חדירה למערכות מחשב – היקפה הרצוי והמצוי של העברה

שרון אהרוני־גולדנברג*

א. מבוא

ב. היבטים תאורטיים של חדירה למערכות מחשב

1. הפונקציות של מערכות מחשבים
2. תיאור תופעת המחשוב הפולשני ומאפייניה
3. נזקי תופעת המחשוב הפולשני
   - 3.1 פגיעה בשיקולים תועלתניים
   - 3.2 פגיעה בחירויות אדם
4. הסייגים להגנת הסודיות במערכות מחשבים
   - 4.1 צידוקים לחדירה שלטונית למערכות מחשב: מניעת פשיעה ושמירת הסדר החברתי
   - 4.2 צידוקים אזרחיים לחדירה פרטית למערכות מחשב
5. החלק התאורטי – לסיום

ג. חדירה למחשב אל מול האזנת סתר – הדין הקיים

1. הדמיון והשוני בין חוק המחשבים לבין חוק האזנת סתר
   - 1.1 אי־תחולה מקבילה: הסיפה לסעיף 4 לחוק המחשבים
   - 1.2 אי־תחולה מקבילה: הוראות החיפוש השונות בשני החוקים
2. קו הגבול בין חדירה למחשב לבין האזנת סתר – הדין הקיים
   - 2.1 שלב הטיוטה – יירוט המידע הנמצא במחשב
     - 2.1.1 יירוט המידע הנמצא במחשב: תחולת עברת החדירה למחשב
     - 2.12 יירוט המידע הנמצא במחשב: אי־תחולת העברה של האזנת סתר
   - 2.2 שלב המעבר של המידע בקווי תקשורת: עברת האזנת סתר
   - 2.3 קליטת מידע הנמצא בתחנות הביניים בדרכו למחשב היעד
     - 2.3.1 קליטת מידע הנמצא בשרת של ספק שירות האינטרנט
       - 2.3.1.1 חדירה למחשב של ספק שירות אינטרנט: אי־

---

* מרצה למשפטים באוניברסיטת בר אילן.
ברצוני להודות לפרופ׳ אמיר הרצברג, לעו״ד עדנה נוימן, לד״ר יעל וילצ׳ק־אביעד וללירון שיו על הערותיהם המועילות.

תחולה לכאורית של חוק האזנת סתר
2.3.1.2 חדירה למחשב של ספק שירות אינטרנט: תחולת עברת האזנת סתר
2.3.2 יירוט מידע הנמצא בדואר מבוסס רשת (Web Mail) וטרם נמשך
2.3.3 יירוט הודעה שהושארה ב"קולן" וטרם נמשכה
2.4 יירוט מידע ממחשב הנמצא בהליך קבלת מסר בזק (On Line)
2.5 יירוט המידע לאחר קבלתו במחשב היעד
2.6 קו הגבול בין חוק המחשבים לבין האזנת סתר – סיכום
3. היתרים לחדירה למחשב – הדין הקיים
3.1 חיפוש במערכות מחשב: הדין הקיים
3.2 צידוקים אזרחיים לחדירה פרטית למחשב – הדין הקיים
ד. חדירה שלטונית ופרטית למחשבים: סיכום ומסקנות

א. מבוא

עידן המחשב פתח בִּפני בָּנֶיהָ של החברה המודרנית צוהר לאפשרויות אדירות של קִדמה טכנולוגית ופיתוח אישי. המחשב הפך לעמוד התווך של החברה המודרנית, המנתב במידה רבה את חייהם של אזרחי המודרְנה. עם זאת, מערכות מחשבים משמשות גם אבן שואבת לגורמים לא קרואים, החודרים אליהן ומיירטים תקשורת בין מחשבים. הסגת גבול זו מבוצעת הן על ידי גורמים שלטוניים, מטעמי הגנה על ביטחון המדינה ועל השלום, והן על ידי גורמים פרטיים, המונעים ממגוון מניעים: "האקרים" (פַּצְחָנים), המעוניינים לפתח את כישורי המחשב שלהם או להתריע מפני פרצות אבטחה;[1] תאגידים מסחריים – במסגרת ריגול תעשייתי;[2] גורמי פשע,

1 האקרים רבים טוענים, כי ההצדקה לפועלם היא עקרון פתיחות ונגישות המידע לציבור או הרצון להתריע על פרצות אבטחה ברשתות מחשבים, ראו למשל, ת"פ (שלום ת"א) 6681/02 **מדינת ישראל נ' להט**, תק־של 03(3) 17300 (2003). אך בפועל מוכח כי יש שהם פורצים למערכות מחשבים בחיפוש אחר הנאה, הגשמה עצמית וידע במחשבים או מתוך נקמה אישית, ראו Orly Turgeman-Goldschmidt, *Hackers' Accounts: Hacking as a Social Entertainment*, 23(1) SOC. SCI. COMP. REV. 8, 18 (2005). גם הרצון לחסוך כסף מהווה מניע, בייחוד ל־Phreackers, אנשים הפורצים למערכות טלפוניה ממוחשבות כדי לחסוך בעלות השיחות. ראו ת"פ (מחוזי ת"א) 40250/99 **מדינת ישראל נ' בדיר**, תק־מח 01(3) 1793 (2001) (להלן: פרשת **בדיר**). יש מקרים שבהם החדירה למחשב נעשית כדי לדלות מידע אישי על הזולת ע"פ (מחוזי ת"א) 71227/01 **מדינת ישראל נ' טננבאום**, תק־מח 02(2) 1540 (2002) (להלן: עניין **טננבאום**).

2 ראו ת"פ (מחוזי ת"א) 40061/06 **מדינת ישראל נ' האפרתי**, תק־מח 06(1) 9608 (2006) (להלן:

שמטרתם – גנבת משאבים כלכליים;[3] עובדים,[4] מעבידים או סתם אנשים הפועלים מתוך שעמום וסקרנות.[5,6] קליטה בסתר של תקשורת בין מחשבים וחדירה למחשב או למערכות מחשב מאפשרות איסוף מידע מהמערכת ומהוות לעתים שלב ראשוני לפגיעה במערכות מחשבים, למשל על ידי שיבוש המידע הממוחשב באמצעות תכנות זדוניות.[7] את מכלול עברות המחשב ניתן לכנות בשם "תופעת המחשוב הפולשני", אך לצורך הגיוון הלשוני, לעתים אכנה בשם כולל זה גם חדירה למערכות מחשב.

תלותה של החברה המודרנית במערכות מחשוב ופגיעתם הקשה של החודרים אליהן מצריכות התייחסות משפטית מעמיקה בנוגע להשלכות הנורמטיביות והמעשיות של חדירה אסורה למחשבים. מטרתו של מאמר זה הנה לבחון מהו גְדֵרה הראוי של עברת החדירה למחשב, ולנתח את הדין הקיים בנושא. התזה המובעת בחיבור הנה ליברטריאנית בעיקרה, והיא באה ליצור פלטפורמה משפטית אשר תגן על ערך סודיות המידע הממוחשב. עם זאת, לתפיסתי, יש מקום לסייג את איסור החדירה למחשב, ובמקרים מסוימים, על הדין לאפשר חדירה למחשב, הן לגורמים אזרחיים והן לגורמים שלטוניים במסגרת דיני חיפוש מבוקרים.

"פרשת הסוס הטרויאני" או פרשת **האפרתי**) שם היה מדובר בהחדרת תוכנת ריגול שהוסוותה במידע ממוחשב לגיטימי, למחשבים. התכנה אפשרה "לצלם" את המידע שהיה במחשב הנחדר. קיימות גם תכנות מעקב המוחדרות למחשבי הגולשים באתרים. ה"קוקיס", למשל, מאפשרים מעקב אחרי נתוני הגלישה של הגולש ותקשורת עם האתר שהחדיר אותם: ה־"Spyware" (רוגלות) סורקות את מחשב הגולש ומעבירות ממנו מידע לגופי פרסום.

3 פגיעה זו במערכות מחשבים עלולה להיעשות מתוך המערכת עצמה, כגון בת"פ (מחוזי ת"א) 40182/02 **מדינת ישראל נ' אלון**, תק־מח 2003(1) 3160, 3215 (2003) (להלן: ענין **אלון**) או על ידי גורם חיצוני – כמו במקרים של *Phishing* – דואר אלקטרוני המסווה כדואר מגוף ידוע, שמטרתו לפתות את הגולש למסור את פרטיו האישיים.

4 מחקרים מוכיחים כי 75% מהפריצות למחשבים ארגוניים בוצעו בידי עובדי הארגון. ראו א' דורון "שוטרים וגנבים" **מעריב –עסקים און ליין**, 19.12.1999. נתונים אלו מתאמתים גם לנוכח העובדות העולות מפסקי הדין העוסקים בנושא. ראו: ת"פ 12360/97 (תל אביב) **מדינת ישראל נ' שפירא**, דינים שלום יח 863 (1998) (להלן: עניין **שפירא**); ת"פ 5177/99 **מדינת ישראל נ' גרינברג**, דינים מחוזי לב(9) 393 (2000) (להלן: ענין **גרינברג**); ת"פ 8243/97 (שלום חי') **מדינת ישראל נ' פז**, תק־של (1) 479 (1998); ת"פ (שלום י־ם) 3813/99 **מדינת ישראל נ' רפאלי**, דינים שלום טז 862 (2000) (להלן: עניין **רפאלי**); ע"פ (מחוזי ת"א) 71103/01 **רום נ' מדינת ישראל**, תק־מח 2003(2) 9297 (2003); ת"פ (מחוזי י־ם) 1256/01 **מדינת ישראל נ' צדוק**, תק־מח 2002(3) 15231 (2002); ענין **אלון**, לעיל ה"ש 3.

5 ראו עניין **שפירא**, שם.

6 Shah מציינת, כי לעתים יש שיתוף פעולה בין האקרים אזרחיים, לבין רשויות השלטון לצורך איסוף ראיות על פושעים, ראו: Monica R. Shah, *The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace*, 105 COLUM. L. REV. 250 (2005).

7 "קראקרים" – פרצנים – פורצים למערכות מחשבים במטרה לשבשם, לרוב לצורך ונדליזם כשלעצמו.

בחלקו הראשון של המאמר יידונו ההיבטים התאורטיים של סוגיית החדירה למערכות מחשב. במסגרת זו תנותח הפגיעה באינטרסים ובחירויות האדם שנוצרת בעקבות חדירה למערכות מחשב, וייערך דיון בסייגים להגנת המידע הממוחשב – בצורך להתיר חדירה למערכות מחשב מסיבות שלטוניות ומסיבות של **עזרה עצמית**. בחלקו השני של החיבור ייבחן הדין הקיים בנוגע לאיסור חדירה למחשב והאזנת סתר לתקשורת בין מחשבים, לרבות הסייגים להגנת סודיות המידע הממוחשב וייושמו הוראות סעיף 4 לחוק המחשבים, התשנ"ה–1995 וסעיף 2(א) לחוק האזנת סתר, התשל"ט–1979 על סיטואציות שונות של מחשוב פולשני. כן יוסבר מדוע, בניגוד לפסיקת בתי המשפט, לא ניתן להרשיע **במקביל** בשני הסעיפים, וייעשה ניסיון לפתור את השאלה הפתוחה שהותיר בית המשפט העליון בערעור על פרשת **בדיר**[8] ב"צריך עיון": מתי חדירה למערכות מחשב מסוימות תהווה עברה על סעיף 4 לחוק המחשבים ומתי היא תהווה עברה על סעיף 2 לחוק האזנת סתר? אציין כי להכרעה בשאלה זו יש השלכות נורמטיביות ומעשיות רבות, שכן הקריטריונים של חוק האזנת סתר מספקים ענישה מחמירה יותר ואף בקרה שיפוטית יעילה יותר על החיפוש השלטוני, לעומת אלו הקבועות בחוק המחשבים ובפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969 (להלן: "הפסד"פ" או "הפקודה").

ב. היבטים תאורטיים של חדירה למערכות מחשב

בבואנו לסקור את היבטיה הנורמטיביים של סוגיית החדירה למערכות מחשב, נשאלת השאלה מהו הדין הראוי בנוגע לתופעת המחשוב הפולשני: האם יש להגן מפני חדירה **למידע ממוחשב** או שמא מפני חדירה **למחשב**? מהו סוג המידע הממוחשב שעליו ראוי לפרוש את הגנת החוק? מהו קו הגבול הווירטואלי המסמן את הטריטוריה הממוחשבת, ושהסגתו תהווה עברה? בניסיון לענות על שאלות אלו, ייבחנו בחלק זה של המאמר הפונקציות שממלאות מערכות המחשבים; תיסקר תופעת המחשוב הפולשני, ככל שהיא נוגעת לחדירה למחשב ולהאזנת סתר לתקשורת בין מחשבים; ינותחו הנזקים שתופעת המחשוב הפולשני גורמת להם; יותוו היסודות העיקריים הראויים של עברת הסגת גבול למערכות מחשב; ויידונו הסייגים להגנת סודיות המידע הממוחשב בהקשר האזרחי והשלטוני.

1. הפונקציות של מערכות מחשבים

פיתוחו של הקולוסוס, אב הטיפוס של המחשב האלקטרוני המודרני, עם סיומה של

---

8 ע"פ 10343/01 **בדיר נ' מדינת ישראל**, תק־על 2003(2) 649 (2003) (להלן: ערעור **בדיר**).

מלחמת העולם השנייה,[9] שימש אבן היסוד של עידן חדש – עידן המחשב. ואכן, מערכות מחשבים הפכו לחלק מהותי מהחיים המודרניים, הן עבור המשתמש הפרטי והן במגזר העסקי והציבורי. ציוני דרך נוספים בכינונה של מהפכת המחשבים היו פיתוחה ב־1969 של רשת המחשבים, ה־ARPANet, כחלק מניסיון של משרד ההגנה האמריקני להגן על מידע ממוחשב מפני התקפה גרעינית;[10] והמצאת טכנולוגיית ה־World Wide Web על ידי Tim Berners-Lee. כך פתחה רשת האינטרנט (מִרְשֶׁתֶת) את שעריה, לא רק בפני אנשי צבא ואקדמיה, אלא גם בפני הציבור הרחב.[11]

מהו המחשב ומה תפקידו? ניתן לאמץ **הגדרה פונקציונלית של מחשב**, בהתאם לפעולות שהוא מבצע. מערכות המחשבים המודרניות כבר אינן מוגבלות לתפקיד של מכונת חישוב מתקדמת; יש להן תפקידים שונים ומגוונים בחברה המודרנית, וניתן לעמוד על חמש פונקציות חיוניות ועיקריות, הקשורות זו לזו, שהן ממלאות: במערכות מחשב מאוחסנים מאגרי מידע עצומים בנושאים שונים, כך שהן מהוות **כלי אחסון** ראשון במעלה של מידע; מעין מחסן המכיל את מצבור הידע, החכמה והרעיונות של הכלל והפרט בחברה המודרנית. המחשב אף מהווה **כלי חישוב** אריתמטי, הנדסי, כלכלי, פיזיקלי ועוד; באמצעותו מתאפשרות פעולות חישוביות מורכבות, במהירות גבוהה ובדייקנות מרבית. כמו כן, המחשב משמש **כלי בקרה ושליטה במערכות**, המסייע בניהול גופים ובתיקון מחשבים ובשדרוגם ממרחק. קשה להתעלם גם **מתפקידו החברתי־בידורי** של המחשב, המאפשר חשיפה למוזיקה, לסרטים, למשחקים ולהימורים, מעין טלוויזיה ורדיו אינטראקטיביים, ומשמש עבור רבים גם כרשת חברתית.[12]

מערכות מחשבים אף מהוות **כלי תקשורת**. די בקו תקשורת כדי ליצור באמצעות המחשב תקשורת בפריסה עולמית, ולהעביר ולקבל מידע במהירות, בזול ולכמות עצומה של מכותבים. להיותו של האינטרנט כלי תקשורת, שני פנים: הפן האחד נוגע לכך שהמחשב מהווה **כלי לאיתור מידע**, המאפשר היחשפות למגוון יצירות

---

9 סיימון סינג **המשפט האחרון של פרמה – החידה ששיגעה את המוחות המבריקים ביותר בעולם במשך 358 שנים** 205 (עודד שכטר מתרגם, 1997).

10 Dorothy E. Denning & Peter J. Denning, *The Internet after Thirty Years*, *in* INTERNET BESIEGED: COUNTERINGING CYBERSPACE SCOFFLAWS 75 (Dorothy E. Denning & Peter J. Denning eds., 1998).

11 אסתר דייסון **מהדורה 2.0 – תכנית מתאר לחיים בעידן הדיגיטלי** 35 (גרוסלרנר מתרגמת, 1998).

12 ראו: דייסון, שם, בעמ' 10. המחברת מתייחסת אל הרשת "כאל בית במובן הרגשי של המילה"; Richard C. Mackinnon, *Punishing the Persona: Correctional Strategies for the Virtual Offender*, *in* VIRTUAL CULTURE: IDENTITY & COMMUNICATION IN CYBERSOCIETY 206 (Steven G. Jones ed., 1997): "Cybersociety is the emergence of community from a complex set of social formations in a space enacted by mediating technology". בנוסף ראו: INTERNET BESIEGED, לעיל ה"ש 10, בעמ' 11, 15.

ספרותיות, למחקרים מדעיים, לפרסומות ולנושאים מגוונים אחרים, והכול בעיקר באמצעות אתרי האינטרנט. היבט זה מסייע להרחיב אופקים, לצמצם פערים חברתיים ולקדם את החברה. הפן השני נוגע להיותו של האינטרנט **כלי ביטוי המוני**,[13] בעל פלטפורמות מגוונות: דואר אלקטרוני (להלן: גם "מייל" או "אימייל") לתקשורת אישית ומקצועית[14] ולרשימות תפוצה המוניות; צ'אטים וקבוצות דיון; ואתרי יומן אישיים (Blogs). כך מועמדת במה להבעת דעות ולביטוי, אשר במידה רבה הנה בלתי מצונזרת או מוסדרת.[15] לפן זה יש חשיבות חברתית כבירה הנובעת מגיוון הדעות המובעות באמצעות מערכות המחשבים.[16]

יתרונותיהן של פונקציות אלו של מערכות מחשבים נובעות גם מהיותן זולות – בלתי תלויות במשאב יקר – הנייר; קומפקטיות – אחסון רב במקום מצומצם; ויעילות – מאפשרות עיבוד, העתקה וניוד. סקירת חמש הפונקציות שממלא המחשב (כלי אחסון של מידע, כלי חישוב, כלי שליטה ובקרה, כלי חברתי־בידורי וכלי תקשורת) מעלה, כי למחשב תפקיד חיוני, הן בהיבט האישי והן בהיבט החברתי. ואמנם, מהפן האישי, תפקידו של המחשב, ובמיוחד המחשב האישי (Personal Computer – PC), הנו כל כך משמעותי, עד שניתן לומר כי הוא מהווה **קניין מכונן של הפרט וחלק בלתי נפרד מאישיותו של האדם**.[17] מההיבט החברתי – הכוללני יותר, ניתן לומר כי המחשב מאפשר את ההתפתחות המדעית והתרבותית של החברה

---

13 ראו Reno v. American Civil Liberties Union, 521 U.S. 844 (1997), שם נקבע, כי האינטרנט הוא אמצעי התקשורת ההמוני ביותר שאי־פעם היה קיים.

14 לחשיבות המחשב ככלי עבודה מרכזי, שבו משתמש כיום עורך הדין על מנת להעביר מידע ומסמכים ללקוחות, ראו: ב"ש (מחוזי ת"א) **093341/06 מדינת ישראל נ' היינץ**, תק־מח 07(3) **12846 (2007)** (להלן: **פרשת היינץ**).

15 ראו ניבה אלקין־קורן "המתווכים החדשים "בכיכר השוק הוירטואלית" **משפט וממשל** ו 381, 385 **(2001)**; עניין *Reno*, לעיל ה"ש 13; תב"מ **16/01 סיעת ש"ס נ' ח"כ אופיר פינס־פז**, פ"ד נה(3) 159 **(2001)**.

16 Y. Amichai-Hamburger, *Internet and Personality*, 18 COMPUTERS IN HUMAN BEHAVIOR 1 (2002), מציין, כי השיח המקוון מהווה מקור לתיווך חברתי וזירה הפועלת למיתון מתחים הטבועים בחברה.

17 ראו עמדתה של פרופ' Radin, ולפיה ישנם קניינים שהם כל כך משמעותיים (למשל, דירת מגורים) עד כי הם מהווים חלק מאישיותו של היחיד, Margaret J. Radin, *Property and Personhood*, 34 STAN.BL. REV. 957 (1982). כן ראו חנוך דגן **קנין על פרשת דרכים** 38, 40 **(2005)**: "הקשר שלנו למשאבינו מוסבר (ומוצדק) במידה שהם משקפים בה את זהותנו. המשאבים שלנו יכולים להיות שיקוף של העבר וההווה שלנו; גילויים חיצוניים של אישיותנו [...] ככל שמשאב אכן מבטא את זהות בעליו – [...], ככל שקיימת זיקה כזו של השתקפות ה'אני' במשאב – כן אנשים נקשרים למשאבים שבבעלותם, ולפיכך חשים פגיעה אישית, ולא רק גירעון חומרי, כאשר משאבים המשקפים כך את זהותם ניטלים מהם". במהלך כנס ("Victimology and the Law", אוניברסיטת בר־אילן, **9.5.2007**), טבע הפסיכיאטר פרופ' סילפן את הביטוי שלפיו המחשב הנו אקסטנציה של המוח האנושי.

המודרנית; הוא מוביל לחיסכון בזמן תפעול ובעלויות, וכך מתאפשרים הגברת הפיתוח, הכלכלה והסחר העולמיים; מערכות תקשורת ממוחשבות אף משמשות אמצעי לגיוון הדעות המושמעות בחברה הדמוקרטית. המסקנה הראשונה מהניתוח דלעיל הנה שקיים **אינטרס תרבותי-חברתי-כלכלי לחזק ולשמר את מערכות המחשב של הכלל ושל הפרט מפני פגיעה**. המסקנה השנייה, הנובעת מהיות המחשב בעל פונקציות מגוונות, הנה כי על הגדרת ה"מחשב" בעברת החדירה למחשב להביא לידי ביטוי את מגוון הפעולות שהוא מבצע וכי לפיכך, עליה לכלול, למשל, גם כלי תקשורת ממוחשבים, כגון טלפון סלולרי.[18]

2. תיאור תופעת המחשוב הפולשני ומאפייניה

תופעת המחשוב הפולשני, המתבטאת בהסגת גבול למערכות מחשב, נמצאת בצדה האפל של מהפכת המחשבים, והיא בעלת כמה מאפיינים ייחודיים, המקשים על מניעתה ועל הרתעה מפניה. המאפיין העיקרי של מחשוב פולשני הנו **הקלות** שבה ניתן לחדור למחשב הזולת או להאזין לתקשורת בין מחשבים. ואכן, מחשוב פולשני הוא זמין, זול ולרוב, נשלט מרחוק, גם תוך חציית גבולות בינלאומיים.[19] די במחשב המחובר לרשת ובתכנת פריצה, ובמקרים אחרים ניתן להסתפק בטלפון צלילים.[20] **פוטנציאל ניצול המשאבים** המתאפשר מחדירה למחשב הנו אדיר, עובדה המעצימה את **הפיתוי** לחדור למחשבים: ניתן לחשוף מידע מסחרי, מודיעיני ואישי; ולגנוב כסף, שיחות טלפון וזמן אוויר. את החדירה למחשב ניתן לבצע באופן **מוסווה** **ובהיחבא**, דבר המקשה על איתור החודר, על תפיסתו ועל העמדתו לדין.[21]

מאפיין נוסף של תופעת המחשוב הפולשני נוגע **לפרופיל הנפשות הפועלות**: עד לאחרונה היה מדובר באנשים ובגופים נורמטיביים, נטולי עבר פלילי,[22] אך כיום ניכרת מגמת שינוי מסוימת, ובמידה רבה נראה שימי התום של פשיעת מחשבים

18 כך, לדוגמה, מהבחינה הפונקציונלית, מרבית הטלפונים הסלולריים המודרניים עונים על הגדרת "מחשב" – הם משמשים כלי תקשורת, כלי אחסון של מידע (תמונות, מספרי טלפון), כלי שליטה ובקרה (יומן פגישות, הערות) וכלי חישוב (מחשבון).

19 ואכן, חלק ניכר מתופעת המחשוב הפולשני, כגון "קוקיס", וירוסים ופעילות של האקרים (ראו עניין **טננבאום**, לעיל ה"ש 1), חוצה גבולות.

20 בפרשת **בדיר**, לעיל ה"ש 1, הנאשמים השתמשו בטלפונים כדי לחדור למכשירי קולן ולהאזין להודעות שהושארו בהם או כדי לגנוב שיחות טלפון. להרחבה ראו פרק ג' למאמר זה.

21 ואכן, "הערכה מקובלת בענף המחשבים טוענת, שמתוך כלל פריצות המחשבים המבוצעות כיום, רק 5% מזוהות" (עופר שלח, "שלא תדעו" **מעריב**, 6.4.1999, 5). מפרשת **האפרתי**, לעיל ה"ש 2, עולה, כי בחברות הניזוקות לא היו מודעים לעצם החדרת תוכנת הריגול למערכות המחשב שלהן. גם רשויות השלטון עשויות לערוך חיפוש סמוי במחשבים – No-knock search.

22 Turgeman-Goldschmidt, לעיל ה"ש 1.

חולפים להם.[23] שכיחותה של התופעה בקרב קבוצות נורמטיביות עשויה לנבוע מכך שבעיניהם מדובר בפגיעה במחשב – במכונה, במובחן מהפגיעה באנשים "הנמצאים מאחוריו".[24] ייתכן שהדבר נובע אף מהיעדר הפנמה של העובדה שהזכות לפרטיות והזכות לקניין רוחני ראויות להגנה. למרות הנזקים הנובעים מתופעת המחשוב הפולשני, **היחס הציבורי** אל פעולותיהם של ההאקרים הוא לעתים חיובי או לכל הפחות כאל מעשה שובבי, מתוחכם וחף מתווית פלילית.[25] כך גם באשר ל"קוקיס" (Cookies): אתרים רבים נוהגים להחדיר למחשבי הגולשים בהם קבצים האוספים (לרוב בסתר) מידע על הגולש והמוסרים אותו לאתר. חלק מאותם "קוקיס" מונחים להישאר לעד במחשב הגולש (Permanent Cookies) ולהעביר לאתר מידע מזהה על אודות הגולש, כגון נתוני הגלישה שלו, בכל גלישה חוזרת שלו באתר.[26] למרות הפגיעה בחירויות האדם הנגרמת בדרך זו, התופעה איננה מעוררת סערה, ודומה שהציבור בכללותו מקבל את המצב הקיים כדבר שאין בלתו.[27]

אפיון אחר של התופעה הוא **הקושי הכרוך בניהול הליכים משפטיים**, פליליים ואזרחיים כאחד, נגד החודרים למחשבי הזולת: המחשב הוא מין יצור כלאיים, המורכב מ"מיטלטלין" מוחשיים (החומרה) וממידע ערטילאי ממוחשב; איסוף המידע על שהתרחש בחדירה למחשב (Computer Forensics) אינו פשוט, שכן ניתן להעתיק את המידע הממוחשב מבלי לשנות או "להעלים" את המקור, וזאת בניגוד לגנבת חפץ מוחשי, אשר חשים בחסרונו; כמו כן, קשה להוכיח את הקשר בין הפורץ לבין הפריצה.[28]

---

23 ב"ש (מחוזי חי') 4096/04 **שטרנברג נ' מדינת ישראל**, תק־מח 2)04) 9078 (2004) (פריצה למחשב בנק לצורך גניבה).

24 ראו PETER J. NEUMANN, COMPUTER RELATED RISKS 274–275 (1995), שם נאמר: "People seem naturally predisposed to *depersonlize* complex systems. Computers are not people, and therefore need not be treated humanly"; בנוסף ראו: Turgeman-Goldschmidt, לעיל ה"ש 1, בעמ' 16: "The offence is not physically tangible (i.e. there's no physical sense of committing the offence)".

25 ראו עניין **טננבאום**, לעיל ה"ש 1. עם זאת, כיום היחס אל ההאקרים עובר שינוי, והם מתחילים להיחשב כעבריינים (ראו Turgeman-Goldschmidt, לעיל ה"ש 1; כן ראו עמדתו של ד"ר יעקב הכט, המציין שכיום ההאקרים מוגדרים לעתים כגנבים או כוונדליסטים. ראו, יעקב הכט "האקרים: בין טכנופיליה לפשיעה ווירטואלית" **תרבות דיגיטלית** (2004), ניתן לצפייה: www.isoc.org.il/magazine/magazine5_2.html (נבדק לאחרונה ב – 11.1.2009).

26 www.webopedia.com/TERM/P/persistent_cookie.html. (נבדק לאחרונה ב־11.1.2009).

27 P. M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 822–823 (2000).

28 לכך מתווסף גם הסיכוי הנמוך לקבלת פיצוי נזיקי בגין הנזקים כאשר מדובר בגורמים פרטיים, הנובע **מהיעדר כיס עמוק** של המזיק; שכן לעתים ההאקרים הם צעירים חסרי אמצעים, שאין באפשרותם לפצות בגין הנזקים הכלכליים שגרמו להם. כך, למשל, מתכנת וירוס I Love You שפגע במיליוני מחשבים היה סטודנט מחוסר אמצעים.

