EDNAKARNAVAL LIBRARY FOR THE MASSES

פרק 4 - התפישה הפיזית ביחס לאיסוף ראיות בחקירה פלילית במרחב הסייבר

א. הקדמה

בפרק זה אציג תפישה יסודית נוספת החולשת על האופן שבו המשפט מתייחס לראיות דיגיטליות המצויות במרחב הסייבר: התפישה המקבילה את הראיות הללו לראיות חפציות, המצויות במרחב הפיזי. *התפישה הפיזית* משמעה, בתמצית, שהראיות הדיגיטליות מושוות לראיות מן המרחב הפיזי. כתוצאה מהקבלה זו, בין הראיות הדיגיטליות לבין הראיות במרחב הפיזי, נוצר חסר דו-כיווני באופן שבו חולשים דיני איסוף הראיות על החקירה הפלילית במרחב הסייבר: מצד אחד, נפגע הפיתוח המשפטי של סמכויות איסוף הראיות הרלוונטיות לראיות הדיגיטליות והמתאימות לטיבן. מצד שני, נפגע השיח החוקתי הרלוונטי לאיזון פעולתה של הרשות החוקרת במרחב הסייבר, במובן זה שלא כל הזכויות החוקתיות, על מובנן ה"דיגיטלי", ולא כל הטוענים לזכויות הנפגעים כתוצאה מהחקירה הפלילית במרחב הסייבר – מובאים בחשבון. בפרק זה אציג את האופן שבו התפישה הפיזית מגולמת במשפט הישראלי, כמו גם בשיטות משפט נוספות, בעיקר במשפט האמריקני. לאחר מכן, אראה כי התפישה הפיזית שגויה בשל העובדה שהיא חוטאת לאופייה של הראיה הדיגיטלית, השונה במספר מובנים מזה של הראיה הפיזית, וכתוצאה מכך היא מובילה לחסר בכל הנוגע לצרכיה של הרשות החוקרת במרחב הסייבר. בהמשך, פרק 5 יוקדש לדיון החוקתי הנחסר כתוצאה מהתפישה הפיזית, כמו גם כתוצאה מהתפישה הטריטוריאלית, עליה עמדתי בפרק הקודם.

מטרת הפרק הנוכחי, כקודמו, היא לחשוף תפישות יסודיות סמויות החולשות על החקירה הפלילית במרחב הסייבר. ההצגה של התפישות – הטריטוריאלית והפיזית – היא באופן נפרד, ומכאן נובע לכאורה שאין זיקה בין שתי התפישות. למעשה, יכולה להישמע טענה ששתי תפישות אלה נגזרות למעשה מתפישה מעין-מוֹניסטית של הראיות הדיגיטליות ככאלו המיוצגות באטומים ולא בסיביות.[1] הכשל בהבנת הדיגיטציה מוביל לניסיונות למקם את הראיות ולהקבילן לחפצים. עם זאת, מצאתי שהשאלות שמעורר עניין הטריטוריאליות שונות מאלה שמעוררת סוגיית הפיזיות, כפי שיובהר במהלך הדברים, ועל כן בחרתי לפצל את הדיון.

---

[1] על תפישת המידע כמיוצג בסיביות ראו ניקולאס נגרופונטי **להיות דיגיטלי** (תרגום עמנואל לוטם, 1996).

EDNAKARNAVAL LIBRARY FOR THE MASSES

ב. אבחון התפישה הפיזית

אציג את פרישתה של התפישה הפיזית, תחילה ביחס לדיני המחשבים בכלליות, ולאחר מכן ביחס לאיסוף ראיות דיגיטליות באופן מפורט. אראה כיצד שימוש של מחוקקים ושופטים בביטויים מן העולם הפיזי משליכים על אופן ההתבוננות על דיני איסוף הראיות הדיגיטליות, הן בשלב הגדרת סמכויות האיסוף ברמה הכללית והן בשלב ההסמכה לביצוע פעולות האיסוף ברמה הקונקרטית. הצגת התפישה הפיזית בדיני המחשבים ככלל תסתמך על ניתוח של חוקרי משפט וטכנולוגיות מידע, ואילו הצגת התפישה הפיזית ביחס לדיני איסוף הראיות הדיגיטליות תיערך באופן מפורט ביחס לדין הישראלי, תוך הפניות לדין הזר.

1. התפישה הפיזית בדיני המחשבים הכלליים

בפרק הקודם הצגתי את השימוש במטאפורת המרחב המקוון כמקום, המבססת את התפישה הטריטוריאלית ביחס למרחב המקוון. כן עמדתי על המטאפורה ככלי מחויב המציאות בחשיבה המשפטית מחד גיסא, וכאמצעי להבניית הניתוח המשפטי והכוונת תוצאתו מאידך גיסא. אעמוד עתה בקצרה על מטאפורות ואנלוגיות "חפציות" או "פיזיות" ביחס למרחב המקוון, כאשר בשלב זה של הדיון ההתמקדות אינה ביחס לאיסוף ראיות דיגיטליות אלא לדיני המחשבים באופן כללי.

התפישה של המידע כ"חפץ" או כ"נכס" שכיחה במשפט.[2] דוגמה *אחת* למטאפורה חפצית ביחס למידע דיגיטלי היא דוגמת השימוש במשפט האמריקני בעוולת השגת גבול במיטלטלין (trespass to chattels) בכל הנוגע לשימוש במידע מהאינטרנט בלא רשות מאת "ממחזיק".[3] על פי הגדרת ה-Restatement האמריקני בנזיקין, העוולה מתבצעת כאשר נוצר מגע פיזי עם המיטלטלין ("Physical contact with the chattel").[4]

---

[2] ראו למשל: Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 580-597 (2001); אברהם נ. טננבוים "על המטאפורות בדיני המחשבים והאינטרנט" **שערי משפט** ד 359, 386-388 (2006).

[3] ראו למשל: Dan L. Burk, *The Trouble With Trespass*, 3 J. SMALL & EMERGING BUS. L. 1 (1999); Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421 (2002); Kathleen K. Olson, *Cyberspace as Place and the Limits of Metaphor*, 11 CONVERGENCE 10 (2005). ליישום פסיקתי של עוולת השגת גבול במיטלטלין בארצות-הברית, ראו למשל: eBay Inc. v. Bidder's Edge Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); America Online v. National Health Care Discount, Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001); Oyster Software, Inc. v. Forms Processing, 2001 WL 1736382 (N.D. Cal. 2001). כן ראו בפסיקה הישראלית את ת"ק (שלום ת"א) 6000/03 **אבן חן נ' סויסה** (פורסם ב"נבו", 15.9.2003). אולם השוו, מנגד, עם Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003), שם נדחתה האנלוגיה להשגת גבול במיטלטלין בנוגע לעובד לשעבר באינטל ששלח מיילים לעובדים בחברה, בהם הכפיש את החברה. לביקורת על השימוש באנלוגיה, ראו גם חיים רביה "בעלי בקר וסכסוכי מחשב" (21.9.2003) http://www.law.co.il/articles/web-issues/2003/09/21/222/.

[4] ראו: Restatement (Second) of Torts § 217 (American Law Institute, 1965).

EDNAKARNAVAL LIBRARY FOR THE MASSES

דוגמה *שניה* להקבלת המידע הממוחשב לחפצים פיזיים היא בכל הנוגע להשוואת אמצעי אבטחת המידע למנעולים,[5] ובכלל זה הקבלת המידע המוצפן למידע האגור בכספת.[6] מנעולים וכספות מתאימים לשמירה על חפצים, ולאו דווקא לשמירה על מידע. מייקל פרומקין (Froomkin) הסביר כי אנלוגיית המנעולים אינה מתאימה למידע באינטרנט, שכן המידע הוא תקשורתי באופיו. משכך הוא, הרי שבתוספת אנלוגיית המנעולים, יומשל המידע המוגן באינטרנט למטענים בנמלי ים ואוויר. מכאן, הראה פרומקין, קצרה הדרך להפחתת ההגנה על הפרטיות במידע המוגן, שכן מטענים בנמלים זוכים להגנה מועטה יחסית על הפרטיות מבחינת המשפט האמריקני.[7]

כדוגמה *השלישית* למטאפורה החפצית ביחס למידע הדיגיטלי ניתן למנות את השימוש במונח "החזקה" ביחס למידע. מושג ה"מחזיק" במידע רלוונטי בהקשרים משפטיים שונים. לדוגמה, המחזיק במאגר מידע חייב ברישום המאגר[8] הוא יכול להיות מורשע בעבירה של החזקת חומר תועבה ובו דמותו של קטין[9] או בעבירה של החזקת חומר הסתה לאלימות או לטרור.[10] מונח ה"החזקה" עורר שאלות משפטיות גם בכל הנוגע לחפצים פיזיים. לשם כך, למשל, פותחו מבחני הידיעה והשליטה ומבחני ההחזקה הקונסטרוקטיבית כדי להתמודד עם מקרים שבהם לא הייתה צמידות פיזית בין המחזיק לבין החפץ המוחזק, או במקרים בהם נקשרו מספר אנשים לאותו חפץ.[11] בכל הנוגע להחזקת מידע ממוחשב, בפרט באינטרנט, פותח מבחן המכיר בהפרדה פיזית חוצת-מדינות בין המידע לבין מחזיקו, בתנאי שקיימת נגישות ושליטה ממשית במידע.[12] עם זאת, חשוב לציין כי מונח ההחזקה ממשיך להציב קשיים משפטיים הנובעים מאופיו של המידע במרחב המקוון. כך, למשל, שאלה פתוחה היא האם צפייה בתכנים באינטרנט (Viewing או שימוש ב-Video-Streaming), להבדיל מהורדה שלהם (Download), מהווה "החזקה". באופן טכני-פורמלי, טכנולוגיית הצפייה כוללת הורדה של המידע אל

---

[5] ראו ע"פ (מחוזי ת"א) 71227/01 **מדינת ישראל נ' טננבאום**, תק-מח 2002(2) 1540, 1544-1548 (2002). לעמידה על הרטוריקה הקניינית הנקוטה ביחס למידע הממוחשב בפרשת אהוד טננבאום, שכונה גם ה"אנלייזר", ראו מיכאל בירנהק "משפט המכונה: אבטחת מידע וחוק המחשבים" **שערי משפט** ד 315, 352-356 (2006).

[6] ראו: A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip and the Constitution*, 143 U. PA. L. REV. 709, 871-874 (1995). כן ראו: Nathan K. McGregor "The Weak Protection of Strong Encryption: Passwords, Privacy, and the Fifth Amendment" 12 VANDERBILT J. ENT. & TECH. L. 581, 602-603 (2010).

[7] ראו Froomkin, שם.

[8] ראו סעיף 8(א) ביחד עם סעיף 31א(א)(1) לחוק הגנת הפרטיות, התשמ"א – 1981 (להלן – "חוק הגנת הפרטיות"). ראו עוד את סעיף 3 לחוק המגדיר "'מחזיק', לעניין מאגר מידע' – מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש".

[9] ראו סעיף 214(ב3) לחוק העונשין, התשל"ז – 1977.

[10] ראו סעיף 144ד3 לחוק העונשין.

[11] ראו, למשל, ע"פ 250/84 **הוכשטט נ' מדינת ישראל**, פ"ד מ(1) 813 (1986); ע"פ 1478/91 **מדינת ישראל נ' רובבשי**, פ"ד מו(1) 829 (1992).

[12] ראו ע"פ 1761/04 **שרון נ' מדינת ישראל**, פ"ד נח(4) 9, 16-19 (2004).

EDNAKARNAVAL LIBRARY FOR THE MASSES

מחשב הקצה וטעינתו מתוכו, אך המידע אינו נשמר במסודר כקובץ במחשב הקצה עם גמר הצפייה, אלא הוא נותר אגור בזיכרון המטמון (ה-Cache memory), זאת עד שיידרס על-ידי מידע אחר.[13] לשאלת הצפייה כהחזקה נפקות ממשית הולכת וגוברת נוכח המעבר מפרקטיקה של "הורדה" לפרקטיקה של "צפייה".[14] אמחיש להלן את הסוגיה ביחס לעבירה של החזקת חומרי תועבה פדופיליים.

בעניין **Diodoro** פסק בית-המשפט העליון של מדינת פנסילבניה, ברוב דעות של שבעה שופטים כנגד שניים, כי ניתן להרשיע אדם בעבירה של החזקת (Possession) חומרי תועבה פדופיליים על פי הקונסטרוקציה שצפייה כוללת החזקה זמנית בזיכרון המטמון, ומכאן שפורמלית נחשבת הצפייה כהחזקה. ככל שהנאשם מודע לקיומה של החזקה זמנית זו, הרי שיש מקום להרשיעו בעבירה.[15] המהלך הפרשני המאפשר לראות ב"צפייה" כ"החזקה" נסמך כאמור על הוכחת מודעותו של הנאשם לנקודה טכנולוגית ולא למהות של ההגנה על קטינים המופיעים במיצג המתועב וקטינים אחרים העתידים להיפגע מצרכני אותם תכנים פדופיליים. ייתכן שמונח נייטרלי יותר מבחינה טכנולוגית, כ"צריכה" או "שימוש", היה מונע את הקושי המשפטי הנובע מבחירה במונח "פיזי" במהותו, כ"החזקה", ואכן לאחרונה תוקן חוק העונשין, התשל"ז – 1977, כך שסעיף 214(ב3) לחוק יכלול גם איסור על צריכת התכנים הפדופיליים, מעבר לאיסור הקיים על החזקת התכנים.[16]

---

[13] ראו: Brian D. Davison, *A Web Caching Primer*, 5 IEEE INTERNET COMPUTING 38, 39 (Jul.-Aug. 2001). המעבר מהורדה של התכנים לצריכתם און-ליין משמעותו, מבחינת משתמש הקצה, שצפייה חוזרת במידע תחייבו להתקשר שוב אל האתר בו מצוי המידע המבוקש. זאת כיוון שהקובץ שנצפה בעבר אינו שמור באופן מסודר הנגיש לצפייה חוזרת.

[14] לאבחון מגמה זו ראו למשל: Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227. 1230-1231 (2004). אציע כמה הסברים לשינוי מגמת הצריכה של תכנים באינטרנט מהורדה לצפייה און-ליין: *האחת*, כיוון שקצבי ההורדה של מידע מהאינטרנט הלכו וגברו, עלות "רוחב הפס" הלכה והוזלה, כך שעבור משתמשי האינטרנט, צריכה על דרך של צפייה און-ליין הפכה לחלופה זולה ונוחה יחסית. *השניה*, אתרי אינטרנט רבים המאפשרים צפייה בתכנים עשויים להעדיף, מבחינה כלכלית, כניסה חוזרת של משתמשי אינטרנט אליהם, כיוון שכך החשיפה של המשתמשים לפרסומות תהיה גדולה יותר, וניתן יהיה לגבות ממפרסמים תשלום גבוה יותר. אתרים אלה ייצרו פלטפורמה של צפייה און-ליין בלבד, ללא אפשרות להורדה של התכנים. כזה הוא, למשל, המודל של אתר Youtube. *השלישית*, מבחינת משתמש הקצה הוא עשוי להעדיף להוזיל עלויות של רכישת אמצעי אחסון לכמויות מידע גדולות, ולעתים הוא אף יהיה מעוניין במכוון שלא יישמרו התכנים בהם צפה.

[15] ראו: Commonwealth of Pennsylvania v. Diodoro, 970 A. 2d 1100 (Pa. Super. 2009). לפסיקה דומה ראו גם: United States v. Tucker, 305 F. 3d 1193 (10th Cir. 2002); United States v. Romm, 455 F. 3d 990 (9th Cir. 2006). בפסיקה הישראלית קיימת התייחסות בודדת של בית-משפט השלום בתל-אביב לנושא בעניין **פלוני**. באותו מקרה הנאשם הודה במסגרת הסדר טיעון בעבירה של החזקת חומרי תועבה ובהם דמויות של קטינים. בית המשפט העיר בגזר הדין שצפייה בתכנים פדופיליים אינה עבירה פלילית, וכמוה גם הגלישה באינטרנט בחיפוש אחרי תכנים פדופיליים אינה אסורה. ראו ת"פ (שלום ת"א) 7936/07 **מדינת ישראל נ' פלוני**, תק-של 2009(2) 6796 (2009). המדינה ערערה על קולת העונש באותו המקרה, ובית-המשפט המחוזי קיבל את הערעור. בית-המשפט המחוזי נמנע מלהתייחס להערת השופט מור לגופה, אם כי הובעה הסתייגות כללית מקביעותיו של בית-המשפט קמא. ראו ע"פ (מחוזי ת"א) 7493/09 **מדינת ישראל נ' פלוני**, תק-מח 2009(3) 13925 (2009).

[16] ראו חוק העונשין (תיקון מס' 118), התשע"ה – 2014, ס"ח 32. כמו כן, הפללה ישירה של צרכן התכנים הפדופיליים מופיעה בדין הזר. ראו, למשל, את סעיף 9 לאמנת מועצת אירופה בדבר פשעי מחשב: Council of Europe Convention on Cybercrime (Budapest, 2001) http://conventions.coe.int/Treaty/en/Treaties/html/185.htm; סעיף 20 לאמנת מועצת אירופה בנושא הגנת ילדים מפני ניצול מיני: Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote, 2007)

בצד הדוגמאות הנ״ל, המלמדות על שימוש במטאפורות ואנלוגיות חפציות, ניתן להצביע על תהליך מעניין נוסף המשעתק את התפישה הפיזית של המרחב המקוון, ולפיו המרחב המקוון מפעפע לתוך המרחב הפיזי, באופן שממזג בין החפצי לבין הדיגיטלי. בעיקר הדבר בולט ביחס ל״השתלטות״ האינטרנט על עולם הסלולר.[17] מכשירי הסמארטפון משמשים יותר ויותר לתעבורת נתונים מאשר לצרכי טלפוניה.[18] הם נחזים לחפצים (מד-חום, פלס, מפת דרכים, כלי נגינה וכיוצא בזה). באמצעות האינטרנט ניתן להפעיל מערכות ״בית חכם״ ולהפעיל מזגן, דוד חשמל וגם לשחרר את האזעקה.[19] האקר ש״יפרוץ״ למכשיר המפעיל את מערכת ה״בית החכם״, יוכל באמצעות זאת גם לפרוץ אל הבית עצמו, וכך האנלוגיה בין פריצה למחשב לבין פריצה לבית תחדל מלהיות אנלוגיה ותהפוך למציאות כפשוטה.[20]

אם לסכם עד כאן, המשפט נוטה להתבונן על המרחב הווירטואלי על בסיס תפישה פיזית. זאת תוך שימוש במטאפורות ואנלוגיות מן העולם הפיזי על מנת לבחון סוגיות משפטיות במרחב המקוון. בנוסף, תהליכי הפעפוע בין האינטרנט והדיגיטציה לבין העולם הפיזי מייצרים קושי תפישתי להפריד בין המרחב הווירטואלי לבין המרחב הפיזי, ומכאן שקשה עוד יותר לחשוף ולאפיין את התפישה הפיזית ביחס למידע הדיגיטלי, לא כל שכן קשה לבקר אותה. אעבור עתה מן הדוגמאות הכלליות ביחס לדיני המחשבים לטיעון הממוקד יותר ביחס לחקיקה המסדירה את סמכויות איסוף הראיות הדיגיטליות בחקירה פלילית במרחב המקוון. אמחיש את הטיעון בהתייחס לחקיקה הישראלית, תוך הפניות לדין הזר.

---

http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm; סעיף 163.1(4.1) לקוד הפלילי הקנדי – An Act Respecting the Criminal Law, R.S.C. 1985, c. C-46, שם נקבע איסור על גישה (Accessing) לפורנוגרפיית קטינים.

[17] השתלטות שרק תלך ותגבר עם המעבר לטכנולוגיית ה-LTE (Long Term Evolution) המבשרת על הדור הרביעי של עולם הסלולר. ראו, למשל, אמיתי זיו ״דור 4 בסלולר – הזדמנות ענקית בהמתנה״ **דה מרקר** 18.7.2011 http://www.themarker.com/hitech/1.670272; ולהסבר מפורט יותר ראו: http://sites.google.com/site/lteencyclopedia/home.

[18] ראו למשל: ״סיסקו: תעבורת הנתונים הסלולרית תגדל פי 26 עד 2015״ **אנשים ומחשבים** 20.2.2011 http://www.pc.co.il/?p=53833.

[19] דוגמה זו מתחברת לתחום רחב הרבה יותר המכונה "Internet of Things", שבו חפצים ומכשירים מהמרחב הפיזי יחוברו לאינטרנט ויוכלו לקבל הוראות ולשדר מידע דרך הרשת. להרחבה על תחום מתפתח זה ראו: Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (22.6.2009) http://www.rfidjournal.com/article/view/4986; Rob Van Kranenburg, The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID (2008) http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf.

[20] על האנלוגיה בין פריצה לבית לבין חדירה לחומר מחשב, ראו לעיל פרק 3 בה״ש 67.

EDNAKARNAVAL LIBRARY FOR THE MASSES

2. התפישה הפיזית ביחס לדיני איסוף הראיות בחקירה פלילית במרחב הסייבר

סמכויות האיסוף במשפט הישראלי מבוססות ברובן על חקיקה ישנה. פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט – 1969 (להלן - "הפסד"פ") מבוססת על פקודה מנדטורית.[21] חוק האזנת סתר, התשל"ט – 1979 (להלן - "חוק האזנת סתר") שגם הוא רלוונטי לענייננו, אף הוא כבר בן יותר מ-30 שנה. הפסד"פ, כמו גם חוק האזנת סתר, תוקנו בשנת 1995 והוכנסה אליהם, לראשונה, ההתייחסות ל"חומר מחשב" ול"תקשורת בין מחשבים".[22] אולם, המדובר בתיקונים תוספתיים, ולא בניסוח מחדש של החוקים המסמיכים בכל הנוגע לראיות דיגיטליות. רק חוק סדר הדין הפלילי (סמכויות אכיפה - נתוני תקשורת), התשס"ח – 2007 (להלן - "חוק נתוני תקשורת"), שגם הוא רלוונטי לענייננו, נחקק בעת האחרונה אך הוא מטפל בתחום מצומצם יחסית, בין מכלול סמכויות האיסוף. בשים לב להתפתחויות הטכנולוגיות, בפרט בתחום המיחשוב והתקשורת, ניתן לדבר בהחלט על חקיקה המפגרת אחרי המצב הקיים בשטח. הפיגור הוא בשני מובנים: (א) במובן הפשוט של אי התייחסות החוק להתפתחויות טכנולוגיות משמעותיות כגון כניסתו של האינטרנט לחיינו. החקיקה המסדירה את סמכויות האיסוף אינה מתייחסת כלל לאינטרנט; (ב) במובן עמוק יותר, לעתים סמוי, שעניינו באופן בו תופס המחוקק את הראיה הדיגיטלית. כפי שאראה בהמשך, המחוקק תופש את הראיה הדיגיטלית בכלים ובאופן שבו הוא מתייחס לראיות במרחב הפיזי, ובאופן אמיתי לא בידל את הראיות הדיגיטליות מהן, גם אם מצא לנכון להתקין מספר הוראות ייחודיות ל"חומר מחשב".[23]

מעניין לציין שכבר לפני יותר משני עשורים הובעה בספרות המשפטית התמיהה על כך שהחקיקה בתחום דיני הראיות והחקירה בכלל (לרבות נושא סמכויות האיסוף שממין ענייננו) קפאו על מקומם ונשארו כשהיו מאז קום המדינה, ובהתבסס על המשפט המנדטורי.[24] מהפכת המיחשוב, ובפרט המעבר מעידן המחשב הבודד לעידן הרשתי של האינטרנט, טרפו את הקלפים שוב, והותירו את החוקים הנוהגים בלתי רלוונטיים עוד לחקירה בסביבה הדיגיטלית. בשנת 1986 ניסח השופט דן ביין

---

[21] ראו פקודת סדר הדין הפלילי (מעצר וחיפוש), 1924, חא"י, כרך א', 459.

[22] לתיקון הפסד"פ בשנת 1995, ראו סעיף 11 לחוק המחשבים, התשנ"ה - 1995 (להלן – "חוק המחשבים") (תיקון עקיף של סעיף 1, 23א ו-32 לפסד"פ). לתיקון חוק האזנת סתר בשנת 1995, ראו חוק האזנת סתר (תיקון), התשנ"ה – 1995, ס"ח 180. תיקון נוסף הרלוונטי לענייננו בוצע בפסד"פ בשנת 2005. ראו חוק לתיקון פקודת סדר הדין הפלילי (מעצר וחיפוש) (תיקון מס' 12) (חיפוש ותפיסת מחשב), התשס"ה – 2005, ס"ח 526.

[23] הדיון כאן מתייחס לסמכויות האיסוף של ראיות דיגיטליות בערוץ החקיקה המרכזי המכוון כלפי משטרת-ישראל. לא אעסוק בסמכויות איסוף נפרדות כפי שנוסחו עבור רשויות חקירה מיוחדות, שאינן המשטרה, לדוגמה הרשות לניירות-ערך (ראו חוק ניירות ערך, התשכ"ח – 1968, סעיפים 56א-56ג), רשות המסים (סעיפים 108-109 לחוק מס ערך מוסף, התשל"ו – 1975; סעיפים 135-140, הנוספים על סעיף 227, לפקודת מס הכנסה [נוסח חדש], התשכ"א – 1961 (להלן – "פקודת מס הכנסה")), הרשות להגבלים עסקיים (סעיפים 45-46 לחוק ההגבלים העסקיים, התשמ"ח – 1988), סמכותו של קצין בודק והמשטרה הצבאית החוקרת לגבי "מקום צבאי" (סעיפים 245ג-250, 256 לחוק השיפוט הצבאי, התשט"ו - 1955) ועוד. עם זאת אעיר כי להבנתי, מעיון בכל אותם דברי חקיקה שלא יטופלו כאן, עולה כי הם מבטאים עמדות או איפיונים דומים בקשר לסמכויות האיסוף.

[24] גרשון אוריון "מגמות אינקוויזיטוריות בדיני הראיות" **משפט פלילי, קרימינולוגיה ומשטרה** כרך א' 115, 123-124 (גרשון אוריון עורך, 1986).

EDNAKARNAVAL LIBRARY FOR THE MASSES

הצעה לרפורמה חקיקתית במה שכינה "אמצעים משטרתיים", כאשר הכוונה להסדרה חוקית של דיני המעצר והעיכוב, סמכויות האיסוף השונות והחילוט.[25] ביין ניסח את הצעתו, על פי דבריו הוא, כהצעה ראשונית המוגשת כבסיס לדיון בוועדת מומחים.[26] הצעתו לא התייחסה לחומר מחשב. בשנת 1996 התכנסה ועדה מטעם משרד המשפטים, בראשות שופט בית-המשפט העליון, דב לוין, ובהשתתפות שופטים נוספים, נציגי אקדמיה, נציג משטרת-ישראל, נציג השוק הפרטי ונציגי היועץ המשפטי לממשלה. הוועדה התבססה בעבודתה בין היתר על הצעתו הנ"ל של ביין. בחודש מאי 1996 הוגש דין וחשבון הוועדה לסדר דין פלילי (אמצעים משטרתיים) (חיפוש, הצגה, תפיסה וחילוט) (להלן - "דו"ח ועדת לוין"). מסקנות הוועדה לא יושמו עד היום בחקיקה. הוועדה הציעה מספר חידושים: חובת פירוט רבה יותר בצו החיפוש, חובת עריכת פרוטוקול מפורט של מהלך החיפוש, סמכות של חשוד לבקש צו חיפוש במצבים מסוימים, סמכות להוצאת צו לחיפוש סמוי בפשעים חמורים. בדו"ח הוועדה מבוטא הניסיון להתחשב בזכויות הפרט המוגנות אשר עוגנו בחוק יסוד: כבוד האדם וחירותו והוכרו באופן מפורש כמשליכות על פעולת רשויות החקירה בעניין **גנימאת** שנפסק בשנת 1995.[27] ניסיון זה נתמך גם בספרות המשפטית המתייחסת להשלכות חוק היסוד על הפרוצדורה הפלילית.[28] בכל הנוגע לחדירה לחומר מחשב, הוועדה למעשה לא חידשה על מה שנכתב שנה קודם לכן בחוק המחשבים, אשר תיקן את הוראות הפסד"פ וקבע סמכות חדירה מפורשת לחומר מחשב. במהלך השנים בוצעו מספר תיקונים בפסד"פ ובחוק האזנת סתר אשר לא יישמו המלצות מדו"ח ועדת לוין. גם חוק נתוני תקשורת משנת 2007 אינו מיישם את המלצות ועדת לוין, באשר הוא נועד להסדיר נושא ספציפי שוועדת לוין לא התייחסה אליו במפורש. דומה כי בחלוף השנים התיישן דו"ח לוין. כאמור, הוא לא ייחד כל התייחסות נפרדת לאיסוף של ראיות דיגיטליות. בנוסף לכך, גם בניסיונה של הוועדה למנות את הזכויות המוגנות הניצבות אל מול צרכי החקירה – ישנם חסרים משמעותיים. הוועדה מנתה רק את הזכות לפרטיות,

---

[25] דן ביין "הצעת חוק סדר הדין הפלילי (אמצעים משטרתיים)" **משפט פלילי, קרימינולוגיה ומשטרה** כרך א' 265 (גרשון אוריון עורך, 1986).

[26] שם, בעמ' 265, 271.

[27] דנ"פ 2316/95 **גנימאת נ' מדינת ישראל**, פ"ד מט(4) 589 (1995).

[28] ראו אהרן ברק "הקונסטיטוציונליזציה של מערכת המשפט בעקבות חוקי היסוד והשלכותיה על המשפט הפלילי (המהותי והדיוני)" **מחקרי משפט** יג 5, 21-25 (1996). ברק מנה מספר השפעות של חוקי היסוד על סדר הדין הפלילי, ובין היתר על דיני החיפוש והתפיסה. ברק ציין כי דיני החיפוש והתפיסה צריכים לקיים את דרישותיה של פסקת ההגבלה. הסטטוס קוו המשפטי לגבי מידת ההוכחה הדרושה לצורך הוצאת צו חיפוש יכול שישתנה בעקבות חקיקת חוקי היסוד, כמו גם הסנקציה הראייתית בגין איסוף ראיות שלא כדין על-ידי הרשות החוקרת. ראו עוד עמנואל גרוס "הזכויות הדיוניות של החשוד או הנאשם על פי חוק יסוד: כבוד האדם וחירותו" **מחקרי משפט** יג 155, 160-163 (1996); משה שלגי וצבי כהן **סדר הדין הפלילי** 71-77 (2000); יעקב קדמי **על סדר הדין בפלילים**, חלק ראשון (ב) 680, 722-723, 734 (2008); יורם שחר "סדר דין פלילי" **ספר השנה של המשפט בישראל** 375 (אריאל רוזן-צבי עורך, 1993). שחר התייחס לעצם תחולתו של חוק יסוד: כבוד האדם וחירותו על המשפט הפלילי הדיוני, אך עמדתו היא שהשלבים התחיליים של הליכי אכיפת החוק (ביצוע החיפוש והמעצר) חשובים פחות מההליכים המאוחרים יותר של ההליך הפלילי (שם, בעמ' 394).

ובמידה מוגבלת בלבד גם את זכות הקניין.[29] הנהנה מהזכויות החוקתיות, על פי עבודת הוועדה, הוא בעל החפץ שלגביו מבוצעת פעולת האיסוף. כפי שאראה בפרק הבא, בכל הנוגע לאיסוף ראיות דיגיטליות קיים שיח חוקתי עשיר יותר, במובן של סוג הזכויות הנוגעות בעניין וכן במובן של זהות השחקנים האוחזים באותן זכויות.

