

משפט המכונה: אבטחת מידע וחוק המחשבים

מאת

ד"ר מיכאל בירנהק*

המאמר דן בחוק המחשבים, התשנ"ה-1995, בשני צירים מרכזיים. הראשון, הוא ניתוח פרשני של החוק. המחבר מראה כיצד הפרשנות התכליתית של חוק המחשבים צריכה לנבוע מהבנת הטכנולוגיה שבה מדובר. את הוראות חוק המחשבים יש לפרש, לפיכך, על רקע עקרונות יסוד של אבטחת מידע. פרשנות זו באה על רקע תפישה רחבה יותר של היחס המורכב והדיאלקטי שבין משפט לטכנולוגיה. הפרשנות המוצעת מספקת הנחיה כיצד יש לפרש את העבירות השונות של החוק, ובמיוחד את העבירות שעניינן חדירה שלא כדין לחומר מחשב, שיבוש והפרעה למחשב ועריכת נגיף מחשב, וקושרת אותן לעקרונות של אימות זהות, בקרת גישה, שלמות המידע וזמינותו. על רקע סביבה פרשנית זו, מתנגד המאמר להחלת העולה של הסגת גבול במיטלטלין בסביבה הממוחשבת.

הציר השני של המאמר בוחן את גורלו של חוק המחשבים בפסיקת בתי המשפט בעשור האחרון, ומנסה לפענח את עמדת בתי המשפט בשאלת היחס שבין משפט לטכנולוגיה. הדיון מצביע על שני נרטיבים עיקריים שהתפתחו בפסיקה בקשר לעבירות מחשב. האחד מגולם בפרשת האנלייזר, ובו משרטט בית המשפט את ההאקד כילד סורר ומקצה לעצמו את תפקיד המחנך ומושיע הטכנולוגיה. הנראטיב השני מגולם בפרשת אבי מזרחי. הדיון שם משקף תפישה רחבה ונכונה יותר של הסביבה הטכנולוגית ושל תפקיד המשפט בה.

* מרצה בכיר ומנהל במשותף של המרכז למשפט וטכנולוגיה, הפקולטה למשפטים, אוניברסיטת חיפה. תודה לניבה אלקין-קורן, רחל ארדוד, אורן גול-אייל, טל זרסקי, נמרוד קולובסקי, חיים רביה וברכה שפירא שהעירו הערות מועילות, וכן לעוזרי המחקר תומר אפלדורף ומיכאל גבע. האחריות, כרגיל, שלי בלבד. זכויות היוצרים שמורות למחבר, ומאמר זה מתפרסם תחת רישיון של Creative Commons, המתיר כל שימוש שאינו מסחרי, לרבות העתקה, הפצה ופרסום, ובכלל זה הכנת יצירות נגזרות, כל עוד יישמר ייחוס המאמר לכותבו ולמקום פרסומו וכל עוד השימוש ביצירות הנגזרות יהיה בתנאים זהים. הרישיון המלא נמצא ב: <http://creativecommons.org/licenses/by-nc-sa/1.0/il>

- א. מבוא
- ב. על משפט ועל טכנולוגיה
- ג. על חוק המחשבים
- ד. אבטחת מידע
- ה. הנועזים (עברייני המחשב) והאמיצים (השופטים)
- ו. סיכום

א. מבוא

פרשת "הסוס הטרויאני" שנחשפה בסוף חודש מאי 2005 הייתה את הציבור בתדהמה: לפי החשד, חברות מובילות במשק נעזרו בשירותיהם של חוקרים פרטיים כדי להחזיר תוכנת ריגול, "סוס טרויאני", למחשביהן של חברות מתחרות.¹ "סוס טרויאני" מאפשר "לשאוב" מידע רגיש ממחשבי הקורבן, ללא רשות, כמובן, וללא ידיעת הקורבן, ומכאן הכינוי של תוכנות ריגול מעין אלה. הפרשה עוררה עניין רב, ובעת כתיבת מאמר זה היא מתגלגלת בבתי המשפט. מובן שהמשפט הוא רק כלי אחד להתמודד עם תופעות מעין אלה, ולצידו אמורות לפעול מערכות חברתיות של חינוך, אתיקה ועוד. האם בידי המשפט כלים להתמודד עם ריגול תעשייתי המתבצע באמצעות מערכות מחשב? אני סבור שחוק המחשבים, התשנ"ה-1995 (להלן: "החוק"), מספק מענה הולם, אלא שכלל חוק, גם הוא טעון פרשנות. מאמר זה מציג פרשנות תכליתית של החוק, שקושרת אותו לעקרונות יסוד של אבטחת מידע, המקובלים במדעי המחשב. פרשנות תכליתית זו באה על רקע תפישה רחבה יותר של יחס דיאלקטי בין משפט לטכנולוגיה. זהו ציר אחד של המאמר.