המסקנה המדאיגה העולה ממצרף מאפיינים אלו הנה שישנה **תת־הרתעה** בנושא תופעת המחשוב הפולשני, הנובעת הן מהקלות והפיתוי הרב הכרוכים בה, והן מהקושי ומאי־הכדאיות שבנקיטת הליכים משפטיים.

3. נזקי תופעת המחשוב הפולשני

על רקע התלות הגוברת במערכות המחשבים, ראוי לבחון את הנזקים שהחדירה למערכות מחשב גורמת. ואמנם, ניצול לרעה של כלי רב־עצמה זה, המחשב, עשוי להוביל לפגיעות כבדות בשני ממדים עיקריים: בממד האחד — הציבורי — ישנה פגיעה בשיקולים תועלתניים, ובממד השני — האישי — נגרמת פגיעה בערכים הומניסטיים. להלן ייבחנו נזקים אלו.

3.1 פגיעה בשיקולים תועלתניים

מחשוב פולשני עלול לבלום את הקִדמה התרבותית־כלכלית־מדעית המופקת מהפונקציות המועילות שממלא המחשב. לדוגמה, חשיפת מידע באמצעות חדירה למחשב פוגעת בפונקציה של המחשב ככלי אחסון וככלי תקשורת, שהרי היא מפרה את סודיות המידע המאוחסן בו והופכת אותו פגיע לשינויים. העמסת יתר על מערכות מחשב, הנגרמת בשל חדירה אליהן, פוגמת בדייקנות של מערכות שליטה ובקרה ממוחשבות. פגיעה במערכות מחשב קריטיות עלולה אף לשתק את המשך הפעילות התקינה של החברה; כשמדובר במערכות מחשב של תשתיות לאומיות, החיוניות לפעילות התקינה של החברה, כגון של שדות תעופה, הדבר אף עלול לגרום לאבדן חיים.[29] החשש ממעקב במערכות מחשב אף עלול להוביל להשפעה מצננת (Chilling Effect) על הרצון להשתמש במחשבים ולגרום למשל לרתיעה ממסחר אלקטרוני.[30] באופן עקיף, רתיעה זו מונעת מהחברה ליהנות מפירותיהן של

---

29 נייר עמדה, "לוחמה בטרור בזירת המידע", תלמידי הסדנה הרב־תחומית במשפט וטכנולוגיה, הפקולטה למשפטים, אוניברסיטת חיפה 3—4. (ניבה אלקין־קורן ומיכאל בירנהק עורכים, 2002), ניתן לצפייה בכתובת: www.cri.haifa.ac.il/technical/terror_info.pdf (נבדק לאחרונה ב־11.1.2009). (להלן: "לוחמה בטרור בזירת המידע").

30 ואכן, ממחקר שנערך בנושא זה בקהילייה האירופית עולה, שכשהנשאלים קיבלו מידע על תופעת ה"קוקיס", הדבר גרם להם שלא לרצות להשתמש באינטרנט: europa.eu.int/en/comm/eurostat/research/supcom.95/21/cookies.htm (נבדק לאחרונה ב־11.1.2009). לממצאים דומים הוביל סקר שנערך בשנת 2002 בקהילה האירופית (Questionnaire on the Implementation of the Data Protection Directive 95/46/EG) (להלן: "הסקר האירופי") בקרב קרוב ל־10,000 נסקרים. מהסקר עלה, כי החשש שמא ייעשה שימוש לרעה במידע פרטי שלהם גורם לרוב המכריע של הנסקרים (כ־70%) להימנע מלערוך קניות מקוונות.

הפונקציות החיוביות של מערכות המחשבים.[31]

3.2 פגיעה בחירויות אדם

הפילוסוף הידוע מונטסקיה (1689–1755) מציין, כי "החירות היא הזכות לעשות כל מה שהחוקים **מרשים**; ואם יוכל אזרח לעשות את מה שהם אוסרים, לא תהא לו עוד חירות, משום שלשאר האזרחים תהא אותה יכולת כשלו".[32] כמפורט בסעיף זה, תופעת המחשוב הפולשני פוגעת **במצבור**[33] חירויות אדם בסיסיות – חופש הביטוי, האוטונומיה, הקניין והפרטיות –שניתן לכנותו בשם "**זכות הסודיות במידע הממוחשב**".

חשיפת המידע הממוחשב של היחיד בחברה ללא הסכמתו גוררת פגיעה **בפרטיותו** של המשתמש במחשב. ההגנה על חירות זו עונה על צרכים אישיים וחברתיים חשובים: היא מאפשרת לפרט לפתח רעיונות ללא חשש מלגלוג על רעיון שטרם הבשיל או טעות שלא אותרה; להשיג מנוחה ממטרדים חיצוניים (כמו, למשל, פרסומות חודרניות הקופצות על צג המחשב); לתקשר עם הזולת בסודיות – מבלי שצד לא קרוא יקלוט את התקשורת בין המחשבים;[34] בנוסף, הגנת הפרטיות מונעת סממנים שלטוניים טוטליטריים, הנובעים ממעקב אחרי הפרט, בין היתר באמצעות חדירה למרחבו הממוחשב וריכוז מידע רב ולא רלוונטי עליו.

חדירה למרחבו הממוחשב של הפרט, למשל לתכתובת האלקטרונית שלו, פוגעת גם **בחופש הדעות והביטוי של** הפרט. ואמנם, ג'ון סטיוארט מיל מציין כי כשאנשים תלויים בדעת הקהל לפרנסתם, הם חוששים מדעת הקהל, לא פחות מכפי שהם חוששים מהחוק.[35] לפיכך, החשש מחיפוש פרטי או שלטוני במחשב ומחשיפת דעתו האמיתית עלולים לגרום ליחיד להימנע מלהשתמש במחשב לצורך פיתוח חשיבה אישית, השונה מזו המקובלת על החודרים, ולגרום לו לצנזר את דעותיו. ואכן, סולבה טוען כי מעקב אחרי הפרט פוגע בחופש הביטוי שלו ובחופש ההתאגדות, וכי הדבר

---

31 בב"ש (מחוזי ת"א) 90868/00 **נטוויז'ן נ' צבא ההגנה לישראל**, תק־מח 2000(2) 57734 (2000), הדגיש (בהערת אגב) סגן הנשיא אבן ארי, שקיים אינטרס ציבורי לעודד את השימוש החופשי במחשבים כאמצעי תקשורת.

32 מונטסקיה **על רוח החוקים** (קלוד קליין עורך, עידו בסו מתרגם, 1998).

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

34 ראו רות גביזון "הזכות לפרטיות ולכבוד" **זכויות האדם בישראל – קובץ מאמרים לזכרו של ד"ר חמן שלח ז"ל** (1994). וכן WESTIN F. WESTIN, PRIVACY AND FREEDOM, 32–39 (1967) סובר, כי הפרטיות מאפשרת ליחיד לפנות לקרובים לו או לגורמים מקצועיים, כמו פסיכולוג, עורך דין, רופא וכו', ולגלות את אשר על לבו, ביודעו כי הם ישמרו את סודותיו. אך השוו למסקנות בית המשפט בפרשת **היינץ**, לעיל ה"ש 14.

35 ג'ון סטיוארט מיל **על החירות** 59 (מהדורה ראשונה, אריה סימון מתרגם, 1946).

עלול למנוע פעילות חוקית ולגיטימית של אנשים, להפחית את קשת הדעות שהם מבטאים ולהגביל את החופש להיות פעיל בפעילות פוליטית.[36] החשש מחדירה למאגרי המידע של אתרי האינטרנט וביטול האנונימיות של מביעי הדעות בהם, למשל, עלול להרתיע מהשתתפות בשיח הציבורי הדמוקרטי המקוון, לפגוע באפשרות לפתח דעה אישית ייחודית ולמנוע מהחברה את התועלת שבגיוון החשיבה האנושית. לפיכך, ההגנה על סודיות המידע הממוחשב, למשל השמירה על חסיונה של כתובת ה־IP של גולש בפורומים באינטרנט, מאפשרת לפרט אנונימיות ובתוך כך – את היכולת לבטא את דעתו בחופשיות, ותורמת באופן עקיף לשיח החברתי. ואילו החשש מחדירה למאגרי המידע של האתרים וביטול האנונימיות של מביעי הדעות באתרי אינטרנט, עלול להרתיע מהשתתפות בשיח הציבורי הדמוקרטי המקוון. כך אף תיפגע האפשרות לפתח דעה אישית ייחודית ותימנע מהחברה התועלת שבגיוון החשיבה האנושית.

תופעת המחשוב הפולשני פוגעת אף **בחירות הקניין**, המוגנת בחוק־יסוד: כבוד האדם וחירותו[37] והמתפרשת אף על קניין רוחני.[38] מהו הקניין הממוחשב? ג'ון לוק (1704–1632), ההוגה העיקרי של ההומניזם המודרני, מנה את הזכות לחיים, לחירות **ולרכוש** כ"זכויות טבעיות" של כל אדם, המוקנות לו מכוח טבעו וכבודו האנושי ובלי תלות בכוחו של שלטון כלשהו. לשיטתו, הואיל ולכל אדם זכות על גופו, הרי שיש לו גם זכות טבעית למלאכת כפיו ולפרי עמלו (תאוריית העבודה): "הואיל ועבודה זו היא בלא ספק קניינו של העובד, רק הוא בלבד יכול להיות בעל זכות ביחס למה שצרפה אליו עבודתו".[39] יישום תפיסה זו במרחב הסיברקינטי מעלה, כי הביטוי הממוחשב של הכתיבה של הפרט ושל פועלו במחשבו שייך לו, וזאת מתוקף קניינו המוחשי במחשב שבו נאגר ביטוי זה ומתוקף העבודה שהושקעה בהפקתו.[40] לפיכך, בעלותו הקניינית של הפרט משתרעת לא רק על המחשב הפיזי, אלא גם על המידע הממוחשב שהפיק הפרט ואחסן במחשבו; העבודה הכרוכה ביצירת המידע הממוחשב ואחסונו בקניינו הפיזי של האדם – במחשבו, הם שמובילים לבעלות בו. מדובר

---

36 Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 San Diego L. Rev. 745, 475–476 (2007).

37 בס' 3 לחוק־יסוד: כבוד האדם וחירותו (שמירה על הקנין, "אין פוגעים בקנינו של אדם") ובס' 2 לחוק זה (כבודו של אדם). וראו: אהרן ברק "כבודו של האדם כזכות חוקתית" **הפרקליט** מא 271 (1994).

38 ע"א 6821/93 **בנק המזרחי המאוחד בע"מ נ' מגדל כפר שיתופי**, פ"ד מט(4), 221, 456–457 (1995). המושג "קניין" כולל גם **זכות אובליגטורית**. ייתכן אף שלמידע הממוחשב, שהנו קניין ערטילאי, מעמד חזק מזה של הזכות האובליגטורית, שכן מדובר במידע האגור במחשב – בדבר פיזי.

39 ג'ון לוק **על הממשל המדיני** פרק ה – על הקניין (מהדורה שניה, יוסף אור מתרגם, 1997).

40 ראו בדומה: Wendy J. Gordon, *A Property Right in Self-Expression; Equality and Individualism in the Natural Law of Intellectual Property*, Yale L.J. 1533 (1993).

בבעלות **בכל מידע** שנאגר במחשב ובמערכות התקשורת המקשרות בין מחשבים, בין שמדובר ביצירה אינטלקטואלית, שדיני זכויות יוצרים פורשים כנפיהם עליה, ובין שמדובר במידע אישי רגיש או רק סתמי. הוא הדין בנוגע לקבצים המכילים Non-Content Information, למשל קובץ המפרט את רישום הכניסות והיציאות למחשב או את רשימת האתרים שבהם גלשו מהמחשב; קבצים אלו מגלמים את הביטוי של עובדות שהן פרי מעשיו של הגולש, את העשייה המקוונת של הפרט, ולפיכך מהווים חלק מקניינו הפרטי־אישי.[41] והכול בכפוף לכך שמדובר במידע מקורי, שאין לזולת זכויות בו (בניגוד למקרה שבו מדובר, למשל, בתכנה מועתקת).

משמעותה של הבעלות הקניינית הנה הזכות לשימוש בלעדי ולמניעת שימוש או חדירה של אחר. בכל הנוגע לבעלות הקניינית במידע הממוחשב האגור במחשבו של הפרט, מדובר בזכות השליטה של בעל המידע הממוחשב לשלוט על כל הקשור בהסגת גבול אליו ולמנוע חדירה למידע זה או שימוש לא מורשה בו.[42] בהקשר של הבעלות במידע הממוחשב, משמעותה של חירות הקניין הנה הזכות לשימוש בלעדי במידע זה, ללא עין זרה צופייה, וזאת שעה שבעל המידע אינו חושף אותו לעיון הציבור, למשל, אינו מפרסם את הביטוי הכתוב הממוחשב באתר אינטרנט. בגדר השליטה במידע ניתן לכלול גם את הזכות למנוע חדירת זרים לקניין הממוחשב, למנוע את העתקתו הלא מורשית ולשלוט על פרסומו.[43] לפיכך על עברת החדירה למחשב לאסור גישה לא מורשית אליו, ולא לחול רק כשנגרם נזק למידע הממוחשב. עם זאת, ברי שכאשר מדובר במידע ממוחשב **הפתוח** לעֵינֵי כול, למשל באתר אינטרנט או על צג המחשב במקום ציבורי, פוחתת משמעותית שליטתו הקניינית של בעל המידע הממוחשב על מי שרשאי לצפות בו.[44]

---

41 תפיסה דומה באה לידי ביטוי בס' 5(4) לחוק זכות יוצרים, התשס"ח–2007, ממנו עולה כי זכות היוצרים חלה על דרך הביטוי של עובדה או נתון ובס' 2(5) לחוק הגנת הפרטיות, התשמ"א–1981.

42 ניתן לטעון, שהפועל היוצא של גישה זו הנו שהפרטיות נתפסת כקניינו של הפרט, אם כי תפיסה זו מצריכה ניתוח נפרד. ראו גם: עמדת השופט אריאל בע"פ 5026/ 97 **גלעם נ' מדינת ישראל**, תק־על 99 (2) 1149 (1999): "פרטיותו של אדם היא כבודו וגם קניינו"; מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 11 (2007).

43 בפרשת Donaldson v Beckett, 4 Burr. 2408 (1774), המהווה אבן הפינה לזכויות היוצרים באנגליה נקבע, כי למחבר זכות ייחודית להחליט אם לפרסם את הספר פרי יצירתו, ועיקרון תקדימי זה עדיין מהווה את הבסיס לדיני זכויות יוצרים. בישראל באה לידי ביטוי זכות הפרסום בס' 11(2) לחוק זכות יוצרים, התשס"ח–2007, הקובע כי ליוצר נתונה הזכות הבלעדית לפרסם את היצירה. סבורתני, כי על הדין הראוי לפרוש את הגנתו על מידע ערטילאי שלא פורסם, אף אם אינו עומד בדרישות היצירה הספרותית המוגנת כיום בדיני זכויות יוצרים, וזאת הואיל ומידע כאמור חוסה בצל דיני הגנת הפרטיות.

44 ראו שרון אהרוני־גולדנברג ואריה רייך "חדירה למחשב כעוולה נזיקית" **שערי משפט** ד 415, 429 (2006).

ההבחנה בין קניין במחשב עצמו, לבין בעלות על המידע הממוחשב יוצרת מצב שבו תיתכן בעלות על המידע הממוחשב, במובחן מהבעלות הקניינית על המחשב עצמו, כמו, למשל, במקרה שבו קובץ פרטי של ראובן מאוחסן כדין במחשבו של שמעון.[45] סיטואציה זו, של **קניין מעורב**, מתעוררת לעתים קרובות שעה שמדובר במחשבים הנמצאים בסביבת העבודה – שבה המעביד מספק לעובדו מחשב, וזה מאחסן בו מידע אישי. משנעשה עירוב תחומין זה בין הקניין הפרטי־ערטילאי לבין הקניין המוחשי, נחלשת, באופן יחסי, השליטה הקניינית של שני בעלי הזכויות השונים – של העובד והמעביד. בכל הנוגע להגבלת זכות השליטה של העובד בקניין הערטילאי אשר יצר – בקובץ המחשב הפרטי, הרי שככלל, שעה שאין מדובר במידע ערטילאי שנוצר לצורך העבודה, כי אם במידע פרטי, ראוי לראות את הקניין בו כשייך לעובד.[46] עם זאת, ייתכן שזכותו של העובד לפרטיות נסוגה אל מול האינטרסים הקנייניים והכלכליים של המעביד, בכל הקשור למידע ממוחשב הנוגע לאתרים שבהם גלש העובד או בכל הנוגע לכותרת של התכתובת שלו.[47] ודוק: ספק רב אם המעביד רשאי לפרסם ברבים וללא צידוק ראוי מידע זה, וזאת נוכח זכותו של העובד לפרטיות.

נעבור לבחון את האופן שבו מוגבלת שליטתו הקניינית של המעביד על מחשבו, בכל הנוגע לגישה למידע הממוחשב הפרטי השייך לעובדו והמאוחסן במחשבו. לגישתי, כאשר קובץ מחשב אישי־פרטי של ראובן מאוחסן כדין במחשבו של שמעון, אין לשמעון זכות קנויה לעיין בו או לפותחו. על פי תפיסה זו, ככלל, מעביד איננו רשאי לפתוח קבצים פרטיים של עובדו, המאוחסנים במחשב שהוא עצמו סיפק לו, ולעובד שמורה הזכות להשתמש באופן סביר בקניין המעביד בסביבת העבודה, מבלי שהמעביד יפגע בפרטיותו בו. גישה זו משתקפת בהסכם הקיבוצי שנערך ביום 25.6.2008 בין הסתדרות העובדים הכללית החדשה לבין לשכת התיאום של הארגונים הכלכליים (להלן: "ההסכם הקיבוצי"), שממנו עולה כי למעביד – לבעל המחשב – אין זכות לחדור לקבצים של עובדיו, אף שאלו מאוחסנים במחשבו שלו.

ניתן לבסס את התפיסה המוצעת על יסודות מספר, אשר יפורטו להלן. ראשית, מהבחינה הקניינית הטהורה, הואיל והמידע הממוחשב הפרטי איננו פרי עמלו של

---

45 ודוק: אין הכוונה ליצירה משותפת, כהגדרתה בחוק זכות יוצרים, התשס"ח–2007, אלא לבעלות באובייקטים השונה זה מזה – המידע הממוחשב והמחשב עצמו.

46 כך, למשל, על פי ס' 34 לחוק זכות יוצרים, התשס"ח–2007, המעביד הוא הבעלים הראשון של זכות היוצרים ביצירה שנוצרה על ידי עובדו לצורך עבודתו ובמהלכה, אלא אם כן הוסכם אחרת.

47 ראו בדומה עמדת השופט ארמון בעניין עב' (אזורי נצ') 1158/06 **אפיקי מים נ' פישר**, תק־עב 08 (2) 586 (2008), המבחין בין כניסה לתוכן ההודעה לבין חשיפת כותרת התקשורת האלקטרונית (Non Content Information). עם זאת, אין בדברים אלו כדי להכשיר איסוף מידע על מיקומו של מכשיר טלפון סלולרי שניתן לעובד על ידי מעבידו. וראו בעניין זה את הצעת החוק הפרטית לתיקון חוק הגנת הפרטיות (תיקון – מסירת נתוני תקשורת), התשס"ז–2007.

בעל המחשב ואף לא פועל יוצא של יצירתו, הרי שהוא איננו בעל זכות השליטה ביחס אליו – לרבות הזכות המוקנית לפתוח קובץ זה ולעיין בו; הזכות הטבעית למלאכת כפיו ולפרי עמלו שייכת ליוצר – למי שהזיע ועמל בגיבושה, גם שעה שהיצירה מגולמת בקניין מוחשי השייך לאחר. תפיסה דומה באה לידי ביטוי באופן ברור יותר גם בכל הנוגע לרכישת ספר; הבעלות הקניינית של הרוכש על הספר שקנה (הקניין המוחשי) איננה מקנה לו את הזכות להעתיק את היצירה (הקניין הערטילאי) ולשווקה.

שנית, זכותו של בעל המחשב הפיזי, המעביד, מתנגשת עם זכותו לפרטיות של המשתמש המורשה במחשב. וסבורתני, שבאיזון שבין שתי הזכויות על הדין לפרוץ את גדר הטריטוריה הקניינית של היחיד, וזאת כדי להגן על פרטיותו של זולתו. כך, למשל, ראוי לאסור הקלטה בסתר של שיחת הזולת, אף כשהמאזין בסתר הנו **בעליו** של מכשיר הטלפון שממנו מתבצעת השיחה.[48] בדומה, העובד רשאי לפרטיות בחדר האמבטיה הנמצא **בבעלות** מעבידו. ואכן, בבסיס דיני הגנת הפרטיות עומדת ההנחה שלפיה הפרטיות נעה עם האדם באשר הוא, וכי היא אינה כפופה לבעלות קניינית במקום שבו נמצא הפרט. לעניין זה יפים דבריו של הנשיא (דאז) ברק בפרשת **פלונית**: "סביב כל אדם יש מרחב שבתוכו הוא זכאי להיות עם עצמו. מרחב זה נע עם האדם עצמו. היקפו של המרחב נגזר מהצורך להגן על האוטונומיה של הפרט. על כן הוא עשוי לחול גם במקום בו אין לפרט כל קניין (כגון בית הוריו, בית חולים, תא טלפון)".[49] בהקשר זה ניתן להמשיל את הקובץ האישי הממוחשב המאוחסן במחשב הזולת לחדר בבית מלון. לתייר השוהה בחדר יש בו שליטה קניינית מוגבלת, הנובעת מדיני הגנת הפרטיות, והמאפשרת לו למנוע כניסה או הצצה לא מורשית לחדרו ולמתרחש בו, וזאת, אף שהבעלות הקניינית בחדר שייכת לאחר.

שלישית, כאמור, עניין לנו במקרה שבו ראובן מאחסן את קבציו **כדין** במחשב של שמעון. במקרה זה גישתו של ראובן לקניין של שמעון נעשית בהסכמתו או לפחות כדין,[50] ואילו גישתו של שמעון לקובץ של ראובן נעשית תוך פגיעה בחירויות יסוד שלו, לקניין ערטילאי, לפרטיות, וכמפורט להלן – לאוטונומיה, שהרי היא נעשית

48 ראו גם יורם שחר "הבטחון הפרטי והדין" **עיוני משפט** יג, 121, 147 (1988): "אין החוק יוצר זיקה כלשהי בין זכויותיו של המאזין בנכס בו מתבצעת ההאזנה לבין איסור האזנת סתר, ואף המצוי בתחום פרטיותו הקניינית עצמה אינו קונה בכך היתר להאזין למי שהורשו או אף הוזמנו להימצא באותו תחום".

49 בג"ץ 6650/04 **פלונית נ' בית הדין הרבני האזורי בנתניה**, תק־על 2006(2) 1736, 1746 (2006).

50 ראו בנושא זה את הערת בית הדין לעבודה בעב' (אזורי ת"א) 10121/06 **איסקוב נ' הממונה על חוק עבודת נשים**, תק־עב 2007(3) 2594 (2007): "בהתחשב בהיקף השעות שעובד שוהה במקום העבודה, ובטשטוש המסוים – בחלק מסוגי העיסוקים – בין הבית לעבודה, מצופה – כתניה מכללא בחוזה העבודה – לאפשר לעובד פרקי זמן קצרים לצרכים חברתיים ופרטיים בהיקף סביר. כדוגמא – שיחות טלפון קצרות עם בני משפחתו".

ללא הסכמתו. כך שבאיזון שבין פעולה שנעשית כדין ובהסכמה, לבין כזו שנעשית תוך פגיעה בזכויות יסוד, גוברת זכותו של מי שפועל כדין. מצבור טיעונים אלו מעלה, שככלל, שליטתו הקניינית של בעל המחשב במחשבו נסוגה אל נוכח זכויות מנוגדות של יוצר קובץ המחשב, ובכלל זה זכותו של היוצר לפרטיות, לאוטונומיה ולקניין ערטילאי בקבציו הפרטיים המאוחסנים במחשב.

חירות האדם נוספת הנפגעת בעקבות חדירה למערכות מחשב ללא הסכמה הנה הזכות **לאוטונומיה**, המושתתת על ערך הכבוד המגולם בחוק־יסוד: כבוד האדם וחירותו, והמתבטאת בחופש הבחירה של הפרט.[51] היותו של המחשב קניין מכונן של היחיד והכלל בחברה המודרנית; היות הזכות לאוטונומיה אם כל יתר הזכויות;[52] נפיצותה של תופעת המחשוב הפולשני ונזקיה המרובים – כל הגורמים הללו מובילים למסקנה, **כי על ההסכמה לשמש קו הגבול המפריד בין מעשה לגיטימי של כניסה למרחבו הממוחשב של הזולת, לבין עברה או עוולת מחשבים.** על פי תפיסה זו, הפרט הוא בעל הזכות לבחור אם להתיר חשיפה של מרחבו הווירטואלי בפני הזולת, וזכותו להסכים או לסרב לחדירה למחשבו.[53] ניתן להסיק מגישת האוטונומיה, כי קיימת חזקת אי־הסכמה לכניסה למחשבו המסחרי או האישי של הזולת, וכי נטל קבלת ההסכמה להיכנס למחשב הזולת מוטל על הנכנס. מכאן שחדירה לא מורשית למרחבו הממוחשב של הפרט וחשיפת סודותיו מהווה הפרה של האוטונומיה האישית והמסחרית שלו להחליט מה ייעשה ברכושו ובמידע שלו. לעומת זאת, כשמדובר באתר אינטרנט, הפתוח לציבור הגולשים, ברי כי יש הסכמה משתמעת לכניסה לאתר.[54]

51 אהרן ברק **פרשנות חוקתית** כרך שלישי 421 (1994); ע"א 2781/93 **עלי דעקה נ' בית החולים "כרמל"**, פ"ד נג(4) 526, 573–575 (1999). לסקירה מאלפת של המקורות הספרותיים הדנים במהותה של הזכות לאוטונומיה ושל ההסכמה במשפט הפלילי ראו: רות קנאי "הסכמת הנפגע במשפט הפלילי" **משפטים** כט 389, 391, 404, 418 (1998). לניתוח יסודות ההסכמה בחוקים שונים ראו דוד קרצ'מר **דיני הנזיקין – העוולות השונות – תקיפה וכליאת שוא**, 12–14, 16–17 (גד טדסקי עורך, 1981). לסקירת הזכות לאוטונומיה בהקשר של תופעת המחשוב הפולשני ראו שרון אהרוני־גולדנברג **תופעת המחשוב הפולשני – סעדים משפטיים** (חיבור לשם קבלת "תואר דוקטור במשפטים", אוניברסיטת בר־אילן – הפקולטה למשפטים, 2005).

52 פרשת **פלונית**, לעיל ה"ש 49.

53 מאידך, יש הסוברים כי ראוי שקו הגבול יסומן באמצעות **מנגנון הגנה טכנולוגי** או אולי גרימת **נזק** למערכת המחשב. גישות מעניינות אלו מצריכות התייחסות נפרדת החורגת מטווח דיון זה. ראו D. Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 473 (2003); O. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. REV. 1596, 1649–1653 (2003). האחרון למשל סבור כי ראוי להכפיף את עברת החדירה למחשב לפיצוח של מנגנון הגנה טכנולוגי. גישה זו מחצינה את עלויות המגננה הטכנולוגית לכתפי בעל הקניין ואף מצמצמת את שליטתו הקניינית ברכושו.

54 בחינת מהותה של החדירה **לאתרי אינטרנט** מצריכה דיון נפרד ומעמיק יותר. ראו בעניין זה את

לעתים, אף על פי שניתנה הסכמה לכניסה למחשב, תהווה הגישה אליו עברה, שכן כדי שההסכמה אכן תכשיר את הכניסה למרחבו הממוחשב של הזולת, עליה לעמוד בשלושה מבחני עזר – **הסכמה מדעת, חופשית ומותאמת**, כמפורט להלן:

א. על ההסכמה להיות מותאמת למה שנעשה בפועל במחשב; קרי יש לבחון לְמה, למי ועד מתי ניתנה ההסכמה.[55] כך, למשל, אמנם הבנק שבו עבדה אתי אלון התיר לה להפעיל את המחשב, אך **היה זה לצורך עבודתה**, ולא **לשם גנבת משאבים ממוחשבים**.[56]

ב. על ההסכמה להיות מדעת[57] – מבוססת על המידע המלא בנוגע להשלכות הכניסה למחשב;[58] כך ניתן לטעון כי החדרת "קוקיס" נעשית בהסכמת הגולש, שכן השארת ברירת המחדל בתכנת הדפדפן המאפשרת הכנסת "קוקיס" למחשב, כמוה כהסכמה משתמעת לכניסה למחשב. ואולם, בהתבסס על תפיסת ההסכמה מדעת ניתן לגרוס, כי ההרשאה האוטומטית להחדרת "קוקיס" – לאו הסכמה מדעת היא, וזאת מכמה סיבות: (1) את נושא ה"קוקיס" מאפיין חוסר מודעות ציבורי; (2) לרוב, הגולש אינו מודע לאפשרות שינוי ברירת המחדל הקיימת בדפדפן; ו־(3) אין לדעת מראש מהי הפעולה שעושה ה"קוקי" שהוחדר למחשב – סריקת כל המחשב או רק העתקת נתוני הגלישה באתר.[59]

ג. על ההסכמה להיות חופשית, כנה ואמיתית,[60] ולהינתן אל מול אלטרנטיבות אמיתיות להסכמה. לעניין זה יפים דבריו של Raz:

> "If having an autonomous life is an ultimate value, then having a sufficient range of acceptable options is of intrinsic value, for it is constitutive of an autonomous life that is lived in circumstances where acceptable alternatives are present".[61]

ניתוחו מעורר המחשבה של השופט אבי טננבוים בת"פ (שלום י־ם) 3047/03 **מדינת ישראל נ' מזרחי**, תק־של 04(1) 5911 (2003) (להלן: **פרשת מזרחי**). וכן eBay, Inc v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–1070 (2000).