התפתחות משמעותית בהקשרנו ארעה בשנת 2014, עת פורסמה הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע״ד – 2014[30] (להלן – ״הצעת חוק החיפוש״ או ״הצעת החוק״). הצעת החוק, המסדירה את כלל דיני החיפוש, התפיסה וההמצאה, כוללת פרק נפרד לאיסוף ראיות דיגיטליות, וכפי שאראה להלן, גלומה בה מידה מסוימת של הכרה בייחודיות הראיה הדיגיטלית לעומת הראיה הפיזית.[31]

בחזרה אל הדין הקיים. אסקור בקצרה את הוראות החוק המרכזיות המכוננות את סמכויות האיסוף כלפי ראיות דיגיטליות במשפט הישראלי. כפי שאראה, החקיקה התפתחה באופן אבולוציוני מהבחנה בין שניים – חיפוש והמצאה – להבחנה בין שלושה – חיפוש, המצאה והאזנה. עם זאת, ההתפתחות האמורה מנוונת יחסית לעושר הפעולות המתבקשות לצורך התמודדות עם מאפייניה של הראיה הדיגיטלית.

<u>א) התפישה הכפולה – חיפוש והמצאה</u>

ההבחנה היסודית בדיני איסוף הראיות הייתה בין חיפוש במקום לבין המצאת מסמך. החיפוש מבוצע על-ידי הרשות החוקרת במקום פיזי מסוים.[32] לעומת זאת, ההמצאה היא פעולה שאינה מבוצעת בפועל על-ידי הרשות החוקרת. החוקר אינו לוקח את המוצג או המסמך המבוקש, אלא מקבל אותו מאדם המחזיק בו, על פי צו שיפוטי המורה לו לעשות כן,[33] או מרצונו הטוב והחופשי של אותו אדם. החיפוש וההמצאה נועדו להניב איסוף של חפצים על-ידי תפיסתם. החפצים שייתפסו, מורה המחוקק, הם אלה שרלוונטיים לצרכי חקירה, משפט, או חילוט עתידי.[34] על בסיס התפישה הכפולה האמורה, של חיפוש

---

[29] עמ׳ 1-9 לדו״ח ועדת לוין. ההתייחסות לזכות הקניין היא בעיקר בהקשר של סמכויות החילוט בסוף ההליך, ולא בהקשרים שבמוקד עיסוקי כאן, קרי שלב איסוף הראיות בתחילת החקירה.

[30] ה״ח הממשלה 867. הצעת החוק עברה בקריאה ראשונה בכנסת ה-19, ותהליך חקיקתה נקטע עקב פיזור הכנסת.

[31] ראו להלן בפרק 4(ד).

[32] ראו סעיף 23 לפסד״פ (חיפוש על פי צו בית-משפט) וסעיף 25 לפסד״פ (חיפוש שלא על פי צו בית-משפט). החיפוש יכול שיתבצע גם על גופו של אדם, לפי סעיף 29 לפסד״פ, סעיף 28(ב) לפקודת הסמים המסוכנים [נוסח חדש], התשל״ג – 1973, סעיף 5(5) לפקודת המשטרה [נוסח חדש], התשל״א – 1971, סעיף 3(ב) לחוק סמכויות לשם שמירה על ביטחון הציבור, התשס״ה – 2005.

[33] ראו סעיף 43 לפסד״פ.

[34] ראו סעיף 32(א) לפסד״פ.

EDNAKARNAVAL LIBRARY FOR THE MASSES

והמצאה, פותחו הדינים המקבילים לגבי איסוף ראיות דיגיטליות. כפי שאראה להלן סמכות החדירה לחומר מחשב עוצבה על בסיס סמכות החיפוש במקום, ואילו סמכות ההמצאה של חומר מחשב עוצבה על בסיס סמכות ההמצאה של חפצים ומסמכים.

<u>חדירה לחומר מחשב</u>: סמכות זו מוסדרת בפרק השלישי לפסד״פ, בעיקר בסעיף 23א. החדירה לחומר מחשב נתפשת, מבחינת המחוקק, כמעין מקרה פרטי של חיפוש בחצרים, זאת בראש ובראשונה לנוכח סעיף 23א(א) הקובע כי – *״חדירה לחומר מחשב וכן הפקת פלט תוך חדירה כאמור, יראו אותן כחיפוש...״*. כלומר, חדירה לחומר מחשב זוכה להתייחסות הפסד״פ כחיפוש בחצרים,[35] במספר תוספות שנועדו לייחד במידה מסוימת את החדירה לחומר מחשב.[36] נקודת המוצא של חיפוש בחצרים מציבה שתי דרישות לגבי החדירה לחומר מחשב, אשר לטענתי אינן מועילות לשרת את הזכויות של הנחפש כראוי: *האחת*, כי *״תופש הבית או המקום שמחפשים בו, או אדם מטעמו, ייתן לו להיות נוכח...״*. *השנייה*, כי תותר נוכחות שני עדים שאינם שוטרים, אלא אם מתקיימים מספר חריגים הנקובים בפסד״פ (טעמי דחיפות, היתר שיפוטי מיוחד או ויתור מצד תופש המקום על נוכחות העדים).[37]

בכל הנוגע לדרישת שני העדים, תכליתה של הדרישה להבטיח את טוהר המידות של עורכי החיפוש ואת טוהר הראיות שייאספו בחיפוש.[38] דרישת שני העדים מתאימה לחיפוש בחצרים, שם ניתן לראות בעין בלתי מזוינת האם המשטרה הורסת, משנה או שותלת ראיות. ואולם, בכל הנוגע לאיסוף ראיות דיגיטליות, דרישת נוכחות שני העדים שאינם שוטרים אינה מתאימה לערך אותו היא נועדה לשרת. החדירה לחומר המחשב היא פעולה טכנית במהותה, המצריכה ידע ייחודי. החדירה מתבצעת באמצעות תוכנות מחשב, הפועלות במהירות גבוהה, ומפיקות תוצאות לפעולתן. לא כל הפעולות

---

[35] עיון בהצעת חוק המחשבים, אשר הוסיף בתיקון עקיף את הוראת סעיף 23א לפסד״פ, מעלה כי בדברי ההסבר מכונה החדירה לחומר המחשב לא אחת בשם ״חיפוש במחשב״, וצוין מפורשות כי *״מוצע שסמכות חדירה למחשב תיעשה על פי הכללים החולשים על ביצוע חיפוש״*. ראו הצעת חוק המחשבים, התשנ״ד – 1994, ה״ח 2278, בעמ׳ 484. גם עיון בדברי-הכנסת בנוגע להצעת חוק המחשבים מעלה כי ההתייחסות לחדירה לחומר המחשב היא כאל חיפוש בחצרים עם מספר מגבלות ייחודיות. הדוברים חוזרים ומכנים את פעולת האיסוף ״חיפוש במחשב״ ולא ״חדירה לחומר מחשב״, וחוזרים ומשווים את החדירה לחומר המחשב לחיפוש בחצרים. ראו ד״כ 139, 9989 (התשנ״ד) וד״כ 143, 10817 (התשנ״ה).

[36] ראו הוראות סעיפים 23א, 26(ב), 32(ב), 32(ב1) ו-32א לפסד״פ, שם נקבע כי: (א) החדירה לחומר מחשב תיעשה על-ידי בעל תפקיד מיומן לביצוע פעולות כאמור; (ב) החדירה לא תיעשה אלא בצו בית-משפט, בשונה מחיפוש במקום שיכול להתבצע ללא צו במקרים המתאימים; (ג) צו החדירה לחומר מחשב יפרט את מטרות החיפוש ותנאיו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש; (ד) יש להאריך את התפיסה הראשונית של מחשב מוסדי תוך 48 שעות, ואילו מחשב שאינו בשימושו של מוסד – יש להאריך את תפיסתו הראשונית בחלוף 30 יום, אלא אם כן מתכוונים להשתמש במחשב כראיה או לחלטו; (ה) למחזיק במחשב קמה זכות לקבלת העתק מחומר המחשב שנתפס ממנו תוך 4 ימים ממועד התפיסה, כאשר קיימות סמכויות לקצין משטרה ולבית-המשפט להשהות את מסירת ההעתק.

[37] ראו סעיף 26(א) לפסד״פ; ב״ש (מחוזי י-ם) 1153/02 **מדינת ישראל נ׳ אברג׳יל**, תק-מח 02(2) 3784, 3795 (2002) (שם חייב בית-המשפט את המשטרה לבצע חדירה למחשב תפוס בנוכחות שני עדים מטעמו של החשוד, אחד מהם אף יכול שיהיה מומחה מחשבים); ב״ש (שלום י-ם) 7458/02 **מועדון יוניק אינטרנט נ׳ משטרת ישראל**, תק-של 02(4) 13841, 13845 (2002).

[38] ב״ש (מחוזי ת״א) 91637/03 **אופיר נ׳ ימ״ר ת״א**, תק-מח 03(2) 7390, 7395 (2003).

מוצגות על מסך או ניתנות לצפייה והבנה, בוודאי לא על-ידי עין בלתי-מיומנת. היכולת לשמור באורח נאות על טוהר המידות של שוטר רשלן או כזה המשתיל ראיות בזדון – מוגבלת משמעותית במקרה של חדירה לחומר מחשב. לעומת זאת, פעולה בדיעבד, של בחינת מאפיינים של החומר האגור במחשב שנתפס, ואולי גם הטלה של חובות תיעוד מוגברות על פעולות החדירה לחומר המחשב, יאפשרו השגה של אותן מטרות של פיקוח מפני שתילת ראיות, שינוין או מחיקתן מבלי משים וכיוצא בזה. לסיכום, ההפניה בדיני החדירה לחומר מחשב אל דרישת נוכחות שני העדים מגלמת תפישה פיזית, לפיה החדירה לחומר המחשב שקולה לחיפוש פיזי, ולא היא.

הדברים שהובאו לעיל יפים גם לעניין הדרישה שתופש המקום בו נערך החיפוש יהיה נוכח בו. גם כאן, לא ברור במה תועיל נוכחותו של המחזיק במובן של פיקוח על פעולות השוטרים. מעבר לכך, לא ברור כלל מיהו ה"תופש" עליו מדברת הוראת הפקודה, כאשר באים "להעתיק" את ההוראה ולהחילה על חדירה לחומר מחשב: הלא בכל הנוגע למחשבים ישנה אבחנה מובהקת בין מחזיק המקום בו נמצא חומר המחשב, לדוגמה ספקי שירותי אירוח או אחסון למיניהם, לבין המשתמש בפועל בחומר המחשב, כגון מנהלי אתרים או משתמשי שירות אחסון קבצים. על פניו, לא ברור מה תהיה התועלת המהותית בעצם נוכחות תופש המקום בשלבי ההעתקה והחיפוש הממוחשבים.

בטרם אעבור להמצאת חומר מחשב, אציין כי התפישה הפיזית ביחס לפעולת החדירה לחומר מחשב, אינה נחלתו של המשפט הישראלי בלבד. גם במשפט האמריקני, למשל, זוהתה תפישה פיזית ביחס לאופן בו מוסדרת חוקית הפעולה של חדירה לחומר מחשב. דיני החדירה לחומר מחשב פותחו במשפט האמריקני לאורו של התיקון הרביעי לחוקה האמריקנית המעניק הגנה מפני Unreasonable Search and Seizure. מלים אלה כוונו לחפצים ומקומות, לא למידע.[39]

<u>המצאת חומר מחשב</u>: הסמכות כולה מוסדרת בסעיף 43 לפסד"פ. הסעיף לאקוני למדי וזה נוסחו:

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

הסעיף מתייחס למעשה באופן כללי להצגת חפצים, כאשר חוק המחשבים תיקן בשנת 1995 את הגדרת "חפץ" שבסעיף 1 לפסד"פ, כך שיכלול גם חומר מחשב. בכך, הפך סעיף 43 לפסד"פ – אשר לא תוקן

[39] ראו: Orin Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L. J. 85 (2005).

EDNAKARNAVAL LIBRARY FOR THE MASSES

בעצמו מאז שנת 1969 עת נערך הנוסח החדש לפסד"פ[40] – למקור הסמכות להמצאת חומר מחשב, להוציא את המקרה הפרטי של נתוני תקשורת המוסדר החל משנת 2007 בחוק נפרד ויפורט להלן. בשונה מחדירה לחומר מחשב, הכוללת דרישות נוספות מעבר לאלו המנויות לגבי חיפוש בחצרים, הרי שבמקרה של המצאת חומר מחשב, אין כל דרישה ייחודית או נוספת אל מול המצאת חפץ שאינו חומר מחשב. הסעיף למעשה מדבר על הצגה או המצאת חפץ, ולכאורה לא נובעת ממנו הסמכות לתפוס את החפץ המוצג ולשלול אותו מאת מחזיקו, אבל הפרקטיקה הנוהגת היא שהמשטרה תופסת ראיות באמצעות סעיף זה כתחליף לשימוש בצו חיפוש.[41]

מקרה פרטי של סעיף 43 לפסד"פ, ביחס ל"נתוני תקשורת",[42] מטופל במפורט בחוק נתוני תקשורת. במלים אחרות, כל המצאה של חפץ וכן של ראיות דיגיטליות תיעשה לפי סעיף 43 לפסד"פ, למעט המצאה של נתוני תקשורת, אשר יכול שתיעשה לפי חוק נתוני תקשורת בלבד (ככתוב בסעיף שמירת הדינים – סעיף 12 לחוק).[43] חוק נתוני תקשורת מבטא גישה המשוחררת במידה מסוימת מכבלי ה"פיזיות" ביחס לנתוני התקשורת. לפיכך, נקבעו בחוק סמכויות המכירות בתכונת הנדיפות של הראיה הדיגיטלית ובתכונתה כראיה מצטברת: הסמכות לקבלת נתוני תקשורת בהיתר מנהלי במקרים דחופים מאפשרת בנסיבות המנויות בחוק להתגבר על בעיית הנדיפות של הראיה הדיגיטלית;[44] הסמכות לקבלת נתוני תקשורת עתידיים (לפרק זמן של עד 30 יום קדימה) מאפשרת להתמודד עם

---

[40] להשלמת התמונה אציין כי גם הנוסח החדש בשנת 1969 התבסס על הנוסח המנדטורי משנת 1942, ולפיו: "אם סבור שופט שלום כי יש צורך או כי רצוי להראות כל מסמך או כל דבר אחר לשם כל חקירה, דרישה, או משפט, יכול הוא להוציא כתב הזמנה לכל אדם אשר, לפי הסברא, נמצא המסמך או הדבר בחזקתו או ברשותו, ובו יהא נדרש האיש לבוא ולהראותם או לדאוג להראייתם בזמן ובמקום שצוינו בכתב ההזמנה". ראו פקודת סדר הדין הפלילי (מעצר וחיפוש), חא"י כרך א', ל"ג 431, סעיף 15.

[41] ראו רע"פ 8600/03 **מדינת ישראל נ' שרון**, פ"ד נח(1) 748, 759-760, 767-768 (2003), שם מציין בית-המשפט את הפרקטיקה האמורה. הפרקטיקה מתאפשרת לנוכח סעיף 32 לפסד"פ, הקובע את סמכות התפיסה כסמכות עצמאית לעומת סמכות החיפוש.

[42] "נתוני תקשורת" מוגדרים בסעיף 1 לחוק, הן על דרך החיוב והן על דרך השלילה: נתוני תקשורת הם אחד משלושת אלה – נתוני מנוי, נתוני תעבורה ונתוני מיקום; כמו כן, נתוני תקשורת, בכל מקרה, לא יכללו נתוני תוכן. היסוד השלילי נועד לבדל את נתוני התקשורת מהאזנת סתר מחד גיסא ומהמצאת חומר מחשב אחר שאינו נתוני תקשורת מאידך גיסא, ולמנוע בכך עירוב תחומין. בכל זאת נודעו מצבים לא-ברורים, כגון כתובת URL, אשר לכאורה נדמית כנתון תקשורת, אך למעשה היא מאפשרת חשיפה לתוכן. ראו, לעניין זה, 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).

[43] יצוין כי החוק מסמיך את הרשות החוקרת לקבל נתוני תקשורת ממאגרים של בעלי רישיון בזק בלבד. כאלה הם למשל חברות הטלפון הקווי, הבין-לאומי והסלולרי וספקיות הגישה לאינטרנט. ומה באשר לנתוני תקשורת המצויים אצל מי שאינם בעלי רישיון בזק, כדוגמת מנהלי אתרי אינטרנט מכל סוג שהוא, ספקי שירותי דוא"ל, ספקי שירותי VoIP (Voice over IP)? אלה אינם כלולים בחוק נתוני תקשורת מחד גיסא, ומאידך גיסא, בשל אופן הניסוח של סעיף שמירת הדינים בחוק נתוני תקשורת, הם אף אינם כלולים – כבעבר – בסעיף 43 לפסד"פ. נוצרה כאן למעשה לאקונה בחוק, אשר אינה מגלמת להערכתי כל הכרעה מכוונת, אלא מדובר בטעות בהליך החקיקה אשר טעונה תיקון. כתוצאה מן הלאקונה האמורה נשללת לכאורה האפשרות – בכל תנאי – להסמיך את הרשות החוקרת לאסוף נתוני תקשורת ממי שאינם בעלי רישיון בזק, וזאת, ניתן להניח, בלי כוונת מכוון. הנחיית פרקליט המדינה בנושא נתוני תקשורת מורה כי במקרה של פנייה למי שאינו בעל רישיון בזק לצורך קבלת נתוני תקשורת, יחול סעיף 43 לפסד"פ, אולם הרשות החוקרת תטיל על עצמה מגבלות נוספות כרוחו של חוק נתוני תקשורת. ראו "קבלת נתוני תקשורת" **הנחיות פרקליט המדינה** 7.6 (התשע"ב).

[44] סעיף 4 לחוק נתוני תקשורת. על פי סעיף 4(א) התנאים להיתר מנהלי כאמור הם כי מדובר במניעת עבירה מסוג פשע, גילוי מבצעה או הצלת חיים. בנוסף, על פי הסעיף, התנאי להיתר מנהלי הוא כי מדובר ב"צורך, שאינו סובל דיחוי". הצורך שאינו סובל דיחוי יכול להיות, על פי לשון הסעיף, גם חשש מפני התנדפות הראיה.

EDNAKARNAVAL LIBRARY FOR THE MASSES

ראיות מצטברות הנאגרות על בסיס קבוע.[45] גם הניסיון של חוק נתוני תקשורת להבנות את שיקול הדעת המשטרתי בעת הגשת הבקשה לצו ואת שיקול הדעת השיפוטי בעת הוצאת הצו השיפוטי המסמיך – מתקדם באופן משמעותי מזה שמופיע ביחס לחדירה לחומר מחשב וביחס להמצאת חומר מחשב,[46] ומגלם הכרה מפותחת יותר בזכויות החוקתיות העתידות להיפגע כתוצאה מפעולות האיסוף שמכוח החוק.[47]

ב) מתפישה כפולה לתפישה משולשת – חיפוש, המצאה והאזנה

בשנת 1979 נחקק חוק האזנת סתר הישראלי. החוק הכיר בכך שלצד חפצים ומסמכים, אותם ניתן לתפוס במסגרת חיפוש או כתוצאה של צו המצאה, יש מקום להכיר במידע נוסף בעל חקירתי שמטבעו הוא במצב תקשורתי. איסופו של מידע זה הוא על דרך של יצירת תיעוד, קליטת המידע בעת מעברו,

---

[45] סעיף 3(י) לחוק נתוני תקשורת.

[46] אשר לצו לקבלת נתוני תקשורת, החוק מציב את התנאים כדלקמן: (1) החשד צריך להיות לגבי עבירה מסוג עוון או פשע (בסיס עבירות רחב יחסית); (2) דרישת תכלית: הצלת חיי אדם או הגנה עליהם; גילוי עבירות, חקירתן או מניעתן; גילוי עבריינים והעמדתם לדין; חילוט רכוש על פי דין. על השופט להשתכנע שהצו המבוקש ישרת את אחת התכליות הנ״ל, אולם אין דרישה להוכחת רמת חשד מסוימת לעצם קיומה של עבירה או הסתברות להתרחשותה של עבירה עתידית (סעיף 3(א)); (3) הגורם השיפוטי המוסמך הוא שופט שלום (סעיף 2(א)); (4) על הבקשה לצו לקבלת נתוני תקשורת להיחתם על-ידי קצין משטרה מכל דרגה שהיא שהוסמך לעניין זה על-ידי מפכ״ל המשטרה (סעיף 3(א)); (5) החוק מַבנה את אופן הגשת הבקשה לצו לקבלת נתוני תקשורת (סעיף 3(ד)): הבקשה תוגש בכתב ותיתמך בהצהרה לאחר אזהרה או בתצהיר של המבקש (סעיף 3(ג)). יש לציין את העובדות המקנות סמכות לבית-המשפט, פרטי קצין המשטרה מגיש הבקשה, תמצית העובדות והמידע עליו מבוססת הבקשה, התכלית הרלוונטית, סוג נתוני התקשורת המבוקשים, פרק הזמן לגביו מבוקשים נתוני התקשורת (צופה פני עבר או צופה פני עתיד), פרטי הזיהוי של המנוי או המתקן לגביו מבוקשים הנתונים, ניתן להגיש חומר חסוי לתמוך בבקשה. לבקשה יש לצרף החלטות בבקשות קודמות לקבלת נתוני תקשורת והעתקים מן הבקשות הקודמות ופרוטוקולים של הדיונים בבקשה ככל שאלה נדונו בפני בית-משפט אחר (למעט במקרים דחופים – לפי הוראת סעיף 3(ו)(2)); (7) הצו יכול לחול על קבלת נתוני תקשורת עתידיים ל-30 יום לכל היותר, לפי הוראת סעיף 3(ז) סיפא לחוק, וניתן להאריך את התקופה או לבקש צווים נוספים לאחר מכן, לפי סעיף 3(יא); (8) ישנו ניסיון להבנות את שיקול דעתו של השופט הדן בבקשה (סעיף 3(ז)): על בית-המשפט להתחשב בתכלית המבוקשת וכיצד הצו יוכל לתרום למימושה של התכלית, במידת הפגיעה בפרטיותו של אדם, בחומרת העבירה ובסוג נתוני התקשורת המבוקשים. הבניה נוספת של שיקול דעתו של השופט מופיעה בסעיף 3(א) אמצע וסיפא לחוק ולפיה על השופט לפרט את האופן בו תקבל הרשות החוקרת את נתוני התקשורת. כן נקבע שלא תותר מסירת נתוני התקשורת אם יש בכך כדי ״לפגוע, במידה העולה על הנדרש, בפרטיותו של אדם״. דהיינו, הוכנסה התיבה של המידתיות החוקתית, זאת ביחס לזכות לפרטיות בלבד; (9) ישנה הבניה של הצו עצמו, כאשר הבניה זו אמורה להשליך מן הסתם על שיקול דעתו של השופט בעת מתן הצו: יש לפרט נימוקים למתן הצו (מותר לחסות את הנימוקים מפני הנמען לצו), סוג נתוני התקשורת שאושרו, זהות המתקן לגביו יתקבלו נתוני התקשורת ככל שהם ידועים, פרק הזמן לגביו תותר הקבלה של נתוני התקשורת, מועד מתן הצו ותום תוקפו, כאשר לכל היותר ניתן להוציא צו בתוקף ל-30 יום, ואת התקופה ניתן להאריך מעת לעת (סעיף 3(ח)-3(יא)); (10) בכל הנוגע לצו ביחס לנתוני תקשורת של בעלי מקצועות חסויים על פי כל דין, ישנן דרישות נוספות: יש לציין במפורש בבקשה האם המנוי שלגביו מבוקשים נתוני התקשורת שייך לבעל מקצוע חסוי על פי כל דין (סעיף 3(ד)(7) לחוק נתוני תקשורת); כן יש למסור ״פירוט ברור״ בבקשה על כך שיש חשד שבעל המקצוע החסוי מעורב בעבירה נשואת הבקשה (סעיף 3(ב) לחוק); על בית-המשפט לשקול את היות בעל המנוי מי שנהנה מחיסיון על פי דין (סעיף 3(ז) לחוק); בשונה מהחובה הרגילה של השופט לנמק את מתן הצו לנתוני תקשורת, במקרה של בעל מקצוע חסוי עליו למסור ״נימוקים מפורטים״ (סעיף 3(ח)(1)); בשונה מהמקרה הרגיל, בו לא נדרש להוכיח את רמת החשד לביצוע העבירה, כאן נדרשת הוכחה ברמה של ״יסוד לחשד״ שבעל המקצוע החסוי מעורב בעבירה.

חוק נתוני תקשורת נתקף על-ידי האגודה לזכויות האזרח ולשכת עורכי-הדין כבלתי-חוקתי מחמת היותו פוגע יתר על המידה בזכות לפרטיות, זאת על בסיס הטיעונים הבאים: (א) נטען כי הסמכויות בחוק צריכות להימסר רק לגבי עבירות מסוג פשע; (ב) על החוק לדרוש ״חשד סביר״ כתנאי לקבלת נתוני תקשורת, שכן עתה הוא מאפשר קבלתם לצרכים מודיעיניים כלליים; (ג) אין לאפשר קבלה של נתוני תקשורת לגבי בעלי מקצועות חסויים המעורבים בעבירה בהיתר מנהלי אלא בהיתר שיפוטי בלבד; (ד) אין לאפשר, במסגרת העברת מאגר הבעלויות על מספרי הטלפון, הקבועה בחוק, גם העברה של מספרי טלפון ״חסויים״, שבעליהם ביקשו שלא יפורסמו לכלל הציבור; (ה) היה מקום לקבוע סעיף פסלות ראיות עצמאי בחוק בדומה לזה הקבוע בסעיף 13 לחוק האזנת סתר. בית-המשפט העליון, בהרכב מורחב, דחה את העתירות. ראו בג״ץ 3809/08 **האגודה לזכויות האזרח בישראל נ׳ משטרת ישראל**, תק-על 12(2) 3622 (2012). עם זאת, בית-המשפט העליון קבע כי יש לפרש בצמצום ובקפדנות את הסמכויות מכוח החוק.

[47] ארחיב עוד על סוגיית ההבניה של שיקול-הדעת בעת ההסמכה לביצוע פעולות איסוף של ראיות דיגיטליות, להלן בפרק 6(ה)(3).

EDNAKARNAVAL LIBRARY FOR THE MASSES

ולא על דרך של העתקת המידע כשהוא במצב "נייח".[48] פעולת האזנת הסתר נתפשת, על פי המבחנים שמציב החוק לרשות החוקרת, כפעולה הפוגענית ביותר, ולפיכך הוצבו ערובות פרוצדוראליות-פורמליסטיות קפדניות יחסית כדי לאשר פעולת חקירה זו.[49] גם ברמת הפסיקה ניתן לציין את חוק האזנת סתר כנבדל מבחינת עוצמת ההגנה על הזכות לפרטיות.[50]

---

[48] מעניינת במיוחד ההתפתחות בעניין זה במשפט האמריקני. האזנת הסתר צמחה מתוך הגנת התיקון הרביעי לחוקה האמריקנית, המגן מפני חיפושים בלתי סבירים. ראו: Katz v. United States, 389 U.S. 347 (1967). הפסיקה בעניין *Katz* הפכה פסיקה קודמת משנת 1928, בה נקבע לגבי האזנת סתר טלפונית, כי אינה מהווה חיפוש, באשר אינה מתבצעת בחצריו של אדם, ועל כן אינה מצריכה הסמכה שיפוטית או אחרת. ראו: Olmstead v. United States, 277 U.S. 438 (1928). דעת המיעוט של השופט ברנדייס בעניין *Olmstead* הפכה 39 שנים מאוחר יותר לדעת הרוב בעניין *Katz*. לאחר הפסיקה בעניין *Katz* נחקק בשנת 1986 ה-ECPA, ר"ת של Electronic Communications Privacy Act אשר קודד בסעיפים 2510-2522 ל-Title 18 של ה-.U.S.C. כאן כבר מגולמת הכרה מפורשת בהאזנת סתר כקטגוריה נפרדת מחיפוש.

[49] אפרט על הבלמים שמציב החוק בשלב הגשת הבקשה לצו האזנת סתר ובשלב הוצאת הצו: (1) החשד צריך להיות לגבי עבירה מסוג פשע (סעיף 6(א)). (2) דרישת תכלית: גילוי, חקירה או מניעה של עבירות; גילוי או תפיסה של עבריינים; חקירה לצרכי חילוט (סעיף 6(א)), כאשר על השופט להשתכנע שההאזנה תשרת את אחת מהתכליות האמורות. (3) צו האזנת סתר יכול שיוצא על-ידי נשיא בית-משפט מחוזי או סגנו שמינה לכך (סעיף 6(א)). (4) על הבקשה לצו האזנת סתר יכול לחתום קצין משטרה בדרגת ניצב משנה (נצ"מ) בלבד אשר הוסמך לעניין האזנות סתר על-ידי מפכ"ל המשטרה (סעיף 6(א)). (5) הבקשה לצו האזנת הסתר מובנה על-ידי ניסוח הטופס במסגרת התוספת לתקנות האזנת סתר (בקשה להיתר האזנה), התשס"ח – 2007. הבקשה צריכה לכלול התייחסות לפרטי החשוד, או קו הטלפון או המקום שלגביו מבוקשת ההאזנה; מהות החשדות וסעיפי העבירה; פירוט התכלית שלשמה מבוקשת ההאזנה; משך ההאזנה המבוקשת; סוג ההאזנה; דרך ההאזנה המבוקשת; פרטי קצין המשטרה החתום על הבקשה. לבקשה יש לצרף את הבקשות הקודמות הנוגעות לאותו אדם באותו תיק חקירה, ההחלטות בבקשות אלה והחומר שהוצג לבית-המשפט במסגרת הדיונים בבקשות אלה (תקנה 4(ג)). (6) בדיון בבקשה, במעמד צד אחד, בפני השופט המוסמך, יתייצב קצין משטרה בדרגת סגן ניצב (סנ"צ) ומעלה (סעיף 6(ב)). (7) הצו יכול לעמוד בתוקף לשלושה חודשים לכל היותר, וניתן להאריכו מעת לעת (סעיף 6(ה)). (8) הצו עצמו מובנה במידה מסוימת, באופן הבא: יש לתאר את זהות המואזן, או זהות הקו המואזן, וכן מקום ביצוע השיחות וסוגן. כן יש לתאר את דרכי ההאזנה שהותרו. גם תקנות האזנת סתר מבנות למעשה את הצו עצמו על-ידי קביעת הטופס, כולל קביעת רובריקה למילוי נימוקים ההחלטה להיענות או לסרב לבקשה להאזנת סתר. התייחסות ספציפית צריכה להינתן בצו לשאלה האם תותר כניסה למקום על מנת להתקין את ציוד ההאזנה, לפרקו או לסלקו. ככל שתותר כניסה כאמור, על הצו יפרט את המקום האמור (סעיף 10א).

קיימות דרישות נוספות לאחר ביצוע הצו: (1) קיימת חובת דיווח חודשי של מפכ"ל המשטרה ליועץ המשפטי לממשלה על כמות צווי האזנת הסתר שניתנו, כמו גם עם צווי האזנת סתר לגבי בעלי מקצועות חסויים על פי דין ולגבי חברי-כנסת (סעיף 6(ו)). (2) קיימת חובת דיווח שנתי של השר לביטחון פנים ליו"ר ועדת חוקה, חוק ומשפט של הכנסת על מספר הבקשות ומספר ההיתרים שניתנו לצווי האזנת סתר למטרות פליליות (סעיף 6(ז)). חובת דיווח זו אינה חלה לגבי האזנות למטרות הגנה על ביטחון המדינה.

