבין-לאומי הפומבי, לעתים כעיקרון מוסרי טבעי, לעתים מנהג ביחסים דיפלומטיים בין-מדינות וללא תוקף משפטי מחייב ועוד. ראו Joel R. Paul, *The Transformation of* Informal Foreign Affairs Formalism: The Act of State Doctrine and the Reinterpretation of *International Comity*, 71 LAW & CONTEMP. PROB. 19, 19–21 (2008); Jake S. Tyshow, *International Comity*, 43 VA. J. INT'L L. 275 (2002); שם סוקר המחבר גישות שיפוטיות שונות בפסיקה האמריקנית לעקרון ה-Comity.

67 ראו Paul, *Comity in International Law*, שם, בעמ' 78.

68 אין זאת אומרת שסטנדרט גמיש אינו יכול לחייב את בתי המשפט. עצם תחולתו של הסטנדרט יכולה להיות מחייבת, אולם מרחב התמרון השיפוטי במסגרת יישום הסטנדרט יכול להיות גמיש.



שהכוונה לפרלמנט של אותה מדינה ולא של מדינה אחרת. במקרה כזה עצם ההכרה בהגנה של חסינות דיונית קיימת בשתי המדינות – המדינה החוקרת והמדינה הזרה – ורק ה"שיבוץ" של נחקר מסוים למסגרת המוכרת של חסינות דיונית הוא שמשנתנה. מצב זה שונה ממצב של ייבוא כלל משפטי חדש שאינו קיים כלל במדינה החוקרת.

3. סוג מתקל הדינים החוקתי: בהקשרנו הנדון יש להבחין בין שתי קטגוריות מצבים: האחת, מצב של מתקל דינים חוקתי הנובע ממקום הימצא הראיה הדיגיטלית הנאספת בלבד; השנייה, מצב של מתקל דינים חוקתי הנובע (גם) ממיקום יעד פעולת האיסוף או הצדדים השלישיים המושפעים ממנה.<sup>69</sup> נראה כי קטגוריית המצבים השנייה דלעיל מקימה טענה חזקה יותר להחלת דיני החוקה של המדינה הזרה במדינה החוקרת. זאת על בסיס התפישה שנשאי הזכויות החוקתיות הם האנשים (יעד הפעולה והצדדים השלישיים) ולא הראיות עצמן.<sup>70</sup> עם זאת מתקל הדינים החוקתי אפשרי בהחלט כאשר גם כאשר יעד פעולת האיסוף או הצדדים השלישיים יושבים במדינה החוקרת, והראיה הדיגיטלית מצויה בטריטוריה של מדינה זרה. זאת כאשר יוכח שהמידע הדיגיטלי במדינה הזרה מוקם שם מתוך כוונה להיכפף לדיניה של אותה מדינה זרה. כך הוא למשל כאשר חברה בין-לאומית הפועלת באינטרנט (נניח ספקית של שירות אינטרנטי כלשהו) מחליטה למקם את שרתיה במדינה מסוימת לצורכי תכנון סביר של ההגנות והסיכונים המשפטיים שיחולו עליה בשל מיקום שרתיה באותה מדינה. לעומת זאת מקרה שבו תוקפה של טענת מתקל הדינים יהא חלש יותר הוא כאשר, נניח, אדם פרטי מחליט למקם את חשבון הדוא"ל שלו אצל ספקית שירות כלשהי, אשר מיקום שרתיה בחו"ל, אך לא ידוע לו במדויק או לא משנה לו במיוחד, ולימים אותו אדם נחקר במדינתו על חשד לביצוע עברה כלשהי, והמדינה אוספת את הדוא"ל שלו, שממוקם כאמור בחו"ל.

עינינו הרואות כי ניתן לפתח מערך שיקולים מפורט למדי בנוגע לנסיבות שבהן ייובאו הגנות החוקה של המדינה הזרה אל המדינה החוקרת דרך עקרון ה-Comity. אולם חרף כל האמור נראה כי קיימות מכשולות מעשיות ניכרות ביישום עקרון ה-Comity בהקשרנו הנדון: ראשית, בעניינינו הדיון השיפוטי בשלב ההסמכה של הרשות החוקרת הוא במעמד צד אחד (ex parte), בנוכחות נציג הרשות החוקרת והשופט בלבד, ולא תהיה אפשרות לנהל דיון על מהות הדין הזר הרלוונטי. כידוע, הדין הזר הוא עניין שבמומחיות ולא בידיעה שיפוטית, ולכן יהא על שופט לשמוע עדים ולקבל חוות דעת באשר לדין הזר, והדבר אינו אפשרי במסגרת הליך במעמד צד אחד; שנית, לא אחת אין בידי רשויות החקירה מידע מלא על זהות החשוד, זהות שאר הנוגעים בדבר (ה"שחקנים" העשויים לטעון להגנות חוקתיות) או אפילו מקום אגירתו של המידע המבוקש, ועל כן לא תהיה כל אפשרות מעשית לשקול את כל השיקולים הצריכים לעניין ולייבא נכונה את ההגנות החוקתיות הזרות; שלישית, הליכי החקירה הם לא אחת הליכים דחופים, בגלל

69 כזכור, שתי קטגוריות מצבים אלה מניחות: (א) שהמדינה הזרה מיישמת מודל תחולה אקסטררה-טריטוריאלית להגנות החוקתיות שלה (שכן מדינה שמיישמת מודל טריטוריאלית בלבד להגנות החוקה שלה אינה מקימה זכות לטעון לפגיעה חוקתית על פי דיניה, כאשר מדינה אחרת פועלת אקסטררה-טריטוריאלית כלפיה); (ב) שפעולת האיסוף היא אקסטררה-טריטוריאלית (במשקפי התפישה הטריטוריאלית). כאמור, בהמשך אדון במצב שבו הפעולה עצמה היא כלפי ראייה האגורה בטריטוריה המדינתית ובכל זאת נטען למתקל דינים חוקתי.

70 אפתח תפישה זו בפרק ו ואכנה אותה התפישה הפרסונלית.

צורכי החקירה, ועל כן אף אם היה ניתן להתגבר על המכשלות הקודמות, לא תהיה אפשרות לערוך דיון שלם בנושא כה מכביד מבחינה משפטית; רביעית, יש לזכור כי בחלק מהמדינות, וגם במדינת ישראל במצבים מסוימים,<sup>71</sup> קיימת סמכות לביצוע פעולות איסוף ראיות בהסמכתו של גוף מנהלי ולא שיפוטי. במקרה כזה האפשרות כי יקוים דיון במעמד שני צדדים ויבחן הדין הזר כדבעי – נראית דמיונית עוד יותר, בעיקר כאשר הגוף המנהלי אינו בהכרח בעל השכלה משפטית.

בסיכומו של דבר, חרף היתרונות העיוניים הגלומים בשימוש בעקרון ה־Comity נראה שהמכשלות המעשיות מייתרות כל אפשרות לערוך, בשלב ההסמכה לביצוע פעולת האיסוף, דיון אמתי בבררת הדינים החוקתית. לכל היותר יוכל בית המשפט לבחון לאחר מעשה, למשל בשלב ההגשה של הראיה במשפט (אם יוגש כתב אישום), את מערך הדינים הזר.

עתה למקרה שבו הרשות החוקרת תפעל בתוך הטריטוריה שלה ולפעולתה תהא השלכה על תושב זר הטוען לתחולת דיני החוקה של מדינתו על הסיטואציה החקירתית. במרץ 2011 הזדמן לבית המשפט בוורגינייה להידרש לשאלת החלתם של עקרונות חוקתיים של מדינה זרה (איסלנד) במסגרת בחינתה של פעולת חקירה באינטרנט. באותו מקרה דן בית המשפט בהתנגדות לצו שהופנה לאתר המסרים החברתיים Twitter לחשיפת פרטי מנוי, פרטי התקשורת, פרטים על אמצעי התשלום ועוד באשר לכמה מנויים, ובהם חברת פרלמנט מאיסלנד ואזרח הולנדי. הרקע להוצאת הצו היה חקירה בקשר לאתר ההדלפות Wikileaks שבו פורסמו רכבות פריטי מידע שסווגו כסודיים מבחינת הממשל האמריקני. המתנגדים לצו טענו לפגיעה בחופש הביטוי ובפרטיותם, לפי התיקון הראשון והרביעי (בהתאמה) לחוקה האמריקנית. בית המשפט דחה את טענותיהם לגופן, אולם ציין באמרת אגב כי הוא מטיל ספק רב אם חברת הפרלמנט האיסלנדית והאזרח ההולנדי זכאים להגנת החוקה האמריקנית במקרה זה, שכן מקום מושבם מחוץ לגבולות ארצות הברית.<sup>72</sup> זאת, הגם שמבחינת התפישה הטריטוריאלית פעולת האיסוף המבוקשת מבוצעת בתוככי ארצות הברית, שכן שרתי Twitter ממוקמים בארצות הברית. יתרה מזאת, חברת הפרלמנט האיסלנדית טענה להגנה חוקתית מיוחדת, של חסינות מתוקף תפקידה על כל דבריה לרבות "ציוציה" בטוויטר. היקף החסינות, כך טענה, לפי הדין האיסלנדי רחב מהיקף החסינות המקבילה לפי הדין האמריקני. בית המשפט האמריקני סירב להחיל את הגנות הדין האיסלנדי ודחה בעניין זה טענות לתחולת עיקרון של Comity.<sup>73</sup> ההנמקה המרכזית של בית המשפט הייתה כי למעשה אין מדובר בפעולת איסוף אקסטר-טריטוריאלית, ועל כן אין מקום להתחשב בשיטות משפט זרות בעניין זה.

הסיטואציה דנן היא של איסוף ראיות דיגיטליות שלא מחוץ לטריטוריה המדינתית. הפעלת הסמכות, לדידה של המדינה החוקרת, היא פנימית בלבד ואינה חורגת מגבולות המותר לכל מדינה על פי המשפט הבינ-לאומי. אולם כיוון שיעד פעולת האיסוף, או צדדים שלישיים המושפעים ממנה, מושבם במדינות אחרות, הם יכולים לבקש לפרוש את הגנת החוקה של

71 כך, למשל, בסעיף 4 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 (להלן – חוק נתוני תקשורת) ובסעיף 7 לחוק האזנת סתר, התשל"ט–1979 (להלן – חוק האזנת סתר).

72 ראו In re Application of the United States, 830 F. Supp. 2d 114 (E.D. Va., 2011).

73 שם, בעמ' 19–22 להחלטה.

מדינת מושבם פרישה אקסטרה-טריטוריאלית אל משפטה הפנימי של המדינה החוקרת.<sup>74</sup> הבעיות המעשיות שציינתי לעיל בנוגע לייבוא הגנות חוקתיות זרות בעת שהמדינה החוקרת פועלת אקסטרה-טריטוריאלית, מתקיימות גם בסיטואציה שלפנינו. נוסף על כך, פעולתה של המדינה החוקרת אינה אקסטרה-טריטוריאלית, אפילו לא במשקפי התפישה הטריטוריאלית. מכאן שהנטייה לייבא עקרונות חוקתיים של שיטות משפט זרות לבחינת פעולתה של הרשות החוקרת בתוך הטריטוריה שלה תהא מוחלשת ביותר, שכן הדבר עלול להיתפש כחתיירה תחת תפישת הריבונות של המדינה החוקרת.

אם לשוב להחלטה בעניין *Twitter*, דומני אפוא שהחלק השני של ההחלטה בדבר אי-החלת ההגנות החוקתיות של משתמשי טוויטר הזרים – תואמת את שתיארתי. לעומת זאת בכל הנוגע לחלק הראשון של ההחלטה, שבו הובעה העמדה שלתושבי המדינות הזרות אשר המידע שלהם אגור בשרתי טוויטר בארצות הברית אין זכות ליהנות גם מהגנות החוקה האמריקנית – עמדה זו סותרת את הצעתי לפרוש את הגנות החוקה של המדינה החוקרת פרישה אוניברסלית, היינו על כל פעולת איסוף ראיות שמבצעת המדינה החוקרת ללא קשר לזהות הגורמים המושפעים מן הפעולה.

### ג) סיכום

בפרק ג הצגתי את מאפייני התפישה הטריטוריאלית באשר לחקירה הפלילית במרחב הסייבר. הראיתי כיצד תפישה זו משפיעה על סמכויות איסוף הראיות בחקירה פלילית בסייבר. בדומה, כפי שהראיתי זה עתה, התפישה הטריטוריאלית משליכה על הדיון החוקתי בחקירה הפלילית במרחב הסייבר. כפי שהראיתי, נקודת המוצא היא כי הגנות החוקה נפרשות טריטוריאלית על כל הנוכחים בה. מלבד זאת בתי המשפט הכירו בהרחבות התחולה אל מחוץ לטריטוריה בהקשרים שונים ועל בסיס מודלים שונים.

כפי שטענתי, יש להרחיב את פרישת המשפט החוקתי של המדינה החוקרת לפרישה אוניברסלית, במובן זה שכל אימת שהרשות החוקרת המדינתית תפעל לאיסוף ראיות במרחב הסייבר בחקירה פלילית, יהיה עליה להחיל את דיני החוקה של מדינתה על הסיטואציה החקירתית, ואין נפקא מינה אם מושפעי החקירה הם תושבי המדינה החוקרת אם לאו. מודל תחולה זה מגלם משפט חוקתי של חובות (על הרשות) נוסף על משפט חוקתי של זכויות (של הנחקרים). הוא יאפשר למדינה החוקרת לרכוש לגיטימציה לפעולתה האקסטרה-טריטוריאלית במרחב הסייבר. בנוסף, שקלתי גם את אפשרות ההחלה של המשפט החוקתי הזר על פעולה אקסטרה-טריטוריאלית (במשקפי התפישה הטריטוריאלית כמובן) של המדינה החוקרת במרחב הסייבר. לכאורה, אפשרות זו מרככת את הפגיעה בריבונותן של מדינות זרות הכרוכה בפעולתן ואת הפגיעה בזכויותיהם של יעד פעולת האיסוף והצדדים השלישיים המושפעים ממנה, אולם קשיים מעשיים הופכים את המהלך האמור לבלתי ניתן ליישום.

74 על מנת שתטען טענה שכזאת של החלת הגנות החוקה של מדינה זרה על המדינה החוקרת, חובה שמבחינת יעד פעולת האיסוף, או הצדדים השלישיים המושפעים מן הפעולה (קרי מבחינת הטוענים לזכות), מודל הפרישה החוקתית של מדינתם יהיה אקסטרה-טריטוריאלית, שאם לא כן הוא לא יתפרש כלל על פעולת האיסוף הנדונה.

#### ד. התפישה הפיזית בחקירה הפלילית והשפעתה על טיב הפגיעה בזכויות החוקתיות

עד כה הראיתי כיצד המרחב הקיברנטי משליך על שני ממדים של הדיון החוקתי בהקשר של חקירה פלילית במרחב הסייבר: ממד זיהוי ה"שחקנים" נשאי הזכויות הנפגעים מפעולות איסוף הראיות באינטרנט (מי נפגע?) וממד הזיהוי של היקף פרישת הזכויות החוקתיות מבחינה טריטוריאלית (איפה הפגיעה?). עתה אנתח את הממד השלישי שעניינו בזיהוי הזכויות החוקתיות הנפגעות מפעולות איסוף הראיות במרחב הסייבר ובעמידה על טיב הפגיעה בהן (איך או כמה נפגע?). ממד זה מושפע מהתפישה הפיזית החולשת על דיני איסוף הראיות הקיימים. תפישה זו מגלמת הנחות בדבר טיבן של פעולות איסוף הראיות ופוטנציאל הפגיעה המגולם בהן, כאשר הנחות אלה אינן בהכרח מתאימות לחקירה הפלילית במרחב הסייבר. אעיר תחילה כמה הערות מתודולוגיות: מטרתי היא להאיר היבטים מסוימים של זכויות חוקתיות הנוגעות לסמכויות איסוף הראיות במרחב הסייבר, אשר נדרשים לצורך עריכת איזון מול ההפעלה של סמכויות איסוף הראיות. התייחסותי תהא הן לסמכויות האיסוף הקיימות כיום והן לאלה הנחסרות כתוצאה מהתפישה הפיזית ואשר פורטו בפרק הקודם. ההתמקדות כעת תהא בהשפעתה של התפישה הפיזית על הדיון החוקתי באשר לדיני איסוף הראיות הדיגיטליות בחקירה פלילית במרחב הסייבר.<sup>75</sup> לכן אין לראות בדיון זה משום ניתוח מלא של הזכויות הדיגיטליות בחקירה פלילית במרחב הסייבר אלא ניתוח הקשרי של הזכויות המושפעות מהתפישה הפיזית, כפי שהיא מיושמת בזירת החקירה הקיברנטית. כמו כן בחלק זה של הדיון לא אערוך את האיזונים החוקתיים העקרוניים והקונקרטיים בין צורכי החקירה לבין הזכויות החוקתיות הנוגעות בדבר, אלא אציג את ההיבטים החוקתיים הכבויים כפועל יוצא מהתפישה הפיזית.<sup>76</sup> את הסינתזה בין צורכי החקירה לבין הדיון החוקתי אערוך בפרק הבא.

75 בדומה לזה, לסיג טען שעצם החלתה של החוקה האמריקנית על האינטרנט אינה תלויה בעובדה שמדובר במרחב שונה במהותו מן העולם הפיזי; אשר לאופן ההחלה, כאן כבר יש להתחשב בהחלט במאפייניה של הרשת. ראו L.J. 869, 872-877 (1996). לביטוי של עמדה זו בפסיקה הישראלית, ראו ע"א 1622/09 גוגל ישראל בע"מ נ' חב' ברוקרטוב, בפס' 3 לפסק דינו של המשנה לנשיא ריבלין (פורסם בנבו, 1.7.2010), שם נפסק כי "זכות הקיימת המרחב הפיזי – קיימת גם במרחב הווירטואלי". באותו מקרה הייתה הבעיה עם הפרוצדורה הקיימת בחקיקה למימוש הזכות (חשיפת גולש אנונימי בטענה לפגיעה בקניין רוחני). בענייננו, הבעיה היא במודעות למלוא היבטי הזכות בהקשר הקיברנטי אך לא בעצם קיומה של הזכות.

76 כפי שצינתי בפרק ד.ב.2, גם ללא העמידה על ההיבטים הייחודיים של הזכויות החוקתיות הנוגעות באיסוף ראיות דיגיטליות בחקירה פלילית במרחב הסייבר הדין הישראלי לוקה בחסר בכל הנוגע לבחינה החוקתית הנערכת בשלב ההסמכה של הרשות החוקרת לאיסוף ראיות דיגיטליות. להוציא את חוק נתוני תקשורת, הוראות החוק האחרות חסרות פירוט בנוגע להבניית שיקול הדעת השיפוטי בתהליך ההסמכה של הרשות החוקרת לאיסוף ראיות דיגיטליות. גם הפסיקה הישראלית, בהחרגה מסוימת של חוק האזנת סתר, מיעטה להציג ניתוח חוקתי קפדני של בקשות ההסמכה של הרשות החוקרת. מכאן שגם במנותק מהדיון שאערוך להלן יש לשקול רפורמה באופן עריכת הדיון החוקתי בשלב ההסמכה לביצוע פעולות האיסוף בחקירה הפלילית במרחב הסייבר.

ייתכן שפסיקתו המנחה של בית המשפט העליון ברע"פ 10141/09 בן חיים נ' מדינת ישראל (פורסם בנבו, 6.3.2012) תביא לשינוי מגמה באשר להתייחסותו של בית המשפט למעמדו המכריע של שלב ההסמכה של הרשות החוקרת לבצע פעולות איסוף. באותו מקרה נדונה שאלת הסמכות של המשטרה

## 1. הזכות לפרטיות

רבות נכתב על הזכות לפרטיות, על פיתוחה, על עמימותה ועל ערכיה המוגנים.<sup>77</sup> בקרב החוקרים היו מי שניסו להציע קטגוריות או מצבים של פרטיות<sup>78</sup> ומי שביקשו להציע ערך או הגדרה מופשטת אחת שתחבוק את כל הביטויים המעשיים של פרטיות.<sup>79</sup> בהקשר הדיגיטלי

לערוך חיפושים בהסכמה על הגוף ובמקום, בלא צו שיפוטי, ואף בלא עילה המוכרת בפסד"פ לעריכת חיפוש, על סמך הסכמה של הנחפש בלבד. הניתוח בפסק הדין עשיר מבחינה חוקתית, ובחינת החיפושים הנדונים נערכת לאורה של דוקטרינת ההסכמה מדעת כמאפשרת ויתור על הזכות לפרטיות. אמנם פסק הדין נכתב בהתייחס לחיפוש על הגוף וחיפוש במקום, אולם היות שדיני איסוף הראיות הדיגיטליות במשפט הישראלי נגזרים מדיני איסוף הראיות הפיזיות – ניתן להניח שקביעותיו של פסק הדין יחולו באותה מידה גם על הראיות הדיגיטליות. בשלב זה עדיין מוקדם לבחון את השלכותיו המעשיות של פסק הדין בעניין בן חיים מעבר לסוגיה הקונקרטי שנדונה בו, שהיא סוגיית החיפוש בהסכמה ללא צו שיפוטי מסמיך.

77 לדיון ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 57–88; ראם שגב "פרטיות – משמעותה וחיבותה" פרטיות בעידן של שינוי 25, 25–27 (תהילה שוורץ אלטשולר עורכת, 2012); כן ראו Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002). סולוב טען כי בשל עמימותה של הגדרת הפרטיות בתי המשפט נכשלים ביישום הזכות במקרים שונים. ראו Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 558–560 (2006).

78 ראו למשל את הסיווג הנזיקי של ויליאם פרוסר (Prosser), שלפיו "פרטיות" כוללת את אלה: הגנה מפני התערבות חיצונית במרחב פרטי של אדם; פרסום פרטים מביכים על אודות אדם לציבור; הצגת אדם באור כוזב; שימוש בשמו או בדיוקנו של אדם למטרת רווח. ראו William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960). כן ראו את הסיווג שמביא אלן וסטין (Westin) ליחידות (Solitude), לאינטימיות, לאנונימיות ולהגנה מפני התערבות חיצונית: ALAN F. WESTIN, *PRIVACY AND FREEDOM* (1967) 31–32. ראו עוד בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 67–82. סולוב הציע לאפיין את הזכות לפרטיות על בסיס מכלול של מצבי האיום על הזכות לפרטיות. ראו Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, בעמ' 558–560. סולוב ציין ארבע קטגוריות: איסוף מידע; עיבוד מידע; הפצת מידע; חדירה למידע. כן הציע לחלק את ארבע הקטגוריות ל-16 תת-קטגוריות. קטגוריית איסוף המידע נחלקת ל-1) Surveillance (מעקב חזותי או קולי) ול-2) Interrogation (תשאול וחקירה). קטגוריית עיבוד המידע נחלקת לאלה: 1) Aggregation (איחוד פיסות מידע ממקורות שונים על אודות אדם), 2) Identification (קישור מידע לאדם מסויים), 3) Insecurity (התשלולות בשמירה על מידע באופן שמאפשר זליגה שלו או חדירה לא מורשית אליו), 4) Secondary use (שימוש במידע שלא למטרה שלשמה נמסר) ו-5) Exclusion (אי-ידיעת האדם על המידע האישי שלו המצוי במאגרי המידע השונים). קטגוריית הפצת המידע נחלקת לאלה: 1) Breach of confidentiality (הפרת חובת סודיות), 2) Disclosure (גילוי מידע על אדם באופן שיביא לשיפוט מוקדם שלו), 3) Exposure (חשיפת אדם באופן מביך – עירום, אבל או כדומה), 4) Increased accessibility (הנגשת מידע), 5) Blackmail (סחיטה תוך איום בגילוי מידע על אדם), 6) Appropriation (נטילת זהות) ו-7) Distortion (הפצת מידע כוזב על אודות אדם). קטגוריית חדירה למידע נחלקת ל-1) Intrusion (חדירה למרחב הפרטי של אדם) ול-2) Decisional interference (התערבות בהחלטותיו של אדם בענייניו האישיים). הטקסונומיה של סולוב מעודכנת לעידן האינטרנט. תכליתה רחבה מתכליתו של הדיון שאני מבקש לערוך. סולוב ביקש לתאר את כל האיומים על הזכות לפרטיות ולא רק את אלה המתעוררים בהקשר של איסוף ראיות דיגיטליות בחקירה פלילית באינטרנט. משכך הוא, חלק מהמצבים שהוא מתאר, לדוגמה Blackmail ו-Insecurity, אינם רלוונטיים לחקירה הפלילית. חלק אחר מהמצבים שתיאר, לדוגמה Interrogation, Disclosure וכדומה, אינם רלוונטיים במיוחד לאינטרנט או לראיות דיגיטליות.