55 U.S. v. Morris 502 U.S. 817 (1991).

56 עניין **אלון**, לעיל ה"ש 3.

57 ראו עניין **עלי דעקה**, לעיל ה"ש 51, בעמ' 597.

58 ראו הגדרת "הסכמה" בס' 3 לחוק הגנת הפרטיות (תיקון התשס"ז), התשמ"א–1981: "'הסכמה' – הסכמה מדעת, במפורש או מכללא".

59 http://europa.eu.int/en/comm/eurostat/research/supcom.95/21/cookies.htm (נבדק לאחרונה ב־11.1.2009).

60 יעקב קדמי **על הדין בפלילים** חלק שני 742 (1995); קנאי "הסכמת הנפגע", לעיל ה"ש 51, בעמ' 391, 404, 408.

61 Joseph Raz, The Morality of Freedom 205 (1068).

פרופ' Schwartz[62] טוען, כי חופש ההסכמה של הגולשים ברשת הנו מוגבל, שכן האופציה היחידה המאפשרת לגולש להגן על פרטיותו היא להפסיק לגלוש. לדבריו, מצב זה של "תיפגע או תפסיק" – המכונה על ידו "מלכודת האוטונומיה", נובע מכמה סיבות: קיימת אסימטריה ביחסי הכוחות שבין הגורמים שעוסקים בעיבוד מידע אישי לבין הגולשים, ועובדה זו מגבילה את יכולת הפרט להגן על פרטיותו; ברירות המחדל הטכנולוגיות של תעשיית המחשבים מוטה לרעת ההגנה על פרטיות הגולש, וממקסמות את האפשרות לדלות עליו מידע. ואכן, לרוב, ברירת המחדל המותקנת בתכנת הדפדפן במחשבים רבים, מאפשרת החדרת "קוקיס".[63] היעדר זה של יכולת לבחור ביישומים שיגנו על הפרטיות של הגולש באינטרנט מונע מהחברה "Collective Goods".[64]

להלן תיבחן סוגיית הפגיעה בזכות לאוטונומיה בקונטקסט של **סביבת עבודה**, שבה המעביד מודיע כי הוא מנטר את המידע הממוחשב של עובדיו המאוחסן במחשביו. בפרשת **איסקוב**[65] נקבע על ידי בית הדין האזורי לעבודה, כי יש לראות בעובדת ששלחה מייל אישי ממחשב מעסיקה, כמי שהסכימה מכללא לעיון המעביד בו, שכן "התובעת ידעה שאין מדובר בתיבת דואר אלקטרוני המיועדת לעניינים אישיים או אינטימיים אלא קיימת אפשרות כי תוכן ההודעות יגיע לצדדים שלישיים (כולל החברה עצמה)". בית הדין ציין, שבפני העובדת ניצבה האפשרות שלא לעשות שימוש בתיבת הדואר של מעסיקה ובכך למנוע פגיעה בפרטיותה.[66] סבורתני, שהלכה למעשה, תפיסה זו מכשירה חדירה כללית של מעסיקים למידע ממוחשב אישי של עובדיהם, גם במקרים שבהם לא התעורר חשד כלשהו כנגד העובד, תוך פגיעה בלתי

---

62 Schwartz, לעיל ה"ש 27, בעמ' 822–823.

63 אמנם ניתן לטעון, כי לגולש יש אלטרנטיבה להחדרת ה"קוקיס" – הוא יכול לשנות את ברירת המחדל, לסרב להחדרת "קוקיס" או להכפיף כל כניסה של "קוקי" להסכמה ספציפית שלו. ואולם, סגירת האופציה להחדרת "קוקיס" גורמת לכך שאותו גולש לא יורשה כלל לגלוש באתרי אינטרנט רבים. כמו כן, שינוי ברירת המחדל למצב שבו כל החדרת "קוקיס" למחשב תיעשה בכפוף לאישור הגולש, עלולה להפוך את הגלישה לטרדנית, שכן, כמעט בכל לחיצת מקש תופיע חלונית שבה יתבקש הגולש לאפשר או לדחות השתלת "קוקי". ראו גם נייר העמדה של **המועצה הציבורית להגנת הפרטיות** (20.2.2006), שבו הומלץ שלא להשתמש באמצעים המנטרים את פעילות הגולש באתר, כדוגמת "קוקיס".

64 שם, בעמ' 206.

65 פרשת **איסקוב**, לעיל ה"ש 50 (השׁ' דוידוב-מוטולה). בעניין זה טענה התובעת שהיא פוטרה מחמת הריונה, ואילו המעסיק טען שהיא פוטרה לפני כניסתה להיריון. כראיה, הגיש המעסיק עותקים מהודעות דואר אלקטרוני ששלחה התובעת מהמחשב של מקום העבודה, שמהן עלה שהיא חיפשה עבודה חלופית עוד לפני ההיריון. העובדת התנגדה להצגת ההודעות בטענה, שבהתאם לחוק האזנת סתר ולחוק הגנת הפרטיות, התשמ"א–1981, חל איסור על המעביד לעיין ולהעתיק הודעות דואר אלקטרוני של העובד. ההחלטה נמצאת כיום בערעור בפני בית הדין הארצי לעבודה (בר"ע 570/07).

66 שם, פס' 12 להחלטה.

מוצדקת בחירוויות העובדים – לפרטיות, לקניין ואף לאוטונומיה, וזאת משתי סיבות עיקריות. ראשית, הואיל והסכמה שניתנה מכוח יחסים בלתי שווים, כגון יחסי עובד־מעביד, שבהם צד אחד נחות יותר, איננה חופשית;[67] כאשר אין בידי העובד ברירה אלא להסכים לפגיעה בפרטיותו או להפסיק לעבוד, הרי מדובר במעשה שנעשה ללא הסכמתו, תוך פגיעה בזכותו לאוטונומיה. שנית, ראוי להבחין בין הסכמה לבין ידיעה; העובדה שהעובד יודע שהמעביד פוגע בפרטיותו, אין פירושה שהוא **מסכים** לכך מכללא. הד לתפיסה זו ניתן למצוא בהחלטת בית הדין האזורי לעבודה בעניין **אפיקי מים**, שם היה מדובר, בין היתר, בעיון של מעביד בתכתובת אלקטרונית של העובד, אשר נמצאה על שרתיו. השופט ארמון קבע כי:[68]

> "ניתן לראות כל משתמש ברשת, כבעל ציפייה סבירה לפרטיות ולמניעת הגעה לתוכן התכתובת האלקטרונית וזאת כל עוד הוא לא ויתר על כך באופן מפורש. אותה ציפייה סבירה, מצדיקה – לדעתי – קביעה שלפיה כל עוד אין **ויתור מפורש** של העובד על זכותו לפרטיות, יהיה קשה מאד להגיע למסקנה על כך שיש לראות אותו כמי שויתר על כך, באמצעות לימוד של הסכמה מכללא. וכך – גם אם מדובר במידע שנשמר במאגר מידע משותף שאינו שאינו בבעלותו הקניינית של העובד, אלא של מעבידו. עצם העובדה שהעובד ידע שהתכתובת שלו נשמרת בשרת שבבעלות המעביד ואשר למעביד גישה אליו, אינה יכולה להספיק כדי ללמד שהעובד הסכים, מכללא, לכך שהמעביד יהיה רשאי לעיין באותה תכתובת" (ההדגשה שלי – ש.א.ג.).

מעניין לציין כי בסקר שנערך בקהילה האירופית, ענו מרבית הנסקרים שאין להתיר למעביד לקרוא דואר אלקטרוני של עובדו, שנשלח או נתקבל במחשבי המעביד. חלק

---

67 ראו דב"ע (ארצי) 4-70/97 **אוניברסיטת תל־אביב נ' ההסתדרות הכללית**, פד"ע ל 385, 404, 411 (1997), שם נקבע, כי הסכמה לפגיעה בפרטיות צריכה להיות חופשית: "יחסי עובד – מעסיק אינם יחסים שווי כוחות; מצבו של העובד הוא בדרך כלל נחות מזה של המעסיק. לכן החלטתו של העובד לעמוד במבחני התאמה אינה ניתנת תמיד מ'רצונו החופשי'". וראו גם עמדתו של מ' גולדברג "הגנת הפרטיות של העובד וחובות הגילוי שלו כלפי מעבידו" **עבודה חברה ומשפט** ט 85, 88, 100–101 (2002). בנוגע למקרים בהם ישנה הסכמה מפורשת של העובד ובנוגע לטשטוש הקיים בין הפרטי למסחרי. בת"א (מחוזי ת"א) 1285/89 **צוקרמן נ' מורגנשטרן**, תק־מח 1999(4) 16417 (1999), נדחתה הטענה שלפיה קיימת הסכמה מכללא של העובד לפגיעה בפרטיותו על ידי האזנת סתר לשיחותיו הפרטיות עם ידידתו מחוץ לנישואין, וזאת נוכח האינטרס הקנייני של המעביד. השופט סטרשנוב קבע, כי זכותו החוקתית לפרטיות של העובד גוברת על זכותו הקניינית של המעביד, במיוחד כשיש איסוף של מידע שאינו רלוונטי, הנוגע לצנעת הפרט (שם, בעמ' 16439–16442).

68 פרשת **אפיקי מים**, לעיל ה"ש 47, בעמ' 588.

קטן יותר של הנסקרים ענה בדומה, אך סייג את הכלל האמור – אלא אם כן יש חשד רציני שהעובד עבר עברה פלילית. רק 4% מהנסקרים סברו שיש לאפשר למעביד לקרוא את הדואר האלקטרוני של עובדיו אם זה הכרחי לקיומו התקין של העסק.[69] מבחינה זו, ההסכם הקיבוצי הנו ראוי, באשר, כאמור, הוא יוצא מנקודת הנחה שלעובד יש זכות לסודיות במידע הממוחשב שלו, האגור במחשב העובד, אך כי ישנם מקרים שבהם אינטרסים מנוגדים – בעיקר כלכליים – של המעביד יאפשרו לו לחדור לקובצי העובד האגורים במחשבו.[70] בכך נותן ההסכם הקיבוצי ביטוי לרגשות הרווחים בקרב הציבור הרחב.

הנה כי כן, הכניסה הלא מורשית למרחבו הממוחשב של הזולת פוגעת במצבור חירויות אדם – בזכות לפרטיות, בחופש הביטוי, בחירות הקניין ובזכות לאוטונומיה – המצטברות לכדי **זכות לסודיות במידע הממוחשב. פגיעה מצטברת זו שמה לְאַל** את **חירות השימוש במחשב**, שכן היא מגבילה את שליטתו המורשית של היחיד במידע הממוחשב שלו ובמחשבו, ובאופן עקיף היא אף פוגמת באינטרסים חברתיים־תועלתניים.

משנותחו חירויות האדם הנפגעות בעקבות תופעת המחשוב הפולשני – חירות הפרטיות, הביטוי, הקניין והאוטונומיה – נשאלת השאלה: **איזה סוג של פגיעה בזכות הסודיות במידע הממוחשב ראוי להתייחסות משפטית מחמירה יותר: חדירה למחשב או קליטת תקשורת בין מחשבים (האזנת סתר)?** לתשובה על שאלה זו – פנים לכאן ולכאן: מחד, ניתן לטעון שהפגיעה בזכות הסודיות בתקשורת בין מחשבים הנגרמת בהאזנת סתר חמורה יותר מזו הנגרמת מחדירה למחשב, שכן שיחה של הפרט, ובכלל זה תקשורת בין מחשבים, הנה ערך חשוב בחברה המודרנית, ולשם אפשורה נדרשת הגנה על סודיות התקשורת.[71] כמו כן, קליטת תקשורת בין מחשבים פוגעת בפרטיותם של שני הצדדים לשיחה, ואילו כשמדובר בחדירה למחשב ובחשיפת מידע שלא תוקשר, אזי רק פרטיותו של **צד אחד** (בעל המידע) נפגעת.[72]

מאידך, לדעתי, הפגיעה בזכות הסודיות הנגרמת בעקבות **חדירה למחשב חמורה**

---

69 הסקר האירופי, לעיל ה"ש 29.

70 בס' 3.ד. להסכם נקבע, כי "בהתקיים נסיבות שמקימות למעסיק סביר סיבה להניח בתום לב, כי העובד עושה במחשב שימוש בלתי חוקי או שימוש החושף את המעסיק לתביעות צד שלישי או שימוש שיש בו כדי לפגוע בעסק, רשאי־המעסיק לבצע פעולות לבדיקת שימוש העובד במחשב, באינטרנט ו/או בדוא"ל, והכל במידה ראויה וסבירה, לפרק זמן סביר ותוך צמידות למטרה. לכל כניסה לתיבת דואר אישית, הנושאת כתובת עם שם העובד בלבד ולקבצים אישיים שלו, נדרשת הסכמה מפורשת מצב העובד, ואם ביקש זאת העובד, יעשה הדבר בנוכחותו". בסעיף קטן ה' נקבע, כי "שימוש במידע אישי, שנאסף על ידי מעסיק על פי סעיף זה, יהיה בהתאם לכללים ותוך פגיעה פחותה בפרטיות העובד. מידע שהושג שלא כדין ובניגוד להסכם זה לא יעשה בו שימוש".

71 Westin, לעיל ה"ש 34.

72 להבחנה שבין האזנת סתר ובין חיפוש במחשב ראו גם "לוחמה בטרור בזירת המידע", לעיל ה"ש 29.

יותר מזו הנגרמת בעקבות יירוט מידע הנמצא בהליכי תקשורת בין מחשבים, וזאת מכמה נימוקים. ראשית, הפרט זקוק למקום שבו יוכל לנהל יומן אישי ממוחשב, בלי עין בוחנת; יש לו צורך במרחב שבו יוכל לנסח טיוטות של תכתובת אלקטרונית, מבלי שניתן יהיה לגלות את תוכנה לפני שליחתה. שנית, את סודותיו הכמוסים ביותר שומר האדם לעצמו – במחשבו, ואינו מפרסם, ופירוש הדבר שחשיבותו וסודיותו של המידע המאוחסן רבה יותר מאשר זו של מידע שתוקשר לזולת; ואכן, לפני שליחת המכתב (המייל, למשל), הפרט נמצא עדיין בשלבי ההתלבטות, הניסוי והטעייה, ואילו כאשר נשלח המכתב לדרכו יש יותר שלמות עם תוכנו ואף אבדן מסוים של השליטה הקניינית בו. שלישית, חדירה למחשב חושפת את הגורם המחפש **לכל המידע האגור במחשב**, ואילו המידע המועבר בתקשורת בין מחשבים מוגבל.[73] רביעית, וחשוב מכול, חדירה למחשב **מאפשרת לגורם החודר לשנות את המידע שנחשף**, לשבשו ולשתול במחשב מידע אחר, ואילו בהאזנת סתר הגורם המאזין הנו פסיבי ואינו יכול לשנות את המידע המנוטר.

לעובדה שיש להגן ביתר שאת על סודיות המידע הממוחשב מפני חדירה למחשב, מאשר מפני האזנת סתר לתקשורת בין מחשבים, ראוי שתהיינה השלכות על הדין הרצוי ועל פרשנותו של הדין המצוי: על דיני החיפוש הנוגעים למחשב (ודיני פסלות הראיה הנגזרים מהם) להחמיר יותר בכל הנוגע לחיפוש במחשב; ראוי גם שהענישה בגין עברת חדירה למחשב תחמיר יותר מזו הנוגעת לקליטת תקשורת בין מחשבים; כמו כן, על הפיצוי המוענק לקרבן חדירה למחשב להיות גבוה יותר מזה הניתן לניזוק בגין האזנת סתר.[74]

4. הסייגים להגנת הסודיות במערכות מחשבים

תופעת המחשוב הפולשני פוגעת בתפקודה התקין של החברה ובערכים הומניסטיים ראויים להגנה – הזכות לפרטיות, לחופש ביטוי, לקניין רוחני ולאוטונומיה, ולפיכך על הדין להתייחס אליה בחומרה. עם זאת, עקרון הסודיות במידע הממוחשב איננו מוחלט, ויש **לאזנו** עם עקרונות משמעותיים אחרים, כגון הצורך במניעת פשיעה והגנת חירויות אדם אחרות. בפרק זה ייערך דיון נורמטיבי **לא ממצה** בהיבטים שונים של עקרונות אלו. הדיון ייפתח בצורך החברתי לאפשר חדירה שלטונית למערכות מחשב ויירוט תקשורת בין מחשבים (חיפוש במידע הממוחשב), ולאחר מכן ייבחן

---

73 לדוגמה, אדם כותב טיוטת מכתב ורק לאחר מכן לשלוח אותו לחברו. כעבור זמן מה ישיב החבר את תשובתו. בפועל, חדירה לשני המחשבים של שני החברים או אפילו רק לאחד מהם, מובילה לאותה התוצאה – קריאת התכתובת ביניהם, ולא רק את הנוסח של אחד מהם.

74 בנוגע לצורך בחקיקת עוולת חדירה למחשב ראו: שרון אהרוני־גולדנברג ואריה רייך, לעיל ה"ש 44, אך השוו למיכאל בירנהאק, "משפט המכונה: אבטחת מידע וחוק המחשבים" **שערי משפט ד** 315 (2006).

הצורך לאפשר חדירה פרטית למערכות מחשבים במסגרת סעד העזרה העצמית.

4.1 צידוקים לחדירה שלטונית למערכות מחשב – מניעת פשיעה ושמירת הסדר החברתי

חיפוש שלטוני בכליו של אדם ובכלל זה – האזנת סתר לתקשורת בין מחשבים או חדירה למחשב, מהווים כלי שלטוני הכרחי, שמטרתו הראשונית הנה ההגנה על הביטחון, על החוק ועל הסדר החברתי. מבחינה זו, השימוש האינטנסיבי במערכות מחשבים ואופיין התיעודי הופכים אותן לאוצר בלום של ראיות מפלילות ומידעים מודיעיניים עבור רשויות השיטור. עם זאת, דיני חיפוש מקלים עלולים להוביל לפגיעה יתרה בחירויות אדם ואף לריכוז מידע רב ומיותר על היחיד.

ניתן להצביע על שלוש דרכים להשגת איזון ראוי בין הצורך החברתי בחיפוש מטעם הרשות המבצעת בכליו הממוחשבים של הפרט, לבין ההגנה על עקרון הסודיות: הדרך הראשונה נוגעת להתניית הליך החיפוש בבקרה משפטית ולהתנייתו בקבלת צו שיפוטי. כך תתאפשר בקרה אובייקטיבית של הצורך לחדור למרחבו הווירטואלי של הפרט ושל היקף החיפוש, אשר תהווה מחסום חיוני בפני חיפושים נמהרים ומיותרים[75] ובפני רדיפה שלטונית של האזרח. את המקרים שבהם לא יידרש צו חיפוש ראוי להגביל לסיטואציות יוצאות דופן, כגון כאלו שבהן נשקפת סכנה מידית וחמורה לחיי אדם ולרכושו.

הדרך השנייה להשגת האיזון הראוי בין ערך הסודיות במידע הממוחשב לבין הצורך בשמירה על החוק והסדר הנה אימוץ סף ראיות לכאורי גבוה לצורך קבלת צו חיפוש או האזנה. אין מקום לאפשר לרשויות החקירה לצאת ל"מסעות דיג" מפוקפקים שמא יעלו דבר מה בחכותיהן,[76] אלא צריך שתהיה תשתית ראייתית כדי להתיר פגיעה כה קשה בזכויות הפרט. כמו כן, כאשר מדובר בעברה קלה יחסית (עוון), יש לדרוש סף ראיות גבוה יותר להוכחת החשד ולהפך.[77,78]

---

75 ברע"א 1917/92 **סקולר נ' ג'רבי**, פ"ד מז(5) 764 (1993) נפסק, כי השאלה הראשונה שעל בית המשפט להשיב עליה היא **מידת החיוניות והחשיבות** של המידע שאותו מבקשים לחשוף.

76 ראו עמדת הנשיא (דאז) שמגר בע"פ 2286/91 **מדינת ישראל נ' אילוז**, פ"ד מה(4) 289, 297 (1991) (להלן: עניין **אילוז**), המציין כי "אין להתיר האזנה ללא בסיס ראשוני רק כדי לדוג אחר מידע. על השופט להשתכנע, על יסוד המידע המובא לפניו, שאכן יש צורך אמיתי בנקיטת האמצעי מרחיק הלכת של פגיעה בצנעת הפרט כדי למנוע עבירות או לגלות עבריינים".

77 בעניין **אילוז**, שם, נקבע כי "אופי העבירה הנחקרת משליך במישרין על שיקול הדעת, אם להתיר האזנה או לאו, וכי אין, למשל, להתיר האזנה לשם קידום החקירה בעבירות קלות, שמידת חומרתן איננה מצדיקה נקיטת אמצעי בעל אופי כה חמור". בדומה, בע"פ 1302/92 **מדינת ישראל נ' נחמיאס**, פ"ד מט(3) 309, 331 (1995) קבע השופט בך, כי על השופט הדן בבקשה להאזנת סתר "לבחון האם מדובר בחשד לביצוע עבירה חמורה" וכי יש לבחון דרכים חלופיות פחות חודרניות.

78 אם כי חיפוש גלוי במחשבים נעשה במעמד הנפגע ונציגו: ב"ש (מחוזי י-ם) 1153/02 **מדינת**

הדרך השלישית והחשובה ביותר להשגת איזון בין הצורך בשמירה על סודיות המידע לבין הצורך בהגנה על החוק והסדר נוגעת לחיזוקה של הבקרה השיפוטית על הליך החיפוש. הבקשות לצווי האזנת סתר (ובמידה פחותה בהרבה – לחיפוש במערכות מחשב) נעשות במעמד צד אחד – קרי, רק בהשתתפות השוטר המבקש את הצו מבית המשפט. כפי שהצעתי במסגרת דיוני הוועדה לתיקון פקודת סדר הדין הפלילי (חיפוש במחשבים) (2006–2007), יש להעביר את בקשת צו החיפוש לתגובתו של צד שלישי אובייקטיבי, **מעין סנגור ממונה מטעם בית משפט**, האמון על זכויות אדם וטכנולוגיה, אשר ייצג את האינטרסים של הנפגע בהיעדרו. גוף אובייקטיבי זה יגיב על הבקשה לחיפוש, יציג בפני השופט את האינטרסים העשויים להיפגע בשל מתן הצו המבוקש, ויצביע על דרכים חלופיות, פוגעניות פחות, לביצוע החקירה. כך תתאפשר בחינה מעמיקה של היקף הפגיעה בזכויותיו של החשוד ובאינטרסים החברתיים. יצוין כי ועדת החקירה הפרלמנטרית לנושא האזנות הסתר (ועדת חוקה, חוק ומשפט) שוקלת הצעה מעין זו כדי לחזק את מנגנוני הבקרה של הליכי מתן צווי האזנות הסתר.[79]

4.2 *צידוקים אזרחיים לחדירה פרטית למערכות מחשב*

אינטרסים **המצדיקים פגיעה בערך הסודיות** אינם נחלתו של גורמי שלטון בלבד, כי אם גם של **הפרט**. לאחרונה, למשל, גרמה בעקיפין הגנה יתרה על הסודיות למותו של אדם נכה, אשר קפא למוות במכוניתו שנתקעה בבוץ, לאחר שלא אותר במשך שעות הלילה. חברת איתוראן החזיקה במידע ממוחשב על אודות מיקום מכוניתו של הנכה, אך סירבה למסור פרטים אלו, בהיעדר פנייה מהמשטרה, וזאת, בהסתמך על חוק הגנת הפרטיות.[80] טרגדיה זו ממחישה את השלכותיה השליליות של הגנה יתרה על סודיות המידע הממוחשב, העלולה להוביל לפגיעה בדמים – למותו של נשוא המידע. בתורה בא לידי ביטוי איזון ראוי בין הצורך בהגנת סודיות המידע האישי והמסחרי, לבין צרכים תועלתניים אחרים – הגנה חברתית ואישית: מחד, הגנת סודיות המידע של הפרט מתבטאת בציווי "לא תלך רכיל בעמך" (ויקרא יט 16), ומאידך קיימת **חובה** להגן על גופו של אדם ורכושו, אף תוך פגיעה בעקרון הסודיות: "לא תעמוד על דם רעך" (שם).[81]

ישראל נ' אברג'יל, תק־מח 2(02) 3784 (2002).

79 שחר אילן "למרות הביקורת הקשה של הכנסת – עליה של 22% במספר האזנות הסתר ב – 2007" **הארץ** 19.2.2008, 7.

80 ראו: יגאל חי "מת מקור נכה שמכוניתו שקעה בבוץ ליד נתב"ג" **הארץ**, ניתן לצפייה בכתובת: www.haaretz.co.il/hasite/pages/ShArtPE.jhtml?itemNo=937004&contrassID=2&subContrassID=21&sbSubContrassID=0 (נבדק לאחרונה ב־11.1.2009).

81 על פי ההלכה היהודית, לפרט יש זכות שפרטי אמת עליו – בין סודיים, בין מעוררי שנאה (אף כי

ואכן, אל מול אינטרס סודיות המידע הממוחשב של בעליו מצויים, לעתים, האינטרסים המנוגדים של זולתו, ובכלל זה זכויות אדם, כגון הזכות לקניין (למשל, מניעת זליגת סודות מסחריים), והצורך להגן על חיי אדם שמידע אודותם נמצא במחשב הזולת ועוד.[82] לפיכך יש מקום להכיר בסייגים אזרחיים לאינטרס החשוב של הגנת הסודיות מפני חדירה למידע הממוחשב, ולאפשר איזון בין הצורך להגן על עקרון סודיות המידע הממוחשב, לבין צרכים מנוגדים של הפרט. ניטול לדוגמה מקרה של אדם שנתבע, והמידע שיכול לבסס את טענות ההגנה שלו נמצא בקובץ שיצר התובע, והמאוחסן במחשבו של הנתבע;[83] אמנם על פי תפיסה הזכות לסודיות במידע הממוחשב, הקובץ שייך לתובע שיצר אותו, ואולם ייתכן שלנתבע יש זכות לגיטימית להתגונן מפני תביעה משפטית בלתי מבוססת, על ידי חדירה למידע הממוחשב של הזולת הנמצא במחשבו הוא.[84] מסקנה זו מתחזקת לאור כך שהקניין במידע הערטילאי המאוחסן במחשב הזולת הנו קניין מוחלש, וזאת נוכח התבססותו על משאבים רכושיים השייכים לזולת – המחשב, אספקת החשמל, תכנות ההפעלה ועוד.

כמפורט להלן, את הסייגים האזרחיים לעקרון סודיות המידע הממוחשב ראוי להפעיל באמצעות התערבות שיפוטית של בתי המשפט או באמצעות עקרון העזרה

לא בהכרח מבזים) – לא ייחשפו, הן על ידי חיפוש במסתריו והן על ידי הפצתם לזולת (לפרוט ראו: אהרוני־גולדנברג, לעיל ה"ש 51). עקרון הסודיות נשמר מנימוקים של תועלת ציבורית ופרטית בכל הנוגע לערכים החשובים לחברה היהודית, כגון צניעות. מאידך, עקרון הסודיות מסויג בשל צרכים תועלתניים. מקור הסייג הוא בפסוק 'לא תעמוד על דם רעך'. "**דם**" מפורש בהקשר זה כמתייחס לדיני נפשות או לדמים – הפסד כספי. סייגים תועלתניים אחרים הם הצורך בלימוד תורה ובמניעת עברות. ראו גם עמדת הרמב"ם: "כל היכול להציל ולא הציל עובר על 'לא תעמוד על דם רעך', וכן הרואה את חברו טובע בים או לסטים באים עליו ויכול להצילו (יצילו) הוא בעצמו או שישכור אחרים" (הלכות רוצח ושמירת הנפש, פרק א', יד). וכן ראו ספר החנוך, פרשת קדשים, מצווה רלו: "אלא אם כן תהיה כונתנו לסלוק הנזיקין ולהשבית ריב". לגבולות הפעלת סעד ה־Mutual Help במקרים של פגיעה בסודיות, ראו: רבי ישראל הכהן מראדין (החפץ חיים, הלכות רכילות, כלל ט, סעיפים א־ב); שו"ת יחווה דעת לרב עובדיה יוסף (חלק ד', סימן ס'). כן ראו Ellie Spitz, *Pointers for American Legislation on Computer Privacy: Insights from Jewish Law*, 63 NATL JEW. L. REV. II, 77 (1986). עמדה מעניינת מביע גם הגר"ח פאלג'י בשו"ת חקקי לב, ח"א יו"ד סי' מ"ט בנוגע לשאלה האם שליח רשאי לפתוח מכתב אותו הוא מעביר, מתוך חשש שהמכתב מכיל מידע שיגרום לו נזק כלכלי. הרב קובע שבצד איסור כללי לפתיחת מכתבים של הזולת, מותרת פתיחת אגרת השייכת לזולת "**בכדי להציל את עצמו ולהיות מציל מידם**", כאשר מדובר בסיטואציה של "**דבר האבד**" – אפילו שמדובר באבדן כלכלי בלבד.