החוק מחריג שתי קבוצות מן הכלל – הקבוצה האחת היא של חברי-כנסת מואזנים (ראו חוק חסינות חברי הכנסת, זכויותיהם וחובותיהם (תיקון מס' 32), התשס"ד – 2005, ס"ח 1991 עמ' 260, אשר קבע את הוראת סעיף 2א לחוק) והקבוצה השניה היא של בעלי מקצועות חסויים מואזנים (ראו סעיף 9א לחוק האזנת סתר), כשהכוונה לבעלי המקצועות המנויים בסעיפים 48-51 לפקודת הראיות [נוסח חדש], התשל"א – 1971 בלבד (עורך-דין, רופא, פסיכולוג, עובד סוציאלי וכהן דת) (להלן – "פקודת הראיות"). ההחרגה באה לידי ביטוי ב – (1) טיב העבירות אשר בגינן ניתן להתיר האזנת סתר למואזנים הנמנים על שתי קבוצות אלה; (2) רמת החשד הנדרשת היא "יסוד לחשד"; (3) צמצום תכליות ההאזנה המותרות; (4) הכבדה בהליך אישור עצם הגשת הבקשה לבית-המשפט; (5) קביעה כי דרך ההאזנה המותרת תהיה בהקלטה בלבד, אלא אם כן קבע השופט אחרת מטעמים מיוחדים שיירשמו, וכי השופט יבצע את העיון והסינון הראשוניים של חומר החקירה הרלוונטי. עוד שלוש הוראות ייחודיות מבדלות את חברי-הכנסת לחומרה אף יותר מבעלי המקצועות החסויים: (6) העלאה נוספת של הדרג השיפוטי שמאשר את הצו: לא עוד נשיא בית-משפט מחוזי או סגנו שמונה לכך, אלא שופט של בית-המשפט העליון; (7) העלאה של הדרג המשטרתי המופיע בבקשה להאזנת הסתר: לא עוד קצין בדרגת סנ"צ אלא קצין בדרגת נצ"מ ומעלה; (8) במקרה של האזנה כדין למואזן שאינו ח"כ, אשר עלתה בה אגב אורחא שיחה עם ח"כ, תופסק ההקשבה לשיחה, ותובא לעיון השופט שנתן את ההיתר. ההקלטה לא תתומלל, והשופט יחליט מה לעשות עם ההקלטה. כאמור, הוראה מקבילה אינה קיימת לגבי האזנת סתר אגב אורחא לבעלי מקצועות חסויים, אולם המשטרה נוהגת כך בפועל גם לגביהם: ראו דין וחשבון ועדת החקירה הפרלמנטרית בעניין האזנות סתר, התשס"ט – 2009, בעמ' 23-25. כן ראו פרוטוקול מס' 9 של ועדת החקירה הפרלמנטרית בנושא האזנות סתר (11.11.2007), המצוי ב: http://www.knesset.gov.il/protocols/data/html/wiretapping_inq/2007-11-11.html, שם מובאים דברים מתוך דין וחשבון של משרד המשפטים לבדיקת משטר האזנות הסתר בראשות המשנה ליועץ המשפטי לממשלה, עו"ד לבנת משיח. המלצות דו"ח לבנת משיח גובשו לכדי הצעות חוק שטרם הוכרע בהן בוועדת החוקה, חוק ומשפט של הכנסת. ראו הצעת חוק האזנת סתר (תיקון מס' 5), התשס"ח – 2008, ה"ח הממשלה 397, סעיף 5 וכן דברי ההסבר הכלליים להצעת-החוק; הצעת חוק האזנת סתר (תיקון מס' 6), התשס"ט – 2009, ה"ח הממשלה 455, סעיף 5 וכן דברי ההסבר הכלליים להצעת-החוק.

[50] כך, בעניין *נחמיאס*, מנה בית-המשפט העליון כמה נקודות בנוגע לשיקול-הדעת השיפוטי בעת שקילת בקשה לצו האזנת סתר: (א) חומרת העבירה; (ב) האפשרות להשיג את התוצאה החקירתית המקווה באמצעות סמכויות איסוף פוגעניות פחות; (ג) רמת החשד נגד המואזן הפוטנציאלי; (ד) בירור פוטנציאל האזנה לצדדים שלישיים נוספים על המואזן; (ה) בירור ממדיה של הפגיעה העודפת בפרטיות העתידה להיווצר כתוצאה מאישור צו ההאזנה; (ו) בירור ההצדקות לגבי משך תקופת

EDNAKARNAVAL LIBRARY FOR THE MASSES

כמו במקרה של חדירה לחומר מחשב, שהורכבה על הבסיס של חיפוש במקום, גם האזנת סתר לתקשורת בין מחשבים הורכבה על הבסיס של חוק האזנת סתר הכללי (לתקשורת טלפונית ולשיחה בעל פה), זאת בתיקון לחוק משנת 1995.[51] חוק האזנת סתר מניח כי תקשורת בת-האזנה כוללת העברה בו-זמנית של מידע מהשולח אל המקבל,[52] דהיינו שהמידע מגיע למקבל בו-זמנית עם יציאתו מהשולח, כפי שמתרחש בעת ביצוע שיחת טלפון או בעת שיחה בעל פה בין שני אנשים או יותר. "חומר המחשב" נתפש אפוא בחקיקה הישראלית כבעל שני מצבי צבירה דיכוטומיים: מצב אחד שבו הוא אגור במחשב כ"חפץ", שאז הוא בר-חדירה (על-ידי הרשות החוקרת) או בר-המצאה (על-ידי צד שלישי), ומצב שני מנוגד שבו הוא נמצא בתקשורת בין מחשבים, שאז הוא בר-האזנה. החלוקה המשולשת ביחס לסמכויות האיסוף – חיפוש (לרבות חדירה לחומר מחשב), המצאה (לרבות המצאת חומר מחשב) והאזנה (לרבות לתקשורת בין מחשבים) – מקובלת גם במשפט האמריקני.[53]

<u>ג) כשלי סיווג כתוצאה מהתפישה המשולשת</u>

כתוצאה מהחלוקה הקשיחה-יחסית לשלוש קטגוריות של פעולות איסוף – חיפוש, המצאה והאזנה – נוצרים כמה כשלי סיווג ביחס לראיות דיגיטליות. אעמוד על שלושה: *האחד*, ביחס למעמדה של פעולת "מעקב חיי" אחר גלישות באינטרנט; *השני*, ביחס למעמדה של קליטת פעולות אוטומטיות של תקשורת בין-מחשבים; *השלישי*, ביחס למעמדה של פעולת איסוף של מידע העובר בתקשורת א-סינכרונית. כפי שאראה, ביחס לשתי הפעולות הראשונות, מקובל לסווגן כפעולות של האזנת סתר, הגם שבמהותן אין המדובר ב"שיחה" במובן של העברת מסרים הדדית בין שני אנשים או יותר. ביחס לפעולה השלישית, כשל הסיווג הוא מכיוון אחר: אמנם מדובר בהעברת מסרים בין שני אנשים או יותר, אולם קיימת אי בהירות ממשית ביחס ל"שיבוץ" של פעולת האיסוף האמורה: האם צריכה להיות ממוקמת בקטגוריית ההמצאה על-ידי ספק שירותי התקשורת או בקטגוריית האזנת הסתר?

ההאזנה. בית-המשפט העליון מדגיש כי השימוש באמצעי החריג של האזנת סתר צריך להיעשות במשורה, וניכרת התייחסות בעיקר לפרטיותו של יעד ההאזנה ולפרטיותם של צדדים שלישיים. ראו ע"פ 1302/92 **מדינת ישראל נ' נחמיאס**, פ"ד מט(3) 309, 331-333 (1992). ראו עוד את פסק-דינו של הנשיא ברק בע"פ 1668/98 **היועץ המשפטי לממשלה נ' נשיא בית המשפט המחוזי בירושלים**, פ"ד נו(1) 625 (1998), בו הוא מעביר את צו האזנת הסתר שעמד לערעור תחת שבט הביקורת של מבחני המידתיות החוקתיים. כן ראו הניתוח בדו"ח ועדת החקירה הפרלמנטרית בעניין האזנות סתר, שם, בעמ' 5-12.

[51] בשנת 1995 הוספה התיבה "בתקשורת בין מחשבים" להגדרת "שיחה" בסעיף 1 לחוק האזנת סתר, התשל"ט - 1979. ראו גם לעיל ה"ש 22.

[52] כך על פי פסיקת בית-המשפט העליון בע"פ 1497/92 **מדינת ישראל נ' צוברי**, פ"ד מז(4) 177, 194-198 (1992). בין היתר פסק בית-המשפט העליון כי: *"פשוטו של מקרא ותכליתו של דבר החקיקה מצביעים על כך שהמדובר בהאזנה לשיחה או בהקלטתה, בעת קיום השיחה, היינו על פעולות המתבצעות בו-זמנית עם קיומה של השיחה"*. דרישת הבו-זמניות הוכרה גם בפסיקה האמריקנית: United States v. Turk, 526 F.2d 654 (5th Cir. 1976).

[53] אורין קֶר (Kerr) מיין את סמכויות האיסוף במשפט האמריקני באותו אופן. ראו: Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 293-299 (2005).

<u>1) מעמדן של גלישות באינטרנט</u>

הקושי הפרשני ביחס למעמדן של גלישות באינטרנט נובע מהגדרת "שיחה", שהיא מושא ההאזנה. "שיחה" מוגדרת בסעיף 1 לחוק כך: *""שיחה" – בדיבור או בבזק, לרבות בטלפון, בטלפון אלחוטי, ברדיו טלפון נייד, במכשיר קשר אלחוטי, בפקסימיליה, בטלקס, בטלפרינטר או בתקשורת בין מחשבים"*. ההגדרה חסרה מרכיב משמעותי, הנראה אינטואיטיבית כמחויב המציאות, המבהיר מהי "שיחה" להבדיל מההגדרה כיצד מבצעים את ה"שיחה". וכך, למשל, ניתן היה לצפות שההגדרה תציין ש"שיחה" הינה חילופי דברים בין שני אנשים ויותר או כדומה.[54]

בעידן האינטרנט צפה ועולה שאלה ייחודית: מה דינן של גלישות באינטרנט, שאינן כוללות החלפת מסרים בין שני אנשים או יותר? בגלישות באינטרנט הכוונה לפעולות כמו שאילתות חיפוש במנוע חיפוש, קריאה באתר אינטרנט חדשותי (כדוגמת Ynet), עיון בחשבון בנק פרטי של משתמש האינטרנט, צפייה בטלוויזיה (IPTV) או האזנה למוסיקה דרך האינטרנט, וכדומה. הגלישות באינטרנט הן פעולות עצמיות שמבצע משתמש האינטרנט. הן כוללות באופן פורמלי תקשורת בין מחשבים, אולם הן אינן כוללות תקשורת ישירה בין אנשים, כי אם תקשורת בין אדם מצד אחד לבין מחשב מצד שני. יש לשים לב שבדוגמאות אלה של גלישות באינטרנט כלולות שתי תת-קטגוריות: *האחת*, גלישות באתרים פתוחים לכלל הציבור (כדוגמת Ynet); *השנייה*, גלישות במסגרת "סגורה" (כדוגמת הכניסה לחשבון הבנק האינטרנטי או הקלדת מילות חיפוש במנוע חיפוש).

<u>2) מעמדן של פעולות אוטומטיות של תקשורת בין-מחשבים</u>

קיימת קטגוריה נוספת של פעולות בתקשורת בין-מחשבים, אשר נכללות באופן פורמלי בהגדרה של "שיחה" בחוק האזנת סתר, הגם שאין בהן משום החלפת מידע בין שני אנשים או יותר. הכוונה למצבים בהם מחשב המחובר לאינטרנט ולשירותים מסוימים, מקיים התקשרות עם אתר אחר לצורך קבלת עדכוני גרסאות, בדיקות תקינות התקשורת, פעולה של "עוגייה" (Cookie) שהושתלה במחשב או כדומה. במצבים אלה, ההתקשרות היא בין שני מחשבים (כאמור, בקטגוריה של גלישות באינטרנט ההתקשרות היא בין אדם, באמצעות מחשב, לבין מחשב). יתר על כן, ההתקשרות מתבצעת באופן אוטומטי, פעמים רבות בלא יוזמתו של מי ממשתמשי המחשב, ולעתים אף בלא ידיעתם.

---

[54] עיון בהצעת חוק האזנת סתר, התשל"ט – 1979 ובהצעת החוק לתיקון מספר 1 לחוק האזנת סתר, אשר הרחיבה כאמור את הגדרת ה"שיחה" גם ל"תקשורת בין מחשבים", מלמדים כי ההנחה הסמויה של המחוקק הינה כי "שיחה" כוללת חילופי דברים בין שני אנשים ויותר. התכלית של החוק היא להגן על "סוד שיח". ראו דברי ההסבר להצעת החוק המקורית, שנקראה הצעת חוק דיני העונשין (האזנת סתר), התשל"ח – 1978, ה"ח תשל"ח 1361. ראו גם: הצעת חוק האזנת סתר (תיקון), התשנ"ד – 1994, ה"ח התשנ"ד 2292.

3) מעמדה של תקשורת א-סינכרוניות

כאמור, המידע הממוחשב נתפש בדין הפוזיטיבי הנוכחי בישראל כבעל שני מצבי צבירה אפשריים: מצב "נייח" ומצב "נייד", קרי מצב שבו דינו כדין "חפץ" ומצב שבו דינו כדין "שיחה". ואולם, בעולם התקשורת, בפרט בעידן האינטרנט, מוכרים יצירי כלאיים, של תקשורת א-סינכרונית. בתקשורת הא-סינכרונית לא מתקיימת בו-זמניות בין מועד יציאת המסר לבין מועד קליטתו אצל הנמען.[55] בין צורות התקשורת הא-סינכרוניות המוכרות לנו כיום ניתן למנות, כדוגמה, את הדוא"ל, מסרון ה-SMS (הודעת טקסט) או ה-MMS (הודעה עם תמונה), הודעה בתא-קולי טלפוני והעברת הקבצים באמצעות שרת FTP. נוסף על אלה, קיימות צורות נוספות של תקשורת א-סינכרונית ובהן כל הפלטפורמות לשיתוף בתכנים (כדוגמת פייסבוק, Flickr, אינסטגרם, בלוגים שונים ועוד רבים), אלא שפלטפורמות אלה בדרך כלל מכוונות לתקשורת מרבים-אל-רבים (Many to many) ועניייני כאן בתקשורת אישית או סודית יותר מיחיד-אל-יחיד (One to one). עידן האינטרנט העשיר את אמצעי התקשורת הא-סינכרונית.[56] אמצעי תקשורת אלה אינם זוכים להתייחסות פרטנית במסגרת החוקים המסמיכים את הרשות החוקרת לאסוף ראיות דיגיטליות.[57] מכאן נובע קושי ממשי, אותו אפרט בהרחבה בהמשך, לסווג את הפעולה כראוי במסגרת התבניות של החוק הקיים, הכוללות כאמור שלוש אפשרויות: חיפוש, המצאה והאזנה. קושי זה ממחיש בצורה מובהקת במיוחד את חוסר יכולתו של המשפט, על תבניותיו ה"פיזיות", להתאים לסיטואציות שמתעוררות במרחב הקיברנטי. חוסר יכולת זה מייצר אי בהירות באשר למידת ההגנה החוקתית הראויה לתקשורת הא-סינכרונית, ובה בעת אי הבהירות משליכה גם על פעולתן של רשויות החקירה, שאינן יודעות כיצד עליהן לפעול כדי לאסוף תוכן של תקשורת א-סינכרונית מספק השירות.

[55] ראו: Nimrod Kozlovski, *A Paradigm Shift in Online Policing – Designing Accountable Policing* 88-93 (J.S.D. Dissertation, Yale Law School, 2005).

[56] להשלמת התמונה אציין כי בעידן האינטרנט הורחבו גם צורות התקשורת הסינכרוניות כגון: VoIP (שיחה קולית בשירותים כגון Skype, Viber, Tango ואחרים) או שימוש בתוכנות להעברת מסרים מידיים (כדוגמת WhatsApp, Messenger, ICQ וכו').

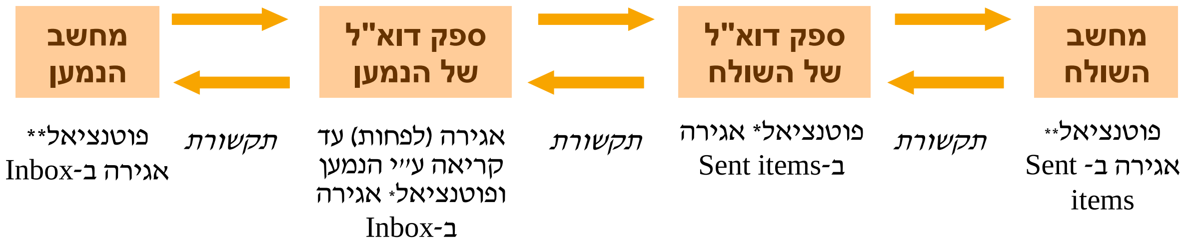
[57] ראו את הגדרת "קוי" נשוא-האזנה בסעיף 1 לתקנות האזנת סתר (בקשה להיתר האזנה), התשס"ח - 2007. זהו המקום היחיד בו מתייחסת החקיקה (מחוקק המשנה) לתקשורת א-סינכרונית כלשהי במסגרת כינון סמכויות האיסוף של הרשות החוקרת, ואולם התייחסות זו אינה לצרכי הגדרת תחומי הסמכות, אלא לצרכי הבניה של הבקשה והצו להאזנת סתר בלבד. התקנות אינן תורמות להכרעה בסוגיה אימתי דוא"ל יטופל כהאזנת סתר ואימתי יטופל כ"חומר מחשב" בר חדירה, הכל כפי שיפורט להלן.

EDNAKARNAVAL LIBRARY FOR THE MASSES

תרשים מס׳ 4.1 ממחיש את המשמעות של תקשורת א-סינכרונית, באמצעות אופן ביצוע ההתקשרות באמצעות דוא״ל:[58]

[58] תיאור ״מסעה״ של הודעת הדוא״ל נלמד מ: LINDA VOLONINO, REYNALDO ANZALDUA & JANA GODWIN, COMPUTER FORENSICS: PRINCIPLES AND PRACTICE 282-307 (2006). לתיאור במקורות משפטיים, ראו למשל: United States v. Councilman, 418 F.3d 69 (1st Cir. 2005). כן ראו פרוטוקול מס׳ 10 של ועדת החקירה הפרלמנטרית בנושא האזנות סתר (2.12.2007), המצוי ב: http://www.knesset.gov.il/protocols/data/html/wiretapping_inq/2007-12-02.html. כן ראו דו״ח ועדת החקירה הפרלמנטרית בעניין האזנות סתר, התשס״ט – 2009, בעמ׳ 26-28. להתייחסות דומה אל מסעו של הדוא״ל ראו שרון גולדנברג-אהרוני ״חדירה למערכות מחשב – היקפה הרצוי והמצוי של העברה״ **ספר דייויד וינר** (דרור ארד-אילון, יורם רבין ויניב ואקי עורכים) 429, 459-477 (2009).

<u>תרשים מס׳ 4.1 – מעברה של הודעת דוא״ל</u>



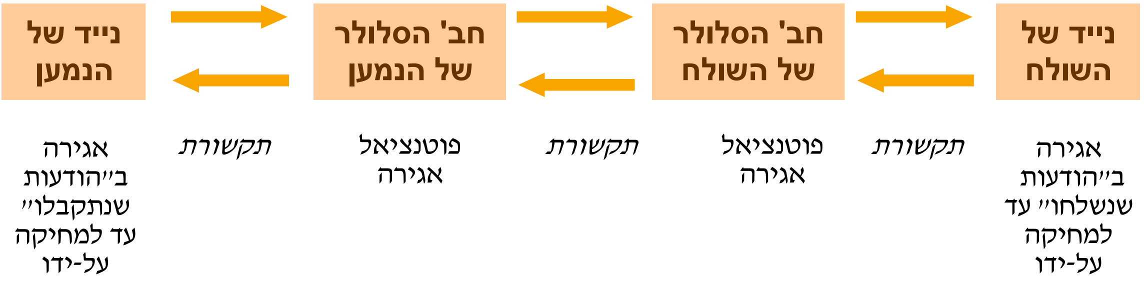
* האגירה תתבצע אם מדובר בשירות דוא״ל רשתי (Webmail או Web-Based Email) והנגיש באמצעות דפדפן אינטרנט. לדוגמה: Gmail, Yahoo!Mail.

** האגירה תתבצע אם מדובר בשירות דוא״ל המותקן במחשב הקצה, לפיו מועבר הדוא״ל מועבר באמצעות Mail User Agent (MUA) כדוגמת תוכנת Microsoft Outlook.

התרשים מייצג ארבעה מחשבים המעורבים בתהליך העברתו של הדוא״ל. ההצגה נעשית באופן טיפוסי בלבד, ואם, למשל, מחשבו של השולח מחובר ברשת מקומית, אז עשויה להיתוסף ״תחנה״ נוספת בדרך, שהינה שרת הדוא״ל של הרשת המקומית בה מותקן מחשבו של השולח. על פי התרשים, במחשבו של השולח נערכת הודעת דוא״ל, והוא שולח את ההודעה לכיוונו של הנמען. עם הלחיצה על פקודת ה״שליחה״, משוגר הדוא״ל לספק הדוא״ל של הנמען. במידה שמדובר בתוכנת דוא״ל המותקנת ב״שולחן העבודה״ של השולח (MUA), הרי שבמקביל לשליחת הדוא״ל נשמר העתק ממנו בתיקיית Sent items במחשבו של השולח. במידה שמדובר בספק שירותי דוא״ל באינטרנט (Webmail), העתק מן ההודעה נשמר ב-Sent items בחשבון הדוא״ל של השולח באותו שרת אינטרנט של שירות הדוא״ל (ולא במחשבו של השולח). ספק הדוא״ל של השולח מנתב את הודעת הדוא״ל לספק הדוא״ל של הנמען. הודעת הדוא״ל מגיעה לשרת של ספק הדוא״ל של הנמען, ומשם היא מנותבת לחשבונו של הנמען אצלה. ושוב, אם מדובר ב-Webmail, הרי שההודעה נאגרת בתיקיית ה-Inbox בשרת האינטרנט של שירות הדוא״ל של הנמען; אם, לעומת זאת, מדובר במשתמש בעל תוכנת דוא״ל המותקנת ב״שולחן העבודה״, הרי שבמחשב הקצה של הנמען מתקבלת הודעה נוספת בתיבת ה-Inbox. על פי הגדרות הרשת של הנמען, יכולה ההודעה הנכנסת להישמר במלואה במחשב הקצה של הנמען עם הַגיע ההודעה ל-Inbox, או שיכולה ההודעה להיוותר בשרת הדוא״ל הנכנס, ורק עם ה״הקלקה״ על הודעת הדוא״ל, ההודעה ״תורד״ אל מחשב הקצה. ועוד, כאשר הודעת הדוא״ל מועתקת מספקית שירותי הדוא״ל של הנמען אל מחשבו, יכולה ההודעה להישמר גם אצל ספקית שירותי הדוא״ל במקביל או להימחק משם, תלוי באופן בו הוגדרה תיבת הדוא״ל של הנמען.

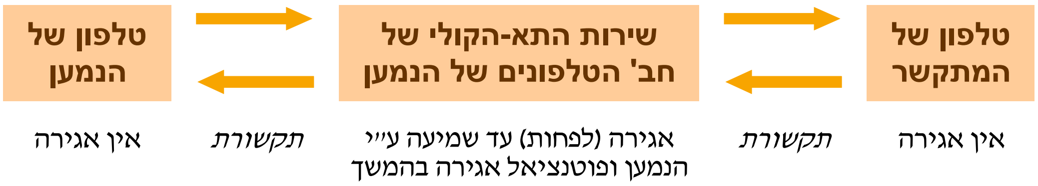
לגבי שליחת הודעת SMS או MMS, תהליך מעבר של הודעה מעין זו ניתן לתיאור בתרשים שלהלן (תרשים מס' 4.2):[59]

<u>תרשים מס' 4.2 – מעבר של הודעת SMS/MMS</u>



ולגבי הודעה בתא קולי, הדברים ניתנים לתיאור בתרשים שלהלן (תרשים מס' 4.3):[60]

<u>תרשים מס' 4.3 – מעבר של הודעה בתא-קולי</u>



---

[59] על "מסעה" של הודעת ה-SMS ניתן ללמוד למשל מהבקשה לתביעה ייצוגית שהוגשה נגד חברת פלאפון תקשורת בע"מ על כך שהיא נוהגת לשמור הודעות SMS שנשלחו עבור לקוחותיה המנויים בחברת פלאפון. כתוצאה מההד התקשורתי שליווה את הגשת הבקשה, הודיעה החברה על הפסקת שמירת הודעות ה-SMS של לקוחותיה. ראו נועם שרביט "פלאפון מודה: שומרת את כל תכני ה-SMS; בקשה לייצוגית: 'מדובר בהאזנת סתר'" **גלובס Online** 28.7.2009 http://www.globes.co.il/news/article.aspx?did=1000484932; כן ראו מארק שון "בעקבות הייצוגית: פלאפון שינתה המדיניות ותפסיק לשמור SMS" **כלכליסט** 29.7.2009 http://www.calcalist.co.il/local/articles/0,7340,L-3337025,00.html. ההליך בת"צ (מחוזי מר') 21185-07-09 **סודרי נ' פלאפון תקשורת בע"מ** (לא פורסם, 7.9.2011) הסתיים בהסכם פשרה בעקבות מהלכיה של פלאפון ותשלום שכר טרחתו של התובע הייצוגי. כמו כן, ראו הגדרת "הודעת מסר קצר" (SMS) בסעיף 74ב לרשיון כללי לפלא-פון תקשורת בע"מ למתן שירותי רדיו טלפון נייד בשיטה התאית (רט"ן) (נוסח משולב מיום 20.8.2007), המצוי ב: http://www.moc.gov.il/new/documents/legislation/r_klaliim/pelephone_meshulav.pdf, והוצא מכוח סמכותו של שר התקשורת לפי סעיף 4 לחוק התקשורת (בזק ושידורים), התשמ"ב – 1982 (להלן – "חוק התקשורת"). להגדרה נוספת של שירות SMS המלמדת עוד ועוד, בתיקון מס' 40 לחוק התקשורת משנת 2008, בו הותקן סעיף 30א לחוק, ונאסר על הפצת דואר זבל (דוא"ז) באמצעים שונים, הרי שבחר המחוקק להגדיר, בין היתר, את שני האופנים הבאים לשליחת דוא"ז: באמצעות "הודעה אלקטרונית" (מקביל לדוא"ל), המוגדרת כ"מסר בזק מקודד המועבר באינטרנט אל נמען או קבוצה של נמענים, וניתן לשמירה ולאחזור בדרך ממוחשבת"; ובאמצעות "הודעת מסר קצר" (מקביל ל-SMS או MMS), המוגדרת כ"מסר בזק הכולל כתב, לרבות אותות או סימנים, או מסר בזק הכולל חוזי או שמע, ומועבר באמצעות רשת בזק ציבורית אל ציוד קצה של נמען או קבוצה של נמענים". מעניין לציין כי במסגרת הגדרת "הודעה אלקטרונית" הוכנס לעצם ההגדרה האלמנט של שמירת המסר המועבר ואף אחזורו בדיעבד. לעומת זאת, במסגרת ההגדרה של "הודעת מסר קצר" נעלם אלמנט ההגדרה, וכביכול נשללת האגירה אצל חברת הסלולר. ייתכן שהשוני האמור מבטא את עמדת המחוקק על האופן בו ראוי שתועבר הודעת ה-SMS, אולם בפועל, מבחינה טכנולוגית, בוודאי שאין מניעה (וככל הנראה כך נעשה בפועל) שהודעת ה-SMS תיאגר אצל חברת הסלולר. יוער עוד, כי חרף הפרסום בכלי התקשורת, לפיו חברת פלאפון הפסיקה את שמירת הודעת ה-SMS של לקוחותיה, הרי שניתן להניח כי למצער במקרה שבו מכשיר הטלפון של הנמען כבוי, והודעת ה-SMS אינה יכולה להיקלט במכשיר הקצה שלו, הרי שחברת הסלולר אוגרת למעשה את ההודעה עבורו עד שידליק את מכשירו.

[60] לתיאור מפורט יותר על התפתחות התא-הקולי הטלפוני, ראו למשל: J.D. Gould & S.J. Boies, *Speech Filing-Office System for Principals*, 23 IBM SYSTEMS J. 65 (1984); Michael H. Martin, *All Your Messages in One Place*, FORTUNE 172 (12.5.1997).

מהו תרגומם של התרשימים לשפה המשפטית? אין ספק כי בכל המצבים שתוארו לעיל, בהם עובר המידע בתקשורת, הרי שלפי הגדרת החוק הישראלי, מדובר ב"שיחה" אשר קליטתה בעת מעברה בקווי התקשורת הללו תהווה האזנת סתר. כן אין ספק, שכל אימת שנוצרת אגירה במכשירי הקצה, בין של השולח ובין של הנמען, הרי שקליטת המידע האגור ממכשירי הקצה נעשית על דרך של עיון, הקשבה או העתקה ולא על דרך של הקלטה, כלומר לא יידרש לייצר תיעוד בזמן אמת. על כן, לא מבוצעת בשלב זה פעולה טכנית של האזנה אלא של חדירה לחומר מחשב על-ידי הרשות החוקרת או המצאה של חומר מחשב על-ידי צד שלישי שמצטווה לעשות כן. מבחינה מהותית המדובר בשיחה שהגיעה ליעדה ותועדה בלא כל קשר לפעולת הרשות החוקרת. הרשות החוקרת, במקרה זה, "תופסת" את התיעוד האמור.

הסוגיה המצויה במחלוקת פרשנית מכבידה, בשל החלוקה הקיימת כיום במשפט הישראלי בין חומר מחשב כ"חפץ" לחומר מחשב כ"תקשורת בין מחשבים", היא סוגיית מעמדו של המסר, בעת שהוא אגור אצל ספק השירות, בדרכו אל הנמען. כפי שאראה בהמשך, מחלוקת זו מתקיימת גם בעוד שיטות משפט. חשוב לציין כי הקושי מתעורר ביחס לאגירת המידע אצל ספק השירות רק בטרם נקרא / נפתח על-ידי הנמען. ככל שמדובר במצב בו לאחר הפתיחה על-ידי הנמען ממשיך המסר האלקטרוני להיאגר אצל ספק השירות, הרי שלכאורה דינו של המידע כדין כל מידע אגור שמבקשים לאסוף אותו, בין בצו חדירה לחומר מחשב ובין בצו המצאת חומר מחשב. יש לזכור כי לפחות במקרה של דוא"ל והודעה בתא-קולי, הרי שמתאפשר למשתמש לשמור את התוכן של המסר האלקטרוני בשרתי ספק השירות גם לאחר קריאתו. במובן זה, של שמירה לאחר קבלת המסר, תיבת דוא"ל (או שירות התא הקולי) מתפקדים לא רק ככלי להעברת מסרים אלא גם ככלי אחסון לכל דבר ועניין.[61]

בישראל הובעו עמדות שונות ביחס למעמדו של המידע שטרם הגיע לנמען ואשר אגור אצל ספק השירות. אציג את העמדות על דרך של תיאור המקרים הבולטים שבאו בפני בתי-המשפט בסוגיה: הפרשה הראשונה בה התעוררה השאלה הייתה פרשת **בדיר**. לאחים בדיר יוחסו עבירות רבות של מרמה, חדירה לחומר מחשב ועוד. בין היתר, הואשמו בעבירה על חוק האזנת סתר, על בסיס העובדה שהם התקשרו עם תאים קוליים של אחרים, תוך פיצוח סיסמאות הכניסה לתאים הקוליים והקשבה להודעות שהושארו בהם. הפרקליטות טענה שהקשבה להודעה בתא-קולי של בזק, אשר הנמען שלה

---

[61] עד לפני מספר שנים, חלק מהתחרות בין ספקיות שירותי הדוא"ל מסוג Webmail כללה הגדלה של נפחי האחסון של התיבה. בעניין זה, ראו, למשל, שירות בלומברג "מייקרוסופט תציע נפח אחסון מוגדל של דואר אלקטרוני - במענה לגוגל ויאהו" **גלובס Online** 24.6.2004 http://www.globes.co.il/news/docview.aspx?did=808555. אדר שלו "שירות הדוא"ל Hotmail Live גדל ל-5 גיגה בייט" **Ynet** 14.8.2007 http://www.ynet.co.il/articles/1,7340,L-3437367,00.html.