79 ראו את הטענה של בירנהק, המבקש להגן על עמדתו של אלן וסטין (Westin) ולהחילה גם בסביבה הדיגיטלית, כי יש לראות בפרטיות כשליטה של אדם על המידע על אודותיו. ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 89–108; בירנהק "שליטה והסכמה", לעיל ה"ש 8, בעמ' 41–49, וכן: WESTIN, לעיל ה"ש 78, בעמ' 7. ראו עוד Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968). כן ראו את

והאינטרנטי קיים קושי מוגבר להגדיר ולהכיל את מושג הפרטיות. בהקשרנו הנדון כאן אתבסס, כנקודת מוצא, על הקביעה היסודית שהזכות לפרטיות היא זכות יסוד חוקתית מרכזית הניצבת כבלם אל מול פעולת הרשות החוקרת,<sup>80</sup> הן מבחינה היסטורית<sup>81</sup> והן מבחינה נורמטיבית, ולרבות בעידן הסייבר.<sup>82</sup> טענתי היא שאף שמרכזיותה של הזכות לפרטיות בדיני החקירה אינה מוטלת בספק, הרי שבשל התפישה הפיזית החולשת על דיני איסוף הראיות, מובנים שונים של הזכות לפרטיות מוחמצים וחסרים הן בפרקטיקה השיפוטית והן בשיח האקדמי על אודות האכיפה הפלילית במרחב הסייבר. בשל החמצה זו עלול להיווצר עיוות באשר לאיזון הראוי בין צורכי החקירה לבין ההגנה החוקתית על הפרטיות.

אשוב ואזכיר את הנחות התפישה הפיזית שעליהן עמדתי בפרק הקודם. התפישה הפיזית מניחה את ההנחות האלה בנוגע לראיות הדיגיטליות במרחב הסייבר: האחת, הראיה מיוצגת הצגה פיזית חפצית (באטומים); השנייה, תוכנה של הראיה ומשמעותה אינם נפרדים מן החפץ הפיזי שבו הם מיוצגים; השלישית, הראיה אינה ניתנת להעתקה, ומכאן שהיא בת-תפיסה בלבד; הרביעית, השימוש בראיה תלוי בהחזקתו בפועל באופן פיזי בתוספת שליטה אפקטיבית בו. לעומת אלה הראיות הדיגיטליות מתאפיינות באלה: האחד, המידע מיוצג בביטים; השני, המידע ניתן להעתקה מלאה; השלישי, המידע מנותק פיזית מהמשתמש בו, הוא מבוזר ומוחזק בידי מתווכים; הרביעי, המידע ניתן לאחזור ולכרייה באמצעים ממוחשבים; החמישי, המידע מצטבר

הצעתה של הלן ניסנבאום (Nissenbaum) לתפוש את הפרטיות כזכות הקשרית הנפגעת כאשר מופרות "נורמות מידע" (Informational norms) בדבר זרימת מידע: HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE (2010). ראו עוד את הצעתה של רות גביון לתפוש את הזכות לפרטיות כמשקפי רעיון הגישה, או ליתר דיוק – לתפוש את הרעיון במונחי הגבלת הגישה של אחרים אל האדם: Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).

80 הזכות לפרטיות ניצבת כבלם הן במישרין מול פעולות האיסוף של הרשות החוקרת עצמה והן באופן המורכב משתי חוליות: רשות חוקרת מול ספק שירות וספק שירות מול משתמש המחשב והאינטרנט. בסיטואציה האחרונה אמנם סמכות האיסוף של הרשות החוקרת מופעלת במישרין כלפי ספק השירות, אולם הנהנה מהזכות לפרטיות הוא משתמש המחשב מושא החקירה.

81 גלגוליה הקדמונים של הזכות לפרטיות, עוד לפני שנוסחה כזכות עצמאית בידי סמואל וורן (Warren) ולואיס ברנדייס (Brandeis) במאמרם המכונן: Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), כללו זכות להגנת האזרחים מפני פעולות חיפוש ותפיסה (Search & Seizure) של הרשויות. ראו במשפט האנגלי: Entick v. Carrington, [1765] EWHC KB J98; ובמשפט האמריקני ראו את התיקון הרביעי לחוקה (1789), הקובע חירות מפני חיפושים ותפיסות בלתי סבירים (U.S. Const. Amend. IV). היבטים אלה של הזכות לפרטיות אינם שנויים במחלוקת, והם חלק מהיבטי הליבה של הזכות גם כיום.

82 ראו למשל Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 799 (2004); Peter P. Swire, *Katz is Dead, Long Live Katz*, 102 MICH. L. REV. 904 (2004); Patricia L. Bellia, *Surveillance Law Through Cyberlaw's United States v. Jones*, 72 GEO. WASH. L. REV. 1375 (2004); Riley v. California, 134 S. Ct. 2473 pp. 17–18, (2012), (בנוגע למעקב באמצעות GPS); 25 (בניגוד לחיפוש בטלפון סלולרי "חכם"), ובפסיקה הישראלית ראו בג"ץ 3809/08 האגודה לזכויות האזרח בישראל נ' משטרת ישראל (פורסם בנבו, 28.5.2012), שבו נדונו סמכויות המשטרה לאיסוף נתוני תקשורת.

וניתן לאגירה; השישי, המידע נדיף; השביעי, המידע פגיע; השמיני, המידע ניתן בנקל להצפנה, להסוואה או לטשטוש.

תפישה פיזית הנשענת על יסודות אלה עלולה להוביל להתחשבות מצומצמת ביותר בזכות הפרטיות בהקשר של דיני איסוף ראיות בחקירה פלילית במרחב הסייבר. אראה כיצד התפישה הפיזית מתעלמת מהתפתחויות טכנולוגיות ביכולות האיסוף, האגירה, השחזור והכרייה של המידע, המשפיעות על עיצובה של הזכות לפרטיות בהקשרנו. כן אראה כיצד מבחינה משפטית מערך הדינים הקיים, המסדיר את סמכויות האיסוף של הרשות החוקרת, מחמיץ את מלוא מובניה של הפגיעה בפרטיות בהקשר של חקירה פלילית במרחב המקוון. בנוסף, כפי שצינתי לעיל, השתחררות מהתפישה הפיזית פותחת פתח להכרה במכלול סמכויות איסוף נוספות.<sup>83</sup> בחלק זה של הדיון אראה גם את הפגיעות המגולמות בסמכויות נוספות אלה.

### א) השלכת ההתפתחויות הטכנולוגיות על הזכות לפרטיות

הטכנולוגיה משפיעה על הזכות לפרטיות בשני כיוונים: העצמת הפגיעה בפרטיות והגברת הפרטיות. אתייחס תחילה לטכנולוגיות הפוגעות בפרטיות. הטכנולוגיה המיושמת בזירה הקיברנטית מאפשרת לשכלל את היכולות בתחומים אלה: (1) איסוף המידע, (2) אגירתו, (3) שחזורו ו־(4) כרייתו. אשר ליכולות איסוף המידע, אלה עשירות, מגוונות ומתפתחות כל העת. כלי האיסוף העצמתיים יכולים, מצד אחד, להקיף כמויות מידע גדולות, ומצד שני הם יכולים לאסוף נתוני מידע מסוגים שונים שנוצרים במסגרת פעילותו המקוונת של משתמש המחשב והאינטרנט, ומצד שלישי הם יכולים לכלול שאילתות מורכבות לצורך איסוף ממוקד של המידע הדרוש וכדי למנוע היצף מידע. בעבר נודעו כלי איסוף ברמה תשתיתית כ־Carnivore<sup>84</sup> ו־Echelon<sup>85</sup>, קרי כלי איסוף הפועלים על צומתי זרימת מידע באינטרנט כגון ספקי גישה לאינטרנט, וב־2013 הודלף דבר קיומו של פרויקט PRISM, אשר מאפשר איסוף קבוע של מידע מספקיות השירות הגדולות ביותר בשוק האינטרנט, כ־Facebook, Apple, Google, Microsoft, Yahoo! ורבים אחרים.<sup>86</sup> כן ידועים כלי איסוף ברמה טקטית כלפי משתמש קצה מסוים, כ־Key

83 ראו פרק ד.ג.1..

84 מדובר בתוכנת ניטור שפיתח ה־FBI והמסוגלת לנטר תכנים וכן נתוני תקשורת תוך שאילתות ממוקדות למניעת היצף מידע. משנת 2005 לערך עבר ה־FBI להשתמש בתוכנות שנמכרו לו על־ידי חברות פרטיות, אשר מספקות יכולות מאותו סוג. ראו אסף הרדוף הפשע המקוון 238 (2010) והמקורות המצוטטים שם; עמיר פוקס "טרור ופרטיות – הצעה לחשיבה מחודשת על הכלים להתמודדות עם פעילות טרור באינטרנט" פרטיות בעידן של שינוי 231, 245 (תהילה שוורץ אלטשולר עורכת, 2012) והמקורות המצוטטים שם.

85 מדובר בכלי ניטור עצמתי ביותר, הכולל תקשורת נתונים אינטרנטית מכל סוג, בתוספת תקשורת בגלי רדיו, טלפון קווי ועוד. כלי זה משרת חמש מדינות: ארצות הברית, קנדה, בריטניה, אוסטרליה וניו זילנד. ה־Echelon מסוגל לנטר כשלושה מיליארד תשדורות ביום. ראו הרדוף, שם, בעמ' 239 והמקורות המצוטטים שם; פוקס, שם, בעמ' 246 והמקורות המצוטטים שם.

86 את תכנית ה־PRISM הדליף עובד ה־NSA לשעבר, אדוארד סנאורן, לעיתונים ה־"גארדיאן" וה־"ווישינגטון פוסט". ראו Barton Gellman & Laura Poitras, U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program, THE WASHINGTON POST (6.6.2013) [http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story.html](http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html); Glenn Greenwald

logger Systems (KLS) ללכידת הקלדות מקלדת, תוכנות לניטור תעבורת אינטרנט, כ"רחרחנים" שונים (Sniffers). כלי האיסוף ברמה הטקטית מצריכים "הקמה" של יכולת האיסוף בכל פעם שמבקשים לאסוף מידע על אודות יעד מסוים,<sup>87</sup> ואילו בכלי האיסוף ברמה התשתיתית יכולת האיסוף קיימת ופועלת, וכאשר מבקשים לאסוף מידע על אודות יעד מסוים, יש להכליל אותו ביעדי הניטור. כלי ניטור אלה מסוגלים לאסוף נתוני תוכן ושלל נתוני metadata על אודות התוכן, אשר השימושים בהם רבים ומגוונים. נוסף על ההתעצמות של כלי האיסוף השונים, גם חוויית השימוש באינטרנט מתפתחת בכיוונים כאלה שהיא מאפשרת הסגרה של יותר ויותר נתוני מידע אישי. כך, למשל פיתוח הטכנולוגיה של VoIP אפשרה לקיים שיחות בעל פה באמצעות האינטרנט, ושיחות אלה הן בנות האזנה. האינטרנט דור 2.0 מסמל מעבר מצריכת תכנים להעלאה דינמית של תכנים בידי משתמשי האינטרנט, ותכנים אלה ניתנים לניטור ולשייך למשתמש אינטרנט מסוים. ההנגשה והניידות של האינטרנט, עם המעבר למכשירי סלולר דור 3.0 ומעלה ועם הנגשת האינטרנט במקומות ציבוריים באמצעות טכנולוגיית Wi-Fi, מאפשרת לאכן פיזית את משתמש האינטרנט במועד מסוים.<sup>88</sup>

בצד שכלול יכולות איסוף המידע באופן העלול להעצים את הפגיעה בפרטיות, הוזלו מאוד עלויות אגירת המידע. שאלת נפח אחסון המידע הפכה כמעט לחלוטין לזניחה מבחינה כלכלית.<sup>89</sup> תאגידים רבים משקיעים הון בניהול מידע בכמויות עצומות (Big data)<sup>90</sup> משום שאגירת המידע העצום יצרה קשיים במיציא יעיל של המידע. גידול פוטנציאל אגירת המידע לצד שכלול יכולות איסוף המידע מייצרים פגיעה מוגברת בזכות לפרטיות. גם יכולות שחזור המידע במקרה שנמחק או נעלם השתפרו, ושחזור קבצים מחוקים הפך גם הוא לאפשרי בעלויות סבירות.<sup>91</sup>

- 
- & Ewen MacAskill, *NSA Prism Program Taps into User Data of Apple, Google and Others*, THE GUARDIAN (6.6.2013) <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> 87
- דוגמאות לשיטות של הקמת יכולת האיסוף הן אלה: חדירה פיזית למחשב והשתלטת רכיב הניטור, שליחת דוא"ל במסווה תמים ובו צרופה שנועדה "להדביק" את מחשבו של היעד ברכיב האיסוף, או כל אמצעי אחר של "הנדוס אנושי" (social engineering).
- 88 לדיון ציבורי בנושא, שהתעורר בכלי התקשורת באפריל 2011, ראו למשל עומר טנא "פרל הרבור בכוס מים" דה מרקר 39 (28.4.2011); יוסי גורביץ' "אפל לא לבד: גם הטלפונים של מיקרוסופט אוספים מידע על מיקום הלקוחות" כלכליסט (27.4.2011), [http://www.calcalist.co.il/internet/articles/0,7340, \(27.4.2011\), Declan McCullagh, How police have obtained iphone, ipad tracking logs, CNET \(21.4.2011\) http://news.cnet.com/8301-31921\\_3-20056344-281.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://www.calcalist.co.il/internet/articles/0,7340, (27.4.2011), Declan McCullagh, How police have obtained iphone, ipad tracking logs, CNET (21.4.2011) http://news.cnet.com/8301-31921_3-20056344-281.html?part=rss&subj=news&tag=2547-1_3-0-20)
- 89 לא למותר להזכיר שוב את "חוק מור", לעיל בפרק המבוא ה"ש 27.
- 90 במושג ה-"Big data" הכוונה לאתגר מתפתח בתחום טכנולוגיות המידע (Information technology) בכל הנוגע לאיסוף, חיפוש, כרייה, שיתוף, ניתוח והצגה של מידע שברשות תאגידים שונים. ראו למשל Martin Hilbert & Priscila Lopez, *The World's Technological Capacity to Store, Communicate, and Compute Information*, SCIENCE 332, 60 (2011). ליישומים שונים העשויים לנצל את יתרונות ה-Big data, ראו למשל Steve Lohr, *Sizing Up Big Data, Broadening Beyond the Internet*, THE NEW YORK TIMES (20.6.2013), at F1
- 91 ראו לעיל בפרק ד ה"ש 90 את פירוט התוכנות הפורנויות המאפשרות שחזור קבצים מחוקים. כן יש חברות מסחריות המציעות שירותי שחזור של קבצים מחוקים. ראו למשל [www.mitsy.com](http://www.mitsy.com), [www.tictac.co.il](http://www.tictac.co.il)



אלמנט טכנולוגי חשוב נוסף המעצים את הפגיעה בפרטיות הוא שכלול ופיתוח היכולות של כריית המידע.<sup>92</sup> כריית המידע חשובה במיוחד לגורמי אכיפת החוק בשל חוסר היכולת לבחון בעין אנושית את כל כמויות המידע העצומות ובשל העובדה שהראיות הדיגיטליות במרחב הסייבר מתאפיינות בכיזוריות, והרכבתן יחדיו עשויה ליצור שלם הגדול מסך כל חלקיו.<sup>93</sup> השלם כולל מידע על אודות המידע, ובכך מעניק ממד נוסף של עומק לתמונת המידע המתקבלת.<sup>94</sup>

ליכולות כריית המידע השלמה ניכרת על הזכות לפרטיות בפרט בכל הנוגע לסיטואציה של חקירה פלילית: חקירה פלילית טיפוסית במרחב הסייבר תכלול מספר רב של פעולות איסוף;

92 תהליך כריית המידע (data mining) משמעו הצלבת נתונים ממקורות מידע שונים לצורך בנייתה של תמונת מידע עשירה, מדויקת ומועילה יותר לכורה המידע. כריית מידע משמשת גופי מודיעין, גופי חקירה וגם גופים מסחריים. להרחבה ראו עומר טנא "הסתכל בקנקן וראה מה יש בו: נתוני תקשורת ומידע אישי במאה העשרים ואחת" רשת משפטית: משפט וטכנולוגיות מידע 287, 314–318 (ניבה אלקין-קורן ומיכאל בירנהק עורכים, 2009). כן ראו Lee Tien, *Privacy, Technology and Data Mining*, 30 OHIO N. U. L. REV. 389 (2004). טל ז'רסקי ניתח את תופעת כריית המידע וניצולה לרעה הן בידי גופים מסחריים והן בידי רשויות השלטון. ראו: 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); Tal Z. Zarsky, *Online Privacy, Tailoring, and Persuasion*, in PRIVACY AND TECHNOLOGIES OF IDENTITY – A CROSS-DISCIPLINARY CONVERSATION (Katherine Strandburg & Daniela Stan Raicu eds.) 209, 213–214 (2006); Tal Z. Zarsky, *The Data Mining Balancing Act*, in EUROPEAN DATA PROTECTION: IN GOOD HEALTH? (Serge Gutwirth et al. eds., 2012) 79, 79–88. לתופעה זו השפעות ברמת הפרט (יצירת אשליה של אוטונומיה כשבפועל נפגע מרחב שיקול הדעת של הפרט) וברמת הכלל (תיווצר אפשרות של תאגידים מסחריים לשלוט על השיח הציבורי, על המוצרים בשוק, ובכך ייפגע השוק החופשי). כריית המידע באמצעות המנגנון השלטוני מחזקת את מטאפורת "האח הגדול" האורוליאני, ואילו כריית המידע בידי תאגידים מחזקים את החשש מפני "אח גדול תאגידי".

ביוני 2013 התפרסם בכלי התקשורת העולמיים דבר קיומה של תכנית ה-Boundless informant. מדובר בפרויקט ניטור מידע של ה-NSA, שדבר קיומו הודלף לעיתונות אף הוא בידי אדוארד סנאורן, ב-8.6.2013. פרויקט זה כולל עיבוד ומיצוי מידע מיותר מ-500 מקורות של מידע תוכני (האזנת סתר) ומטה-דאטה (נתוני תקשורת) בעולם. על פי הפרסומים, יותר מ-3,000,000,000 פריטי מידע נוספים ל"אוקיינוס המידע" אשר מתוכו מפיק ה-Boundless informant את המידע הערכי שבביל עובדי ה-NSA. ראו Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, THE GUARDIAN (11.6.2013) <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>. אמנם מדובר בפרויקט לצורכי ביטחון ולא לצורכי חקירה פלילית, אולם הוא מלמד על הכוח, כמו גם על פוטנציאל הפגיעה, המגולם ביכולות גבוהות של כריית המידע.

93 ראו Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1398 (2000). בארצות הברית נדון פיתוח של מערכת ממוחשבת שתאפשר לשלב את כל מאגרי המידע המוחזקים בין הסוכנויות הממשלתיות האמריקניות הרבות עם מאגרי המידע של חברות פרטיות באופן שיאפשר גילוי תבניות של התנהגות חשודה. מערכת זו כונתה: The Total Information Awareness System (TIA), והקונגרס האמריקני הפסיק את פיתוחה ביולי 2003. ראו <http://epic.org/privacy/profiling/tia/>; U.S. DEPARTMENT OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM: REPORT OF THE TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE 1–5 (2004).

94 בירנהק דימה את הדברים ל"שובל של מידע". ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 169–190.

הפְּרִיִּיטְצִיָּה של הליך ההסמכה השיפוטית לפעולות החקירה השונות עלולה לפגוע בהבנה כוללת של עומק הפגיעה בפרטיות, הכרוך במידע אישי הנאסף ומורכב מתוך פיסות מידע נפרדות המוכמנות בתוך ארכיוני מידע עצומים. יתרה מזאת, הליך ההסמכה השיפוטית הוא רק מסלול אחד שדרכו עוברת הרשות החוקרת בבואה לאסוף מידע בחקירה פלילית. בצד מסלול זה ניתן למנות מקורות נוספים, ובהם מידע שמחזיקה הרשות החוקרת עצמה, לדוגמה מאגר המרשם הפלילי מכוח חוק המרשם הפלילי, מאגר בעלויות על מספרי טלפון מכוח חוק נתוני תקשורת, מאגר כתובות של משרד הפנים המועבר לרשות המשטרה מכוח פרק ד לחוק הגנת הפרטיות המסדיר העברת מידע בין גופים ציבוריים ועוד; מידע גלוי הניתן לאיסוף מהאינטרנט, כגון תכנים של תגובות, מידע פתוח מתוך רשתות חברתיות וכדומה; מידע המושג מכוח הסמכה מנהלית קונקרטיה, לדוגמה הסמכות לקבל נתוני תקשורת במקרים דחופים. מכאן נובע שיש מקום להעשיר את הבקרה (הפנימית, של הרשות החוקרת, והשיפוטית) על פעולת איסוף קונקרטיה בכך שהיא תיבחן לנוכח האפשרות להרכיב באמצעותה פרופיל מידע שלם, עשיר ופוגעני.