82 ראו בדומה, מיגל דויטש **קניין** חלק א 356 (1997), המציין כי אל מול אינטרס השימוש של אדם בקניינו מצוי אינטרס השימוש של שכנו בקניינו שלו. השימוש על ידי האחד, לעתים קרובות למדי יהא בו משום הפרעה לשימוש של האחר.

83 ראו בדומה פרשת **איסקוב**, לעיל ה"ש 50.

84 אך השוו לעמדת השופט אריאל בפרשת **גלעם**, לעיל ה"ש 42, המתייחס לסיטואציה יותר קיצונית מהנדונה.

העצמית.[85] ככלל, יש לאפשר פנייה של גורמים פרטיים לבית המשפט לקבלת צו חיפוש במחשבי הזולת (מעין "אבעיה" או מנגנון Pre-Ruling), שבמסגרתה יובאו לדיון האינטרסים המתנגשים עם עקרון סודיות המידע הממוחשב. בית המשפט יפסוק אם ליתן צו עשה, המתיר למבקש לחדור לחומר המחשב של זולתו, ובכך לפגוע בעקרון סודיות המידע הממוחשב, ואם לאו. כך, שעה שלמשל, תלויה ועומדת תביעת עובד כנגד מעביד, והמעביד חושב שחומר המחשב הנמצא במחשב שהוא סיפק לעובדו עשוי לסייע לו בהגנתו, יוכל המעביד לפנות לבית הדין, במעמד צד אחד, לקבלת צו עשה, המתיר חדירה לחומר המחשב של העובד. קבלת צו כמבוקש עשויה לשמש תעודת כשרות ולייתר טענות עתידיות בדבר פסלות הראיות שהופקו בדרך זו.

עם זאת, הפנייה לערכאות שיפוטיות לצורך קבלת צו המתיר חדירה למחשב הזולת כרוכה באבדן זמן יקר ובעלות גבוהה, ולעתים קרובות חיי היום־יום הופכים אותה ללא מעשית.[86] בשל סיבות אלו, מכיר המשפט בצורך לאפשר ליחיד לפגוע בחירויות זולתו בסיטואציות מסוימות, אף **ללא** התערבות של ערכאה שיפוטית, למשל, באמצעות סעד **העזרה העצמית** (Self Help) או עזרת הגומלין (Mutual Help). הפעלתם של סעדים עצמיים, אף שהנה חיונית במקרים רבים, עלולה להיות גם בעלת השלכות שליליות, שכן יש בה כדי לפגוע בחירות הפרט להשתמש במערכות מחשבים בסודיות, לצמצם את הריבונות השלטונית ולהוביל למעגל חוזר של התקפות והתקפות נגד.[87] לפיכך ראוי **לסייג את השימוש בעשיית דין עצמי**

---

85 **עקרון עשיית הדין העצמי** מוגדר כ"סיפוקה של דרישה, או הבטחה של דרישה, על ידי מעשה עצמאי של הדורש. הבחנו בין מושג זה ובין הגנה הפרטית אגב דוגמת התקיפה, לפי המבחן של מועד גמר ההתקפה. כלומר כל עוד נמשכת ההתקפה על זכויותיו של אדם, נחשבות פעולותיו למניעת פגיעה בגדר הגנה פרטית; הסתיימה ההתקפה בהצלחת המתקיף לשנות את המצב הקיים, הרי כל ניסיון של הנפגע להחזיר בכוחות עצמו את המצב לקדמותו הוא בבחינת עשיית דין לעצמו" – אהרן ברק **דיני הנזיקין – חלק כללי** 540 (מהדורה שנייה, גד טדסקי עורך, התשל"ז).

86 השופטת פרוקצ'יה מונה את יתרונות סעד העזרה העצמית – מהירות, יעילות וחיסכון בהוצאות וקובעת: "צרכי החיים מכתיבים היזקקות מוגבלת לשימוש בכוח עצמי כדי לשנות מצב עובדתי ומשפטי אולם הגבולות לכך בדרך כלל צרים ומוגדרים היטב" (רע"א 4311/00 **מדינת ישראל נ' בן שמחון, פ"ד** נח(1) 827, 838 (1993) (להלן: עניין **בן שמחון**). ראו אף ע"א 1226/90 **בנק לאומי נ' הסתדרות הרבנים דאמריקה, פ"ד** מט(1) 177, 202 (1995): "נכונות המשפט להכיר בתוקף המשפטי של סעדים מסוג ה'עזרה העצמית' מושתתת על אדני צדק והגינות". וראו גם עמדת השופט אלון בע"א 756/80 **רוזנשטיין נ' סולומון**, פ"ד לח(2) 113, 122 (1984): "התבססות מלאה של יישום שלטון החוק בחיי יום יום יכול שתביא עמה הקלה פורתא מקנאותה המופלגת של מערכת המשפט נגד עשיית דין עצמית, במקרים סבירים והולמים".

87 ראו עמדת השופטת פרוקצ'יה (עניין **בן שמחון**, שם, בעמ' 837): "ככלל, המשפט מסתייג מעשיית דין עצמית. חסרונותיה גלויים לעין, בראש ובראשונה מן הטעם שהתרתה מסכנת את שלום הציבור ואת הסדר הציבורי. היא עלולה לגרור למעשי אלימות בין בעלי־דין יריבים; היא

ולהפעילו במשורה ובהתקיים מרבית **הקריטריונים** הבאים, שאינם מהווים רשימה ממצה:

הפרט נזקק להגן באופן מידי על גופו או על רכושו מפני פגיעה, ואין באפשרותו לדחות את פעילותו עד לפנייה בבקשה להתערבות שיפוטית או משטרתית; הפנייה לרשויות אלו איננה אפשרית, יעילה או מעשית (המשטרה, למשל, אינה עוסקת בנושאים אלה; התמשכות הדיון המשפטי יפגום באפשרות מניעת הנזק); מדובר במצבי **הגנה** ולא התקפה (מגן ולא חרב); הסעד העצמי לא נעשה מתוך זדון, רצון להציק או לנקום; הצעדים שננקטו עומדים במבחן הסבירות, ואין מדובר במעשה קיצוני;[88,89] להתערבות העצמית סיכויי הצלחה גבוהים;[90] המידע שנאסף הנו רלוונטי;[91] והעזרה העצמית הובילה לפגיעה **נקודתית** בזולת ואיננה מהווה הפרה **שיטתית** של חירויות הזולת.

נותנת בידי בעל־דין את הכוח להעריך בעצמו את גבולות זכויותיו תוך סיכון שלא יעריכם נכונה". ראו ענין ת"פ (שלום ת"א) 4833/99 **מדינת ישראל נ' אייזק** (טרם פורסם, 13.2.2002). בעניין זה, המתלונן והנאשם גלשו ברשת האינטרנט, תוך שימוש בשמות כיסוי. בין השניים פרץ סכסוך ברשת. לטענת המתלונן, הנאשם גרם ל"העפתו" (ניתוקו) מהרשת בכל פעם שהתחבר אליה. בתגובה, המתלונן איתר את הנאשם, איכן את כתובתו וחשף את פרטי זהותו האמיתית ואת מספר הטלפון שלו. המתלונן ביקש מהנאשם פיצוי כספי על הניתוקים ועל השיבושים, שלדעתו הכניס למחשבו ושגרמו להשבתת המחשב. בעקבות כך, הנאשם וחבריו דקרו את המתלונן ופצעו אותו קשה.

88 גישה מעין זו באה לידי ביטוי בתמ"ש (משפחה י־ם) 010350/03 **ק.א. נ' ק.ג.**, תק־מש 2)05(143, 145 (2005), שם קבע השופט מרכוס, כי "אין זה ראוי לצפות מאדם המגלה חומר שעשוי לעזור לו בהתגוננות בפני תביעה שהוגשה נגדו, לפעול כאלטרואיסט ולהימנע מלעשות שימוש בחומר כדי לא לפגוע בבת זוגו לשעבר".

89 פרשת **פלונית**, לעיל ה"ש 49, עסקה בבעל שצילם את אשתו בנפרד בביתה, ללא רשותה וידיעתה, בהיותה עם גבר אחר, ונקבע כי "הפגיעה בפרטיותה של העותרת במקרה שלפנינו היא חריפה וקיצונית. המשיב פגע בגרעין הקשה של הזכות לפרטיות. הוא חדר – כשהוא מצוייד במצלמה מלווה בשני חבריו שצפו בכל המתרחש – למיטתה של העותרת. אין לך פגיעה קשה מזו בפרטיות. פגיעה זו היא מעבר לכל מידה ראויה". ניתן לאבחן פסק דין זה, המתייחס לחדירה לביתו – למרכז ההוויה הפרטית של האדם – מכניסה למחשבו, וזאת למרות היותו של המחשב המודרני קניין מכונן של הפרט. כן ראו עמדתו של הרב דייכובסקי, השואל: "אדם הנשוי לאשה ומגיעות אליו שמועות כי אשתו אינה נאמנה לו, וכתוצאה מכך אסורה עליו, האם אינו זכאי לברר את האמת? האם אין זו זכותו וחובתו של כל אדם לדעת את מצבו האישי שלו ושל בן הזוג הקשור עמו? המושג 'תום לב' משמעותו כי הדבר לא נעשה באופן שרירותי בכדי להציק או להכאיב לזולת, אלא נעשה בכדי לאמת או לשלול שאלה קיומית הנוגעת לאדם" (שם, דברי הנשיא דאז ברק, בעמ' 1748).

90 Jay P. Kesan & Ruperto P. Majuca, *Hacking Back: Optimal Use of Self-Defense in Cyberspace*, *in* SAFETY & SECURITY IN A NETWORKED WORLD (2005) ניתן למצוא באתר האינטרנט: www.oii.ox.ac.uk/microsites/cybersafety/?view=programme&&day=8&session ID=14 (נבדק לאחרונה ב־11.1.2009).

91 עניין **צוקרמן**, לעיל ה"ש 67.

ככלל, אף שהגנות העזרה העצמית משמשות כלי איזון בין הצורך בהגנה על סודיות המידע, ובין הצורך להגן על אינטרסים ראויים אחרים, הפעלתם כרוכה באי־ודאות לגבי המותר והאסור, דבר המעמיד בסימן שאלה את השימוש היעיל בהן. לפיכך, כאשר אין חשש מידי לנזק לחיי אדם או לרכוש, ראוי לפנות לבית המשפט לקבלת צו המתיר חדירה למחשבי הזולת.

כעיקרון, ההסכם הקיבוצי בין ההסתדרות ללשכת התיאום של הארגונים הכלכליים מאזן במידה ראויה בין אינטרס הגנת הפרטיות של העובד לבין האינטרסים המנוגדים של המעביד. האינטרסים של המעביד המוגנים בהסכם זה נוגעים לצורך לקבוע כללי שימוש במחשב, סילוק חומר שנפלט מהמחשב ופעולות ניטור ואחזקה שוטפות (סעיף 3.א להסכם);[92] וכן לצורך להתגונן מפני שימוש לא ראוי במחשב. כך, סעיף 3.ד. להסכם מאפשר למעביד לבדוק את שימוש העובד במחשב, שעה שהתקיימו נסיבות הנותנות לו סיבה סבירה להניח בתום לב, כי העובד עושה במחשב שימוש בלתי חוקי, או שימוש החושף את המעסיק לתביעות או שימוש שיש בו כדי לפגוע בעסק. בנוסף, כאשר מדובר בכניסה לקבצים אישיים של העובד, נדרשת הסכמתו המפורשת של האחרון.[93] חשיבותו הגדולה של ההסכם נובעת מכך שהוא מבהיר, במידה רבה, את האינטרסים העומדים על כף המאזניים ומכך שהוא מאפשר פגיעה בעקרון סודיות המידע הממוחשב רק כאקט הגנתי ונקודתי, ולא כפעולה שגרתית. עם זאת, דומתני, כי ראוי היה להביא בהסכם לידי ביטוי כמה עקרונות נוספים, אשר עליהם עמדתי לעיל: ראשית, המעסיק נזקק להגן על האינטרסים שלו באופן מידי, ואילו התערבות חיצונית של המשטרה או בתי המשפט איננה אפקטיבית או אפשרית בסיטואציה זו; שנית, לחדירה לקובץ המחשב של העובד יש סיכוי לתקן במידת מה את החשד שהתעורר (סיכויי ההצלחה של ההתערבות העצמית); והמידע שנאסף רלוונטי לבעיה שנתעוררה. בהערת אגב אציין, כי ההסכם אינו נותן מענה לאינטרס המעביד להתגונן מפני תביעה שהוגשה כנגד בעל המחשב, אף כי ייתכן שהחוק הקיים – חוק הגנת הפרטיות – דווקא מאפשר זאת (ראו סעיף 18(2) ג לחוק הגנת הפרטיות).

5. החלק התאורטי – לסיום

אופיו הערטילאי של עולם המחשבים המודרני מציב אתגרים רבים עבור המשפטן – במיוחד בנוגע לשאלת פריסתה הראויה של עברת החדירה למחשב. התשובה על שאלה זו הנה, כי האינטרס החברתי בהגנת מערכות המחשב מפני חדירה ונזקיה

92 בהקשר זה ראוי יהיה להבהיר את מהותן של אותן פעולות ניטור שוטפות ולוודא שאין בהן כדי לכלול מעקב שוטף אחרי פעולות העובדים במחשביהם.

93 ברי, כי את הסיפה לס' 3.ד. להסכם הקיבוצי ראוי לפרש כתנאי מצטבר לרישה של הסעיף.

הקשים של תופעת המחשוב הפולשני – מצריכים הגדרה רחבה של עברת החדירה למחשב, שתכלול את היסודות הבאים: הגדרה רחבה של המונח "מחשב", אשר תביא לידי ביטוי את הפונקציות המגוונות שהוא ממלא (כלי חישוב, כלי תקשורת, כלי שליטה ובקרה וכו'). כמו כן, האובייקט שעליו ראוי להגן בחוק מתפרש גם על המידע הממוחשב, ולא רק על המחשב הפיזי. מידע מוגן זה יכול להיות סתמי, ולאו דווקא בעל ערך כלכלי, רגשי או ספרותי. היסוד האחרון נוגע לרכיב ההסכמה; הסכמתו של בעל המידע הממוחשב הסגור במחשב (לא באתר פתוח לציבור) היא שמסמנת את קו הגבול של הטריטוריה הממוחשבת. יישום תפיסה זו יועיל לחברה מהבחינה הכלכלית והתרבותית ואף יענה על יסודות הומניסטיים חשובים: הזכות לפרטיות, לחופש הביטוי, לקניין ולאוטונומיה.

עם זאת, ראוי לאזן את הזכות לסודיות המידע הממוחשב עם צרכים תועלתניים וחירויות אדם אחרות. בהקשר הציבורי, מדובר בצורך הקיומי בשמירת הביטחון, החוק והסדר, שמכוחו ניתן להתיר חיפוש שלטוני בכליו של הפרט. צורך זה יש להפעיל במשורה, וזאת כדי למנוע פגיעה יתרה בחירויות אדם, ולפיכך הוצע לאמץ שלושה מנגנוני איזון: הכפפת הליך החיפוש לבקרה משפטית, העלאת סף הראיות והפעלת סנגור ממונה בדיונים הנוגעים לבקשות חיפוש המתבצעים במעמד צד אחד.

בהקשר **האזרחי**, ראוי להתיר במקרים מסוימים חדירה פרטית למחשב. ככלל, הדבר ייעשה במסגרת שיפוטית, שבה ייבחנו האינטרסים המנוגדים. שעה שהדבר אינו מעשי או פרקטי, יש מקום להפעלה **במשורה** של סעד עשיית דין עצמי, וזאת, בהתקיים קריטריונים מסייגים, לרבות הצורך בהגנה **מידית** על גוף או רכוש מפני פגיעה. אמנם מצב זה יוצר חוסר שוויון מסוים, שכן החיפוש השלטוני מוגבל בצו שיפוטי, ואילו סעד העזרה העצמית אינו מוגבל – ואולם יש לזכור כי החיפוש השלטוני מסוכן יותר, בהיותו ריכוזי ועוצמתי.

ג. חדירה למחשב אל מול האזנת סתר – הדין הקיים

בישראל קיימות שתי הוראות חוק עיקריות המסדירות את נושא היירוט והחדירה אל מידע ממוחשב: חוק המחשבים וחוק האזנת סתר (ובמידה מסוימת גם סעיף 2 לחוק הגנת הפרטיות). בחוק המחשבים נאסרה חדירה למידע ממוחשב ("חומר מחשב") המאוחסן במחשב (סעיף 4 לחוק), ואילו בחוק האזנת סתר נאסרה האזנה – קליטה של תקשורת בין מחשבים, המכונה "שיחה" (סעיף 2(א) לחוק). בחלק זה של המאמר תנותחנה הוראות חוק המחשבים וחוק האזנת סתר, תוך ניסיון ליישמם בסיטואציות שונות של מחשוב פולשני.

יצוין כי קו הגבול בין שתי הוראות אלו אינו ברור וכי בתי המשפט[94] והפרקליטות

94 פרשת **נטוויז'ן**, לעיל ה"ש 31; בש"פ 6703/00 **נטוויז'ן נ' צבא ההגנה לישראל** (לא פורסם,

התלבטו רבות בניסיון לתחם את הגבול שבין חדירה למחשב, מחד, והאזנת סתר, מאידך, וכך הגיעו לתוצאות שונות וסותרות. ענין **בדיר**[95] עסק בחדירה למערכת תא קולי ממוחשב (להלן: "קולן")[96] ובהאזנה שלא כדין להודעות שהושארו בו. הנאשם הורשע גם בעברה על סעיף 2 לחוק האזנת סתר וגם בעברה על סעיף 4 לחוק המחשבים. בדיון בערעורו של **בדיר** בבית המשפט העליון[97] זוכה הנאשם, בהסכמת הפרקליטות, מעברה על סעיף 2 לחוק האזנת סתר, ושוחרר על אתר ממאסרו.[98,99] בעניין זה השאיר בית המשפט העליון ב"**צריך עיון**" את המענה לשאלה: האם חדירה למערכות מחשב וקריאת מסר תקשורת שכבר התקבל בו, מהווה עברה על סעיף 4 לחוק המחשבים או עברה על סעיף 2 לחוק האזנת סתר? היעדר הכרעה משפטית זו הוביל לערפל בנוגע לדין הקיים ואף לפסילת ראיות שהושגו בחיפוש במערכות מחשב. כך, למשל, במסגרת חקירת פרשת הסוס הטרויאני הורה פרקליט המדינה להפעיל את הליכי החיפוש במחשבים מכוח הפקודה, ולא מכוח חוק האזנת סתר; אך בית המשפט המחוזי בפרשת **פילוסוף**[100] **פסל את הראיות** שהופקו בדרך זו, תוך יישומה של דוקטרינת פרי העץ המורעל.

1. הדמיון והשוני בין חוק המחשבים לבין חוק האזנת סתר

מקור אי־ההבנה בנוגע לתחולת שני הסעיפים (סעיף 4 לחוק המחשבים וסעיף 2 (א) לחוק האזנת סתר) נובע מכך, שלכאורה ישנה הקבלה בין היסוד ההתנהגותי של עברת החדירה למחשב לעברת האזנת סתר וכן בשל החפיפה הנובעת מדרישת יסוד ההסכמה הקבועה בשתי עברות אלו; בחוק האזנת סתר יסוד **ההסכמה** מנוסח באופן

6.4.2000); פרשת **בדיר**, לעיל ה"ש 1; ערעור **בדיר**, לעיל ה"ש 8; ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף**, תק־מח 2007(4) 9542 (2007). (להלן: עניין **פילוסוף**).

95 פרשת **בדיר**, לעיל ה"ש 1, פרט אישום 43 (פרשת "ברק"). בענין **בדיר**, שם, נקבע, כי חדירה לתא לקולי ממוחשב באמצעות הטלפון והאזנה להודעה קולית שהוקלטה בתא הקולי מהווה עברה על ס' 2 לחוק האזנת סתר. מהעובדות המפורטות בהכרעת הדין אין זה ברור אם היה מדובר בהודעה קולית שכבר נמשכה על ידי בעל התא הקולי, או כזו שממתינה למשיכתה בתחנת ביניים – במרכזיית התקשורת של חברת בזק. כמפורט להלן, לשאלה זו יש משמעות משפטית רבה.

96 בפרשת **בדיר**, לעיל ה"ש 1, בעמ' 1841 מגדיר בית המשפט מערכת קולן, כ"מערכת מענה קולי (ומכונה לעתים "דואר קולי", "תא קולי" או "תיבה קולית") – I.V.R, אוטומטית, אינטראקטיבית, המספקת למתקשר שירותי מסרים קוליים, ומופעלת באמצעות מכשיר הטלפון".

97 ערעור **בדיר**, לעיל ה"ש 8.

98 שם.

99 אציין, כי בדיון בערעורו של **בדיר** בבית המשפט העליון (שם) בוטלו בהסכמה ההרשעות בעבירות האזנת סתר להודעה קולית שהוקלטה בתא קולי (אישומים 31, 43 ו – 15).

100 עניין **פילוסוף**, לעיל ה"ש 94.

מפורש,[101] ואילו בחוק המחשבים הוא מתבטא במונח המפתיע בהקשר זה — "שלא כדין".[102] כך שלכאורה, במצבים מסוימים אותה פעילות יכולה לבוא בגדר שני החוקים, למשל כשמיורט מידע ממוחשב, הנמצא בתחנות מעבר או בשלבי הביניים (קליטת דואר אלקטרוני, הנמצא על שרת של ספק שירות אינטרנט (להלן: גם "ISP" — Internet Service Provider) או כשנעשית חדירה למחשב הנמצא בתהליך של קבלת מידע (חדירה סימולטנית לקבלת מסר בזק).

לדעתי, למרות הדמיון הרב בין סעיף 2(א) לחוק האזנת סתר ובין סעיף 4 לחוק המחשבים, לא ניתן להפעילם במקביל, וזאת משתי סיבות: האחת, שהסיפה לסעיף 4 לחוק המחשבים קובע כי שעה שמבוצעת חדירה למחשב שהיא גם האזנת סתר, לא יחול סעיף 4; והשנייה — שלכל אחד מהחוקים ישנה פרוצדורות חיפוש שונה.[103] להלן תיבחנה לעומק שתי טענות אלו.

1.1 אי־תחולה מקבילה: הסיפה לסעיף 4 לחוק המחשבים

סעיף 4 לחוק המחשבים (חדירה לחומר מחשב שלא כדין) קובע:

> "החודר שלא כדין לחומר מחשב הנמצא במחשב, דינו — מאסר שלוש שנים; לענין זה, 'חדירה לחומר מחשב' — חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר".

מלשון הסעיף עולה, שחדירה למחשב יכולה להתבצע בשלוש דרכים: התקשרות עם מחשב, התחברות למחשב והפעלת המחשב. בסיפה לסעיף 4 הודגש, שחדירה לחומר מחשב אינה יכולה להיות חדירה המהווה האזנת סתר: "**אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר**" (ההדגשה שלי — ש.א.ג.). פשיטא אפוא מלשון הסיפה לסעיף 4 לחוק המחשבים, **שחדירה למידע ממוחשב הבאה בגדר עברת האזנת הסתר, אינה יכולה להיות עברת חדירה למחשב**. מסקנה זו מתיישבת גם עם **ההיסטוריה החקיקתית** של חוק המחשבים, שממנה עולה, שככלל, חוק זה אינו נוגע

---

101 "האזנת סתר" מוגדרת בס' 1 לחוק האזנת סתר כ"האזנה ללא הסכמה של אף אחד מבעלי השיחה".

102 כמפורט בה"ש 127 להלן.

103 למרות הדמיון הרב שבין שתי עברות אלו, קיים בינן גם שוני רב המתבטא בשתי נקודות עיקריות: השוני האחד נובע מ**רמות ענישה שונות**: עברה על ס' 4 לחוק המחשבים, דינה מאסר שלוש שנים, ואילו עברה על ס' 2(א) לחוק האזנת סתר – דינה מאסר חמש שנים. השוני השני מתבטא בתחולה שונה של דוקטרינת פרי העץ המורעל.

לתקשורת בין מחשבים.[104] ואמנם, מחוק המחשבים הוצאו הגדרות והוראות הנוגעות לקווי תקשורת ולהאזנת סתר, והם תוקנו ישירות בחוק האזנת סתר.[105]

הואיל וחדירה למחשב אינה יכולה להיות במקביל גם האזנת סתר, **לא ניתן להרשיע נאשם גם בהאזנת סתר וגם בחדירה למחשב.** ואולם, בפרשת **מדינת ישראל נ' בדיר**,[106] הורשע הנאשם, שחדר לתא קולי ממוחשב והאזין להודעה קולית שהוקלטה בו על ידי מתקשר אחר, **במקביל**, גם בעבירה על סעיף 4 לחוק המחשבים וגם בעבירה על סעיף 2 לחוק האזנת סתר, וזאת בהתעלם מהסיפה לסעיף 4.[107] בדומה, בפרשת **פילוסוף**, שם היה מדובר בתכנה שאפשרה לצפות בכל הקבצים במחשב הנגוע,[108] הורשעו הנאשמים, גם בעבירה על סעיף 4 וגם בעבירה על סעיף 2(א) לחוק האזנת סתר, אם כי מיעוט העובדות המפורטות בפסק הדין אינו מאפשר לשפוך אור על שיקולי הרשעה כפולה זו.

---

104 בדברי ההסבר לס' 6 לטיוטת חוק המחשבים (לא פורסמה), נאמר כי: "התקשרות או התחברות לתקשורת בין מחשבים לא תהיה בגדר חדירה לפי סעיף זה, אולם היא תהיה האזנה, אשר יחולו עליה דיני האזנת סתר". למעמדה של ההיסטוריה החקיקתית ככלי פרשני, ראו אהרן ברק **פרשנות בחקיקה** כרך שני 369—372 (1994).

105 מנוסחו הסופי של החוק נגרעו סעיפים 6—6-15 להצעת חוק המחשבים, אשר התייחסו ל"**מערכות תקשורת בין מחשבים**", ל"**דרכי תקשורת בין מחשבים**" ול"**קווי המסר המחברים בין המחשבים בעולם כולו**" (לאינטרנט). כמו כן, הוצאת המונח "מערכות התקשורת המחוברות" אל המחשב מהגדרת "מחשב" בנוסחו הסופי של חוק המחשבים מהווה הסדר שלילי שמטרתו להוציא מגדר החוק את האינטרנט כרשת תקשורת. לדעתי, במונח "מערכות התקשורת המחוברות" למחשב הכוונה הנה לקווי תקשורת המחוברים למחשב, ולא לאמצעי תקשורת כגון מרכזיה או מכשיר קולן ממוחשבים. למסקנה זו ניתן להגיע גם מעיון בדברי ההסבר לס' 11 בהצעת חוק המחשבים, התשנ"ד—1994, ה"ח 2278 (להלן: "הצעת חוק המחשבים"), נקבע: "חדירה לחומר מחשב... יראו אותן כחיפוש. (ג) קבלת מידע מתקשורת בין מחשבים אגב חיפוש לפי סעיף זה לא תיחשב כהאזנת סתר לפי חוק האזנת סתר". בדברי ההסבר לס' 31א להצעת חוק המחשבים נאמר: "במחשבים בעלי מערכות תקשורת תיתכן קליטה של חומר חדש המתקבל במחשב בזמן החיפוש. אף שיש בזה מרכיב התנהגותי של האזנת סתר, מוצע להבהיר שחומר שנקלט כאמור תוך ביצוע צו חיפוש אינו כפוף להוראות חוק האזנת סתר, המחייב קבלת צו מיוחד כדי לבצע את האזנת הסתר". ס' 11 לחוק המחשבים הוא היוצא מן הכלל (חריגים לענייני חיפוש ותפיסה של חומר מחשב), המעיד על הכלל: כאשר אדם פרטי חודר למחשב הנמצא בהליך של קבלת תקשורת מחשבים המדובר בהאזנת סתר ולא בחדירה למחשב. מאידך, כאשר גוף חקירה חודר למחשב מכוח צו ובמהלך החיפוש מתקבל מסר אלקטרוני, חל החריג הקבוע בס' 11. אך השוו לעמדת בית המשפט המחוזי בעניין בפרשת **בדיר**, לעיל ה"ש 1, בעמ' 12—13 להכרעת הדין.

106 פרשת **בדיר**, שם, אישום מספר 43.

107 החלטה זו, ככל שהיא נוגעת להרשעה בהאזנת סתר, בוטלה **בהסכמה** במסגרת ערעור **בדיר** לבית המשפט העליון, לעיל ה"ש 8, ונותרה על כנה ההרשעה בעברת החדירה למחשב כדי לעבור עברה אחרת (ס' 4 ו־5 לחוק המחשבים).

