פרק ד

התפישה הפיזית באשר 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. 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, ומצד 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 מהחקירה הפלילית במרחב הסייבר – מובאים בחשבון. בפרק זה אציג את האופן שבו התפישה הפיזית מגולמת במשפט הישראלי, כמו גם בשיטות משפט אחרות, בעיקר במשפט האמריקני. לאחר מכן אראה כי התפישה הפיזית שגויה משום שהיא חוטאת לאופייה של הראיה הדיגיטלית, השונה בכמה מובנים מזה של הראיה הפיזית, ולפיכך היא מובילה לחסר בכל הנוגע לצרכיה של הרשות החוקרת במרחב הסייבר. בהמשך, פרק ה יוקדש לדיון החוקתי הנחסר כתוצאה מהתפישה הפיזית, כמו גם כתוצאה מהתפישה הטריטוריאלית, שעליה עמדתי בפרק הקודם.

מטרת הפרק הנוכחי, כקודמו, היא לחשוף תפישות יסודיות סמויות החולשות על החקירה הפלילית במרחב הסייבר. ההצגה של התפישות – הטריטוריאלית והפיזית – היא של כל אחת מהן בנפרד, ומכאן נובע לכאורה שאין זיקה בין שתי התפישות. אולם למעשה, יכולה להישמע טענה ששתי תפישות אלה נגזרות מתפישה מעין־מוניסטית 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 לוטס, 1996).

nevo.co.il

ב. אבחון התפישה הפיזית

אציג את פרישתה של התפישה הפיזית, תחילה בנוגע לדיני המחשבים בכלליות, ולאחר מכן בנוגע לאיסוף ראיות דיגיטליות במפורט. 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 באשר לדיני איסוף הראיות הדיגיטליות תיערך במפורט בנוגע 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 באשר 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" באשר למרחב המקוון, כאשר בשלב זה של הדיון ההתמקדות אינה באיסוף ראיות דיגיטליות אלא בדיני המחשבים באופן כללי.

תפישת 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 "מחזיקו".[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 בנבו, 15.9.2003). אולם השוו, מנגד, ל־Intel Corp. v. Hamidi, 71 P.3d 296 (Cal., 2003), שם נדחתה האנלוגיה להשגת גבול במיטלטלין בנוגע לעובד לשעבר באינטל ששלח מיילים לעובדים בחברה שבהם 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 (1965).

דוגמה שנייה 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" באשר למידע. מושג ה"מחזיק" במידע רלוונטי בהקשרים משפטיים שונים. לדוגמה, המחזיק במאגר מידע חייב ברישום המאגר.[8] הוא יכול להיות מורשע בעברה של החזקת חומר תועבה ובו דמותו של קטין[9] או בעברה 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 שבהם נקשרו כמה אנשים לאותו חפץ.[11] בכל הנוגע להחזקת מידע ממוחשב, בעיקר באינטרנט, פותח מבחן המכיר בהפרדה פיזית חוצת־מדינות בין המידע לבין מחזיקו, בתנאי שקיימת נגישות למידע ושליטה ממשית בו.[12] עם זאת חשוב לציין כי מונח ההחזקה ממשיך להציב קשיים משפטיים הנובעים מאופיו של המידע במרחב המקוון. כך למשל שאלה פתוחה היא אם צפייה בתכנים באינטרנט (Viewing או שימוש ב־Video-Streaming), להבדיל מהורדה שלהם (Download), מהווה "החזקה". מבחינה טכנית־פורמלית, טכנולוגיית הצפייה כוללת הורדה של המידע אל מחשב הקצה וטעינתו מתוכו, אך המידע אינו נשמר במסודר כקובץ במחשב הקצה עם גמר הצפייה, אלא הוא נותר אגור בזיכרון המטמון (ה־Cache memory), עד שיידרס על ידי

---

5 ראו ע"פ (מחוזי ת"א) 71227/01 **מדינת ישראל נ' טננבאום**, פ"מ תשס"א(2) 595, 603–605 (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).

nevo.co.il

מידע אחר.[13] לשאלת הצפייה כהחזקה נפקות ממשית הולכת וגוברת בשל המעבר מפרקטיקה של "הורדה" לפרקטיקה של "צפייה".[14] אמחיש להלן את הסוגיה ביחס לעברה 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 בעברה של החזקת (Possession) חומרי תועבה פדופיליים על פי הקונסטרוקציה שצפייה כוללת החזקה זמנית בזיכרון המטמון, ומכאן שפורמלית נחשבת הצפייה להחזקה. אם הנאשם מודע לקיומה של החזקה זמנית זו, הרי שיש מקום להרשיעו בעברה.[15] המהלך הפרשני המאפשר לראות ב"צפייה" "החזקה" נסמך כאמור על הוכחת מודעותו של הנאשם לנקודה טכנולוגית ולא למהות ההגנה על קטינים המופיעים במיצג המתועב וקטינים אחרים העתידים להיפגע מצרכני אותם תכנים פדופיליים. ייתכן שמונח ניטרלי 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 באופן שסעיף 214(ב3) לחוק יכלול גם איסור על צריכת התכנים הפדופיליים מלבד האיסור הקיים על החזקת התכנים.[16]

---

13 ראו Brian D. Davison, *A Web Caching Primer*, 5 IEEE INTERNET COMPUTING 38, 39 (Jul.–Aug. 2001). המעבר מהורדת התכנים לצריכתם און־ליין משמעותו, מבחינת משתמש הקצה, שצפייה חוזרת במידע תחייבו להתקשר שוב אל האתר שבו 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, ולמשתמשי האינטרנט הפכה צריכה על דרך של צפייה און־ליין לחלופה זולה ונוחה יחסית; **השנייה**, 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, ויהיה ניתן 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 שצפה בהם.

15 ראו Commonwealth of Pennsylvania v. Diodoro, 970 A. 2d 1100 (Pa. Super., 2009). לפסיקה דומה ראו גם United States v. Romm, 455 F. 3d 990 (9th Cir., 2006); United States v. Tucker, 305 F. 3d 1193 (10th Cir., 2002). בפסיקה הישראלית קיימת התייחסות בודדת של בית משפט השלום בתל אביב לנושא בעניין **פלוני**. באותו מקרה הודה הנאשם במסגרת הסדר טיעון בעברה של החזקת חומרי תועבה, ובהם דמויות של קטינים. בית המשפט העיר בגזר הדין שצפייה בתכנים פדופיליים אינה עברה פלילית, וכמוה גם הגלישה באינטרנט בחיפוש אחרי תכנים פדופיליים אינה אסורה. ראו ת"פ (שלום ת"א) 7936/07 **מדינת ישראל נ' פלוני** (פורסם בנבו, 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** (פורסם בנבו, 30.9.2009).

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

nevo.co.il

בצד הדוגמאות הללו, המלמדות על שימוש במטאפורות ובאנלוגיות 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 ופחות לצורכי 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 "הבית החכם" יוכל באמצעות זאת לפרוץ גם 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 ובאנלוגיות 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 באשר למידע הדיגיטלי, לא כל שכן קשה לבקר אותה. אעבור עתה מן הדוגמאות הכלליות בנוגע לדיני המחשבים לטיעון הממוקד יותר בנוגע לחקיקה המסדירה את סמכויות איסוף הראיות הדיגיטליות בחקירה פלילית במרחב המקוון. אמחיש את הטיעון בהתייחס לחקיקה הישראלית, תוך הפניות לדין הזר.

2. התפישה הפיזית באשר 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

מיני: Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote, 2007) 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 ג בה"ש 67.

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

nevo.co.il

לענייננו, אף הוא כבר בן יותר משלושים שנה. הפסד״פ, כמו גם חוק האזנת סתר, תוקנו בשנת 1995 והוכנסה אליהם, לראשונה, ההתייחסות ל״חומר מחשב״ ול״תקשורת בין מחשבים״.[22] אולם מדובר 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, בעיקר בתחום המחשוב והתקשורת, ניתן לדבר בהחלט על חקיקה המפגרת אחרי המצב הקיים בשטח. הפיגור הוא בשני מובנים: (א) במובן הפשוט של אי־התייחסות החוק להתפתחויות טכנולוגיות חשובות כגון כניסתו של האינטרנט לחיינו. החקיקה המסדירה את סמכויות האיסוף אינה מתייחסת כלל לאינטרנט; (ב) במובן עמוק יותר, לעתים סמוי, שעניינו תפישת המחוקק את הראיה הדיגיטלית. כפי שאראה בהמשך, המחוקק תופש את הראיות הדיגיטליות בכלים ובאופן שבו הוא מתייחס לראיות במרחב הפיזי, ובאופן אמתי לא בידל את הראיות הדיגיטליות מהן, גם אם מצא לנכון להתקין כמה הוראות ייחודיות ל״חומר מחשב״.[23]

מעניין שכבר לפני יותר משני עשורים הובעה בספרות המשפטית התמיהה על שהחקיקה בתחום דיני הראיות והחקירה בכלל (לרבות נושא סמכויות האיסוף שממין ענייננו) קפאו על מקומן ונשארו כשהיו מאז קום המדינה, ובהתבסס על המשפט המנדטורי.[24] מהפכת המחשוב, ובעיקר המעבר מעידן המחשב הבודד לעידן הרשתי של האינטרנט, טרפו את הקלפים שוב, והותירו את החוקים הנוהגים לא רלוונטיים עוד לחקירה בסביבה הדיגיטלית. בשנת 1986 ניסח השופט דן ביין 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 שלו, כהצעה ראשונית המוגשת כבסיס לדיון בוועדת מומחים.[26] הצעתו לא התייחסה לחומר מחשב. בשנת 1996 התכנסה ועדה מטעם משרד המשפטים, בראשות שופט

---

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 בשביל 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 אפיונים דומים בקשר לסמכויות האיסוף.

24 גרשון אוריון ״מגמות אינקוויזיטוריות בדיני הראיות״ משפט פלילי, קרימינולוגיה ומשטרה א 115, 123—124 (גרשון אוריון עורך, 1986).

25 דן ביין ״הצעת חוק סדר הדין הפלילי (אמצעים משטרתיים)״ משפט פלילי, קרימינולוגיה ומשטרה א 265 (גרשון אוריון עורך, 1986).

26 שם, בעמ׳ 265, 271.

nevo.co.il

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 זו של ביין. בחודש מאי 1996 הוגש דין וחשבון הוועדה לסדר דין פלילי (אמצעים משטרתיים) (חיפוש, הצגה, תפיסה וחילוט) (להלן – דוח ועדת לוין). מסקנות הוועדה לא יושמו עד היום בחקיקה. הוועדה הציעה כמה 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. בדוח הוועדה מבוטא הניסיון להתחשב בזכויות הפרט המוגנות אשר עוגנו בחוק־יסוד: כבוד האדם וחירותו והוכרו במפורש 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 כמה תיקונים בפסד"פ ובחוק האזנת סתר אשר לא יישמו המלצות מדוח 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 דוח לוין. כאמור, הוא לא ייחד כל התייחסות נפרדת לאיסוף ראיות דיגיטליות. נוסף על כך, גם בניסיונה של הוועדה למנות את הזכויות המוגנות הניצבות אל מול צורכי החקירה – יש חסרים ניכרים. הוועדה מנתה רק את הזכות לפרטיות, ובמידה מוגבלת בלבד גם את זכות הקניין.[29] הנהנה מהזכויות החוקתיות, על פי עבודת הוועדה, הוא בעל החפץ שבענייננו 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 חשובה בהקשרנו אירעה בשנת 2014, עת פורסמה הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד–2014[30] (להלן – הצעת חוק החיפוש או

---

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 כמה 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 באשר למידת ההוכחה הדרושה לצורך הוצאת צו חיפוש יכול שישתנה בעקבות חקיקת חוקי היסוד, כמו גם הסנקצייה הראייתית בגין איסוף ראיות שלא כדין בידי 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).

29 בעמ' 1–9 לדוח 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.

nevo.co.il

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, התפתחותה של החקיקה הייתה אבולוציונית 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.

א) התפישה הכפולה – חיפוש והמצאה

ההבחנה היסודית בדיני איסוף הראיות הייתה בין חיפוש במקום לבין המצאת מסמך. החיפוש מבוצע בידי הרשות החוקרת במקום פיזי מסוים.[32] לעומת זאת ההמצאה היא פעולה שאינה מבוצעת בפועל בידי 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 באמצעות תפיסתם. החפצים שייתפסו, מורה המחוקק, הם אלה שרלוונטיים לצורכי חקירה, משפט או חילוט עתידי.[34] על בסיס התפישה הכפולה האמורה, של חיפוש והמצאה, פותחו הדינים המקבילים באשר לאיסוף 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.

חדירה לחומר מחשב: סמכות זו מוסדרת בפרק השלישי לפסד״פ, בעיקר בסעיף 23א. החדירה לחומר מחשב נתפשת, מבחינת המחוקק, כמעין מקרה פרטי של חיפוש בחצרים, בראש ובראשונה בשל 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] בכמה תוספות שנועדו לייחד במידה מסוימת את החדירה לחומר מחשב.[36] נקודת

---

31 ראו להלן בפרק ד.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.