חיבורן של היכולות הטכנולוגיות החדשניות לאיסוף המידע, לאגירתו, לכרייתו ולשחזורו מעורר דיון בדבר זכותו של אדם להימחק ממאגרי המידע השונים באינטרנט (The right to be forgotten).<sup>95</sup> למען הדיוק, אני סבור כי אין לראות ב"הזכות להימחק" משום זכות עצמאית אלא אמצעי להגנת הזכות לפרטיות בהקשרים מסוימים המתעוררים בעידן הסייבר ביתר שאת, בבחינת מתן ביטוי לפרטיות במידע כשליטה של אדם על המידע המתייחס אליו. כן ניתן לראות בזכות להימחק משום ביטוי לזכות הקניין במידע, במובן של ריבונות במידע והיכולת לנהוג כלפיו מנהג בעלים, לרבות מחיקתו של המידע. מנגד ניתן לטעון כי זכות זו עלולה לפגוע בחופש העיתונות, בעיקר כשמדובר בזכות להימחק ממאגרים הפתוחים לעיון הציבור (זכותו של עיתונאי לאסוף מידע בעל עניין לציבור, והאפשרות להורות על מחיקת המידע עלולה להצר

95 בינואר 2012 פורסמה הצעה לרגולציה של האיחוד האירופי בנושא הגנת מידע אישי, וכלולה בה הזכות להימחק. ראו A Proposal 2012/0011 (COD) for Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art. 17 [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf). זכות זו, על פי ההצעה, תקים חובה של השולט במידע לפעול למחיקת המידע, לרבות כלפי צדדים שלישיים המעבדים את המידע הזה. עוד על ההצעה וניתוח המצב המשפטי הנוהג שלפיו הזכות אינה קיימת בדין האמריקני ראו Steven C. Bennett, *The "Right to be Forgotten": Reconciling EU and US Perspectives*, 30 *Berkeley J. Int'l L.* 161 (2012). לפיתוח מובנים עיוניים שונים של הזכות ראו Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to be Forgotten" in Big Data Practice*, 8 *SCRIPTED* 229 (2011) [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1986719](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719). בישראל ראו את הוראת סעיף 14 לחוק הגנת הפרטיות, שלפיה אדם רשאי לדרוש תיקון או מחיקה של מידע על אודותיו המצוי במאגר מידע אם ורק אם המידע "אינו נכון, שלם, ברור או מעודכן". נובע מכך, לכאורה, כי אם המידע המצוי במאגר נכון, הרי שמרגע שיצא מרשותו של האדם ועבר לרשותו של בעל מאגר המידע, אין לו עוד זכות לדרוש את מחיקתו, והדבר תלוי בהסכמת בעל המאגר. ראו בעניין זה את פסק הדין שדחה את תביעתו של לקוח נגד חברות סלולר בדרישה כי הנתונים הנוגעים למכשירי הטלפון הסלולרי שלו שהיו מנויים בחברות אלה – יימחקו: ת"א (מחוזי ת"א) 1994/06 לירן נ' פלאפון תקשורת בע"מ (פורסם בנבו, 30.11.2010). באותו מקרה סירבו הנתבעות למלא את בקשתו של התובע.

זכות זו). מימוש הזכות אף עלול להוביל להתערבות לא ראויה באוטונומיה של ספקית השירות לנהל את המידע אצלה כראות עיניה. מימוש הזכות להימחק או להישכח מְשַׁרְת תכלית דומה לתכלית שבבסיס עקרון "תקנת השבים", המוכרת בחוק המרשם הפלילי ותקנת השבים, התשמ"א-1981. הזיכרון הדיגיטלי משול לבור ללא תחתית בשל הוזלת עלויות אגירת המידע, התפשטות המרחב המקוון, השתכללות יכולות אחזור המידע וכן שינוי תרבותי מסוים בתפישת השיתוף במידע באינטרנט הכוללת חשיפה עצמית מוגברת. מכאן התעורר הצורך הפרקטי בפיתוח השיח על זכותו של אדם לשלוט במידע על אודותיו, גם אם זה אגור ומנוהל בידי ספקית שירות. הכרה בזכות להימחק מגלמת הכרעה כי מידע שמוחק ומנוהל בידי אחר אינו שולל מהאדם את הזכות לדרוש את מחיקתו, וכי זכות זו תגבר על זכותו של אותו אחר לנהל את המידע שברשותו כרצונו.

אסכם עד כאן. התפישה הפיזית, כפי שהיא מגולמת בדיני איסוף הראיות הדיגיטליות בחקירה פלילית, מביאה להתעלמות המשפט מיכולות טכנולוגיות הולכות ומשתכללות לאיסוף המידע ממקורות שונים ולאגירה לא מוגבלת של המידע, מהיכולת לשחזר מידע שנמחק ומהיכולת לכרות את המידע כרייה מיטבית להרכבת פרופיל מידע עשיר ומדויק. יכולות אלה מתמודדות עם תכונותיו של המידע הדיגיטלי במרחב המקוון כנדיף מצד אחד אך מצטבר וניתן לאגירה מצד שני, כמבוזר על פני ספקיות שירות שונות וכניתן לאחזור ולכרייה באמצעים ממוחשבים. יכולות אלה מאפשרות לייצר פגיעות קשות יותר בפרטיות, הן במובן היקפי המידע על אודות משתמש המחשב והאינטרנט והן במובן איכותו של מיצוי המידע על אודותיו.

עד כאן בדבר טכנולוגיות המגבירות את הפגיעה בפרטיות. עתה אדון בטכנולוגיות המגבירות פרטיות (Privacy Enhancing Technologies – PETs) ובהשפעתן על הזכות לפרטיות. ה-PETs הן טכנולוגיות המאפשרות סודיות בתכנים וסודיות באשר לזהותו האמתית של משתמש המחשב והאינטרנט.<sup>96</sup> אתייחס עתה לאמצעים להשגת סודיות בתכנים, ובהמשך, כשאדון בזכות לאנונימיות/פסידונימיות, אתייחס לאמצעים להשגת סודיות באשר לזהותו האמתית של משתמש המחשב והאינטרנט. שני אמצעים מרכזיים משמשים להשגת סודיות בתכנים – הגנת ססמה והצפנה. התפישה הפיזית באשר לראיות הדיגיטליות במרחב הסייבר מתעלמת מתכונה מובנה של ראיות אלה, כניתנות להצפנה ולהסוואה בנקל.

שימוש בהצפנות ובהגנת ססמאות יכול להיעשות בידי משתמשי המחשב והאינטרנט עצמם, בידי מקום העבודה שלהם או בידי ספקיות השירות שלהם כחלק מחבילת התוכן שהן מעניקות (למשל שירותי דוא"ל המתחייבים לשימוש בפרוטוקול מוצפן להעברת המידע ממשתמש האינטרנט ואיליו). על פי גישה אמריקנית המבכרת את מבחן הציפייה הסבירה לפרטיות כמבחן להענקת הגנה חוקתית של התיקון הרביעי לחוקה,<sup>97</sup> שימוש יזום, או לפחות שימוש מודע,

96 את הטכנולוגיות להשגת סודיות בתכנים הצגתי בפרק ד.ג.ג.1. את הטכנולוגיות להשגת אנונימיות או שמירה על פסידונימיות הצגתי בפרק ב.ג.1.

97 לפיתוח דוקטרינת ה-"Reasonable expectation of privacy", ראו Katz v. United States, 389 U.S. 347, 361 (1967) (שם דובר בהאזנת סתר לשיחת טלפון). כן ראו California v. Greenwood, 486 U.S. 35, 39-40 (1988) (שם דובר בשאלה אם איסוף חומרים אישיים שנזרקו לזבל הוא פגיעה בציפייה סבירה של בעליה של האשפה לפרטיות). כן ראו California v. Ciraolo, 476 U.S. 207, 215 (1986) (שם דובר בצילום מן האוויר של שטח אדמה שגודר בגדר בגובה של כארבעה מטרים); Kyllo v. United States, 533 U.S. 27 (2001) (שם דובר בשימוש גלאי תרמי בידי רשויות החקירה על מנת לאתר אם נפלס חום

בהצפנות ובסמאות יצדיק מתן הגנה מוגברת של פרטיות למשתמש המחשב והאינטרנט.<sup>98</sup> מנגד, קלות השימוש ב־PETs, העלויות הנמוכות של השימוש והתפוצה הרחבה שלהם עשויות להפוך את השימוש בטכנולוגיות אלה לכמעט־סטנדרט שגרתי, ולפיכך עלולה להשתנות תפישתן כמקומות ציפיה סבירה לפרטיות. לעומת זאת המודל האירופי והישראלי להגנת הפרטיות תופשים את הזכות לפרטיות תפישה רחבה מגדרי מבחן הציפיה הסבירה לפרטיות,<sup>99</sup> ומכאן שהשימוש באמצעי ההצפנה או הסממה לא הוא שיגדיר את המידע כפרטי (שכן המידע יהיה מוגן ממילא), אלא לכל היותר יהיה ביטוי לזכות לפרטיות. במילים אחרות, ההצפנה / הסממה לא תיצור פרטיות אלא תבטא את יישומה של הפרטיות במובן של שליטה או במובן של מניעת גישה אל סוד שיחו של אדם.

חריג מביתו של אדם שיתאים לחשדות בדבר גידול מריחואנה בחממות בתוך הבית). לביקורת על מבחן הציפיה הסבירה לפרטיות כמבחן פרטיות נוזל, המחמיץ את מהותה השלמה של הזכות לפרטיות והופך אותה לזכות תלויה־הקשר, של נסיבות, זמן ומקום, ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 72, 86-447.

98 לסיג טען שפרשנות תכליתית של התיקון הרביעי לחוקה, ברוח עידן האינטרנט, מחייבת החלה מוגברת שלו על מקרה שבו מידע הוצפן או הוגן בסממה, ולכן תידרש הסמכה שיפוטית מיוחדת על מנת לאפשר לרשות החוקרת לחדור למידע שכוה. ראו LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 114-118 (1999). זו גם עמדתה של סוזן ברנר: Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 U. FL. J. TECH. L. & POL'Y 123, 182-190 (2002). כן ראו את עמדתו של אנדרו שפירו (Shapiro), שהשווה את פיצוח ההצפנות וסממאות ההגנה לפתיחתה של כספת במהלך חיפוש בחצרים: ANDREW L. SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 73 (1999). מנגד, אורין קר העלה טיעון פוזיטיבי בנוגע למשפט האמריקני, שלפיו הצפנת מידע מצד חשוד אינה יכולה להעניק לו הגנת פרטיות מוגברת לעומת מידע ממוחשב אחר שאינו מוצפן. זאת, כיוון שלדעתו מבחן הציפיה הסבירה לפרטיות, שפותח מתוך הדיון בתיקון הרביעי לחוקה האמריקנית, חל על שלב תפיסת המידע בלבד ולא על שלב העיון בו. על כן, מסביר קר, מלבד זאת לא תידרש הסמכה נוספת של הרשות החוקרת על מנת לפצח את ההצפנה או את סממת ההגנה של קבצים מסוימים, לאחר שכבר הגיעו לידיה. ראו Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503 (2001). קר אף יצא נגד אנלוגיית הכספת שהוזכרה לעיל וגרס כי אנלוגיית כתב החידה מתאימה יותר. לשיטתו, נכון יותר לראות בקובץ מוצפן דבר הדומה למכתב שנתפס והוא כתוב בשפה אחרת המצריכה תרגום, או לפתק שרשם אדם בכתב יד שבמכוון הפך אותו ללא קריא, או לחידה אשר לאחר עיון מדוקדק בה מצליחים לפענח את הכתוב בה. ראו Kerr, שם, בעמ' 520-524. ראו גם את פרשנותו של רפאל ויניק (Winick) לחוקה האמריקנית, שלפיה היא אינה מקנה ציפיה מוגברת לפרטיות באשר למידע מוצפן: Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75, 89 (1994). עמדה זו תואמת את התפישה של הפסד"פ בישראל בכל הנוגע לצו החדירה לחומר מחשב, שלפיה תפיסתו והעתקתו של המידע הן העיקר ולא העיון בו.

99 אמנם מבחן הציפיה הסבירה לפרטיות מוחל לעתים (אם כי לא החלה גורפת) גם במשפט הישראלי: סעיף 1(8) לחוק האזנת סתר; אלכס שטיין "האזנת סתר ומעקבים אלקטרוניים נסתרים כאמצעים לקידומה של חקירה פלילית ובטחונות" משפטים יד 527, 535-536 (1985); ת"פ (שלום ת"א) 2762/94 מדינת ישראל נ' טל, בעמ' 39-41 (פורסם בנבו, 2.10.1995); ע"ע (ארצי) 90/08 איסקובי-ענבר נ' מדינת ישראל – הממונה על חוק עבודת נשים, בפס' 24, 48 ו-81 (פורסם בנבו, 8.2.2011). אולם בירנהק מראה כי ככלל מודל הגנת הפרטיות הישראלי רחב מן המודל האמריקני ותואם יותר את המודל האירופי. ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 217-244.

## ב) סמכויות איסוף הראיות והשלכתן על הזכות לפרטיות

בחלק זה אשוב למפת סמכויות האיסוף הקיימות בדין הישראלי. אראה, לאורו של הדין שערכתי ביכולות הטכנולוגיות לאיסוף, לאגירה, לשחזור ולכרייה של מידע, כיצד מבנה סמכויות איסוף הראיות הקיים אינו משרת כדבעי את הזכות לפרטיות. לאחר מכן אשוב אל פעולות איסוף הראיות הדיגיטליות שמניתי לעיל בפרק הקודם כסמכויות אפשריות המבטאות השתחררות מהתפישה הפיזית ואבחן את הפגיעות בפרטיות המגולמות בסמכויות מוצעות אלה. כזכור, הדין הישראלי באשר לסמכויות האיסוף מתאפיין בשלוש תבניות – חדירה, המצאה והאזנה.<sup>100</sup> אשר לסמכות החדירה לחומר מחשב, הוראות הפסד"פ המסדירות סמכות זו מדגישות את אלמנט החיפוש והתפיסה של המחשב כחפץ, ואילו הפעולות באשר למידע כשלעצמן – איסופו, אגירתו, שחזורו וכרייתו – אינן מטופלות למעשה בפסד"פ.<sup>101</sup> הנחת המוצא של המחוקק היא שסמכות ההאזנה היא הפוגענית ביותר, שכן היא מייצרת תיעוד להיקפי מידע גדולים, היא מגלמת פגיעה עודפת בצדדים שלישיים וכוללת עודפי מידע רבים. כיום בשל השתכללות יכולות האיסוף, האגירה, השחזור והכרייה של המידע, אפשר לטעון את ההפך, כי פעולה צופה פני עבר, של חדירה לחומר מחשב, תסב פגיעה מקיפה מפגיעתה של האזנה בכל הנוגע לפן של היחשפות להיקפי מידע אישי.<sup>102</sup> חדירה של רשויות החקירה למחשב אחד יכולה לכלול חשיפה לכמויות מידע אישי מסוגים שונים ובנפחים עצומים. בין סוגי המידע השונים אפשר שיימצא גם מידע שהמשתמש במחשב אינו מודע לקיומו, כיוון שהוא נובע מפעולות תיעוד אוטומטיות של המחשב; מידע הכולל תיעוד של תוכני תקשורת ("סוד שיח"); מידע הכולל חומרים שמשתמש המחשב מחק והניתנים לשחזור (לא תמיד בידיעתו של משתמש המחשב בדבר אפשרות שחזור המידע); מידע שיכול ליהנות מחיסיון מקצועי (כגון מידע רפואי, מידע שנועד להחלפה בין עורך דין ללקוח וכדומה); מידע אינטימי (תכנים מיניים למשל). לצד כל אלה עשוי המחשב לכלול גם סוגי מידע אחרים, שלא דווקא הגנת הפרטיות נפרשת עליהם, כגון מידע עסקי בעל ערך כלכלי.

נקודה חשובה נוספת היא שהתפישה הפיזית מביאה להחמצתו של הפוטנציאל להפחתת הפגיעה בפרטיות באמצעות שימוש בטכנולוגיות של אחזור מידע. כיוון ששלב הלוואי של התפישה הפיזית הוא שבמוקד, הרי שסמכות העיון במידע שבמחשב התפוס היא על פי רוב לא מוגבלת. לעומת זאת הפניית הזרקור למידע שבמחשב התפוס, על זיקותיהם השונות של הגורמים בעלי העניין והקשר למידע, בתוספת טכניקות האחזור המתוחכמות המאפשרות לדלות מידע רלוונטי מבלי לעיין בכלל המידע, עשויים להביא למיתון מסוים בפגיעה בפרטיות הנגרמת מעצם העיון והשימוש במידע המצוי במחשב התפוס. וכך, בית המשפט יוכל לבקר ולהגביל את

100 ראו בפרק ד.ב.2.ב).

101 ראו בפרק ד.ג.2..

102 עדיין אלמנטים אחרים מבחינים בין האזנה לחדירה, ובראשם אלמנט הסתר האינהרנטי להאזנה, לעומת חדירה לחומר מחשב במצב המשפטי הקיים שאינה סמויה מפני החשוד. בכל הנוגע לפעולת סתר, אם תיק החקירה מסתיים בהחלטה לגנוז אותו (בלא שימוע לחשוד), סביר להניח שיעד פעולת ההאזנה לא ידע על ביצועה לעולם. יש בכך פגיעה בפרטיות במובן של תחושת מעקב כללית של כלל הציבור שאינו יודע אם היה יעד בעבר לפעולת סתר שכזאת או יהיה יעד לה בעתיד.

הרשות החוקרת לא רק באשר לסוגיית התפיסה של המחשב, אלא גם, ואולי אף בעיקר, באשר לסוגי התכנים שיותר לרשות החוקרת לעיין בהם ולהשתמש בהם.

סמכות ההמצאה של מידע ממוחשב בידי צד שלישי רלוונטית במיוחד לחקירות פליליות במרחב הסייבר, שכן המידע הדיגיטלי מתאפיין בכיזוריות ובהיותו מוחזק בידי ספקיות שירות שונות. גם כאן, כבמקרה של סמכות ההמצאה, ליכולות האיסוף והאגירה השלכה ניכרת על היקפו ואיכותו של המידע שאפשר שאותן ספקיות שירות יסגירו על אודות לקוחותיהם. בנוסף, מבחינת המובנים השונים של הפגיעה בפרטיות, הסגרתו של המידע מספקית השירות לרשות החקירה היא הפרה של חובת סודיות שלה כלפי הלקוח שלה.<sup>103</sup> אמנם כאשר מדובר בפעולה כפויה של ספקית שירות, מכוח הוראה שיפוטית מחייבת, הרי שספקית השירות תהא מוגנת מאחריות פלילית או נזיקת כלפי משתמש המחשב והאינטרנט,<sup>104</sup> אולם יש להבחין בין פטור מאחריות לבין עצם הפגיעה בזכות. הפגיעה בזכות לפרטיות, במובן של הפרת יחסי האמון בין משתמש המחשב והאינטרנט לבין ספקית השירות, מתקיימת גם כאשר ספקית השירות פטורה מאחריות. בנוסף, מבחינת הלקוח ההעברה האמורה של המידע היא משום שימוש במידע שלא למטרה שלשמה נמסר (פגיעה בעקרון "צמידות המטרה"),<sup>105</sup> ושימוש זה פוגע באפשרותו של האדם לשלוט במידע על אודותיו גם לאחר יציאתו מידו.<sup>106</sup>

אשר לסמכות ההאזנה, גם כאן היכולות הטכנולוגיות משכללות מאוד את האמצעים והמוקדים שניתן להאזין להם (לכידת הקלדות, ניטור ברמת הפורטים של תעבורת האינטרנט, ניטור ברמת הנתב (router) הביתי, ניטור ברמת IP אצל ספקית הגישה לאינטרנט, ניטור ברמת ספקית התשתית לגלישה באינטרנט וניטור אצל ספקית שירות מסוימת כגון ספקית שירותי דוא"ל לתכונות של חשבון דוא"ל מסוים). היכולות הטכנולוגיות אף השתכללו בכיוון של הרחבת היקפי ההאזנה האפשרית ברזומנית.

סמכויות החדירה, ההמצאה וההאזנה אינן כוללות התייחסות לתהליך הטיפול במידע לאחר איסופו הראשוני בידי הרשות החוקרת. וכך, בכוחה של הרשות החוקרת להצליב את המידע עם

103 במונחי הטקסונומיה של Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, מדובר בפגיעה מסוג Breach of confidentiality. על פי חוק הגנת הפרטיות, מקורה של חובת הסודיות בהקשרנו יכולה לקום מכוח הסכם (סעיף 2(8) לחוק) או מכוח העובדה שספקית השירות מנהלת ומחזיקה מאגר מידע (סעיף 16 לחוק).

104 ראו סעיף 18(2)(ב) לחוק הגנת הפרטיות, הקובע כדלקמן: "במשפט פלילי או אזרחי בשל פגיעה בפרטיות תהא זו הגנה טובה אם נתקיימה אחת מאלה: ... (2) הנתבע או הנאשם עשה את הפגיעה בתום לב באחת הנסיבות האלה: ... (ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה" (ההדגשה שלי – ח"ו). כן ראו סעיף 16 לחוק, הקובע: "לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי" (ההדגשה שלי – ח"ו). בהקשר הפלילי ראו גם את הוראת הצידוק הכללית בסעיף 34(1) לחוק העונשין הקובעת: "לא יישא אדם באחריות פלילית למעשה שעשה באחד מאלה: (1) הוא היה חייב או מוסמן, לפי דין, לעשותו".

105 במונחי הטקסונומיה של Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, מדובר בפגיעה מסוג Secondary use.

106 פגיעה בעקרון צמידות המטרה יכול להתקיים גם כאשר מידע של צד שלישי אגור במחשב של נחקר שהמטרה תפסה אותו מידי (של הנחקר), וגם במצב של המצאת מידע בידי ספקית שירות על אודות לקוח שלה.

מאגרי מידע אחרים שברשותה, כאשר הכוונה הן למאגרים שהיא בנתה והן למאגרים שהיא קיבלה מידע מהם בדרך של העברת מידע בין גופים ציבוריים. הצלבת מידע זה וכריית המידע הממוקד מתוכו מתבצעים למעשה בידי הרשות החוקרת ללא בקשה ממוקדת בעניין זה.<sup>107</sup> תהליכי הצלבת המידע ה"חדש" עם מידע קיים במאגרי הרשות החוקרת אינם מבוקרים למעשה בשלב ההסמכה לביצוע פעולת האיסוף, והם לכאורה אינם בידיעתו של הגורם שמסמיך את הרשות החוקרת, וממילא הוא אינו שוקלם. לפיכך פעולת האיסוף הקונקרטי עלולה להיות בעלת אפקט רחב ומעמיק הרבה יותר, ויתרה מזאת, שיקול הדעת של הגורם המסמיך את הרשות החוקרת לבצע את פעולת האיסוף עלול להיות מוטא בשל אי-הבאתן בחשבון של הפגיעות הנוספות הכרוכות בתהליכי הכרייה וההצלבה עם מאגרי המידע הקיימים בידי הרשות החוקרת. ועוד, יש לציין כי מאגרי המידע המצויים בידי הרשות החוקרת, המשמשים בסיס לכרייה ולהצלבה עם המידע החדש שנאסף בחקירה, ככלל אינם גלויים לציבור, ומכאן שקיימת פגיעה בחופש המידע ומועצמת התחושה הציבורית הכללית של "חברת מעקב".<sup>108</sup>

אעבור עתה להתייחס להיבטי הפגיעה בפרטיות המגולמים בסמכויות האיסוף שנחסרות במשפט הישראלי בשל התפישה הפיזית החולשת על דיני איסוף הראיות במרחב הסייבר. בפרק ד.ג.3. מניתי פעולות אפשריות, שאינן קיימות בדין הנוכחי, וטענתי שיש מקום לבחון את אפשרות ההכרה בהן. בחינה זו מתאפשרת רק כתוצאה מהשתחררות ממשולש הסמכויות – חדירה, המצאה והאזנה – שמגלם כאמור תפישה פיזית באשר לדיני איסוף הראיות.