EDNAKARNAVAL LIBRARY FOR THE MASSES

טרם האזין לה, מהווה האזנת סתר אסורה. בית-המשפט המחוזי בתל-אביב הרשיע את האחים בעבירה על חוק האזנת סתר במקרה זה.[62]

לאחר הגשת כתב-האישום בעניין *בדיר*, ועוד בטרם ניתנה הכרעת-הדין, נחקרה במשטרה הצבאית החוקרת (מצ״ח) פרשייה, במסגרתה ביקשה מצ״ח לקבל את החומר האגור בתיבת דוא״ל של החשוד במועד ביצוע הצו (צופה פני עבר), וכן ביקשה לקבל לידיה את כל הדוא״ל שיתקבל בתיבה במשך 60 הימים ממועד ביצוע הצו (צופה פני עתיד), כל זאת בצו מכוח סעיף 43 לפסד״פ. בית-משפט השלום נעתר לבקשה. צו ההמצאה מוען לחברת נטוויזין, וזו התנגדה לצו, כאשר טענתה העיקרית הייתה כי המדובר בפעולה של האזנת סתר ולא המצאת חומר מחשב. בית-משפט השלום, במסגרת עיון חוזר, שב ואישר את החלטתו המקורית.[63] חברת נטוויזין הגישה ערר על ההחלטה לבית-המשפט המחוזי בתל-אביב. בין לבין הגיעה הסוגיה הנדונה אל שולחנה של פרקליטת המדינה דאז, עדנה ארבל, שקבעה כי דוא״ל, כמו גם הודעה בתא קולי, המצויים אצל ספק השירות – ניתן לתופסם במסגרת צו המצאה, ואילו קבלה עתידית של דוא״ל או הודעות בתא הקולי, המצויות אצל ספק השירות – דינן כדין האזנת סתר. עמדה זו הובעה על-ידי המדינה בערר בעניין **נטוויזין**, ולמעשה נסתיים שם הדיון.[64]

מונדיר בדיר, הנאשם המרכזי בעניין *בדיר*, ערער לבית-המשפט העליון, כשבאמתחתו החלטת בית-המשפט המחוזי בעניין *נטוויזין* ממנה נלמדת גם עמדתה של פרקליטת המדינה. במסגרת הדיון בערעור, המדינה הסכימה לזיכויו של בדיר מן האישומים שייחסו לו האזנת סתר לתאים קוליים.[65] המדינה נאלצה לעשות כן כדי לשמור על קוהרנטיות עם עמדתה כפי שהובעה בעניין *נטוויזין*, כי חומר הקיים אצל ספק השירות בעת ביצוע החדירה אינו בר-האזנה, וכי האזנת סתר רלוונטית רק לגבי קליטת חומר שעתיד להגיע לספק השירות. בעניין *בדיר*, לעומת זאת, דובר בהקשבה להודעות קיימות, ולא עתידיות, אשר נמצאו בתאים הקוליים. אלמלא נסוגה המדינה מהרשעת האחים בדיר בנקודה זו, הרי שהיה נובע מעמדתה כי דין שונה לאזרח ולרשות החוקרת: אותה פעולה הייתה נחשבת פעם כהאזנת סתר אסורה (כשמדובר בנאשם) ופעם כפעולת המצאה (כשמדובר ברשות החוקרת).[66] מספר

---

[62] ת״פ (מחוזי ת״א) 40250/99 **מדינת ישראל נ׳ בדיר**, תק-מח 2001(3) 1793, 1926-1929 (2001).

[63] ב״ש (שלום ת״א) 6703/00 **חברת נטוויזין בע״מ נ׳ צה״ל** (לא פורסם, 6.4.2000).

[64] ב״ש (מחוזי ת״א) 90868/00 **חב׳ נטוויזין נ׳ צבא ההגנה לישראל**, תק-מח 2000(2) 57734, 57738 (2000).

[65] ע״פ 10343/01 **בדיר נ׳ מדינת ישראל**, תק-על 2003(2) 649 (2003). פסק-הדין לאקוני וכולל מספר שורות, בהן מתועדת הודעת המדינה על הסכמתה לזיכויו של מונדיר בדיר מאישומי האזנת הסתר, ללא הסבר לגבי טעמי ההסכמה.

[66] בכל הנוגע להאזנת סתר, בחר המחוקק הישראלי בטכניקת חקיקה לפיה אותה הגדרה ניתנה הן לעבירה של האזנת סתר אסורה והן לפעולת החקירה של האזנת סתר. כלומר, ההוראה המסמיכה את הרשות לפעול על פי דין היא אותה הוראה המגדירה אימתי תתבצע עבירה של האזנת סתר. כך נעשה גם במקרה של חדירה לחומר מחשב בחוק המחשבים: העבירה של חדירה שלא כדין לחומר מחשב היא בעלת אותם יסודות כשל פעולת החקירה של חדירה לחומר מחשב, כאשר הראשון נעשה שלא כדין ואילו השני נעשה על פי צו בית-משפט. טכניקת חקיקה זו היא שחידדה את הסתירה הפנימית שעלולה היתה להיווצר בעמדת המדינה. יוער כי אין המדובר בטכניקת חקיקה הייחודית למדינת ישראל. כך, גם בבריטניה, למשל,

EDNAKARNAVAL LIBRARY FOR THE MASSES

חודשים לאחר פסק-הדין, פורסמה גם הנחיית פרקליטת המדינה 14.15 הדנה בסוגיה, שלפיה מידע אגור אצל ספק השירות בעת ביצוע צו ההמצאה – דינו כ"חפץ" בר-תפיסה ובר-המצאה, ואילו כאשר מתבקש לקבל מסרי דוא"ל עתידיים (או בהתאם גם הודעות קוליות שיגיעו בעתיד לתא הקולי), הרי המדובר בפעולה שהיא על פי מהותה האזנת סתר.[67]

הפעם הבאה בה התעוררה הסוגיה הייתה במסגרת **פרשת הסוס הטרויאני** (להלן - עניין **פילוסוף I**).[68] במסגרת חקירת חשדות לריגול עסקי פלילי באמצעות תוכנת סוס טרויאני, ביקשה המשטרה לקבל תכתובות דוא"ל של כמה מהחשודים בפרשה, הן דוא"ל צופה פני עבר והן דוא"ל צופה פני עתיד. פרקליט המדינה דאז, ערן שנדר, שינה את עמדת הפרקליטות, וקבע שכל עוד פעולת האיסוף היא העתקה של דוא"ל לאחר הגיעו לספק השירות, הרי אין נפקא מינה אם הבקשה היא אך ורק צופה פני עבר, או שהיא כוללת גם אלמנט של צפיית פני עתיד.[69] על פי הנחייתו של שנדר, הוצאו צווי חדירה לחומר מחשב,[70] וספקיות השירות צייתו לצווים. בפרשת הסוס הטרויאני ההתנגדויות התעוררו לא בשלב ביצוע הצו, כבמקרה *נטוויז'ן*, אלא בשלב הגשת הראיות לבית-המשפט, על-ידי באי-כוח הנאשמים, שגרסו כי הפעולה שבוצעה עלתה כדי האזנת סתר, ועל כן דין הראיות שנאספו מכוחה להיפסל לפי סעיף 13 לחוק האזנת סתר, שכן המדובר בהאזנת סתר שנעשתה בלא היתר כדין. בית-המשפט המחוזי קיבל את הטענה, ופסק כי למעשה כל דוא"ל שנמצא אצל ספק שירות ואשר טרם נקרא על-ידי הנמען – דינו כדין "שיחה" שלא הסתיימה ועל כן תפיסת החומר האמור מחייבת צו האזנת סתר.[71] החלטתו של בית-המשפט המחוזי בפרשת הסוס הטרויאני ניתנה במסגרת החלטת ביניים בהליך פלילי,[72] וכך, בפעם השנייה מאז עניין *בדיר*, נמנעה הכרעה של בית-המשפט העליון בסוגיה.

מוגדרת פעולת האיסוף של האזנת סתר באותו האופן בו מוגדרת העבירה הפלילית של האזנת סתר. ראו: Regulation of Investigatory Powers Act (RIPA), 2001 § 1, 3-4.

[67] ראו "תפישת הודעות קוליות האגורות בתא קולי ומסרים בדואר אלקטרוני האגורים במחשבי ספק השירות" **הנחיות פרקליט המדינה** 14.15 (התשס"ג, התשס"ד). בתחילת שנת 2012 נמחקה ההנחיה מאתר האינטרנט של משרד המשפטים.

[68] ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף**, תק-מח 07(1) 4872 (2007).

[69] ראו עניין *פילוסוף I*, לעיל ה"ש 68, בעמ' 4875, 4880.

[70] יוער כי אמנם הוצאו צווי חדירה לחומר מחשב ולא צווי המצאה, אולם בפועל לא בוצעה חדירה משטרתית למחשבי ספקיות השירות, ואילו הספקיות המציאו את התכנים המבוקשים כתחליף-חיפוש. כך עולה מקריאת החלטת בית-המשפט בעניין *פילוסוף I*. עוד על המצאה כתחליף-חיפוש ראו, למשל, עניין *שרון*, לעיל ה"ש 41.

[71] לעומת זאת, אם הדוא"ל נקרא כבר על-ידי הנמען, הרי שאיסופו מספק השירות לא יהווה פעולה של האזנת סתר, כי אם פעולה של חדירה לחומר מחשב או המצאה, תלוי בנסיבות (האם המשטרה ביצעה את הפעולה בעצמה או דרשה שתבוצע על-ידי ספק שירותי הדוא"ל). ראו לעניין זה גם את: ת"א (מחוזי מרכז) 4559-09-07 **א.ע. (המנוח) נ' ק.פ. בע"מ** (פורסם ב"נבו", 9.6.2011). בקשת רשות ערעור על החלטה זו נדחתה, מבלי שבית-המשפט העליון נדרש לסוגיית מעמדו של הדוא"ל לגופו של עניין. ראו רע"א 5263/11 **פלוני נ' פלוני**, תק-על 11(3) 2827 (2011).

[72] בסופו של דבר, כל נאשמי פרשת הסוס הטרויאני הורשעו, כך שהתביעה, אשר עתירתה לקבילות הראיות נדחתה, לא יכלה, מבחינה דיונית, להביא את הסוגיה לבחינתו של בית-המשפט העליון.

EDNAKARNAVAL LIBRARY FOR THE MASSES

עמדת בית-המשפט בעניין *פילוסוף I* נתמכת על-ידי קוזלובסקי[73] ועל-ידי גולדנברג-אהרוני.[74] גולדנברג-אהרוני דימתה את השליחה של המידע לנמען, דרך ספק השירות, לנסיעה ברכב, כאשר בדרך נעצר הרכב ברמזור. אין המדובר בסיום הנסיעה כי אם בעצירה שאינה משנה את מהות וכיוון הנסיעה. אבקש לחלוק, בכל הכבוד, על המטאפורה הזאת, או על המטאפורה שבחר בית-המשפט בעניין *פילוסוף I*, של רכב הנוסע מתל-אביב לחיפה ועוצר בדרך לתדלק. שתי המטאפורות הללו מבטאות קונספציות מחשבתיות של עולמות תוכן אחרים. המטאפורות הללו, מלבד היותן שובות לב, יכולות גם לשבות את המחשבה. לטעמי מטאפורת הרמזור או תחנת הדלק רחוקה יותר מן האנלוגיה הבאה: ניתן לדמות שליחת הודעה בדוא״ל באמצעות ספק שירות למצב בו ראובן מחפש את שמעון בטלפון, מתקשר לביתו או למקום עבודתו, ולוי עונה לטלפון. ראובן משאיר הודעה לשמעון אצל לוי ומבקש שלוי יעבירה לשמעון. אין ספק שהדברים שאמר ראובן ללוי מיועדים למעשה לשמעון. אולם, אין ספק כי השיחה של ראובן ולוי היא שיחה מושלמת. נניח עוד שלוי רשם את הדברים שראובן אמר לו על פתק. האם תפיסת הפתק הזה, עוד בטרם הגיע לעיניו של שמעון, מחייבת צו האזנת סתר? על פי הלוגיקה של פסק-הדין בעניין *פילוסוף I*, נראה שהתשובה חיובית לכאורה. עם זאת, ברי כי בפועל הדין הוא תפיסת פתק שכזה לא תיעשה אלא בצו חיפוש או המצאה (בהתאם לנסיבות).

לאחר ההחלטה הנ״ל בעניין *פילוסוף I*, עתרה ההגנה בתיק להרחבה נוספת של מושג ״האזנת הסתר״, הפעם אל הדוא״ל המתקבל במחשב הקצה של הנמען אך טרם נפתח על-ידו. עתירתה זו של ההגנה המשיכה למעשה את הרציונל של החלטת בית-המשפט, אך בה בעת האירה לטעמי את המשגה הבסיסי שבה. ההחלטה בעניין *פילוסוף I* מתמקדת בשאלת קריאת הדוא״ל על-ידי הנמען כפרמטר לקביעה האם הדוא״ל הגיע לידו אם לאו. אם כך הוא הדבר, צדקה לכאורה ההגנה בטענה שגם במחשב קצה של אדם יכול להימצא דוא״ל שטרם נקרא על-ידי הנמען. על פי מבחן *פילוסוף I*, לכאורה גם דוא״ל שכבר הגיע למחשב הקצה ונאגר בו, אך טרם נקרא על-ידי הנמען, יכול להיחשב למידע בר-האזנה בלבד ולא בר-חדירה. בית-המשפט דחה את עתירת ההגנה להרחבת התחולה של החלטת *פילוסוף I* אל מחשבי הקצה, ומהחלטתו נובע כי יעד השליחה של הדוא״ל הוא המחשב ולא האדם עצמו העומד מאחורי המחשב. על כן, ה״שיחה״ מגיעה אל יעדה עם הגיעה אל מחשב הקצה של הנמען, ולאו דווקא עם קריאת הדברים על-ידי הנמען (עניין **פילוסוף II**).[75]

---

[73] ראו נמרוד קוזלובסקי **המחשב וההליך המשפטי** 96-109 (2000). דבריו של קוזלובסקי נכתבו לפני ההחלטה בעניין *פילוסוף I* אך הם תומכים בתוצאתה האופרטיבית.

[74] ראו גולדנברג-אהרוני, לעיל ה״ש 58, בעמ׳ 459-477.

[75] ת״פ (מחוזי ת״א) 40206/05 **מדינת ישראל נ׳ פילוסוף**, תק-מח 07(3) 12198, 12204-12205 (2007).

EDNAKARNAVAL LIBRARY FOR THE MASSES

באותו היום בו ניתנה החלטת בית-המשפט בעניין *פילוסוף II*, ניתנה החלטה בסוגיה דומה שהתעוררה במסגרת פרשת **חפציבה**. מכשיר הטלפון הסלולרי של אחד מחשודי הפרשה נתפס, והמשטרה ביקשה לעיין בתכנים שנאגרו במכשיר, לרבות במסרוני SMS שנאגרו בזיכרון המכשיר. המשטרה פתחה את המכשיר כיומיים לאחר תפיסתו, ובאמצעות צו חדירה לחומר מחשב עיינה במסרוני ה-SMS שנאגרו בו.[76] בין היתר, היו במכשיר גם הודעות SMS שבעל המכשיר טרם עיין בהם, ואף הודעות שנשלחו לחשוד לאחר מועד תפיסת המכשיר ובטרם העיון של המשטרה ב-SMS. החשוד טען כי הפעולה שביצעה המשטרה עלתה כדי האזנת סתר, ובית-משפט השלום דחה את עתירתה. נקבע, כי עם הגיע ההודעות למכשיר הטלפון של החשוד, הרי שאף אם זה טרם עיין בהן, ואף אם ההודעות נשלחו לאחר תפיסת המכשיר על-ידי המשטרה, הרי שמהותית המדובר בפעולה של עיון ב״חומר מחשב״ אגור כ״חפץ״, ולא ביירוט תשדורת בעת מעברה.[77]

ועוד, בשנת 2009 ניתנה הכרעת-דינו של בית-המשפט המחוזי בנצרת בעניינו של נאשם שחדר לתיבת דוא״ל של חברתו לשעבר בהזדמנויות שונות ועיין בתכתובות שלה עם אחרים.[78] הנאשם הועמד לדין בעבירות של חדירה לחומר מחשב כדי לעבור עבירה אחרת, לפי סעיף 5 לחוק המחשבים, ופגיעה בפרטיות. הנאשם הורשע בעבירות אלה בבית-משפט השלום, ובמסגרת הדיון בערעורו, קבע בית-המשפט המחוזי כי קריאת תכתובות הדוא״ל אצל ספק השירות מהווה פעולה של האזנת סתר ולא של חדירה לחומר מחשב. בשונה מעניין *פילוסוף I*, בית-המשפט לא הבחין בין דוא״ל המועתק מספק שירותי הדוא״ל בטרם נקרא על-ידי הנמען, לבין דוא״ל אשר כבר נקרא על-ידי הנמען אך נותר אגור בתיבת הדוא״ל שלו.[79]

נוסף על הפסיקה בתחום סדר הדין הפלילי, ההתייחסות לדוא״ל (ולאמצעי תקשורת א-סינכרוניים אחרים גם כן) מתעוררת גם בתחום דיני העבודה, במסגרת שאלת סמכותו של מעביד לעיין בתכתובות דוא״ל של עובדיו המצויות בשרת הדוא״ל המשרדי. מצד אחד, המדובר בשרת דוא״ל

---

[76] מכשיר טלפון סלולרי הוא למעשה מכשיר דו-שימושי מבחינה משפטית: מצד אחד, בכל הנוגע לקיום שיחות הטלפון, הרי שמדובר בציוד קצה שבאמצעותה מתבצעת שיחה. מצד שני, בכל הנוגע לזיכרון של מכשיר הטלפון הסלולרי, ולכל האגור בו (ספר טלפונים, יומן שיחות, משחקים, לוח פגישות, תמונות, הודעות SMS, מוזיקה וכדומה), הרי שמדובר ב״חומר מחשב״ אשר החדירה אליו מחייבת הצטיידות בצו חדירה לחומר מחשב. ראו ת״פ (מחוזי ת״א) 40107/08 **פרקליטות מחוז ת״א-פלילי נ׳ פטימר**, תק-מח 08(4) 3665 (2008), שם נפסק כי עיון במידע האגור בטלפון סלולרי מהווה חדירה לחומר מחשב לכל דבר ועניין.

[77] ב״ש (שלום ת״א) 3544/07 **אדר נ׳ יאח״ה** (לא פורסם, 18.9.2007).

[78] ע״פ (מחוזי נצ׳) 264/09 **פלוני נ׳ מדינת ישראל** (לא פורסם, 10.11.2009).

[79] בית-המשפט המחוזי בנצרת הסתמך על ההחלטה בעניין *פילוסוף I* במסגרת פסק-דינו, אך דומה שעצם היישום של אותה החלטה נעשה באופן שגוי ומרחיב יותר. כנובע מפסק-דין זה בעניין *פלוני*, הרי שגם אם הנמען קרא את הדוא״ל, ואין ספק עוד שה״שיחה״ ב״תקשורת בין מחשבים״ הגיעה ליעדה, והנמען החליט לשמור כגיבוי את העתק תכתובת הדוא״ל בתיבת הדוא״ל, הרי שעדיין המדובר בפעולה של האזנת סתר ולא חדירה לחומר מחשב. זאת בניגוד לעניין *פילוסוף I*, שם נקבע כי רק אם הדוא״ל טרם נקרא על-ידי הנמען דינו כדין ״שיחה״, הכפופה לחוק האזנת סתר, ולא כדין ״חומר מחשב״, הכפוף להוראות הפסד״פ.

EDNAKARNAVAL LIBRARY FOR THE MASSES

שבבעלותו של המעביד ובתיבות דוא"ל שהוקצו לעובדים על-ידו. מצד שני, הדוא"ל יכול לשמש את העובדים גם לענייניהם הפרטיים, והוא עשוי להיתפס כ"אזור" פרטיות של העובד בתוך מקום העבודה, בדומה, למשל, לתא השירותים שבמקום העבודה.

אגב הדיון המורכב בשאלת סמכותו של מעביד לעיין בדוא"ל של עובדיו, נשאלה השאלה הצריכה לענייננו: האם פעולת עיון שכזו מהווה האזנת סתר או פגיעה בפרטיות על דרך של העתקת תוכן של מסר אלקטרוני שלא נועד לפרסום (לפי סעיף 2(5) לחוק הגנת הפרטיות)?[80] גם כאן, הובעו מספר עמדות שונות בעניין. פסק-הדין המנחה של בית-הדין הארצי לעבודה בעניין **איסקוב-ענבר** לא עסק בשאלה זו במישרין, ובפסיקת בית-הדין האזורי לעבודה במקרה זה, נקבע כי העתקת הדוא"ל מהשרת או עיון בו, זמן רב לאחר הגיעו ליעדו, לא תיחשב כהאזנת סתר, שכן אין מדובר בניטור תעבורה בזמן אמת.[81] לעומת זאת, במקרהו של מבקר הפנים של עיריית טבריה, **בנימין אליהו**, נפסק ביחס לתכתובות דוא"ל שלו שהוצאו משרת העירייה, כי על פניו מדובר בהאזנת סתר אסורה, אך כיוון שממילא מדובר בפגיעה אסורה בפרטיות, הכרעה ישירה בין השניים היא למעלה מן הדרוש.[82]

מקרה נוסף אותו אמנה עניינו בתביעה כספית בשל טענה להפרת הסכם שיווק בלעדי (פרשת **רויכמן שיש ואבן בע"מ**).[83] באותו מקרה התבקש בית-המשפט להכריע בדבר קבלת שלושה מסרוני SMS אשר נטען לגביהם כי הושגו בהאזנת סתר אסורה. המסרונים הושגו בדרך הבאה: בעל מכשיר הטלפון הסלולרי מסר את מכשירו לידיו של אחר על מנת שיסייע לו בהגדלת תצוגת המסך (שכן אבדו

---

[80] הדיון בכל הנוגע לסמכותו של מעביד לעיין בתכתובות דוא"ל של עובדיו נוגע להיבטים אחרים שאינם רלוונטיים לענייננו בפרק זה, לדוגמה: האם בעלותו של המעביד על שרת הדוא"ל המשרדי משפיעה על סמכותו לעיין בדוא"ל של העובדים? האם יש מקום ליצירת תנאים בהם יותר למעביד לעיין בתכתובות דוא"ל של עובדיו ללא כל צורך באישור בית-משפט לכך? לדיון כולל על סמכותו של מעביד לעיין בדוא"ל של עובדיו, וגיבוש קריטריונים עקרוניים להתרת עיון שכזה בנסיבות מתאימות, ראו מיכאל בירנהק "מעקב בעבודה: טיילור, בנת'האם והזכות לפרטיות" **עבודה, חברה ומשפט** יב 9 (2010); מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 407-464 (2010).

[81] לפסיקת בית-הדין האזורי לעבודה ראו עב' (אזורי ת"א) 10121/06 **איסקוב ענבר נ' הממונה על חוק עבודת נשים**, תק-עב 07(3) 2594, 2603 (2007). לפסיקת בית-הדין הארצי לעבודה ראו ע"ע 90/08 **איסקוב-ענבר נ' הממונה על חוק עבודת נשים**, תק-אר 11(1) 201 (2011). נראה כי נוכח העובדה שבית-הדין הארצי לעבודה פסל את הראיות שבמחלוקת עקב פגיעה אסורה בפרטיות, לא נדרש לדון במקרה הפרטי של האזנת סתר (על מבחני פסלות הראיה הקבועים בסעיף 13 לחוק האזנת סתר). יצוין עוד כי היועץ המשפטי לממשלה הוזמן להתייצב לדיון בערעור נוכח חשיבות הסוגיה והשלכות הרוחב שלה, והוא בחר להתייצב לדיון. בתגובת היועץ המשפטי לממשלה הובעה העמדה, הקוהרנטית עם עמדת פרקליטות המדינה שפורטה לעיל במסגרת פרשת הסוס הטרויאני, כי פעולתו של המעביד אינה עולה כדי האזנת סתר, שכן המעביד עיין בתקשורת אגורה. ראו עמדת היועץ המשפטי לממשלה כפי שהוגשה בע"ע 90/08 **איסקוב-ענבר נ' הממונה על חוק עבודת נשים**.

[82] ראו עמר"מ (מחוזי מר') 13028-04-09 **אליהו נ' עיריית טבריה**, תק-מח 10(1) 9973, 9982-9987 (2010). באותו מקרה דובר בתביעה משמעתית נגד מבקר הפנים של עיריית טבריה. במסגרת ההליך הוגשו תכתובות דוא"ל של מבקר הפנים, אשר הוצאו משרת הדוא"ל של העירייה על-ידי חברה ששירותיה נשכרו על-ידי ראש העיר, זוהר עובד. בית-הדין למשמעת של עובדי רשויות המקומיות קבע כי לא זו בלבד שלא מדובר בפעולה שאינה עולה כדי האזנת סתר (שכן מדובר בחומר שכבר ש"נח" בשרת ואינו במצב תקשורתי), אלא אף לא מדובר בפעולה העולה כדי פגיעה בפרטיות, שכן מדובר בשרת בבעלות העירייה, אשר הנתבע מוחזק כמי שיודע שלפחות אנשי תחזוקת המחשבים הינם בעלי גישה למידע שבתיבה שלו. ראו ת"מ (משמעת רשויות מקומיות) 46/06 **עיריית טבריה נ' אליהו** (לא פורסם, 22.10.2007). הנתבע הגיש ערעור לבית-המשפט המחוזי, שם נפסק כי פעולת התובע עולה כדי פגיעה בפרטיות (בהיעדר הסכמה מדעת לעיון כאמור) ולמעשה עולה גם כדי האזנת סתר. עוד קבע בית-המשפט המחוזי כי האבחנה של השופט כבוב בעניין *פילוסוף I*, בין תכתובות דוא"ל שטרם נקראו על-ידי הנמען לבין אלה שנקראו בפועל על-ידו אינה צריכה לעניין, וכי בשני המצבים ראוי לראות בעיון משום האזנת סתר אסורה.

[83] ראו ת"א (מחוזי ת"א) 1477-09 **רויכמן שיש ואבן בע"מ נ' שחף אבן ושיש בע"מ**, תק-מח 11(1) 26435 (2011).

EDNAKARNAVAL LIBRARY FOR THE MASSES

לו משקפיו). אותו אחר דפדף במכשיר ועיין, בניגוד להרשאה המקורית, בשלושה מסרונים. בית-המשפט קבע כי אין המדובר בהאזנת סתר ממספר טעמים, לא כולם צריכים לענייננו. לענייננו, חזר בית-המשפט על הקביעה כי נוכח העובדה שהמסרונים נצפו כאשר היו במצב אגירה ולא במצב תקשורתי, הרי שאין המדובר בהאזנת סתר. קביעה זו למעשה דומה לקביעה בעניין *פילוסוף II*.

מהתרשימים שהצגתי לעיל, עולה אבחנה בין **תקשורת בתנועה (in transit communication)** לבין **תקשורת אגורה (stored communication)**. אבחנה זו נעדרת מהחקיקה הקובעת את סמכויות האיסוף בישראל, אך מוכרת בארצות-הברית[84] ובאוסטרליה[85] למשל כאבחנה המבדלת בין פגיעות העולות כדי האזנת סתר לבין פגיעות העולות כדי תפיסה של חומר מחשב (לאחר ביצוע צו המצאה או צו חדירה לחומר מחשב). עם זאת, גם במשפט האמריקני לא נפתרה הדילמה באשר לאופן ההתייחסות הראוי לתקשורת א-סינכרונית, בעת שהיא נאגרת אצל ספק השירות בטרם הגיעה אל הנמען, וישנן פסיקות סותרות בעניין.[86] גם אמנת מועצת אירופה בדבר פשעי מחשב מבחינה בין יירוט תקשורת בין

---

[84] ראו 18 U.S.C. §§ 2510, 2703-2704.

[85] ראו: Telecommunications (Interception and Access) Act, 1979 §§ 5-6 (Au.). הוראות החוק המעגנות את האבחנה האמורה נקבעו בתיקונים לחוק משנת 2004 ו-2006.