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, בכמה 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).

nevo.co.il

המוצא של חיפוש בחצרים מציבה שתי דרישות באשר לחדירה לחומר מחשב, אשר לטענתי אינן מועילות לשרת את הזכויות של הנחפש כראוי: **האחת**, כי "תופש הבית או המקום שמחפשים בו, או אדם מטעמו, יינתן לו להיות נוכח..."; **השנייה**, כי תותר נוכחות שני עדים שאינם שוטרים אלא אם מתקיימים כמה 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 לא מזוינת אם המשטרה הורסת ראיות, משנה אותן או שותלת אותן. ואולם, בכל הנוגע לאיסוף ראיות דיגיטליות, דרישת נוכחות שני העדים שאינם שוטרים אינה מתאימה לערך שאותו 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 מוצגות על מסך או ניתנות לצפייה ולהבנה, בוודאי לא בעין לא מיומנת. היכולת לשמור שמירה נאותה על טוהר המידות של שוטר רשלן או כזה המשתיל ראיות בזדון – מוגבלת מאוד 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 השגתן 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 שלפיה החדירה לחומר המחשב שקולה לחיפוש פיזי, ולא היא.

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

---

36 ראו הוראות סעיפים 23א, 26(ב), 32(ב), 32(ב1) ו־32א לפסד"פ, שם נקבע: (א) החדירה לחומר מחשב תיעשה בידי 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 מתכוונים להשתמש בו כראיה או לחלטו; (ה) למחזיק במחשב קמה זכות לקבלת העתק מחומר המחשב שנתפס ממנו בתוך ארבעה 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**, פ"מ תשס"א(2) 728, 753–743 (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**, בפס' 5 (פורסם בנבו, 20.11.2002).

38 ב"ש (מחוזי ת"א) 91637/03 **אופיר נ' ימ"ר ת"א**, בעמ' 8 להחלטה (פורסם בנבו, 13.7.2003).

nevo.co.il

בטרם אעבור להמצאת חומר מחשב, אציין כי התפישה הפיזית בנוגע לפעולת החדירה לחומר מחשב אינה נחלתו של המשפט הישראלי בלבד. גם במשפט האמריקני, למשל, זוהתה תפישה פיזית באשר לאופן שבו 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. מילים אלה כוונו לחפצים ולמקומות, ולא למידע.[39]

המצאת חומר מחשב: 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 להצגת חפצים, כאשר חוק המחשבים תיקן בשנת 1995 את הגדרת ״חפץ״ שבסעיף 1 לפסד״פ כדי שיכלול גם חומר מחשב. בכך, הפך סעיף 43 לפסד״פ – אשר לא תוקן בעצמו מאז שנת 1969 עת נערך הנוסח החדש לפסד״פ[40] – למקור הסמכות להמצאת חומר מחשב, להוציא את המקרה הפרטי של נתוני תקשורת המוסדר למן שנת 2007 בחוק נפרד, ויפורט להלן. בשונה מחדירה לחומר מחשב, הכוללת דרישות נוספות על אלו המנויות לגבי חיפוש בחצרים, במקרה 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 אין 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, באשר ל״נתוני תקשורת״,[42] מטופל במפורט בחוק נתוני תקשורת. במילים אחרות, כל המצאה של חפץ ושל ראיות דיגיטליות תיעשה לפי סעיף 43

---

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

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, 760–759, 768–767 (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 לא יכללו נתוני תוכן. היסוד השלילי נועד לבדל את נתוני התקשורת מהאזנת סתר מחד גיסא ומהמצאת חומר מחשב אחר שאינו נתוני תקשורת מאידך גיסא, ובכך למנוע 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, 318–314 (ניבה אלקין־קורן ומיכאל בירנהק עורכים, 2009).

nevo.co.il

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״ כשמדובר בנתוני 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 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 בהרבה מזה שמופיע בנוגע לחדירה לחומר מחשב ובנוגע להמצאת חומר מחשב,[46] ומגלם הכרה מפותחת יותר בזכויות החוקתיות העתידות להיפגע כתוצאה מפעולות האיסוף שמכוח החוק.[47]

---

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, ובשל אופן הניסוח של סעיף שמירת הדינים בחוק נתוני תקשורת הם אף אינם כלולים – כבעבר – בסעיף 43 לפסד״פ מאידך גיסא. נוצרה כאן למעשה לאקונה בחוק, אשר אינה מגלמת להערכתי כל הכרעה מכוונת, אלא מדובר בטעות בהליך החקיקה אשר טעונה תיקון. בשל 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 עברה מסוג פשע, גילוי מבצעהּ 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.

45 סעיף 3(י) לחוק נתוני תקשורת.

46 אשר לצו לקבלת נתוני תקשורת, החוק מציב את התנאים כדלקמן: (1) החשד צריך להיות בעברה מסוג עוון או פשע (בסיס עברות רחב יחסית); (2) דרישת תכלית: הצלת חיי אדם או הגנה עליהם; גילוי עברות, חקירתן או מניעתן; גילוי עבריינים והעמדתם לדין; חילוט רכוש על פי דין. על השופט להשתכנע שהצו המבוקש ישרת את אחת התכליות הללו, אולם אין דרישה להוכחת רמת חשד מסוימת לעצם קיומה של עברה או הסתברות להתרחשותה של עברה עתידית (סעיף 3(א)); (3) הגורם השיפוטי המוסמך הוא שופט שלום (סעיף 2(א)); (4) על הבקשה לצו לקבלת נתוני תקשורת להיחתם בידי קצין משטרה מכל דרגה שהיא שמפכ״ל המשטרה הסמיכו לעניין זה (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 שעליו מבוססת הבקשה, התכלית הרלוונטית, סוג נתוני התקשורת המבוקשים, פרק הזמן שלגביו מבוקשים נתוני התקשורת (צופה פני עבר או צופה פני עתיד), פרטי הזיהוי של המנוי או המתקן שבעניינו 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) סיפה לחוק, וניתן להאריך את התקופה או לבקש צווים

nevo.co.il

ב) מתפישה כפולה לתפישה משולשת – חיפוש, המצאה והאזנה

בשנת 1979 נחקק חוק האזנת סתר הישראלי. החוק הכיר בכך שלצד חפצים ומסמכים שניתן לתפסם במסגרת חיפוש או לפי 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, ולא על דרך של העתקת המידע כשהוא במצב "נייח".[48] פעולת האזנת הסתר נתפשת,

---

נוספים לאחר מכן, לפי סעיף 3(יא); (8) יש ניסיון להבנות את שיקול דעתו של השופט הדן בבקשה (סעיף 3(ז)): על בית המשפט להתחשב בתכלית המבוקשת ולבחון כיצד הצו יוכל לתרום למימושה של התכלית, במידת הפגיעה בפרטיותו של אדם, בחומרת העברה ובסוג נתוני התקשורת המבוקשים. הבניה נוספת של שיקול דעתו של השופט מופיעה בסעיף 3(א) אמצע וסיפה לחוק, ולפיה על השופט לפרט את האופן שבו 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, וזאת באשר לזכות לפרטיות בלבד; (9) יש 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 שבענייננו יתקבלו נתוני התקשורת ככל שהם ידועים, פרק הזמן שלגביו 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 לנתוני תקשורת של בעלי מקצועות חסויים על פי כל דין, יש דרישות נוספות: יש לציין במפורש בבקשה אם המנוי שבענייננו 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 החשד שבעל המקצוע החסוי מעורב בעברה מושא 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, שבו לא נדרש להוכיח את רמת החשד לביצוע העברה, כאן נדרשת הוכחה ברמה של "יסוד לחשד" שבעל המקצוע החסוי מעורב בעברה.

את חוק נתוני תקשורת תקפו האגודה לזכויות האזרח ולשכת עורכי הדין כלא חוקתי מחמת היותו פוגע יתר על המידה בזכות לפרטיות, זאת על בסיס הטיעונים האלה: (א) נטען כי הסמכויות בחוק צריכות להימסר רק באשר לעברות 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 בנוגע לבעלי מקצועות חסויים המעורבים בעברה 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** (פורסם בנבו, 28.5.2012). עם זאת קבע בית המשפט העליון 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 ו.ה.3..

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 שבה נקבע בעניין האזנת סתר טלפונית כי אינה בבחינת 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.

nevo.co.il

על פי המבחנים שמציב החוק לרשות החוקרת, כפעולה הפוגענית ביותר, ולפיכך הוצבו ערובות פרוצדורליות־פורמליסטיות קפדניות יחסית כדי לאשר פעולת חקירה זו.[49] גם ברמת הפסיקה ניתן לציין את חוק האזנת סתר כנבדל מבחינת עצמת ההגנה על הזכות לפרטיות.[50]

---

49 אפרט על הבלמים שמציב החוק בשלב הגשת הבקשה לצו האזנת סתר ובשלב הוצאת הצו: (1) החשד צריך להיות בנוגע לעברה מסוג פשע (סעיף 6(א)); (2) דרישת תכלית: גילוי, חקירה או מניעה של עברות; גילוי או תפיסה של עבריינים; חקירה לצורכי חילוט (סעיף 6(א)), כאשר על השופט להשתכנע שההאזנה תשרת את אחת מהתכליות האמורות; (3) צו האזנת סתר יכול שיוצא בידי 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 שמפכ״ל המשטרה הסמיכו לעניין האזנות סתר (סעיף 6(א)); (5) הבקשה לצו האזנת הסתר מובנה באמצעות ניסוח הטופס במסגרת התוספת לתקנות האזנת סתר (בקשה להיתר האזנה), התשס״ח–2007. הבקשה צריכה לכלול התייחסות לפרטי החשוד, או לקו הטלפון או למקום שבעניינו מבוקשת ההאזנה; מהות החשדות וסעיפי העברה; 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, את ההחלטות בבקשות אלה ואת החומר 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, כך: יש לתאר את זהות המואזן או את זהות הקו המואזן, וכן את מקום ביצוע השיחות וסוגן. כן יש לתאר את דרכי ההאזנה שהותרו. גם תקנות האזנת סתר מבנות למעשה את הצו עצמו באמצעות קביעת הטופס, כולל קביעת רובריקה למילוי נימוקי ההחלטה להיענות או לסרב לבקשה להאזנת סתר. התייחסות ספציפית צריכה להינתן בצו לשאלה אם תותר כניסה למקום על מנת להתקין את ציוד ההאזנה, לפרקו או לסלקו. ככל שתותר כניסה כאמור, על הצו לפרט את המקום האמור (סעיף 10א).
קיימות דרישות נוספות לאחר ביצוע הצו: (1) קיימת חובת דיווח חודשי של מפכ״ל המשטרה ליועץ המשפטי לממשלה על מספר צווי האזנת הסתר שניתנו, כמו גם על צווי האזנת סתר לבעלי מקצועות חסויים על פי דין ולחברי 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 על 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 השנייה 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 באלה: (1) טיב העברות אשר בגינן ניתן להתיר האזנת סתר למואזנים הנמנים עם 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 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 באשר להאזנת סתר אגב אורחא לבעלי מקצועות חסויים, אולם המשטרה נוהגת כך בפועל גם בעניינם: 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

nevo.co.il

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), וזאת 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 (בידי הרשות החוקרת) או בר־המצאה (בידי צד שלישי), ומצב שני מנוגד שבו הוא נמצא בתקשורת בין מחשבים, שאז הוא בר־האזנה. החלוקה המשולשת באשר לסמכויות האיסוף — חיפוש (לרבות חדירה לחומר מחשב), המצאה (לרבות המצאת חומר מחשב) והאזנה (לרבות לתקשורת בין מחשבים) — מקובלת גם במשפט האמריקני.[53]

ג) כשלי סיווג הנובעים מהתפישה המשולשת

בשל החלוקה הקשיחה יחסית לשלוש קטגוריות של פעולות איסוף — חיפוש, המצאה והאזנה — נוצרים כמה כשלי סיווג ביחס לראיות דיגיטליות. אעמוד על שלושה: **האחד**, באשר למעמדה של פעולת "מעקב חי" אחר גלישות באינטרנט; **השני**, באשר למעמדה של קליטת פעולות אוטומטיות של תקשורת בין־מחשבים; **השלישי**, באשר למעמדה של פעולת איסוף של

דברים מתוך דין וחשבון של משרד המשפטים לבדיקת משטר האזנות הסתר בראשות המשנה ליועץ המשפטי לממשלה, עו"ד לבנת משיח. המלצות דוח 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 בעקבות אישור צו ההאזנה; (ו) בירור ההצדקות באשר למשך תקופת 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), שבו הוא מעביר את צו האזנת הסתר שעמד לערעור תחת שבט הביקורת של מבחני המידתיות החוקתיים. כן ראו הניתוח בדוח 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, 198–194 (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 קֵר (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).

nevo.co.il

מידע העובר בתקשורת א־סינכרונית. כפי שנראה, אשר לשתי הפעולות הראשונות, מקובל לסווגן כפעולות של האזנת סתר, הגם שבמהותן אין מדובר ב"שיחה" במובן של העברת מסרים הדדית בין שני אנשים או יותר. אשר לפעולה השלישית, כשל הסיווג הוא מכיוון אחר: אמנם מדובר בהעברת מסרים בין שני אנשים או יותר, אולם קיימת אי־בהירות ממשית באשר ל"שיבוץ" של פעולת האיסוף האמורה: האם צריכה להיות ממוקמת בקטגוריית ההמצאה על ידי ספק שירותי התקשורת או בקטגוריית האזנת הסתר?