108 הכרעת הדין בת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף**, תק־מח 2007 (3) 12198, פס' 4 (2007) (להלן: הכרעת הדין בענין **פילוסוף**).

1.2 אי־תחולה מקבילה: הוראות החיפוש השונות בשני החוקים

הסיבה השנייה לכך ששתי העברות (חדירה למחשב והאזנת סתר) אינן יכולות לחול במקביל ושיש צורך להבהיר את תחולתן נובעת מהוראות **דיני החיפוש** השונות, שאותן יש להפעיל בכל אחד מהחוקים: הליכי חיפוש שלטוני **במחשב** מוסדרים בפקודת סדר הדין הפלילי, ובמיוחד בסעיף 23א, ואילו ההליכים לקבלת צו **האזנת סתר** לתקשורת בין מחשבים מוסדרים בחוק עצמו. קבלת צו חיפוש על פי החוק הלא נכון עלולה **לפסול את הראיות שהושגו בדרך זו** מחמת דוקטרינת פרי העץ המורעל.[109] ואכן, כאמור, במסגרת חקירת פרשת הסוס הטרויאני הורה פרקליט המדינה לקבל צו חיפוש על פי הפסד"פ לצורך יירוט של תכתובת אלקטרונית שטרם הגיעה ליעדה מהשרת של ספק השירות, ולא על פי חוק האזנת סתר,[110] אך בית המשפט המחוזי[111] **פסל את הראיות** שהופקו בדרך זו, הואיל והן הופקו על פי הליך חיפוש שגוי.

2. קו הגבול בין חדירה למחשב לבין האזנת סתר – הדין הקיים

כדי ליתן מענה לשאלה מתי חל סעיף 4 לחוק המחשבים ומתי – סעיף 2(א) לחוק האזנת סתר, נבחן את המצבים העובדתיים השונים שבהם ניתן להפעיל את שני החוקים בכל הנוגע למערכות מחשבים. לצורך כך **נמשיל את התקשורת בין המחשבים למסע**, שתחילתו בכתיבת מסר אלקטרוני במחשב א'; המשכו בשליחתו למחשב ב'; וסיומו בהגעתו ליעד – למחשב ב'; כשבכל אחד משלבי המסע ניתן ליירט את המסר המועבר:

בשלב הראשון, נכתבת **הטיוטה** במחשב. טיוטא זו, כמו כל מידע ממוחשב אחר, מאוחסנת במחשב;

בשלב השני, **המסר נשלח** בקווי התקשורת הפנימיים המחברים בין המחשב לקווי התקשורת החיצוניים;

בשלב השלישי, **עובר המסר** בין השרתים השונים של ספקי האינטרנט;

בשלב הבא, **המסר מתקבל** במחשב היעד;

לבסוף, **המסר נשמר במחשב** היעד ומאוחסן בו.

---

109 ס' 13 לחוק האזנת סתר, פרק ד' – דיני ראיות.

110 יצוין כי לתביעה הכללית ישנם שני כובעים בכל הנוגעים להפעלה וליישום של חוק המחשבים וחוק האזנת סתר: האחד – של מאשימה, ובמובן זה עדיף, מבחינתה, להרשיע נאשמים בעברה על חוק האזנת סתר, וזאת בשל רמת הענישה הגבוהה הקבועה בו. והכובע השני – של מי שמייצגת את רשויות הביטחון והשיטור (המשטרה, השב"כ) ובתפקיד זה תועדף הפעלתו של חוק המחשבים, שבו מופעלת דוקטרינה מצומצמת יותר של דוקטרינת פרי העץ המורעל.

111 עניין **פילוסוף**, לעיל ה"ש 94.

ננסה ליישם להלן את יסודות שני החוקים – חוק האזנת סתר וחוק המחשבים – בכל אחד משלבי המסע הווירטואלי של ההודעה האלקטרונית.

2.1 שלב הטיוטה – יירוט המידע הנמצא במחשב

בסעיף זה תיבחן תחולתם האפשרית של שני סעיפי חוק – סעיף 4 לחוק המחשבים וסעיף 2(א) לחוק האזנת סתר – בכל הנוגע ליירוט מידע המאוחסן במחשב. כמפורט להלן, במקרה כאמור יחול סעיף 4 לחוק המחשבים ולא סעיף 2 (א) לחוק האזנת סתר.

2.1.1 יירוט המידע הנמצא במחשב: תחולת עברת החדירה למחשב

כאשר מבוצעת כניסה למידע ממוחשב הנמצא במחשב, ללא הסכמת בעל המידע, מתקיימים יסודותיה של עברת החדירה למחשב. זוהי עברה התנהגותית, שאינה דורשת הוכחת נזק. הואיל ולא מצוין בין מרכיבי העברה יסוד נפשי כלשהו, הרי שבהתאם לסעיפים 19 ו־20 לחוק העונשין, מדובר ב"עברה שותקת" הדורשת הלך נפשי מסוג "מחשבה פלילית" (מודעות לעובדות ולנסיבות).[112] המונח "מחשב"[113] פורש בצורה רחבה וראויה בפרשת **בדיר**,[114] שם נקבע כי הוא כולל גם מרכזיית טלפון ממוחשבת וגם מענה קולי ממוחשב – קולן.[115,116] פרשנות זו פותחת פתח ליישום

---

112 ס' 19 לחוק העונשין, התשל"ז–1977 (תיקון מס' 39, פורסם ביום 23.8.1994 ונכנס לתוקף ב – 23.8.95) חל על חוק המחשבים, אשר נכנס לתוקף אחריו (נתקבל ב – 17.7.95, פורסם בשנת 1995 בס"ח התשנ"ה, 366 ונכנס לתוקף שלושה חודשים מיום פרסומו). הסעיף קובע את הכלל שלפיו: "אדם מבצע עברה רק אם עשאה במחשבה פלילית, זולת אם – (2) העברה היא מסוג העברות של אחריות קפידה". על פי ס' 22 (א) לחוק העונשין, "אדם נושא באחריות קפידה בשל עברה, אם נקבע בחיקוק ... שהעברה אינה טעונה הוכחת מחשבה פלילית או רשלנות" – היינו, יש צורך בקביעה מפורשת שמדובר באחריות קפידה. לפיכך, בהיעדר הוראה מפורשת להלך נפשי או לכך שמדובר בעברה שאינה טעונה הוכחת מחשבה פלילית או רשלנות, הרי שההלך הנפשי הנדרש בס' 4 לחוק המחשבים הוא של **מחשבה פלילית**. ראו גם מיגל דויטש "חקיקת מחשבים בישראל" **עיוני משפט** כב 427, 436 (1999) ופרשת **בדיר**, לעיל ה"ש 1. אך השוו לנעמי אסיא **דיני מחשבים – הלכה למעשה** כרך ב 213 (מהדורה שנייה, 1999) ולהחלטת בית משפט השלום בפרשת **מזרחי**, לעיל ה"ש 54, שם נקבע, כי הואיל ולא הייתה לנאשם **כוונה** לחדור למחשב, אלא רק לבדוק את רמת האבטחה של האתר, מעשיו אינם בגדר העברה. מסקנה משפטית זו הושארה בצריך עיון בע"פ (מחוזי י־ם) 8333/04 **מדינת ישראל נ' מזרחי** תק־מח 04(3) 4821 (2004).

113 כמוגדר בס' 1 לחוק המחשבים.

114 פרשת **בדיר**, לעיל ה"ש 1.

115 נקבע בפרשת **בדיר**, שם, כי מרכזיית טלפון מהווה "מחשב" הואיל והיא פועלת באמצעות תוכנה והואיל והמחשב מהווה חלק מהותי, הנדרש להפעלתה של מרכזיית תקשורת מודרנית.

החוק, לא רק על מחשבים קלאסיים, המשמשים כלי חישוב, אלא גם על מחשבים המפעילים פונקציות נוספות, כגון כלי תקשורת וכו'. כך ניתן מענה חקיקתי ראוי למגוון הפונקציות שממלא המחשב בחברה המודרנית.

סעיף 4 לחוק המחשבים נוגע ל"חדירה לחומר מחשב הנמצא במחשב". "חומר מחשב", כהגדרתו בסעיף 1 לחוק המחשבים, מורכב מ"מידע" ומ"תכנה".[117] עולה שסעיף 4 לחוק המחשבים פורש הגנה רחבה וראויה על המידע הממוחשב, שכן הוא חל על כל סוג של מידע ממוחשב (ולא על פלט), ללא קשר לאופיו ולחשיבותו – ללא הגבלה למידע אישי, מסחרי או תקשורתי. חומר המחשב שאליו בוצעה החדירה יכול לכלול טיוטת דואר אלקטרוני או כל מידע אחר המאוחסן במחשב.[118] הביטוי "חדירה לחומר מחשב הנמצא במחשב" מלמד שעל חומר המחשב להיות מאוחסן במחשב ובמצב נייח. למסקנה זו מובילה גם הגדרת "מידע" בסעיף 1 לחוק המחשבים, המתייחסת לנתונים "מאוחסנים". כך, למשל, טיוטת דואר אלקטרוני המאוחסנת במחשב מהווה "חומר מחשב". מכאן, שככלל, קליטת מידע הנמצא בהליכי זרימה, למשל לצורך תקשורת בין מחשבים, אינה יכולה לבוא בגדר סעיף 4 לחוק המחשבים, שכן המידע אינו בגדר "מאוחסנים" ואינו "נמצא במחשב", אלא במצב נייד – בדרכי תקשורת בין מחשבים.

בית המשפט קבע, כי תפקידו של המחשב במרכזייה (שולי או עיקרי) אינו משנה את הגדרתה של המרכזיה כמחשב וכי אפילו אם המחשב רק מסייע לעבודה של המרכזיה, היא עדיין באה בגדר הגדרת "מחשב", שכן התוכנות שבמחשב המרכזיה הן שאפשרו את ביצוע החדירה אליה. עוד נקבע, כי **בדיקה פונקציונלית** של הקולן מלמד, כי המחשב שבקולן איננו בבחינת "מחשב עזר" כהגדרתו בס' 1 לחוק המחשבים, וכי יש לו תפקיד משמעותי, אשר אינו מתמצה רק בביצוע פעולות אריתמטיות; המחשב שבקולן מפעיל אותו, וכמו כן החדירה אליו מתאפשרת ממרחק, בשל היותו מחשב.

לדעתי, חשיבותו של המחשב במכשיר שאליו בוצעה החדירה איננה מהווה אחד מיסודות הגדרת "מחשב" או "מחשב עזר". כדי לבחון את עובדת היותו של מכשיר אלקטרוני בבחינת "מחשב", המבחן אותו ראוי לאמץ הנו **מהותי**, ולא פונקציונלי, ולהיעשות לאור הגדרת עברת החדירה למחשב; רק כאשר נעשית הפעלה של המחשב במכשיר המשולב מתקיימת העברה. לעומת זאת, מי שמפעיל מכשיר משולב (כמו מטוס, שמשולב בו מכשיר ניווט ממוחשב) **מבלי** להפעיל את חומר המחשב שבמכשיר המשולב **איננו** חודר למחשב; פעולתו מהווה חדירה למחשב רק כאשר מופעל החלק הממוחשב במכשיר המשולב.

116 ראו עמדת בית המשפט המחוזי בת"פ (מחוזי י־ם) 2077/06 **מדינת ישראל נ' אריש**, תק־מח 2007(4) 10862 (2007) (להלן: עניין **אריש**), שלפיה קיים דמיון רב בין מחשב לבין טלפון סלולרי, מבחינת הרציונל בבסיס הדין המיוחד למחשבים, מבחינת המידע המאוחסן בהם ודרך פעולתם. ואמנם גישה זו הנה ראויה, שכן יש להתרחק מהגישה שלפיה "מחשב רגיל" הנו המחשב הביתי, עם צג ומקלדת.

117 "**מידע**" מוגדר בסעיף זה, כ"נתונים, סימנים, מושגים או הוראות, למעט תוכנה, המובעים בשפה קריאת מחשב".

118 "חומר המחשב" בהקשר זה יכול לכלול את רשימת הקבצים המאוחסנים במחשב, קובץ מסוים או דואר אלקטרוני.

מסעיף 4 לחוק המחשבים ניתן ללמוד על **שלוש דרכי "חדירה למחשב"**, המהוות חלק מהעברה: א. התקשרות עם מחשב;[119,120] ב. התחברות למחשב;[121] ג. הפעלת המחשב. כלומר, הסעיף אוסר חדירה לחומר המחשב הנמצא במחשב, על ידי הפעלתו של חומר המחשב הנמצא במחשב, והחדירה יכולה להיעשות, הן ממרחק והן ישירות. הפרשנות הראויה של המונח "הפעלה" כוללת, לא רק את הפעלתו ממצב של Off ל־On,[122] אלא גם הפעלה של פונקציה מסוימת במחשב – הפעלה של חומר המחשב. עמדה זו נסמכת על לשון החוק, אשר איננה מתייחסת ל"חדירה למחשב", אלא לחדירה (הפעלה) של חומר המחשב הנמצא במחשב.[123] מכאן שפתיחת קבצים סגורים במחשב דולק ללא הסכמה באה בגדר היסודות ההתנהגותיים של עברת החדירה למחשב.[124,125]

119 התקשרות למחשב נעשית על ידי תקשורת נתונים בין מחשבים ממרחק, ראו עניין **טננבאום**, לעיל ה"ש 1, התקשרות טלפונית באמצעות טלפון וללא מחשב ובפרשת **בדיר**, לעיל ה"ש 1; עניין **שפירא**, לעיל ה"ש 4; עניין **רפאלי**, לעיל ה"ש 4, וכן התקשרות טלפונית באמצעות טלפון וללא מחשב. בפרשת **בדיר**, לעיל ה"ש 1, מתוארת חדירה למחשבים המבוצעת באמצעות טלפון וקו טלפון מבלי שה־Phreacker עושה שימוש במחשב (עברות טלפוניה). כעולה מפרשה זו, ההתקשרות האסורה כוללת: התקשרות למרכזיית טלפונים ממוחשבת באמצעות מכשיר טלפון, לחיצה על ספרות מסוימות וקבלת קו חיוג חיצוני; התקשרות למרכזיית טלפונים ממוחשבת והגדרת תיבה קולית; התקשרות לקולן והקשבה להודעות שהוקלטו בו ועוד.

120 ייתכן שהיה מקום להגדיר חדירה למחשב בצורה צרה יותר, אשר לא תכלול גם התקשרות לגיטימית עם המחשב, כגון שליחתמיילים ותפחית את הערפול המשתמע מכך. כך, הגדרה ראויה שאולי תהיה ראויה יותר ל"חדירה למחשב" הנה שליטה על פעולות המחשב.

121 ייתכן שבמונח "התחברות" הכוונה היא לחיבור מכשירים חיצוניים למחשב, כגון מודם המשגר אותות מהמחשב הנחדר למכשיר הקולט אותות אלו.

122 בענין **בדיר** (פרשת ערוץ הקניות), לעיל ה"ש 1, נפסק בהערת אגב, שחדירה למחשב יכולה להתבצע גם בהפעלתו של המחשב על ידי חיבורו לזרם החשמל והדלקתו.

123 ראו גם דויטש, לעיל ה"ש 82, בעמ' 442. דויטש, ממחוקקי חוק המחשבים, מציין כי "הגדרת החדירה האסורה היא 'חדירה לחומר מחשב הנמצא במחשב'; לכן היא כוללת מצבים בהם אדם (כגון עובד), היה מורשה לחדור למחשב, אך חדר לקובץ מסוים אליו לא הורשה לחדור". בכמה מקרים הורשעו עובדים ומורשי גישה למחשב בעברת חדירה למחשב בכמה תיקים. ראו למשל: ת"פ (שלום ת"א) 7343/03 **מדינת ישראל נ' נגרין**, תק־של 2004(1) 23216 (2004); ת"פ (שלום ת"א) 5887/05 **מדינת ישראל נ' בזרוקוב**, תק־של 2006(3) 4343 (2006).

124 עולה שס' 4 לחוק המחשבים נפרש על מגוון רב של טכנולוגיות חדירה לחומר מחשב הנמצא במחשב, אך כי טכנולוגיות פולשניות המוגבלות לקליטתו של המידע הממוחשב – ללא חדירה אליו, אינן באות בגדרו. ישנה אפשרות טכנולוגית לנטר את הקרינה האלקטרומגנטית הנפלטת ממצג המחשב, ממקלדת המחשב, ממנוע המחשב או מהמדפסת. מלשון ס' 4 לחוק המחשבים עולה, שניטור הקרינה האלקטרומגנטית איננו מהווה עברה על הסעיף, שכן: **קרינה אלקטרומגנטית** אינה "חומר מחשב"; היא אינה נמצאת במחשב; ואין בניטורה "הפעלת המחשב", "התקשרות" או "התחברות" אתו, אלא רק קליטה של מידע חיצוני למחשב.

125 חדירה לחומר מחשב הנמצא במחשב כדי לעבוד עברה אחרת אסורה על פי ס' 5 לחוק המחשבים. ליישום הסעיף ראו: ת"פ (שלום חי') 4888/02 **מדינת ישראל נ' לרמן**, דינים שלום

סעיף 4 מתייחס לחדירה "שלא כדין לחומר מחשב הנמצא במחשב". כאמור, פירושו המפתיע של המונח "שלא כדין" בחוק המחשבים, הנו בין היתר – **"ללא הסכמה"** או **"ללא הרשאה"**.[126] כך שהמונח "שלא כדין" בעברת החדירה למחשב הופך את הסכמתו של בעל חומר המחשב לגדר וירטואלית, שרק היא יכולה להכשיר את הגישה אל חומר המחשב. פירוש לא שגרתי זה יוצר חוסר בהירות באשר ליסוד קריטי זה, ודומתני, כי לצורך הבהירות, ראוי לכלול את יסוד ההסכמה מפורשות בחוק – בדומה למצב הקיים בחוק הגנת הפרטיות ובחוק האזנת סתר. סעיף 4 לחוק המחשבים אינו קובע מסמרות בשאלה **מי** יכול לתת את הסכמתו כדין לחדירה לחומר המחשב, ואין בחוק התייחסות **לבעלות הקניינית** במחשב שאליו מבוצעת החדירה, שכן המחוקק מסתפק בקביעה הכוללנית שלפיה העברה מתייחסת לחדירה שנעשתה ללא הסכמה. כאמור בפרק ב', סעיף 3.2 דלעיל, יש להבחין בין בעלות קניינית במחשב, לבין הבעלות במידע שבמחשב – למשל, קובץ. מכאן, שסעיף 4 יכול לחול גם במקרה של פתיחת קבצים ללא הרשאה על ידי מי שמורשה להשתמש במחשב עצמו ושניתן להרשיע אדם בחדירה לחומר מחשב הנמצא במחשב.[127] לסיכום, לדעתי, ניתן להחיל את סעיף 4 לחוק המחשבים גם על אנשים החודרים למידע הממוחשב מתוך המערכת עצמה, כמו למשל עובדים ומעבידים. זוהי תחולה רחבה וראויה של החוק, הנותנת מענה ראוי לחירות האוטונומיה, הקניין, חופש הביטוי והפרטיות של יוצר המידע הממוחשב. שונה היא גישת בית הדין בפרשת **איסקוב**,[128] שקבע לאקונית כי סעיף 4 לחוק המחשבים לא יחול על העתקת קובץ של עובד שאוחסן במחשב המעביד, וכי אין זה סביר שסעיף 4 לחוק המחשבים, יפורש כאוסר על מעסיקים כניסה למחשבים הנמצאים **בבעלותם**.[129] נוכח אי־הבהירות באשר לתחולת חוק המחשבים, בכל הנוגע לחדירה של בעל המחשב לקובץ מחשב של עובד שהנו מורשה שימוש במחשב, ההסכם הקיבוצי הכללי בנוגע לחדירת מעביד לקבצים של עובדו תורם באופן ראוי להבהרת הדין הקיים. ניתן לראות בהסכם זה פריטה לפרוטות

סז 764 (2006) (להלן: ענין **לרמן**).

126 ראו פרשת **בדיר**, לעיל ה"ש 1; דויטש, לעיל ה"ש 82, בעמ' 431; ואהרוני־גולדנברג, לעיל ה"ש 51, בעמ' 291–300. כל פרשנות אחרת עלולה להפוך כניסה מורשית ומודעת למחשב הזולת לעברה פלילית. אך השוו למיכאל בירנהק "משפט המכונה: אבטחת מידע וחוק המחשבים" **שערי משפט** ד 315 (2006).

127 אמנם החוק אינו מכסה מקרים שבהם יש הצצה גרידא בצג המחשב, ואולם אין לגזור מכך גזרה שווה למקרה שבו יש הפעלה אקטיבית של המחשב כדי לראות בו עוד פרטים במסמך הפתוח או כדי לפתוח קבצים נוספים.

128 לעיל ה"ש 50. יצוין, כי בפרשה זו נסקר הדין הזר הקיים בנוגע לקריאה לא מורשית של דואר אלקטרוני של עובדים על ידי מעביד, אך ללא ניתוח יתרונותיו וחסרונותיו, ומבלי להתייחס לשוני הרב שבין הדין הזר, לדין הפוזיטיבי הישראלי.

129 גם בעניין **אפיקי מים**, לעיל ה"ש 47, מאמץ בית הדין את כללי הציפייה הסבירה לפרטיות, ולא את חוק המחשבים עצמו או את חוק הגנת הפרטיות.

של החוק, האוסר חדירת מעביד לקובץ מחשב של עובדו, אך גם הגנה על אינטרסים תועלתניים ראויים של המעביד.

2.1.2 *יירוט המידע הנמצא במחשב: אי־תחולת עברת האזנת סתר*

בסעיף זה תיבחן התפיסה שלפיה סעיף 2(א) לחוק האזנת סתר (האזנת סתר שלא כדין), הקובע, כי "המאזין האזנת סתר שלא על פי היתר כדין, דינו – מאסר חמש שנים", איננו חל על יירוט מידע המאוחסן במחשב. כעולה מצירופם של סעיף 1 (הגדרות) וסעיף 2(א) לחוק האזנת סתר, עברת האזנת סתר מורכבת מהיסודות דלהלן: א. האזנה, קליטה או הקלטה ב. לשיחת הזולת, לרבות בתקשורת בין מחשבים, ובהתייחס לנתונים "המועברים" (הנמצאים בתנועה); ג. ההאזנה נעשית סימולטנית לשיחה – בזמן אמת; ד. באמצעות מכשיר;[130] ה. ללא הסכמת בעלי השיחה. ו. ההלך הנפשי – מודעות לעובדות ולנסיבות (עברה שותקת). להלן ייבחנו בהרחבה את החשובים שבמרכיבים אלו.

"**האזנה**" מוגדרת בסעיף 1 לחוק האזנת סתר כ"האזנה לשיחת הזולת, קליטה או העתקתה של שיחת הזולת, והכל באמצעות מכשיר". הגדרה זו מלמדת על הרחבת הפרשנות המילולית המקובלת של המושג "האזנה" – לא רק קליטה באמצעות חוש השמיעה, אלא גם קליטה או העתקה של נתונים. המונח "**שיחה**" מוגדר בסעיף 1 לחוק האזנת סתר, כדלקמן: "בדיבור או בבזק, לרבות בטלפון [...] בפקסימיליה, בטלקס, בטלפרינטר או בתקשורת בין מחשבים".[131] המונח "**בזק**" (שפירושו המילוני – טלקומוניקציה) מוגדר בסעיף 1 לחוק האזנת סתר, כ"סימנים, אותות [...], **המועברים** באמצעות תיל". הדיבר "המועברים" מלמד שעל המידע המתוקשר (מסר הבזק) להימצא **בתנועה** המעבירה אותו מהמחשב של השולח למחשב של הנמען – להיות נייד ולא נייח.[132] ואכן, כאשר המסר נמצא בקווי התמסורת הוא זז ומתקדם, ואיננו עומד במקום, שכן במצב נייד הוא יתמוסס ויתנדף. לפיכך, כעיקרון, **מידע השמור במחשב**, לרבות טיוטת דואר אלקטרוני, **איננו בגדר "שיחה"** ב"בזק", שכן הוא

---

130 אין בחוק האזנת סתר הגדרה למונח "מכשיר". בע"פ 1497/92 **מדינת ישראל נ' צוברי**, פ"ד מז (4) 177, 193 (1993) (להלן: פרשת **צוברי**), פורש המונח "**מכשיר**" כמתייחס למכשור אלקטרוני או לכלים כיוצא באלה, המאפשרים האזנה. מכאן ניתן להסיק, כי "מכשיר" האזנה כולל גם מחשב וגם מכשיר טלפון דיגיטאלי, ולא רק אמצעי ציתות **מיוחד** כמו מכשיר הקלטה נסתר.

131 בחוק האזנת סתר, כמו בחוק המחשבים, אין הבחנה בין **סוג המידע** שלו מאזינים ואופיו והוא חל על כל סוג של "שיחה" לרבות בנושא אישי, מקצועי, סודי וכללי. בנוסף הגנת החוק נפרשת גם על תאגידים, וזאת בניגוד לתחולתן המצומצמת של חלק מהוראות ס' 2 לחוק הגנת הפרטיות.

132 מסקנה זו עולה גם מדברי ההסבר להצעת חוק המחשבים (שהובילה לתיקון התשנ"ה לחוק האזנת סתר), שם הוצע שקליטה בסתר של מידע הנמצא בתנועה – "**מוזרם** במערכות תקשורת בין מחשבים" – תהווה "מקרה מיוחד של האזנת סתר". (ההדגשה שלי – ש.א.ג).

אינו במצב צבירה נייד – של "המועברים". קו פרשני זה, המדגיש את חשיבות המונח "המועברים", אומץ גם על ידי בית המשפט המחוזי בענין **פילוסוף**.[133] אין בחוק האזנת סתר הגדרה למונח "**תקשורת בין מחשבים**",[134] וסביר להניח, שהמושג כולל, בין היתר, תקשורת ב – Ethernet, פקס־מודם, ומודם. לפיכך "שיחה" יכולה להתבטא במשלוח דואר אלקטרוני ממחשב אחד למשנהו; בהתכתבות ב־ICQ או בהקלטת הודעה בקולן (תקשורת בין טלפון למחשב – הקולן).[135]

בפרשת **צוברי**[136] הוסיף בית המשפט העליון יסוד לסעיף 2(א) לחוק האזנת סתר – את **דרישת הסימולטניות**, וקבע כי הסעיף נוגע להאזנה, לקליטה ולהקלטה, בעת קיום השיחה. כך נוצרת הבחנה בין האזנת סתר הנעשת **סימולטנית** לקיום השיחה שמאזינים לה, לבין הקשבה בדיעבד לשיחה שהוקלטה: על הקליטה בסתר של ההודעה להיעשות במקביל (בו־זמנית) להעברתה בקווי התמסורת. הקלטת שיחה[137] בעת קיומה ללא הסכמה מהווה האזנת סתר, "גם אם אין שמיעה (קרי, האזנה) בו־זמנית בעת שההקלטה מתבצעת, ואף אם אין אפשרות טכנית להאזנה בו־זמנית". אף שדרישת הסימולטניות איננה מצוינת בחוק מפורשות, היא משתמעת ממבנה סעיפיו הקטנים של סעיף 2 לחוק האזנת סתר ומהמונח "המועברים".[138]

---

133 ענין **פילוסוף**, לעיל ה"ש 94.

134 בחוק האזנת סתר אין הגדרה של "מחשב", אף שבס' 15 להצעת חוק המחשבים, הוא הסעיף המתקן את חוק האזנת סתר, הוצע להגדיר "מחשב" "כהגדרתו בחוק המחשבים", אך הדבר לא בא לידי ביטוי בנוסח הסופי של התיקון לחוק האזנת סתר. עם זאת, ניתן לפנות להגדרת "מחשב" בחוק המחשבים על דרך ההיקש. ראו: ת"א (מחוזי ת"א) 699/96 **דסק מערכות אלקטרוניקה בע"מ נ' פימא מערכות אלקטרוניקה בע"מ**, דינים מחוזי כו (7) 730 (1997).

135 ס' 1 לחוק האזנת סתר מביא רשימה ארוכה, אך לא ממצה ("לרבות"), של האמצעים שדרכם יכולה להיעשות "שיחה" לא ישירה ב"בזק". המונח "**תקשורת בין מחשבים**" מהווה רק דוגמה המעידה על הכלל לפיו: "שיחה" ב"בזק" כוללת גם מסרים המועברים בין מחשבים ובין מכשירי קצה – למחשבים, כגון בין טלפון למחשב.

136 פרשת **צוברי**, לעיל ה"ש 130 , בעמ' 194–195.

137 **הקלטה** – הפעלת מכשיר הקלטה הרושם את השיחה (פרשת **צוברי**, שם, בעמ' 195).