סמכות ההמצאה העתידית של מידע דיגיטלי מבטאת את ההכרה בכך שהמידע במרחב המקוון מבוזר ומוחזק בידי מתווכים, והוא מצטבר אצלם באופן רציף. מכאן שאפשר שיקום צורך חקירתי בהמצאה רציפה של המידע, להבדיל מהמצאה חד-פעמית או רב-פעמית (אך לא רציפה). ההמצאה העתידית פוגעת בפרטיות בכמה מובנים: ראשית, היא משכללת את יכולות האיסוף המידע של הרשות החוקרת.<sup>109</sup> יכולות האיסוף מורכבות הן מסוגי המידע שניתן לאספו והן מגיוון בנקודות האיסוף של המידע (במחשבי הקצה, בשרת שבו נאגר המידע או בכל "תחנה" אחרת של המידע). המידע עלול להשתנות בין ה"תחנות" השונות, ואפשרות גישה חקירתית אל "תחנות" המידע השונות מעשירה את פוטנציאל המידע הניתן לאיסוף. נוסף על כך, ההמצאה בידי צד שלישי מקלה על הרשות החוקרת את הצורך לפתח יכולות עצמאיות

107 במונחי הטקסונומיה של Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, מדובר בפגיעה מסוג Aggregation. כפי שצינתי לעיל בפרק ד בה"ש 97, אין מניעה חוקית מפורשת מהמשרה מלאגור את המידע העצום שהיא אוספת כדין במסגרת רבבות חקירות הכוללות חדירה לחומר מחשב.

108 חוק חופש המידע, התשנ"ח-1998, כולל חריג מיוחד לרשויות אכיפת החוק, ובכללן רשויות החקירה, המאפשר להימנע מלגלות לציבור פרטים על מאגרי המידע שברשותן. סעיף 9(ב) (8) לחוק קובע כי אין חובה למסור מידע במענה לבקשה לפי חוק חופש המידע, כאשר מדובר ב – "מידע על אודות שיטות עבודה ונהלים של רשות ציבורית העוסקת באכיפת החוק, או שיש לה סמכות חקירה או ביקורת או בירור תלונות על פי דין, אם גילויו עלול לגרום לאחד מאלה:

(א) פגיעה בפעולות האכיפה או הביקורת או בירור התלונות של הרשות;

(ב) פגיעה בהליכי חקירה או משפט או בזכותו של אדם למשפט הוגן;

(ג) גילוי או מתן אפשרות לגלות את קיומו או זהותו של מקור מידע חסוי".

109 במונחי הטקסונומיה של Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, מדובר בפגיעה מסוג Surveillance, אשר למעשה מתקיימת בכל סמכויות האיסוף שאסקור להלן.

לאיסוף, לפיענוח ולהפקה קבילה ראייתית של המידע באותה "תחנה". על כן ניתן לומר כי ככל שמרחיבים את מגוון נקודות איסוף המידע, מורחבת הלכה למעשה גם יכולת איסוף המידע. כפועל יוצא מכך נפגעת תחושת השליטה של אדם על המידע על אודותיו, וכן נפגע חופש הפעולה העצמית או החברתית שלו; שנית, ההמצאה העתידית כופה על ספקית השירות להפר למעשה את האמון שהיא חבה כלפי לקוחותיה; שלישית, אם ההמצאה העתידית סמויה מפניו של מושא הפעולה, הרי שמדובר בפעולת סתר כלפיו, ועצם פעולה בסתר כלפי מידע על אודות אדם היא פגיעה מסוג אחר בפרטיותו.<sup>110</sup> פעולת הסתר, וליתר דיוק הידיעה של משתמשי המרחב המקוון על האפשרות לביצוע פעולות סתר בידי רשויות החקירה,<sup>111</sup> מייצרת אפקט מצנן על פעילות משתמשי המחשב והאינטרנט. היא פוגעת באוטונומיה של הרצון החופשי שלהם, בתחושת השליטה שלהם בפעולותיהם ברשת ובאפשרותם לערוך בחירות רציונליות של פעולותיהם.

סמכות ה־Preservation (שמירה מכאן ולהבא) המוצעת מגלמת פגיעה בפרטיות כמוכנים האלה: האחד, מדובר באגירת מידע על אודות אדם, ואלמלא פעולת השמירה מכאן ולהבא, היה המידע מתנדף (או משתנה). בכך המידע יוצא משליטתו של האדם ואף יוצא ממסגרת ההסכמה בינו לבין ספקית השירות, הסכמה שמגבילה את אופני שמירת המידע וגלגולו לגופים אחרים; השני, משתמש המחשב והאינטרנט על פי רוב אינו מודע לקיומה של הוראת השמירה האמורה, קרי שמדובר בפעולת סתר בעניינו המגלמת, כפי שהסברתי לעיל לגבי סמכות ההמצאה העתידית, פגיעה מסוג נוסף בפרטיות; השלישי, תכלית שמירת המידע היא לאפשר בסופו של דבר לרשויות החקירה לעיין במידע.<sup>112</sup> למרות זאת הוראת שמירת המידע מפרקת את פעולת האיסוף לשני שלבים: שמירה ולאחר מכן עיון. ייתכן שלאחר שלב השמירה תפתח החקירה באופן שלא יהיה עוד כל צורך במידע (למשל אם יסתבר שהחשוד נקי מכל רבב, או אם החשוד יודה, ויימצאו תוספות ראייתיות מספיקות להודאתו כך שניתן יהיה לסיים את החקירה). במצב דברים כזה החקירה לא תגיע לשלב השני, של עיון במידע, ואם המידע שנאסף יוחזר לבעליו או יימחק – הרי שתיגרם פגיעה מופחתת במוכן הקונקרטי (להבדיל מהפגיעה במוכן הרחב של תחושת המעקב במרחב הממוחשב). עם זאת ייתכן שהחקירה תפתח לשלב שבו תידרש מסירה של המידע לרשויות החקירה. השימוש בצווים לשמירת מידע עלולה להוביל למעין רדוקציוניזם, על דרך של פירוק פעולות איסוף מורכבות לגורמים: "שמר עכשיו, עיין מאוחר יותר". הרדוקציוניזם הפרוצדורלי הזה עלול להביא להזנחה של השקלול הערכי הנדרש ולהוביל להכרעות שיפוטיות/מנהליות (תלוי במקור המסמך לפעולה) פוגעניות במיוחד מבלי שנשקלה התמונה בכללותה. אמחיש זאת בדוגמה הזאת: נניח שהרשות החוקרת מבקשת לאסוף את כל התכנים המגיעים לשרת כלשהו שחשוד מחזיק אצל חברה המספקת שירותי אחסון (hosting).

110 במונחי הטקסונומיה של Solove, שם, מדובר בפגיעה מסוג Exclusion.

111 לרשויות החקירה אינטרס חזק לשמר את יכולות האיסוף שלהן בחיסיון, כיוון שחשיפת היכולות משמעה גם חשיפת "נקודות התורפה" מבחינת רשויות החקירה, היינו חשיפת סוגי המידע שאין באפשרותן לאסוף. חשיפה זו עשויה להביא לנהירת משתמשים לשירותים מקוונים החסונים מפני עיני "האח הגדול".

112 ראו Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, 25–32 (2008).



נניח עוד שספקית שירותי האירוח אינה נוהגת לגבות את התכנים בשרת של החשוד, ותכנים אלה משתנים מעת לעת. עתה נניח שהמשטרה מעוניינת לעקוב אחרי הנעשה בשרת של החשוד למשך תקופה של שלושים יום מהיום. חששה של המשטרה הוא שאם תוציא צו חדירה לחומר מחשב ותבצע אותו בעוד שלושים יום, הרי שמידע רב שהיה בשרת יימחק בינתיים. אפילו אם תוציא המשטרה צווי חדירה לחומר מחשב בתחילת מניין שלושים הימים ובסיומם, עדיין היא עלולה להחמיץ מידע חשוב לחקירה. כיום האפשרות היחידה שבידי המשטרה היא לבקש מבית המשפט צו האזנת סתר ולנטר את ההתקשרויות הנכנסות והיוצאות מהשרת על מנת לעקוב אחרי הפעילות במשך שלושים הימים. לעומת זאת במשטר משפטי המתיר צווי שמירה יכולה המשטרה לפרק את פעולתה לשניים, ובכך להמעיט בכל אחד משני השלבים את הביקורת הקפדנית יותר של האזנת סתר: בשלב הראשון תתבקש שמירה של המידע בלבד אצל ספקית שירותי האירוח. בשלב זה הפגיעה בחשוד לכאורה פחותה, כיוון שהמשטרה לא תעיין במידע, וגם ספקית שירותי האירוח עצמה רק תשמר את המידע ואף היא לא תעיין בו או תגלה את תוכנו. בשלב השני תתבקש המצאה בלבד של מידע שכבר קיים ברשותה של ספקית שירותי האירוח. כל אחד משני השלבים האלה כשלעצמו, השימור ולאחר מכן ההמצאה, אינו כולל את היסודות של האזנת סתר. במילים אחרות, הגישה של "שמר עכשיו, עיין מאוחר יותר" אינה רק פירוק של פעולת איסוף לשני שלבים כרונולוגיים, אלא היא עלולה גם לפרק את פעולת האיסוף מבחינת ההגנות המהותיות של הדין מפני פעולת הרשות החוקרת.

היות שפעולת שמירה מטרתה לאפשר המצאה מאוחר יותר, ייתכן לדרוש כי אפשרות ההמצאה ומשמעותה יישקלו כבר בעת מתן הוראת השמירה. אמנם הוראות השמירה מכאן ולהבא מוצאות בשלבי החקירה הראשוניים בלבד, כאשר מהות החשד, מעגל החשודים וחיוניות הראיות המבוקשות עוד אינם מבוררים עד תום, אולם עדיין ניתן להניח לחומרה שהמידע המבוקש יוסגר לרשויות. זאת כמובן נוסף על הפגיעה המגולמת בשמירה כשלעצמה, כאשר מידע על אודות אדם נאגר, על פי רוב בלי ידיעתו, ובניגוד למהלך הפעולה הרגיל של הגורם שנצטווה לשמור את המידע. ועוד, יש מקום לשקול, במסגרת בקשת ההמצאה המאוחרת, אם המידע שהמצאתו מתבקשת הוא מידע הקיים דרך כלל ברשות הנמען לצו המבוקש, או שמא מדובר במידע שנאסף בהוראה כפויה של צו שמירה קודם.

סמכות ה־Retention פוגעת בפרטיות בכמה מובנים: האחד, היא מייצרת איסוף מידע כלפי כלל האזרחים, ללא חשד ספציפי, תוך התגברות על האפשרות שהמידע יתנדף מאליו. איסוף המידע פוגע בוודאות ברוב של משתמשים נורמטיביים לטובת אפשרות לייצר תיעוד של פעילות עבריינית של מיעוט. בשל שמירת המידע דרך קבע עלול להיווצר אפקט של פן אופטיקון<sup>113</sup> מצנן על פעילות משתמשי המחשב והאינטרנט אשר יחששו לדבר בחופשיות ולפעול בחופשיות

113 על הפן אופטיקון כתב במקור ג'רמי בנת'האם (Bentham), ומישל פוקו (Foucault) חזר אל המודל הארכיטקטוני של הפן אופטיקון. כן ראו OSCAR H. GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993) וגובר בטכנולוגיות מעקב ובמחשוב (נכון לתקופת כתיבת הספר). עוד ראו Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996), שם המחברת דנה בחשש מפני עידוד טכנולוגיות של מעקב אחרי הרגלי הגלישה באינטרנט לצורך מניעת הפרות של זכויות יוצרים באינטרנט. ראו עוד בירנהק, "שליטה והסכמה", לעיל ה"ש 8, בעמ' 60-67.

מתוך הידיעה שמעשיהם מתועדים לפרק זמן לא מבוטל.<sup>114</sup> העובדה שהמידע נאסף דרך קבע על כלל משתמשי המרחב הקיברנטי, הגם שהיעד האמתי הוא המיעוט החשוד בביצוע עברות פליליות, מעוררת שאלות בכיוון של מידתיות השימוש באמצעי (retention) לצורך השגת המטרה (איתור עבריינים ואיסוף ראיות לביצוען של העברות). דיון מעין זה נערך בבית המשפט הגבוה לצדק של האיחוד האירופי (ECJ), אשר בחן – ולבסוף פסל – את הדירקטיבה האירופית משנת 2006 בדבר שימור מידע (Data retention directive).<sup>115</sup> בנוסף, ללא אמצעי פיקוח מתאימים קיים חשש שספקית השירות תשתמש במידע האמור לצרכיה שלה או תעבירו לצד מעוניין אחר, ובכך לא זו בלבד שהמידע ייאגר שלא בשליטתו של משתמש המחשב והאינטרנט, אלא שגם עלולים להתבצע במידע שימושי המשך שאינם בידעתו, לא כל שכן בשליטתו.<sup>116</sup>

השני, בעיית הרדוקציוניזם, שעליה עמדתי לעיל בהקשר של סמכות השמירה מכאן ולהבא (Preservation), מתעוררת גם בהקשר של סמכות ה־Retention במלוא החרפות. הוראת השימור דרך קבע אינה התחנה הסופית מבחינת רשויות החקירה אלא היא תחנת המוצא. כאשר יתעורר חשד קונקרטי, תפנה הרשות החוקרת לספקית השירות ותבקש את המצאת המידע שברשותה. במועד זה, של דרישת ההמצאה, הוראת השימור דרך קבע ותוצאותיה כבר ייתפשו כמוכנות מאליהן, וכך המשקל המצטבר של שימור דרך קבע והמצאה לרשות על בסיס חשד קונקרטי – לא יובא בחשבון.

הסמכות להורות על יצירת תשתית המאפשרת לרשות לאסוף ראיות דיגיטליות נועדה לשרת את הרשות החוקרת באופן שלא תיחסמנה האפשרויות, מבחינה טכנולוגית, לאסוף ראיות דיגיטליות במרחב הסייבר. מנקודת מבטה של הגדרת סמכויות האיסוף מדובר בסמכות נפרדת במהותה, אולם מנקודת מבטה של הזכות לפרטיות, מדובר בסמכות שנועדה לשרת שירות מכשירי הפעלה של סמכויות אחרות אשר תפגענה בהמשך בפרטיות, כגון סמכות ההאזנה או ההעתקה של המידע. יש לשים לב שהגם שמדובר בסמכות מכשירנית, השלכתה היא גורפת, והפוטנציאל המגולם בה הוא לפגיעה בכלל ציבור משתמשי המחשב והאינטרנט, היינו לפגיעה עודפת בשיעור ניכר.<sup>117</sup>

114 ראו Catherine Crump, *Data Retention: Privacy, Anonymity and Accountability Online*, 56 STAN. L. REV. 191 (2003).

115 ראו Digital Rights Ireland Ltd. v. Minister of Communications, Marine and Natural Resources, ECJ C-293/12 [2014].

116 במונחי הטקסונומיה של Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, מדובר בפגיעה מסוג Secondary use, ובמונחי בירנהק, במקורות המצוטטים לעיל ה"ש 8, תהא זו פגיעה בעקרון "צמידות המטרה". במונחי חוק הגנת הפרטיות מדובר בפגיעה על דרך של שימוש במידע שלא למטרה שלשמה נמסר, על פי הגדרת סעיף 2(9) לחוק.

117 בהקשר של הפעלת סמכויות ביטחון פורסם בהמשך לפרשת סנאודן, שהזכרתי לעיל בה"ש 86 ו-92, כי ה־NSA האמריקני, בשיתוף עם ה־GCHQ, סוכנות הסיגינט הממשלתית של בריטניה, הצליחו לפצח את מרבית ההצפנות אשר בשימוש ספקיות השירות הגדולות באינטרנט. עוד פורסם כי בחלק מן המקרים ספקיות שירות גדולות, כגון מיקרוסופט, יצרו תשתית טכנולוגית בשביל ה־NSA, אשר תאפשר לה לנטר תעבורת רשת כשהיא לא מוצפנת. ראו Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, THE NEW YORK TIMES (5.9.2013) [http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&\\_r=0](http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&_r=0)

הסמכות לחדירה סמויה לחומר המחשב והעתקת המידע ממנו, כמו גם הסמכות לתיעוד סמוי של הפעילות במחשב הקצה, אלה הן שתי סמכויות שהכרה בהן נועדה להשלים, מבחינת רשויות החקירה, את מכלול אפשרויות הניטור והאיסוף הסמויים של מידע ממחשב הקצה, כאשר הגדרת האזנת הסתר, כפי שהיא מנוסחת היום, על פי התבניות של התפישה הפיזית, אינה מאפשרת אותם. מבחינת הזכות לפרטיות מדובר בשתי סמכויות נוספות המעמיקות את הפגיעה בפרטיות באמצעות הרחבת האפשרויות של איסוף המידע על אודות אדם ובאמצעות הרחבת מעגל פעולות הסתר.<sup>118</sup>

הסמכות לפיצוח הצפנות והתגברות על סממאות מתייחסת לסט הכלים המשפטיים שמוענק לרשות החוקרת על מנת להתגבר על השימוש בטכנולוגיה מגבירת פרטיות מצד משתמש המחשב והאינטרנט או מצד ספקית השירות שלו. המצב המשפטי הקיים כיום בישראל הוא שאם יש לרשויות החקירה האפשרות הטכנית להתגבר על ההצפנה או על הגנת הסממה, הרי שבאפשרותה לפעול בעניין ללא צורך בהסמכה קונקרטיה נוספת לשם כך.<sup>119</sup> זאת כיוון שהתפישה הפיזית אינה מתייחסת לתכונתו האינהרנטית של המידע הדיגיטלי כניתן להצפנה ולהגנה בסממה בנקל, ועל כן מטבע הדברים אין התייחסות חוקית או שיפוטית לסוגיה. כשמבקשת הרשות החוקרת לכפות על אדם למסור את מפתח ההצפנה שלו או את סממתו, מתעוררת שאלה במישור של הזכות לאי-הפללה עצמית. בכל הנוגע לשימוש בהצפנות/סממאות והזכות לפרטיות, כאן קיימת מחלוקת בין הגישה האמריקנית לגישה האירופית (והישראלית): הגישה האמריקנית תראה בשימוש בהצפנות/סממאות משום פעולה המגבירה ציפייה לפרטיות ולפיכך מכוננת, או למצער מעצימה, את הזכות לפרטיות באשר למידע הנדון. לעומתה, הגישה האירופית והישראלית מכירה בזכות לפרטיות כזכות בעלת תוקף עצמאי. לפיכך השימוש בהצפנה/סממה אינו אלא מתן ביטוי לזכות אך אינו פעולה המקימה את הזכות או מעצימה אותה.<sup>120</sup> יצוין עוד כי במקרה שבו תצווה ספקית שירות להסיר את ההצפנה או את הגנת הסממה מעל תכניו של משתמש שהוא לקוח שלה, להבדיל ממצב שבו המשתמש עצמו יצטוו לעשות כן, הרי שמבחינת המשתמש, מלבד הפגיעה בסודיות התכנים בשל ההוראה הכופה, ייפגע גם אמונו בספקית השירות.<sup>121</sup>

הנשיאה בנייש עמדה בפסק דינה בעתירה נגד חוקתיות חוק נתוני תקשורת, על "המורכבות שבהצבת איזונים חוקתיים ותחימת גבולותיה של הזכות לפרטיות בעידן הנוכחי".<sup>122</sup> הכרה זו של בית המשפט העליון היא צעד חשוב בכיוון פיתוח פסיקתי של הזכות לפרטיות באופן שתכיל את המעבר מאיסוף ראיות פיזיות לאיסוף ראיות דיגיטליות בחקירה פלילית. בחלק זה ביקשתי לפתח את הדיון העיוני בהיבטי הזכות לפרטיות בהקשר של איסוף ראיות דיגיטליות בחקירה פלילית במרחב הסייבר, ובדגש על ההיבטים המושפעים מההינתקות

118 הרחבת מעגל פעולות הסתר היא, במונחי הטקסונומיה של Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, פגיעה מסוג Exclusion.

119 ראו פרק ד.ג.3.

120 למחלוקת בין הגישה האירופית לאמריקנית, ראו לעיל טקסט לה"ש 96–99.

121 במונחי הטקסונומיה של Solove, *A Taxonomy of Privacy*, לעיל ה"ש 77, מדובר בפגיעה מסוג breach of confidentiality. ראו גם לעיל טקסט לה"ש 103–104.

122 ראו עניין האגודה לזכויות האזרח בישראל, לעיל ה"ש 82, בעמ' 3627.

מן התפישה הפיזית של הראיות הדיגיטליות. הצבעתי על התפתחויות טכנולוגיות שונות המשכללות את יכולות האיסוף, האגירה, השחזור והכרייה של המידע הדיגיטלי. התפתחויות אלה מגבירות את הפגיעה בזכות הפרטיות, כאשר התפישה הפיזית באשר לדיני איסוף הראיות מחמיצה במידה רבה את המשמעותיות הפוגעניות של התפתחויות אלה. לאחר מכן הצגתי את מערך הסמכויות המשפטיות הקיימות כיום בדין הישראלי באשר לדיני איסוף הראיות הדיגיטליות בחקירה פלילית במרחב הסייבר והראיתי כי מערך זה, המגלם תפישה פיזית, חוטא לעושר המובנים של הפגיעה בפרטיות הנוצרת מהמעבר מזירת החקירה הפיזית לזירת החקירה הקיברנטית. בנוסף, גם הרחבה של מערך הסמכויות המשפטיות מחייבת הכרה במשמעותיות הפגיעה בפרטיות לצורך עריכת איזון בין צורכי החקירה לבין מערך ההגנות החוקתיות.

## 2. הזכות לקניין במידע

התפישה הפיזית מניחה כי תוכנה של הראיה ומשמעותה אינם נפרדים מן החפץ הפיזי שבו הם מיוצגים. לעומת זאת המידע הדיגיטלי נפרד מן החומרה שעליה הוא מוטבע. להפרדה זו נפקויות שונות: האחת, מידע הראוי להגנה קניינית יכול לשאת את ההגנה בקשר עם כל "מקום" שבו הוא נמצא או חפץ שעליו הוא מוטבע. כך למשל התפישה המודרנית של חסיון עורך דין – לקוח גורסת כי המידע החסוי אסור בעיון של רשויות החקירה בכל מקום שבו הוא נמצא, בין שזה במחשבו של עורך הדין ובין שזה במחשבו של הלקוח;<sup>123</sup> שנית, החומרה יכולה להשתייך לאדם אחד, והמידע – לאדם אחר. וכך למשל יכול מעביד שרכש מחשב בשביל עובדיו להסכים לתפיסת המחשב כחפץ, אך אינו יכול בהכרח להסכים בשם העובד המשתמש במחשב שהמשטרה תחדור למידע שבו.<sup>124</sup> במילים אחרות, פעולת התפיסה (Seizure) ביחס למידע אינה בעלת משמעות כבמקרה של תפיסת חפץ פיזי; פעולות החדירה, ההעתקה, העיון והשימוש במידע הן הפעולות בנות המשמעות המורכבת יותר מבחינת פגיעה בזכויות חוקתיות. זכות הקניין, ככלל, מתפרשת על המחשב כחפץ.<sup>125</sup> ברגע שניתקת הזיקה בין המידע לבין החפץ, אפשר שתתעוררנה כמה שאלות: אם זכות הקניין נפרשת על המידע כשלעצמו, כולו או על סוגים מסוימים שלו; מה הרלוונטיות של זכות הקניין ביחס למידע בהקשר של איסוף ראיות בחקירה פלילית במרחב הסייבר, בייחוד בשים לב שמידע אישי מוגן מפני חדירה, העתקה, עיון ושימוש מכוח הזכות לפרטיות; מה טיב ההגנה מכוח זכות הקניין, או מהו מובנה של זכות הקניין הצריך לעניינו. ארון בתמצית בשאלות הללו כסדרן.