1) מעמדן של גלישות באינטרנט

הקושי הפרשני בנוגע 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 חשוב, הנראה אינטואיטיבית כמחויב המציאות, המבהיר מהי "שיחה", להבדיל מההגדרה כיצד מבצעים את ה"שיחה". וכך, למשל, היה ניתן לצפות שההגדרה תציין ש"שיחה" היא 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 למוזיקה דרך האינטרנט וכדומה. הגלישות באינטרנט הן פעולות עצמיות שמבצע משתמש האינטרנט. פורמלית הן כוללות 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).

2) מעמדן של פעולות אוטומטיות של תקשורת בין־מחשבים

קיימת קטגוריה נוספת של פעולות בתקשורת בין־מחשבים הנכללות פורמלית בהגדרה של "שיחה" בחוק האזנת סתר הגם שאין בהן משום החלפת מידע בין שני אנשים או יותר. הכוונה למצבים שבהם 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,

---

54 עיון בהצעת חוק האזנת סתר, התשל"ט–1979 ובהצעת החוק לתיקון מס' 1 לחוק האזנת סתר, אשר הרחיבה כאמור את הגדרת ה"שיחה" גם ל"תקשורת בין מחשבים", מלמד כי ההנחה הסמויה של המחוקק היא כי "שיחה" כוללת חילופי דברים בין שני אנשים ויותר. תכליתו 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 1361. ראו גם הצעת חוק האזנת סתר (תיקון), התשנ"ד–1994, ה"ח 2292.

nevo.co.il

בקטגוריה של גלישות באינטרנט ההתקשרות היא בין אדם, באמצעות מחשב, לבין מחשב). יתר על כן, ההתקשרות מתבצעת אוטומטית, פעמים רבות בלא יזמתו של מי ממשתמשי המחשב, ולעתים אף בלא ידיעתם.

3) מעמדה של תקשורת א־סינכרונית

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, בעיקר 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] עם צורות התקשורת הא־סינכרוניות המוכרות לנו כיום ניתן למנות, כדוגמה, את הדוא"ל, המסרון (SMS) או ה־MMS (הודעה עם תמונה), הודעה בתא קולי טלפוני והעברת הקבצים באמצעות שרת FTP. נוסף על אלה, קיימות עוד צורות 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), ועניינו 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, שאפרט על אודותיו בהרחבה בהמשך, לסווג את הפעולה כראוי במסגרת התבניות של החוק הקיים, הכוללות כאמור שלוש אפשרויות: חיפוש, המצאה והאזנה. קושי זה ממחיש המחשה 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.

תרשים 4.1 ממחיש את המשמעות של תקשורת א־סינכרונית, באמצעות אופן ביצוע ההתקשרות בדוא"ל:[58]

---

55 ראו Nimrod Kozlovski, *A Paradigm Shift in Online Policing – Designing Accountable Policing* 88–93 (J.S.D. Dissertation, 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 "קו" מושא ההאזנה בסעיף 1 לתקנות האזנת סתר (בקשה להיתר האזנה), התשס"ח–2007. זהו המקום היחיד שבו החקיקה (מחוקק המשנה) מתייחסת לתקשורת א־סינכרונית כלשהי במסגרת כינון סמכויות האיסוף של הרשות החוקרת, ואולם התייחסות זו אינה לצורכי הגדרת תחומי הסמכות אלא לצורכי 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 – הכול כפי שיפורט להלן.

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

nevo.co.il

תרשים 4.1 — מעברה של הודעת דוא״ל

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

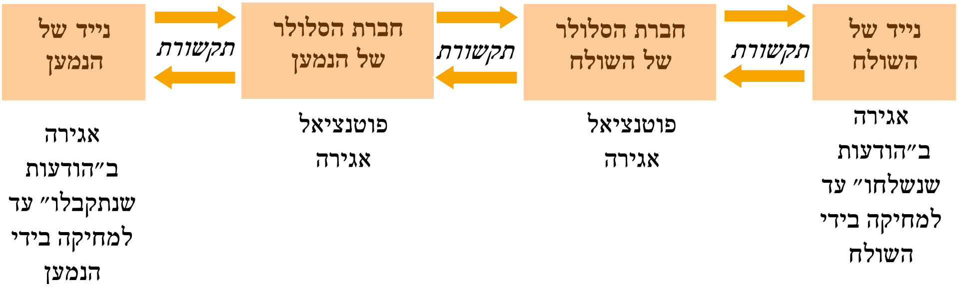
** האגירה תתבצע אם מדובר בשירות דוא״ל המותקן במחשב הקצה, שלפיו הדוא״ל מועבר באמצעות Mail User Agent (MUA) כדוגמת תוכנת Microsoft Outlook.

התרשים מייצג ארבעה מחשבים המעורבים בתהליך העברתו של הדוא״ל. ההצגה היא טיפוסית בלבד, ואם למשל מחשבו של השולח מחובר ברשת מקומית, אז עשויה להיתוסף עוד ״תחנה״ בדרך, שהיא שרת הדוא״ל של הרשת המקומית שבה 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. אם מדובר בתוכנת דוא״ל המותקנת ב״שולחן העבודה״ של השולח (MUA), הרי שבמקביל לשליחת הדוא״ל נשמר העתק ממנו בתיקיית Sent items במחשבו של השולח. אם מדובר 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; לעומת זאת אם 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, יכול שההודעה הנכנסת תישמר במלואה במחשב הקצה של הנמען עם הַגיע ההודעה ל־Inbox, או שההודעה תיוותר 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, אפשר שההודעה תישמר באותה עת גם אצל ספקית שירותי הדוא״ל או להימחק משם, תלוי בהגדרתה של תיבת הדוא״ל של הנמען.

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 דוח 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 העבירה״ **ספר דייויד וינר** 429, 459—477 (דרור ארד־אילון, יורם רבין ויניב ואקי עורכים, 2009).

אשר לשליחת הודעת מסרון (SMS) או MMS, תהליך מעברה של הודעה מעין זו ניתן לתיאור בתרשים שלהלן (תרשים 4.2):[59]

תרשים 4.2 — מעברה של הודעת SMS/MMS

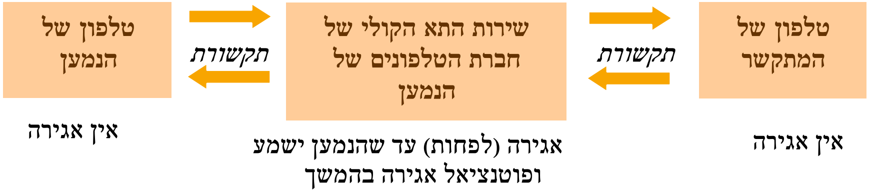


59 על ״מסעו״ של המסרון (ה-SMS) ניתן ללמוד למשל מהבקשה לתביעה ייצוגית שהוגשה נגד חברת פלאפון תקשורת בע״מ על שהיא נוהגת לשמור מסרונים שנשלחו ללקוחותיה המנויים בחברת פלאפון. בעקבות ההד התקשורתי שליווה את הגשת הבקשה הודיעה החברה על הפסקת שמירת המסרונים של לקוחותיה. ראו נועם שרביט ״פלאפון מודה: שומרת את כל תוכני 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** (פורסם בנבו, 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, שבו הותקן סעיף 30א לחוק, ונאסר על הפצת דואר זבל (דוא״ז) באמצעים שונים, הרי שבחר המחוקק להגדיר, בין היתר, את שני האופנים האלה לשליחת דוא״ז: באמצעות ״הודעה אלקטרונית״ (מקביל לדוא״ל), המוגדרת ״מסר בזק מקודד המועבר באינטרנט אל נמען או קבוצה של נמענים, וניתן לשמירה ולאחזור בדרך ממוחשבת״; באמצעות ״הודעת מסר קצר״ (מקביל ל-SMS או MMS), המוגדרת ״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 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 בדבר האופן שבו ראוי שיועבר המסרון, אולם בפועל, מבחינה טכנולוגית, ודאי שאין מניעה (וככל הנראה כך נעשה בפועל) שהמסרון ייאגר אצל חברת הסלולר. יוער עוד כי חרף הפרסום בכלי התקשורת, שלפיו חברת פלאפון הפסיקה את שמירת המסרונים של לקוחותיה, הרי שניתן להניח כי למצער במקרה שבו מכשיר הטלפון של הנמען כבוי, והמסרון אינו יכול להיקלט במכשיר הקצה שלו, הרי שחברת הסלולר אוגרת למעשה את המסרון בשבילו עד שידליק את מכשירו.

nevo.co.il

ואשר להודעה בתא קולי, הדברים ניתנים לתיאור בתרשים שלהלן (תרשים 4.3):[60]

תרשים 4.3 — מעברה של הודעה בתא קולי



מהו תרגומם של התרשימים לשפה המשפטית? בכל המצבים שתוארו לעיל, שבהם עובר המידע בתקשורת, אין ספק שלפי הגדרת החוק הישראלי מדובר ב״שיחה״ אשר קליטתה בעת מעברה בקווי התקשורת הללו תהיה 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 אין מבוצעת בשלב זה פעולה טכנית של האזנה אלא של חדירה לחומר מחשב בידי הרשות החוקרת או המצאה של חומר מחשב בידי צד שלישי שמצטווה לעשות כן. מבחינה מהותית מדובר 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 הנמען קרא/פתח אותו. אם מדובר במצב שבו גם לאחר שהנמען פתח את המסר האלקטרוני, המסר עדיין נאגר 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 מתאפשר 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) מתפקדת לא רק ככלי להעברת מסרים אלא גם ככלי אחסון לכל דבר ועניין.[61]

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).

61 עד לפני כמה 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 Live Hotmail גדל ל־5 גיגה בייט״ **Ynet** (14.8.2007) http://www.ynet.co.il/articles/1,7340,L-3437367,00.html.

nevo.co.il

בישראל הובעו עמדות שונות בנוגע 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 שבה התעוררה השאלה הייתה פרשת **בדיר**. לאחים בדיר יוחסו עברות רבות של מרמה, חדירה לחומר מחשב ועוד. בין היתר הואשמו בעברה על חוק האזנת סתר, על בסיס העובדה שהם התקשרו עם תאים קוליים של אחרים תוך פיצוח ססמאות הכניסה לתאים הקוליים והקשבה להודעות שהושארו בהם. הפרקליטות טענה שהקשבה להודעה בתא קולי של בזק שהנמען שלה טרם האזין לה, היא האזנת סתר אסורה. בית המשפט המחוזי בתל־אביב הרשיע את האחים בעברה 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 שבמסגרתה 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), וכל זאת בצו מכוח סעיף 43 לפסד״פ. בית משפט השלום נעתר לבקשה. צו ההמצאה מוען לחברת נטוויז׳ן, וזו התנגדה לצו. טענתה העיקרית של חברת נטוויז׳ן הייתה כי מדובר בפעולה של האזנת סתר ולא בהמצאת חומר מחשב. בית משפט השלום, במסגרת עיון חוזר, שב ואישר את החלטתו המקורית.[63] חברת נטוויז׳ן 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 לתפסם במסגרת צו המצאה, ואילו קבלה עתידית של דוא״ל או הודעות בתא הקולי, המצויות אצל ספק השירות – דינן כדין האזנת סתר. עמדה זו הביעה המדינה בערר בעניין **נטוויז׳ן**, ולמעשה נסתיים שם הדיון.[64]

מונדיר בדיר, הנאשם המרכזי בעניין **בדיר**, ערער לבית המשפט העליון, כשבאמתחתו החלטת בית המשפט המחוזי בעניין **נטוויז׳ן**, שממנה נלמדת גם עמדתה של פרקליטת המדינה. במסגרת הדיון בערעור הסכימה המדינה 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 **נטוויז׳ן**, כי חומר הקיים אצל ספק השירות בעת ביצוע החדירה אינו בר־האזנה, וכי האזנת סתר רלוונטית רק לקליטת חומר שעתיד להגיע לספק השירות. לעומת זאת בעניין **בדיר** 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] כמה חודשים לאחר פסק הדין פורסמה גם

---

62 ת״פ (מחוזי ת״א) 40250/99 **מדינת ישראל נ׳ בדיר**, פרק עשרים ושבעה (פורסם בנבו, 3.9.2001).

63 ב״ש (שלום ת״א) 6703/00 **חברת נטוויז׳ן בע״מ נ׳ צה״ל** (פורסם בנבו, 6.4.2000).

64 ב״ש (מחוזי ת״א) 90868/00 **חב׳ נטוויז׳ן נ׳ צבא ההגנה לישראל** (פורסם בנבו, 22.6.2000).

65 ע״פ 10343/01 **בדיר נ׳ מדינת ישראל** (פורסם בנבו, 2003). פסק הדין לאקוני וכולל כמה שורות שבהן מתועדת הודעת המדינה על הסכמתה לזיכויו של מונדיר בדיר מאישומי האזנת הסתר, ללא הסבר על אודות טעמי ההסכמה.