138 מסקנה זו יסודה במספר יסודות נוספים: ראשית, כעולה מדברי ההסבר להצעת חוק האזנת סתר (תיקון), התשנ"ד–1994, ה"ח 544, מטרתו של התיקון היתה רק **להרחיב את הטכניקות של העברת המסרים**, במיוחד בכל הקשור לתקשורת **אלחוטית** וסלולרית, ולא לשנות את הסדרי החוק. שנית, גם האזנה לשליחת הודעה שמשודרת בפקסימיליה צריכה להיעשות במקביל להעברתה ולכן דורשת סימולטניות, שכן עצם קריאת שדר הפקסימיליה אינו מהווה האזנת סתר. שלישית, כמפורט בפרשת **צוברי**, לעיל ה"ש 130, הרציונל שעומד מאחורי דרישת הסימולטניות, נובע מהמבנה המשולב של שלושת חלקיו של ס' 2 לחוק: התקנת מכשיר האזנה (ס' 2(ב)), הפעלת המכשיר (ס' 2 (א)) והשימוש במידע בתום השיחה (ס' 2 (ג)), ואינו קשור לסוג הטכנולוגיה בה מדובר. רביעית, בדברי ההסבר להצעת חוק המחשבים נאמר, שקליטה של דואר אלקטרוני, המתקבל תוך כדי חיפוש במחשב, מהווה מהבחינה ההתנהגותית האזנת סתר – ומכאן שגם כאן יש התייחסות לדרישת הסימולטניות.

אמנם בעניין **בדיר**[139] (החלטה שבוטלה בהסכמה) נאמר, כי עם תיקון התשנ"ה לחוק האזנת סתר דרישת הסימולטניות אינה תקפה עוד, אלא שבית המשפט המחוזי פירש את דרישת הסימולטניות כנוגעת **לזמינות מקבילה** של בעלי השיחה[140], אף שלמעשה היא נוגעת **לשעת הקליטה על ידי המאזין בסתר**. ואכן, יסוד "המועברים" עדיין קבוע בחוק, והוא מלמד שעל ההאזנה להיעשות במקביל למעבר של מסר הבזק בקו התקשורת. דומה שגם בעניין **פילוסוף** אומצה התפיסה שלפיה דרישת הסימולטניות בחוק האזנת סתר — שרירה וקיימת.[141]

לסיכום, כניסה למחשב וויירוט טיוטת מייל או כל מידע אחר המאוחסן מחשב מהווה עברה על סעיף 4 לחוק המחשבים ולא על סעיף 2(א) לחוק האזנת סתר, שכן אין מדובר בתקשורת בין מחשבים; במידע הנמצא במצב צבירה של "המועברים"; ובקליטה סימולטנית של שיחה.

2.2 *שלב המעבר של המידע בקווי תקשורת: עברת האזנת סתר*

הטכנולוגיה המודרנית מאפשרת לנטר בסתר תקשורת המועברת בקווי תקשורת בין מחשבים (קוויים או אלחוטיים), באמצעים רבים. למשל, באמצעות מכשיר **אנאלייזר** (מכשיר לתיקון מחשבים), המאפשר לקלוט את המידע הזורם בקווי התקשורת המקשרים בין מחשבים או באמצעות *Receiver*, היכול לקלוט תקשורת אלחוטית בין מחשבים. קליטת המידע העובר בקווי התמסורת בדרכו ממחשב א' למחשב ב' אינה מהווה עברה על סעיף 4 לחוק המחשבים, שכן נתונים אלו אינם מהווים "חומר מחשב **הנמצא במחשב**", אלא מידע המוזרם **בקווי התקשורת** המחברים בין מחשבים.

יירוט המידע הנמצא במעבר בקווי התקשורת המחברים בין מחשבים מהווה עברת האזנת סתר: שכן מדובר ב"קליטה"; של "שיחה" ב"בזק" — ב"תקשורת בין מחשבים"; המידע נמצא בהליכי מעבר ("המועברים"); הקליטה נעשית סימולטנית לשיחה; באמצעות מכשיר והכול בהתקיים יתר יסודות הסעיף — היעדר הסכמה וההלך הנפשי. עברת האזנת הסתר חלה, הן לגבי קליטת מידע העובר **בקווי התקשורת הפנימיים** המחברים בין המחשב לקווי התקשורת החיצוניים (למשל לקו טלפון של בזק), והן לגבי יירוט מידע המוזרם **בקווי התקשורת החיצוניים**, המחברים

139 עניין **בדיר**, לעיל ה"ש 1, בעמ' 1927.

140 כפי שנקבע בעניין **בדיר** (שם), אין צורך ששני הצדדים לשיחה — הנמען והמוסר, ישוחחו בו זמנית ואין כוונה שעל הצדדים לשיחה להיות **זמינים לשיחה באותו הרגע**. ואכן, בחוק אין דרישה ששני הצדדים — הנמען והמוסר ישוחחו בו זמנית. לפיכך, קליטה של הודעה שהוקלטה בקולן לפני משיכתה על ידי הנמען האזנת סתר, אף אם במחשב המיועד אין מי שיקרא את המסר.

141 לעיל ה"ש 97.

בין מערכות המחשב בעולם כולו.[142]

2.3 קליטת מידע הנמצא בתחנות הביניים בדרכו למחשב היעד

ניתוחם של סעיף 4 לחוק המחשבים וסעיף 2(א) לחוק האזנת סתר מלמד כי הם יוצרים ביניהם חלוקת עבודה. סעיף 4 לחוק המחשבים מתמקד במידע **המאוחסן במחשב**, ואילו סעיף 2(א) לחוק האזנת סתר נוגע למידע הנמצא **בהליכי מעבר** בדרכי תקשורת המחברות בין מחשבים – **בקווי תקשורת**. הליך התקשורת בין מחשבים כולל תחנות ביניים, שאופיין תלוי בסוג התקשורת שבה מדובר: תקשורת במייל כוללת עצירת ביניים בשרתי ספק שירות אינטרנט (להלן גם: ISP); תקשורת בדואר מבוסס רשת (WebMail) כוללת עצירת ביניים בספק ה-WebMail; תקשורת טלפונית והשארת הודעה בקולן כוללות את אחסון המידע במרכזיית תקשורת ממוחשבת עד למשיכתו מהטלפון הנמען.

להלן ייבחן הדין הקיים בנוגע לחדירה לכל אחת מתחנות הביניים בדרכו של המידע ליעדו (ספק תקשורת, Web-Mail והודעת שמוקלטת בקולן). על פי התפיסה המוצעת, אף שלכאורה בכל הנוגע למידע הנמצא בתחנות ביניים בדרכו אל היעד חל סעיף 4 לחוק המחשבים, יש לראות ביירוט מידע בדרכו למחשב היעד והמאוחסן זמנית בתחנת ביניים – אקט של האזנת סתר.

2.3.1 קליטת מידע הנמצא בשרת של ספק שירות האינטרנט

בסעיף זה תיבחן הסיטואציה של חדירה לשרת (מחשב המשרת מחשבים אחרים) של ספק שירות אינטרנט ויירוט מייל הנמצא בו, בטרם נמשך על ידי הנמען. התהליך המהיר של שליחת מסר באינטרנט הנו מורכב למדי: כאשר נשלח דואר אלקטרוני ממחשב למחשב היעד, הוא נחלק לכמה חבילות העוברות בתחנות ביניים רבות של שרתי ספקיות שירות. לאחר מכן מתאגדות כל החבילות למסר אחד, המוחזק בשרת ספק שירות האינטרנט (למשל, חברת ברק 013) עד למשיכתו משם ממחשב היעד – המנוי של ספק השירות.[143] לכאורה, כאשר נעשית חדירה לשרת של ספק שירות אינטרנט ומיורט דואר אלקטרוני המאוחסן בו, מדובר בעברה על סעיף 4 לחוק המחשבים, שכן מתקיימים בפעולה זו יסודותיה ההתנהגותיים של העברה ("חדירה

---

142 וזאת הואיל וקווי התקשורת הפנימיים אינם בגדר "מחשב". ואמנם, בדברי ההסבר לס' 31א להצעת חוק המחשבים, לעיל ה"ש 105, בעמ' 484 נאמר, כי "יש מקום להבחין בין התקשרות או התחברות עם מחשב, דבר שהוגדר כחדירה למחשב, לבין התחברות או התקשרות **לקווי התקשורת** של המחשב, דבר שהוגדר כהאזנה בחוק האזנת סתר" (ההדגשה שלי – ש.א.ג.).

143 אברהם טננבוים "השלכות רשת האינטרנט על המשפט המהותי" **שערי משפט** א 133 (1998).

לחומר מחשב הנמצא במחשב"): דואר אלקטרוני מהווה "חומר מחשב"; שרת של ספק של שירותי אינטרנט מהווה "מחשב", כהגדרתו בסעיף 1 לחוק המחשבים;[144] הדואר **מאוחסן** במחשב; וקליטתו, בין על ידי צו שיפוטי ובין בחדירה פרטית, מהווה חדירה לחומר מחשב.

2.3.1.1 חדירה למחשב של ספק שירות אינטרנט: אי־תחולה לכאורית של חוק האזנת סתר

קיימים טיעונים מספר המקשים על החלת סעיף 2 (א) לחוק האזנת סתר בסיטואציה של חדירה למחשב של ספק שירות ויירוט מסר שטרם נמשך על ידי מחשב היעד. ראשית, כאמור, על מסר הבזק להיות בתנועה – "**המועברים**" – (ראו סעיף 0 דלעיל), ואילו הדואר האלקטרוני הנמצא בשרת ה־ISP עד למשיכתו על ידי הנמען הנו **נייח**. טיעון שני הועלה בכמה החלטות שיפוטיות, והוא נובע מהמונח "בעל שיחה", המוגדר בסעיף 1 לחוק האזנת סתר, ככל אחד מאלה: "(1) המדבר; (2) מי שהשיחה מיועדת אליו; (3) המשדר בבזק; (4) מי שהמסר המועבר בבזק מיועד להיקלט אצלו; למעט הנותן שירות של העברת מסר בבזק, למען זולתו או מטעם זולתו". בפרשת **נטוויז'ן נ' צה"ל**[145] קבע בית משפט השלום,[146] שחדירה לשרת של ספק שירות באינטרנט בשלב שבו הדואר האלקטרוני טרם נמשך אינה מהווה האזנת סתר. בהחלטה נקבע, שהואיל וה־ISP, הנותן שירות של העברת מסרים בבזק למען בעלי שיחה (השולח והנמען), אינו "בעל שיחה", הרי שהדואר האלקטרוני השמור אצלו איננו בגדר "שיחה" כהגדרתה בחוק האזנת סתר. אף שהחלטה זו בוטלה בהסכמה,[147] ראוי להסביר מדוע אין לקבלה. העובדה שספק שירות אינטרנט אינו "בעל שיחה" איננה רלוונטית לשאלה מתי מתקיימת "שיחה" בתקשורת בין מחשבים", אלא רק לשאלה **מי רשאי להסכים להאזנה לשיחה**.[148] העובדה שהשיחה עוברת דרך ה־ISP, שאינו רשאי להסכים ליירוטה בסתר, אינה משנה את עצם קיומה של "שיחה" שקליטתה בסתר מהווה האזנת סתר.

2.3.1.2 חדירה למחשב של ספק שירות אינטרנט: תחולת עברת האזנת סתר

למרות הקושי בהחלתו של סעיף 2(א) לחוק האזנת סתר ("המועברים") בסיטואציה

---

144 פרשת **נטוויז'ן** ועניין **ופילוסוף**, לעיל ה"ש 94.

145 פרשת **נטוויז'ן**, לעיל ה"ש 94, שם ביקשה המדינה צו חיפוש בחומר המחשב של ספק הגישה לאינטרנט.

146 בהסתמך על אמרת אגב של בית המשפט המחוזי בפרשת **בדיר**, לעיל ה"ש 1.

147 מבלי שערכאת הערעור הכריעה בעניין.

148 "'האזנת סתר'"האזנת סתר" – האזנה ללא הסכמה של אף אחד מבעלי השיחה".

של חדירה לשרת ספקית שירות ויירוט מייל שטרם נמשך, ותחולתה הלכאורית של עברת החדירה למחשב בסיטואציה זו הרי שפרשנות תכליתית ולשונית מלמדות כי הדבר מהווה עברת האזנת סתר. ואמנם, כל התהליך שעובר הדואר האלקטרוני עד להגעתו ליעד – למחשב הנמען, מהווה "תקשורת" בשלביה השונים, ויש לראות בעצירה הזמנית של מסר הבזק בשרת ספק השירות **חלק בלתי נפרד** מהליך **תקשורת בין מחשבים**;[149] ההמתנה על השרת של ספק התקשורת היא רק **אתנחתה** בדרכו של המייל – ליעדו, ואין לראות בה **אחסון** של המידע, אלא המשך של מצב הניידות. לפיכך, כל זמן שמסר הבזק נמצא בשרת ספקית השירות בהמתנה למשיכתו על ידי מחשב היעדהוא בא בגדר "**המועברים**", וקליטתו בסתר מהווה האזנת סתר לתקשורת בין מחשבים.[150] **המטפורה** הבאה ממחישה מסקנה זו: קבוצת אנשים נוסעת מתל-אביב לירושלים במונית – בשלב זה האנשים "מועברים". גם כשהמונית עוצרת ברמזור, הקבוצה עדיין נמצא בתהליך של העברה ליעדה, שכן זוהי עצירה זמנית במסגרת התנועה הכללית.[151] קו פרשני זה הוצע בעבודת הדוקטורט שלי,[152] ודומה

149 בדומה, בית המשפט האמריקני קבע בפסק דין United States v. Councilman, 18 U.S.C.S 2510 (2005), כי יירוט דואר אלקטרוני הנמצא באחסון זמני מפר את חוק האזנה הסתר הפדרלי (Wiretap Act, 18 U.S.C. §§ 2510–2522): "the term 'Electronic Communication' includes transient electronic storage that is intrinsic to the communication process for such communication". פסק הדין ניתן לצפייה גם בכתובת: www.ca1.uscourts.gov/pdf.opinions/03-1383EB-01A.pdf (נבדק לאחרונה ב-11.1.2009).

150 ואכן, בפרשת **נטוויז'ן**, לעיל ה"ש 94, (שאיננה מהווה תקדים מחייב, שכן הצדדים הגיעו בו להסכמות), טען ספק האינטרנט שהעברת מסר הבזק (דואר אלקטרוני) איננה מסתיימת עד להגעתה ליעד הסופי – לבעל השיחה, וכי דואר המצוי על גבי מחשבי הספק בהמתינו שהמנוי ימשוך אותו ויקרא אותו הנו "שיחה" מסוג "בזק" שטרם נסתיימה. בערר בעניין זה הודיעה המדינה, שכאשר תבקש בעתיד צו היתר להאזנה לתקשורת בין מחשבים, שאמורה לעבור דרך ספק שירות אינטרנט, היא תפנה לבית המשפט המחוזי בהתאם לחוק האזנת סתר ולא בהתאם לחוק המחשבים.

151 חיזוק לעמדתי זו ניתן למצוא בדברי ההסבר להצעת התיקון לחוק האזנת סתר (ס' 15 להצעת חוק המחשבים), שם ההתייחסות היא ל"מידע רב זורם במערכות תקשורת בין מחשבים" – "מערכות" תקשורת ולא רק "דרכי" התקשורת עצמם; **התחנות** שבדרך הן חלק ממערכות אלו, והן כוללת גם את ספק השירות. כמו כן, כיום ניתן לבצע תקשורת **בעל פה**, באמצעות האינטרנט. גם שיחות אלו מבוצעות באמצעות מחשבים ועוברות דרך תחנות ביניים ושרתי אינטרנט של ספקיות שירות. לפיכך לא סביר להוציא האזנה לשיחות אלו כשהן בדרכן ליעדן, מגדר "האזנת סתר".

152 ראו אהרוני-גולדברג, לעיל ה"ש 51. בדומה, בית המשפט האמריקני קבע בפסק דין United States v. Councilman, 18 U.S.C.S 2510 (2005), כי יירוט דואר אלקטרוני הנמצא באחסון זמני מפר את חוק האזנה הסתר הפדרלי (Wiretap Act, 18 U.S.C. §§ 2510–2522): "the term 'Electronic Communication' includes transient electronic storage that is intrinsic to the communication process for such communication". פסק הדין ניתן לצפייה גם בכתובת: www.ca1.uscourts.gov/pdf.opinions/03-1383EB-01A.pdf (נבדק לאחרונה ב-

שבית המשפט המחוזי בפרשת **פילוסוף** הגיע לאותה מסקנה, ותוך שימוש במטפורה דומה (תחנת דלק),[153] בקובעו שחוק האזנת סתר הוא שחל בסיטואציה של העתקת דואר אלקטרוני הנמצא אצל ספק השירות שטרם נמשך על ידי מחשב היעד.

המסקנה שסעיף 2 (א) לחוק האזנת סתר הוא שחל בסיטואציה זו מתחזקת אל נוכח העובדה, שהוא פורש הגנה טובה יותר על עקרון סודיות המידע הממוחשב, המתבטאת בהוראות החיפוש, בעקרון פרי העץ המורעל וברף הענישה, ולפיכך, ראוי להחילו כדי להגן כיאות על עקרון סודיות המידע הממוחשב. משניתן להחיל גם את סעיף 4 לחוק המחשבים וגם את סעיף 2 לחוק האזנת סתר בסיטואציה של יירוט מייל המאוחסן בשרת ISP ושטרם נמשך, הרי שיחול רק סעיף 2 לחוק האזנת סתר – שכן, כאמור, הסיפה לסעיף 4 לחוק המחשבים קובע מפורשות שחדירה למחשב איננה האזנת סתר.

2.3.2 יירוט מידע הנמצא בדואר מבוסס רשת (Web Mail) וטרם נמשך

דרך מקובלת נוספת לתקשורת אלקטרונית נעשית באמצעות **דואר מבוסס רשת** (WebMail) – ספק ה WebMail – משמש ממשק, המציג את הודעות הדואר האלקטרוני בדף אינטרנט בדפדפן.[154] יירוט הודעות מייל הנמצאות ב־WebMail, לפני שאלו נמשכו על ידי הנמען, כמוהו כיירוט Mail משרת ISP: יש לראות בשרת של ספק ה־WebMail תחנת ביניים של המסר האלקטרוני בדרכו אל הנמען, וביירוט – האזנה, הנעשית סימולטנית לשלב קיומה של ה"שיחה" (מטפורת הרמזור).[155] לפיכך חל בעניין חוק האזנת סתר. גם פרשנות נורמטיבית מובילה למסקנה זו. אין נפקא מינה לעובדה שאת הודעת המייל הזו יכול הנמען למשוך מכל סוג של מחשב ולכך שהמידע איננו מאוחסן במחשב האישי שלו. כאמור, ראוי להתרחק מתפיסה קניינית, שלפיה רק כאשר המידע מגיע למחשב האישי של הנמען מסתיימת השיחה, שכן הבעלות הקניינית במחשב שבו נעשית החשיפה למידע איננה רלוונטית.

(11.1.2009).

153 בעניין **פילוסוף**, לעיל ה"ש 94. נקבע, כי ראוי לבחון את מסעה של הודעת הדוא"ל בתווך האלקטרוני מתוך השקפה כוללת על תהליך תעבורת הדואר אלקטרוני מרגע שיגורו מנקודת המוצא ועד להגעתו למחשב היעד וכי תפיסת המסר על מחשב ספק השרות מהווה תפיסה ב"זמן אמת" במהלך תהליך העברה ולפני שהסתיימה ה"תקשורת בין מחשבים", כהגדרת חוק האזנת סתר ל"שיחה".

154 בדרך זו הנמען גולש ממחשב כלשהו לאתר של ספק שירות WebMail, מקיש את ססמתו וקורא את ההודעה שנשלחה אליו, ללא צורך לאחסנה במחשבו. ראו http://he.wikipedia.org (נבדק לאחרונה ב־11.1.2009).

155 השיחה מסתיימת כאשר הנמען מושך את המכתב או נחשף אליו באחת ההתחברויות שלו ל־WebMail.

2.3.3 יירוט הודעה שהושארה ב"קולן" וטרם נמשכה

שאלה דומה בנוגע לתחולת סעיף 4 לחוק המחשבים וסעיף 2 (א) לחוק האזנת סתר מתעוררת כאשר צד שלישי מאזין להודעות שהוקלטו במכשירי קולן. כאשר א' מתקשר לטלפון של ב' ומשאיר לו הודעה במשיבון הממוחשב שלו וההודעה טרם נמשכה על ידי ב', ההודעה מאוחסנת במרכזייה הממוחשבת של חברת הטלפונים. לכאורה מתקיימים בעניין זה יסודות **סעיף 4 לחוק המחשבים**: מדובר בחדירה ל"חומר מחשב" – ההודעה הקולית שמשאיר המתקשר; הקולן ומרכזיית "בזק" מהווים "מחשב", כהגדרתו בסעיף 4 לחוק המחשבים, שכן הם כוללים תכנה המאפשרת להם לפעול;[156] והחדירה מתבטאת בהתקשרות למחשב.[157] ואולם, לדעתי, יירוט הודעה שהוקלטה בקולן בטרם נמשכה על ידי הנמען מהווה עברה על סעיף 2(א) **לחוק האזנת סתר**: ההודעה מהווה תקשורת ב"בזק"; מדובר בתקשורת בין מחשבים (בין מרכזיית טלפון ממוחשבת ובין "**מחשב**" היעד – הקולן); מסר הבזק נמצא במצב של "המועברים" – בתחנת ביניים בדרכו ליעד (מטפורת הרמזור);[158] השיחה טרם הסתיימה ומתקיימת דרישת הסימולטניות.[159] לפיכך, הואיל ומכוח הסיפה לסעיף 4 לחוק המחשבים, כשמתקיימים יסודות עברת החדירה למחשב ויסודות עברת האזנת הסתר חוק האזנת סתר גובר, הרי שיירוט מסר שטרם נמשך מקולן מהווה עברת האזנת סתר.[160]

2.4 יירוט מידע ממחשב הנמצא בהליך קבלת מסר בזק (On Line)

נעבור לבחון את הדין בהמשכו של "המסלול" המקוון שעובר מסר הבזק – כאשר מבוצעת חדירה למחשב הנמצא בהליך של קבלת מסר אלקטרוני, כגון קבלת הודעת דואר אלקטרוני או קליטת הודעה ב-ICQ.[161] מחד, חלה במקרה זה עברת החדירה

---

156 ענין **בדיר**, לעיל ה"ש 1

157 בעניין **בדיר**, שם, אישום 43, הנאשם חדר לתא קולי והאזין להודעות שהושארו בו. הוא הורשע בחדירה למחשב כדי לעבור עברה אחרת ובעברת האזנת סתר. מהעובדות המפורטות בפסק הדין לא ברור אם מדובר ביירוט של הודעות שכבר נמשכו על ידי מחשב היעד או כאלו שטרם נמשכו.

158 שם.

159 בענין **בדיר**, שם, נקבע, שבהאזנה להודעות שהושארו בקולן יש משום האזנת סתר, שכן התקשרות לתא קולי, המנוהל באמצעות מחשב, יכולה להיכלל ב"תקשורת בין מחשבים", אך ההחלטה בוטלה בהסכמת התביעה הכללית במסגרת הערעור (התביעה הכללית משמשת גם כבאת כוחן של רשויות השלטון בבואן לקבל צווי חיפוש והאזנת סתר).

160 אך השוו, כאמור, לעניין **בדיר**, שם, אישום 43, שבוטל בהסכמה.

161 סוגיה דומה עשויה להתעורר במצב הבא: עבריין מחשבים חודר למחשב של המשטרה הנמצא בחדר הישיבות, כדי לשמוע את הנאמר בו, משנה את הגדרת המיקרופון המחובר למחשב ו"הופך" אותו לרמקול, המאפשר לו לשמוע את המתרחש בחדר הישיבות ("האזנה אקוסטית").

למחשב, שכן יש חדירה למחשב וקליטה של חומר מחשב הנמצא בו, ומאידך, חל סעיף 2(א) לחוק האזנת סתר, שכן מדובר ביירוט **סימולטני** של מסר בזק **מועבר**, ובלבד שמתקיים ההלך הנפשי הנדרש – מודעות לכך שהמחשב מחובר לרשת ושניתן לקלוט שיחות בצורה זו.[162] לפיכך, על פי הסיפה לסעיף 4 לחוק המחשבים, כאשר שני הסעיפים עשויים לחול, חוק האזנת סתר גובר. ואולם בהכרעת הדין בפרשת **פילוסוף**,[163] שם היה מדובר בתכנת סוס טרויאני "המאפשרת לצפות בכל הקבצים במחשב הנגוע",[164] הודה הנאשם במסגרת עסקת טיעון, בין היתר, בעברה על סעיף 2 לחוק האזנת סתר ובעברה על סעיפים 4 ו־5 לחוק המחשבים. מהעובדות המפורטות בהכרעת הדין לא ניתן להבין אם התכנה קלטה **בזמן אמת** גם מיילים שנתקבלו במחשב שבו הוחדרה התכנה. אם היא לא קלטה מסר בזק שהתקבל בזמן אמת, אלא רק צילמה את תוכן המחשב מדי פעם,[165] הרי ההרשעה בהסכמה בסעיף 2 לחוק האזנת סתר איננה מוצדקת.

בהערת אגב אעיר, כי בפרשת הסוס הטרויאני ובפרשות אחרות[166] הורשעו מתכנתי תכנות ריגול או תכנות זדוניות בעברה על **סעיף 6 לחוק המחשבים** (נגיף מחשב).[167] ספק בעיניי אם הרשעות אלו מתיישבות עם ההיסטוריה החקיקתית של הסעיף ועם תכליתו.[168] פרשנות לשונית של סעיף 6 לחוק המחשבים מעלה, כי הוא מתייחס **לתכנה מידבקת**, היכולה להפיץ את עצמה ולהדביק מחשבים שעמם היא באה במגע (ההתייחסות למונח "בלתי מסוימים" בלשון הסעיף עצמו), ולא לתכנה

162 עם זאת, לכלל זה ישנו **חריג, הנוגע לחיפוש שלטוני**, כמפורט בתת־פרק 7.1 למאמר זה.

163 הכרעת הדין בענין **פילוסוף**, לעיל ה"ש 108.

164 שם, בעמ' 1630 לפרוטוקול, ס' 4 להכרעת הדין.

165 ראו הגדרת פעולותיה של התכנה בפרשת **האפרתי**, לעיל ה"ש 2.

166 ראו פרשת **האפרתי**, לעיל ה"ש 2, תפיסה משפטית זו באה לידי ביטוי בשורה ארוכה של פסקי דין: ענין **גרינברג**, לעיל ה"ש 4;ת"פ 2591/04 (שלום ת"א) **מדינת ישראל נ' אנור**, תק־של 04(4) 4617 (2004); הכרעת הדין בענין **פילוסוף**, לעיל ה"ש 108; ענין **לרמן**, לעיל ה"ש 125. וראו גם הערת האגב של בית המשפט בת"פ (שלום חי') 8243/97 **מדינת ישראל נ' פז**, תק־של 98(1) 479 (1998), שממנה עולה כי בית המשפט ער לקושי הפרשני המובע במאמר זה. אך השוו לת"פ (שלום ת"א) 12187/01 **מדינת ישראל נ' אוברציגר**, תק־של 02(3) 15879 (2002), שם אדם שהחדיר תכנת סוס טרויאני מוסווית למחשבים הואשם והורשע בעברה על ס' 4 לחוק המחשבים בלבד, ולא בעברה על ס' 6(ב) לחוק זה.

167 ס' 6 לחוק המחשבים קובע: "(א) העורך תוכנה באופן שהוא מסגלה לגרום נזק או שיבוש למחשב או לחומר מחשב בלתי מסויימים, כדי לגרום שלא כדין נזק או שיבוש למחשב או לחומר מחשב, מסויימים או בלתי מסויימים, דינו – מאסר שלוש שנים. "(ב)"ב. המעביר לאחר או המחדיר למחשב של אחר תוכנה אשר סוגלה לגרום נזק או שיבוש כאמור בסעיף קטן (א), כדי לגרום שלא כדין נזק או שיבוש כאמור, דינו מאסר חמש שנים".

168 בדברי ההסבר לס' 8 להצעת חוק המחשבים הודגש, שהכוונה היא לווירוסים שמוחדרים למחשב שלא על מנת להזיק למחשב הספציפי אליו הם מוחדרים, אלא כדי לפגוע במחשבים בלתי מסוימים.

זדונית המשבשת את המחשב **הספציפי** שאליו הוחדרה או המאפשרת חדירה אליו.[169] גם מכותרתו של סעיף 6 ("נגיף מחשב") עולה, כי הוא מתייחס להוראות מחשב "מידבקות", המשכפלות עצמן למחשבים אחרים.[170] ואמנם, "נגיף מחשב" מוגדר, הן במילון והן בספרות המקצועית, תכנת מחשב המשכפלת עצמה ומעבירה העתקים של עצמה למחשבים אחרים.[171] פרשנות תכליתית של הסעיף מובילה אף היא למסקנה זו: נגיף המחשב כמוהו כנשק ביולוגי המורכב **מנגיפים**, והוא מסוגל להדביק אינספור מחשבים. בשל פוטנציאל הרס עצום זה נכרך, באופן חריג, גם **שלב ההכנה** – תכנות התכנה המידבקת, בגדר המעשה הפלילי. מדובר בעברת הכנה טרם הופצה התכנה ונגרם נזק, ולמתכנת יש **שהות לחזור בו מכוונותיו הזדוניות**, ולפיכך, יש לפרשו בצמצום, ולא לכלול בגדרה תכנה הנעדרת יכולת שכפול עצמי, אף אם פגיעתה קשה.