[86] ראו: Steve Jackson Games, Inc. v. United States, 36 F.3d 457 (5th Cir. 1994). באותו מקרה נתפס שרת BBS (Bulletin Board System) אשר סיפק גם שירות דוא"ל. נשאלה השאלה מה דינה של התפיסה הזאת, וכן נדונה בפרט השאלה מה דינן של הודעות דוא"ל אשר טרם נקראו על-ידי הנמען ואשר נאגרו בשרת, זאת להבדיל מהודעות דוא"ל שנקראו אך נשמרו בשרת (כיוון שלא נמחקו על-ידי הנמען). בית-המשפט הפדרלי לערעורים קבע כי אין המדובר בהאזנת סתר כי אם בפעולת תפיסה. ראו גם: Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). במקרה מעט שונה זה נדון עניינו של טייס בחברת התעופה של מדינת הוואי, אשר תבע את מעסיקיו, על שחדרו לאתר האינטרנט שהקים. התובע נהג לשלוח לאתר האינטרנט הנ"ל תכנים ביקורתיים נגד מעסיקיו. הכניסה לאתר האינטרנט התאפשרה אך ורק באמצעות הקצאת שם משתמש וסיסמה. סגן נשיא החברה המעסיקה חדר לאתר האינטרנט באמצעות שם משתמש וסיסמה אשר לא הוקצו לו על-ידי התובע, ואותם השיג בלי ידיעתו של התובע. בית-המשפט הפדרלי לערעורים בחן את מעשהו של סגן נשיא החברה המעסיקה, ועמד על האבחנה בין יירוט תשדורות בתהליך שיגורן לבין כניסה וצפייה בתיעוד של התשדורות. ועוד בעניין *Konop*, בית-המשפט נדרש לשאלה האם כוונת המחוקק הייתה להטיל על רשויות אכיפת החוק את החובה להוציא צווי האזנת סתר ולא צווי חיפוש במצבים של גישה ל-"stored communication". בית-המשפט קבע כי הגם שהתנאים להוצאת צווי האזנת סתר קפדניים יותר מן התנאים להוצאת צווי חיפוש, הרי שדווקא בשים לב לכך, אין לומר כי כוונת המחוקק הייתה להטיל את החובה הקפדנית יותר במקרה של "stored communication" (לעיל, בעמ' 881). ראו גם: United States v. Lamb, 945 F. Supp. 441, 455-459 (N.D.N.Y. 1996), שם הוכשרה פעולת חדירה משטרתית לתיבת דוא"ל של חשוד (ולא האזנת סתר) במסגרת חקירה בחשד לעבירות של החזקה והפצה של תכנים פדופיליים. במקרה Fraser v. Nationwide Mutual Insurance co., 352 F.3d 107 (3rd Cir. 2003), נדונה הסיטואציה בה המשיבה חדרה לתכתובות דוא"ל של המערער שנמצאו בשרת הדוא"ל וצפתה בתכנים. בית-המשפט הפדרלי לערעורים בחן האם מדובר בפעולה המהווה "האזנת סתר" אם לאו, וקבע כי: "Every circuit court to have considered the matter has held that an "intercept" under the ECPA must occur contemporaneously with transmission." (לעיל, בעמ' 113). בהמשך פסק-הדין מובא אזכור של הפסיקה האמריקנית אשר ביצעה את האבחנה הברורה בין תפיסה מ-"stored communication" לבין "האזנת סתר" המתבצעת "contemporaneously with transmission". בסופו של דבר, סיכם בית-המשפט שם: "We adopt the reasoning of our sister circuits and therefore hold that there has been no 'intercept' within the meaning of Title I of ECPA." (לעיל, בעמ' 114). לפסיקה נוספת התומכת בעמדה, לפיה העתקת תכתובות דוא"ל שלא נקראו משרת הדוא"ל מהווה תפיסה ולא האזנה, ראו: United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996); Theofel v. Farey-Jones, 359 F. 3d 1066 (9th Cir. 2003); United States v. Jones, 364 F. Supp. 2d 1303 (D. Utah 2005); Garcia v. Haskett, 2006 U.S. Dist. Lexis 46303 (N.D. Cal. 2006). אל מול עמדה זו, ניצב למשל פסק-דינו של בית-המשפט הפדרלי לערעורים בעניין *Councilman*, לעיל ה"ש 58, שם מצויה קביעה שיפוטית הפוכה ולפיה ספקית שירותי דוא"ל המעתיקה דוא"ל של העובד מבצעת פעולה של האזנת סתר. כן ראו קביעה דומה בהקשר של העתקת תכנים האגורים בתאים קוליים: United States v. Smith, 155 F.3d 1051 (9th Cir. 1998). עוד מעניין לציין את Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548 (S.D.N.Y. 2008), שם, במסגרת תביעה בתחום דיני העבודה, פסק בית-משפט בניו-יורק, כי מעביד שחדר שלא כדין

EDNAKARNAVAL LIBRARY FOR THE MASSES

מחשבים בעת מעברה לבין העתקת תקשורת אגורה, ואולם ברמה היישומית עדיין קשה לומר כי נמצאת באמנה הכרעה מלאה בשאלת ההתייחסות אל התקשורת הא-סינכרונית בעת שהיא אגורה אצל ספק השירות ובטרם התקבלה אצל הנמען.[87]

4) סיכום ומסקנות

ראינו לעיל כיצד התפישה המשולשת – חדירה לחומר מחשב, המצאה והאזנה – מייצרת קשיי סיווג משמעותיים ביחס לפעולות חקירה שונות בזירה האינטרנטית. קשיי סיווג אלה נובעים מכך שהתפישה המשולשת פותחה עבור חקירה בסביבה פיזית, ומכאן שלא צפתה מראש את המצבים שמתעוררים בחקירה בסביבה דיגיטלית. הדוגמה של התקשורת הא-סינכרונית היא המובהקת ביותר כדי להמחיש את אי הבהירות הנוצרת כתוצאה מסיווג פעולות במרחב הדיגיטלי על פי התבניות המשפטיות של המרחב הפיזי. ראינו שאי-הבהירות נוגעת לשני צדדיו של המטבע, הן בכל הנוגע להעמדה לדין של נאשמים בעבירות של חדירה לחומר המצוי אצל ספקי שירות והן בכל הנוגע לסיווג פעולת האיסוף שבה מדובר. אי הבהירות האמורה מסבה נזק משולש: *האחד*, נפגמת הוודאות ביחס לסוג ההגנה החוקתית ומידתה אשר יוענקו לתכנים אלה; *השני*, נפגמת הוודאות של הרשות החוקרת ביחס למקור סמכותה לבצע את פעולת איסוף הראיות. "מחיר הטעות" ביחס למקור הסמכות עשוי להיות פסילה של פעולת האיסוף כראיה במשפט; *השלישי*, ככל שמדובר בהעמדה לדין של נאשמים או בהגשת תובענה נגד נתבעים בגין מעשים של "פריצה" לתיבות דוא"ל או ספקים אחרים של שירותי תקשורת א-סינכרונית, הרי שאי הבהירות עלולה להוביל לאישום / תובענה שגויים בשל כשלי סיווג של פעולתם.

ג. פריצת גבולות התפישה הפיזית – דיון נורמטיבי

עד כה הצגתי את התפישה הפיזית במובנה הפוזיטיבי, הגדרתי אותה והראיתי את ביטוייה בדין הישראלי (ולפרקים גם בדין הזר). עתה אעבור לבחינה נורמטיבית, שמטרתה "לקלף" את המעטה מעל

למיילים של עובד אינו מבצע עבירה מתחום האזנת הסתר, אלא מבצע עבירה על הוראות ה-SCA (Stored Communication Act, 18 U.S.C 2701-2712). באותו מקרה, חרף התוצאה המשפטית, בית-המשפט נסמך, ככל הנראה בטעות, על פסק-הדין בעניין *Councilman*. לפסיקה דומה לזו שנקבעה בעניין *Pure Power Boot Camp*, בהקשר של תיק גירושין בין בני זוג, ראו: Jennings v. Jennings, 736 S.E.2d (S.C. 2012). לסקירה נוספת של אי-הבהירות במשפט האמריקני בסוגיה דנן, ראו: Dorothy H. Murphy, *United States v. Councilman and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?*, 6 N.C. J.L. & TECH. 437 (2005); Katherine A. Oyama, *E-Mail Privacy After United States v. Councilman: Legislative Options For Amending ECPA*, 21 BERKELEY TECH. L.J. 499 (2006). עוד יצוין כי עמדת משרד המשפטים האמריקני היא כי הסיטואציה של העתקת תכתובת דוא"ל מספק שירותי הדוא"ל, בטרם נקראה ההודעה על-ידי הנמען, נתפסת כ-stored communication ולא כיירוט תקשורת בעת מעברה. ראו: DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 122-127 (2009) (hereinafter: "DOJ Manual").

[87] ראו אמנת מועצת אירופה בדבר פשעי מחשב, לעיל ה"ש 16, סעיפים 19, 21.

EDNAKARNAVAL LIBRARY FOR THE MASSES

לביטוייה של התפישה אל עבר ההנחות העומדות בבסיסה. במסגרת הדיון להלן אטען לכישלונה של התפישה הפיזית ביחס לאיסוף ראיות במרחב הסייבר במספר מובנים: *האחד*, היא אינה מתאימה למציאות הקיברנטית ולטיבה של הראיה הדיגיטלית (ביקורת ארכיטקטונית וטכנולוגית); *השני*, היא ממקדת את תשומת הלב המשפטית על שלבי הלוואי של איסוף המידע הדיגיטלי (ביקורת משפטית פרקטית); *השלישי*, היא מביאה להחסרה של פעולות איסוף ראיות דיגיטליות, לא בשל הכרעה חוקתית בין צרכי החקירה למידת ההגנה החוקתית הראויה, אלא בשל החמצה של עצם האפשרות להכיר בפעולות איסוף שכאלה.

1. ביקורת ארכיטקטונית וטכנולוגית על התפישה הפיזית

המעבר מראיות פיזיות לראיות דיגיטליות, והמעבר הנוסף מראיות דיגיטליות במחשב בודד (Stand alone) למחשבים המחוברים לרשתות מחשבים, ובראשן האינטרנט, משנים כמה מהתכונות הבסיסיות של הראיות. כיוון שסמכויות איסוף הראיות נוסחו עבור ראיות במרחב הפיזי, והשינויים וההתאמות נעשו בשיטה תוֹסַפְתִית, הרי שתכונותיהן של הראיות הדיגיטליות במרחב הסייבר אינן באות לידי ביטוי, לא במסגרת קביעת קשת הסמכויות של הרשות החוקרת, ולא במסגרת קביעת קשת ההגנות החוקתיות למול פעולת הרשות החוקרת.

בכל הנוגע לראיות במרחב הפיזי, ניתן להצביע על ארבע הנחות:[88] *האחת*, הראיה מיוצגת באופן פיזי-חפצי (באטומים); *השנייה*, תוכנה של הראיה ומשמעותה אינם נפרדים מן החפץ הפיזי בו הם מיוצגים; *השלישית*, הראיה אינה ניתנת להעתקה ומכאן שהיא בת-תפיסה בלבד; *הרביעית*, השימוש בראיה תלוי באחזקתו בפועל באופן פיזי בתוספת שליטה אפקטיבית בו. לעומת אלה, לראיות הדיגיטליות במרחב הסייבר תכונות אחרות, אשר בהצטברן יחד נראה כי הן בעלות נפקות ממשית לצורך קביעת סמכויות האיסוף של המדינה במסגרת חקירה פלילית:[89]

א. **המידע מיוצג בביטים**: הוא אינו בעל נוכחות או משמעות פיזית. גיבויו של המידע על גבי התקן פיזי מכל סוג שהוא (דיסק קשיח, דיסק-און-קי, תקליטור וכדומה) הוא עניין חסר משמעות

---

[88] השוו ל-Kozlovski, לעיל ה"ש 55, בעמ' 48-102, שמנה את מאפייני האינטרנט כזירת העבירה, ואילו אני מתמקד במאפיינים הרלוונטיים של הראיה הדיגיטלית באינטרנט לצורך פיתוח מערך סמכויות איסוף מתאים לצרכי החקירה ומאוזן מבחינה חוקתית. המדובר אפוא בפרספקטיבה קרובה, אך לא זהה, ומכאן השוני בין המאפיינים. מאפיין הבין-לאומיות, המתואר אצל קוזלובסקי, נדון בפרק 3 העוסק בתפישה הטריטוריאלית ביחס לדיני איסוף הראיות הדיגיטליות באינטרנט.

[89] שלוש התכונות הראשונות הן למעשה היפוכן של ארבע ההנחות שמניתי ביחס לראיות החפציות במרחב הפיזי (התכונה הראשונה היא היפוכה של שתי ההנחות הראשונות ביחס לראיות החפציות).

EDNAKARNAVAL LIBRARY FOR THE MASSES

והשפעה על תוכן המידע. מכאן שתוכן המידע נפרד מן החפץ הפיזי עליו הוא מוטבע.[90] על פי רוב, המידע עצמו הוא בעל הערך הממשי, מבחינת הזכות לפרטיות, לחופש ביטוי ולקניין. המידע אף עשוי להשליך על ניהול עסקיו של המחזיק במידע. לעומת זאת, ההתקן הפיזי עליו מוטבע המידע על פי רוב חסר חשיבות, למעט ערכו הכלכלי, שיחסית אינו גבוה.

ב. **המידע ניתן להעתקה מלאה**: בשל העובדה שמדובר במידע דיגיטלי, ניתן לייצר העתקים מושלמים של המקור, באמצעות העתקה פורנזית של הדיסק הקשיח לדיסק קשיח אחר או באמצעות Imaging של הדיסק הקשיח לקובץ סגור (ובמידת הצורך, אף חתום דיגיטלית) הכולל את המבנה והחלוקה של הדיסק הקשיח המקורי שהועתק.[91]

ג. **המידע מנותק פיזית מאת המשתמש בו**, הוא **מבוזר ומוחזק על-ידי מתווכים**:[92] המשתמש הקבוע במידע, לדוגמה בעל חשבון הדוא"ל בשירות Webmail, אינו מחזיק את הדוא"ל

---

[90] תכונתו זו של המידע הדיגיטלי עוררה את הדיון מתחום זכויות היוצרים סביב "דרישת הקיבוע", לפיה תנאי להגנה על זכות היוצרים הוא כי היצירה תהיה "מקובעת בצורה כלשהי" (סעיף 4(א)(1) לחוק זכות יוצרים, התשס"ח – 2007), קרי שהמידע יהיה מוצמד לחפץ פיזי כלשהו. לדיון וביקורת על דרישה זו בעידן של זכויות יוצרים דיגיטליות, ראו מיכאל בירנהק "קריאה תרבותית: החוק ושדה היצירה" **יוצרים זכויות: קריאות בחוק זכות יוצרים** 83, 113-115 (מיכאל בירנהק וגיא פסח עורכים, 2009); יואב מזא"ה "דרישת הקיבוע ומות היצירה הספונטנית", **יוצרים זכויות** שם, בעמ' 599. לביקורת דומה על דיני זכויות היוצרים במשפט האמריקני, ראו: Douglas Masson, *Fixation on Fixation: Why Imposing Old Copyright Law on New Technology Will Not Work*, 71 Ind. L.J. 1049 (1996).

[91] העתקה פורנזית משמעה שכל ביט וביט, כל סקטור וסקטור בדיסק הקשיח המקורי מועתק אל דיסק קשיח משטרתי, שמנוקה תחילה באופן מוחלט. העתקה פורנזית מאפשרת לשמור על המיקום האמיתי של כל קובץ וקובץ בתוך הדיסק הקשיח. כמו כן, העתקה פיזית כותבת על הדיסק המשטרתי גם את הביטים הפגומים בדיסק הקשיח המקורי, באופן שיאפשר לקבל תמונת ראי מושלמת ככל הניתן. וחשוב מכל, העתקה פורנזית מאפשרת העברה גם של מקומות בדיסק הקשיח שעברו מחיקה (delete או format), אלא שהביטים הכוללים את המידע לא נמחקו לגמרי. כך מתאפשר לשחזר קבצים מחוקים, דבר שהינו יקר ערך מבחינה פורנזית-חקירתית, וגם יכול להיות יקר ערך עבור חשוד שינסה לחלץ קובץ מחוק בעל פוטנציאל מזכה. תוכנות המספקות שירות של העתקה פורנזית ומקובלות בשימוש על-ידי יחידות חקירה שונות בעולם הן, למשל, IXimager Ilook ו-Encase. לפירוט על תוכנת Ilook ראו: http://www.perlustro.com; ולתוכנת Encase ראו: http://www.guidancesoftware.com/products/ef_index.asp.

בשל העובדה שהעתקה פורנזית יוצרת עותק מושלם של המקור, נקבע בפקודת הראיות כי פלט של "רשומה מוסדית" ממוחשבת דינו כדין מקור, ואף הוצע לסייג את כלל הראיה הטובה ביותר ביחס להעתק ממוחשב של ראיה דיגיטלית. ראו בהתאמה: פקודת הראיות, סעיפים 35-36, 41ב; הצעת חוק לתיקון פקודת הראיות (מס' 15) (מקור והעתק כראיה), התשס"ו- 2006, ה"ח הממשלה 232 (בשלב זה המשך קידום ההצעה, לקראת קריאה שניה ושלישית, נעצר). עוד על האנכרוניסטיות של כלל הראיה הטובה ביותר בעידן של מידע דיגיטלי הניתן לשכפול מושלם, ראו קוזלובסקי, לעיל ה"ש 73, בעמ' 329-330; ע"א 6205/98 **אונגר נ' עופר**, תק-על 2001(2) 299 (2001).

ככלל, משטרת-ישראל מעדיפה לעיין בחומר המחשב מתוך העתק פורנזי שהיא מבצעת, בסמוך לאחר תפיסת המחשב בחיפוש. מתי לא תבוצע העתקה פורנזית? (א) אם בשל בעיית חומרה או תוכנה נאלצת היחידה החוקרת לוותר על תפיסת המחשב ולבצע את החדירה למחשב במקום בו מבוצע החיפוש. (ב) אם מדובר בחדירה סמויה למחשב באמצעות התקשרות מרחוק (לא ניתן כיום לבצע העתקה פורנזית באמצעות התקשרות מרחוק). (ג) אם מדובר בהמצאה של חומר מחשב על-ידי צד ג'. (ד) כשמדובר בבדיקה של תקליטורים, בדרך כלל היחידה החוקרת תעיין ישירות בתקליטור, ולא תשכפל אותו קודם לכן, מתוך הנחה שלא ניתן "לכתוב" על תקליטור שום דבר בעת העיון בו (למעט תקליטורי re-writeable ובהפעלה קודמת של תוכנת צריבה). (ה) לעתים במסגרת בדיקה של מכשירי טלפון סלולרי, גם כן מתוך הנחה שהמידע בטלפון הסלולרי לא ישונה על-ידי מגע עם המכשיר המקורי. בית-המשפט עשוי להכשיר ממצאי חדירה לחומר מחשב שהתקבלו כתוצאה מחדירה לחומר המחשב המקורי והעתקתו ה"לוגית" בלא ביצוע העתקה פורנזית. ראו ת"פ (מחוזי י-ם) 426/09 **מדינת ישראל נ' אולמרט** 377-394 (פורסם ב"נבו", 10.7.2012).

גם בארצות-הברית המצב בפועל דומה: רשויות החקירה נוהגות לעבוד על העתק פורנזי של המחשב שנתפס בחקירה למעט בחריגים תלויי-נסיבות. העבודה על ההעתק הפורנזי אינה מנויה בחקיקה, אלא בנהלי משרד המשפטים האמריקני לגורמי החקירה. ראו: DOJ Manual, לעיל ה"ש 86, בעמ' 76-79. כן ראו: Bill Nelson, Guide to Computer Forensics and Investigations 50-51 (2004).

[92] ראו: Francis Cairncross, The Death of Distance – How the Communications Revolution Is Changing Our Lives 75-98 (2001); Daniel E. Geer, *The Physics of Digital Law: Searching for*

EDNAKARNAVAL LIBRARY FOR THE MASSES

במחשבו האישי. המידע מוחזק על-ידי מתווך, במקרה זה ספקית שירותי הדוא"ל. יתר על כן, לא זו בלבד שהמידע מוחזק על-ידי ספקית השירות, אלא שסך המידע בשימושו של אדם מבוזר על פני מספר רב של ספקיות שירות שונות.

ד. **המידע ניתן לאחזור וכרייה באמצעים ממוחשבים**: מצד אחד, כאמור, המידע מבוזר במספר רב של מקומות, ומוחזק ברשות מספר רב של מתווכים במרחב הסייבר, בפרט באינטרנט. מצד שני, המידע המבוזר ניתן לאיחוד, מיון ואחזור לפי שאילתות ממוקדות. זאת לנוכח תכונת הקישוריות של האינטרנט בתוספת פיתוח יכולות חיפוש ואחזור "חכמות". כתוצאה מכך, "שובל המידע" שמותיר כל משתמש מחשב[93] ניתן לאיסוף והרכבה של פרופיל אישי עשיר, הכולל לא אחת פריטי מידע עודפים על יעד החקירה.

ה. **המידע מצטבר וניתן לאגירה**: כיוון שעלויות אחסון המידע הופכות לעניין זניח עם השנים,[94] הרי שמידע דיגיטלי שנוצר במחשבים שונים אינו נמחק, והוא מצטבר והולך. יכולות אחזור המידע השתכללו, בתוספת הקישוריות באמצעות האינטרנט בין מצבורי המידע השונים - כל אלה מגבירים את הפוטנציאל החקירתי בקשר למידע מחד גיסא, ומגבירים את עוצמת הפגיעה כתוצאה מעיון במידע, אחזורו וניתוחו, מאידך גיסא.

ו. **המידע נדיף**: ככל שאין אחסון ושמירה מתוכננים מראש, קיימת אגירה זמנית ב"מחסניות" זיכרון העשויות להתמלא ולהתרוקן עם הזמן. כך, למשל, גם מידע שנמחק ממחשב אישי במחיקה רגילה (הכוללת העברה ל"סל המחזור"), אינו נמחק באופן סופי, אלא עובר לאותו מחסן של תאי זיכרון הניתנים ל"דריסה" על-ידי מידע חדש שיוסף אל המחשב. אולם, אם לא יתוסף מידע חדש למחשב וימלא את מלוא תכולת הדיסק הקשיח במחשב, המידע ה"מחוק" לא ייעלם מן המחשב.

ז. **המידע פגיע**: המידע הדיגיטלי פגיע לשינויים בלתי מכוונים, כתוצאה מעדכונים אוטומטיים, וירוסים וכיוצא בזה. מכאן נובע שדיני איסוף הראיות בחקירה פלילית באינטרנט צריכים להכיר במגבלות אלה של המידע הדיגיטלי. לא די באיסוף המידע הדיגיטלי, אלא יש לוודא כי נאסף במועד הנכון, הקשור לביצוע העבירה הנחקרת.

ח. **המידע ניתן להצפנה, הסוואה או טשטוש בנקל**: יכולת ההסוואה, הגנת הסיסמה, הסתרת זהות מחבר המידע, שולחו או מקבלו – כל אלה הפכו לפעולות פשוטות, ללא עלות, הניתנות

Counterintuitive Analogies, in CYBERCRIME – DIGITAL COPS AND LAWS IN A NETWORKED ENVIRONMENT 13 (Jack M. Balkin et al. eds., 2007).

93 להרחבה בדבר סוגי המידע המיוצרים באותו שובל של מידע, ראו בירנהק, **מרחב פרטי**, לעיל ה"ש 80, בעמ' 169-190.

94 כפי שפירטתי לעיל בפרק המבוא בה"ש 27.

EDNAKARNAVAL LIBRARY FOR THE MASSES

לביצוע באופן מידי. שיטות ההסוואה מגוונות והן מכוונות הן כלפי זהות מקבל או שולח המידע והן כלפי תוכן המידע עצמו.[95]

מאפיינים אלה מייחדים את הראיה הדיגיטלית במרחב הסייבר מהראיה החפצית במרחב הפיזי. נראה כי הם מחייבים היפרדות מהתפישה הפיזית ביחס לאיסוף ראיות דיגיטליות במרחב הסייבר. בהמשך הפרק אבחן את השלכותיהן של התכונות שמניתי לעיל על צרכי החקירה במרחב הסייבר.

2. התפישה הפיזית מדגישה את שלבי הלוואי של הליך איסוף הראיות הדיגיטליות

הטענה שאציג להלן, היא שהמחוקק, ובעקבותיו בית-המשפט והרשות החוקרת, מתמקדים בפעולות הפיזיות שהן בפריפריה של איסוף הראיות הדיגיטליות, ולא בפעולות המהותיות המרכזיות, המגלמות את הפגיעות המשמעותיות יותר בזכויות הנחקרים, של עיון במידע, סינונו, אחזורו וניתוחו. אתמקד תחילה בפעולה של חדירה לחומר מחשב ולאחר מכן אחיל בקצרה את הדברים על פעולת ההמצאה של חומר מחשב. בהקשר זה, המחוקק מתייחס בעיקר לסמכות הכניסה, התפיסה וההעתקה של חומר המחשב, ופחות לעצם העיון במידע הממוחשב. אבהיר את הדברים באמצעות פנייה אל אב-הטיפוס של חדירה לחומר מחשב במסגרת חקירה גלויה. השלבים הטיפוסיים הם:[96]

(א) כניסה לחצרים – עם צו או בלעדיו (במסגרת העילות המותרות לכניסה בלא צו);

(ב) ביצוע חיפוש בחצרים;

(ג) תפיסת חפצים שונים במסגרת החיפוש, לרבות מחשבים;

(ד) העתקת תוכן המחשב התפוס להתקן משטרתי;

(ה) ביצוע פעולות איתור, עיון ומיון המידע – על גבי ההעתק שנוצר בהתקן המשטרתי;

(ו) הפקת חומר הראיות הרלוונטי שנמצא על גבי ההעתק המשטרתי לתקליטור או לתדפיס.

---

[95] אתייחס להצפנת תכנים להלן בפרק 4(ג)(3)(ז), כשאציג את פעולת האיסוף של חיוב במסירת מפתח הצפנה או סיסמת ההגנה. בכל הנוגע לאמצעים להסוואת זהות מקבל או שולח המסר, ראו: Kozlovski, לעיל ה"ש 55, בעמ' 52-62; Matthew Edman & Bulent Yener, *On Anonymity in an Electronic Society: A Survey of Anonymous Communication System*, 42 ACM COMPUTING SURVEYS art. 5 (2009); בירנהק, **מרחב פרטי**, לעיל ה"ש 80, בעמ' 388-393.

[96] ראו: DOJ Manual, לעיל ה"ש 86, בעמ' 76-79, 85-87. לתיאור דומה ראו קוזלובסקי, לעיל ה"ש 73, בעמ' 80-85. ראו גם הצגה דומה על-ידי קֶר, שאיבחן כי החיפוש הטיפוסי בחצרים הוא הליך חד-שלבי (הכניסה, התפיסה והעיון מתבצעים כלפי החפץ בהליך הנתפס כהליך אחד מבחינה רעיונית), ואילו החדירה הטיפוסית לחומר המחשב הינה הליך דו-שלבי: הכולל שלב פיזי (כניסה, תפיסה של המחשב, פירוקו והעתקתו) ושלב אלקטרוני (של עיון במידע). ראו: Kerr, לעיל ה"ש 39, בעמ' 85-95.

EDNAKARNAVAL LIBRARY FOR THE MASSES

מבחינת החוק הישראלי, החוליה המהווה "חדירה" היא שלב ההעתקה של חומר המחשב המקורי להעתק משטרתי. בשלב זה מתבצעת ההתערבות במחשב התפוס ובחומר המחשב שבתוכו, או במילותיו של החוק – מתבצעת ה"הפעלה" של המחשב התפוס.[97] כל שאר הפעילות מרגע זה נחשבת לעבודה על גבי העתק, ואינה עונה למעשה עוד על ההגדרה של "חדירה" לחומר מחשב, כיוון שברגע שהועתק חומר המחשב להתקן משטרתי, התפישה היא שהסתיימה ההתערבות בחומר המחשב של המחזיק ממנו הוא נתפס.[98] עם זאת, דווקא בשלב זה מתבצעות הפעולות שנתפשות אינטואיטיבית כפוגעניות יותר, לפחות במובנים של פגיעה בזכות לפרטיות ובסוד המסחרי (ככל שמדובר במידע בעל ערך כלכלי): בשלב זה מתבצע העיון במידע, הכולל כרייה של המידע, צפייה בו, ניתוחו והפקתו.

החוק אמנם מציין שעל צו החדירה לחומר מחשב לפרט את *"מטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש"*.[99] אולם, מבחינה מעשית הוראה זו אינה מקוימת על-ידי בתי-המשפט והצווים מוצאים ביחס לכל חומר המחשב הנמצא במקום ביצוע החיפוש.[100] יתרה

---

[97] המונח "חדירה לחומר מחשב" מוגדר בסעיף 4 לחוק המחשבים, התשנ"ה – 1995, אליו מפנה סעיף 23א לפסד"פ (שם מוגדרת פעולת החקירה של "חדירה לחומר מחשב". "חדירה" היא כל "הפעלה", "התקשרות" או "התחברות" עם מחשב.

[98] החוק הישראלי אף אינו מתייחס כלל לטיפול במידע הדיגיטלי המועתק לאחר תום ההליכים בתיק החקירה (החלטה לגנוז את התיק או לאחר העמדה לדין ותום המשפט). הפסד"פ כולל הוראות לעניין טיפול במוצגים, כאשר גם כל הוראות הטיפול במוצגים מגלמות גישה "חפצית": ניתן להחזיר את התפוס לבעליו או למחזיקו על פי דין (סעיפים 35 ו-37 לפסד"פ), ניתן למוכרו במידה שמדובר במוצג מתכלה (סעיף 38 לפסד"פ), ניתן לחלט את התפוס במידה ששימש לביצוע עבירה (סעיף 39 לפסד"פ), לחלטו לטובת אוצר המדינה בהיעדר בעלים (סעיף 42 לפסד"פ) או לחלטו על פי כל דין אחר (ראו סעיפים 35 ו-36, 36א-36י לפקודת הסמים המסוכנים; סעיפים 21-23 לחוק איסור הלבנת הון, התש"ס – 2000; פרקים ג'-ה' לחוק מאבק בארגוני פשיעה, התשס"ג – 2003). עם זאת, העתק מכל סוג שהוא של החפץ שנתפס אינו זוכה להתייחסות המחוקק. מכאן, שאין חובה להשמיד את ההעתק, או להחזירו לבעליו. אין מניעה חוקית מפורשת מהמשטרה מלאגור את המידע העצום המועתק על-ידיה כדין במסגרת רבבות חקירות הכוללות חדירה לחומר מחשב. אמנם הוראת סעיף 8 לחוק הגנת הפרטיות עשויה לחייב רישום מאגר מידע שכזה אצל רשם מאגרי המידע, וסעיף 10 לחוק אף מקנה סמכויות פיקוח לרשם, אולם מבחינה מעשית קשה לראות לטעמי כיום ברשם מאגרי המידע משום גורם שבכוחו יהיה לפקח אפקטיבית על המשטרה בעניין זה. זאת נוכח מגבלות כוח האדם של רשם מאגרי המידע ומיעוט השימוש בסמכויות הפיקוח שלו כלפי רשויות החקירה והביטחון. להרחבה על תחומי הפעילות, כמו גם על יכולת האכיפה, של רשם מאגרי המידע, ראו דו"חות הרשות למשפט, טכנולוגיה ומידע, בפרק המתייחס לרשם מאגרי המידע (תפקיד בו אוחז ראש הרשות), מצוי בפורטל ועדת החוקה של הכנסת באתר www.knesset.gov.il/huka. חשש דומה הובע על-ידי פול אוֹם (Ohm) ביחס למשפט האמריקני. ראו: Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, Chapter III (2008).

[99] ראו סעיף 23א(ב) סיפא לפסד"פ.

[100] אמירה זו מבוססת על כך שבכל ההחלטות השיפוטיות בהן נדון עניינו של צו חדירה לחומר מחשב, ואשר ניתן היה ללמוד על נוסח הצו השיפוטי שהסמיך חדירה או קבלה של חומר מחשב, הרי שהצו נוסח באופן הגורף ביותר האפשרי. ראו למשל ב"ש (שלום ראשל"צ) 1209/06 **נטוויזי'ן בע"מ נ' יאח"ה**, תק-של 06(1) 27238 (2006), שעניינו צו חדירה לחומר מחשב שהוציאה המשטרה במעמד צד אחד ואשר מופנה לחברת נטוויזי'ן, במסגרת חקירת חשדות לפרסום אתרי הימורים בלתי חוקיים בפורטל האינטרנט "נענע" אשר היה בבעלות חברת נטוויזי'ן. במסגרת חקירתה של עבירה זו, שאינה מן החמורות בספר החוקים (ולא הניבה כתב-אישום בסופו של דבר), הוסמכה המשטרה – במעמד צד אחד – לתפוס כל חומר מחשב מרשותה של ספקית הגישה לאינטרנט הגדולה בישראל. כן ראו ב"ש (שלום נצ') 1248/03 **תשעים הכדורים מסעדה נ' משטרת ישראל**, תק-של 03(1) 18313 (2003); ב"ש (שלום אי') 2162/03 **מדינת ישראל נ' כהן**, תק-של 03(2) 17432 (2003); ב"ש (שלום י-ם) 4304/03 **צוקרמן נ' אגף המכס והמע"מ**, תק-של 03(2) 31588; ב"ש (שלום רמ') 1269/05 **מדינת ישראל נ' מילר**, תק-של 05(2) 21836 (2005); מע' (שלום ת"א) 14132/05 **מדינת ישראל נ' עו"ד שטריים**, תק-של 05(3) 25358 (2005); ב"ש (מחוזי י-ם) 4642/05 **דויטש נ' מדינת ישראל**, תק-מח 05(3) 2856 (2005); ת"פ (שלום י-ם) 1934/05 **מדינת ישראל נ' ואנונו**, תק-של 06(1) 9785 (2006) (דוגמה נדירה למקרה בו נפסל צו החיפוש בהחלטת ביניים במסגרת ההוכחות, לאחר שבית-המשפט מצא שהצו נוסח באופן גורף ביותר מבחינת החומרים שהותרו בעיון וכן לא הייתה הצדקה להגביל את החדירה לחומר מחשב כך שלא תותר נוכחות של שני עדים מטעמו של הנאשם בעת החדירה; יצוין כי בסופו של דבר הורשע הנאשם, ולכן המדינה לא העמידה את החלטת הביניים האמורה במבחן ערכאת הערעור); ת"פ (מחוזי י-ם) 2077/06 **מדינת ישראל נ' אריש**, תק-מח 07(1) 10109 (2007); ב"ש (שלום טב') 1528/07 **בוזגלו נ' משטרת ישראל**, תק-של 07(1) 13378 (2007); ת"פ (מחוזי ת"א) 40205/05 **מדינת ישראל נ' ויינשטיין**, תק-מח 07(2) 9670 (2007); ב"ש (שלום אי') 1152/08

EDNAKARNAVAL LIBRARY FOR THE MASSES

מזאת, הנחיית חטיבת החקירות במשטרת-ישראל, המדריכה את החוקרים כיצד להכין בקשות לצווי חדירה לחומר מחשב, מנחה אותם לבקש *"כל מסמך או חפץ הדרושים לחקירה, לרבות מחשב, דבר המגלם חומר מחשב וחומר מחשב של מוסד הנמצא במקום, וכן חדירה נמשכת לחומר מחשב לצורך בדיקה או הפקת פלטים".*[101]

בהקשר של המצאת חומר מחשב, כמו בהקשר של חדירה לחומר מחשב, ואף באופן בוטה יותר, אין כל התייחסות של המחוקק לשלב העיון במידע.[102] תחת זאת המחוקק מתייחס לפעולות אחרות המתאימות לעולם החפצי: "הצגה" או "המצאה" ותפיסה כפועל יוצא מאלה.