66 בכל הנוגע להאזנת סתר בחר המחוקק הישראלי בטכניקת חקיקה שלפיה אותה הגדרה ניתנה הן לעברה 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 עברה של האזנת סתר. כך נעשה גם במקרה

נבו nevo.co.il

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 הודעות קוליות שיגיעו בעתיד לתא הקולי), הרי מדובר בפעולה שהיא על פי מהותה האזנת סתר.[67]

הפעם הבאה שבה 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 התעוררו ההתנגדויות לא בשלב ביצוע הצו, כבמקרה **נטוויז׳ן**, אלא בשלב הגשת הראיות לבית המשפט, בידי באי כוחם של הנאשמים, שגרסו כי הפעולה שבוצעה עלתה כדי האזנת סתר, ועל כן דין הראיות שנאספו מכוחה להיפסל לפי סעיף 13 לחוק האזנת סתר, שכן מדובר בהאזנת סתר שנעשתה בלא היתר כדין. בית המשפט המחוזי קיבל את הטענה ופסק כי למעשה כל דוא״ל שנמצא אצל ספק שירות ושהנמען טרם קרא אותו – דינו כדין ״שיחה״ שלא הסתיימה, ועל כן תפיסת החומר האמור מחייבת צו האזנת סתר.[71] החלטתו של בית המשפט

של חדירה לחומר מחשב בחוק המחשבים: העברה 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 שהייתה עלולה להיווצר בעמדת המדינה. יוער כי אין מדובר בטכניקת חקיקה הייחודית למדינת ישראל. כך, גם בבריטניה למשל מוגדרת פעולת האיסוף של האזנת סתר כפי שמוגדרת העברה 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** (פורסם בנבו, 5.2.2007) (להלן – עניין **פילוסוף I**).

69 ראו שם, בפס׳ 3 ו־5.

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 החלטתו של בית המשפט בעניין **פילוסוף I**. עוד על המצאה כתחליף־חיפוש ראו למשל עניין **שרון**, לעיל ה״ש 41.

71 לעומת זאת אם הנמען כבר קרא את הדוא״ל, הרי שאיסופו מספק השירות לא יהיה פעולה של האזנת סתר כי אם פעולה של חדירה לחומר מחשב או המצאה, תלוי בנסיבות (אם המשטרה ביצעה את הפעולה בעצמה או שדרשה שספק שירותי הדוא״ל יבצעה). ראו לעניין זה גם את ת״א (מחוזי מרכז) 4559-09-07 **א.ע. (המנוח) נ׳ ק.פ. בע״מ** (פורסם בנבו, 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** (פורסם בנבו, 26.7.2011).

nevo.co.il

המחוזי בפרשת הסוס הטרויאני ניתנה במסגרת החלטת ביניים בהליך פלילי,[72] וכך, בפעם השנייה מאז עניין **בדיר**, נמנעה הכרעה של בית המשפט העליון בסוגיה.

בעמדתו של בית המשפט בעניין **פילוסוף I** תומכים קוזלובסקי[73] וגולדנברג־אהרוני.[74] גולדנברג־אהרוני דימתה את שליחתו של המידע לנמען דרך ספק השירות לנסיעה ברכב, כאשר בדרך נעצר הרכב ברמזור. אין מדובר בסיום הנסיעה כי אם בעצירה שאינה משנה את מהות הנסיעה ואת כיוונה. 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, לבד מהיותן שובות לב, יכולות גם לשבות את המחשבה. לטעמי מטאפורת הרמזור או תחנת הדלק רחוקה יותר מן האנלוגיה הזאת: ניתן לדמות שליחת הודעה בדוא״ל באמצעות ספק שירות למצב שבו 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 שיחתם 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 כי תפיסת פתק שכזה לא תיעשה אלא בצו חיפוש או המצאה (בהתאם לנסיבות).

לאחר ההחלטה הזאת בעניין **פילוסוף I** עתרה ההגנה בתיק להרחבה נוספת של מושג ״האזנת הסתר״, הפעם אל הדוא״ל המתקבל במחשב הקצה של הנמען, שהנמען טרם פתח אותו. 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 בידי הנמען כפרמטר לקביעה אם הדוא״ל הגיע לידו אם לאו. אם כך הוא הדבר, צדקה לכאורה ההגנה בטענה שגם במחשב קצה של אדם יכול להימצא דוא״ל שהנמען טרם קרא אותו. על פי מבחן **פילוסוף I**, לכאורה גם דוא״ל שכבר הגיע למחשב הקצה ונאגר בו, אך הנמען טרם קרא אותו, 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 הנמען את הדברים (עניין **פילוסוף II**).[75]

באותו היום שבו 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 במסרונים שנאגרו בזיכרון המכשיר.

---

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

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** (פורסם בנבו, 18.9.2007).

nevo.co.il

המשטרה פתחה את המכשיר כיומיים לאחר תפיסתו, ובאמצעות צו חדירה לחומר מחשב עיינה במסרונים שנאגרו בו.[76] בין היתר היו במכשיר גם מסרונים 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 עתירתו. נקבע, כי עם הגיע ההודעות למכשיר הטלפון של החשוד, הרי שאף אם זה טרם עיין בהן, ואף אם ההודעות נשלחו לאחר תפיסת המכשיר בידי המשטרה, הרי שמהותית מדובר 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 בעברות של חדירה לחומר מחשב כדי לעבור עברה אחרת, לפי סעיף 5 לחוק המחשבים, ופגיעה בפרטיות. הנאשם הורשע בעברות אלה בבית משפט השלום, ובמסגרת הדיון בערעורו קבע בית המשפט המחוזי כי קריאת תכתובות הדוא״ל אצל ספק השירות היא פעולה של האזנת סתר ולא של חדירה לחומר מחשב. בשונה מעניין **פילוסוף I** לא הבחין בית המשפט בין דוא״ל המועתק מספק שירותי הדוא״ל בטרם קרא אותו הנמען, לבין דוא״ל שהנמען כבר קראו על אף הוא 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 מדובר בשרת דוא״ל שבבעלותו של המעביד ובתיבות דוא״ל שהקצה לעובדים, ומצד 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 היא האזנת סתר או פגיעה בפרטיות על דרך של

---

76 מכשיר טלפון סלולרי הוא למעשה מכשיר דו־שימושי מבחינה משפטית: מצד אחד, בכל הנוגע לקיום שיחות הטלפון, הרי שמדובר בציוד קצה שבאמצעותו מתבצעת שיחה; מצד שני, בכל הנוגע לזיכרון של מכשיר הטלפון הסלולרי, ולכל האגור בו (ספר טלפונים, יומן שיחות, משחקים, לוח פגישות, תמונות, מסרונים, 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** (פורסם בנבו, 2.6.2008), שם נפסק כי עיון במידע האגור בטלפון סלולרי הוא בבחינת 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 יישומה של אותה החלטה נעשה באופן שגוי ומרחיב יותר. כנובע מפסק דין זה בעניין **פלוני**, לעיל, 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 מדובר בפעולה של האזנת סתר ולא חדירה לחומר מחשב. זאת בניגוד לעניין **פילוסוף I**, שם נקבע כי רק אם הנמען טרם קרא את הדוא״ל, דין הדוא״ל כדין ״שיחה״ הכפופה לחוק האזנת סתר, ולא כדין ״חומר מחשב״, הכפוף להוראות הפסד״פ.

nevo.co.il

העתקת תוכן של מסר אלקטרוני שלא נועד לפרסום (לפי סעיף 2(5) לחוק הגנת הפרטיות)?[80] גם כאן הובעו כמה 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 ייחשבו האזנת סתר, שכן אין מדובר בניטור תעבורה בזמן אמת.[81] לעומת זאת במקרהו של מבקר הפנים של עיריית טבריה **בנימין אליהו** נפסק ביחס תכתובות דוא"ל שלו שהוצאו משרת העירייה, כי על פני הדברים מדובר בהאזנת סתר אסורה, אך כיוון שממילא מדובר בפגיעה אסורה בפרטיות, הכרעה ישירה בין השניים היא למעלה מן הדרוש.[82]

מקרה נוסף שאמנה 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 מסרונים אשר נטען כי הושגו בהאזנת סתר אסורה. המסרונים הושגו בדרך הזאת: בעל מכשיר הטלפון הסלולרי מסר את מכשירו לידיו של אחר על מנת שיסייע לו בהגדלת תצוגת המסך (שכן

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 שבהם 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** (פורסם בנבו, 15.7.2007). לפסיקת בית הדין הארצי לעבודה ראו ע"ע 90/08 **איסקוב־ענבר נ' הממונה על חוק עבודת נשים** (פורסם בנבו, 8.2.2011). נראה כי היות 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 בשל 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**, בפס' 23–28 (פורסם בנבו, 11.3.2010). באותו מקרה דובר בתביעה משמעתית נגד מבקר הפנים של עיריית טבריה. במסגרת ההליך הוגשו תכתובות דוא"ל של מבקר הפנים אשר חברה שראש העיר, זוהר עובד, שכר את שירותיה, הוציאה משרת הדוא"ל של העירייה. בית הדין למשמעת של עובדי הרשויות המקומיות קבע כי לא זו בלבד שאין מדובר בפעולה שאינה עולה כדי האזנת סתר (שכן מדובר בחומר שכבר "נח" בשרת ואינו במצב תקשורתי), אלא אף אין מדובר בפעולה העולה כדי פגיעה בפרטיות, שכן מדובר בשרת בבעלות העירייה, אשר התנבע מוחזק כמי שיודע שלפחות אנשי תחזוקת המחשבים הם בעלי גישה למידע שבתיבה שלו. ראו ת"מ (משמעת רשויות מקומיות) 46/06 **עיריית טבריה נ' אליהו** (פורסם בנבו, 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 ההבחנה של השופט כבוב בעניין **פילוסוף I**, בין תכתובות דוא"ל שהנמען טרם קרא לבין אלה שקרא בפועל 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** (פורסם בנבו, 16.3.2011).

nevo.co.il

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

מהתרשימים שהצגתי לעיל עולה הבחנה בין **תקשורת בתנועה (in transit communication)** לבין **תקשורת אגורה (stored communication)**. הבחנה זו נעדרת מהחקיקה הקובעת את סמכויות האיסוף בישראל, אך מוכרת בארצות הברית[84] ובאוסטרליה[85] למשל כהבחנה 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, ויש פסיקות סותרות בעניין.[86] גם אמנת מועצת אירופה בדבר

---

84 ראו 18 U.S.C. §§ 2510, 2703–2704.

85 ראו Telecommunications (Interception and Access) Act, 1979 §§ 5–6 (Au.). הוראות החוק המעגנות את ההבחנה 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 בעיקר השאלה מה דינן של הודעות דוא"ל אשר הנמען טרם קראן ואשר נאגרו בשרת, זאת להבדיל מהודעות דוא"ל שנקראו אך נשמרו בשרת (כיוון שהנמען לא מחקן). בית המשפט הפדרלי לערעורים קבע כי אין מדובר 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 הזה תכנים ביקורתיים נגד מעסיקיו. הכניסה לאתר האינטרנט התאפשרה אך ורק באמצעות הקצאת שם משתמש וססמה. סגן נשיא החברה המעסיקה חדר לאתר האינטרנט באמצעות שם משתמש וססמה אשר לא הוקצו בידי התובע, ושאותם השיג בלי ידיעתו של התובע. בית המשפט הפדרלי לערעורים בחן את מעשהו של סגן נשיא החברה המעסיקה ועמד על ההבחנה בין יירוט תשדורות בתהליך שיגורן לבין כניסה וצפייה בתיעוד של התשדורות. ועוד בעניין *Konop*, בית המשפט נדרש לשאלה אם 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 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 לעברות של החזקה והפצה של תכנים פדופיליים. במקרה Fraser v. Nationwide Mutual Insurance co., 352 F.3d 107 (3rd Cir., 2003), נדונה הסיטואציה שבה חדרה המשיבה לתכתובות דוא"ל של המערער שנמצאו בשרת הדוא"ל וצפתה בתכנים. בית המשפט הפדרלי לערעורים בחן אם מדובר בפעולה שהיא "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 ההבחנה 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, שלפיה 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.

פשעי מחשב מבחינה בין יירוט תקשורת בין 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 ניכרים באשר לפעולות חקירה שונות בזירה האינטרנטית. קשיי סיווג אלה נובעים מכך שהתפישה המשולשת פותחה בשביל 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 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 בעברות של חדירה לחומר המצוי אצל ספקי שירות והן בכל הנוגע לסיווג פעולת האיסוף שבה מדובר. אי־הבהירות האמורה מסבה נזק משולש: **האחד**, נפגמת הוודאות באשר לסוג ההגנה החוקתית ומידתה אשר יוענקו לתכנים אלה; **השני**, נפגמת הוודאות של הרשות החוקרת באשר למקור סמכותה לבצע את פעולת איסוף הראיות. "מחיר הטעות" בשאלת מקור הסמכות עשוי להיות פסילה של פעולת האיסוף כראיה במשפט; **השלישי**, כשמדובר בהעמדה לדין של נאשמים או בהגשת תובענה נגד נתבעים בגין מעשים של

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 שלפיה 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). כן מעניין לציין גם את פסק הדין בעניין 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 למיילים של עובד אינו מבצע עברה מתחום האזנת הסתר אלא עברה על הוראות ה־SCA (Stored Communication Act, 18 U.S.C. 2701– 2712). באותו מקרה, חרף התוצאה המשפטית, נסמך בית המשפט, 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 קרא הנמען את ההודעה 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) (להלן – DOJ Manua).