123 ראו רע"פ 8873/07 היינץ ישראל בע"מ נ' מדינת ישראל (פורסם בנבו, 2.1.2011). בפרט הדברים אמורים לאור תכונותיו של המידע הדיגיטלי ככזה הניתן להעתקה ולהעברה בלחיצת כפתור.

124 בעניין R. v. Cole, [2012] SCC 53 (Ca.) נדרש בית המשפט העליון הקנדי למקרה שבו מורה נאשם בהחזקת תכנים פדופיליים במחשב נייד שקיבל מטעם בית הספר שבו הועסק. במחשב נייד זה שמר המורה תכנים מקצועיים וגם תכנים אישיים. המעביד, בית הספר, מסר למשטרה הסכמה כי זו תחדור למחשב, והמשטרה חדרה על בסיס הסכמה זו למחשב והפיקה ראיות בלא צו שיפוטי מסמך. נקבע כי הופרה הציפייה הסבירה של המורה לפרטיות, וברוב דעות של שישה שופטים כנגד אחד, נקבע כי יש לפסול את הראיות הדיגיטליות שנאספו.

125 ראו Ohm, לעיל ה"ש 112. כן ראו סעיף 32 לפסד"פ, ביחד עם סעיף 1 לפסד"פ המגדיר "חפץ" ככולל גם "חומר מחשב", וזה מוגדר בסעיף 1 לחוק המחשבים, התשנ"ה–1995, ככולל גם "מידע".

אשר לשאלה הראשונה: זכות הקניין נפרשת על מידע מסוגים שונים ובאופנים שונים. למשל, בדין הישראלי מידע שהוא "סוד מסחרי" מוגן מפני גזל.<sup>126</sup> זכות היוצרים מגנה מפני הפרת הזכות הבלעדית לעשות ביצירה פעולות שונות, כגון העתקה, פרסום ראשון, ביצוע פומבי, שידור ועוד.<sup>127</sup> הסימן המסחרי מקנה לבעליו זכות לשימוש ייחודי.<sup>128</sup> הפטנט מגן מפני ניצול המצאה רשומה ומפורסמת בלי רשות מן הבעלים או שלא כדין.<sup>129</sup> חסיון עורך דין-לקוח מגן על המידע שהוחלף בין עורך הדין ללקוח בקשר לשירות המקצועי.<sup>130</sup> לעומת זאת קיימים סוגי מידע אחרים שאינם מוגנים כשלעצמם מכוח זכות הקניין, ולמעשה לא כל מידע, כשלעצמו, מוגן מכוח זכות הקניין.<sup>131</sup> כך הוא למשל באשר למידע שפורסם ברבים או באשר למידע עסקי שאינו עולה כדי "סוד מסחרי".<sup>132</sup> עם זאת קולות שונים קוראים להרחבת ההגנה הקניינית על מידע כדי שתחבוק סוגי מידע רבים יותר או אף את כל סוגי המידע.<sup>133</sup>

- 126 ראו סעיף 6 לחוק עוולות מסחריות, התשנ"ט – 1999 (להלן – חוק עוולות מסחריות); ע"א 312/74 החברה לכבלים ולחוטשי חשמל בישראל בע"מ נ' קריסטטיאנפולר, פ"ד כט(1) 316, 319–320 (1974); בג"ץ 1683/93 יבין פלסט בע"מ נ' בית הדין הארצי לעבודה, פ"ד מז(4) 702, 706 (1993); ע"א 1142/92 ורגוס בע"מ נ' כרמקס בע"מ, פ"ד נא(3) 421, 429–430 (1997); עב (אזורי חי) 1800/00 טנקו אינטרנשיונל (97) בע"מ נ' גיא (פורסם בנבו, 18.5.2006).
- 127 ראו סעיף 11 לחוק זכות יוצרים, התשס"ח–2007 (להלן – חוק זכות יוצרים). ודוק, דיני זכויות היוצרים מגנים על היצירה, לא דווקא על המידע המרכיב אותה. הגנת זכות היוצרים אינה חלה על העובדות, אלא על דרך ביטויין. דרך ביטוי המקובעת בדרך כלשהי ומקורית תוגן, ואילו המידע הגולמי כשלעצמו – לא יוגן.
- 128 ראו סעיף 46 לפקודת סימני מסחר [נוסח חדש], התשל"ב–1972.
- 129 ראו סעיף 49 לחוק הפטנטים, התשכ"ז–1967. ודוק, ההגנה היא על ההמצאה, אך המידע כשלעצמו, שעל בסיסו נוצרה ההמצאה, אינו מוגן, אלא להפך – הוא גלוי לעיני כולי עלמא.
- 130 ראו בהקשר זה את עמית איתי "החסינות הראייתיים כמוסד קנייני" 64–82 (חיבור לתואר "מוסמך" במשפטים, אוניברסיטת תל-אביב, 2012).
- 131 כך הוא למשל בכל הנוגע למידע חדשותי, עובדה, נתון, רעיון ועוד. ראו סעיף 5 לחוק זכות יוצרים. כן ראו (ROGER SMITH, PROPERTY LAW 5 (6<sup>th</sup> ed., 2009).
- 132 חוק עוולות מסחריות מגדיר בסעיף 5 "סוד מסחרי": "מידע עסקי, מכל סוג, שאינו נחלת הרבים ושאינו ניתן לגילוי כדין בנקל על ידי אחרים, אשר סודיותו מקנה לבעליו יתרון עסקי על פני מתחיריו, ובלבד שבעליו נוקט אמצעים סבירים לשמור על סודיותו".
- 133 קיימת הגנה, או למצער הכרה, בקניין רוחני במובן רחב יותר, כפי שנקבע ברע"א 5768/94 א.ש.י.ר. יבוא יצור והפצה נ' פורום אביזרים ומוצרי צריכה בע"מ, פ"ד נב(4) 289, 491–492 (1999): "גם מוצר שאינו מוגן על ידי חוקי הקניין הרוחני עשוי לגלם קניין רוחני. קניין רוחני הוא, לצורך זה, קניין רוחני מבחינה מהותית, ולא בהכרח במובן של חוקי הקניין הרוחני. זהו קניין רוחני במובן רחב... (בעמדה זו תמכו שישה מתוך שבעת שופטי ההרכב בתיק). עוד על גישה מרחיבה למידע כקניין רוחני בהקשר של העברה של הפרת אמונים בתאגיד, ראו יובל קרניאל הפרת אמונים בתאגיד 70–72, 79 (2003). כן ראו שרון גולדנברג-אהרונאי "חדירה למערכות מחשב – היקפה הרצוי והמצוי של העברה" Susan W. ; (2009) Brenner, *Should Criminal Liability Be Used to Secure Data Privacy?*, in SECURING PRIVACY IN THE INTERNET AGE 271, 280–279 (Anupam Chander, Lauren Gelman & Margaret J. Radin eds., 2008). ברנר בוחנת במאמר זה את עברות המידע וקוראת לשימוש בעברות כנגד הקניין לצורך הפללת עברייני מידע, שכן למידע יש פן קנייני מלבד הפן של הפרטיות.

עתה לשאלה השנייה: מה הרלוונטיות של ההגנה הקניינית לענייננו? ניתן לזהות חפיפה מסוימת בין ההגנה הקניינית על המידע לבין ההגנות על המידע מכוח הזכות לפרטיות.<sup>134</sup> החפיפה בולטת יותר ככל שעסקינן בתאוריות מרחיבות, יחסיות ונורמטיביות לקניין ולפרטיות. כך למשל הגישה של בירנהק לפרטיות כשליטה<sup>135</sup> והגישה של חנוך דגן לקניין כמוסדות המסדירים יחסים בין פרטים בדבר משאב מסוים<sup>136</sup> תימצאנה בחפיפה מסוימת.<sup>137</sup> עם זאת החפיפה, כפי שטוען בירנהק, אינה מלאה, ויש מקום לבידול הדיון בפרטיות מהדיון בקניין. את הפרטיות כשליטה יש לתפוש כנובעת מערכים של אוטונומיה של הרצון ושל כבוד, ולא דווקא של קניין.<sup>138</sup> מבחינה מעשית, לשיטתו של בירנהק, תאגיד למשל אינו רשאי לטעון לפגיעה מכוח הזכות לפרטיות אלא לכל היותר לפגיעה בזכות הקניין.<sup>139</sup> על פי גישה זו, התאגיד יכול

134 כביטוי מעשי לחפיפה זו ראו למשל את פסק דינו של בית המשפט העליון האמריקני: Florida v. Jardines, 133 S. Ct. 1409 (2013). באותו מקרה נדונה השאלה הזאת: כאשר המשטרה משתמשת בכלבי גישוש לאיתור סמים בביתו של חשוד, בהעמדה את הכלב סמוך לדלת הכניסה לבית (אם כי מחוץ לבית) – האם מדובר בחיפוש המצריך צו שיפוטי? בית המשפט פסק, ברוב דעות, כי מדובר בפעולה המחייבת צו חיפוש. ההנמקה של דעת הרוב נחלקה בין הנמקה קניינית, שלפיה מדובר בפעולה הפולשת לקניינו של אדם, לבין הנמקה מתחום הפרטיות, שלפיה מדובר בשימוש באמצעים מיוחדים לחשיפת מידע על אודות החשוד (להנמקה הקניינית ראו פסק דינו של השופט Scalia, ולהנמקה מתחום הפרטיות ראו פסק דינם של השופטים Kagan, Ginsburg & Sotomayor).

135 ראו בירנהק "שליטה והסכמה", לעיל ה"ש 8; בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 89–108.  
136 ראו חנוך דגן קניין על פרשת דרכים 80–37 (2005). דגן יצא נגד ההגדרה הקלאסית, הבלקסטוניאנית, של קניין הרוואה בה זכות שביטויה האולטימטיבי הוא בשרירות הבעלים (Sole and despotic dominion) בנוגע לקניין. ראו WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, Vol. II, Ch. 1 (2<sup>nd</sup> ed. 1915). לביטויי הגישה הבלקסטוניאנית בפסיקה הישראלית, ראו למשל את רע"א 7112/93 צודלר נ' יוסף, פ"ד מח(5) 550, 567 (1994); ראו את עמדת השופטים טירקל, חשין ומצא ברע"א 6339/97 רוקר נ' סלומון, פ"ד נה(1) 199 (1999). דגן ראה בגישה הבלקסטוניאנית גישה המציעה הגדרה אחידה-מוניסטית לקניין, ואילו לדידו הגדרת קניין היא פלורליסטית ותלויה במשאב שבו מדובר ובמערכת היחסים בנוגע אליו. עוד על תפישות פלורליסטית של קניין, ראו Gregory S. Alexander, *Pluralism and Property*, 80 FORDHAM L. REV. 1017 (2011).  
137 ראו LAWRENCE LESSIG, CODE VERSION 2.0 230–228 (2006). לסיג הציע להמשיג את הפרטיות כקניין ברמה העקרונית וברמה המעשית, ואף טען כי המשגה זו תועיל לשדרוג מעמדה של הזכות לפרטיות.

138 ראו בירנהק "שליטה והסכמה", לעיל ה"ש 8, בעמ' 46–47. בירנהק מבקר שם את עמדתו של לסיג, שלפיה הזכות לפרטיות חופפת למעשה את זכות הקניין. בירנהק, המצדד בהבנת ה"פרטיות כשליטה", מציין כי הגם שהמונח "שליטה" נשמע קנייני באופיו, אין לתפוש את הפרטיות כזכות הנלמדת מזכות הקניין: השליטה שמסבירה ומצדיקה את הפרטיות אינה שליטה במשאב רגיל אלא שליטה של האדם בעצמו, בוהותו, באישיותו, במידע על אודותיו ובגלגוליו של המידע ובשימושים שנעשים בו מרגע שהמידע יוצא מידי. ראו גם Yofi Tirosh & Michael Birnhack, *Naked in Front of the Machine: Does Airport Scanning Violate Privacy?*, 74 OHIO ST. L.J. 1263, 1299–1302 (2013).

139 ראו בירנהק "שליטה והסכמה", לעיל ה"ש 8, בעמ' 46–47. לעמדה בפסיקה שלפיה אין פרטיות לתאגיד, ראו בג"ץ 648/99 נאוי נ' יו"ר הכנסת (פורסם בנבו, 1.2.1999); ע"א 5893/91 טפחות בנק משכנתאות לישראל בע"מ נ' צבאח, פ"ד מח(2) 573, 591–592 (1994); ת"א (שלום חי) 4901/08 גרפונט בע"מ נ' פלד (פורסם בנבו, 22.7.2009); מיגל דויטש עוולות מסחרית וסודות מסחר 491–489 (2002). מנגד, ראו פסיקה המצדדת בטיעון שלפיו יש פרטיות לתאגיד: בש"א (מחוזי ת"א) 5416/04 מגורים יו"ם נ' פלאפון תקשורת (פורסם בנבו, 14.9.2004); בש"א (מחוזי ת"א) 1614/02 מולטיליק בע"מ נ' רב בריח (פורסם בנבו, 7.2.2002); ת"א (מחוזי חי) 1563/95 קיסרית יצור רהיטים בע"מ נ' ארט חברה לביטוח בע"מ (פורסם בנבו, 28.11.2000). מבחינת הוראות חוק הגנת הפרטיות, השאלה

בהחלט להחזיק ברשותו מידע אישי מוגן-פרטיות, אלא שהטוענים לזכות זו יכולים להיות עובדי התאגיד, לקוחותיו או כל אדם אחר שהתאגיד מחזיק מידע על אודותיו, אולם התאגיד כשלעצמו אינו זכאי לטעון לפגיעה בפרטיות. עם זאת מידע עסקי, בעל ערך כלכלי, בין של אדם פרטי ובין של תאגיד, מגלם אינטרסים קנייניים מבחינת זכות השימוש במידע, הזכות למנוע מאחרים גישה אל המידע והאפשרות לסחור במידע, ותחול עליו הגנה מכוח זכות הקניין. כשמדובר בתאגיד, תחול ההגנה הקניינית תחולה ייחודית, וכשמדובר באדם פרטי, תחול ההגנה הקניינית לצד הגנת הפרטיות על המידע, ותשלים אותה.

אעבור עתה לשאלה השלישית: מה טיב ההגנה הקניינית בהקשר של חקירה פלילית במרחב הסייבר? כאמור לעיל, התפישה הפיזית לוקה בהאחדת המידע והמחשב כחפץ. יש מקום בהתבוננות על המידע ה"נתפס" בחקירה כראיה שאיסופה מקים שאלות עצמאיות בקשר לזכות הקניין. הגדרת אגד הזכויות הקנייניות באשר למידע, בעיקר מידע במרחב הקיברנטי, היא משימה מורכבת.<sup>140</sup> בהקשר של איסוף ראיות דיגיטליות בחקירה פלילית במרחב הקיברנטי אצביע על שתי השלכות אפשריות של התפישה הפיזית על זכות הקניין: השלכה על זכות השימוש של הבעלים<sup>141</sup> במידע והשלכה על זכות הבעלים לשלול מאחרים חשיפה אל המידע. אשר לזכות השימוש של הבעלים במידע, זכות זו מחדדת את הפער בין הראיה הפיזית לבין הראיה הדיגיטלית. הראיה הדיגיטלית, ככלל, ניתנת להעתקה מושלמת, שאינה מפחיתה מתוכן המידע ומהנתונים על אודות התוכן. הראיה הפיזית פעמים רבות אינה ניתנת להעתקה כלל, או שההעתקה חלקית מבחינת התכונות של החפץ שאותן היא מעבירה להעתק.<sup>142</sup> בכל הנוגע לאיסוף ראיות דיגיטליות בחקירה פלילית במרחב הסייבר, בפני הרשות החוקרת עומדת פעמים רבות הבחירה בין העתקת המידע הדרוש לבין שלילתו מאת בעליו. ההגנה הקניינית, בהיבט של זכות השימוש של הבעלים במידע, תבכר העתקה על פני שלילה.

נותרה פתוחה במידה מסוימת: אמנם סעיף 3 לחוק ממצט "תאגיד" מהגדרת "אדם", ומכאן שלכאורה אין פרטיות לתאגיד, אולם סעיף 2(5) לחוק מדבר בפגיעה בפרטיות על דרך של "העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב..."; כמו כן חוק-יסוד: כבוד האדם וחירותו, המעגן בסעיף 7 את הזכות לפרטיות, אינו ממצט את התאגידים מתוך הגנת הסעיף. על כל פנים, הטעון של בירנהק ביחס לשאלת הפרטיות לתאגיד אינו ממוקד רק במישור הדוקטרינרי כי אם בעיקר במישור הנורמטיבי.

140 ראו Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission*, *Trades and Ecosystem*, 83 MINN. L. REV. 129 (1998). לשיטתה של קרול רוז (Rose), מושג הבעלות על המידע, מידת הנגישות אל המידע, יכולת השליטה על המידע לרבות הזכות למחקו כאשר הוא מצוי בידי ספקיות שירות – כל אלה ואחרים מקבלים במרחב הסייבר משמעויות שונות מאשר כשמדובר מקרקעין או במיטלטלין פיזיים. רוז התייחסה לקניין במרחב הקיברנטי בהקשר כללי, לא בהתייחס לחקירה פלילית אשר במסגרתה מתבקש איסוף מידע. כאמור, הטעון שלי כאן ממוקד הרבה יותר, ועניינו בנפקות התפישה הפיזית להגנת זכות הקניין במרחב הסייבר בהקשר של איסוף ראיות בחקירה פלילית בלבד.

141 ב"בעלים" כוונתי לגורם שממנו נאסף המידע הדיגיטלי.

142 במרחב הפיזי התחליף להעתקה דיגיטלית הוא צילום. כאשר מדובר במסמך כתוב, הצילום עשוי לספק תחליף סביר. כאשר מדובר במוצג פיזי שאינו מסמך, או כאשר מבקשים לאסוף ראיות מן המסמך כחפץ (לדוגמה טביעות אצבע, השוואת כתב יד, איסוף דנ"א), הצילום אינו מספק תחליף.

בכל הנוגע לזכות השימוש של הבעלים במידע, הפסד"פ, שמגלם ככלל תפישה פיזית באשר לראיות הדיגיטליות,<sup>143</sup> כולל הוראה המתייחסת לאפשרות למסירת העתק של המידע שנאסף תוך ארבעה ימים מיום התפיסה, על פי בקשת "אדם המשתמש במחשב שנתפס לפי הוראות חוק זה או שיש לו חומר מחשב במחשב כאמור".<sup>144</sup> ההוראה כוללת שני סייגים המגלמים התנאה על זכות השימוש של הבעלים במידע: חשש מפני שיבוש החקירה וחשש לביצוע עברה בעקבות מסירת ההעתק.<sup>145</sup> נראה אפוא כי הוראת הפסד"פ הזאת מגלמת התחשבות מסוימת בזכות השימוש של הבעלים במידע. עם זאת ההוראה מסויגת בתחולתה, היא תלויה בבקשה מצד מי שמשתמש במחשב שנתפס או מי שיש לו מידע האגור באותו מחשב (זה האחרון לא תמיד ידע על התפיסה של המחשב), ובכל מקרה היא מגיעה לאחר מעשה (ex post). ניתן לחשוב על עיגון זכות ההעתקה מראש (ex ante), כהוראה שתחול ברגע תפיסת המחשב, וניתן אף לחשוב על הוראה הפוכה מן הקבוע היום, שלפיה הרשות החוקרת תעתיק לרשותה את המידע שהיא מבקשת לאסוף מבלי לתפוס כלל את המחשב.

אשר לזכות לשלול מאחרים חשיפה אל המידע, הכוונה כאן – בהקשר של דיני איסוף הראיות – לא רק לשימור זכות השימוש במידע בידי מי שהמידע נאסף ממנו, אלא גם לשלילה מאחרים את עצם החשיפה אל המידע. משמע, שהתרופה בדמות מתן אפשרות העתקה למי שהמידע נאסף מרשותו אינה משרתת את הזכות הנדונה עתה. הזכות לשלול מאחרים חשיפה אל המידע רלוונטית לסודות עסקיים, שעיקר ההגנה עליהם מתבטאת בשלילת החשיפה של אחרים אליהם.<sup>146</sup> זאת להבדיל ממידע מוגן אחר, כגון זכות היוצרים, שהוא חשוף לאחרים, אולם ההגנה עליו מתבטאת למשל בהגבלת זכות השימוש ביצירה המורכבת מאותו מידע. בכל הנוגע לסודות עסקיים, הפגיעה בזכות לשלול מאחרים חשיפה אל המידע מתבטאת הן בעצם ההעתקה והעיון של הרשות החוקרת במידע זה והן באפשרות של צדדים נוספים (נחקרים אחרים) להיחשף אל המידע האמור בעקבות פעולת האיסוף.

143 כמפורט בפרק ד.ב.2..

144 סעיף 32א(א) לפסד"פ כפי שהוסף בתיקון מס' 12 משנת 2005. ודוק, הוראה זו של הפסד"פ מנוסחת בלשון קניינית, ותחולתה על כל המידע שנאסף בחקירה והשייך למבקש. זאת להבדיל מהוראת סעיף 74 לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב-1982 (להלן – חוק סדר הדין הפלילי), אשר מעניק זכות לעיון בחומר החקירה הרלוונטי לאישום רק בשלב המשפט ומכוח הזכות להליך הוגן.

145 סעיף 32א(ב) לפסד"פ. הכוונה בסייג של ביצוע עברה בעקבות מסירת ההעתק למצב שבו, למשל, כלול בחומר המחשב הנדון תוכן פדופילי, האסור בהחזקה. מסירתו של העתק מידע זה חזרה לרשות המבקש משמעה ביצוע עברה פלילית בחסות מימוש הזכות לקבלת ההעתק. עוד יש לשים לב שסעיף 32א(א) לפסד"פ קובע כי קצין משטרה יכול לדרוח את מימוש זכות ההעתקה מעת לעת עד ל-16 ימים, ולאחר מכן בית המשפט רשאי להאריך את מועד מימוש הזכות מעת לעת בהארכות שלא תעלינה על 15 יום כל פעם. לדיון קצר ביחס שבין סעיף 32א(א) לפסד"פ, הקובע את הזכות הקניינית, לבין סעיף 32א(ב) לפסד"פ, המסייג אותה, ראו ה"ת (שלום ת"א) 35320-09-12 משטרת ישראל נ' הלוי (פורסם בנבו, 27.12.2012). באותו מקרה קבע בית המשפט כי על המשטרה להאיץ את קצב בדיקת המחשבים שנתפסו מידי המבקש על מנת להשלים את מיון הקבצים המתרים בהעתקה, לשיטתה, לעומת הקבצים האסורים בהעתקה.

146 מובן שגם מידע אישי מוגן-פרטיות מגלם זכות לשלול מאחרים גישה אליו כחלק משליטתו העצמית של אדם על המידע על אודותיו. הנה לפנינו חפיפה מסוימת בין פרטיות לבין קניין, מבחינת המשמעות האופרטיבית של הזכות על סוגי מידע מסוימים, גם אם המקור הנורמטיבי שונה.