ביקורת דומה, על כי השלבים הפיזיים של החדירה אל חומר המחשב תופסים את תשומת הלב המשפטית, בעוד ששלבי העיון במידע גופו נזנחים – מובעת גם ביחס למשפט האמריקני על-ידי אורין קֶר. קר הביע חשש שעקב נוסחו של התיקון הרביעי לחוקה האמריקנית, וההתייחסות אל החדירה לחומר המחשב באופן חד-שלבי כאמור, עלולה להיווצר תוצאה פרשנית לפיה רק התפיסה של המחשב המקורי תיחשב לפעולת "תפיסה", וכל שאר הפעולות – העתקת המחשב ועיון בהעתק – לא ייחשבו לפוגעות בזכויות חוקתיות.[103] ביקורתו של קֶר היא מכיוון המשפט החוקתי. לטענתו, הפיתוח של ההגנה החוקתית על פרטיות במידע הממוחשב מבוססת על תפישה חפצית או פיזית. אני סבור כאמור כי הביקורת על קיומה של תפישה פיזית ישימה גם לעניין בחינת סמכויות האיסוף במשפט הישראלי, ולא רק לעניין בחינת ההגנות החוקתיות בפני הסמכויות הקיימות.

בהמשך לטיעון, לפיו ההתמקדות המשפטית היא אפוא בשלבי הלוואי של איסוף הראיות הדיגיטליות (החיפוש הפיזי והתפיסה של המידע על גבי ההתקן החפצי שלו), אראה להלן כי התפישה הפיזית עלולה גם להביא להחמצה של צרכי חקירה רבי חשיבות במרחב הממוחשב.

3. התפישה הפיזית וצמצום קשת פעולות איסוף הראיות הדיגיטליות במרחב הסייבר

התפישה הפיזית, המושלת בדין הישראלי בקשר לאיסוף ראיות דיגיטליות, מונעת את האפשרות לבחון את כינונן העצמאי של פעולות איסוף שונות ביחס לראיות דיגיטליות בחקירה פלילית במרחב הסייבר.

מדינת ישראל נ' גיגי, תק-של 08(2) 22887 (2008); עניין *פטימר*, לעיל ה"ש 76; ת"פ (שלום חי') 1826/08 **מדינת ישראל נ' הלוי**, תק-של 11(4) 28577 (2011).

[101] ראו "תפיסה וחיפוש במחשב" **הנחיות חטיבת החקירות** 03.300.035 (2007).

[102] כאמור, סמכות ההמצאה כולה מנוסחת בקיצור רב במסגרת סעיף 43 לפסד"פ שמקורו בפקודה מנדטורית שנוסחה מחדש בשנת 1969. ראו לעיל בפרק 4(ב)(2)(א).

[103] Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 560-561 (2005). כן ראו: Kerr, לעיל ה"ש 39. ראו גם, בהתייחס למשפט האמריקני, את Kozlovski, לעיל ה"ש 55, בעמ' 337-338.

להלן אמנה רשימה של פעולות איסוף ראיות, שקיים צורך חקירתי המצדיק בחינה ודיון בהן.[104] חלק מן הפעולות, כפי שאראה, הוכרו במדינות אחרות. ייאמר מיד שאין כוונתי בשלב זה של הדיון לטעון שפעולות אלה מוצדקות במשטר המשפטי הישראלי. כל כוונתי בשלב זה היא להציג את קשת פעולות האיסוף שהחקירה הפלילית במרחב הסייבר עשויה לפתוח, ככל שמשתחררים מהתפישה הפיזית ביחס לחקירה הפלילית במרחב הסייבר. בהמשך, בפרט בפרק 5, אעמוד על הפגיעות החוקתיות הגלומות בפעולות אלה, ולאחר מכן, בפרק 6, אציע מודל המגלם בחינה הולמת יותר, הן מההיבט של צרכי החקירה והן מההיבט של הניתוח החוקתי, של נושא איסוף הראיות הדיגיטליות בחקירה פלילית במרחב הסייבר.

<u>א) המצאה עתידית של מידע דיגיטלי</u>

אחת מתכונותיה של הראיה הדיגיטלית, עליה עמדתי לעיל, היא כי היא מצטברת וניתנת לאגירה. בנוסף, התקשורת המקוונת מתווכת על-ידי ספקיות שירות שונות. כתוצאה משני אלה, עשוי לעלות הצורך החקירתי לדרוש מספקית השירות להמציא נתונים על פני רצף של זמן, במסגרת מעקב אלקטרוני של רשויות החקירה ביחס לפעילות חשודה מסוימת. כדוגמה לצורך חקירתי זה, נניח שאתר אינטרנט מסוים חשוד כאתר שדרכו משתמשי אינטרנט מחליפים ביניהם תכנים פדופיליים, האסורים בהפצה על פי חוק. עוד נניח שהמשטרה מבקשת לעקוב לפרק זמן מסוים אחר הפעילות באתר על מנת להגיע אל החשודים. במקרה כזה, תידרש המצאה עתידית של נתוני הגלישה לאתר האינטרנט, פרטי הזיהוי של הגולשים, התכנים שהעלו או העבירו דרך האתר וכדומה. את הנתונים האלה יוכל להמציא מנהל האתר (כספק שירות מסוג אחד, במידה שאינו חשוד בעצמו כמספק הפלטפורמה לפעילות החשודה) או מנהל שירותי האיחסון של האתר (כספק שירות מסוג שני).

להבהרת סמכות ההמצאה העתידית של מידע דיגיטלי, אבחין בינה לבין סמכות האזנת הסתר. לכאורה, איסוף נתוני תוכן עתידיים בלא ידיעת החשוד מהווה פעולה של האזנת סתר. אולם, בענייננו קיימים כמה אלמנטים מאבחנים מהאזנת סתר: *האחד*, הכוונה בקטגוריה הנדונה כעת לאיסוף מידע לאחר אגירתו במחשב, ולא ביצירת תיעוד למידע העובר בתקשורת בין מחשבים. *השני*, הכוונה בקטגוריה הנדונה לפעולה של המצאה, קרי פעולה שאינה מתבצעת טכנית על-ידי הרשות החוקרת, אלא על-ידי צד שלישי (להוציא מקרה של המצאה על-ידי חשוד), הממציא את המידע לפי דרישת הרשות החוקרת. מכאן שגם אם פעולת ההמצאה נעשית שלא בידיעת החשוד, עדיין אין המדובר

---

[104] פעולות האיסוף שאדון בהן להלן הן כאלה שאינן קיימות כיום בדין הישראלי. זאת בניגוד לקטגוריות המצבים שתיארתי לעיל בפרק 4(ב)(2)(ג), בהם קיים כיסוי חוקי עקרוני בדין הישראלי, אולם נוכח תבניות החוק הקיים – חדירה, המצאה והאזנה – נוצרים כשלי סיווג מסוימים.

EDNAKARNAVAL LIBRARY FOR THE MASSES

באלמנט סתר מוחלט, כפי שמתרחש בפעולה של האזנת סתר. קיים ספק אם חוק האזנת סתר יוכל לכסות את הסיטואציה הנדונה כאן. אפילו אם נקרא, על דרך של קל וחומר, סמכות לביצוע פעולת סתר חלקית, היכן שקמה סמכות לבצע פעולת סתר מלאה, עדיין לא ניתן לקרוא לתוך חוק האזנת סתר פעולה של המצאה במקום פעולה המתבצעת על-ידי הרשות החוקרת עצמה.

סמכות ההמצאה הקיימת כיום בחקיקה הישראלית בסעיף 43 לפסד״פ מניחה סיטואציה של הצגת חפץ או המצאת מסמכים חד פעמית, זאת בהתאם לתפישה הפיזית החולשת על סמכות זו. אין מניעה לדעתי, מבחינת לשונו של סעיף 43 לפסד״פ, לדרוש המצאה חוזרת, רב-פעמית, אולם החוק אינו מתייחס לאפשרות לדרוש המצאה רצופה, של מסירת המידע עם הגעתו לידי הנמען לצו. סעיף 3 לחוק נתוני תקשורת, המדבר על מקרה פרטי של המצאת נתוני תקשורת של בעלות רישיון בזק, מכיר באפשרות של רשויות החקירה לקבל נתוני תקשורת עתידיים שיגיעו לאחר הוצאת צו נתוני תקשורת ומסירתו לידי בעלת רישיון הבזק. ההגבלה בחוק נתוני תקשורת היא להמצאה עתידית למשך 30 יום.

ב) הוראות שמירה מכאן ולהבא (Preservation)

מבחינת צרכי החקירה במרחב המקוון, ניתן להבחין בין שלושה מצבים אפשריים:

1. מצב שבו ספקית השירות[105] נוהגת לאחסן את המידע המבוקש לחקירה דרך קבע, לא מכוח הוראה שבדין אלא לצרכיו שלו או כתוצאה מהסכם שלו עם הלקוח, ובשלב מסוים הרשות החוקרת מעוניינת לקבל את המידע האמור. דוגמה לכך היא של ספקיות הגישה לאינטרנט בארץ, אשר על פי תנאי רישיון הבזק שלהן אינן מחויבות בשמירת נתונים,[106] אולם הן מבצעות שמירה זו לצרכים שלהן בכל מקרה (לצרכי חיוב הלקוח – Billing, בקרות איכות וכדומה), זאת לפרק זמן לא ידוע ולא קבוע. בהמשך לדוגמה זו, הרשות החוקרת תוכל לקבל את המידע באמצעות צו לקבלת נתוני תקשורת לפי סעיף 3 לחוק נתוני תקשורת. דוגמה אחרת היא של מנהל אתר חברתי השומר, כחלק מהשירות ללקוחותיו, תכנים שאלה העלו או קיבלו במסגרת האתר.

2. מצב שבו ספקית השירות אינה נוהגת לאחסן את המידע המבוקש דרך קבע, והרשות החוקרת עשויה להיות מעוניינת לקבל לידיה את סוג המידע המבוקש מכאן ולהבא, למשך פרק זמן נתון,

---

[105] כוונתי כאן ב״ספקית שירות״ לספקית מכל סוג שהוא – ספקית גישה, ספקית שירותי אירוח וספקית שירותי איחסון זמני. אבחנה זו לקוחה מהצעת חוק מסחר אלקטרוני, התשס״ח – 2008, ה״ח הממשלה 356, וזו מבוססת על האבחנה כפי שמופיעה בדירקטיבה האירופית לסחר אלקטרוני: 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.

[106] ראו לעיל פרק 2, בה״ש 184.

לצרכי איסוף מידע חקירתי. במקרה כזה הפעולה הנדרשת מספקית השירות היא שמירה (Preservation), ולאחר מכן, לפי הצורך החקירתי, תוכל לפנות בבקשה להמצאה של החומר שנשמר. דוגמה לכך יכולה להיות במצב בו מבוקשת שמירת תכנים בדף אישי של משתמש בפייסבוק או שמירת תכני תיבת דוא״ל, לפני שאלה משתנים או נמחקים על-ידיד בעל חשבון הפייסבוק / הדוא״ל.

3. מצב שבו ספקית השירות אינה נוהגת לאחסן את המידע המבוקש דרך קבע, אך הרשות החוקרת מעוניינת לקבל מידע שעבר ברשותה של ספקית השירות בעבר. מטבע הדברים, מצב שכזה אינו ניתן לפתרון באמצעות צו המצאה או צו שמירה. האפשרות היחידה לאפשר קבלה של נתונים מסוג כזה היא לקבוע בחקיקה או בהוראה מחייבת של הרגולטור חובה כללית, שאינה תלויה בחשד המתעורר סביב חקירה נתונה, אשר תמנע מצב שבו מידע לא יימצא עוד ברשותה של ספקית השירות. יש שני סוגים של הטלת חובה כללית על ספקית השירות בהקשרנו: *האחד*, חובת שימור כללית ודרך קבע (Retention). *השני*, חובה של ספקית השירות ליצור תשתית טכנולוגית כללית כזו אשר תאפשר ביצוע פעולת איסוף עתידית קונקרטית על-ידי הרשות החוקרת. מבחינה עיונית, חובת ה-Retention, כמו גם חובת היצירה של תשתית טכנולוגית מתאימה לצרכי רשויות האכיפה, שונות במהותן מסמכויות האיסוף האחרות שמניתי עד כה ביחס לראיות דיגיטליות - חדירה לחומר מחשב, המצאת חומר מחשב והאזנת סתר לתקשורת בין מחשבים – כיוון שהן אינן תלויות בחשד קונקרטי. המדובר למעשה בחובות כלליות המוטלות בכפייה על ספקי השירות השונים לשמור את המידע ברשותם, כך שבבוא העת תוכל הרשות החוקרת להפעיל סמכות ולקבל את המידע המבוקש על-ידה. דהיינו, הטלת חובת Retention וחובת יצירת תשתית הטכנולוגית מהווה הפעלה של סמכות איסוף עקיפה, כזו הבונה פוטנציאל איסופי עתידי, ואינה מהווה פעולת איסוף קונקרטית כשלעצמה.

על קטגוריית המצבים הראשונה לא ארחיב, כיוון שהנתונים בקטגוריה זו יתקבלו על דרך של הפעלת סמכות לדרוש המצאה של מידע, סמכות אליה כבר התייחסתי לעיל, אשר אין בה חידוש. אפרט על סמכות להורות על שמירת מידע מכאן ולהבא, על פי הוראה קונקרטית (preservation). בחלק שלאחריו אדון בחובת השימור דרך קבע (חובת ה-Retention) ובהמשך, אתייחס לחובה ליצור תשתית טכנולוגית כללית לתועלת רשויות אכיפת החוק.

EDNAKARNAVAL LIBRARY FOR THE MASSES

הוראת שמירת המידע מכוונת בדרך כלל לצד שלישי, ספקית השירות,[107] ומורה לו לשמור את חומר המחשב האגור ברשותו ביחס לחשוד מסוים. הוראת השמירה נועדה למנוע מצב שבו, אלמלא ההוראה המחייבת, יימחק או ישתנה המידע העשוי להיות רלוונטי לחקירה. הוראת השמירה, בדומה לצו ההמצאה, מתייחסת לשני "שחקנים" מרכזיים: (1) ספקית השירות הנמענת לצו אשר נדרשת לבצע את הוראת השימור ו-(2) החשוד בגינו מבוקש שימור הנתונים. מעבר לכך, צבירת המידע מגלמת פגיעה כללית גם בצדדים שלישיים שהתקשרו עם החשוד וכן בציבור משתמשי המחשב בכללותו, אשר תחושת ה"עין הצופה" עלולה לצנן את פעילותו הלגיטימית. על הפגיעות המגולמות בהוראות השמירה ארחיב להלן בפרק 5. סמכות השמירה מכאן ולהבא יכולה להיות רלוונטית גם לראיות במרחב הפיזי, אולם בסביבה המקוונת הצורך החקירתי בהכרה בסמכות זו – מוגבר. זאת כיוון שפוטנציאל הנדיפות או הפגיעות של המידע הוא גבוה, ומנגד פוטנציאל האגירה (על דרך של שמירה) של המידע אף הוא גבוה.

הסמכות להורות על שמירת מידע אינה מנויה במפורש בחקיקה הישראלית. ניתן לנסות לקרוא אותה במשתמע כסמכות הנבלעת בתוך הסמכות לדרוש המצאה או תפיסה של חומר מחשב,[108] בבחינת אמצעי שפגיעתו פחותה המשרת את התכלית בנסיבות העניין. אולם ככלל אין זה ראוי לקרוא במשתמע מתוך החוק קיומה של סמכות איסוף ראיות, וראוי שזו תוגדר במפורש. **באמנת מועצת אירופה בדבר פשעי מחשב** מוכרת במפורש הסמכות להורות על שמירת מידע, הן תוכני והן נתוני תקשורת, ומתחייב כי כל המדינות שחתמו על האמנה ואישררו אותה יאפשרו לשמר מידע על פי בקשה של מדינה אחרת שהינה צד לאמנה.[109] החוק **בארצות-הברית** מכיר אף הוא בסמכות להורות לספקי שירות לשמור מידע ממוחשב, ואף נקבע כי הסמכות להורות על שמירת מידע כאמור נתונה בידי גורמי הרשות המבצעת (תביעה, משטרה) ולא בידי גורם שיפוטי.[110]

---

[107] עם זאת, בדומה לסעיף 43 לפסד"פ, גם צו שמירת מידע יכול להיות ממוען לחשוד עצמו, הגם שניתן להניח שהפניית צו שמירה לחשוד, כצו המצאה לחשוד, תתבצע לעתים רחוקות מאד.

[108] הכוונה לסמכות ההמצאה לפי סעיף 43 לפסד"פ, ולחלופין לסמכות התפיסה המנויה בסעיף 32 לפסד"פ, ביחד עם סעיף 34 לפסד"פ המאפשר לבית-המשפט להורות כיצד לנהוג בתפוס. והשוו, לעניין פרשנות אפשרית זו, עם קביעת בית-המשפט ביחס לסמכותו להורות על "הקפאת" חשבון בנק מכוחם של סעיפים אלה: בש"פ 5015/99 **התאחדות משפטנים בלתי תלויים נ' מדינת ישראל**, פ"ד נה(1) 657 (1999); ת"פ (מחוזי י-ם) 1071/01 **מדינת ישראל נ' רבינוביץ**, תק-מח 10(3) 16430, 16433 (2010); ה"ת (שלום ת"א) 25797-03-11 **אושרי פ. בע"מ נ' מדינת ישראל**, תק-של 11(4) 554, 555 (2011).

[109] ראו אמנת מועצת אירופה בדבר פשעי מחשב, לעיל ה"ש 16, סעיפים 16-17.

[110] ראו: 18 U.S.C. § 2703(f). כן ראו: DOJ Manual, לעיל ה"ש 86, בעמ' 139-140.

ג) הוראות שימור דרך קבע (Retention)

במשפט הישראלי לא נוהג, דרך כלל, משטר של הטלת חובות שימור כלליות. צווי ההמצאה והצווים לקבלת נתוני תקשורת, המופנים לצדדים שלישיים כדוגמת חברות אשראי, חברות סלולר או ספקיות גישה לאינטרנט, מוצאים למעשה בהסתמך הרשויות על כך שאותם גורמים נוהגים לשמור את הנתונים המבוקשים ברשותם באופן וולונטרי ודרך קבע. כחריגים ניתן לציין את משטר שימור הנתונים המוחל על הבנקים לגבי חלק מהנתונים הבנקאיים,[111] ואת משטר ניהול פנקסי החשבונות עבור רשויות המס המחייבים שמירת נתונים מסוימים להוכחת נכונות הדיווחים של ספקי השירות לרשויות המס.[112] כיוון שהשימור נעשה במרבית המקרים באופן וולונטרי, הרי המדיניות של אותם צדדים שלישיים יכולה להשתנות והם יתחילו למחוק את הנתונים הללו, באופן שישנה את ההסתמכות של הרשות החוקרת. אתר Rotter.net, הכולל גם פורום גולשים פעיל הודיע בעבר כי הפסיק לשמור נתוני IP של גולשים באתר.[113] משמעות הודעה זו היא כי אם יידרש בעתיד על-ידי רשויות החקירה או בית-המשפט לחשוף כתובת IP של גולש מסוים, לא תהיה לו אפשרות טכנית לעשות זאת. בשל היעדר משטר שימור מידע כללי בישראל, אין באפשרותן של הרשויות לעשות דבר בנדון. כן יכולה להתעורר שאלה מה תוכל הרשות החוקרת לעשות במקרה שלקוח של חברה מסוימת יבקש כי פרטיו יימחקו ממאגר מידע ממוחשב מסוים. בהנחה שבעלת מאגר הנתונים תסכים לעשות כן מבחינתה[114] והדבר לא ייאסר בהוראה כופה של המדינה,[115] דומה כי גם כאן הרשות החוקרת תאבד את היכולת לקבל את הנתונים הללו.

מבחינה טכנולוגית, יש להבחין בין שני סוגים של פעולות שימור מידע: *האחד*, שימור מידע אשר ברגיל מגיע לאגירה זמנית אצל ספק השירות ולאחר מכן נמחק או משתנה; *השני*, שימור של מידע אשר ברגיל אינו נאגר זמנית אצל ספק השירות, אולם באפשרותו הטכנית לקלוט את המידע ולאוגרו, והוראת השימור מביאה את ספק השירות לאגור את המידע לראשונה. שימור מידע מן הסוג השני קרוב יותר להקלטה מאשר שימור, באשר הוא מייצר תיעוד היכן שברגיל לא היה אמור להיווצר

---

[111] ראו למשל "שמירת מסמכים" **הוראות המפקח על הבנקים** מס' 419 (15.1.2006). על פי הוראה זו, תאגיד בנקאי מחויב לשמור מסמכים הקשורים לניירות ערך סחירים לתקופה של שבע שנים לפחות מהמועד המאוחר מבין קבלת המסמך או ביצוע העסקה. בנוסף, תאגיד בנקאי מחויב בהגנה על המסמכים האמורים ולאפשר את יכולת הגישה אליהם.

[112] ראו הוראות מס הכנסה (ניהול פנקסי חשבונות), התשל"ג -1973.

[113] ראו גל מור "מפעיל רוטר.נט: לא אהיה השטינקר של המערכת" **Ynet** 30.3.2006 http://www.ynet.co.il/articles/1,7340,L-3234413,00.html.

[114] במקרה שבעלת מאגר המידע לא תסכים לבקשת המחיקה, עלולה להיווצר "תחרות" בין בעלת המאגר לבין האדם הפרטי שפרטיו מצויים במאגר. לעניין זה, ראו את הדיון בנוגע ל"זכות להימחק" (The right to be forgotten), להלן בפרק 5(ד)(1)(א).

[115] כדוגמת ההוראות הכופות שנמנו לעיל בה"ש 111-112.

EDNAKARNAVAL LIBRARY FOR THE MASSES

תיעוד (ולו זמני). כיום, כשדנים בחובות שימור דרך קבע (retention), הכוונה היא לשימור של מידע אגור ולא ליצירת תיעוד או הקלטה דרך קבע. עם זאת, מבחינת היכולות הטכניות וצרכי החקירה, בהחלט ייתכן שיעלה הצורך ביצירת תיעוד דרך קבע, כסוג חדש, ייתכן פוגעני יותר, של שימור מידע דרך קבע.

משטר משפטי של Retention בולט באיחוד האירופי. **דירקטיבת האיחוד האירופי** משנת 2006 מחייבת את מדינות האיחוד לקבוע הוראות מחייבות של שימור מידע לפרקי זמן שנעים בין 6 ל-24 חודשים (לפי החלטתה הפנימית של המדינה) לגבי נתוני תקשורת באינטרנט ובתחום הטלפוניה.[116] הדירקטיבה מציינת כי אין לחייב בשמירת נתוני תוכן.[117] לאחרונה, פסק בית-הדין הגבוה לצדק של האיחוד האירופי (ECJ – European Court of Justice) כי דינה של הדירקטיבה האמורה – להיפסל, בשל העובדה שהיא קובעת פגיעה גורפת בפרטיות, שלא על בסיס חשד קונקרטי.[118] חרף הפסיקה האמורה, ההוראות בדין הפנימי של מדינות האיחוד האירופי, אשר פעלו על פי הדירקטיבה האמורה, עומדות בעינן, שכן הן כפופות לביקורת חוקתית פנים-מדינתית, ואינן יכולות להתבטל מאליהן כתוצאה מן הפסיקה האמורה. **בארצות-הברית**, בה הוכרה סמכות ה-Preservation, לא הוכרה סמכות להטיל חובות שימור כלליות. ניסיון להכניס חובות שימור כלליות לספקי שירות שונים במסגרת ה- USA PATRIOT Act משנת 2001 - לא צלח. לאחרונה קבע בית-משפט פדראלי לערעורים כי חוק ה- PATRIOT אינו מתיר ל-NSA לאסוף נתוני תקשורת (טלפונית ואינטרנטית) באופן רוחבי, שלא על

---

[116] ראו: Directive 2006/24/EC of the European Parliament and of the Council (15.3.2006) on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105. כן ראו: Jeremy Warner, *The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps*, 2 U. OTTAWA L. & TECH. J. 75, 80-90 (2005) לתיאור התפתחות משטר ה-Retention במשפט האירופי. כן ראו: Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, 45 (2003). כדוגמה ליישום הוראות הדירקטיבה בחקיקה הפנימית של מדינות האיחוד האירופי, ראו למשל את חוק הביטחון היומיומי בצרפת: Loi sur la sécurité quotidienne 2001 (LSQ), שם נקבעו חובות שימור מידע על ספקי שירות באינטרנט למשך שנה.

לדיון בביקורות על משטר ה-Retention, ראו למשל: Catherine Crump, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191 (2003); Patrick Breyer, *Telecomunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, 11 EUROPEAN L.J. 365 (2005). כן ראו אתר האינטרנט של קבוצת העבודה הגרמנית בנושא שימור מידע (German Working Group on Data Retention): http://www.vorratsdatenspeicherung.de/content/view/13/37/lang,en/.

[117] ראו סעיף 5.2 לדירקטיבה.

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

EDNAKARNAVAL LIBRARY FOR THE MASSES

בסיס חשד קונקרטי וממוקד, אף אם הדבר נעשה למטרות חקירה ומניעה של טרור.[119] אף לאחר חקיקת חוק ה-PATRIOT נערכו כמה ניסיונות, שלא הושלמו, להטיל חובות שימור כלליות לצרכי חקירה של עבירות מין בקטינים באמצעות האינטרנט.[120] כאמור, משטר שימור המידע דרך קבע עורר התנגדויות מהכיוון החוקתי. ארחיב על כך בפרק הבא, בו אדון בהשלכות הזירה האינטרנטית על השיח החוקתי בקשר לדיני איסוף הראיות בחקירה פלילית.

ד) <u>הוראות ליצירת תשתית המאפשרת לרשות לאסוף ראיות דיגיטליות</u>

הכוונה כאן להוראות המטילות חובה לספק תשתית טכנולוגית לשימוש עתידי קונקרטי על-ידי הרשות החוקרת. סמכות זו נבדלת מחובת השימור דרך קבע (Retention) בשני המובנים הבאים: (א) חובת ה-Retention למעשה כוללת את החובה ליצור תשתית הטכנולוגית מתאימה לשימור המידע, אלא שבנוסף אליה היא גם כוללת שימוש גורף באותה תשתית טכנולוגית לצורך שימור הנתונים בפועל. כתוצאה מכך, חובת ה-Retention מגלמת פגיעה ישירה יותר בזכות לפרטיות, באשר פוטנציאל הפגיעה הגורפת לא רק קיים מבחינה טכנולוגית אלא גם ממומש מבחינה מעשית, בעצם אגירת הנתונים דרך קבע על-ידי ספקית השירות. עם זאת, בהחלט יש להביא בחשבון את הפגיעה הפוטנציאלית המגולמת בהוראות המחייבות את ספקיות השירות ליצור תשתית טכנולוגית לצרכי הרשות החוקרת – פגיעה זו נוגעת לתחושת המעקב הכללית (פן-אופטיקון האינטרנטי) וכן פוגעת בחופש העיסוק ובקניינן של ספקיות השירות. (ב) חובת ה-Retention מטילה נטל ישיר על ספקית השירות, בעוד שההוראות המחייבות יצירה של תשתית טכנולוגית מניחות כי פעולות שימור המידע והגישה אליו ייעשו על-ידי הרשות החוקרת עצמה. יש בכך משום ניסיון להקטין את הנטל המונח על כתפי ספקית השירות (אם כי גם יצירת תשתית טכנולוגית עלולה לגזול משאבים מהספקית), הגם שאין להתעלם מן העובדה שהטלת

---

[119] ראו: ACLU v. Clapper, 2015 WL 2097814 (2nd Cir. 2015). בכך פסל בית-המשפט הפדראלי לערעורים את הפרקטיקה לפיה הממשל האמריקני נהג לפרש את סעיף 215 לחוק ה-PATRIOT ככזה המאפשר, הלכה למעשה, שמירת מידע לא-תוכני (דהיינו נתוני metadata) ביחס לחלק נכבד מאזרחי המדינה.

[120] ראו למשל: The Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY), H.R. 1076 (111th Congress, 2009), ניתן לעיון ב: http://www.govtrack.us/congress/bill.xpd?bill=h111-1076. ב-25.5.2011 הוצגה הצעת חוק: Protecting Children from Internet Pornographers Act of 2011, H.R. 1981 (112th Congress, 2011), ניתן לעיון ב: http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.1981. הצעת החוק אושרה בקריאה ראשונה בבית הנבחרים ביולי 2011. כמה נציגים של בית הנבחרים האמריקני הביעו הסתייגות מבחירת השם של הצעת החוק, שלכאורה דן בהגנה על קטינים בפני תוכן מיני פוגעני, בעוד שבפועל, דרך סוגיה זו, הוחדרה סוגיה של שימור מידע דרך קבע, המתייחסת לאגירה של נתוני הגלישה של כל מנוי אצל ספק השירות. "ספק השירות" מוגדר בצורה רחבה החלה על כל: "provider of an electronic communication service or remote computing service". ראו: Declan McCullagh, *House Panel Approves Broadened ISP Snooping Bill*, CNET (28.7.2011) http://news.cnet.com/8301-31921_3-20084939-281/house-panel-approves-broadened-isp-snooping-bill/.

חובות שכאלה על ספקיות התקשורת משמעה התערבות ישירה של המשפט באופן הפיתוח הטכנולוגי של ספקיות השירות.

החובה ליצור תשתית טכנולוגית לשימוש עתידי של רשויות החקירה אינה סמכות הנדרשת לראשונה בעידן הסייבר, ולמעשה, כבר בעידן של טלפוניה קווית נדרשו חברות הטלפון לבנות תשתית טכנולוגית אשר תאפשר האזנת סתר על-ידי רשויות החקירה. עם זאת, בעידן הסייבר ניתן לומר כי נפתח פער טכנולוגי הולך וגובר בין הרשות החוקרת לבין מכלול השירותים והיישומים שהרשת מאפשרת. כמו כן, נוכח התופעה שלפיה הפעילות במרחב הסייבר, בפרט באינטרנט, מתווכת לרוב על-ידי ספקיות שירות שונות, הטלת החובה עליהן לספק תשתית טכנולוגית לשימוש רשויות החקירה מאפשרת דילוג מעבר למשוכה הייחודית הניצבת בפני הרשות החוקרת בזירה הממוחשבת.