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

nevo.co.il

״פריצה״ לתיבות דוא״ל או ספקים אחרים של שירותי תקשורת א־סינכרונית, אי־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 לביטוייה של התפישה אל עבר ההנחות העומדות בבסיסה. במסגרת הדיון להלן אטען לכישלונה של התפישה הפיזית באשר לאיסוף ראיות במרחב הסייבר בכמה 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 להחסרת פעולות איסוף ראיות דיגיטליות לא בשל הכרעה חוקתית בין צורכי 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 בשביל ראיות במרחב הפיזי, והשינויים וההתאמות נעשו בשיטה תוֹסַפְתִית, הרי שתכונותיהן של הראיות הדיגיטליות במרחב הסייבר אינן באות לידי ביטוי לא במסגרת קביעתה של קשת הסמכויות של הרשות החוקרת ולא במסגרת קביעתה של 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 שבו הם מיוצגים; **השלישית**, הראיה אינה ניתנת להעתקה, ומכאן שהיא בת־תפיסה בלבד; **הרביעית**, השימוש בראיה תלוי בהחזקתו בפועל באופן פיזי בתוספת שליטה אפקטיבית בו. לעומת אלה 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, החסן נייד (דיסק און קי), תקליטור וכדומה] הוא עניין חסר משמעות והשפעה על תוכן המידע. מכאן שתוכן המידע נפרד מן החפץ הפיזי שעליו

---

88 השוו ל־Kozlovski, לעיל ה״ש 55, בעמ׳ 48–102, שמנה את מאפייני האינטרנט כזירת העברה, ואילו אני מתמקד במאפיינים הרלוונטיים של הראיה הדיגיטלית באינטרנט לצורך פיתוח מערך סמכויות איסוף מתאים לצורכי החקירה ומאוזן מבחינה חוקתית. מדובר אפוא בפרספקטיבה קרובה, אך לא זהה, ומכאן השוני בין המאפיינים. מאפיין הבין־לאומיות, המתואר אצל קוזלובסקי, נדון בפרק ג, העוסק בתפישה הטריטוריאלית באשר לדיני איסוף הראיות הדיגיטליות באינטרנט.

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

nevo.co.il

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 שעליו מוטבע המידע הוא על פי רוב חסר חשיבות, למעט ערכו הכלכלי, שיחסית אינו גבוה.

ב. המידע ניתן להעתקה מלאה: היות 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 ואת החלוקה של הדיסק הקשיח המקורי שהועתק.[91]

---

90 תכונתו זו של המידע הדיגיטלי עוררה את הדיון מתחום זכויות היוצרים סביב "דרישת הקיבוע", שלפיה 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 ולביקורת 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 מועתקים אל דיסק קשיח משטרתי, שמנוקה תחילה לחלוטין. העתקה פורנזית מאפשרת לשמור על המיקום האמתי 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 מכול, 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 שהוא יקר ערך מבחינה פורנזית־חקירתית, וגם יכול להיות יקר ערך לחשוד שינסה לחלץ קובץ מחוק בעל פוטנציאל מזכה. תוכנות המספקות שירות של העתקה פורנזית ומקובלות בשימוש ביחידות 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.
היות 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 באשר להעתק ממוחשב של ראיה דיגיטלית. ראו בהתאמה: פקודת הראיות, סעיפים 35–36, 41ב; הצעת חוק לתיקון פקודת הראיות (תיקון מס' 15) (מקור והעתק כראיה), התשס"ו–2006, ה"ח הממשלה 232 (בשלב זה המשך קידום ההצעה לקראת קריאה שנייה 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**, פ"ד נה(1) 71 (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 שבו 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 בידי צד ג; (ד) כשמדובר בבדיקה של תקליטורים, בדרך כלל היחידה החוקרת תעיין ישירות בתקליטור ולא תשכפל אותו קודם לכן, מתוך הנחה שאי אפשר "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 במגע עם המכשיר המקורי. בית המשפט עשוי להכשיר ממצאי חדירה לחומר מחשב שהתקבלו מחדירה לחומר המחשב המקורי והעתקתו ה"לוגית" בלא ביצוע העתקה פורנזית. ראו ת"פ (מחוזי י-ם) 426/09 **מדינת ישראל נ' אולמרט**, בפס' 858–880 (פורסם בנבו, 10.7.2012).

nevo.co.il

ג. **המידע מנותק פיזית מאת המשתמש בו, הוא מבוזר ומוחזק בידי מתווכים:**[92] המשתמש הקבוע במידע, לדוגמה בעל חשבון הדוא״ל בשירות Webmail, אינו מחזיק את הדוא״ל במחשבו האישי. המידע מוחזק אצל מתווך, במקרה זה ספקית שירותי הדוא״ל. יתר על כן, לא זו בלבד שהמידע מוחזק אצל ספקית השירות, אלא שסך המידע בשימושו של אדם מבוזר על פני מספר רב של ספקיות שירות שונות.

ד. **המידע ניתן לאחזור ולכרייה באמצעים ממוחשבים:** מצד אחד, כאמור, המידע מבוזר במספר רב של מקומות ומוחזק ברשות מספר רב של מתווכים במרחב הסייבר, בעיקר באינטרנט. מצד שני, המידע המבוזר ניתן לאיחוד, למיון ולאחזור לפי שאילתות ממוקדות. זאת בשל תכונת הקישוריות של האינטרנט בתוספת פיתוח יכולות חיפוש ואחזור ״חכמות״. בעקבות זאת ״שובל המידע״ שמותיר כל משתמש מחשב[93] ניתן לאיסוף ולהרכבה 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, תוך ניצול הקישוריות של המרחב המקוון, המאפשרת למזג בין מצבורי המידע השונים. כל אלה מגבירים את הפוטנציאל החקירתי בקשר למידע מחד גיסא, ומגבירים את עצמת הפגיעה 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 סופית אלא עובר לאותו מחסן של תאי זיכרון הניתנים ל״דריסה״ על ידי מידע חדש שיוסף אל המחשב. אולם אם לא ייתוסף מידע חדש למחשב וימלא את מלוא תכולת הדיסק הקשיח במחשב, לא ייעלם המידע ה״מחוק״ מן המחשב.

ז. **המידע פגיע:** המידע הדיגיטלי פגיע לשינויים לא 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 העברה הנחקרת.

ח. **המידע ניתן להצפנה, להסוואה או לטשטוש בנקל:** יכולת ההסוואה, הגנת הססמה, הסתרת זהות מחבר המידע, שולחו או מקבלו הפכו לפעולות פשוטות, ללא עלות, הניתנות

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 בנוהלי 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 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.

nevo.co.il

לביצוע 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 באשר לאיסוף ראיות דיגיטליות במרחב הסייבר. בהמשך הפרק אבחן את השלכותיהן של התכונות שמניתי לעיל על צורכי 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 אלה:[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.

מבחינת החוק הישראלי, החוליה המהווה "חדירה" היא שלב ההעתקה של חומר המחשב המקורי להעתק משטרתי. בשלב זה מתבצעת ההתערבות במחשב התפוס ובחומר המחשב

---

95 אתייחס להצפנת תכנים להלן בפרק ד.ג.3.ז) כשאציג את פעולת האיסוף של חיוב במסירת מפתח הצפנה או ססמת 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 של קֶר, שאבחן 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 היא 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.

nevo.co.il

שבתוכו, או במילותיו של החוק – מתבצעת ה"הפעלה" של המחשב התפוס.[97] כל שאר הפעילות מרגע זה נחשבת לעבודה על גבי העתק ולמעשה אינה עומדת עוד בהגדרה של "חדירה" לחומר מחשב, כיוון שברגע שהועתק חומר המחשב להתקן משטרתי, התפישה היא שהסתיימה ההתערבות בחומר המחשב של המחזיק שממנו הוא נתפס.[98] עם זאת דווקא בשלב זה מתבצעות הפעולות שנתפשות אינטואיטיבית כפוגעניות יותר, לפחות במובנים של פגיעה בזכות לפרטיות ובסוד המסחרי (כשמדובר 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 אין בתי המשפט מקיימים הוראה זו, והצווים מוצאים ביחס לכל חומר המחשב הנמצא במקום ביצוע החיפוש.[100] יתרה מזאת, הנחיית חטיבת החקירות במשטרת ישראל, המדריכה את החוקרים

---

97 המונח "חדירה לחומר מחשב" מוגדר בסעיף 4 לחוק המחשבים, התשנ"ה–1995, שאליו 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, וכל הוראות הטיפול במוצגים מגלמות גישה "חפצית": ניתן להחזיר את התפוס לבעליו או למחזיקו על פי דין (סעיפים 35 ו־37 לפסד"פ), ניתן למכרו אם מדובר במוצג מתכלה (סעיף 38 לפסד"פ), ניתן לחלט את התפוס אם שימש לביצוע עברה (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 שהיא מעתיקה 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 שיהיה בכוחו לפקח אפקטיבית על המשטרה בעניין זה. זאת בשל מגבלות כוח האדם של רשם מאגרי המידע ומיעוט השימוש בסמכויות הפיקוח שלו כלפי רשויות החקירה והביטחון. להרחבה על תחומי הפעילות של רשם מאגרי המידע ועל יכולת האכיפה שלו ראו דוחות הרשות למשפט, טכנולוגיה ומידע, בפרק המתייחס לרשם מאגרי המידע (תפקיד שראש הרשות אוחז בו), מצוי בפורטל ועדת החוקה של הכנסת באתר www.knesset.gov.il/huka. חשש דומה הביע פול אוֹם (Ohm) בנוגע 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) סיפה לפסד"פ.

100 אמירה זו מבוססת על כך שבכל ההחלטות השיפוטיות שבהן נדון עניינו של צו חדירה לחומר מחשב, ואשר היה ניתן ללמוד על נוסח הצו השיפוטי שהסמיך חדירה או קבלה של חומר מחשב, הרי שהצו נוסח בניסוח הגורף ביותר האפשרי. ראו למשל ב"ש (שלום ראשל"צ) 1209/06 **נטוויז'ן בע"מ נ' יאח"ה** (פורסם בנבו, 29.1.2006), שעניינו צו חדירה לחומר מחשב שהוציאה המשטרה במעמד צד אחד ואשר מופנה לחברת נטוויז'ן במסגרת חקירת חשדות לפרסום אתרי הימורים לא חוקיים בפורטל האינטרנט "נענע" אשר היה בבעלות חברת נטוויז'ן. במסגרת חקירתה של עברה 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** (פורסם בנבו, 25.2.2003); ב"ש (שלום אי')

nevo.co.il

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 ביתר בוטות, 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, ואילו שלבי העיון במידע גופו נזנחים – מביע אורין קֶר גם ביחס למשפט האמריקני. קר הביע חשש שבשל נוסחו של התיקון הרביעי לחוקה האמריקנית ובשל ההתייחסות אל החדירה לחומר המחשב כאל חד־שלבי כאמור, עלולה להיווצר תוצאה פרשנית שלפיה רק תפיסתו 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, פיתוח 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 שלפיו 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 צורכי חקירה רבי חשיבות במרחב הממוחשב.

2162/03 **מדינת ישראל נ' כהן** (פורסם בנבו, 26.6.2003); ב"ש (שלום י-ם) 4304/03 **צוקרמן נ' אגף המכס והמע"מ** (פורסם בנבו, 3.4.2003); ב"ש (שלום רמ') 1269/05 **מדינת ישראל נ' מילר** (פורסם בנבו, 14.6.2005); מע' (שלום ת"א) 14132/05 **מדינת ישראל נ' עו"ד שטריים** (פורסם בנבו, 28.9.2005); ב"ש (מחוזי י-ם) 4642/05 **דויטש נ' מדינת ישראל**, פ"מ תשס"ד(1) 440 (2005); ת"פ (שלום י-ם) 1934/05 **מדינת ישראל נ' ואנונו** (פורסם בנבו, 19.2.2006) (דוגמה נדירה למקרה שבו נפסל צו החיפוש בהחלטת ביניים במסגרת ההוכחות, לאחר שבית המשפט מצא שניסוחו של הצו 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** (פורסם בנבו, 14.6.2007); ב"ש (שלום טב') 1528/07 **בוזגלו נ' משטרת ישראל** (פורסם בנבו, 11.2.2007); ת"פ (מחוזי ת"א) 40205/05 **מדינת ישראל נ' ויינשטיין** (פורסם בנבו, 13.6.2007); ב"ש (שלום אי') 1152/08 **מדינת ישראל נ' גיגי** (פורסם בנבו, 10.6.2008); עניין **פטימר**, לעיל ה"ש 76; ת"פ (שלום חי') 1826/08 **מדינת ישראל נ' הלוי** (פורסם בנבו, 2.11.2011).