בכל הנוגע לזכות לשלול מאחרים חשיפה אל המידע אמנה ארבעה שלבים שונים של ההליך הפלילי, על פי סדרם הכרונולוגי, שבהם קיים פוטנציאל חשיפה של המידע לאחרים: השלב הראשון הוא שלב החשיפה של הרשות החוקרת אל המידע. מניעת החשיפה האמורה משמעה למעשה הטלת מעין חיסיון ראייתי.<sup>147</sup> מבחינת בעל המידע הסודי, הפקעת הבלעדיות במידע על-ידי הרשות החוקרת מסוכנת הן במובן של חשיפת אנשי הרשות החוקרת עצמם והן במובן של פוטנציאל זליגת המידע הסודי מכיוון הרשות החוקרת לגורמים נוספים. כאשר בעל המידע הסודי הוא יעד פעולת האיסוף, וכאשר בעל המידע הוא בעל החיסיון, מתאפשר לשקול את עניינו מבעוד מועד (ex ante), טרם ביצוע פעולת האיסוף עצמה. עם זאת, כאשר המידע הקשור בבעל המידע הסודי, הטוען את אותה טענת חיסיון בפני הרשות החוקרת, מתגלה אגב אורחא, תוך כדי ביצוע פעולת איסוף כלפי יעד אחר, קיים קושי מובנה בשקילת עניינו מבעוד מועד, ומתחייבת קביעת מנגנון הגנה תוך כדי ביצוע פעולת האיסוף על מנת לאזן ככל הניתן את הפגיעה בזכות. במשפט הישראלי פותחו מנגנוני הגנה כאלה בנוגע לתכנים הנהנים מחיסיון ראייתי.<sup>148</sup>

147 החסינות הראייתיים בדין הישראלי מוסדרים בסעיפים 47–51 לפקודת הראיות [נוסח חדש], התשל"א–1971 (להלן – פקודת הראיות), וכוללים את הזכות לאי-הפללה עצמית ואת הזכות לחסינות של בעלי מקצוע מסוימים: עורך דין, רופא, פסיכולוג, עובד סוציאלי וכהן דת. כמו כן, בעלי מקצועות נוספים זכו להכרה פסיקתית, גם אם לא בחקיקה, ובראשם העיתונאים והבנקאים. ראו ב"ש 298/86 ציטרין נ' בית הדין המשמעתי של לשכת עורכי הדין במחוז תל אביב, פ"ד מא(2) 337 (1987) (לעניין חיסיון עיתונאי); רע"א 1917/92 סקולר נ' גרבי, פ"ד מז(5) 764 (1993) (לעניין חיסיון בנקאי–לקוח). על פי סעיף 52 לפקודת הראיות, כשהחסינות מוחלים הם חוסמים, אפילו מפני המדינה, את האפשרות להיחשף ולהשתמש במידע. זו לשון הסעיף: "הוראות פרק זה [פרק החסינות בפקודת הראיות – הערה שלי, ח"ו] יחולו הן על מסירת ראיות בפני בית משפט ובית דין והן על מסירתן בפני רשות, גוף או אדם המוסמכים על פי הדין לגבות ראיות...". נובע מן הסעיף הזה כי אם מדובר בבעל מקצוע הנהנה מחיסיון מלא (עורך דין וכהן דת), הרי שהרשות החוקרת מחויבת להימנע מפעולות איסוף כלפיו במישרין, אלא אם הוא מעורב בעצמו בעברה (שאו החיסיון אינו חל עליו, שכן אין מדובר בחסינות אישית של בעל המקצוע אלא בחיסיון מקצועי). אם מדובר בבעל מקצוע הנהנה מחיסיון יחסי (רופא, פסיכולוג, עובד סוציאלי, עיתונאי), הרי שהרשות החוקרת אינה מנועה מלבצע פעולת איסוף כלפיו, ככל שבית המשפט יאשר את הדבר.

בחרתי להציג כאן את דיני החסינות במשקפיים "קנייניים", אולם ניתן בהחלט להציג את עניינם במסגרת נפרדת של הזכות לחופש העיסוק של הנהנה מהחיסיון, הזכות לפרטיות של בעל החיסיון (ככל שמדובר בחיסיון שמגלם היבטי פרטיות מובהקים, כגון חיסיון רופא–מטופל או פסיכולוג–מטופל), חופש העיתונות (כשמדובר בחיסיון עיתונאי), הזכות להליך הוגן (כשמדובר בחיסיון עורך דין–לקוח). אמנה שני מנגנונים מעין אלה: האחד, כאשר מסמכים משפטיים שהוחלפו בין עורך דין לבין לקוח נמצאו במחשבו של הלקוח (הלקוח היה יעד החדירה לחומר המחשב ולא עורך הדין). ראו עניין היינץ, לעיל ה"ש 123. בית המשפט קבע כי גם אם החומרים הנטענים נתפסים ברשותו של הלקוח ולא ברשותו של עורך הדין, הם עדיין יוכלו להיחשב חסויים. בית המשפט הכיר בכך שכיום טיטות ומסמכי הכנה לקראת משפט מועברים בדואר אלקטרוני בין עורך הדין לבין לקוחו, וכך נוצרים למסמכים עותקים – הן במשרד עורך הדין והן ברשות הלקוח; השני, כאשר מתבצעת האזנת סתר ובאקראי נקלטות שיחות של יעד ההאזנה עם בעל מקצוע הנהנה מחיסיון מקצועי. לעניין זה ראו ע"פ 5135/11 מדינת ישראל נ' ברקו (פורסם בנבו, 31.5.2012). כן ראו דין וחשבון צוות הבדיקה בנושא האזנות הסתר, התשס"ה–2005, פרק ה(8) (דוח לבנת משיח); דין וחשבון ועדת החקירה הפרלמנטרית בעניין האזנות סתר, התשס"ט–2009, בעמ' 23–25; הצעת חוק האזנת סתר (תיקון מס' 6), התשס"ט–2009, ה"ח הממשלה .455

השלב השני הוא שלב החשיפה של צדדים שלישיים הטוענים לזכויות במידע או בחלקו ומבקשים להעתיקו לרשותם. הכוונה כאן לגורמים הטוענים כי במחשב שתפסה הרשות החוקרת אגור חומר ששייך להם והם מבקשים להעתיקו לרשותם.<sup>149</sup> היות ששרת אחד, למשל, יכול לכלול חומרים של כמה גורמים שונים, אף כאלה שאין ביניהם כל מגע (למשל כשמדובר בשרת של ספקית שירותי אירוח או אחסון), הרי שעלול להיווצר מצב שבו צד שלישי כאמור ייחשף למידע מוגן של אחרים, וזאת במסגרת בקשתו לממש את זכותו להעתיק את המידע השייך לו. השלב השלישי הוא שלב החשיפה של חשודים/נאשמים אחרים במסגרת זכותם לקבלת חומר החקירה שנאסף. עם הגשת כתב אישום, ולמעשה במידה מסוימת עוד קודם לכן עם ההודעה על האפשרות שיוגש כתב אישום נגד חשוד, בכפוף לשימוע,<sup>150</sup> קמה זכות לעיון בחומר החקירה שנאסף, כאשר בגדר "חומר החקירה" כל החומר הנחשב כבעל פוטנציאל רלוונטיות להוכחת האישום או להפרכתו. מזכות עיון נגזרת גם זכות העתקה של המידע.<sup>151</sup> ככל שהמידע הממוחשב המוגן קניינית הוא חלק מחומר החקירה הרלוונטי להוכחת האישום, וככל שבעל המידע אינו החשוד/הנאשם, הרי שעשוי להיווצר מתקל חוקתי משולש:<sup>152</sup> מצד אחד טוען בעל המידע לזכות קניינית לשלול מאחרים חשיפה אל המידע; מצד שני טוען החשוד/הנאשם לפגיעה בזכותו להליך הוגן אלמלא ייחשף אל המידע האמור במסגרת ניהול הגנתו; מצד שלישי מחויבת המדינה לאפשר עיון במידע, שאם לא כן לא תוכל להשתמש בו במסגרת המשפט (אם מדובר בראיית תביעה) או שעלול האישום להתבטל (אם מדובר בראיית הגנה פוטנציאלית).<sup>153</sup> אפשרות מסוימת ל"ריכוך" הפגיעה הקניינית קיימת במשפט הישראלי בדמות האפשרות להעניק זכות עיון במידע שבמחלוקת מבלי להעניק זכות העתקה לאותו מידע. זאת על בסיס הקביעה השיפוטית כי זכות ההעתקה, אף שהיא מצוינת בחוק סדר הדין הפלילי, היא זכות משנית לזכות המרכזית – זכות העיון – ועיקרה עניין שבנוחות.<sup>154</sup>

השלב הרביעי הוא שלב החשיפה אל המידע כשהוא מוגש לבית המשפט כראיה. החשיפה היא הן לנוכחים באולם בית המשפט והן לציבור בכללותו, ככל שההליך המשפטי מפורסם. עקרון פומביות הדין קובע כללים של דלתיים פתוחות בבית המשפט והיתר לפרסום מהלך

149 סעיף 32א(א) לפסד"פ מעניק זכות העתקה לא רק למי שהמחשב נתפס מרשותו, אלא לכל מי שטוען "...שיש לו חומר מחשב במחשב".

150 אמנם סעיף 60א לחוק סדר הדין הפלילי, המעגן את זכות השימוע לפני הגשת כתב אישום בעברות פשע, אינו מונה את זכות העיון, כולו או חלקו, בחומר החקירה, אולם ראו "טיעון לפני הגשת כתב אישום פלילי (שימוע)" הנחיות היועץ המשפטי לממשלה 4.3001 (התשס"ט), סעיף 7; בג"ץ 2678/07 קצב נ' היועץ המשפטי לממשלה (פורסם בנבו, 23.4.2007).

151 ראו סעיף 74 לחוק סדר הדין הפלילי.

152 מקרה כזה אירע בעניין חברת ס', לעיל ה"ש 5.

153 ראו את סעיף 77א(א) לחוק סדר הדין הפלילי, הקובע "סנקצייה" שלפיה ראייה שלא הוענקה לגביה זכות עיון – התביעה לא תוכל להגיש לבית המשפט. אשר לאי-מימוש זכות העיון באופן הפוגע בחשיפה לראיות הגנה, הרי שבמקרה כזה ה"סנקצייה" על אי-מימוש זכות העיון עשויה להיות זיכוי מחמת הגנה מן הצדק. ראו ת"פ (מחוזי ת"א) 40279/08 מדינת ישראל נ' לדר, בפס' 7–21 (פורסם בנבו, 22.8.2010).

154 ראו בש"פ 6640/06 קרוכמל נ' מדינת ישראל (פורסם בנבו, 7.9.2006). מנגנון "ריכוך" זה, של עיון ללא העתקה, יכול לשמש גם לריכוך הפגיעה בפרטיות במסגרת ההליך הפלילי. ראו למשל סעיף 5ב לחוק לתיקון דיני הראיות (הגנת ילדים), התשט"ו–1955; בש"פ 6022/96 מדינת ישראל נ' מזור, פ"ד (ג) 686 (1996); בש"פ 6695/11 מדינת ישראל נ' פלוני (פורסם בנבו, 27.9.2011).

המשפט. החריגים הם סגירת הדלתיים ואיסור הפרסום. הגנה על סוד מסחרי מוכרת כעילה לסגירת דלתות בית המשפט.<sup>155</sup> בנוסף, אם דלתות בית המשפט נסגרו, בררת המחדל מתהפכת מהיתר פרסום ההליך המשפטי לאיסור פרסום ההליך.<sup>156</sup>

לסיכום, עמדתי על טיבה של זכות הקניין באשר למידע הדיגיטלי הנאסף במסגרת חקירה פלילית במרחב הקיברנטי. התפישה הפיזית מביאה להחלה פשטנית של זכות הקניין בעניינינו, שכן היא מובילה להתמקדות במחשב כחפץ ולא במידע האגור בו. לכאורה, התפישה הפשטנית ה"פיזית" של זכות הקניין בהקשרנו יכולה להוביל לתוצאה משפטית של הכול-או-לא-כלום: או הגנה מוחלטת מפני תפיסת המחשב ועיון במידע המצוי בו, או היתר לתפוס את כלל המידע ולעיין בו.<sup>157</sup> לכאורה, יכולה לנבוע תוצאה של הרחבת ההגנה. אולם בפועל נראה כי בשל האינטרס החקירתי ו"מחיר" הדחייה המלאה של בקשתה של הרשות החוקרת לאיסוף המידע הדרוש לה לחקירה, תהא הנטייה להתיר את תפיסתו של המחשב ועיון בפועל בכלל המידע. על כן נכון יותר לתפוש בהקשרנו את זכות הקניין כזכות ה"לובשת" מובן של שימוש במידע בידי בעליו וכן מובן אפשרי של מניעה מאחרים מלהשתמש במידע. הצגתי את סוגי המידע המוגנים באמצעות זכות הקניין ולא דווקא באמצעות זכויות אחרות, כגון הזכות לפרטיות. מכאן שיש חשיבות פרקטית להכרה עצמאית בזכות הקניין, נוסף על החשיבות העיונית הברורה מאליה. כן הצגתי מנגנונים פרוצדורליים שונים בדין הישראלי הקיים, אשר ניתן להשתמש בהם על מנת לשרת הגנות על זכות הקניין. מנגנונים אלה מאוחרים לרגע המכונן של הפעלתה של סמכות איסוף הראיות. עם זאת יש בהם כדי לרכך את עצמת הפגיעה בזכות הקניין. על כל פנים, ראוי שהפגיעה בזכות הקניין תישקל כבר בשלב ההסמכה של הרשות החוקרת לאסוף מידע. זאת משום שלזכות הקניין, בעיקר ההיבט של הזכות לשלול מאחרים – לרבות הרשות החוקרת – חשיפה אל המידע יכולה להיות חשיבות כבר בעצם ההחלטה אם לאשר לרשות החוקרת להיחשף אל המידע אם לאו. בנוסף, התחשבות בזכות הקניין יכולה להוביל מראש להסמכת הרשות החוקרת להעתיק מידע הדרוש לה בלבד או לעיין בו, במקום "לתפוס" את המידע ולמסור העתק ממנו לידי מי שממנו נאסף.

### 3. חופש העיסוק

המידע העסקי הפך לכלי עבודה ממדרגה ראשונה. ככל שהמידע נשלל מאת מחזיקו במסגרת החקירה הפלילית, עלולה להיגרם פגיעה קשה בחופש העיסוק. ניכר כי הפסד פ"פ ניסה לתת ביטוי לזכות לחופש העיסוק, ועל כן נקבע כי "מחשב מוסדי" (של המדינה, רשות מקומית, עסק או מי שמספק שירות לציבור)<sup>158</sup> יוכל להיתפס ל-48 שעות בלבד, ולאחר מכן חובה להביא את ענייניו בפני שופט על מנת שיכריע אם להורות על הארכת התפיסה מעבר לפרק זמן זה.<sup>159</sup> הוראה זו מגלמת תפישה פיזית מובהקת, באשר הדגש הוא על המחשב המוסדי כחפץ בר-תפיסה ולא על

155 ראו סעיף 68(ב)(8) לחוק בתי המשפט [נוסח משולב], התשמ"ד-1984 (להלן – חוק בתי המשפט).

156 ראו סעיף 70(א) לחוק בתי המשפט.

157 ראו עוד לעיל בפרק ד.ג.2..

158 לעניין הגדרת "מחשב מוסדי", מפנה סעיף 32(ב) לפסד"פ לסעיף 35 לפקודת הראיות, המגדיר "מוסד": "המדינה, רשות מקומית, עסק או כל מי שמספק שירות לציבור".

159 סעיף 32(ב) לפסד"פ.

המידע העסקי. בהמשך להבחנה המושגית שהצעתי בהקשר של זכות הקניין בין זכות השימוש של הבעלים במידע לבין הזכות למנוע מאחרים חשיפה אל המידע, נראה כי חופש העיסוק מתמקד בזכות הראשונה. במילים אחרות, העתקת המידע שנאסף ומסירתו לידי מי שממנו נאסף, בהקדם האפשרי – תוכל לרכך במידה ניכרת את הפגיעה בחופש העיסוק. שאלת עצם התפיסה, והארכת התפיסה, של המחשב המוסדי המקורי, אין בה כדי להלום במדויק את התכלית של הפחתת הפגיעה בחופש העיסוק.

נקודה נוספת הראויה לציון בהקשר של חופש העיסוק קשורה לתכונה אחרת של הראיות הדיגיטליות במרחב הקיברנטי, וזו התכונה של המידע כמבוזר ומתווך בידי ספקיות שירות. תכונה זו הפכה את ספקיות השירות ל"שחקניות" מרכזיות במסגרת חקירה פלילית במרחב הסייבר היות שהן בבחינת צומתי מידע.<sup>160</sup> פעולות איסוף שונות שמניתי לעיל מהייכות בראש ובראשונה את ספקיות השירות, והפגיעה המגולמת בהן אינה רק בחשוד אלא במידה רבה גם בחופש העיסוק של ספקיות השירות.<sup>161</sup> מובן שספקיות שירות מסוגים שונים קיימות גם במרחב הפיזי, וספקיות אלה יכולות לקבל צווים להמצאת חומרים בשביל הרשות החוקרת, אולם במרחב הקיברנטי מרכזיותן של ספקיות השירות היא חלק אינהרנטי ממבנה הרשת ומאופן תפקודה. על כן החקירה בסביבה הקיברנטית מייצרת הבדל איכותי מבחינת הפגיעה בחופש העיסוק של ספקיות השירות. על העצמת הפגיעה האמורה להישקל בעת הסמכת הרשות החוקרת לביצוע פעולות איסוף ראיות דיגיטליות במרחב הסייבר באמצעות ספקיות השירות.

#### 4. הזכות לאנונימיות או לפסידונימיות ברשת

משתמשי רשת רבים לובשים זהויות וירטואליות קבועות או משתנות (פסידונימיות). משתמשים אחרים ברשת לובשים "אנטי-זהות", קרי הם מבקשים לנצל את יתרונות האנונימיות המוחלטת. כל אלה גם יחד הן פרקטיקות של הסוואת זהות. אמנם גם במרחב הפיזי ניתן להסוות זהות, אולם ארכיטקטורת המרחב הקיברנטי פתחה מרחב של אפשרויות להשיג הסוואה יעילה של הזהות בקלות, בחינם, במסגרות מגוונות ועשירות.<sup>162</sup> אמצעי הסוואת הזהות במרחב הסייבר מאפשרים להקשות מאוד על פיענוח עברות פליליות ברשת, אולם ברמה הכללית, לא בהקשר של ניצול לרעה בידי גורמים עברייניים, ניתן לדבר על זכות לאנונימיות/פסידונימיות, בין זכות עצמאית ובין זכות הנגזרת מזכויות אחרות, כפי שאפרט להלן. בזכות האנונימיות או הפסידונימיות מתאפשר למשתמש המחשב והאינטרנט לשלוט במידע על אודותיו ובאופן הצגתו העצמית; כן מתאפשר ביטוי חופשי, בייחוד לקבוצות אוכלוסייה מוחלשות ולאנשים המבקשים להתבטא כנגד הקונצנזוס המשטר-חברתי שבסביבתם; האנונימיות/הפסידונימיות מעודדת השתתפות במנגנונים קהילתיים והרחבת המעגלים החברתיים ומאפשרת שכלול של

160 ראו לעיל בפרק ב.ה.1..

161 כן אפשר שתתעורר טענה לפגיעה בזכויות קנייניות של ספקיות השירות עצמן אשר עשויות להיות מופרות בשל דרישת רשויות החקירה: זכות לנהל את עסקן כרצונן וזכות יוצרים או סוד מסחרי מוגנים שלהן. ראו לעיל טקסט לה"ש 15.

162 בפרק ב.ג.1. סקרתי אמצעים טכנולוגיים שונים המאפשרים השגת אנונימיות או שמירה על זהות פסידונימית מבלי לחשוף את זהותו האמתית של משתמש האינטרנט.

עושר ההתנסות האישית של אדם.<sup>163</sup> האנונימיות/פסידונימיות היא, פעמים רבות, הכוח המניע חלק ניכר מהשיח באתרים החברתיים, בבלוגים ובתגובות. הזכות לאנונימיות/פסידונימיות יונקת את חיותה משני מקורות משפטיים מעורבים: חופש הביטוי<sup>164</sup> והזכות לפרטיות ברשת.<sup>165</sup> אלעד אורג אף טען כי הסוואת הזהות ברשת היא אחד

163 ראו אלעד אורג זכות לזהות אינפורמטיבית: עקרון משפטי חדש להגנת קיומה של זהות אינפורמטיבית ויישומו בסביבת מידע מודרני 116–143 (חיבור לשם קבלת תואר "דוקטור למשפטים", אוניברסיטת תל-אביב, 2008). כן ראו יאיר עמיחי-המבורגר ואורן פרו "אנונימיות ואינטראקטיביות באינטרנט – הזכות לפרטיות כמושג רב-ממדי" פרטיות בעידן של שינוי 201, 209–212 (תהילה שוורץ אלטשולר עורכת, 2012). המחברים טענו כי האנונימיות באינטרנט יש בה, מצד אחד, כדי לשחרר אלמנטים שליליים באישיותם של משתמשי הרשת (בדמות התנהגות תוקפנית ואף עבריינית או סוטה), ומצד שני יש בה כדי לשחרר אלמנטים חיוביים באישיותם של משתמשי הרשת (בדמות התנהגות פרו-חברתית ואלטרואיסטית).

164 האתוס המקורי של האינטרנט, לאחר שנפתח לשימוש עולמי כללי, הציג את הרשת כמדיום חופשי, המאפשר לכל אחד להיות דובר, בזול, בלי צורך במערך של הפקה והפצה כבאמצעי מדיה אחרים. ראו קרניאל "חופש הביטוי באינטרנט" עלי משפט א 163, 185–192 (2000); Yuval Karniel & Haim Wisnonsky, *Pornography, Community and the Internet – Freedom of Speech and Obscenity on the Internet*, 30 RUTGERS COMP. & TECH. L. J. 105, 133–140 (2004). משלב מסוים של התפתחות האינטרנט בחרה המדינה להתערב, במישרין או באמצעות הטלת אחריות על ספקי שירות, בתכנים ובגישה אליהם והביאה לשבירת התמונה האידיאלית לכאורה הזאת. ראו למשל DIANE ROWLAND & ELIZABETH MACDONALD, *INFORMATION TECHNOLOGY LAW* 455–487 (3<sup>rd</sup> ed., 2005). כן ראו ניבה אלקין-קורן "המתווכים החדשים 'בכיכר השוק' הווירטואלית" משפט וממשל 365, 377–390 (2002). בארצות הברית חלק מניסיונות ההתערבות של המדינה בתכנים נדונו לכישלון ודווקא אשררו את הזכות לחופש ביטוי באינטרנט. כך למשל ניתן למנות את שורת ניסיונות החקיקה בארצות הברית שביקשו להגן על קטינים מפני חשיפה לתכנים אסורים באינטרנט. בשנת 1996 נחקק ה-CDA (Communications Decency Act). בית המשפט העליון פסל את הגדרות החוק באשר לתכנים האסורים בפרסום באינטרנט, בהיותם עמומים ורחבים מדי באופן הסותר את התיקון הראשון לחוקה. בשנת 1998 נחקק ה-COPA (Child Online Protection Act). החוק נועד לרשת את ה-CDA שכשל במבחנו של בית המשפט העליון, אולם גם את החוק הזה ביטל בית המשפט. לפירוט ההליכים בנוגע לשני חוקים אלה, ראו לעיל בפרק ב בה"ש 127. כן אזכיר את ה-CPPA (Child Pornography Prevention Act) משנת 1996. ה-CPPA קודד כ-18 U.S.C. § 2256. החוק הרחיב את ההגדרה של פורנוגרפיית קטינים לצורך הגנה מפני פרסומים פדופיליים באינטרנט. לפיכך נקבע כי גם הדמיית מחשב של קטין המעורב, או הנחזה להיות מעורב, בפעילות מינית תיאסר. כמו כן כל תמונה של קטין היוצרת את הרושם כי הוא מעורב בפעילות מינית תיאסר בהפצה. בית המשפט העליון האמריקני, ברוב דעות, פסק כי הרחבות אלה של הגדרת פורנוגרפיית הקטינים מופרזות ופוגעות פגיעה לא מידתית בחופש הביטוי. ראו *Aschcroft v. Free Speech Coalition*, 535 U.S. 234 (2002). נקבע כי המחזה רומיאו ויוליה, הסרט "אמריקן בינטי" ועוד עלולים לעלות כדי "פורנוגרפיית קטינים" על פי הגדרתו של ה-CPPA.