בחקיקה הישראלית יש למנות כאן את הוראת סעיף 13(ב)(2)לחוק התקשורת, הקובעת שראש הממשלה רשאי להורות לבעלות רישיון בזק להתקין מתקן או לבצע התאמה טכנולוגית למתקן בזק, לרבות מתן גישה למתקן הבזק, הכל כדי לאפשר לרשויות הביטחון, בכלל זה המשטרה, למלא את תפקידיהן. ההוראה חלה על ספקיות התקשורת (טלפונית, סלולרית, גישה לאינטרנט) בעלות רישיון בזק בלבד, ומכאן שהיא מוגבלת בהיקף פרישתה. במלים אחרות, סמכות איסוף זו קיימת באופן חלקי בלבד במשפט הישראלי. כפי שפירטתי לעיל בפרק 2, **בארצות-הברית** קיימת חקיקה משנת 1994 המחייבות ספקיות תקשורת לבנות תשתית טכנולוגית אשר תאפשר ביצוע האזנות סתר על-ידי רשויות החקיקה.[121] **בבריטניה** ישנן גם כן הוראות חוק המתייחסות לסוגיית החיוב של ספקיות תקשורת, בכללן ספקיות גישה לאינטרנט, לבנות תשתית טכנולוגית שתאפשר האזנת סתר על-ידי הרשויות החקירה.[122]

בסיכומו של דבר, הצורך החקירתי להטיל חובות כלליות על ספקיות שירות במרחב המקוון ליצור תשתית טכנולוגית, שתאפשר איסוף מידע, נועד למעשה לשמור על פוטנציאל עתידי לעיון במידע הדיגיטלי, אשר ברגיל הינו נזיל, ניתן למחיקה או לשינוי, לעתים אף באופן אוטומטי בלא פעולה אקטיבית כלשהי מצד המשתמש במידע או ספק השירות המאחסן את המידע. בכך צורך חקירתי זה משלים את פעולות האיסוף של שימור מידע דרך קבע (Retention) ומכאן ולהבא (Preservation).

---

[121] CALEA (Communications Assistance for Law Enforcement Act), מקודד כ- 47 U.S.C. § 1001-1010.

[122] ראו: Regulation of Investigatory Powers Act, 2001, c. 23 § 12 (Eng.).

ה) חדירה סמויה לחומר מחשב והעתקת המידע ממנו

את פעולת האיסוף של "חדירה סמויה לחומר מחשב" אפשר לחלק לשלוש תת-פעולות נפרדות במהותן: *האחת*, עצם הגישה באופן סמוי לחומר המחשב והכניסה אליו; *השנייה*, ביצוע העתקה סמויה של חומר מחשב, לאחר ביצוע כניסה סמויה כאמור; *השלישית*, עיון בחומר שהועתק באופן סמוי, מבלי שהחשוד יודע על כך. אלמנט הסֵתֶר מייחד את הסמכות הזאת מסמכות החדירה והתפיסה הרגילים.

הצורך החקירתי המיוחד בפעולה של חדירה סמויה לחומר מחשב והעתקת המידע מתוכו נובע מכך שהמידע נדיף ופגיע (ניתן לשינויים). לעתים, עד לפרוץ החקירה הגלויה ותפיסת מחשבו של החשוד, עלול המידע להשתנות, ומצבו עם פרוץ החקירה הגלויה לא יוכל להעיד על מצבו הרלוונטי בעת ביצוע העבירה. לכן, יש אינטרס מובהק לרשויות החקירה להתקרב עד כמה שניתן למידע בצמוד למועד ביצוע העבירה. כיוון שהמידע ניתן להעתקה מרחוק, מתאפשר טכנית לבצע פעולה של חדירה סמויה לחומר מחשב מבלי להגיע פיזית אל המחשב עצמו. כיוון שהמידע ניתן להעתקה מלאה, ניתן לייחס משמעות ראייתית טובה למידע כפי שיתקבל כתוצאה מחדירה סמויה למחשב. זאת לעומת המצב לגבי ראיות פיזיות, אשר אם לא תופסים אותן פיזית (מה שכמובן אינו אפשרי במהלך חיפוש סמוי, שכן אז תתגלה נוכחות החוקרים במקום), ניתן רק להציע תיעוד משני שלהן (כגון צילום), שנפקותו הראייתית עשויה להיות חסרה. בשל כל אלה, ניתן לומר כי הצורך החקירתי בסמכות חדירה סמויה והעתקת המידע מהמחשב הנחדר – מוגבר לעומת הצורך החקירתי בהענקת סמכות חיפוש סמוי בחצרים.[123]

אמחיש את הצורך בפעולת איסוף של חדירה סמויה לחומר מחשב, בשתי דוגמאות: (א) מתעורר חשד שאדם מפיץ תכנים פדופיליים באמצעות מחשבו האישי. המשטרה מעוניינת להעתיק את התכנים האמורים, ולהמשיך לעקוב באופן סמוי אחר פעולתו של החשוד, זאת על מנת לבחון האם הוא משתף בתכנים גם גולשים נוספים. (ב) נניח, בפרפראזה על עובדות המקרה בפרשת הסוס הטרויאני,[124] שמוגשת תלונה על חדירה למחשבו של אדם מסוים. המשטרה בודקת את המחשב הנחדר ומגלה כי הוא נגוע בסוס טרויאני, המשגר קבצים אישיים ועסקיים מהמחשב אל שרת FTP כלשהו. המשטרה מעוניינת להעתיק את התכנים המצויים בשרת ה-FTP לצורך הוכחת גניבת המידע על-ידי החשודים, לכשתאתר אותם ותעצור אותם. חששה של המשטרה הוא כי עד לאיתור החשודים כאמור, המידע

[123] בכל הנוגע לחיפוש סמוי בחצרים, נכון להיום סמכות כזו אינה מותרת במשפט הישראלי, למעט בחוק שירות הביטחון הכללי, התשס"ב - 2002, בו נקבעה בסעיף 10 סמכות לביצוע חיפוש סמוי בכלי רכב ובחצרים למטרות מודיעין, דהיינו שלא למטרות של הצגת ראיות קבילות ומהימנות לבית-המשפט.

[124] לתיאור עובדות המקרה ראו לעיל פרק 2, בה"ש 98.

EDNAKARNAVAL LIBRARY FOR THE MASSES

האגור בשרת ה-FTP יימחק על-ידיהם באופן יזום או אוטומטי. באמצעות פעולה של חדירה סמויה לחומר מחשב תוכל המשטרה לאסוף את הראיות הדיגיטליות מבלי לחשוש שהן תתנדפנה או תשתנינה עד לפרוץ החקירה הגלויה.

על מנת לחדד את הבנת מהותה של סמכות החדירה הסמויה לחומר המחשב אבקש להשוות בקצרה את הסמכות הזאת לשתי סמכויות איסוף אחרות המוכרות כיום בחקיקה הישראלית ואשר גם בהן ישנו אלמנט הסתרה של פעולת האיסוף מפני החשוד: סמכות לביצוע האזנת סתר לתקשורת בין מחשבים וסמכות לדרוש המצאה על-ידי צד שלישי מבלי ליידע את החשוד על כך.

אשר להבדל בין חדירה סמויה למחשב לבין האזנת סתר למחשב: בשתי פעולות אלה אלמנט הסתר קיים, אולם האזנת הסתר היא לתקשורת בין מחשבים, ואילו החדירה הסמויה לחומר המחשב מתייחסת למחשב הקצה עצמו, ולמידע האגור בו. האזנת הסתר צופה פני עתיד במהותה, בהיותה מכוונת לשיחות שיתקבלו מכאן ולהבא, בעוד שהחדירה הסמויה לחומר המחשב צופה פני עבר ומתייחסת למידע הקיים. ההשוואה האמורה מלמדת כי לא ניתן לקרוא לתוך סמכות האזנת הסתר לתקשורת בין מחשבים גם סמכות לביצוע חדירה סמויה לחומר מחשב, ועל כן יש לבחון את האפשרות לכונן הסמכה לפעולה כזאת במפורש על-ידי המחוקק.[125] וכך, אם מותר למשטרה להתקין רכיב שיאזין לתקשורת בין מחשבים, אסור לרכיב זה להעתיק במקביל גם את תכולתו הקיימת של המחשב, שכן הפעולה האחרונה מהווה חדירה סמויה לחומר המחשב.

אשר לאבחנה בין חדירה סמויה למחשב לבין המצאת מידע בלי ידיעת החשוד: המצאה על-ידי צד שלישי לעולם אינה פעולת איסוף סמויה לחלוטין, שכן מטבע הדברים הצד השלישי הנמען לצו נמצא בסוד העניינים. עם זאת, פעולת ההמצאה יכולה להיות סמויה מפני החשוד, ככל שניתנת הוראה שיפוטית על איסור יידוע החשוד. הוראה זו חלה על הצד השלישי הנמען לצו ההמצאה. חוק נתוני תקשורת קובע בסעיף 5 ברירת מחדל של אי-יידוע החשוד: הנמען לצו נתוני תקשורת לא יגלה לכל גורם שהוא את העובדה שמסר נתוני תקשורת, אלא אם כן קבע בית-המשפט אחרת בצו נתוני התקשורת. סעיף 43 לפסד״פ, לעומת זאת, שותק בכל הנוגע לעניין אי-יידוע החשוד (או כל גורם אחר). הפרקטיקה הנוהגת היא שהמשטרה מבקשת מבית-המשפט בצו ההמצאה כי הנמען לצו לא יודיע על דבר ביצוע הצו, ובית-המשפט אינו דוחה את הבקשה.[126] על פי מיטב בדיקתי, פרקטיקה זו לא נתקפה בבתי-

---

[125] הבחינה צריכה להיערך בכפוף לעריכת איזון חוקתי בין הצורך החוקתי לזכויות העתידות להיפגע.

[126] על הפרקטיקה הזאת ניתן ללמוד מהפרסום על תיק החקירה נגד ארקדי גיידמאק, שבו ביקשה המשטרה לקבל נתונים על אודות חשבונות בנק השייכים לגיידמאק. הנתונים התבקשו על פי סעיף 43 לפסד״פ. בטופס המשטרתי של צו ההמצאה הופיע המשפט ״אין/ניתן להודיע לחשוד או לבעלי החשבונות בדבר קיום הצו או החקירה או כל פרט הקשור אליה״. חוקרת המשטרה שערכה את הבקשה מחקה בטעות את המילה ״אין״ במקום את המילה ״ניתן״, והשופטת חתמה על הצו

EDNAKARNAVAL LIBRARY FOR THE MASSES

המשפט, חרף העובדה שהיא מגלמת פגיעה בזכות להליך הוגן (זכות החשוד לדעת על אודות הליכים הננקטים נגדו) ועל כן התרתה אינה דבר המובן מאליו.[127] בשונה מחדירה סמויה לחומר מחשב, כשמדובר בהמצאת חומר מחשב על-ידי צד שלישי ללא יידוע החשוד, מופחת באופן משמעותי החשש להשתלת ראיות. זאת כיוון שאיסוף הראיה בפועל נעשה על-ידי צד שלישי חיצוני, והוא עשוי לגַבּוֹת את פעולת האיסוף שביצע ברשותו, לשמור לעצמו העתק לצרכי התדיינות עתידית סביב הפעולה או כדומה. כמו כן, הצד השלישי הנמען לצו עשוי לעורר התנגדויות לצו ההמצאה, אשר תשרתנה למעשה את החשוד.[128]

פעולת האיסוף של חדירה סמויה לחומר מחשב אינה זוכה להתייחסות בחקיקה הישראלית.[129] בארצות-הברית, מוכרת הסמכות לערוך חיפוש סמוי בחצרים ("Sneak and peek" searches). הסמכות כוללת גם אפשרות לערוך חדירה סמויה למחשב ובלבד שבית-המשפט המסמיך יתייחס מפורשות לכך שמדובר בחדירה לחומר מחשב. התפישה, על פי הדין האמריקני, הינה כי החיפוש הסמוי – והחדירה הסמויה – נעשים תוך השהיית היידוע של המחזיק כדין.[130] השהיית היידוע יכולה על פי רוב להיות לפרקי זמן של ימים או שבועות, אך לא יותר.[131] ישנה הבחנה בין חיפוש סמוי ולבין תפיסה סמויה, אשר תותר במקרים מצומצמים עוד יותר. גם העתקה סמויה, שאינה כוללת תפיסה, נחשבת לפעולה

כמבוקש. כתוצאה מכך, הבנק הנמען לצו יידע את גיידמאק בדבר פעולת האיסוף שבוצעה ביחס לחשבונו. על פי הפרסום, בתגובה הוציא גיידמאק את הכספים מאותם חשבונות בנק, ובכך נמנעה אפשרות הקפאתם או חילוטם. לדיווח על הפרשייה, ראו למשל: יוסי מלמן "הטעות" **הארץ Online** 2.2.2006 http://www.haaretz.co.il/hasite/pages/ShArtPE.jhtml?itemNo=677457&contrassID=2&subContrassID=13&sbSubContrassID=0.

[127] בארצות-הברית נדונה חוקתיותה של הוראת אי-יידוע גורפת לגבי פעולות איסוף של רשויות החקירה האמריקניות המכונות NSL (National Security Letters). המדובר בסמכות לדרוש המצאה של נתונים מסוימים במסגרת הוראה מנהלית (של דרג מסוים ברשויות האכיפה, ולא במסגרת צו שיפוטי). סמכות זו הורחבה משמעותית במסגרת ה- USA PATRIOT Act, חוק פדרלי שנחקק אחרי פיגועי ה-11/9 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act). סמכות ה-NSL שנקבעה ב- 18 U.S.C. § 2709 נתקפה תקיפה חוקתית על-ידי ספקיות גישה לאינטרנט שנדרשו להמציא נתונים בדרך זאת. נטען כנגד היעדר הביקורת השיפוטית על השימוש בסמכות ה-NSL, על הפגיעה שלה הסמכות הזאת הן בזכויות החשוד והן בזכויות של ספק הגישה הנמען לצו. בפרט נטען לגבי הוראת איסור היידוע הגורפת, ובית-המשפט קיבל את הטענות נגד חוקתיות הוראת החוק, לרבות לגבי הוראת איסור היידוע הגורפת. ראו: Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); Doe v. Gonzales, 386 F. Supp. 2d 66 (D. Conn. 2005). בין ההחלטה לבין פסק-הדין בערעור, תוקן החוק כך שנקבע כי לספקיות השירות תהא זכות עמידה בבית-המשפט כדי להתנגד, במקרה נתון, להוראת איסור היידוע. בשל תיקון זה, נקבע כי אין לפסול את פרקטיקת ה-NSL כבלתי-חוקתית. ראו: Doe v. Gonzales, 449 F. 3d 415 (2nd Cir. 2006).

[128] כך אירע למשל בעניין *נטוויז'ן*, לעיל ה"ש 64, שבו ספקית הגישה לאינטרנט התנגדה לביצוע צו המצאה אשר דרש ממנה למסור לרשויות החקירה תכתובות דוא"ל של חשוד.

[129] כאמור לעיל בה"ש 123, דווקא חיפוש סמוי בחצרים זכה להתייחסות המחוקק, במסגרת חוק השב"כ, ונבחנה הוספת סמכות זו במסגרת ועדת לוין.

[130] ראו: 18 U.S.C. § 3103a כפי שתוקן באמצעות ה-USA PATRIOT Act. להרחבה ראו: DOJ Manual, לעיל ה"ש 86, בעמ' 83.

[131] ראו למשל: United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000) שם אושרה בדוחק השהייה של היידוע למחזיק על אודות החיפוש הסמוי שנערך אצלו למשך 45 יום. מנגד, ראו: United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986), שם נפסק כי יידוע המחזיק על אודות החיפוש בחצריו חייב להיעשות תוך זמן סביר אך קצר ("a reasonable, but short, time").

המצריכה התייחסות קונקרטית בצו השיפוטי המסמיך, ואין זו בגדר סמכות לוואי לעצם הכניסה הסמויה.[132]

בקנדה קיימת סמכות חדירה סמויה לחומר מחשב, הנובעת מסמכות החיפוש המנוסחת באורח כללי וגורף בקוד הפלילי הקנדי. החדירה יכולה להיחשב כסמויה באורח זמני בלבד, כאשר בית-המשפט רשאי להאריך את תקופת ההשהיה של ההודעה לפרקי זמן שונים, שלא יעלו על 3 שנים.[133]

בגרמניה נדרש בית-המשפט העליון הפדרלי לסוגיית החדירה הסמויה למחשב בשנת 2008. באותו מקרה נבחנה חוקתיותו של חוק של מדינת North Rhine-Westphalia אשר התיר ביצוע חדירה סמויה למחשבים שונים באינטרנט למטרות איסוף מודיעין וחקירות. החוק נוסח באופן גורף למדי מבחינת היקף הסמכות לבצע חיפושים סמויים. נקבע כי סמכות החדירה הסמויה למחשב, כפי שנוסחה בחוק, פוגעת באופן בלתי מידתי בזכות החוקתית לפרטיות ובתרגומה של זכות זו למרחב הממוחשב. כן נקבע כי ניתן, עקרונית, להתיר חדירה ומעקב סמוי אחר מחשבים באינטרנט אך ורק בנסיבות של סכנה מידית לגופו או לחירותו של אדם, ותוך נקיטת אמצעי זהירות ממשיים להגנת אזורי הפרטיות במחשבו של אדם.[134]

בסיכומו של דבר, נראה כי קיים צורך חקירתי בביצוע חדירה סמויה לחומר מחשב. צורך חקירתי זה מוגבר יחסית למקבילו בעולם הפיזי, לנוכח תכונותיה של הראיה הדיגיטלית כראיה נדיפה ופגיעה מצד אחד, אך גם ניתנת להעתקה (להבדיל ממוצגים חפציים) מצד שני. עם זאת, הדיון בעצם ההכרה בסמכות איסוף של חדירה לחומר מחשב יצטרך להתחשב בפגיעות המיוחדות והחריפות המגולמות בסמכות זו, הן ברמה הקונקרטית של החשוד והן ברמה של כלל ציבור משתמשי המחשב.

<u>ו) תיעוד סמוי של הפעילות במחשב הקצה</u>

הסמכות הקיימת כיום לביצוע האזנת סתר ל"תקשורת בין מחשבים", מתייחסת למעשה לתיעוד התעבורה ממחשב אחד לאחר. התוכן האצור בכל מחשב קצה כשלעצמו – אינו בר-האזנה, וכל עוד אין סמכות לחדירה סמויה והעתקה סמויה של חומר המחשב – הוא אינו בר-העתקה, אלא בשלב החקירה הגלויה. קיימות לפחות שתי קטגוריות נוספות של מצבים, שבהם מתעורר צורך חקירתי שאינו מכוסה במסגרת חדירה והעתקה סמויה של חומר המחשב וכן אינו מכוסה בהאזנת סתר לתקשורת בין

---

[132] ראו: DOJ Manual, לעיל ה"ש 86, בעמ' 83.

[133] ראו: Criminal Code, R.S.C. 1985, c. C-46, s. 487.01 (Ca.).

[134] ראו: Ms. W. v. North Rhine-Westphalia, 1 BvR 370/07 (2008). תרגום רשמי של פסק-הדין לאנגלית מצוי ב: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html.

EDNAKARNAVAL LIBRARY FOR THE MASSES

מחשבים: *האחת*, כאשר נוצר הצורך לתעד את האופן שבו הופק ונצרך בפועל המידע שנשלח ממחשב הקצה ושנשלח אל מחשב הקצה. *השנייה*, כאשר רשויות החקירה מבקשות לאסוף מידע העובר בפועל בתקשורת בין מחשבים, אלא שהוא עובר במצב מוצפן שאינו ניתן לפיענוח, ובמחשב הקצה הוא נשמר במצב מוצפן או שאינו נשמר כלל. אבהיר.

1. ישנם מצבים בהם מידע ממוחשב מסוים זורם בתקשורת בין מחשבים, אך אינו נצפה בפועל על-ידי משתמש הקצה. כך הוא, למשל, במקרה שבו משתמש הקצה פותח מספר חלונות במקביל, ואל כולם מועבר מידע באמצעות האינטרנט, אולם משתמש הקצה צופה בפועל רק באחד מהחלונות הללו. דוגמה נוספת היא כאשר מחשב הקצה של המשתמש מבצע פעולות אוטומטיות של תקשורת בין מחשבים, בעוד שפעולות אלה לא התבצעו ביוזמה של משתמש הקצה, ולעתים אף לא בידיעתו. כיוון שעשוי להתעורר צורך חקירתי בהוכחת השימוש / הצריכה בפועל של החשוד את התכנים העוברים בתקשורת בין מחשבים, הרי שהאזנת סתר ל"תקשורת בין מחשבים" לא בהכרח תספק את הצורך האמור במלואו. גם העתקה סמויה של המידע מהמחשב, לאחר אגירתו (ובהנחה שאכן כל המידע שעבר בתקשורת בין מחשבים אכן נאגר במחשב בסופו של דבר). מכאן, הצורך לבצע פעולה של תיעוד מסך המחשב (Screen capturing או Screen shooting) של משתמש הקצה.[135]

2. הדוגמה המובהקת למידע העובר בפועל בתקשורת בין מחשבים במצב מוצפן, ואינו נשמר במחשב הקצה או שנשמר במצב מוצפן, היא הדוגמה של סיסמאות גישה לאתרים מסוימים. האזנת סתר, כמו גם העתקה סמויה, לא יאפשרו חשיפה של הסיסמה. בנוסף, גם צילום מסך

---

[135] סמכות נוספת, קרובה במהותה, שנדונה בשנים האחרונות בישראל, היא הסמכות לתיעוד חזותי סמוי ברשות היחיד (צילום סתר). סמכות צילום הסתר היא מעין סמכות מקבילה לסמכות האזנת ה"נפח" (קרי האזנה למקום, להבדיל מהאזנה לקו תקשורת מסוים). צילום הסתר מאפשר הוספת ערוץ וידאו לערוץ האודיו, הקיים היום בידי רשויות החקירה במסגרת חוק האזנת סתר. סמכות מעין זו קיימת גם במדינות שונות בעולם: ראו בקנדה: Criminal Code, R.S.C. 1985, c. C-46, s. 487.01 (Ca.); בדרום אוסטרליה: Listening and Surveillance Devices Act 1972, s. 3, 6 (South Au.); בניו-סאות' ויילס שבאוסטרליה: Surveillance Devices Act 2007, s. 4, 17 (New South Wales). בארצות-הברית טרם הוסדר הנושא במפורש בחקיקה, ובשנת 2010 הוצגה הצעת חוק בנושא: Surreptitious Video Surveillance Act of 2010, S. 3214 (111th Congress, 2010). במצב החוקי הקיים הפסיקה נטתה לראות בסמכויות ההאזנה ככוללות גם סמכות לצילום סתר. ראו למשל: United States v. Torres, 751 F.2d 875 (7th Cir. 1984); United States v. Shryock, 342 F.3d 948, 978 (9th Cir. 2003). במסגרת הצעת חוק האזנת סתר (תיקון מס' 6), התש"ע – 2009, ה"ח הממשלה 455, הוצע לכלול סמכות זו: "*שוכנע מי שמוסמך להתיר האזנת סתר לפי חוק זה, כי למטרות ההאזנה נדרש גם תיעוד חזותי ברשות היחיד, רשאי הוא להתיר גם התקנת ציוד הנדרש לשם כך*" (ראו סעיף 9 להצעת החוק, שנועד להוסיף לחוק האזנת סתר את סעיף 10(ב), תחת הכותרת "סמכויות עזר"). הצעת החוק מבוססת על מסקנות צוות בדיקה לנושא האזנות סתר בראשות המשנה ליועץ המשפטי לממשלה דאז, לבנת משיח, שהוגשו ליועץ המשפטי לממשלה בשנת 2005 (בתחילת שנת 2012 הוחל בדיונים בהצעה זו בוועדת חוקה, חוק ומשפט של הכנסת כהכנה לקריאה שניה ושלישית). הבחירה לראות סמכות זו כ"סמכות עזר" מוקשה בעיני, שכן מדובר בסמכות פוגענית באופן משמעותי, שאינו מיועד לתמוך בסמכות ההאזנה, אלא הוא בבחינת כלי חקירה בעל נפקויות ותועלות כשלעצמו.

הצורך החקירתי ביחס לתיעוד חזותי ברשות היחיד לא התעורר ביחס לראיות דיגיטליות. כעולה מהפרוטוקולים של ועדת משיח, הצורך התעורר ביחס למעשים מפלילים מסוימים הנעברים במרחב הפיזי (לדוגמה, תיעוד מפגש מסוים, תיעוד מעשה אלימות של אדם אחד כלפי אחר ועוד). סמכות התיעוד החזותי ברשות היחיד, ככל שתיושם לראיות הנוגעות לפעילות החשוד באינטרנט, תספק מענה חסר. לכאורה ניתן יהיה לתעד את דפי האינטרנט שנצפו בפועל על-ידי משתמש הקצה, על-ידי הפניית מצלמת הסתר אל מחשב הקצה, אולם ככל שמדובר במחשב נייד, יקשה לספק צילום סתר עקבי. יתר על כן, כלי זה לא מסוגל לחשוף סיסמאות המוקלדות על-ידי המשתמש (ולא נראות על מסך המחשב באופן גלוי).

EDNAKARNAVAL LIBRARY FOR THE MASSES

המחשב של משתמש הקצה (Screen capturing) לא ישרת את המטרה החקירתית המבוקשת, שכן על פי רוב הקלדת הסיסמה תוצג על המסך כרצף של כוכביות. לעומת זאת, "הקלטה" של הקלדות המקלדת (Key logging) תספק את המבוקש לעניין זה.

הצורך החקירתי בתיעוד סמוי של הפעילות במחשב הקצה מבקש לנצל את פוטנציאל התיעוד הקיים ביחס לראיה הדיגיטלית, את העובדה שניתן לערוך את התיעוד מרחוק, ואת העובדה שכך ניתן להתגבר על אפשרויות להצפנת התקשרויות ועל אפשרויות לטשטוש, הסוואה, מחיקה או שינוי של הראיות הדיגיטליות. ברי כי ככל שתוכר הסמכות לתעד באופן סמוי את הפעילות במחשב הקצה, הרי שהכרה כזו משמעה פגיעה רחבה בזכויות מוגנות של החשוד וכלל ציבור משתמשי המחשב והאינטרנט. על כך ארחיב להלן בפרק 5(ד).

ז) פיצוח הצפנות והתגברות על סיסמאות

הצפנות וסיסמאות הגנה מגלמות סוג של "עזרה עצמית" של המשתמש במחשב, על-ידי שימוש יזום שלו בטכנולוגיות מגבירות פרטיות המכונות PETs (Privacy Enhancing Technologies). ההצפנה נועדה להגן על המידע מפני חשיפתו על-ידי גורמי חוץ; הסיסמה נועדה לאמת את זהות הגורם הניגש אל המידע. ההצפנה מערבלת את תוכן המידע עצמו, בעוד שהסיסמה חוסמת את הגישה אל המידע, הגם שזה אינו מעורבל.[136] השימוש בהצפנות ובסיסמאות הפך לנפוץ ומקובל עד מאד בעידן האינטרנט, ולעתים חומרי המחשב מוצפנים על-ידי ספקיות השירות השונות באינטרנט מבלי שהמשתמש הפרטי נקט פעולה אקטיבית כלשהי.[137] הצפנות טובות למדי ניתנות כיום להורדה חינם דרך האינטרנט,[138] להתקנה ולהפעלה עצמיים גם על-ידי הדיוטות. הצפנות אלה עלולות לגרום למצב בו פיצוחן יארך זמן רב, יגזול משאבים, ולעתים קרובות אף יהיה פשוט בלתי אפשרי.[139] מכאן, שעלולה להיווצר הטיה אסטרטגית של מאזן ה"כוחות" בין הרשות החוקרת לבין החשוד. מנגד, שימוש בהצפנות ובסיסמאות

---

[136] להרחבה על תורת ההצפנה (קריפטוגרפיה), מטרות ההצפנה וסוגיה השונים, לעומת הגנת הסיסמה, ראו למשל: ALFRED J. MENEZES, PAUL C. VAN-OORSCHOT & SCOTT A. VANSTONE, HANDBOOK OF APPLIED CRYPTOGRAPHY 1-48 (1996).

[137] למעשה מרבית אמצעי התקשורת השונים באינטרנט (דוא"ל, Bluetooth, VoIP ועוד) מאובטחים כיום באמצעי הצפנה ברמה כזאת או אחרת. ראו: Kozlovski, לעיל ה"ש 55, בעמ' 80-87. ראו עוד, למשל את: http://www.skype.com/en/security/#encryption.

[138] ראו, למשל, את האתר http://www.pgpi.org/, המציע הצפנת PGP (Pretty Good Privacy) להורדה ושימוש חינם.

[139] ראו: LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 36 (1999), שם לסיג מגדיר את השימוש בהצפנות באינטרנט כבעל פני יאנוס: מצד אחד הוא עשוי להגביר את תחושת החירות מפני מעקב באינטרנט, אך בה בעת הוא עלול להיות טכנולוגיה הרסנית שתעלה את כוחם של גורמים זדוניים כך שלא ניתן יהיה לטרפד את מעשיהם בזכות הניצול לרעה שלהם את טכנולוגיית ההצפנה הדיגיטלית. כן ראו: Neal Kumar Katyal, *Criminal Law in Cyberspace*, 146 U. PA. L. REV. 1003, 1049-1070 (2001).

מבטא את מימוש הזכות לפרטיות, ועל המשמעות החוקתית של השימוש בטכנולוגיות מגבירות פרטיות אעמוד בפרק הבא.

שאלת גבולות הסמכות של הרשות החוקרת לפתוח הצפנות או סיסמאות הגנה לא נדונה כלל במשפט הישראלי.[140] הדבר נובע מן התפישה הפיזית ביחס לראיה הדיגיטלית, אשר על פיה שלב העיון במידע אינו זוכה להתייחסות, אלא שלב תפיסת המידע והעתקתו בלבד. ככל שהרשות החוקרת תצטייד בצו חדירה כדין, הרי שהעיון במידע, לרבות פיענוח הצפנות ופריצת סיסמאות הגנה, יתבצע ללא כל צורך בהסמכה נוספת,[141] כל עוד המשטרה מצליחה להתגבר על ההגנות הללו בעצמה. כאשר הרשות לא תוכל בעצמה להתגבר על ההצפנה או הגנת הסיסמה, תישאל השאלה מה סמכותה של הרשות החוקרת לדרוש מאדם את מפתח ההצפנה או את הסיסמה, או לחלופין לדרוש מהאדם לספק את המידע השייך לו כשהוא משוחרר מהצפנה או סיסמה. המחוקק הישראלי שותק ביחס לסוגיות אלה. אם להקיש מן הדינים הקיימים אל סוגיה זו, אציין כי ככל שיתבקש הנחקר למסור, במסגרת עדות, את מפתח ההצפנה או הסיסמה, ייתכן שתקום לזכותו באופן ישיר הזכות לאי הפללה עצמית, אשר חלה על אמרות מפלילות.[142] במידה שיתבקש הנחקר למסור את חומרי המחשב שלו כשהגנת

---

[140] אציין שתי התייחסויות משפטיות בישראל לנושא הצפנות: *האחד*, במסגרת פרשת הסוס הטרויאני עלה כי הנאשמים השתמשו בהצפנות לצורך התקשורת ביניהם ולצורך תפעול הסוסים הטרויאניים שהושתלו במחשבים הנחדרים. בית-המשפט העליון ראה בעצם השימוש בהצפנות על-ידי הנאשמים משום גורם המעיד על מסוכנות ועל חשש לסיכול הליכי החקירה והשפיטה בתיק, ולאו דווקא כביטוי לשימוש באמצעים לגיטימיים להגברת פרטיות, במובן של סודיות התקשורת בין אנשים. ראו בש"פ 7368/05 **זלוטובסקי נ' מדינת ישראל**, תק-על 2854 ,(3)05, 2859 (2005). השוו עם: Levie v. State of Minnesota, 695 N.W. 2d 619 (Minn. App. 2005), שם נקבע כי שימוש של נאשם בהצפנות במחשבו יכול להוות ראיה נסיבתית לחובתו, במישור של היסוד הנפשי לביצוע העבירות.