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 ד.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.

nevo.co.il

3. התפישה הפיזית וצמצומה של 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 באשר לראיות דיגיטליות בחקירה פלילית במרחב הסייבר. 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 באשר לחקירה הפלילית במרחב הסייבר. בהמשך, בעיקר בפרק ה, אעמוד על הפגיעות החוקתיות הגלומות בפעולות אלה, ולאחר מכן, בפרק ו, אציע מודל המגלם בחינה הולמת יותר, הן מההיבט של צורכי החקירה והן מההיבט של הניתוח החוקתי, של נושא איסוף הראיות הדיגיטליות בחקירה פלילית במרחב הסייבר.

א) המצאה עתידית של מידע דיגיטלי

אחת מתכונותיה של הראיה הדיגיטלית, שעליה עמדתי לעיל, היא כי היא מצטברת וניתנת לאגירה. בנוסף, התקשורת המקוונת מתווכת בידי 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 באשר לפעילות חשודה מסוימת. כדוגמה לצורך חקירתי זה, נניח שאתר אינטרנט מסוים חשוד כאתר שמשתמשי אינטרנט מחליפים ביניהם דרכו 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, של פרטי הזיהוי של הגולשים, של התכנים שהעלו או העבירו דרך האתר וכדומה. את הנתונים האלה יוכל להמציא מנהל האתר (כספק שירות מסוג אחד, אם אינו חשוד בעצמו כמספק הפלטפורמה לפעילות החשודה) או מנהל שירותי האחסון 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 היא פעולה של האזנת סתר. אולם בענייננו קיימים כמה אלמנטים המבחינים אותה 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 שטכנית לא הרשות החוקרת מבצעת אותה אלא צד שלישי (להוציא מקרה של המצאה בידי חשוד), הממציא את המידע לפי דרישת הרשות החוקרת. מכאן שגם אם פעולת ההמצאה נעשית שלא בידיעת החשוד, עדיין אין מדובר 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

---

104 פעולות האיסוף שאדון בהן להלן אינן קיימות כיום בדין הישראלי. זאת שלא כקטגוריות המצבים שתיארתי לעיל בפרק ד.ב.2.ג), שבהן קיים כיסוי חוקי עקרוני בדין הישראלי, אולם בשל תבניות החוק הקיים – חדירה, המצאה והאזנה – נוצרים כשלי סיווג מסוימים.

nevo.co.il

קל וחומר, סמכות לביצוע פעולת סתר חלקית, במקום שקמה סמכות לבצע פעולת סתר מלאה, עדיין אי אפשר לקרוא לתוך חוק האזנת סתר פעולה של המצאה במקום פעולה המיועדת להתבצע בידי 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 צורכי 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 לצרכיה שלה או בשל הסכם שלה עם הלקוח, ובשלב מסוים הרשות החוקרת מעוניינת לקבל את המידע האמור. דוגמה לכך היא 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 (לצורכי 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 לצורכי איסוף מידע חקירתי. במקרה כזה הפעולה הנדרשת מספקית השירות היא שמירה (Preservation), ולאחר מכן, לפי הצורך החקירתי, תוכל לפנות בבקשה להמצאת החומר שנשמר. דוגמה לכך יכולה להיות מצב שבו מבוקשת שמירת תכנים בדף אישי של משתמש בפייסבוק או שמירה של תוכני תיבת דוא״ל, לפני שבעל חשבון הפייסבוק / הדוא״ל משנה אותם או מוחק אותם.
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 קבלת

105 ב״ספקית שירות״ כוונתי כאן לספקית מכל סוג שהוא – ספקית גישה, ספקית שירותי אירוח וספקית שירותי אחסון זמני. הבחנה זו לקוחה מהצעת חוק מסחר אלקטרוני, התשס״ח–2008, ה״ח הממשלה 356, וזו מבוססת על ההבחנה 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 ב, בה״ש 184.

nevo.co.il

נתונים מסוג כזה היא לקבוע בחקיקה או בהוראה מחייבת של הרגולטור חובת שמירה כללית, שאינה תלויה בחשד המתעורר במהלך חקירה נתונה, אשר תמנע מצב שבו המידע הדרוש 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 בידי הרשות החוקרת. מבחינה עיונית, חובת ה־Retention, כמו גם חובת היצירה של תשתית טכנולוגית מתאימה לצורכי רשויות האכיפה, שונות במהותן מסמכויות האיסוף האחרות שמניתי עד כה באשר לראיות דיגיטליות – חדירה לחומר מחשב, המצאת חומר מחשב והאזנת סתר לתקשורת בין מחשבים – כיוון שהן אינן תלויות בחשד קונקרטי. מדובר למעשה בחובות כלליות המוטלות בכפייה על ספקי השירות השונים לשמור את המידע ברשותם, כדי שבבוא העת תוכל הרשות החוקרת להפעיל סמכות ולקבל את המידע שהיא מבקשת. דהיינו, הטלת חובת Retention וחובת יצירת תשתית הטכנולוגית הן הפעלה של סמכות איסוף עקיפה, כזו הבונה פוטנציאל איסופי עתידי ואינה 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 שכבר התייחסתי אליה לעיל, ואשר 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.

הוראת שמירת המידע מכוונת בדרך כלל לצד שלישי, ספקית השירות,[107] ומורה לו לשמור את חומר המחשב האגור ברשותו בנוגע לחשוד מסוים. הוראת השמירה נועדה למנוע מצב שבו אלמלא ההוראה המחייבת יימחק המידע העשוי להיות רלוונטי לחקירה או ישתנה. הוראת השמירה, בדומה לצו ההמצאה, מתייחסת לשני "שחקנים" מרכזיים: (1) ספקית השירות הנמענת לצו אשר נדרשת לבצע את הוראת השימור ו־(2) החשוד שבגינו מבוקש שימור הנתונים. מלבד זאת, צבירת המידע מגלמת פגיעה כללית גם בצדדים שלישיים שהתקשרו עם החשוד וכן בציבור משתמשי המחשב בכללותו, אשר תחושת "העין הצופה" עלולה לצנן את פעילותו הלגיטימית. על הפגיעות המגולמות בהוראות השמירה ארחיב להלן בפרק ה. 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

---

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 מאוד.

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, לקביעת בית המשפט באשר לסמכותו להורות על "הקפאת" חשבון בנק מכוחם של סעיפים אלה: בש"פ 5015/99 **התאחדות משפטנים בלתי תלויים נ' מדינת ישראל**, פ"ד

nevo.co.il

לא 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 ואשררו אותה יאפשרו לשמור מידע על פי בקשתה של מדינה אחרת שהיא 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]

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 גופים נוהגים לשמור את הנתונים המבוקשים ברשותם וולונטרית ודרך קבע. כחריגים ניתן לציין את משטר שימור הנתונים המוחל על הבנקים באשר לחלק מהנתונים הבנקאיים[111] ואת משטר ניהול פנקסי החשבונות בשביל רשויות המס המחייבים שמירת נתונים מסוימים להוכחת נכונות הדיווחים של ספקי השירות לרשויות המס.[112] כיוון שהשימור נעשה במרבית המקרים באורח 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 בעתיד ידרשו ממנו 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

נה(1) 657 (1999); ת"פ (מחוזי י-ם) 1071/01 **מדינת ישראל נ' רבינוביץ**, בפס' 8 (פורסם בנבו, 19.9.2010); ה"ת (שלום ת"א) 25797-03-11 **אושרי פ. בע"מ נ' מדינת ישראל** (פורסם בנבו, 2.10.2011).

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.

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"הזכות להימחק" (The right to be forgotten), להלן בפרק ה.ד.1.א).

nevo.co.il

ייאסר בהוראה כופה של המדינה,[115] דומה כי גם כאן תאבד הרשות החוקרת 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 ולאגרו, והוראת השימור מביאה את ספק השירות לאגור את המידע לראשונה. שימור מידע מן הסוג השני קרוב להקלטה יותר משקרוב הוא לשימור, באשר הוא מייצר תיעוד במקום שבו ברגיל לא היה אמור להיווצר 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 וצורכי החקירה, ייתכן בהחלט 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) בנוגע לנתוני 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 משום 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 בשל הפסיקה האמורה. **בארצות הברית**, שבה הוכרה סמכות ה־Preservation, לא הוכרה סמכות להטיל חובות שימור כלליות. ניסיון להכניס חובות

---

115 כדוגמת ההוראות הכופות שנמנו לעיל בה"ש 111–112.

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 היום־יומי 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].

nevo.co.il

שימור כלליות לספקי שירות שונים במסגרת ה־USA PATRIOT Act משנת 2001 – לא צלח. לאחרונה קבע בית משפט פדרלי לערעורים כי חוק ה־PATRIOT אינו מתיר ל־NSA לאסוף נתוני תקשורת (טלפונית ואינטרנטית) איסוף רוחבי, שלא על בסיס חשד קונקרטי וממוקד, אף אם הדבר נעשה למטרות חקירה בענייני טרור ומניעתו.[119] אף לאחר חקיקת חוק ה־PATRIOT נערכו כמה ניסיונות, שלא הושלמו, להטיל חובות שימור כלליות לצורכי חקירה של עברות מין בקטינים באמצעות האינטרנט.[120] כאמור, משטר שימור המידע דרך קבע עורר התנגדויות מהכיוון החוקתי. ארחיב על כך בפרק הבא, שבו אדון בהשלכות הזירה האינטרנטית על השיח החוקתי בקשר לדיני איסוף הראיות בחקירה פלילית.

ד) הוראות ליצירת תשתית המאפשרת לרשות לאסוף ראיות דיגיטליות

הכוונה כאן להוראות המטילות חובה לספק תשתית טכנולוגית לשימוש עתידי קונקרטי בידי הרשות החוקרת. סמכות זו נבדלת מחובת השימור דרך קבע (Retention) בשני המובנים האלה: (א) חובת ה־Retention למעשה כוללת את החובה ליצור תשתית טכנולוגית מתאימה לשימור המידע, אלא שנוסף עליה היא גם כוללת שימוש גורף באותה תשתית טכנולוגית לצורך שימור הנתונים בפועל. בעקבות זאת 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 בידי ספקית השירות. עם זאת בהחלט יש להביא בחשבון את הפגיעה הפוטנציאלית המגולמת בהוראות המחייבות את ספקיות השירות ליצור תשתית טכנולוגית לצורכי הרשות החוקרת – פגיעה זו נוגעת לתחושת המעקב הכללית (פַּן אוֹפּטיקון האינטרנטי) וכן פוגעת בחופש העיסוק ובקניינן של ספקיות השירות; (ב) חובת ה־Retention מטילה נטל ישיר על ספקית השירות, ואילו ההוראות המחייבות יצירתה של תשתית טכנולוגית מניחות כי פעולות שימור המידע והגישה אליו ייעשו בידי הרשות החוקרת עצמה. יש בכך משום ניסיון להקל את הנטל המונח על כתפי ספקית השירות (אם כי גם יצירת תשתית טכנולוגית עלולה לגזול משאבים מהספקית), הגם שאין להתעלם מן העובדה שהטלת חובות

---

119 ראו ACLU v. Clapper, 2015 WL 2097814 (2nd Cir., 2015). בכך פסל בית המשפט הפדרלי לערעורים את הפרקטיקה שלפיה הממשל האמריקני נהג לפרש את סעיף 215 לחוק ה־PATRIOT ככזה המאפשר, הלכה למעשה, שמירת מידע לא תוכני (דהיינו נתוני metadata) על חלק 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, אולם בפועל, דרך סוגיה זו, הוחדרה סוגיה של שימור מידע דרך קבע, המתייחסת לאגירתם של נתוני הגלישה של כל מנוי אצל ספק השירות. ״ספק השירות״ מוגדר בהרחבה, וההגדרה חלה 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.

nevo.co.il

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 לרשויות החקירה האזנת סתר. עם זאת בעידן הסייבר ניתן לומר כי נפתח פער טכנולוגי, ההולך ומתרחב, בין הרשות החוקרת לבין מכלול השירותים והיישומים שהרשת מאפשרת. כמו כן בשל התופעה שלפיה הפעילות במרחב הסייבר, בעיקר באינטרנט, מתווכת לרוב בידי ספקיות שירות שונות, הטלת החובה עליהן לספק תשתית טכנולוגית לשימוש רשויות החקירה מאפשרת דילוג מעל המשוכה 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, והכול 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. במילים אחרות, סמכות איסוף זו קיימת באופן חלקי בלבד במשפט הישראלי. כפי שפירטתי לעיל בפרק ב, **בארצות הברית** קיימת חקיקה משנת 1994 המחייבות ספקיות תקשורת לבנות תשתית טכנולוגית אשר תאפשר לרשויות החקירה ביצוע האזנות סתר.[121] גם **בבריטניה** יש הוראות חוק המתייחסות לסוגיית החיוב של ספקיות תקשורת, ובכללן ספקיות גישה לאינטרנט, לבנות תשתית טכנולוגית שתאפשר לרשויות החקירה האזנת סתר.[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 הוא נזיל, ניתן למחיקה או לשינוי, לעתים אף אוטומטית 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).