מן הניסיון האמריקני נמצאנו למדים כי חופש הביטוי באינטרנט עודו זוכה להכרה ולמשקל ניכרים. כך גם באשר לדין הישראלי. ראו למשל קרין ברזילי-נהון וגד ברזילי "חופש הביטוי המעשי והמדומיין באינטרנט: על בטלותה והולדתה המחודשת של הצנזורה" שקט, מדברים!: התרבות המשפטית של חופש הביטוי בישראל 483 (מיכאל בירנהק עורך, 2006). ראו גם פסיקת המשנה לנשיאה ריבלין ברע"א 4447/07 מור נ' ברק אי.טי.סי [1995] החברה לשירותי בוק בינלאומיים בע"מ, פ"ד סג(3) 664, בפס" 14 לפסק דינו של המשנה לנשיאה ריבלין (2010), שבה הוא שב על הרטוריקה המציגה את האינטרנט כ"כיכר העיר" החדשה, הפתוחה לכול והחסומה מפני התערבות שלטונית. התפישה המשפטית האמריקנית היא כי אנונימיות נגזרת מחופש הביטוי, וראו *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). לתפישה זו ביטויים מסוימים בפסיקה הישראלית, וראו

מביטוייה של זכות עצמאית, שאותה כינה "זכות לזהות אינפורמטיבית"<sup>166</sup>. הסוואת הזהות באמצעות אנונימיות/פסידונומיות נובעת ממקורות אלה, ובה בעת היא משרתת את הזכויות הללו ומאשררת אותן במרחב הסייבר. האנונימיות/הפסידונומיות ברשת אף משרתת זכויות חוקתיות אחרות כשוויון וחופש ההתאגדות, דהיינו היא מהווה אמצעי שדרכו אפשר להגשים את הזכות לשוויון ולהתאגדות הגשמה מיטבית.<sup>167</sup>

קיבול משליכה התפישה הפיזית על הזכות לאנונימיות/פסידונומיות? ובכן, התפישה הפיזית מחמצת כליל את תכונתו של המידע הדיגיטלי כמאפשר הסוואת זהות.<sup>168</sup> הטכנולוגיה המאפשרת את הסוואת הזהות מחייבת את המשפט לבחון אם להכיר בזכות לשמר את אותה הסוואת זהות על מנת לשמר את הערכים החיוביים, שמנתי לעיל, אשר הטכנולוגיה הזאת מבקשת לקדם. שיח הזכויות החוקתיות בהקשר של חקירה פלילית במרחב הסייבר אינו מורגל לדין במשמעותה ובמשקלה של הזכות. האנונימיות/פסידונומיות היא כאמור חלק בלתי נפרד מפרקטיקת השימוש ברשת. איסוף ראיות דיגיטליות כדי לחשוף זהות פיזית של משתמש מסוים פוגע במאפיין זה של השימוש ברשת. היות שהמידע הדיגיטלי ניתן לאגירה (ואכן נאגר בפועל), מתווך בידי ספקיות שירות שונות ונפרד מאת מי שהמידע הוא על אודותיו, הרי שיכולות איסוף המידע, אשר בכוחו לפגוע בזכות לאנונימיות/פסידונומיות – גבוהות. חלק מפעולות האיסוף שנדרשו לעיל בפרק הקודם, כגון שימור מידע דרך קבע (Retention), יצירת תשתית טכנולוגית שתאפשר לרשות לאסוף ראיות דיגיטליות או הוראות לספקיות שירות לפיצוח הצפנות או הגנת סמאות, מסכנות במישורן את הזכות לאנונימיות/פסידונומיות, שכן הן מכוונות במידה רבה – גם במחיר של פגיעה עודפת גורפת – להתגברות על יכולות הסוואת הזהות ברשת. קיימת טעמי חשיבות בהכרה בזכות לאנונימיות/פסידונומיות ברשת כזכות עצמאית העומדת על שתי רגליה, או לחלופין כזכות החופפת ישירות חלק מזכות חוקתית אחרת, אך לא כזכות מכשירנית, או זכות מסדר שני, המשרתת זכויות וחירויות אחרות המוגנות חוקתית.<sup>169</sup>

עניין מור, שם, בפס' 11 לפסק דינו של המשנה לנשיאה ריבלין. לדין בחופש הביטוי כמקור לאנונימיות ברשת, ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 306–311.

165 על מקורה של הזכות לאנונימיות/פסידונומיות מהזכות לפרטיות, ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 318–33; מיכאל בירנהק "חשיפת גולשים אנונימיים ברשת" חוקים ב 51, 89–94 (2010). כן ראו עניין מור, שם, בפס' 16 לפסק דינו של המשנה לנשיאה ריבלין; Gavison, לעיל ה"ש 79, בעמ' 428–429. לפי עמדת הפרטיות כגישה, כניסוחה של רות גביוון, אנונימיות נגזרת במישורן מהזכות לפרטיות. על פי עמדת הפרטיות כשליטה, שבה מצדד בירנהק, האנונימיות נגזרת מההצדקות הפרטיקולריות של הזכות לפרטיות במעגלים השונים של השליטה. ראו גם את פסיקתו של בית המשפט העליון הקנדי, אשר קבע כי בקשה של המשטרה הקנדית לחשיפת פרטי זיהוי של משתמש, על סמך נתוני ה-IP שלו, פוגעת בזכותו לפרטיות, במובן של אנונימיות: R. v. Spencer, [2014] SCC 43 (Ca.).

166 ראו אורג, לעיל ה"ש 163, ולעניין היחס בין אנונימיות וכן פסידונומיות (שם-עט) לבין כינון זהות אינפורמטיבית ראו בפרט עמ' 123–143.

167 ראו בירנהק, מרחב פרטי, לעיל ה"ש 8, בעמ' 315–318.

168 ראו פרק ד, טקסט להערה 93.

169 הכוונה בחפיפה חלקית לזכות אחרת היא שהאנונימיות תיתפש כחלק ממובני הזכות לפרטיות ולא כזכות העומדת על שתי רגליה בעצמה ולא כאמצעי להשגת זכות חוקתית מוגנת (פרטיות או חופש ביטוי). אציין כי הרטוריקה של בית המשפט העליון, שהכיר – בהקשר של תביעות לשון הרע ובהקשר של תביעה בגין הפרת זכויות יוצרים – בזכות לאנונימיות, מגלמת תפישה מכשירנית של הזכות ככזו

התבוננות על האנונימיות/פסידונימיות כזכות מכשירנית בלבד תוביל לגישה שלפיה הפגיעה בזכות החוקתית, המגולמת בפעולת איסוף מסוימת החושפת זהות של משתמש ברשת – אינה אלא פגיעה עקיפה בלבד. לעומת זאת התבוננות על הזכות לאנונימיות/פסידונימיות כזכות עצמאית תוביל לגישה שלפיה פעולת איסוף החושפת זהות של משתמש ברשת היא פגיעה ישירה בזכות חוקתית. אמחיש את ההבחנה בין מעמדה של זכות הנפגעת במישורין לבין מעמדה של זכות הנפגעת בעקיפין בלבד: נניח שהרשות החוקרת מבצעת שתי פעולות איסוף – בראשונה היא מבקשת לאסוף תוכן תכתובות דוא"ל של חשוד מסוים מאת ספקית שירותי הדוא"ל; בשנייה היא מבקשת לקבל לידיה נתוני IP של משתמש אינטרנט מסוים במסגרת חקירה פלילית בעברה כלשהי. בדוגמה הראשונה ניתן להצביע על פגיעה ישירה בסוד שיחו של הנחקר, כאשר "סוד שיח" הוא אחד ממובניה של הזכות לפרטיות. בדוגמה השנייה מדובר בפעולה שיש בה פוטנציאל לחשיפת זהות של משתמש אינטרנט. אם נתבונן על הזכות לאנונימיות/פסידונימיות כזכות מכשירנית, הרי שעצם הבקשה לחשיפת הזהות באמצעות נתוני ה-IP תגלם פגיעה עקיפה בלבד בזכות שאותה משרתת האנונימיות/פסידונימיות (פרטיות, ביטוי, שוויון או התאגדות, תלוי בנסיבות). משמעות הפגיעה העקיפה היא שפעולת האיסוף הנדונה תשפיע על עתידן של הזכויות העקיפות שאותן משרתת הסוואת הזהות. לעומת זאת אם נתבונן על האנונימיות/פסידונימיות כזכות עצמאית או כזכות החופפת חלק מהזכות לפרטיות והנפגעת במישורין מהפעולה המבוקשת, הרי שהפגיעה באמצעות חשיפת נתוני ה-IP תהא פגיעה ישירה, עצמאית ונפרדת בזכות מוגנת. במילים אחרות, פגיעה ישירה בזכות משמעה פגיעה המתקיימת בהווה, ואילו הפגיעה העקיפה במובנה כפי שהדגמתי משמעה פגיעה עתידית בזכות העקיפה שאותה משרתת האנונימיות/פסידונימיות. פגיעה עתידית שכזאת היא, מעצם הגדרתה, ערטילאית. מטבע הדברים, פגיעה ערטילאית קשה לשקלול ולאיוון במקרה קונקרטי יותר מפגיעה ישירה, וכך, מבחינה מהותית יש חשש שהאיוון החוקתי הראוי יוחמץ.

## 5. הזכות להליך הוגן

הזכות להליך משפטי הוגן זוכה למעמד של זכות יסוד, הגם שבמשפט הישראלי אינה נקובה במפורש בחוק יסוד.<sup>170</sup> העמדה המקובלת היא שהזכות להליך הוגן נגזרת מחוק-יסוד: כבוד האדם וחירותו.<sup>171</sup> הזכות להליך הוגן מגלמת אינטרס פרטי של החשוד/הנאשם, אך בה בעת

שנועדה לקדם את חופש הביטוי ואת השמירה על הפרטיות. ראו פסק דינו של המשנה לנשיאה ריבלין בעניין מור, לעיל ה"ש 164; כן ראו עניין ברוקרטוב, לעיל ה"ש 75, בעמ' 11.

170 הזכות להליך הוגן הייתה אמורה להופיע במפורש בחוק-יסוד: זכויות במשפט. שלושה נוסחים של חוק היסוד המוצע פורסמו (ראו הצעת חוק-יסוד: זכויות במשפט, התשנ"ד-1994, ה"ח התשנ"ד 100, 324, 335), אלא שהליך החקיקה לא נשא פרי.

171 בג"ץ 11339/05 מדינת ישראל נ' בית-המשפט המחוזי בבאר-שבע, פ"ד סא(3) 93, 124-128 (2006). על פי אהרן ברק, הזכות להליך הוגן נגזרת מ"כבוד האדם". ראו אהרן ברק פרשנות במשפט, כרך ג, פרשנות חוקתית 431-432 (1994); אהרן ברק "כבוד האדם כזכות חוקתית" הפרקליט מא(ג) 271, 280-281 (1994). לאימוץ עמדה זו בפסיקת בית המשפט העליון, ראו ע"פ 9956/05 שי נ' מדינת ישראל, פ"ד סג(2) 742 (2009). על פי גרוס, זכות זו נגזרת דווקא מן הזכות לחירות הנקובה בחוק-יסוד: כבוד האדם וחירותו. ראו עמנואל גרוס "הזכויות הדיניות של החשוד או הנאשם על פי חוק יסוד: כבוד האדם וחירותו" מחקרי משפט יג 155, 169-170 (1996). לגישה דומה, ראו גם מ"ח

היא מגלמת גם אינטרס ציבורי כללי בקיומו של הליך חקירתי ומשפטי ראוי. למעשה אין מדובר בזכות קונקרטית מצומצמת כי אם באגד של זכויות, כגון זכות לקבלת חומר חקירה, זכות לחקירה נגדית, זכות לייצוג הולם וזכות טיעון בהליך אדוורסרי.<sup>172</sup> חלק מן הזכויות הללו רלוונטיות לשלב המשפט בלבד וחלקן לשלב החקירה. בשלב החקירה נפגעת זכות הייצוג וזכות הטיעון פגיעה אינהרנטית, שכן מרבית הפעולות הפוגעניות של הרשות החוקרת מתבצעות מכוח הסמכה שיפוטית במעמד צד אחד (ex parte) בלבד, או בהסמכה מנהלית בלבד. לגורמים המושפעים מפעולת האיסוף, ובראשם יעד הפעולה, אין מעמד לפני ההחלטה אם לאשר את הפעולה אם לאו, ומכאן שיכולה להיגזר חובה על הרשות החוקרת ועל בית המשפט לשקול את שיקולי ההגנה (השופט או בעל הסמכות המנהלית כ"סנגור ממונה לשעה").

בהקשרנו יש שני היבטים של הזכות להליך הוגן הייחודיים לאיסוף ראיות דיגיטליות בחקירה פלילית במרחב הסייבר: האחד, החשש המיוחד לפגיעה במהימנות הראיה הדיגיטלית; השני, הצורך בשקיפות פעולתה של הרשות החוקרת. שני היבטים אלה של הזכות להליך הוגן עשויים להביא להטלת חובות קורלטיביות על הרשות החוקרת, כפי שאפרט.

### חשש לפגיעה במהימנות הראיה הדיגיטלית

חומר מחשב נתון בסיכון רב לעיוות או לשינוי לא מכוונים. המידע הדיגיטלי נדיף ופגיע, ותכונות אלה נמנות עם התכונות המייחדות את המידע הדיגיטלי מהראיות הפיזיות.<sup>173</sup> הראיה הדיגיטלית עלולה להשתנות או להתעוות מהותית אף שלא בכוונה.<sup>174</sup> ניתן להמחיש זאת באמצעות הדוגמה הזאת: נניח שהחוקרת מבקשת לעיין בקובץ Word מסוים האגור במחשב התפוס. פתיחת הקובץ סתם כך ועיון בתוכנו יביאו לשינוי לפחות באחד ממאפייני המסמך והוא פרמטר ה־last accessed (קרי פרמטר המציין מתי נפתח קובץ ה־Word בפעם האחרונה). נקודה נוספת: עצם כניסתה של חוקרת המחשבים אל המחשב לצורך עיון ראשוני בו משנה את חומר המחשב המקורי בכך שכניסה זו נרשמת ב־log event במחשב הנחדר.<sup>175</sup> ועוד נקודה: לעתים מתבצעת שמירה אוטומטית, אחת לפרק זמן מסוים, של קובץ מחשב פתוח. בהמשך לדוגמה האחרונה, יכול להיות שאגב עיונה של החוקרת בקובץ תבוצע שמירה אוטומטית אשר תשנה את מאפיין ה־last saved.<sup>176</sup> מאפיין זה עשוי להתברר לאחר מעשה כרלוונטי לזירת המחלוקת

3032/99 ברנס נ' מדינת ישראל, פ"ד נו(3) 354, 375–377 (2002). גישה אחרת רואה בזכות להליך הוגן זכות חוקתית הנובעת הן מהזכות לכבוד והן מהזכות לחירות: ראו, למשל, עניין רוזנשטיין, לעיל ה"ש 29. כן ראו ישגב נקדימון הגנה מן הצדק 170–174 (מהדורה שנייה, 2009).

172 לתפישה זו, ראו בג"ץ 11339/05, שם, בעמ' 157.

173 ראו בפרק ד.ג.1..

174 ראו נמרוד קוזלובסקי המחשב וההליך המשפטי 35–38 (2000) (והמקורות המצוטטים שם).

175 ראו LINDA VOLONINO, REYNALDO ANZALDUA & JANA GODWIN, COMPUTER FORENSICS: PRINCIPLES AND PRACTICE 251–252 (2006).

176 ראו למשל ת"פ (שלום ת"א) 15417/97 מדינת ישראל נ' אבימור, פ"מ התשנ"ט (ג) 806, 781 (2000). באותו מקרה נדון אישום בעברות של זיוף פרטוקולים באמצעות מחשב. מומחה מטעם ההגנה אישר כי אגב עיון בקבצים יכול להיות שבוצעה שמירה אוטומטית ששינתה מאפיינים של הקובץ (יוער כי אמנם הקביעה התקבלה בידי בית המשפט, אולם באותו מקרה הוכח בפועל ששינוי הקובץ נעשה בזדון בידי הנאשם ולא אוטומטית במחשב או כדומה).



בתיק. דוגמה נוספת: נניח שנתפס מחשב לצורך הבאתו למשרדי היחידה החוקרת. נניח עוד שהמחשב דלוק ומחובר לחשמל. אם החוקרת בחרה לכבות את המחשב "כיבוי מסודר" (סגירת כל החלונות והתוכנות הרצות במחשב וכיבוי), הרי שיכול להיות שמידע יקר ערך מבחינה ראייתית יאבד. לדוגמה, ייתכן שאחד החלונות הפתוחים היה בעל פוטנציאל הוכחתי לקשירה ישירה של המשתמש במחשב לעברות המבוצעות או להוכחת חפותו.<sup>177</sup>

הפגיעה במהימנות הראיה הדיגיטלית עקב חדירה שנעשתה באמצעים לקויים או בחוסר מיומנות עלולה הן להזיק לאינטרס החקירתי לאסוף ראיות להוכחת העברה ולהוכחת זהות מבצעה, והן לפגוע בחשוד באופן שיימנע ממנו להציג ראיות בעלות פוטנציאל מזכה. אולם בשונה מעניינה של הרשות החוקרת, שהיא בעלת "כושר ספיגה" לטעויות הפוגעות בטיב החקירה הפלילית, כשמדובר בנזק לאדם פרטי הטוען לחפותו, אין לו יכולת ספיגה לטעויות מצד הרשות החוקרת. משמעותה של הטעות, מבחינתו, עלולה להיות הרשעת שווא. על כן פותחה בפסיקה הדוקטרינה שלפיה מחדלי חקירה ניכרים של הרשות החוקרת או נזק ראייתי שגרמה אשר הנאשם הציביע עליהם וטען כי מנעו ממנו אפשרות לבסס את גרסתו המזכה, יכול שיעוררו את הספק הסביר, תוך הנחה אוטומטית שהראיות החסרות "פועלות" לזכותו של הנאשם.<sup>178</sup> חשוב לציין כי התרופה של דוקטרינת מחדלי החקירה והנזק הראייתי מוגבלת בהיקף פרישתה, שכן היא אינה מאפשרת להתמודד עם מצבים שבהם הפגיעה אינה מתגלת לחשוד/הנאשם.

על מנת להתמודד עם פגיעות נסתרות במהימנות הראיה הדיגיטלית ניתן להגביל מראש, בשלב ההסמכה לביצוע פעולת האיסוף, את אופן פעולתה של הרשות החוקרת, וכך ימוזער הסיכון לנזק ראייתי. כך למשל יכול בית המשפט לחייב מראש פעולה על גבי העתק פורנזי של הדיסק הקשיח (להבדיל מהעתקה על דרך של פקודות "העתק" ו"הדבק" פשוטות, המבוצעות באמצעות לחיצה על המקשים Ctrl+C ו-Ctrl+V).<sup>179</sup> כן יכול הוא לחייב את החוקרים לשמור העתק של כל המידע שיתפסו, במקום להחזיר את החומרים שנדמים בעיניהם כלא רלוונטיים

177 יודגש כי אין מדובר ברעיון תאורטי בלבד. נאשמים בעברות באמצעות מחשב נוקטים את הטענה המכונה "הגנת הסוס הטרויאני". עיקרה של הטענה ניתן לתמצות כדלקמן: הראיות המפלילות שנמצאו במחשבו של החשוד אינן מעידות שביצע עברות, כיוון שאדם אחר השתלט על מחשבו באמצעות תוכנת סוס טרויאני וביצע את הפעילות העבריינית תוך שימוש במחשבו כ-proxy (כשלוח מטעמו של החשוד האמתי). ראו למשל ע"פ (מחוזי חי') 1126/06 לרמן נ' מדינת ישראל, בפס' 32–44 (פורסם בנבו, 24.5.2007). באותו מקרה נדחתה הטענה. כן ראו בפסיקה האמריקנית *United States v. McCourt*, 468 F.3d 1088 (8th Cir., 2006), גם שם נדחתה הטענה בנוגע לעברת החזקה של חומרים פדופיליים במחשב. לעומת זאת ראו מקרה מבריטניה, שם זוכה נאשם מאשמה של החזקת חומרים פדופיליים במחשבו בעקבות העלאת "הגנת הסוס הטרויאני", ראו *Munir Kotadia, Trojan Horse Found Responsible for Child Porn*, ZDNET UK (1.8.2003) <http://news.zdnet.co.uk/security/0,1000000189,39115422,00.htm>. הוכחה של חלון פתוח מפליל במחשב הנתפס יכולה בהחלט להחליש עד מאוד טענה של "הגנת הסוס הטרויאני", ולעומת זאת חלון פתוח במחשב שבו מודגמת השתלטות מרחוק על המחשב ופעולה מתוכו, יכול לחזק את הטענה.

178 לדוקטרינה זו בפסיקה הישראלית ראו ע"פ 5386/05 אלחורטי נ' מדינת ישראל, בפס' ז (פורסם בנבו, 18.5.2006); ע"פ 10596/03 בשירוב נ' מדינת ישראל, בפס' 20 לפסק דינו של השופט א' לוי (פורסם בנבו, 4.6.2006); כן ראו ע"פ 4855/02 מדינת ישראל נ' בורוביץ, פ"ד נט(6) 776–836 (2005).

179 במרבית החקירות שבהן נדרשת חדירה למחשב, מבוצעת העתקה פורנזית של הדיסק הקשיח שנתפס. ראו לעיל בפרק ד ה"ש 90.

לידי הבעלים ולהשמיד את עותקי המידע שברשותם.<sup>180</sup> אולם מלבד אמצעי זה, ניתן לכוון חובת תיעוד מוגברת ולהחילה על הרשות החוקרת, כפי שאפרט להלן.

### שקיפות פעולתה של הרשות החוקרת

האינטרס לשקיפות פעולתה של הרשות החוקרת הוא אינטרס כפול: ציבורי ופרטי. במישור הציבורי יש אינטרס שהרשות החוקרת, ככל רשות מנהלית, תאפשר שקיפות מרבית. אינטרס זה נקשר הן בזכות הציבור לדעת (חלק מחופש הביטוי),<sup>181</sup> הן בזכות לפרטיות במובן של חירות מפני משטר מעקב<sup>182</sup> והן ביריבות, לפחות הליברלית, המובנה בין האזרחים והתושבים לבין רשויות החקירה המייצגות את השלטון.<sup>183</sup> במישור הפרטי יש לחשוד או לנאשם זכות – כחלק מזכותו להליך הוגן – שכל פעולות האיסוף שבוצעו ייחשפו בפניו. זכות זו אף מעוגנת בסעיף 74 לחוק סדר הדין הפלילי. הדרך להבטיח את האינטרס הציבורי, כמו גם את הזכות הפרטית, היא בקביעת חובות תיעוד שיחולו על הרשות החוקרת. דרישת תיעוד מהרשות החוקרת אינה חדשה במשפטנו ואינה מתקיימת אך ורק בעניין איסוף ראיות דיגיטליות בחקירה פלילית במרחב הסייבר. עם זאת לדרישת התיעוד באשר לחקירה בסביבה דיגיטלית יהיו כמה ניואנסים ייחודיים שאותם אציג להלן. אחלק את ההצגה לשלב ההעתקה של המידע הממוחשב ולשלב מיצוי והפקת המידע מתוכו.