השני, תפישת משרד הביטחון הישראלי היא שהשימוש בהצפנה יכול להיות כפול-פנים, ועלול לשמש בידי מדינות אויב, גורמי טרור וכדומה לצרכים צבאיים ולמניעת חשיפה על-ידי כוחות הביטחון הישראליים, ומכאן שכל הצפנה, לרבות הצפנות מסחריות, מחויבת ככלל ברישום ובפיקוח על-ידי משרד הביטחון. ראו צו הפיקוח על מצרים ושירותים (עיסוק באמצעי הצפנה), התשל"ה – 1974 (להלן - "צו הצופן"); אכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), התשל"ה – 1974. צו הצופן והאכרזה הנ"ל תוקנו ב-1998, ורוככו מעט: הפיקוח הועבר מקצין קשר ראשי של צה"ל למשרד הביטחון והוקלו אמצעי הפיקוח על הצפנות מסחריות. כן ראו לעניין זה את דברי ההסבר באתר האינטרנט של משרד הביטחון: http://www.mod.gov.il/pages/encryption/hakdama.asp. בארצות-הברית, לעומת זאת, אין חיוב ברישום של הצפנות בשימוש בתוך ארצות-הברית, אלא ברישום של הצפנות המיוצאות לחו"ל בלבד. ראו באתר משרד התעשייה והמסחר האמריקני: http://www.bis.doc.gov/encryption/default.htm. עם זאת, מנכ"ל משרד הביטחון רשאי להכריז על סוגי הצפנה שאינם מצריכים רישום ופיקוח כאמור. הללו מכונים "אמצעים חופשיים". על פי פרסומי משרד הביטחון הוכרזו להיום 7051 הצפנות (רובן מסחריות) כ"אמצעים חופשיים". ראו: http://www.mod.gov.il/pages/encryption/docs/Free-means.xls. עיון ברשימה מעלה כי "אמצעים חופשיים" רבים קשורים לתעשיית הסלולר, המחשבים והאינטרנט. עו"ד חיים רביה תקף את החובה לרשום כל הצפנה שלא הוכרזה כפטורה, ולקבל בעבורה רישיון מטעם המדינה. רביה טען כי אין המדובר בדרישה המתאימה לעידן האינטרנט, בה חלק ניכר מהתקשורת מוצפנת באופן אוטומטי, וכל גולשי האינטרנט משתמשים למעשה בהצפנות מעין אלה והופכים לעבריינים בפוטנציה. האכרזה הפוטרת מקבלת רישיון לשימוש באמצעי הצפנה לעולם תפגר אחר שלל ההתפתחויות הטכנולוגיות, ועל כן היא לעולם תביא למצב שבו משתמשים רבים בטכנולוגיות חדשות ייחשבו כמי שלא מקיימים את הוראות משרד הביטחון בעניין. ראו חיים רביה "אי סבירותו של צו הצופן" חלק ראשון-שלישי (25.1.2000, 2.2.2000, 9.2.2000), פורסם באתר: www.law.co.il בקטגורית "מאמרים".

משני המקורות האמורים ניתן להסיק יחס חשדני של המשפט הישראלי להצפנות.

[141] מעניין לציין כי במקרה זה, אי התייחסות המחוקק מלמדת על סמכות גורפת לפיצוח הצפנות ועקיפת סיסמאות, שכן כל שלב העיון במידע נבלע בסמכות החדירה. זאת למרות שהכלל הוא שהיעדר הסמכה מפורשת לרשות החוקרת – משמעה היעדר סמכות, בשל עיקרון חוקיות המנהל, המחייב הסמכה חוקית לכל פעולה פוגענית של הרשות.

[142] הזכות לאי הפללה עצמית מעוגנת בכמה דברי חקיקה: סעיף 47 ביחד עם סעיף 52 לפקודת הראיות; סעיף 2(2) לפקודת הפרוצדורה הפלילית (עדות), 1927; סעיף 28(א) לחוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו – 1996. לעיגונה בפסיקה ראו עניין *שרון*, לעיל ה"ש 41, והפסיקה המצוטטת שם.

ההצפנה או הסיסמה מוסרת מעליהם, וזאת מבלי שימסור לחוקרים את מפתח ההצפנה או את הסיסמה עצמה, כאן לכאורה אין המדובר באמרה אלא בהמצאה, מכוח סעיף 43 לפסד״פ. בכל הנוגע לסמכות לדרוש מסירת מסמכים או חומרי מחשב, קבע בית-המשפט העליון בעניין **שרון** כי חלה הזכות לאי הפללה עצמית, אולם לא חלה זכות השתיקה במובן של זכות שלא להיעתר ככלל לצו.[143] הנפקות המעשית של קיומה של זכות לאי הפללה עצמית בלבד היא שניתן לחייב נחקר למסור את המידע לאחר הסרת הסיסמה או קוד ההצפנה, אף חרף בקשת הנחקר מבית-משפט להימנע מכך, אלא שאם יש במידע שיימסר ערך מפליל כלפי הנחקר, לא יוכל המידע לשמש נגדו בהליך משפטי, אלא כלפי אחרים בלבד.[144]

בבריטניה נקבעה סמכות להורות לאדם על מסירת מפתח הצפנה או סיסמת הגנה, בפרק השלישי של ה-Regulation of Investigatory Powers Act (RIPA) משנת 2000, אשר נכנס לתוקף בפועל החל משנת 2007.[145] סירוב לציית לצו המורה למסור מפתח הצפנה מהווה עבירה פלילית עצמאית, שעונשה בין שנתיים לחמש שנות מאסר (תלוי בסוג העבירה המקורית שבגינה נדרש הנחקר למסור את מפתח ההצפנה כאמור).[146] באוסטרליה קובע ה-Cybercrime Act שנחקק בשנת 2001, כי שופט יכול להורות בצו לאדם לסייע בכל דרך לרשויות לגשת למידע ממוחשב ולהמירו למסמך קריא.[147] הצו יכול שיופנה לכל אדם שיש לו גישה למידע הממוחשב או שיש לו מידע על אמצעי ההגנה על המידע. במלים אחרות, גם מי שאינו בעל הרשאה חוקית לגשת למידע הממוחשב בו מדובר, אולם באפשרותו הטכנית להתגבר על הצפנת המידע (כיוון שמכיר את תוכנת ההצפנה או את הסיסמה לפתיחתה), עשוי להיות נשוא לצו בית-משפט שכזה. העונש על אי קיום הוראות של צו מעין זה – 6 חודשי מאסר. בניו זילנד קובע ה-Search and Surveillance Act משנת 2012, שלאדם המבצע צו חיפוש המתייחס לחומר מחשב קמה הסמכות לדרוש "Access information", ויש בדרישה זו כדי לגבור גם על טענות בדבר הפללה עצמית בנסיבות הנקובות בחוק (דרישת הכרחיות וסבירות הדרישה מצד מבצע החיפוש).[148]

---

[143] עניין *שרון*, שם.

[144] זאת כעולה מסעיף 47 לפקודת הראיות, וכן מעניין *שרון*, שם, בעמ' 762-768.

[145] ראו: Regulation of Investigatory Powers Act, 2001, c. 3, § 49-56 (Eng.). ליישום הסמכות האמורה ראו: R. v. S.&A., [2008] EWCA Crim. 2177 (Eng.).

[146] ראו את עניינו של אוליבר דרייג (Drage) שסירב למסור מפתח הצפנה למחשבו ונשפט בגין עבירה על סעיף 53 ל-RIPA: Kevin Townsend, *Youth Imprisoned for not Disclosing His Computer Password: is RIPA a Suitable Law for a Civilised Country?* (6.10.2010) https://kevtownsend.wordpress.com/2010/10/06/youth-imprisoned-for-not-disclosing-his-computer-password-is-ripa-a-suitable-law-for-a-civilised-country/.

[147] ראו: Cybercrime Act, 2001, Schedule 2 § 12 (Au.).

[148] ראו: Search and Surveillance Act, 2012 § 130 (NZ.).

EDNAKARNAVAL LIBRARY FOR THE MASSES

בארצות-הברית הדבר אינו נקוב בחוק והפסיקה התחבטה בשאלה האם ניתן להורות לאדם למסור מפתח הצפנה אם לאו, או שמא הדבר פוגע בזכות לאי הפללה עצמית. בעניין **Boucher** בית-המשפט בערכאה הראשונה קבע כי הגנת התיקון החמישי לחוקה האמריקנית (הזכות לאי הפללה עצמית) מאפשרת לאדם להימנע ממסירת מפתח ההצפנה.[149] המדינה השיגה על ההחלטה, אלא שבמסגרת ההשגה שינתה את דרישתה: היא לא ביקשה עוד לקבל את מפתח ההצפנה מאת החשוד, אלא ביקשה ממנו להפיק עותק של הדיסק הקשיח שלו לאחר הסרת ההצפנות ממנו. ניואנס זה הביא את בית-המשפט לקבל את עמדת המדינה, ולקבוע כי במצב דברים זה אין המדובר בדרישה מאדם להעיד על דבר העלול להפלילו.[150] עם זאת, בהחלטה מאוחרת יותר של בית-משפט פדרלי לערעורים (עניין **Doe**), נדחתה בקשה של המדינה לקבל העתקים מפוענחים של מחשב נייד וחמישה דיסקים קשיחים חיצוניים של החשוד.[151] ניתן ליישב בין שתי ההחלטות, בעניין *Boucher* ובעניין *Doe*, בהסבר כי בנסיבות המקרה של *Doe*, עצם המענה לדרישת המשטרה משמעה הודאה בכך שהחשוד הוא המשתמש הקבוע במחשב, ובנסיבות בהן לעובדה זו יש משקל ראייתי משמעותי כנגד החשוד, הרי עצם פתיחת ההצפנות על-ידו מפלילה אותו מהווה מעין אמרה כשלעצמה. על כל פנים, ראוי לציין כי עצם הסמכות להורות לנחקר לפתוח את ההצפנות והסיסמאות, בלא שקיימת סמכות לקבל את מפתח ההצפנה או את הסיסמה עצמם – היא בבחינת סמכות עקרה במידה רבה. הלא ככל שאין ברשות החוקרים יכולת להגיע בעצמם אל המידע, הם תלויים בחסדיו של הנחקר, שרשאי להחליט להסתיר חלק מהקבצים מהרשות החוקרת. אין לחוקרים דרך לדעת האם הוסתר מהם מידע מסוים. מכאן שאלמנט הבקרה והסנקציה על הפרה – לא קיימים ביחס לסמכות זו, ולכן מהותה כסמכות מחייבת נפגמת.

דיון מסוג אחר, אשר התנהל בארצות-הברית, עניינו בשאלה האם יש להרחיב את הסמכות לכך שספקיות שירות שונות במרחב הסייבר תחויבנה לבנות "דלת אחורית" (Backdoor) עבור רשויות החקירה, באופן שיתאפשר לפצח את כל ההצפנות בהן נעשה שימוש על-ידי הגולשים לשירות.[152]

---

[149] ראו: In re Boucher, 2007 WL 4246473 (D. Vt . 2007). להחלטות ברוח דומה, ראו: United States v. Rogozin, 2010 WL 4628520 (W.D.N.Y. 2010); United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010).

[150] ראו: In re Boucher, 2009 WL 424718 (D. Vt. 2009). לשימוש נוסף בטקטיקה זו, שאושר על-ידי בית-המשפט, ראו: United States v. Fricosu, 841 F. Supp.2d 1232 (D. Colo. 2012).

[151] ראו: In re Grand Jury Subpoena Duces Tecum, 671 F.3d 1335 (11th Cir. 2012).

[152] לכתיבה מוקדמת על סמכות ליצירת "דלת אחורית" עבור רשויות החקירה, ראו: James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CINC. L. R. 177 (1997); להרחבה נוספת ראו: Kozlovski, לעיל ה"ש 55, בעמ' 218-219; Birnhack & Elkin-Koren, לעיל ה"ש 116, בעמ' 42-43. ודוקו, יצירת "דלת אחורית" אינה זהה להוראות מכוח צו הצופן, כמפורט לעיל בה"ש 140, והיא מגלמת פגיעה רחבה יותר: *ראשית*, היא חלה גם על "אמצעים חופשיים" מרישום במשרד הביטחון. *שנית*, היא חלה על מצבים שבהם הצפנה מסוימת לא נרשמה בהתאם להוראות צו הצופן (בין בזדון ובין מחוסר ידיעה או בתום לב) ובכל זאת נעשה בה שימוש. בהקשר של

רשויות החקירה הסבירו שאם לא יתאפשר להן להשתמש ב"דלת אחורית", ולא יצליחו לגלות את סיסמת הפתיחה של ההצפנה בדרך אחרת (למשל מפיו של עד, מפיו של החשוד עצמו או במסמך כלשהו שייתפס בחיפוש), הן עלולות לעמוד בפני שוקת שבורה, בהנחה שהזכות לאי הפללה עצמית תמנע מהן מלחייב את הנחקר למסור את מפתח ההצפנה / הסיסמה. מבחינה סיווגית, הדיון בסוגיית ה"דלת האחורית" לרשויות החקירה מתקשר לדיון נרחב יותר, בדבר הסמכות לחייב ספקיות שירות במרחב הסייבר ליצור תשתית טכנולוגית אשר תוכל לשרת, במקרה קונקרטי, את רשויות החקירה.[153] דיון זה מעורר את שאלת הפגיעה בזכות לפרטיות במובנה כחירות אישית של כל משתמש מחשב מפני תחושת מעקב כללית של הרשויות אחריו.

לסיכום נקודה זו, אחד ממאפייניו של המידע הדיגיטלי במרחב הסייבר הוא כי ניתן להצפינו או להגן עליו בסיסמה בנקל. בדין הישראלי המסדיר את סמכויות האיסוף אין כל התייחסות להצפנה של מידע דיגיטלי או להגנתו בסיסמה, והטעם לכך הוא שהתפישה הפיזית, החולשת על דיני איסוף הראיות, מזניחה את כל שלב העיון במידע ומבכרת במקומו את שלב התפיסה של המידע. כיוון שההתמודדות עם הצפנות והגנת סיסמאות נעשית בשלב העיון במידע, הרי שהחוק נעדר התייחסות לכך באופן שמביא להחמצת הדיון הנכון בצרכי החקירה למול הזכות לאי הפללה עצמית והזכות לפרטיות במובנה כחירות מפני תחושת מעקב.

ח) סיכום

מניתי סדרה של פעולות איסוף החסרות כתוצאה מהתפישה הפיזית החולשת על איסוף ראיות דיגיטליות במרחב הסייבר. הצורך החקירתי בפעולות איסוף אלה נובע ממאפייני הראיות הדיגיטליות במרחב הסייבר המייחדים אותן לעומת ראיות במרחב הפיזי. טבלה מס' 4.4 מסכמת את החלק הזה, ומציגה את הצרכים החקירתיים החסרים בחקירה הפלילית במרחב הסייבר, כתוצאה מהתפישה הפיזית, ואת המאפיינים הייחודיים של הראיות הדיגיטליות במרחב הסייבר המנביטים אותם. יודגש, שוב, כי בשלב זה של הדיון הצגת פעולות האיסוף נעשתה בהתייחס לצרכי החקירה במרחב הסייבר, תוך התעלמות מתודית מהדיון החוקתי המאזן:

הפעלת סמכויות ביטחון, פורסם לאחרונה, כחלק מפרשת אדוארד סנאודן, עובד ה-NSA אשר הדליף מידע רגיש אליהם נחשף במסגרת עבודתו, כי ספקיות שירות גדולות, כגון מיקרוסופט, יצרו תשתית טכנולוגית עבור ה-NSA, אשר תאפשר לה לנטר תעבורת רשת כשהיא בלתי-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

[153] ראו לעיל בפרק 4(ג)(3)(ד).

<u>טבלה מס' 4.4 – מיון פעולות איסוף הראיות החסרות כתוצאה מהתפישה הפיזית</u>

פעולות האיסוף	המאפיינים הייחודיים של הראיה הדיגיטלית במרחב הסייבר
המצאה עתידית של חומר מחשב	1. המידע מנותק פיזית מהמשתמש בו ומוחזק על-ידי מתווכים 2. המידע מצטבר וניתן לאגירה
הוראות שמירה מכאן ולהבא (Preservation) הוראות שימור דרך קבע (Retention)	1. המידע מנותק פיזית מהמשתמש בו ומוחזק על-ידי מתווכים 2. המידע מצטבר וניתן לאגירה 3. המידע נדיף (הוראות השמירה / שימור דרך קבע ימנעו את נדיפות המידע) 4. המידע פגיע (הוראות השמירה / שימור דרך קבע ימנעו פגיעה במידע) 5. לגבי שימור דרך קבע בלבד – המידע ניתן לאחזור ומיון באמצעים ממוחשבים (לכן קיים ערך חקירתי רב במיצוי ראיות מתוך "בריכת" המידע הענקית הנוצרת משימור דרך קבע, ללא חשד ספציפי)
יצירת תשתית המאפשרת לרשות לאסוף ראיות דיגיטליות	1. המידע מנותק פיזית מהמשתמש בו ומוחזק על-ידי מתווכים (לכן יש לרשות החוקרת עניין בהטלת חובה על ספקי השירות לייצר את התשתית האמורה) 2. המידע נדיף 3. המידע פגיע
חדירה סמויה לחומר מחשב מרחוק והעתקת המידע ממנו	1. המידע מיוצג בביטים - תוכן המידע נפרד מן החפץ הפיזי עליו הוא מוטבע 2. המידע ניתן להעתקה מלאה 3. המידע נדיף (לכן יש לבחון העתקה שלו בשלב סמוי לטובת החקירה) 4. המידע פגיע (לכן יש לבחון העתקה שלו בשלב סמוי לטובת החקירה)
תיעוד סמוי של הפעילות במחשב הקצה	1. המידע נדיף ופגיע (במובן של עדכונים אוטומטיים המשפיעים עליו והמצדיקים תיעוד הפעילות במחשב הקצה ולא ניטור התעבורה מהמחשב ואליו) 2. המידע מיוצג בביטים - תוכן המידע נפרד מן החפץ הפיזי עליו הוא מוטבע 3. המידע ניתן להצפנה, הסוואה או טשטוש
התגברות על הצפנות והגנת סיסמאות	1. המידע ניתן להצפנה, הסוואה או טשטוש

<u>ד. התפישה הפיזית והצעת חוק החיפוש</u>

בפרק זה הצבעתי על התפישה הפיזית החולשת כיום על דיני איסוף הראיות במרחב הסייבר ומניתי פעולות איסוף ראיות דיגיטליות, אשר לכאורה ניתן להציע במסגרת גישה המשוחררת מכבלי ה"פיזיות". הצעת חוק החיפוש מבקשת לצעוד שלב אחד קדימה בכיוון של השתחררות מהתפישה הפיזית ביחס לסמכויות איסוף הראיות בחקירה פלילית. אמנה את ההוראות בהצעת החוק המגלמות "תפישה דיגיטלית" ביחס לקביעת סמכויות איסוף הראיות. איני מונה את כלל ההוראות שבהצעת החוק ביחס לראיות דיגיטליות, אלא כאמור את אלה המבטאות **השתחררות מכבלי התפישה הפיזית**.

1) הכרה בסמכות להורות **בצו בית-משפט** על **שמירת ראיות דיגיטליות מכאן ולהבא** (Preservation). סעיף 74(א) להצעת חוק החיפוש מציין כי בית-המשפט רשאי להורות ל"בעל גישה" לחומר מחשב, הקשור לעבירה אשר קיים חשד סביר שנעברה או שעומדת להיעבר, לשמור את חומר המחשב בדרך ובתנאים שיקבע. הוראת השמירה נועדה להתגבר על תכונת הנדיפות של הראיות הדיגיטליות במרחב הסייבר, ומכאן ההוראה המפורשת כי במסגרת צו השמירה רשאי בית-המשפט - *"...לאסור על מחיקת החומר, כולו או חלקו, או על הכנסת שינוי בו"*.

2) הצעת החוק כוללת סמכות ל**צו שמירה עתידי ולצו המצאה עתידי**. על פי סעיף 74(ב) להצעת החוק, תהיה לבית-המשפט הסמכות להורות על שמירה עתידית ל-90 יום, ממועד מתן צו השמירה, של חומר מחשב הקשור לעבירה. כמובן שלאחר השמירה העתידית כאמור יוכל בית-המשפט להורות על המצאה של המידע שנאגר בדרך זו. על פי סעיף 73(ב) להצעת החוק, יכול בית-המשפט להורות על המצאה עתידית של חומר מחשב, הקשור לעבירה, שיגיע לידי הנמען לצו, זאת תוך 30 יום מיום הוצאת הצו.[154] סמכויות אלה מסדירות באופן מפורש סמכויות שניתן לקרוא לכאורה לתוך החוק הקיים.[155] על כל פנים, סמכויות אלה מתאימות לתכונתה של הראיה הדיגיטלית כראיה הניתנת לאגירה.

3) הצעת החוק כוללת סמכות ל**חדירה סמויה לחומר מחשב** (סעיף 91 להצעת החוק). סמכות החדירה הסמויה מושווית לסמכות האזנת סתר, ומוחלות עליה הוראות פרקים ג' וד' לחוק האזנת סתר. ההגדרה של "חדירה לחומר מחשב", בין סמויה ובין גלויה, היא רחבה ביותר.[156] כיוון שסמכות החדירה הסמויה אינה משנה את מהות ה"חדירה", אלא רק מוסיפה את אלמנט הסתר,[157] הרי שניתן על פי הצעת החוק לקרוא לתוכה את הסמכות לבצע **העתקה סמויה** ואף **ניטור סמוי של הפעילות במחשב הקצה** (על דרך של "הקלטה", מתוך המחשב הנחדר, של מסך המחשב של יעד הניטור). זאת למרות שמנוסח הצעת החוק ודברי ההסבר לה, קשה להסיק כוונה להכליל במפורש סמכות זו. סמכות החדירה הסמויה לחומר המחשב, לרבות העתקה

---

[154] הוראת ההמצאה העתידית מוגבלת למצבים בהם "קיים חשד סביר שעומדת להיעבר עבירה העלולה לסכן את שלומו או ביטחונו של אדם, את שלום הציבור או את ביטחון המדינה", או, לחלופין, "כי קיימת הסתברות גבוהה שתיעבר עבירה". ראו סעיף 73(א) ביחד עם סעיף 5(א) להצעת חוק החיפוש. לעומת זאת, ביחס להוראת השמירה העתידית הדרישה היא ל"חשד סביר... שעומדת להיעבר עבירה". ראו סעיף 74(א) ביחד עם סעיף 9(א) להצעת החוק.

[155] על פרקטיקת השימוש של המדינה בדין הקיים לצורך "צווים עתידיים", ולא רק באשר למידע הקיים במועד הוצאת הצו או ביצועו בלבד – ניתן ללמוד, למשל, מהעובדות המפורטות בהחלטות בעניין *נטוויזין*, לעיל ה"ש 64, ובעניין *פילוסוף I*, לעיל ה"ש 68.

[156] ראו לעיל בה"ש 97.

[157] ראו הגדרת "חדירה לחומר מחשב" בסעיף 72 להצעת חוק החיפוש והשוו עם סעיף 4 לחוק המחשבים.

EDNAKARNAVAL LIBRARY FOR THE MASSES

סמויה ותיעוד סמוי של הפעילות במחשב הנחדר, מוגבלים בזמן, על פי משך הזמן שבו יעמוד הצו בתוקף (30 יום מעת מתן הצו או פרק זמן אחר, כפי שיקבע בית-המשפט).[158]

4) הצעת חוק החיפוש מבקשת להכריע בסוגיית ה**צווים לקבלת תקשורת א-סינכרונית**. נושא ההתמודדות עם תקשורת א-סינכרונית זוכה להתייחסות מעט מסורבלת בהצעת החוק, אך נדמה כי הסרבול מתחייב גם ממורכבות הסוגייה. *ראשית לכל*, קובעת הצעת החוק, בסעיף 77(ב)(1), כי צו להמצאה או לשמירה של תוכן ממוחשב יינתן אם קיים חשד סביר שנעברה עבירה מסוג פשע או כל עבירה, שאינה פשע, על חוק המחשבים, אם קיימת הסתברות גבוהה שתיעבר עבירה כאמור, או אם קיים חשד סביר שעומדת להיעבר עבירה כאמור העלולה לסכן את ביטחונו של אדם, את שלום הציבור או את ביטחון המדינה.

שנית, הצעת החוק קובעת, בסעיף 77(ג), כי אם ספק השירות מעניק רק שירותי "תקשורת בין מחשבים בלבד", ולא "שירות של אחסון מידע", הרי שקליטת התוכן בידי ספק השירות, על פי הוראה של צו שיפוטי - יראו אותה כהאזנת סתר. מן הלאו ניתן לשמוע את ההן: ככל שפונה הרשות החוקרת אל ספק שירות המספק שירותי אחסון המידע לצד שירותי העברה של המידע, לא יחולו הוראות חוק האזנת סתר. במקרה של תקשורת א-סינכרונית, כדוגמת דוא"ל, הרי שספק השירות, לצד העברת המידע מהשולח אל המקבל ולהיפך, גם מספק שירותי אחסון של המידע עד לקריאתו ואף לאחר קריאתו. מכאן נובע, שחוק האזנת סתר אינו חל על הסיטואציה.

שלישית, הצעת החוק מבקשת, בסעיף 110(1), לתקן באופן עקיף את חוק האזנת סתר כך שדרישת הבו-זמניות[159] תוכנס לגדר הגדרת "האזנה" בסעיף 1 לחוק. במלים אחרות, "האזנה" ל"שיחה" תוכל להתבצע רק אם היא מתבצעת תוך כדי התרחשותה של השיחה המואזנת. מכאן שפנייה אל ספק השירות לצורך איסוף תקשורת א-סינכרונית, בעת שהיא "חונה" אצלו, אינה יכולה להיחשב כהאזנת סתר, כיוון שאינה מתבצעת בו-זמנית עם התרחשות השיחה.[160]

---

[158] ראו סעיף 103(א) להצעת חוק החיפוש.

[159] עמדתי על סוגיית הבו-זמניות בהקשר של האזנת סתר, לעיל טקסט לה"ש 52.

[160] בנוסף, קיימות מספר הוראות ייחודיות לגבי פניות אל ספק שירות, בכלל זה לצורך קבלת תקשורת א-סינכרונית. כך, קובעת הצעת החוק, כי במתן צו לספק שירות על בית המשפט לשקול את השאלה האם מדובר בספק שירות (סעיף 65). כן נשקלת אפשרות יידוע החשוד על צו המצאה או חדירה לספק שירות (סעיפים 71 ו-78). בנוסף, בקשה לצו חדירה לספק שירות תוגש באישור האחראי על החקירה בלבד (סעיף 84(א)). על פי דברי ההסבר המפורטים להצעת חוק החיפוש: *"בהוראות האמורות נלקח בחשבון הייחוד של מחשב ספק השירות בעיקר לנוכח כמות המידע הנצבר אצלו עבור כלל לקוחותיו, מה שמדגיש את היקף פוטנציאל הפגיעה בפרטיות כתוצאה מקבלת המידע האגור, ומכאן הזהירות היתירה בקבלת מידע כזה"*.

5) סעיף 95 להצעת חוק החיפוש מקנה סמכות לחייב **מסירה של מפתח הצפנה או סיסמה**. זאת על פי בקשה שתוגש לבית-המשפט על-ידי האחראי על החקירה, במקרה של עבירה מסוג פשע או עבירה אחרת על פי חוק המחשבים, וככל שהצורך החקירתי גובר על הפגיעה בבעל הגישה לחומר המחשב, הכרוכה בחיובו למסור את מפתח ההצפנה או הסיסמה. הבקשה תוגש כאשר אין דרך סבירה אחרת להשגת המידע המבוקש. סירוב לציית לצו ייחשב להפרת הוראה חוקית, לפי סעיף 287 לחוק העונשין, וכן ישמש כחיזוק לראיות התביעה, לפי סעיף 95(ג) להצעת החוק. על פי התפישה של הצעת חוק החיפוש, בכוחו של צו למסירת מפתח הצפנה או סיסמה יש כדי להתגבר על טענה לחיסיון מפני הפללה עצמית, שכן הסמכות לקבלת המידע כבר הייתה נתונה בידי הרשות החוקרת, ואין לראות בהגנת הסיסמה או ההצפנה משום אלמנט המקים את החיסיון על המידע כשלעצמו. הצעת החוק מכירה באפשרות שתיטען טענת חיסיון מפני הפללה עצמית, אם בעצם מסירת מפתח ההצפנה או הסיסמה יש בה, כשלעצמה, כדי להפליל (למשל, אם זירת המחלוקת היא לגבי הזיקה של החשוד למחשב המוגן בסיסמה, ומסירת הסיסמה תסגיר כי החשוד הוא המחזיק במחשב).[161]

* * *

בסיכומו של דבר, הצעת חוק החיפוש בהחלט מקדמת משמעותית את ההתייחסות הייחודית אל הראיות הדיגיטליות כמובחנות מהראיות הפיזיות. בכך היא תורמת לניפוץ התפישה הפיזית ביחס לאיסוף ראיות דיגיטליות. יש לשים לב, כי פעולות איסוף שונות, עליהן עמדתי לעיל, נותרו מחוץ להצעת החוק: אין התייחסות לשימור דרך קבע ואין הוראות בעניין יצירת תשתית לאיסוף ראיות דיגיטליות; כמו כן, הסמכות לבצע העתקה סמויה או ניטור סמוי של הפעילות במחשב הקצה – אינן מנויות במפורש אלא נקראות מתוך סמכות החדירה הסמויה לחומר המחשב.

ה. סיכום

בפרק זה הראיתי כי דיני איסוף הראיות בחקירה פלילית במרחב הסייבר לוקים בתפישת יסוד שגויה, המניחה כי דין הראיות הדיגיטליות במרחב הסייבר כדין חפצים פיזיים. תפישה זו היא תפישה "פיזית" של איסוף הראיות הדיגיטליות. התפישה הפיזית מזניחה תכונות ייחודיות של הראיות הדיגיטליות במרחב הסייבר, המייחדות אותן מראיות במרחב הפיזי. בשל כך נוצרת החמצה דו-כיוונית

---

[161] ראו דברי ההסבר לסעיף 95 להצעת חוק החיפוש.

המשליכה על דיני איסוף הראיות בחקירה פלילית: מחד גיסא, חסרות סמכויות איסוף של המדינה המתאימות לראיות הדיגיטליות במרחב הסייבר; מאידך גיסא, השיח החוקתי המתאים ביחס להפעלת סמכותה של המדינה בחקירה פלילית במרחב הסייבר – חסר אף הוא. בפרק זה עמדתי על החסר בסמכויות האיסוף כתוצאה מן התפישה הפיזית, ואילו בפרק הבא אעמוד על החסר בדיון החוקתי המאזן.

התפישה הפיזית, עליה עמדתי בפרק זה, מצטרפת אל התפישה הטריטוריאלית, לה הוקדש הפרק הקודם בספר. שילובן של שתי התפישות האמורות מגביר את המסקנה כי על מנת שהמדינה תוכל לשמר את סמכותה כאוכפת חוק אפקטיבית במרחב הסייבר, ועל מנת שהגנה חוקתית ראויה תיפרש על משתמשי המרחב הקיברנטי בהקשר של אכיפת החוק הפלילית ברשת, יש מקום לפתח מודל חלופי לחקירה פלילית במרחב הקיברנטי. מודל זה יידון בפרק 6 להלן.