2.5 *יירוט המידע לאחר קבלתו במחשב היעד*

נעבור לבחון את השאלה אם חדירה למחשב ויירוט מסר לאחר שהוא כבר הגיע למחשב היעד מהווה עברה על סעיף 4 לחוק המחשבים או שמא על סעיף 2(א) לחוק האזנת סתר. שאלה זו, שכאמור נותרה בצריך עיון במסגרת ערעור **בדיר** לבית המשפט העליון[172] רלוונטית במקרים רבים: כאשר נעשית חדירה למחשב שאליו הגיע הדואר האלקטרוני; בחדירה לשרת של ספקי אינטרנט והעתקת מייל שנשמר בשרתיו לאחר שכבר נמשך על ידי הנמען(!);[173] בחיפוש במכשיר טלפון סלולרי והעתקת המסרונים (SMS) המאוחסנים בו;[174] בהאזנה להודעות קוליות שנמשכו על ידי הנמען ועדיין מאוחסנות בקולן שאליו חדרו; וביירוט דואר אלקטרוני, המאוחסן

---

169 פרשנות רחבה יותר של המונח "נגיף מחשב" בס' 6, ובמיוחד בס' 6(ב), תביא לכפילות מיותרת בינו לבין ס' 2 לחוק המחשבים.

170 על משקלה הפרשני של הכותרת ראו: אהרן ברק **פרשנות בחקיקה** כרך שני 319 (1994).

171 לפי Merriam-Webster, "A Virus – a computer program, that produces copies of it self" Online Dictionary ניתן לצפייה בכתובת: www.merriam-webster.com/dictionary/virus (נבדק לאחרונה: 10.1.2009); Eugene H. Spafford, *Computer Viruses*, *in* INTERNET BESIEGED, לעיל ה"ש 10.

172 ערעור **בדיר**, לעיל ה"ש 8.

173 מפרשת **נטוויז'ן**, לעיל ה"ש 94, עולה שיש שספקי שירות אינטרנט שומרים בשרתיהם העתקים של מסרים אלקטרוניים שכבר נמשכו על ידי מחשב היעד(!). ניתן לטעון, כי ס' 8 (4) לחוק האזנת סתר פוטר מאחריות בגין פעולה זו, הואיל והיא נעשית "**לצורך מתן השירות**" – לצורך גיבוי למקרה של שיבוש המידע. אך מהבחינה המשפטית הנורמטיבית, תקינותו של הליך זה מוטלת בספק, שכן היא מהווה פתח מסוכן לפגיעה בפרטיות בסודיות המידע הממוחשב, בפרטיות, הן מצד רשויות השלטון והן מצד גורמים פרטיים. לדעתי, ההסכמה של שולח הדואר האלקטרוני ושל הנמען לאחסון המידע ב-ISP נמשכת עד למשיכתו על ידי הנמען ותו לא. האם נאפשר גם לרשות הדואר לשמור עותקים מגלויות "לצורך מתן השירות"?

174 ראו עניין **אריש**, לעיל ה"ש 116.

במחשב של ספק שירות WebMail, לאחר שהוא נקרא על ידי הנמען.

ניתן למנות שתי גישות עיקריות לסוגיה זו: לפי גישת בית המשפט המחוזי בפרשת **בדיר** (אישום 43),[175] קליטת מידע המאוחסן במחשב לאחר שהגיע למחשב זה בתקשורת בין מחשבים (למשל, מסר בזק שהושאר כהודעה בתא קולי) מהווה גם חדירה למחשב וגם האזנת סתר. לעומת זאת, לפי גישת בית המשפט המחוזי בפרשת **פילוסוף 2**,[176] מסר בזק שכבר הגיע למחשב היעד נמצא ב"מצב מובהק של מידע נייח המאוחסן באורך קבע", ולפיכך הוראות החיפוש במחשב ובמשתמע – סעיף 4 לחוק המחשבים, הן שחלות עליו, ולא חוק האזנת הסתר.[177] ואכן, **חדירה למחשב וקריאת הודעות שכבר הגיעו ליעדן במחשב היעד** (או הודעה שנשלחה והעתקה מאוחסן במחשב), **מהווה עברה על סעיף 4 לחוק המחשבים**, ולא האזנת סתר: **המסר אינו בגדר המועברים**, אלא נייח, וההאזנה אינה מתקיימת סימולטנית לקיומה של השיחה, שכן "מסר הבזק" כבר הגיע ליעדו וה"שיחה" נסתיימה[178,179] רציונל זה מתקיים גם כאשר ההודעה הגיעה ליעדה, אך לא נקראה על ידי הנמען, שכן קיומה במחשב היעד איננו קשור לספק השירות.[180] תפיסה זו חלה על כל המצבים הנוגעים לחדירה למחשב ויירוט תקשורת אלקטרונית שהגיעה ליעדה.

עוד אוסיף, כי באמצעים פשוטים ניתן לנטר קרינה הנובעת ממחשבים, למשל

---

175 פרשת **בדיר**, לעיל ה"ש 1. מניתוח העובדות המתוארות (פריצה לתא קולי והשמעת ההודעות שהוקלטו בו על ידי מתקשרים שונים) לא ניתן להבין אם דובר ביירוט הודעות שטרם נמשכו על ידי בעל הקולן (ונמצאות בתחנת ביניים – במרכזית טלפון של חברת בזק), או שמא מדובר במצב שבו ההודעות כבר הגיעו ליעדן במחשב היעד, נמשכו על ידי בעל התא הקולי והמאזין בסתר שמע אותן לאחר משיכתן. כאמור, במסגרת הדיון בערעור בפרשת **בדיר** בבית המשפט העליון טענה הפרקליטות (תוך שינוי עמדתה הקודמת), שתפיסתו של מידע "שתועד במחשב" (בין אם במחשב של ספק השירות ובין אם במחשב המשתמש) מהווה עברה על ס' 4 לחוק המחשבים ולא האזנת סתר. בעקבות כך, ההרשעות בחוק האזנת סתר בוטלו בהסכמה והסוגיה נותרה **בצריך עיון**.

176 ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף**, תק־מח 2007(3) 12198 (2007) (להלן: עניין **פילוסוף 2**).

177 בדומה, בפרשת **נטוויז'ן**, לעיל ה"ש 94, אימץ בית המשפט המחוזי את העמדה שלפיה דואר אלקטרוני המצוי על גבי מחשבי ספק גישה לאינטרנט בהמתינו שהמנוי ימשוך ויקרא אותו הנו "שיחה" ב"בזק" שטרם הסתיימה.

178 ראו גם דיון לעיל במאמר זה.

179 בענין **איסקוב**, לעיל ה"ש 65, נקבע, שככל הנראה, מעביד המעתיק הודעת דואר אלקטרוני של עובד לאחר שזו נשלחה אינו עובר על חוק האזנת סתר, שכן אין מדובר ביירוט או ניטור של הודעות הדואר האלקטרוני במסען הווירטואלי אל מחשב היעד, אלא בהעתקה של הודעות דואר אלקטרוני שנותרו מאוחסנות – בין על המחשב הספציפי שעמד לרשות התובעת בעת עבודתה בחברה, ובין על השרת של החברה – זמן רב לאחר שההודעות הגיעו ליעדן.

180 מענין **פילוסוף 2**, לעיל ה"ש 176, משתמע, שחדירה למחשב ועיון בהודעה שנתקבלה אך טרם **נקראה על ידי הנמען או בהודעה** שכבר **נקראה על ידי הנמען, באה בגדר ס' 4 לחוק המחשבים, שכן מדובר ב"מצב מובהק של מידע נייח המאוחסן באורך קבע"**.

מצג המחשב, כך שהמידע המופיע על צג המחשב יופיע גם על מסך טלוויזיה המוצב בסמוך. למרות תחולתם הרחבה של סעיף 4 לחוק המחשבים ושל סעיף 2 לחוק האזנת סתר, הם אינם חלים בסיטואציה זו, שכן הקרינה האלקטרומגנטית מורכבת מאותות רדיו הנמצאים באוויר, אינה מהווה "חומר מחשב הנמצא במחשב" ולרוב – אף לא תקשורת בין מחשבים. במקרה זה ראוי להחיל את הוראותיו של סעיף 2 לחוק הגנת הפרטיות ובמיוחד – **ס"ק 2 (5)**,[181] המביא לידי ביטוי פרשנות מרחיבה ואולי אף מהפכנית של הזכות לפרטיות: לא רק מידע **על** הפרט יוגן בדיני הגנת הפרטיות, אלא כל כתביו **של** הפרט שלא נועדו לפרסום יוגנו, ללא הגבלה לנושאים שהצנעה יפה להם.[182] הסעיף מבטא תפיסה קניינית של דיני הגנת הפרטיות, שעל פיה הפרטיות נפרשת על כל כתב של הפרט שלא הופקע מרשותו על ידי הסכמתו להפצתו ברבים או לפרסומו.[183,184] הוראת החוק אינה מתייחסת לאופן שבו מתבצעת ההעתקה ואיננה מוגבלת לטכנולוגיה חודרנית ספציפית, וניתן ליישמה גם על תהליך הפענוח החזותי של הקרינה הנובעת ממחשבים.[185] דרישת החוק הנה להעתקה או ל"שימוש"[186] ב"כתב",[187] וניתן ליישמו על כל העתקה או הדפסה של מידע – בין

---

181 המגדיר פגיעה בפרטיות כ"העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו".

182 והשוו לס' 2(9) לחוק הגנת הפרטיות, המתייחס לשימוש בידיעה על "ענייניו הפרטיים של אדם".

183 לשיטתו של זאב סגל "הזכות לפרטיות למול הזכות לדעת" **עיוני משפט** ט 175, 186 (1983), מטרתו המודעת של המחוקק בסעיף זה היתה לגלוש לדיני זכויות היוצרים.

184 הסעיף מתייחד גם בכך שתחולתו אינה מוגבלת לאדם בשר ודם, אלא חלה גם על תאגיד, וזאת הואיל והמונח "אדם" איננו מופיע בו. אך השוו לעמדת בית המשפט ק"פ 15/03 (שלום ת"א) **סהר תעשיות נ' פריאל**, תק-של 05(1) 29571 (2005). שם בוטלה קובלנה פרטיות שהוגשה על ידי תאגיד בגין חדירה לתיבת דואר אלקטרונית והעתקת הודעה שבה, בניגוד לס' 2 (5) לחוק הגנת הפרטיות, בנימוק שהתובע הנו "תאגיד".

185 בבש"א (מחוזי ת"א) 1614/02 **מולטילוק נ' רב בריח השקעות**, תק-מח 2002(1) 851 (2002) קבע הש' זפט, כי הסעיף אינו עוסק באופן העתקת המסמך, אלא די בכך שהמכתב שלא נועד לפרסום הועתק מבלי רשות הנמען או הכותב.

186 בהצעת החוק המקורית נאסרה קריאת מכתב או כתב אחר שלא נועד לפרסום, אך הנוסח הסופי מתייחס לשימוש. המונח "שימוש" מוגדר בס' 3 לחוק הגנת הפרטיות, ויש לפרש כמתייחס גם **להפצת** כתב של הפרט שנתקבל כדין, אך שלא נועד לפרסום, ולא ניתנה הסכמת הנמען או הכותב להפצתו. ולפיכך, ההוראה אינה אוסרת **קריאת** מכתב או כתב אחר שלא נועד לפרסום, כפי שהוצע הדבר בהצעת החוק; לפיכך, כאשר נעשית הצצה בלתי אמצעית במחשב הזולת ובתוכן המידע שבו, אין בדבר משום העתקת הכתב.

187 "כתב" מוגדר בס' 3 לחוק הגנת הפרטיות כ"**לרבות** מסר אלקטרוני" (תיקון התשס"ז–2007). בחוק הפרשנות, התשמ"א – 1981 הגדרת "כתב" הנה רחבה מאוד והיא נפרשת גם על סימנים הניתנים "לפענוח חזותי" (תחילתו של חוק זה ב-1.10.1981, ואילו חוק הגנת הפרטיות נכנס לתוקף לאחר ה-23.8.1981).

דואר אלקטרוני, בין קובץ המאוחסן במחשב ובין גלי הרדיו הנובעים מהמחשבים.[188,189]

2.6 קו הגבול בין חוק המחשבים לבין חוק האזנת סתר – סיכום

חוק המחשבים וחוק האזנת סתר נותנים, ככלל, מענה ראוי להגנת עקרון סודיות המידע הממוחשב, שכן תחולתם אינה כפופה לגרימת נזק, והחוקים חלים על כל סוג של מידע, ללא הבחנה בין מידע אישי רגיש לבין מידע סתמי; גדר ההפרדה בין כניסה כדין למחשב או להאזנה כדין לשיחת הזולת, לבין עברה פלילית, היא פעולה הנעשית ללא הסכמה. כלומר, בחוק המחשבים ובחוק האזנת סתר האוטונומיה של בעל המידע הממוחשב היא המחסום בפני הסגת גבול.

ניתוח החוק הקיים העלה, כי ישנם כמה עקרונות מנחים הנוגעים לקביעת קו הגבול שבין עברת החדירה לחומר מחשב הנמצא במחשב לבין עברת האזנת סתר, בהקשר של "שיחה" בתקשורת בין מחשבים. ראשית, מבחינה עובדתית, ייתכן מצב שבו ישנה חדירה למחשב וגם האזנת סתר לאותו מחשב; ואולם, כעולה מפשוטו של הסיפה לסעיף 4 לחוק המחשבים,[190] במצב זה חוק האזנת סתר הוא הגובר, שכן עברת החדירה למחשב איננה יכולה לחול על מצב שבו החדירה כוללת גם האזנת סתר. שנית, עיון בלשונו של חוק האזנת סתר מלמד, שעל מסר הבזק להיות במצב צבירה של ניידות ומעבר ("**המועברים**"), ולא במצב אחסון קבוע, כנדרש בגדר חוק המחשבים ("נתונים **המאוחסנים**"). פרשנות לשונית זו שוללת את התפיסה שלפיה חדירה למחשב ועיון בדואר אלקטרוני השמור בו מהווה עברת האזנת סתר.

מכאן לסיכום המסקנות הנוגעות לקו התפר שבין חוק האזנת סתר לבין חוק המחשבים. נשוב למטפורת המסע של מסר אלקטרוני, הנשלח ממחשב שבביתו של א' למחשב שבביתו של ב'.

תחילת המסע בכתיבת מידע במחשב א'. על כניסה **למחשב** בשלב זה תחול **עברת החדירה למחשב**.

בהמשכו של המסע, עובר המסר האלקטרוני **לקווי התקשורת**, המקשרים בין מחשבים – קווי הבזק. האזנה להליך העברת מסר הבזק בדרכי תקשורת בין מחשבים מהווה בעליל האזנה ל"שיחה" (תקשורת בין מחשבים והאזנה סימולטנית כשהמסר מועבר) **וחוק האזנת סתר** חל עליה.

---

188 פרשנות ברוח זו עולה מההחלטה בענין **מולטילוק**, לעיל ה"ש 185. כן ראו עניין **לרמן**, לעיל ה"ש 125 (חדירה למחשב ושליפת מכתבים אישיים ממנו).

189 הואיל ולרוב, חדירה למחשב הזולת, המבוצעת באמצעות מחשב, כוללת העתקה של המידע הממוחשב (שכן על צג מחשב הפורץ מופיע הכתב המועתק באופן אוטומטי), הרי שעצם החדירה כוללת את העתקה, ואין זה משנה שאין מבוצעת פעולה נפרדת של שמירה או העתקה.

190 ומכוח ס' 11 לחוק זה, המהווה חריג – יוצא מן הכלל, לענייני חיפוש, המעיד על הכלל.

לאחר מכן המסר האלקטרוני **עובר** בדרכו למחשב היעד **בשרתים השונים של ספקיות שירות באינטרנט**. ראוי לראות את השלב הזה כאתנחתה זמנית במהלך המסע למחשב היעד, ולכן חדירה לשרת של ספק שירות אינטרנט וקריאת הדואר האלקטרוני בשלב זה מהווה **האזנת סתר**, בהתקיים ההלך הנפשי הנדרש (ראו גם עניין **פילוסוף**).[191] מסקנה זו נובעת גם משיקולי מדיניות, כגון חשיבות הזכות לחופש הביטוי של שני הגורמים המתקשרים ביניהם, מהזכות לקניין של ספקי השירות ומהאינטרס הציבורי להגן על תקשורת באינטרנט. הוא הדין בעניין האזנה לשיחה המוקלטת בקולן ממוחשב שטרם נמשכה על ידי הנמען המיועד.

בשלב הבא הדואר האלקטרוני **מתקבל במחשב היעד** (מחשב ב'). כאשר ההאזנה מתבצעת במקביל לתהליך הקליטה של הדואר האלקטרוני במחשב, בזמן אמת – מדובר בהאזנה ל"שיחה" שעליה חל **חוק האזנת סתר**, וזאת הואיל ומסר הבזק עדיין נמצא בשלב מעבר, ומתקיימת דרישת הסימולטניות.

לבסוף, כאשר החדירה למחשב כוללת קריאת דואר אלקטרוני **שכבר נתקבל ונשמר במחשב** (או כשמדובר בהודעה בתא קולי שכבר נשמעה ונמשכה על ידי הנמען), אין מדובר בהאזנת סתר ל"שיחה" ב"תקשורת בין מחשבים": מסר אלקטרוני שכבר הגיע ליעדו איננו בא בהגדרת "המועברים" וקריאתו איננה סימולטנית לקבלתו; מדובר בחדירה לחומר מחשב הנמצא ("נתונים ... המאוחסנים במחשב") במחשב. מסקנה זו עונה על השאלה שהושארה בצריך עיון על ידי בית המשפט העליון בפרשת **בדיר**.[192]

3. היתרים לחדירה למערכות מחשב – הדין הקיים

עד כה נבחן הדין הקיים, ככל שהוא נוגע לדין הקיים באשר לאיסור חדירה למערכות מחשבים בחוק המחשבים ובחוק האזנת סתר. כאמור בפרק ב', סעיף 4 למאמר זה, את עקרון סודיות המידע הממוחשב יש לאזן עם אינטרסים תועלתניים והומניסטיים אחרים, אם כי בדרך מידתית. נסקור, בקצרה, את עיקרי הדין הקיים בכל הנוגע לחיפוש שלטוני במחשבים ולסעדי עזרה עצמית בהקשר של דיני מחשבים.

3.1 חיפוש במערכות מחשב: הדין הקיים

הוראות חוק־יסוד: כבוד האדם וחירותו מחייבות הגנה על הפרטיות מפני חיפוש: "אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו; אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו" (סעיף 7 (ג) ו־(ד)). ככלל, בחוק

191 לעיל ה"ש 94.

192 לעיל ה"ש 1.

המחשבים ובחוק האזנת סתר הליך החיפוש כפוף למנגנון בקרה שיפוטי, למעט בכל הנוגע להאזנה למטרת ביטחון המדינה (סעיף 4 לחוק האזנת סתר). ואולם קיימים חיקוקים רבים, **המאיינים את הצורך** בקבלת צו שיפוטי או המגבילים את הבקרה השיפוטית על החיפוש השלטוני המקוון,[193,194] ולאחרונה אף מסתמנת מגמה דומה

193 על פי חוק הגנת הפרטיות, רשויות הביטחון אינן נדרשות לצווי בית משפט לצורך פגיעה בפרטיות כל עוד הפגיעה בפרטיות נעשתה באופן סביר במסגרת תפקידן ולשם מילויו (ס' 19(ב) לחוק). דומתני, שהגדרת פטור זו גורפת מדי לאור בס' 7 (ג) לחוק־יסוד: כבוד האדם וחירותו וכי ראוי לאמץ מנגנון בקרה שיפוטי על מעקבים פוגעניים, כגון צילום הפרט בביתו, במיוחד כאשר מדובר בפעולות מתוכננות מראש. בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 נעשה ניסיון לאזן בין הערכים המתנגשים של חירויות הפרט, לבין צורכי הביטחון ומניעת הפשיעה: מחד, חוק זה מחייב צו שיפוטי לצורך קבלת נתוני תקשורת מגוונים, לרבות מאגרי המידע של ספקיות שירות (ס' 3), ומאידך, במקרים דחופים, כגון הצלת חיי אדם, הוא מתיר לקבל מידע כאמור גם ללא צו (ס' 4). הדבר מאפשר איסוף נתונים על מיקומו הפיזי של מתקן הבזק – הטלפון הסלולרי, ללא בקרה שיפוטית. בהצעת החוק לתיקון פקודת סדר הדין הפלילי (מעצר וחיפוש) (מס' 13) (קבלת נתוני תקשורת וקובצי נתונים ממאגר מידע של בעל רישיון בזק), התשס"ו–2006, ה"ח 253 הוצע לאפשר לקצין משטרה לערוך חיפוש במחשב של ספקיות שירות בזק **ללא צו משטרתי** (תקנה 242ד') ולאסוף נתונים, לרבות על **מיקומו הפיזי של מתקן הבזק** – המחשב והטלפון הסלולרי. בדברי ההסבר נאמר, כי כיוון שמידע מקביל מופיע במדריך הטלפונים של בזק, הפגיעה בפרטיות הנובעת מכך היא פגיעה של מה בכך. הוראות החוק נגועות בכמה פגמים משמעותיים, שלהלן יפורטו חלקם: הסיפה לס' 3 מתייחס לצורך לאזן בין צרכים חברתיים לבין הזכות לפרטיות, תוך התעלמות מזכויות אחרות הנפגעות בעקבות ה־Data Mining, כגון חופש הביטוי, חופש ההתאגדות והקניין. דומתני, כי הנתונים הנאספים בדרך זו ללא בקרה משמעותית עלול להעמיד בסכנה את מצבור חירויות הפרט הנפגעות כתוצאה מכך ואף להרתיע אנשים משימוש תמים וחופשי במערכות מחשב. ס' 3 מתייחס ל"גילוי עברות", כך שהרשויות עלולות להפעיל את החוק גם במקרים של עברות קלות ביותר – מסוג חטא. אין בחוק דרישה לסף ראיות הוכחתי כלשהו. בנוסף, הוראת ס' 8(א) לחוק זה מאפשרת זרימה חופשית יתר על המידה של המידע שנתקבל בין גורמי החקירה השונים. לעתירה תלויה ועומדת בנושא זה ראו: בג"צ 3809/09 **האגודה לזכויות האזרח נ' משטרת ישראל**. בדומה, בס' 70 לחוק משק הגז הטבעי, התשס"ב–2002 מנויות סמכויות תפיסה וחיפוש דרקוניות, המסמיכות את מנהל רשות הגז הטבעי לחדור לחומר מחשב לשם פיקוח על ביצוע הוראות החוק, **ללא צו** שיפוטי וללא צורך בסף ראיות מחשידות. כן ראו ס' 32 (א) לחוק מאבק בארגוני פשיעה, התשס"ג–2003 (סמכות לתפוס חפצים), המסמיך שוטר לתפוס מחשב, בסיטואציות מסוימות, **ללא צו של בית משפט**.

194 דומתני, כי שומה גם על הרשות המבקרת לעמוד בגדרי הוראות הבקרה השיפוטית בכל הנוגע לחיפוש ולהאזנת סתר במערכות מחשב. על פי ס' 26 לחוק מבקר המדינה (נוסח משולב), התשי"ח–1958, סמכויות המבקר מנויות בחוק ועדות חקירה, התשכ"ט–1968 בשינויים המחויבים, והן מאפשרות לו **לדרוש מעד להמציא מסמכים**. המבקר לא הוסמך בחקיקה לערוך חיפוש בכליו או במחשביו של אדם ללא הסכמתו ואף לא לבצע האזנת סתר לשיחות עובדים בגוף המבוקר. אמנם ס' 12 לחוק ועדות חקירה (צו חיפוש) מסמיך את ועדת החקירה **להוציא צו חיפוש**, אך ס' זה **אינו** נכלל בגדר סמכויות המבקר, שכן רק הסמכויות המנויות בסעיפים 8 עד 11 ו־27(ב) ו־(ד) לחוק ועדות חקירה נמנות בגדר סמכויותיו. ובכל מקרה, ס' 12 לחוק ועדות

בסדרה של הצעות חוק.[195]

פגם חמור נוסף נוגע לדרישות ההוכחה הקיימות, הנמוכות יתר על המידה. במסגרת בקשה לצו חיפוש במחשב[196,197] די בהוכחת "יסוד להניח",[198] ובהליכים לקבלת צו האזנת סתר – "חשד לקיומה של עברה מסוג פשע".[199,200]

עולה, כי הדין הקיים לוקה בחוסר איזון ראוי בין הצורך החברתי בחיפוש בכליו של הפרט, לבין ההגנה על עקרון סודיות המידע הממוחשב. מצב זה אינו ראוי אל נוכח הצורך במנגנוני בקרה אפקטיביים על החיפוש השלטוני ואל נוכח חומרת הפגיעה הנובעת מחדירה לרשות הפרט, וספק אם הוא עומד בעקרון המידתיות המנוי

חקירה מסמיך את הועדה להוציא צו חיפוש רגיל, ואינו כולל את הסמכות הייחודית של חיפוש במערכות מחשב או האזנת סתר. עולה, שעל המבקר להקפיד שלא לחרוג מסמכויותיו ולא לערוך חיפושים במערכות ממחשב בהיעדר הסכמה מבעל המידע הממוחשב – העובד בגוף המבוקר, במובחן מהסכמת הגוף המבוקר – בעל המחשב.

195 ראו הידיעה שלפיה רשויות הביטחון מבקשות להרחיב את רשימת הגופים הציבוריים המבוקרים על ידם, מכוח החוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח–1998, למוסדות, כגון האוניברסיטאות, הבורסה והחברה האחראית על התקשורת הטלפונית היוצאת מישראל (נורית פלתר "השב"כ יפקח על מחשבי האוניברסיטאות והבורסה" **ידיעות אחרונות** 30.4.2007, 17). דומתני, שראוי להפחית לחלוטין את מידת **הגישה** השלטונית אל מערכות המחשבים של יצורי כלאיים מעין אלו.

196 השוו למנגנון החיפוש הראוי הקבוע בס' 16(א) לחוק עוולות מסחריות, התשנ"ט–1999, שעל פיו בית המשפט רשאי להסמיך כונס נכסים לתפוס מחשב או מידע ממוחשב, אם הוכח כי "קיים **חשש של ממש** לביצועה של עוולה" (ההדגשה שלי – ש.א.ג.).

197 והשוו לתיקון מספר ארבע בחוקה האמריקאית בנוגע לחיפש ותפיסה (1791): "The right of People to besecure in their persons, houses, papers, and effects, against unreasonable searches and seizures sall not be violated, and no warrants shall issue, but upon *probable cause,*supported by oath or affirmation, and particularly describing the place to be searched, and the person or thing to be seized" (ההדגשה שלי – ש.א.ג.).

כמו כן ראו: Coletta Christine A., *Laptop Searches at the Unitd States Borders and the Border Searchs Exception to Exception to the Fourth Amendment*, 48 B.C. L. REV. 971 (2007); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

198 כללי הקבילות הראייתית גמישים יותר כאשר היסוד הראייתי הנדרש הוא של "יסוד להניח", אף במה שקשור לעדות שמיעה, ראו בש"פ 1572/05 **זוארץ נ' מדינת ישראל** , תק-על 05(2) 64 (2005).

199 בע"פ 1302/92 **מדינת ישראל נ' נחמיאס**, פ"ד מט(3) 309, 311, 325 (1995) נקבע, כי על השופט הדן בבקשת האזנת סתר לבחון אם אכן יש בידי החוקרים מידע המספיק לעורר **חשד** נגד הנוגעים בדבר, במידה המצדיקה פגיעה בפרטיותם בדרך של האזנת סתר לשיחות הטלפון שלהם, וכי ייתכן שיש מקום לדרוש שהבקשה תלווה בתצהיר של השוטר המבקש.

200 אמנם גם בבקשות מעצר קצר מועד נדרשת הוכחה ראייתית נמוכה, אך שם ניתנת לחשוד **האפשרות להתגונן ולהביע את עמדתו בפני שופט המעצרים**, ואילו בענייני חיפוש והאזנת סתר ובמיוחד בחיפוש סמוי (No-knock search) ההליך נעשה לרוב **במעמד צד אחד.**

בחוק יסוד: כבוד האדם וחירותו. ואכן, אחד הכלים העיקריים המסייעים כיום במשימה הקשה של איזון בין צרכים לערכים מתנגשים הוא **עקרון המידתיות**, הקבוע בפסקת ההגבלה והבוחן את השאלה אם החלטת הרשות הנה מידתית לאור התכלית שהיא באה להגשים.[201] ראוי לפיכך, לתקן את הדין הקיים בהתחשב בעקרונות האיזון שהותוו בסעיף 4.1 לפרק ב׳ דלעיל: התניית הליך החיפוש בבקרה משפטית; העלאת סף הראיות הנדרש לקבלת צו חיפוש והאזנה; ואימוץ מעין סניגור ממונה, שייצג את האינטרס בהגנת סודיות המידע הממוחשב במסגרת בקשות חיפוש הנערכות במעמד צד אחד.