180 מנגד, פעולה זו עלולה לפגוע יתר על המידע בפרטיותו של החשוד, שכן מנקודת מבט של הזכות לפרטיות, השמדת המידע העודף או החזרתו לבעליו לעולם עדיפה. כשמדובר בכמה חשודים בחקירה, יכולות להיווצר סיטואציות של התנגשות זכויות של החשודים. אם למשל תידרש המשטרה לשמור את כל המידע שנאסף מרשות חשוד מס' 1, על פי בקשת חשוד מס' 2, הרי שלדידו של חשוד מס' 1, תיפגע פרטיותו פגיעה מוגברת על מנת לשרת את זכותו של חשוד מס' 2 להליך הוגן.

181 "זכות הציבור" (למעשה המינוח שגוי, ונכון יותר לכנות זאת "אינטרס הציבור") לקבל מידע על אודות הרשות המנהלית היא כלי מרכזי לפיקוח ולביקורת על תקינות פעולותיה של הרשות הציבורית ולהבטחת הגשמת עקרונותיו של המשטר הדמוקרטי. הפיקוח והביקורת הציבוריים הם הן בפועל והן בכוח. פוטנציאל הביקורת התמידי יש בו כדי לגרום אף לרשות עצמה לשפר את פעולתה בידעה כי היא חשופה בקביעות לעינו הביקורתית של הציבור. הצדקה נוספת מכיוון אחר לזכות הציבור לדעת היא בכך ששקיפות פעולתה של הרשות המנהלית יוצרת קרבה בין הפרט לרשות ובתוך כך לחיזוק אמון הציבור בה. ראו ע"א 3213/97 נקר נ' הועדה המחוזית לתכנון ולבנייה, פ"ד נג(4) 625, 649–650 (1999); ע"מ 398/07 התנועה לחופש המידע נ' מדינת ישראל – רשות המיסים, פ"ד סג(1) 284, בפס' 47 לפסק דינה של השופטת ארבל (2008). להרחבה, ראו גם זאב סגל הזכות לדעת באור חוק חופש המידע 11–14, 97–116, 171–183 (2000).

182 ראו Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J. L. & TECH. 257, 264 (2002). עיצוני כתב על חשיבות האחריות כגורם שיש בו כדי למתן את תחושת המעקב של כלל משתמשי הרשת בחברה שבה פוטנציאל איסוף המידע על אודותיהם הולך וגדל.

183 לסקירה כללית על אחריותיות בפעולת רשויות המדינה הליברלית והטלת חובות תיעוד כפועל יוצא מכך, ראו ANDREAS SCHEDLER, LARRY DIAMOND & MARC PLATTNER (EDS.), *THE SELF RESTRAINING STATE: POWER AND ACCOUNTABILITY IN NEW DEMOCRACIES* (1999). לכתובה על אחריותיות במסגרת אכיפה פלילית במרחב הסייבר, ראו Nimrod Kozlovski, *A Paradigm Shift in Online Policing – Designing Accountable Policing* 429–351 (J.S.D. Dissertation, 2005). חשוב לציין כי כתיבתו של קוזלובסקי על אחריותיות אינה נוגעת לדין בזכות להליך הוגן, כפי שאני מבקש לערוך כאן, אלא היא מהווה מרכיב משמעותי בתזה שלו שמודל האכיפה הפלילית צריך להשתנות למודל מניעתי משולב (סקרתי את המודל שמציע קוזלובסקי בפרק ב.ד.7).

אשר לשלב ההעתקה של חומר המחשב: שלב זה נחשב, מבחינה פורמלית, לשלב החדירה לחומר המחשב. ככזה, הפסד"פ מתיר למחזיק בחומר המחשב לנכוך בשלב החדירה,<sup>184</sup> וכן יכול שיתייצבו שני עדים מטעמו של המחזיק בחומר המחשב, אלא אם בית המשפט הורה אחרת, או שטעמי דחיפות הצדיקו שלא ינכחו שני עדים, או שהמחזיק בחומר המחשב ביקש שלא ינכחו שני עדים.<sup>185</sup> בצד דרישות אלה, שיובאו מדיני החיפוש בחצרים, ראוי להטיל חובת תיעוד לפעולות ההעתקה על מנת שיתאפשר לבחון בדיעבד אם פעולת ההעתקה פגמה במקור, זיהמה אותו או ייצרה העתק פגום, שהחסיר או שינה חלק מהנתונים שהיו במקור.<sup>186</sup> זאת, כיוון שהנוכחות הפיזית של מחזיק חומר המחשב ושני העדים מטעמו אין בה כדי להבטיח את החשש מפני פגיעה בהליך ייצור ההעתק.

אשר לשלב מיצוי והפקת המידע מתוך חומר המחשב שנאסף: כוונתי כאן לכלל הפעולות המתבצעות בנוגע למידע עצמו לצורך הפקת ממצאים חקירתיים: אחזורים של מידע על פי שאילתות, שחזור קבצים מחוקים, פתיחת קבצים מוצפנים ומוגני-ססמה, הצלבת המידע עם מידע ממקור אחר והמרת המידע מפורמט "גולמי" לפורמט קריא ונגיש לבעלי הדין ולבית המשפט (לדוגמה המרת תיקיית גיבוי של דוא"ל, כגון \*.dbx או \*.pst \* לקובצי דוא"ל בודדים שניתן לעיין בהם אחד-אחד, כגון \*.eml או \*.msg \*). הדוקטרינה של סעיף 74 הנ"ל, כפי שפותחה באשר לחקירה במרחב הפיזי, קובעת שפעולות של עיון, מיון, סידור, סיכום ראיות וכדומה – אינן עולות כדי פעולות איסוף של ממש, ועל כן אין הן מחייבות תיעוד.<sup>187</sup> ואכן, כיום, ברגע שנתפס מחשב ומבוצע בו עיון, מיון ואיתור של ראיות רלוונטיות, על פי רוב אין תיעוד של פעולות המיצוי וההפקה של המידע, למעט הפלט שהוא התוצר הסופי של פעולות אלה.<sup>188</sup> אולם שלב המיצוי וההפקה של המידע מצדיק תיעוד (auditing) על מנת לשמור כדבעי על זכותו של יעד פעולת האיסוף להליך הוגן, וכל זאת מן הטעמים האלה: האחד, לא תמיד העבודה של חוקר המחשבים תהא על העתק פורנזי מלא, וככל שהעבודה היא על המקור מסיבות שונות (קשיים טכניים בביצוע ההעתקה, טעמי דחיפות מיוחדים שאינם מותירים זמן לעריכת העתק פורנזי מלא ועוד), הרי ששלב המיצוי של המידע הם שלבים של התערבות בחומר ראיות מקורי, והחשש מפני זיהום הראיה מוגבר. התיעוד יאפשר להגנה בדיעבד לראות היכן זוהמה הראיה בתהליך הפקתה, אם זוהמה; השני, ככל שהצו השיפוטי מסמיך את הרשות החוקרת לפעול בתנאים ובמגבלות מסוימים (לדוגמה, נניח שהצו הגביל מראש את סמכות העיון לסוג מסוים של קבצים בלבד, לתכנים מסוימים בלבד או למילות חיפוש מסוימות), יאפשר התיעוד להגנה לבחון בדיעבד אם החוקר עמד במגבלות העיון שהוטלו עליו. אמנם כיום על פי רוב צווי

184 סעיף 28 לפסד"פ, המוחל בשינויים המחויבים על חדירה לחומר מחשב, מכוח הוראת סעיף 23א(א) לפסד"פ. ראו גם בש"פ 3607/13 הלוי נ' משטרת ישראל מפלג הונאה ת"א (פורסם בנבו, 30.6.2013).

185 סעיף 26א(א) לפסד"פ.

186 ראו פרק ד.ב.2.א).

187 השוו לבש"פ 2270/06 אל עילווי נ' מדינת ישראל, פ"ד סא(3) 74, בפס' 12–17 (2006), שם אמנם דובר במזכרים סודיים המוגשים לשופט במסגרת דיוני הארכת מעצר לפני הגשת כתב אישום, אך נקבע הכלל כי ריכוז סיכום ועיבוד של חומר חקירה כשלעצמם אינם חומר חקירה.

188 חרף הפיתוח הפסיקתי של המונח "חומר חקירה" בשנים האחרונות, המונח לא פותח עד כדי יצירת חובות תיעוד לפעולות של מיצוי והפקת מידע במהלך חיפוש, חדירה לחומר מחשב, המצאה או האזנת סתר.

החדירה לחומר מחשב גורפים בנוסחם,<sup>189</sup> אולם כפי שהראיתי לעיל בפרק זה, ההגנה על הזכויות החוקתיות השונות מצדיקה הצרתו של היקף המידע שיותר בעיון; השלישי, כאשר מדובר בפעולות איסוף סמויות, כגון חדירה סמויה למחשב, המצאת חומר מחשב בשלבי החקירה הסמויה או האזנת סתר למחשב, הרי ההצדקות לחובת תיעוד לכל שלב ושלב של הפעולה מקבלות משנה תוקף, בניסיון למתן, גם אם בדיעבד, את הפגיעה המגולמת ברעיון של משטרה חשאית.

מה רמת הפירוט של התיעוד המתבקש? הרמה האופטימלית, מבחינת ההגנה על הזכות להליך הוגן, היא של תיעוד ממוחשב אוטומטי המתעד כל פעולה ופעולה שמבצעת חוקרת המחשבים, כל שאילתה שהיא מקישה, כל מידע שהיא מעיינת בו. כיום תוכנות ההעתקה, המשמשות להעתקת הדיסק הקשיח המקורי שנתפס לדיסק קשיח משטרתי שעליו בדרך כלל מבוצע העיון והסינון של המידע, מספקות תיעוד (auditing) אוטומטי בדרך של לוג שנוצר עם עבודת תוכנת ההעתקה. לוג זה מאפשר לבדוק, ברמה של כל סקטור וסקטור בדיסק הקשיח, אם נפל פגם בתהליך ההעתקה.<sup>190</sup> שלב ההעתקה של הדיסק הקשיח הוא שלב מכריע, שכן למן רגע ההעתקה תעבוד חוקרת המחשבים על ההעתק, וחשוב לוודא שההעתק שעליו עבדה משקף במלואו את המצוי בדיסק הקשיח המקורי. קשה לחשוב על טעם כלשהו להימנע מתיעוד אוטומטי של שלב ההעתקה. גם בשלבי העיון, המיצוי וההפקה של המידע היה ראוי לכאורה לחייב תיעוד אוטומטי של כל הפקודות של חוקר המחשבים ושל כל הפלטים שהוצגו על צג המחשב של חוקר המחשבים.

עם זאת להוציא את המגבלות הטכניות הלא מבוטלות – בדמות האפשרות להרכיב תוכנת תיעוד על כל פעולת איסוף כלפי כל סוגי המחשבים בשים לב לסוג המדיה המועתקת, סוג מכשיר ההעתקה, תנאי ההעתקה הסביבתיים ועוד – קיימת מגבלה פוטנציאלית מהותית אחת, בדמות אינטרס החיסוי של פעולות הרשות החוקרת במקרים מסוימים (חיסיון מטעמי אינטרס ציבורי על שיטות החקירה).<sup>191</sup> מהו אינטרס החיסוי המשטרתי בהקשרנו? לעתים, במסגרת תהליכי המיצוי של המידע הרלוונטי לחקירה נדרשת המשטרה להתגבר על משוכות טכנולוגיות מסוימות, כגון הצפנות,<sup>192</sup> הגנת ססמאות, שימוש בשמות קוד והכמנת הקבצים בשמות בדויים הנחזים להיות תמימים ("התממה").<sup>193</sup> למשטרה יש עניין מובהק להימנע מחשיפת השיטות שבאמצעותן היא מצליחה לדלות מידע מפליל מתוך חומר מחשב שנתפס. לפיכך חשיפת הכלים ששימשו בחקירה ואף חשיפת מילות החיפוש ששימשו לצורך איתור הראיות המפלילות עלולות לחשוף בפני הנחקר – ודרכו גם בפני ציבור העבריינים הפוטנציאליים – את רמת הידע שברשות החוקרים.<sup>194</sup> ברמה הכללית, בהקשרים של חקירה במרחב הפיזי הכירה הפסיקה הישראלית

189 ראו לעיל בפרק ד.ג.2).

190 ראו הפניות לעיל בפרק ד בה"ש 90.

191 ראו סעיף 45 לפקודת הראיות.

192 קולובסקי, לעיל ה"ש 174, בעמ' 57-80; ליישום בפסיקה, ראו ב"ש (מחוזי ת"א) 92331/05 מדינת ישראל נ' פילוסוף (פורסם בנוב, 21.7.2005).

193 להמחשה ניתן לציין את אחת ממילות המפתח בשימוש פדופילים באינטרנט "pthc", שפירושו pre-teen hardcore, קרי של תכנים פדופיליים. פדופילים רבים משתמשים ברשתות לשיתוף קבצים תוך שהם מקלידים את מילת הקוד pthc, וכך כלפי חוץ נראה כי הם מחפשים תכנים חוקיים. ניתן ללמוד על כך למשל, מהפסיקה בעניין: United States v. Wilder, 526 F. 3d 1 (1st Cir., 2008).

194 ענף שלם של אנטי-פורנזיקה (anti-forensics) מקבל לאחרונה מעמד מוכר. אנטי-פורנזיקה הוא תחום בעל שימוש לגיטימי בידי רשויות המדינה לצורך ניקוי עקבות לפעולה חסויה המבוצעת ברשות

באינטרס להגן על שיטות הפעולה של הרשות החוקרת, בנסיבות המתאימות כאינטרס ציבורי לגיטימי המצדיק חיסויו של חומר ראיות.<sup>195</sup> המבחן, על פי הפסיקה, להכשרת תעודת חיסיון על שיטות הפעולה של רשויות החקירה ניתן לניסוח כדלקמן: האם האינטרס באיגילוי שיטות הפעולה גובר על הצורך לגלותן לשם עשיית צדק,<sup>196</sup> כאשר בכל מקרה לא תיתכן פגיעה ממשית בהגנת הנאשם (גם אם האינטרס הציבורי בחיסוי הוא מוגבר במיוחד)? במקרה של פגיעה ממשית שכזאת, הבררה בידי רשויות החקירה והתביעה תהיה בין גילוי התוכן החסוי או הימנעות / חזרה מאישום.

## 6. סיכום

איסוף הראיות בחקירה פלילית הוא פעולה המגלמת פגיעה באגד של זכויות חוקתיות. כך הוא כשאיסוף הראיות הוא במרחב הפיזי, וכך הוא כשאיסוף הראיות הוא במרחב הסייבר. התפישה הפיזית החולשת על דיני איסוף הראיות במרחב הסייבר מביאה להחמצת היבטים שונים של הזכויות החוקתיות הנפגעות מאיסוף הראיות בחקירה הפלילית. מבחני האיזון החוקתיים המוחלים על איסוף הראיות הדיגיטליות הם מבחנים המשועתקים מהדיון ביחס למרחב הפיזי. דיון זה מגלם הנחות מסוימות באשר לתכונותיה של הראיה הנאספת ובאשר ליכולות האיסוף של הרשות החוקרת, ולפיכך הוא מחמיץ מאפיינים חוקתיים מסוימים הנובעים מהתכונות הייחודיות של הראיות הדיגיטליות במרחב הסייבר. בחלק זה עמדתי על המאפיינים

ובסמכות. אולם אנטי-פורנזיקה משרתת האקרים ועברייני מחשב, שמטרתם להסוות את פעילותם העבריינים מעינם החוקרת של רשויות החקירה ושל קרבנותיהם. ראו, למשל Scott Berinto, *The Rise of Anti-Forensics*, available at [http://www.csoonline.com/article/221208/The\\_Rise\\_of\\_Anti-Forensics?page=1](http://www.csoonline.com/article/221208/The_Rise_of_Anti-Forensics?page=1).

195 אינטרס החיסוי הוא אמנם חלק מן האתוס של רשויות הביטחון והמודיעין האמונות על סיכול ומניעה (ראו, כדוגמה בלבד: בש"פ 9074/00 כ"אל נ' מדינת ישראל (פורסם בנבו, 18.12.2000); בש"פ 9086/01 ריבב נ' מדינת ישראל, פ"ד (נו) 163 (2002); בש"פ 7480/05 פחימה נ' מדינת ישראל (פורסם בנבו, 2.10.2005)). אולם אינטרס החיסוי נטען ומוגן גם לא אחת בקשר לפעולתה של הרשות החוקרת ובנימוק של אי-חשיפת שיטות עבודה לציבור העבריינים הפוטנציאליים. ראו למשל ע"פ 484/80 דרעי נ' מדינת ישראל, פ"ד לה(2) 215, 221-220 (1980) בהקשר של מיקומה של מצלמה נסתרת; ע"פ 334/81 הגינזר נ' מדינת ישראל, פ"ד לו(1) 827, 833-834 (1982) בהקשר של מיקומה של תצפית משטרתית; בג"ץ 5274/91 חוזה נ' שר המשטרה, פ"ד מו(1) 724 (1992) בהקשר של זהות עוקבים (אנונימיות העוקבים היא חלק משיטת פעולתם).

196 ביישום המבחן יש להבחין בין שיטות הפעולה השונות: אין דינן של מילות חיפוש שבשימוש הרשות החוקרת לצורך איתור מידע במחשב כדינם של אמצעים משטרתיים לפיצוח הצפנות. על פני הדברים במקרה הראשון האינטרס בחיסוי חלש בממקרה השני, שכן המקרה הראשון עניינו ב"קיצור דרך" למשטרה באיתור חומר מבוקש במחשב, ואילו המקרה השני עניינו ביכולת משטרתית שעקיפתה תאפשר לעבוד על קבצים שאינם ניתנים לפיענוח בידי משטרה, ובכך תאום היכולת המשטרתית לעיין בקבצים שונים בחקירה איום ממשי.

אציין כי בארצות הברית התקיים דיון ער בשאלת חשיפתו של ה-Carnivore, כלי ניטור שבשימוש רשויות החקירה, נוכח דרישתן של ארגוני זכויות, כ-ACLU ו-EPIC, מכוח חוק חופש המידע, לחשיפת קוד המקור של ה-Carnivore או למסירת העתק מן התוכנה. להרחבה בסוגיה ראו Etzioni, לעיל ה"ש 182, בעמ' 287-289. גם בעניין Scarfo נדון עניינו של כלי ניטור של רשויות החקירה, ונדרשה חשיפת יכולותיו של הכלי. בסופו של דבר הוחלט שם שבית המשפט יקבל הסברים מפורטים על כלי הניטור במעמד צד אחד, בלי שהנאשם יוכל להיות שותף לעניין. ראו United states v. Scarfo, 180 F. Supp.2d 572 (D.N.J. 2001). גם Kozlovski, לעיל ה"ש 183, בעמ' 359-364.

המוחמצים כאמור כתוצאה מהתפישה הפיזית, אשר ראוי כי ישוקללו במסגרת עריכת איזון חוקתי בין צורכי החקירה לבין הזכויות המוגנות.

## ה. מסקנות

דיני איסוף הראיות בחקירה פלילית, במרחב הפיזי כמו גם במרחב הסייבר, מגלמים התנגשות בין צורכי החקירה מחד גיסא לבין הזכויות המוגנות מאידך גיסא. בפרק זה מיקדתי את הזרקור לכיווןן של הזכויות המוגנות המושפעות במישורן מתפישות היסוד השגויות שעליהן הצבעתי בפרקים ג ו-ד: התפישה הטריטוריאלית והתפישה הפיזית. הדיון בפרק זה משלים את טענתי בדבר ההחמזה הדו-כיוונית שנגרמת מהתפישה הטריטוריאלית ומהתפישה הפיזית – הן החמזה במישור של צורכי החקירה והן החמזה במישור של השיח החוקתי. כפי שהראיתי כאן, השיח החוקתי מוחמץ בשלושה ממדים הניתנים לתמצות בשלוש שאלות שונות: מי נפגע (זיהוי השחקנים הטוענים לזכויות החוקתיות)? איפה הפגיעה (דיון בהיקף התחולה של ההגנות החוקתיות מבחינה טריטוריאלית)? איך או כמה נפגע (דיון במלוא המובנים של הזכויות החוקתיות הנפגעות כתוצאה מפעולות האיסוף)?

מן הדיון שנערך עד כה נובע כי דיני איסוף הראיות בחקירה הפלילית במרחב הסייבר אינם מותאמים לשינויים הטכנולוגיים (ולשינויים הכלכליים והחברתיים שנגרמו ממהפכת הסייבר). ניסוח הסמכויות, אופן הפעלת שיקול הדעת בעת מתן ההסמכה הקונקרטית לרשות החוקרת וניסוח ההגנות החוקתיות מפני סמכויות אלה – כל אלה ערוכים על פי מונחי המרחב הפיזי. משכך, המשפט כגורם מסדיר על פי המודל הלסיגיני<sup>197</sup> אינו מתפקד כראוי.

יש לפתח את דיני איסוף הראיות בחקירה הפלילית במרחב הסייבר באופן המשוחרר מהכבלים הקונספטואליים של הפיזיות והטריטוריאליות. כך יתאפשר למדינה לאכוף את הדין הפלילי במרחב הסייבר באופן שימנע פגיעה מהותית בריבונותה במובן הפנימי (במישור יחסיה עם תושבי המדינה ומעמדה כמי שמסוגלת לאכוף את החוק ולשמור על הסדר באופן אפקטיבי) ובמובן החיצוני (במישור יחסיה הבין-לאומיים עם מדינות אחרות וחובתה לשמור על הסדר באחריותה באופן שלא תיגרמנה פגיעות שתשלכנה על המדינות האחרות). כמו כן יתאפשר להגשים ולבטא את הערכים המוגנים שבבסיס המשפט החוקתי של המדינה. פיתוח דיני איסוף הראיות במרחב הסייבר באופן המשוחרר מכבלי הטריטוריאליות והפיזיות יביא לבחינה מחדש של סל סמכויות איסוף הראיות הדיגיטליות וכן לבחינה מחדש של אופן עריכת האיזון החוקתי למול סמכויות האיסוף, המבטאות את ההכרה בצורכי החקירה. כוונתי באיזון החוקתי לשניים: איזון עקרוני ברמת החקיקה ואיזון קונקרטי ברמת היישום השיפוטי או המנהלי במקרה נתון. את האיזון החוקתי יש לערוך לאורם של שלושת הממדים שמניתי לעיל: ממד איתור ה"שחקנים" הנפגעים מסמכות האיסוף (ברמה העקרונית) או מפעולת האיסוף המבוקשת (ברמה הקונקרטית); ממד היקף הפרישה הטריטוריאלית של ההגנות החוקתיות; ממד זיהוי הזכויות הנפגעות עצמן ועמידה על המובנים השונים של הפגיעה בהם. בפרק הבא אציע מודל חשיבתי חלופי, שאותו אכנה "המודל הפרסונלי", ולאורו אציע לעצב את דיני איסוף הראיות הדיגיטליות בחקירה פלילית במרחב הסייבר.

197 כפי שפורט לעיל בפרק א.ד..