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 הסמויה לחומר המחשב והכניסה אליו; **השנייה**, ביצוע העתקה סמויה של חומר מחשב לאחר ביצוע כניסה סמויה כאמור; **השלישית**, עיון בחומר שהועתק העתקה סמויה, מבלי שהחשוד יודע על כך. אלמנט הסֵתֶר מייחד את הסמכות הזאת מסמכות החדירה והתפיסה הרגילות.

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.).

nevo.co.il

הצורך החקירתי המיוחד בפעולה של חדירה סמויה לחומר מחשב והעתקת המידע מתוכו נובע מהיותו של המידע 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 העברה. לכן יש אינטרס מובהק לרשויות החקירה להתקרב עד כמה שניתן למידע בצמוד למועד ביצוע העברה. 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 מחדירה סמויה למחשב. זאת, לעומת המצב בעניינן של ראיות פיזיות, אשר אם לא תופסים אותן פיזית (מה שכמובן אינו אפשרי במהלך חיפוש סמוי, שכן אז תתגלה נוכחות החוקרים במקום), ניתן רק להציג תיעוד משני שלהן (כגון צילום), שאפשר שמהימנותו הראייתית תהיה 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 מעקב סמוי אחר פעולתו של החשוד, על מנת לבחון אם הוא משתף בתכנים גם גולשים אחרים; (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 גנבת המידע בידי החשודים, לכשתאתר אותם ותעצור אותם. חששה של המשטרה הוא כי עד לאיתור החשודים כאמור יימחק המידע האגור בשרת ה־FTP ביזמתם או באופן 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 יש אלמנט הסתרה של פעולת האיסוף מפני החשוד: סמכות לביצוע האזנת סתר לתקשורת בין מחשבים וסמכות לדרוש המצאה בידי 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, ולעומתה החדירה הסמויה לחומר המחשב צופה פני עבר ומתייחסת למידע הקיים. ההשוואה האמורה מלמדת כי אי אפשר לקרוא לתוך סמכות האזנת הסתר לתקשורת בין מחשבים גם סמכות לביצוע חדירה סמויה לחומר

---

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

124 לתיאור עובדות המקרה ראו לעיל פרק ב, בה״ש 98.

מחשב, ועל כן יש לבחון את האפשרות שהמחוקק יכונן הסמכה לפעולה כזאת במפורש.[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 היא חדירה סמויה לחומר המחשב.

אשר להבחנה בין חדירה סמויה למחשב לבין המצאת מידע בלי ידיעת החשוד: המצאה בידי 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, אם ניתנת 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. לעומת זאת סעיף 43 לפסד״פ 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 המשפט, אף על פי 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 בידי צד שלישי ללא יידוע החשוד, מופחת באופן משמעותי החשש להשתלת ראיות. זאת כיוון שאיסוף הראיה בפועל נעשה בידי צד שלישי חיצוני, ואפשר שהוא יְגַבֶּה את פעולת האיסוף

---

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 כמבוקש. בעקבות זאת יידע הבנק הנמען לצו את גיידמאק בדבר פעולת האיסוף שבוצעה בנוגע לחשבונו. על פי הפרסום, גיידמאק הוציא בתגובה 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 באשר לפעולות איסוף של רשויות החקירה האמריקניות המכונות NSL (National Security Letters). מדובר בסמכות לדרוש המצאת נתונים מסוימים במסגרת הוראה מנהלית (של דרג מסוים ברשויות האכיפה, ולא במסגרת צו שיפוטי). סמכות זו הורחבה מאוד 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 בידי ספקיות גישה לאינטרנט שנדרשו להמציא נתונים בדרך זאת. נטען נגד היעדר הביקורת השיפוטית על השימוש בסמכות ה־NSL, על הפגיעה שלה הסמכות הזאת הן בזכויות החשוד והן בזכויות של ספק הגישה הנמען לצו. בעיקר נטען נגד הוראת איסור היידוע הגורפת, ובית המשפט קיבל את הטענות נגד חוקתיות הוראת החוק, לרבות בדבר 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 ונקבע בו 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 כלא חוקתית. ראו Doe v. Gonzales, 449 F. 3d 415 (2nd Cir., 2006).

nevo.co.il

שביצע ברשותו, לשמור לעצמו העתק לצורכי התדיינות עתידית על הפעולה או כדומה. כמו כן אפשר שהצד השלישי הנמען לצו יעורר 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 לחדור חדירה סמויה למחשב, ובלבד שבית המשפט המסמיך יתייחס מפורשות לכך שמדובר בחדירה לחומר מחשב. התפישה, על פי הדין האמריקני, היא 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] יש הבחנה בין חיפוש סמוי לבין תפיסה סמויה, אשר תותר בתנאים מצומצמים עוד יותר. גם העתקה סמויה, שאינה כוללת תפיסה, נחשבת לפעולה 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 ניסוח כללי וגורף בקוד הפלילי הקנדי. החדירה יכולה להיחשב סמויה באורח זמני בלבד, כאשר בית המשפט רשאי להאריך את תקופת ההשהיה של ההודעה לפרקי זמן שונים, שלא יעלו על שלוש 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 ניסוח גורף למדי מבחינת היקף הסמכות לבצע חיפושים סמויים. נקבע כי סמכות החדירה הסמויה למחשב, כפי שנוסחה בחוק, פוגעת פגיעה לא מידתית 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 בשל תכונותיה של הראיה הדיגיטלית כראיה

---

128 כך אירע למשל בעניין נטוויזן, 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 השהיה 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 על יידוע המחזיק על אודות החיפוש בחצריו להיעשות בזמן סביר אך קצר (“a reasonable, but short, time”).

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.

nevo.co.il

נדיפה ופגיעה מצד אחד, אך ניתנת להעתקה (להבדיל ממוצגים חפציים) מצד שני. עם זאת יהיה על הדיון בעצם ההכרה בסמכות איסוף של חדירה לחומר מחשב להתחשב בפגיעות המיוחדות והחריפות המגולמות בסמכות זו, הן ברמה הקונקרטית של החשוד והן ברמה של כלל ציבור משתמשי המחשב.

ו) תיעוד סמוי של הפעילות במחשב הקצה

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 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. יש מצבים שבהם מידע ממוחשב מסוים זורם בתקשורת בין מחשבים, אך משתמש הקצה אינו צופה בו בפועל. כך הוא למשל במקרה שבו משתמש הקצה פותח כמה חלונות בעת ובעונה אחת, 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, אך פעולות אלה לא התבצעו ביזמתו של משתמש הקצה, ולעתים אף לא בידיעתו. כיוון שאפשר שיתעורר 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]

---

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 נטתה הפסיקה לראות בסמכויות ההאזנה כוללות 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

nevo.co.il

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 הססמה. בנוסף, גם צילום מסך המחשב של משתמש הקצה (Screen capturing) לא ישרת את המטרה החקירתית המבוקשת, שכן על פי רוב הקלדת הססמה 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, להסוואה, למחיקה או לשינוי של הראיות הדיגיטליות. ברי כי ככל שתוכר הסמכות לתעד את הפעילות במחשב הקצה תיעוד סמוי, הרי שהכרה כזו משמעה פגיעה רחבה בזכויות מוגנות של החשוד ובכלל ציבור משתמשי המחשב והאינטרנט. על כך ארחיב להלן בפרק ה.ד..

ז) פיצוח הצפנות והתגברות על ססמאות

הצפנות וססמאות הגנה מגלמות סוג של ״עזרה עצמית״ של המשתמש במחשב באמצעות שימוש יזום שלו בטכנולוגיות מגבירות־פרטיות המכונות PETs (Privacy Enhancing Technologies). ההצפנה נועדה להגן על המידע מפני חשיפתו בידי גורמי חוץ; הססמה נועדה לאמת את זהות הגורם הניגש אל המידע. ההצפנה מערבלת את תוכן המידע עצמו, ואילו הססמה חוסמת את הגישה אל המידע, הגם שזה אינו מעורבל.[136] השימוש בהצפנות ובססמאות הפך לנפוץ ומקובל עד מאוד בעידן האינטרנט, ולעתים ספקיות השירות השונות באינטרנט מצפינות

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 שנייה ושלישית). הבחירה לראות בסמכות זו ״סמכות עזר״ מוקשה בעיניי, שכן מדובר בסמכות פוגענית מאוד, שאינה מיועדת לתמוך בסמכות ההאזנה, אלא היא בבחינת כלי חקירה בעל נפקויות ותועלות כשלעצמו.

הצורך החקירתי באשר 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 יהיה ניתן לתעד את דפי האינטרנט שמשתמש הקצה צפה בהם בפועל באמצעות הפניית מצלמת הסתר אל מחשב הקצה, אולם כשמדובר במחשב נייד, יקשה לספק צילום סתר עקבי. יתר על כן, כלי זה אינו מסוגל לחשוף ססמאות שמקליד המשתמש (ולא נראות על צג המחשב בגלוי).

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

nevo.co.il

את חומרי המחשב של המשתמש הפרטי מבלי שהלה נקט פעולה אקטיבית כלשהי.[137] הצפנות טובות למדי ניתנות כיום להורדה חינם דרך האינטרנט,[138] להתקנה ולהפעלה עצמיים גם בידי הדיוטות. הצפנות אלה עלולות לגרום למצב שבו 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 ובססמאות 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 ססמאות הגנה לא נדונה כלל במשפט הישראלי.[140] הדבר נובע מן התפישה הפיזית באשר לראיה הדיגיטלית, אשר על פיה

---

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 ולשימוש 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, ומצד אחר הוא עלול להיות טכנולוגיה הרסנית שתעלה את כוחם של גורמים זדוניים באופן שיהיה בלתי אפשרי 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).

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 שימוש הנאשמים בהצפנות משום גורם המעיד על מסוכנות ועל חשש לסיכול הליכי החקירה והשפיטה בתיק, ולאו דווקא ביטוי לשימוש באמצעים לגיטימיים להגברת פרטיות, במובן של סודיות התקשורת בין אנשים. ראו בש״פ 7368/05 **זלוטובסקי נ׳ מדינת ישראל**, בפס׳ 6 ו־9 (פורסם בנבו, 4.9.2005). השוו ל־ Levie v. State of Minnesota, 695 N.W. 2d 619 (Minn. App., 2005), שם נקבע כי שימוש של נאשם בהצפנות במחשבו יכול להיות ראיה נסיבתית לחובתו במישור של היסוד הנפשי לביצוע העברות.
השני, תפישת משרד הביטחון הישראלי היא שהשימוש בהצפנה יכול להיות כפול־פנים, ועלול לשמש בידי מדינות אויב, גורמי טרור וכדומה לצרכים צבאיים ולמניעת חשיפה בידי כוחות הביטחון הישראליים, ומכאן שכל הצפנה, לרבות הצפנות מסחריות, מחויבת ככלל ברישום ובפיקוח של 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 הללו 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. לעומת זאת בארצות הברית 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 מדובר בדרישה המתאימה לעידן האינטרנט, שבו חלק ניכר מהתקשורת מוצפן אוטומטית, וכל גולשי האינטרנט משתמשים

nevo.co.il

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 ססמאות 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 על הגנת הססמה, תישאל השאלה מה סמכותה של הרשות החוקרת לדרוש מאדם את מפתח ההצפנה או את הססמה, או לחלופין לדרוש מהאדם לספק את המידע השייך לו כשהוא משוחרר מהצפנה או ססמה. המחוקק הישראלי שותק באשר לסוגיות אלה. אם להקיש מן הדינים הקיימים אל סוגיה זו, אציין כי ככל שיתבקש הנחקר למסור, במסגרת עדות, את מפתח ההצפנה או את הססמה, ייתכן שתקום לזכותו באופן ישיר הזכות לאי־הפללה עצמית, אשר חלה על אמרות מפלילות.[142] אם יתבקש הנחקר למסור את חומרי המחשב שלו כשהגנת ההצפנה או הססמה מוסרת מעליהם, וזאת מבלי שימסור לחוקרים את מפתח ההצפנה או את הססמה עצמה, כאן לכאורה אין מדובר 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 הססמה 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 ססמת הגנה בפרק השלישי של ה־Regulation of Investigatory Powers Act (RIPA) משנת 2000, אשר נכנס לתוקף בפועל למן שנת 2007.[145] סירוב לציית לצו המורה למסור מפתח הצפנה הוא עברה פלילית עצמאית, שעונשה בין שנתיים לחמש שנות מאסר (תלוי בסוג העברה המקורית שבגינה נדרש

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 למי שאינם 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 ראוי לציין כי במקרה זה אי־התייחסות המחוקק מלמדת על סמכות גורפת לפיצוח הצפנות ועקיפת ססמאות, 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.