אשר לתחולתם המובדלת של דיני החיפוש השונים של חוק המחשבים וחוק האזנת סתר: חוק המחשבים כולל תיקון לפסד״פ בכל הנוגע לחיפוש במערכות מחשב, ואילו הפרוצדורה לקבלת צו להאזנת סתר קבועה בחוק האזנת סתר. ככלל, בחוק האזנת סתר ישנם הליכים מחמירים יותר לקבלת צו שיפוטי ויחסית, הוא מספק הגנה טובה יותר על סודיותו של המידע הממוחשב: על חוק האזנת סתר חלים עקרונותיה המחמירים יותר של פסילת ראיות על פי דוקטרינת ״פרי העץ המורעל״,[202] המאפשרת פסילת ראיות שהושגו שלא כדין ובקרה שיפוטית של החיפוש השלטוני, גם אם בדיעבד; ראיות שהושגו בחיפוש במחשב שאינו כדין, לעומת זאת, תהיינה קבילות בכפוף לדוקטרינת קבילות מצומצמת שמקורה בפסיקה.[203] כמו כן, ניתן לקבל צו להאזנת סתר רק **בעברות חמורות יותר** — בעברות מסוג פשע, ואילו דיני החיפוש במחשבים אינם מוגבלים לרף עברה מסוים.[204]

---

201 ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו (פגיעה בזכויות) מאפשר פגיעה בזכויות יסוד, בין היתר, ב״במידה שאינה עולה על הנדרש״. אף שחלק מדיני החיפוש דנן וכן חוק האזנת סתר נחקקו לפני חקיקתו של חוק יסוד: כבוד האדם וחירותו, על רשויות החקירה להפעיל את סמכויותיהן המאפשרות להן לפגוע בזכויות יסוד בהתאם לעקרון המידתיות הקבוע בפסקת ההגבלה. ראו: ע״פ 98/1668/98 **היועץ המשפטי לממשלה נ׳ נשיא בית־המשפט המחוזי בירושלים**, פ״ד נו (1) 625, 632 (2002) (הנשיא דאז ברק); בג״ץ 5016/96 **חורב נ׳ שר התחבורה**, פ״ד נא(4) 1, 43 (1997); בג״ץ 8070/98 **האגודה לזכויות האזרח נ׳ משרד הפנים**, פ״ד נח(4) 842, 845—846 (2004) (השופטת דורנר); בג״ץ 3379/03 **מוסטקי נ׳ פרקליטות המדינה**, פ״ד נח(3) 865, 908 (2004) (השופט אור).

202 ס׳ 13 לחוק האזנת סתר (ראיות).

203 ע״פ 5121/98 **יששכרוב נ׳ התובע הצבאי הראשי**, תק־על 2006(2) 1093 (2006). ראו גם ת״פ (י־ם) 1934/05 **מדינת ישראל נ׳ ואנונו**, תק־של 2007(3) 365 (2006), שם נפסלו ראיות שהופקו שלא כדין ממחשב.

204 בחוק המחשבים הוגבלו הגורמים היכולים לערוך את החיפוש ל״**בעל תפקיד מיומן**״ — לגורם מקצועי, וזאת, כדי למנוע נזק או שינוי של המידע הממוחשב ואולם בעניין **אריש**, לעיל ה״ש 116, נקבע שבעל תפקיד מיומן לחיפוש בטלפונים סלולריים ״יכול להיות אף **שוטר רגיל**״ או ״אדם סביר״, וזאת אף שגם בטלפון סלולרי יכולות להיות סיסמאות הדורשות פיצוח; גם בו ניתן לשתול ראיות; גם הוא עשוי לאחסן מידע אישי רגיש, ואף על פי שהמידע המאוחסן בו עלול להינזק במהלך חיפוש בלתי מיומן. לפיכך, ראוי להחיל את דיני החיפוש במחשב באופן

ככלל, את חוק האזנת הסתר ראוי לפרש באופן רחב ולהחילו, במידת האפשר, גם על חיפוש במערכות מחשב, שכן מהבחינה העונשית ומבחינת הבקרה השיפוטית על החיפוש השלטוני, חוק זה מספק הגנה טובה יותר על חירויות אדם (קניין, אוטונומיה, פרטיות וחופש ביטוי) ועל הצורך התועלתני לאפשר שימוש חופשי במערכות מחשבים.[205] על פי גישה זו, סיווגו הפרשני של אקט החיפוש כ"האזנת סתר" בא לוודא שהאצבע לא תהיה קלה על מתג החיפוש במערכות מחשבים, וכי תתאפשר פגיעה פחותה בעקרון סודיות המידע הממוחשב. כך אף יושגו יתרונות תועלתניים נוספים, למשל צמצום העומס המוטל על ספק השירות כידו הארוכה של רשויות השלטון במהלך חיפוש בתקשורת בין מחשבים, דבר הכרוך בטרחה רבה.[206] ואכן, בפרשת **פילוסוף**[207] מציין בית המשפט, שמבחינה נורמטיבית שיחה של הפרט המתנהלת באמצעות דוא"ל היא ערך חשוב בחברה, וכי כאשר קיימות שתי פרשנויות אשר שתיהן מתיישבות עם לשון החוק, יש להעדיף את הפרשנות המקיימת את ערכי היסוד של המשפט ומתיישבת עם תכלית החקיקה. עם זאת, כאמור בסעיף 0 דלעיל, מבחינת **הדין הראוי**, על הוראות החוק הנוגעות לחדירה למחשב ולחיפוש בו להחמיר יותר מאלו הנוגעות להאזנת סתר; שכן, בין היתר, חדירה למחשב מאפשרת את שינוי המידע הממוחשב ואת שיבושו, ואילו האזנת סתר הנה **פסיבית**.

כדי לדעת איזו הוראת חיפוש תחול בכל שלב של המסע הווירטואלי יש, כעיקרון, ליישם את כל המסקנות דלעיל בנוגע לתחולתם של חוק המחשבים וחוק האזנת סתר: לפיכך, למשל, כאשר מבוצעת חדירה לתחנת ביניים שבה מאוחסן המסר האלקטרוני בדרכו ליעד, כגון לשרת של ספק שירות האינטרנט, חל חוק האזנת סתר, ועל כן יש להצטייד בצו להאזנת סתר,[208] והוא הדין בעניין בקשות ליירוט תעבורת דואר אלקטרוני **עתידית**.[209] כאשר נעשה חיפוש במחשב ומועתק דואר אלקטרוני שכבר הגיע ליעדו, יש לקבל צו חיפוש על פי הפסד"פ, אף אם הוא טרם נקרא או נפתח על ידי הנמען.[210] עם זאת, סעיף 23א(ג) לפסד"פ קובע **חריג** לכלל זה, הנוגע

שווה על מחשבים "רגילים" ועל מחשבים "שונים", כדוגמת טלפון סלולרי.

205 ראו גם נמרוד קוזלובסקי **המחשב וההליך המשפטי – ראיות אלקטרוניות וסדרי דין** 54 וה"ש 14 (2000), המציין את רפסותן של הוראות הפסד"פ בכל הנוגע לשמירה על פרטיותו של בעל המידע הממוחשב, שכן אין בס' 23א לפסד"פ הנחיות ערכיות להפעלת צו חיפוש.

206 בפרשת **נטוויז'ן**, לעיל ה"ש 94, הבהיר סגן הנשיא אבן ארי את הפגמים הנורמטיביים והפרקטיים הכרוכים בדבר.

207 לעיל ה"ש 94.

208 וראו גם נימוקיו של קוזלובסקי, לעיל ה"ש 205, בעמ' 106.

209 ראו ענין **פילוסוף**, לעיל ה"ש 94, שם נקבע, כי כל דואר שיגיע לאחסון מיום הוצאת הצו בא בגדר האזנת סתר.

210 בענין **פילוסוף 2**, לעיל ה"ש 176, נקבע, שגם תפיסה של הודעה **שטרם** נקראה על ידי הנמען וגם תפיסה של הודעה **שכבר** נקראה על ידי הנמען, באות בגדרם של דיני החיפוש והתפיסה הייחודים למחשבים, שכן מדובר ב"מצב מובהק של מידע נייח המאוחסן באורך קבע", שהוראות החיפוש

לחיפוש שלטוני: "קבלת מידע מתקשורת בין מחשבים אגב חיפוש לפי סעיף זה לא תיחשב כהאזנת סתר לפי חוק האזנת סתר". לפיכך, כאשר **במהלך** חיפוש שלטוני במחשב מתקבל מסר אלקטרוני, ניתן יהיה להעתיקו כדין, אף שמלכתחילה צו החיפוש התיר חיפוש במחשב, ולא האזנת סתר לתקשורת בין מחשבים.[211]

3.2 צידוקים אזרחיים לחדירה פרטית למחשב– הדין הקיים

כמפורט בסעיף 4.2 לפרק ב' דלעיל, כורח המציאות מחייב להתיר, במקרים חריגים ומגודרים, חדירה מסויגת למחשב הזולת לצרכים תועלתניים. ואולם בחוק המחשבים בולט ההיעדר של סייגים לעקרון הסודיות, **ואין** בו חריגים המתירים חדירה פרטית למחשב (למעט כאלו הנוגעים לחיפוש שלטוני). לעומת היעדר זה, בחוק הגנת הפרטיות ישנו ניסיון ראוי לשבח לקיים איזון בין אינטרס הפרטיות מחד, לבין אינטרסים ציבוריים ואישיים מנוגדים.[212] איזון זה בא לידי ביטוי במתח שבין סעיף 2 לחוק הגנת הפרטיות, הכולל עברות ועוולות של פגיעה בפרטיות, לבין פרק ג' לחוק (הגנות), ובמיוחד סעיף 18 לחוק (הגנות מה הן), הקובע הגנות במשפט הפלילי והאזרחי.[213] סעיף זה מכיל בין היתר, הגנה מפני מעשה של פגיעה בפרטיות הזולת שנעשתה על ידי הנתבע או הנאשם בתום לב,[214] באחת מהנסיבות המנויות בסעיף 18

במחשב חלות עליו. בית המשפט מסתמך על סעיף 23א(ג) לפסד"פ ה"מתיר לרשויות החקירה לתפוס הודעות דוא"ל שהתקבלו מ'תקשורת בין מחשבים', 'בזמן אמת', בעת ביצוע החיפוש במסגרת צו חיפוש" וקובע, כי תכליתו של סעיף זה כוללת גם מקרים שבהם הדואר האלקטרוני כבר הגיע ליעדו.

211 בדברי ההסבר לס' 31א להצעת חוק המחשבים נאמר: "במחשבים בעלי מערכות תקשורת תיתכן קליטה של חומר חדש המתקבל במחשב בזמן החיפוש. אף שיש בזה מרכיב התנהגותי של האזנת סתר, מוצע להבהיר שחומר שנקלט כאמור תוך ביצוע צו חיפוש אינו כפוף להוראות חוק האזנת סתר, המחייב קבלת צו מיוחד כדי לבצע את האזנת הסתר".

212 ס' 2 לחוק הגנת הפרטיות כולל עוולה של האזנת סתר וס' 18 לחוק הגנת הפרטיות חל עליו.

213 חוק הגנת הפרטיות כולל, מחד הגנה נרחבת על עיקרון הסודיות, ומאידך – עקרונות מתנגשים (ס' 18 לחוק זה). בהעדר **יסוד מאזן**, כגון עקרון המידתיות, בין הכללים המשפטים הסותרים הללו, ראוי לייבא לס' 18 בחוק הגנת הפרטיות את **עקרון המידתיות** מפסקת ההגבלה בחוק־יסוד: כבוד האדם וחירותו.

214 המונח "תום לב" בחוק הגנת הפרטיות פורש בדרכים שונות וסותרות. כך, בפרשת **גלעם**, לעיל ה"ש 42, בעמ' 1153, קבע הש' אריאל (ברוב דעות), כי מדובר במבחן "**מעורב סובייקטיבי־אובייקטיבי**", כשלחלק הסובייקטיבי יש השפעה רבה יותר במסגרת איזון האינטרסים. וראו גם סגל, לעיל ה"ש 183, בעמ' 198–199. לעומת זאת, הנשיא (כתוארו אז) ברק אימץ מבחן **סובייקטיבי** להגדרת דרישת תום הלב, אשר בפרשת **גלעם** (שם, בעמ' 1164) (מיעוט) התבטא בשאלה – מה סבר הפוגע הספציפי ובפרשת **פלונית**, (לעיל ה"ש 49, בעמ' 1747) – פעולה מתוך אמונה כי הפגיעה הנה במסגרת ההגנה אותה מעלה הפוגע. ובהמשך: "**מקום שהפגיעה בפרטיות אינה מידתית, תקום הנחה שהפוגע פעל שלא בתום לב**". ואולם ספק אם אכן מדובר

(2): "(ב) הפגיעה נעשתה בנסיבות שבהן הייתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה; (ג) הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע; (ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים".[215]

סבורתני, כי ראוי וניתן להשלים את הלאקונה הקיימת בחוק המחשבים בנוגע לחריגים לעקרון סודיות המידע הממוחשב באמצעות היסוד "שלא כדין" הטבוע בסעיף 4 לחוק.[216] משמעותו המקובלת של רכיב רב־תכליתי זה הנה **מעשה שנעשה ללא הֶצדק שבדין**, והוא מאפשר "לייבא" **הֶצדקים** ממקורות חיצוניים לחוק שבו מדובר – מחוקים אחרים או מעקרונות משפט כלליים.[217] כך ניתן להחיל על חוק המחשבים את **ההצדקים להפרת עקרון הסודיות** המנויים בסעיף 18 לחוק הגנת הפרטיות[218] או את העיקרון המשפטי הכללי בדבר עזרה עצמית (Self Help).[219] עם זאת, דומתני, שככלל, את ההגנות המנויות בסעיף 18 לחוק הגנת הפרטיות ובחוקים אזרחיים אחרים[220] ראוי לאמץ במסגרת צו שיפוטי,[221] ורק במקרים חריגים – כהגנת

במבחן סובייקטיבי, אל נוכח הכללתו של עקרון המידתיות ברכיב "תום לב". (ההדגשה שלי – ש.א.ג.).

215 בדברי ההסבר לס' 6 (2) להצעת חוק הגנת הפרטיות, התשמ"א–1980, ה"ח 1453, מוסבר, כי הגנה זו חלה גם על היחסים שבין עובד למעביד, תוך סיוג הסיבות למעקב הבא בגדרה: "הוא הדין לגבי **מעביד** המתחקה [...] אחרי עובדו כדי לברר **אם העובד אינו מפר את חובותיו** לפי הסכם העבודה" (ההדגשה שלי – ש.א.ג.).

216 כך הופך היסוד "שלא כדין" לרכיב **רב משמעויות** בחוק זה, המסדיר את דרישת ההסכמה, הצידוקים ונטלי ההוכחה.

217 מ' חשין **מיטלטלין בדין הנזיקין** 84 (התשל"א); עדי אזר "דין היסוד 'שלא כדין' בדין הפלילי" **עיוני משפט** ח 561, 566–567 (1981) סבור, שהיסוד "שלא כדין" מהווה מכשיר לייבוא **הגנות** מדינים אחרים, לבר פליליים ולבר נזיקיים, לעזרת הנאשם – הנתבע; לדיון בפרשנויותיו האפשריות השונות של המונח "שלא כדין" ראו אהרוני־גולדנברג, לעיל ה"ש 51, בעמ' 291–316. ראו גם מיגל דויטש "חוק המחשבים במבחן העתים – זווית המבט של מציע החוק" **שערי משפט** ד 249 (2006). ע"פ 2/73 **סלע נ' מדינת ישראל**, פ"ד כח(2) 371, 374 (1974); ע"פ 324/73 **דנוך נ' מדינת ישראל**, פ"ד כח(2) 706, 707 (1974). אך השוו לעמדתו המסייגת של ש' ז' פלר **יסודות בדיני עונשין** כרך א 539 (1984).

218 גם עקרון תקנת הציבור יכול לשמש מקור לא אכזב להגנות בתחום זה. בדומה, ניתן להפעיל את זכות העיכבון מכוח הצירוף של ס' 11 ו־13 לחוק המיטלטלין, התשל"א–1971.

219 בענין **סלע**, לעיל ה"ש 217, נפסק, שמכוח היסוד "שלא כדין" הנאשם יוכל להסתמך על עקרון עשיית דין עצמי כצידוק חיצוני למעשיו.

220 לדוגמה, ס' 11 (ג) לחוק המיטלטלין, התשל"א–1971. גם תקנת הציבור עשויה לשמש מקור לא אכזב להגנות בתחום זה.

221 המשפט הישראלי מכיר גם בצורך בקבלת צווי חיפוש פרטיים. ואכן, צווי אנטון פילר מבוססים על התפיסה כי ניתן להתיר לגורם אזרחי לבצע חיפוש (תוך פגיעה בפרטיות), שעה שאינטרסים חשובים תלויים על הכף. תפיסה זו מיושמת גם בנוגע למערכות מחשב. ראו: תק' 387 לתקנות סדרי הדין האזרחי, התשמ"ד–1984 (חיפוש בחומר מחשב) וס' 16 לחוק עוולות מסחריות,

עזרה עצמית.

משניתן להפעיל מנגנוני הגנה על עברת החדירה למחשב, עולה, כי ההסכם הקיבוצי הכללי בנוגע לחדירת מעביד לקובצי מחשב של עובדו הנו בבואה של הדין הקיים, בכל הנוגע לאיסור חדירה למחשב, מחד, ולהיתרים לחדירה למחשב, מאידך. אמנם הוא אינו דן בהגנת עניין אישי כשר, כמו במקרה של מי שחודר לקובץ עובדו כדי להשיג ראייה לצורך הגנתו המשפטית, אך הוא תורם להבהרת הדין הקיים — ובכך טמונה מעלתו העיקרית.

ד. חדירה שלטונית ופרטית למחשבים: סיכום ומסקנות

בראשיתו של מאמר זה נשאלה השאלה: מהו גדרה הראוי של עברת החדירה למערכות מחשבים. הניסיון לענות על קושייה זו מעלה, כי המחשב חיוני להמשך תפקודה התקין של החברה המודרנית, וכי עבור היחיד הוא מהווה קניין מכונן, היורד לשורש נשמתו.[222] עם זאת, למהפכת המחשבים יש גם צדדים אפלים, המתבטאים בתופעת המחשוב הפולשני. ואכן, חדירה שלטונית ופרטית למערכות מחשבים פוגעת באינטרסים תועלתניים, שכן היא בולמת את הקִדמה המתאפשרת הודות לפונקציות החיוביות של מערכות המחשבים ואת תפקודה התקין של החברה). התופעה אף גוררת פגיעה במצבור של חירויות אדם בסיסיות — שניתן לכנותו בשם "**חירות הסודיות במידע הממוחשב**": בזכות לפרטיות; בחופש הביטוי (החשש מחדירה למחשב עלול לגרום ליחיד להימנע מלעשות שימוש במחשב לצורך פיתוח חשיבה ייחודית); בחירות הקניין (שליטת בעל **המידע הממוחשב** — ולא רק בעל המחשב — על המידע הפרטי שיצר, ללא עין זרה צופייה); ובזכות הפרט לאוטונומיה (הסכמה חופשית, מדעת ומותאמת — לְמה ולמי ניתנה ההסכמה). עולה שתופעת המחשוב הפולשני חותרת תחת חירות השליטה של בעל המחשב בנכסיו הגשמיים (המחשב עצמו) והערטילאיים (המידע הממוחשב).

התלות החברתית הרבה במערכות מחשב מחד, ופגיעתה הקשה של תופעת המחשוב הפולשני מאידך, מצריכים את גיוסם של מירב הכלים המשפטיים להגנת זכות הסודיות במידע הממוחשב. לצורך כך יש לאמץ כמה עקרונות משפטיים בחקיקת עברת החדירה למחשב. ראשית, הגדרת ה"מחשב" שעליו תיפרש הגנת החוק תהיה רחבה, כדי להביא בגדרה את הפונקציות המגוונות שממלא המחשב. שנית, לפרט יש זכות טבעית לחומר המחשב שיצר, צבר או אסף והאגור במחשב שלו.

התשנ"ט–1999. ראוי כמובן להכפיף מתן היתרים אלו לקבלת ערבויות להטבת נזקו של הפרט שלמחשביו בוצעה החדירה.

222 ראו רבי צדוק הכהן מלובלין, **ישראל קדושין**, ה': "קניינו של אדם הריהו שייך לשורש נשמתו וכל קנייני האדם הרי הם לצורך קיומו בעולם הזה וחלקי חיותו מתפשטים בהם".

זכות בסיסית זו אינה בוחנת את איכותו ואת אופיו של המידע הממוחשב; המידע האגור במחשב או בקווי תקשורת בין מחשבים מהווה קניינו של יוצרו, ללא קשר לתוכנו, לטיבו ולאופיו ולמקום שבו הוא מאוחסן, ובלבד שאין מדובר במידע ממוחשב המופיע באתרים פתוחים. שלישית, הגנה ראויה על המידע הממוחשב תיפרש על המידע הממוחשב, במובחן מהמחשב עצמו, וזאת, כדי להגן גם מפני חדירה פנימית, כגון של עובדים. רביעית, הפגיעה בסודיות המידע הממוחשב איננה פונקציה של הבעלות הקניינית במחשב שבו הוא נמצא, ולפיכך, ליוצר המידע הממוחשב יש זכות קניינית בו, אם כי מדובר בזכות מוחלשת שעה שמדובר ביציר כלאיים ערטילאי, המאוחסן ברכושו הפיזי של הזולת. כך, מעביד החודר לקובץ אישי של עובד, המאוחסן במחשב שלו, פוגע בפרטיותו למרות בעלותו הקניינית במחשב, שכן זו איננה מכשירה את השליטה במידע האישי השייך לעובד. חמישית, היסוד אשר תוחם את גדרו של המידע הממוחשב הוא הסכמת בעל המידע לגישה אליו; ההסכמה שיסודה בזכות היסוד לאוטונומיה, היא המשמשת מפתח הכניסה למרחבו הווירטואלי של הזולת.

בפרק ג' של המאמר נבחן הדין הקיים. סקירה זו העלתה, כי שילובם של חוק המחשבים וחוק האזנת סתר נותן, ככלל, מענה ראוי להגנת עקרון סודיות המידע הממוחשב, שכן תחולתם אינה כפופה לגרימת נזק, והחוקים חלים על כל סוג של מידע, ללא הבחנה בין מידע אישי רגיש לבין מידע סתמי; גדר ההפרדה בין כניסה כדין למחשב או להאזנה כדין לשיחת הזולת לבין עברה פלילית, היא פעולה הנעשית ללא הסכמה. כלומר בחוק המחשבים ובחוק האזנת סתר האוטונומיה של בעל המידע הממוחשב היא המחסום בפני הסגת גבול. כמו כן נעשה ניסיון לענות על השאלה שהותיר בית המשפט העליון בערעור **בדיר**[223] ב"צריך עיון": איזה חוק חל כאשר מבוצעת חדירה למחשב ומיורט מסר אלקטרוני שכבר הגיע ליעדו. התשובה שניתנה על שאלה זו הנה, שכאשר החדירה למחשב כוללת קריאת דואר אלקטרוני שכבר נתקבל ונשמר במחשב, אין מדובר בהאזנת סתר ל"שיחה", אלא בחדירה למחשב, שעליה חל רק סעיף 4 לחוק המחשבים. לעומת זאת, יש לראות ביירוט מסר אלקטרוני העוצר בתחנות ביניים בדרכו למחשב היעד (למשל, שרת של ספק שירות) אתנחתה זמנית, שחלה עליו עברת האזנת הסתר. במאמר ננקט קו פרשני שונה מזה המאומץ בערכאות בתי המשפט לגבי תחולת הדין הקיים: כך, כשמבוצעת חדירה למחשב ובמקביל – האזנה לתקשורת בין מחשבים, חל רק סעיף 2(א) לחוק האזנת סתר, שכן הסיפה לסעיף 4 לחוק המחשבים קובע מפורשות שהאזנת סתר לא באה בגדר "חדירה". ואכן, את חוק האזנת סתר ראוי **לפרש** באופן רחב ולהחילו, במידת האפשר, גם על חיפוש במערכות מחשב. זאת, מאחר שמהבחינה העונשית ומבחינת הבקרה השיפוטית על החיפוש השלטוני, חוק זה מספק הגנה טובה יותר על חירויות

223 לעיל ה"ש 8.

אדם ועל הצורך התועלתני לאפשר שימוש חופשי במערכות מחשבים.

חרף חשיבותו הרבה, עקרון סודיות המידע הממוחשב איננו אבסולוטי, ויש לאזנו עם צרכים תועלתניים וליברטריאניים מנוגדים, באמצעות דיני החיפוש העצמית והגנות אזרחיות. החיפוש השלטוני מהווה חלק חיוני ממשטר השואף להגן על ביטחון תושביו ועל שלומם. בשל אופיין התיעודי של מערכות מחשב, אינטנסיביות השימוש בהן ואפשרות הגישה ממרחק אליהן, הן מהוות מקור בלתי נדלה של ראיות ומידע עבור רשויות השיטור והביטחון. עם זאת, חדירה שלטונית בלתי מבוקרת עלולה לפגוע במרקם החיים בחברה ולהוביל למשטר שבו השלטון מרכז בידיו מידע רב ומיותר על הפרט. ואולם בחינתו של הדין הקיים בנושא העלתה, כי מידת ההגנה הנפרשת כל אינטרס הסודיות במידע הממוחשב בחוק האזנת סתר ובחוק המחשבים נחלשת במידה ניכרת כאשר מדובר בחדירה שלטונית למערכות מחשב, במיוחד בכל הקשור לצווים הניתנים במעמד צד אחד. פגם חמור נוסף נוגע לדרישות ההוכחה הקיימות, הנמוכות יתר על המידה. לפיכך, את חוסר האיזון הקיים בין הזכות לסודיות במידע הממוחשב לבין האינטרס התועלתני שבשמירת הסדר והביטחון ראוי לתקן בהתחשב בעקרונות האיזון שהותוו במאמר: התניית הליך החיפוש בכליו הממוחשבים של הפרט בבקרה משפטית, שכן זו מהווה מחסום חיוני בפני חיפושים מיותרים ובפני רדיפה שלטונית של האזרח; העלאת סף הראיות הנדרש לקבלת צו חיפוש והאזנה; ואימוץ מעין סנגור ממונה, שייצג את האינטרס בהגנת סודיות המידע הממוחשב במסגרת בקשות חיפוש הנערכות במעמד צד אחד. את המקרים שבהם לא יידרש צו חיפוש יש להגביל לסיטואציות יוצאות דופן, כגון כאלו שבהן נשקפת סכנה מידית, ברורה וחמורה לחיי אדם ולרכושו.

גם הפרט זקוק לאפשרות להגן באופן מידי על גופו או על רכושו מפני פגיעה. ראוי שהדין האזרחי יכיל פרוצדורה אזרחית המאפשרת לגורמים פרטיים חדירה למערכות מחשב של זולתם, שעה שאינטרסים חשובים עומדים על כף המאזניים ואף שהם מנוגדים לעקרון סודיות המידע הממוחשב. בהיעדר אפשרות פרקטית של פנייה לבית המשפט או למשטרה, ראוי להתיר לפרט להפעיל את סעדי העזרה העצמית, שיאפשרו את חדירתו למחשב הזולת – אך במידתיות ובצמצום, וזאת, כדי למנוע מעגלי נקמה בלתי פוסקים ואבדן שליטה שלטוני. עיון ראשוני בחוק המחשבים מעלה, כי הוא נעדר סייגים לעקרון סודיות המידע הממוחשב, שכן הוא אינו מכיל הגנות ספציפיות מפני חדירה למחשב, וזאת בניגוד לחוק הגנת הפרטיות. במאמר הוצע לייבא לחוק המחשבים את ההגנות הכלליות של עשיית דין עצמי ואת ההגנות הקבועות בסעיף 18 לחוק הגנת הפרטיות באמצעות המונח "שלא כדין", במשמעו כ"**ללא צידוק בדין חיצוני**".

לסיום. טכנולוגיית המידע, המסייעת בקידומה הכלכלי, התרבותי והמדעי של החברה, טומנת בחובה אף סכנות רבות, שכן היא מאפשרת לגורמים בלתי קרואים לחדור למערכות מחשבים ולעשות במידע האגור בהן כבשלהם. כך מתווספים אל

יוצר המידע הממוחשב "אחים חורגים" רבים: "האח הגדול", "האח הקטן" (תאגידים, אתרי אינטרנט, חברות פרסום מקוון) ו"האח הבינוני" (האקרים, מעבידים, עובדים וסתם גולשים משועממים). בפועל, תופעת המחשוב הפולשני שמה לְאַל את חירות השימוש והשליטה במידע הממוחשב ועלולה לבלום את הקִדמה שאליה מוליכה מהפכת המחשבים. מאידך, קיימים צרכים תועלתניים וליברטאריניים, המצדיקים כניסה לא מורשית למערכות מחשב – לצורך הגנת אינטרסים חברתיים חיוניים וחירויות אדם. לפיכך, התזה שהוצגה במאמר זה הנה מורכבת. מחד, יוכל עקרון סודיות המידע הממוחשב לשמש "חומת אש" טכנולוגית (*firewall*), **אשר תסגור את** המחשב בפני אורחים בלתי קרואים; מנגד, תיפתח **"דלת אחורית"** (*Backdoor*)[224] שתאפשר גישה מסויגת למידע הממוחשב, וזאת לצרכים תועלתניים והומניסטיים.

---

224 "An undocumented way of gaining access to a program, online service or an entire computer system" ניתן לצפייה בכתובת: www.webopedia.com/TERM/B/backdoor.html. (נבדק לאחרונה ב־10.1.2009).