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.).

nevo.co.il

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. במילים אחרות, גם מי שאינו בעל הרשאה חוקית לגשת למידע הממוחשב שבו מדובר, אולם באפשרותו הטכנית להתגבר על הצפנת המידע (כיוון שהוא מכיר את תוכנת ההצפנה או את הססמה לפתיחתה), אפשר שיהיה מושא לצו בית משפט שכזה. העונש על אי־קיום הוראות של צו מעין זה – שישה 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 הדרישה וסבירותה מצד מבצע החיפוש).[148]

בארצות הברית הדבר אינו נקוב בחוק, והפסיקה התחבטה בשאלה אם ניתן להורות לאדם למסור מפתח הצפנה או שמא הדבר פוגע בזכות לאי־הפללה עצמית. בעניין *Boucher* קבע בית המשפט בערכאה הראשונה 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 מדובר 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 משמעו הודאה בכך שהחשוד הוא המשתמש הקבוע במחשב, ובנסיבות שבהן לעובדה זו יש משקל ראייתי נכבד נגד החשוד, הרי עצם ההיענות לצו היא פעולה של הפללה עצמית מכוח הוראה מחייבת. על כל פנים, ראוי לציין כי עצם הסמכות להורות לנחקר לפתוח את ההצפנות ואת הססמאות, בלא שקיימת סמכות לקבל את מפתח ההצפנה או את הססמה 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

146 ראו את עניינו של אוליבר דרייג (Drage), שסירב למסור מפתח הצפנה למחשבו ונשפט בגין עברה 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.).

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 בבית 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).

nevo.co.il

החוקרת. אין לחוקרים דרך לדעת אם הוסתר מהם מידע מסוים. מכאן שאלמנט הבקרה והסנקצייה על הפרה אינם קיימים ביחס לסמכות זו, ולכן מהותה כסמכות מחייבת נפגמת.

דיון מסוג אחר אשר התנהל בארצות הברית עניינו בשאלה אם יש להרחיב את הסמכות לכך שספקיות שירות שונות במרחב הסייבר תחויבנה לבנות "דלת אחורית" (Backdoor) לשימוש רשויות החקירה באופן שיתאפשר לפצח את כל ההצפנות שבהן נעשה שימוש בידי הגולשים לשירות.[152] 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 לחייב את הנחקר למסור את מפתח ההצפנה / הססמה. מבחינה סיווגית, הדיון בסוגיית "הדלת 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 אחריו של הרשויות.

לסיכום נקודה זו, אחד ממאפייניו של המידע הדיגיטלי במרחב הסייבר הוא כי ניתן להצפינו או להגן עליו בססמה בנקל. בדין הישראלי המסדיר את סמכויות האיסוף אין כל התייחסות להצפנת מידע דיגיטלי או להגנתו בססמה, 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 ססמאות נעשית בשלב העיון במידע, הרי שהחוק נעדר התייחסות לכך ומביא אפוא להחמצת הדיון הנכון בצורכי 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 מראיות במרחב הפיזי. טבלה 4.4 מסכמת את החלק

---

152 לכתיבה מוקדמת על סמכות ליצירת "דלת אחורית" לשימוש 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. ודוק, 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 לפי הוראות צו הצופן (בין בזדון ובין מחוסר ידיעה או בתום לב), ובכל זאת נעשה בה שימוש. בהקשר של הפעלת סמכויות ביטחון פורסם לאחרונה, כחלק מפרשת אדוארד סנאודן, עובד ה־NSA אשר הדליף מידע רגיש שנחשף אליו במסגרת עבודתו, כי ספקיות שירות גדולות, כגון מיקרוסופט, יצרו תשתית טכנולוגית בשביל ה־NSA, אשר תאפשר לה לנטר תעבורת רשת כשהיא לא מוצפנת. ראו Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, THE NEW YORK TIMES (5.9.2013) http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&_r=0.

153 ראו לעיל בפרק ד.ג.3.ד).

nevo.co.il

הזה ומציגה את הצרכים החקירתיים החסרים בחקירה הפלילית במרחב הסייבר בשל התפישה הפיזית וכן את המאפיינים הייחודיים של הראיות הדיגיטליות במרחב הסייבר המנביטים אותם. יודגש, שוב, כי בשלב זה של הדיון הצגת פעולות האיסוף נעשתה בהתייחס לצורכי החקירה במרחב הסייבר ובהתעלמות מתודית מהדיון החוקתי המאזן:

טבלה 4.4 — מיון פעולות איסוף הראיות החסרות בשל התפישה הפיזית

<table>
<tr><th>פעולות האיסוף</th><th>המאפיינים הייחודיים של הראיה הדיגיטלית במרחב הסייבר</th></tr>
<tr><td>המצאה עתידית של חומר מחשב</td><td>1. המידע מנותק פיזית מהמשתמש בו ומוחזק בידי מתווכים
2. המידע מצטבר וניתן לאגירה</td></tr>
<tr><td>הוראות שמירה מכאן ולהבא (Preservation)</td><td rowspan="2">1. המידע מנותק פיזית מהמשתמש בו ומוחזק בידי 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. אשר לשימור דרך קבע בלבד — המידע ניתן לאחזור ולמיון באמצעים ממוחשבים (לכן קיים ערך חקירתי רב במיצוי ראיות מתוך "בְרֵכת" המידע הענקית הנוצרת משימור דרך קבע, ללא חשד ספציפי)</td></tr>
<tr><td>הוראות שימור דרך קבע (Retention)</td></tr>
<tr><td>יצירת תשתית המאפשרת לרשות לאסוף ראיות דיגיטליות</td><td>1. המידע מנותק פיזית מהמשתמש בו ומוחזק בידי מתווכים (לכן יש לרשות החוקרת עניין בהטלת חובה על ספקי השירות לייצר את התשתית האמורה)
2. המידע נדיף
3. המידע פגיע</td></tr>
<tr><td>חדירה סמויה לחומר מחשב מרחוק והעתקת המידע ממנו</td><td>1. המידע מיוצג בביטים — תוכן המידע נפרד מן החפץ הפיזי שעליו 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)</td></tr>
<tr><td>תיעוד סמוי של הפעילות במחשב הקצה</td><td>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 שעליו הוא מוטבע
3. המידע ניתן להצפנה, להסוואה או לטשטוש</td></tr>
<tr><td>התגברות על הצפנות ועל הגנת ססמאות</td><td>1. המידע ניתן להצפנה, להסוואה או לטשטוש</td></tr>
</table>

nevo.co.il

ד. התפישה הפיזית והצעת חוק החיפוש

בפרק זה הצבעתי על התפישה הפיזית החולשת כיום על דיני איסוף הראיות במרחב הסייבר ומניתי פעולות איסוף ראיות דיגיטליות אשר לכאורה ניתן להציען במסגרת גישה המשוחררת מכבלי ה״פיזיות״. הצעת חוק החיפוש מבקשת לצעוד שלב אחד קדימה בכיוון של השתחררות מהתפישה הפיזית באשר לסמכויות איסוף הראיות בחקירה פלילית. אמנה את ההוראות בהצעת החוק המגלמות ״תפישה דיגיטלית״ באשר לקביעת סמכויות איסוף הראיות. איני מונה את כלל ההוראות שבהצעת החוק באשר 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 לעברה 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 **לצו שמירה עתידי ולצו המצאה עתידי**. על פי סעיף 74(ב) להצעת החוק, תהיה לבית המשפט הסמכות להורות על שמירה עתידית לתשעים יום, ממועד מתן צו השמירה, של חומר מחשב הקשור לעברה. מובן שלאחר השמירה העתידית כאמור יוכל בית המשפט להורות על המצאת המידע שנאגר בדרך זו. על פי סעיף 73(ב) להצעת החוק יכול בית המשפט להורות על המצאה עתידית של חומר מחשב הקשור לעברה, שיגיע לידי הנמען לצו, וזאת תוך שלושים יום מיום הוצאת הצו.[154] סמכויות אלה מסדירות במפורש 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 **לחדירה סמויה לחומר מחשב** (סעיף 91 להצעת החוק). סמכות החדירה הסמויה מושווית לסמכות האזנת סתר, ומוחלות עליה הוראות פרקים ג ו־ד 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**

---

154 הוראת ההמצאה העתידית מוגבלת למצבים שבהם ״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) עם סעיף 5(א) להצעת חוק החיפוש. לעומת זאת באשר להוראת השמירה העתידית הדרישה היא ל״חשד סביר... שעומדת להיעבר עבירה״. ראו סעיף 74(א) 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 **נטוויז׳ן**, 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.

nevo.co.il

ואף **ניטור סמוי של הפעילות במחשב הקצה** (על דרך של "הקלטה", מתוך המחשב הנחדר, של מסך המחשב של יעד הניטור). זאת אף שמנוסח הצעת החוק ומדברי ההסבר לה קשה להסיק כוונה מפורשת להכליל סמכות זו. סמכות החדירה הסמויה לחומר המחשב, לרבות העתקה סמויה ותיעוד סמוי של הפעילות במחשב הנחדר, מוגבלים בזמן, על פי משך הזמן שבו יעמוד הצו בתוקף (שלושים יום מעת מתן הצו או פרק זמן אחר, כפי שיקבע בית המשפט).[158]

4. **הצעת חוק החיפוש מבקשת להכריע בסוגיית הצווים לקבלת תקשורת א־סינכרונית.** נושא ההתמודדות עם תקשורת א־סינכרונית זוכה להתייחסות מעט מסורבלת בהצעת החוק, אך נדמה כי הסרבול מתחייב גם ממורכבות הסוגיה. **ראשית לכול** קובעת הצעת החוק, בסעיף 77(ב)(1), כי צו להמצאה או לשמירה של תוכן ממוחשב יינתן אם קיים חשד סביר שנעברה עברה מסוג פשע או כל עברה שאינה פשע, אם קיימת הסתברות גבוהה שתיעבר עברה כאמור, או אם קיים חשד סביר שעומדת להיעבר עברה 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 בה האזנת סתר. מן הלאו ניתן לשמוע את ההן: כאשר פונה הרשות החוקרת אל ספק שירות המספק שירותי אחסון מידע לצד שירותי העברת מידע, לא יחולו הוראות חוק האזנת סתר. במקרה של תקשורת א־סינכרונית, כדוגמת דוא"ל, הרי שספק השירות, לצד העברת המידע מהשולח אל המקבל ולהפך, 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 בעקיפין את חוק האזנת סתר באופן שדרישת הבו־זמניות[159] תוכנס לגדר הגדרת "האזנה" בסעיף 1 לחוק. במילים 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 האזנת סתר, כיוון שאינה מתבצעת בו־זמנית עם התרחשות השיחה.[160]

5. **סעיף 95 להצעת חוק החיפוש מקנה סמכות לחייב מסירה של מפתח הצפנה או ססמה.** זאת על פי בקשה שיגיש לבית המשפט האחראי על החקירה במקרה של עברה מסוג פשע או עברה אחרת על פי חוק המחשבים, וככל שהצורך החקירתי גובר על הפגיעה בבעל הגישה לחומר המחשב, הכרוכה בחיובו למסור את מפתח ההצפנה או את הססמה. הבקשה תוגש כאשר אין דרך סבירה אחרת להשגת המידע המבוקש. סירוב לציית לצו ייחשב להפרת הוראה חוקית,

---

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 כמה הוראות ייחודיות בנוגע לפניות אל ספק שירות, ובכלל זה לצורך קבלת תקשורת א־סינכרונית. כך, קובעת הצעת החוק, כי במתן צו לספק שירות על בית המשפט לשקול את השאלה אם 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".

nevo.co.il

לפי סעיף 287 לחוק העונשין, וכן ישמש חיזוק לראיות התביעה, לפי סעיף 95(ג) להצעת החוק. על פי התפישה של הצעת חוק החיפוש, בכוחו של צו למסירת מפתח הצפנה או ססמה יש כדי להתגבר על טענה לחיסיון מפני הפללה עצמית, שכן הסמכות לקבלת המידע כבר הייתה נתונה בידי הרשות החוקרת, ואין לראות בהגנת הססמה 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 הססמה יש בה, כשלעצמה, כדי להפליל (למשל, אם זירת המחלוקת היא בנוגע לזיקה של החשוד למחשב המוגן בססמה, ומסירת הססמה תסגיר כי החשוד הוא המחזיק במחשב).[161]

בסיכומו של דבר, הצעת חוק החיפוש אכן מקדמת מאוד את ההתייחסות הייחודית אל הראיות הדיגיטליות כמובחנות מהראיות הפיזיות. בכך היא תורמת לניפוץ התפישה הפיזית באשר לאיסוף ראיות דיגיטליות. יש לשים לב כי פעולות איסוף שונות, שעליהן 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 המשליכה על דיני איסוף הראיות בחקירה פלילית: מחד גיסא חסרות סמכויות איסוף של המדינה המתאימות לראיות הדיגיטליות במרחב הסייבר, ומאידך גיסא השיח החוקתי המתאים ביחס להפעלת סמכותה של המדינה בחקירה פלילית במרחב הסייבר – חסר אף הוא. בפרק זה עמדתי על החסר בסמכויות האיסוף בשל התפישה הפיזית, ואילו בפרק הבא אעמוד על החסר בדיון החוקתי המאזן.

התפישה הפיזית, שעליה עמדתי בפרק זה, מצטרפת אל התפישה הטריטוריאלית, שלה 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 ו להלן.

---

161 ראו דברי ההסבר לסעיף 95 להצעת חוק החיפוש.

נבו nevo.co.il