ציר שני של המאמר יבחן את היישום השיפוטי של החוק בעשור האחרון. האם הצליח החוק במשימתו? האם יכול המשפט להסדיר את הטכנולוגיה? הדין שאציע כאן בוחן את פסקי הדין שהצטברו בעשור האחרון בקשר לחוק ומבקש לשאול מהי עמדת בתי המשפט בבואם להחיל חוק על טכנולוגיה:² האם הם סבורים שהמשפט יכול לחול באשר הוא? האם הם סבורים שהטכנולוגיה חסינה מפני המשפט? בדיקה זו אינה

1 ראו <http://www.haaretz.co.il/hasite/pages/LiArtSR.jhtml?objNo=58189>. הפרשה הניכה עד כה מספר החלטות שיפוטיות בקשר למעצרו של חשודים. ראו במיוחד בש"פ 7368/05 זלוטובסקי נ' מדינת ישראל (4.9.05).

2 בדיקת הצלחתו של חוק היא עניין מורכב. מחקר אמפירי יכול לנסות לבחון אם וכיצד שינו "אנשי הטכנולוגיה" את התנהגותם בעקבות חוק מסוים. למשפטן כלים אחרים, גם אם מוגבלים. המשפטן בוחן את פסיקת בתי המשפט. יש לזכור שהפסיקה משקפת רק את מקרי הקצה, ובמישור הפלילי – רק את אלה שצלחו את משוכת שיקול הדעת של המשטרה והתביעה, ולא בהכרח את ההשפעה היומיומית של החוק.

פשוטה, שכן הפסיקה מצומצמת; אין עדיין פסיקה מנחה של בית המשפט העליון ורוב פסקי הדין הם גזרי דין שניתנו בעקבות הסדרי טיעון או החלטות בקשר למעצר חשודים. עם זאת, ניתן כבר כעת להצביע על שתי עמדות שונות מאוד, או על שני נרטיבים כמעט הפוכים, העולים מתוך הפסיקה. האחד מגולם בעניין **אהוד טננבאום** ("האנלייזר"), והשני בעניין **אבי מזרחי**.³ העמדה הראשונה, זו שבעניין **טננבאום**, מקצה לבית המשפט תפקיד מרכזי בהגנת הטכנולוגיה, אולם למצער, מבלי שמתנהל שיח מספק בין המשפט לטכנולוגיה. בעניין **מזרחי** נמצא שיח כזה, וגם התוצאה, בהתאמה, עדיפה בעיניי.

ב. על משפט ועל טכנולוגיה⁴

1. הצגת השאלה

מהו היחס שבין משפט לטכנולוגיה? שאלה זו הטרידה ומטרידה רבים. כל עוד התפתחה הטכנולוגיה בעצלתיים, ובימים בהם רק חלק מהארץ מלאה משפט, ההתנגשויות בין משפט לטכנולוגיה היו מעטות. הקצב המהיר של התפתחות הטכנולוגיה בסוף המאה הקודמת מחייב תשובה. האם ראוי שהמשפט יסדיר את הטכנולוגיה? האם המשפט יכול לכך? עד כה, המשפט היה הזירה החברתית הטבעית של הסדרת ההתנהגות האנושית. אולי כעת המשפט מיותר, שכן "הקוד הוא המשפט", כלומר, אולי הטכנולוגיה משפיעה על התנהגותנו יותר מאשר המשפט?⁵ במאמר זה אטען, כי יש להבין את היחס שבין משפט לטכנולוגיה כיחס דיאלקטי, ואציע לפרש את חוק המחשבים על רקע הבנה זו. בהתאם, אציע לפרש את החוק כך שיהיה קרוב יותר לעולם הטכנולוגי אותו הוא מבקש להסדיר, ולפי עקרונות המשקפים הבנה רצויה של התפתחות הטכנולוגיה ומקומו של המשפט בהתפתחות כזו. אלה

3 ראו דיון **להלן**, חלק ה.

4 ראו גם, מיכאל בירנהק "חורים ברשת פורנוגרפיה, מידע ועיצוב מדיניות בסביבה דיגיטאלית" **פוליטיקה** 13 (התשס"ה) "Shielding"; 101 Michael D. Birnhack & Jacob H. Rowbottom "Children: The European Way" 79 **Chicago-Kent L. Rev.** (2004) 175 אתיקה עיתונאית ברשת על הסדרה פרטית, חופש העיתונות, כוח ותחרות" **פתוח** – **כתב עת בנושא פוליטיקה, תקשורת וחברה** ה' (2003) 173.

5 לטענה, כי הטכנולוגיה הופכת בפועל לגורם מסדיר, ראו **Code and Other Laws of Cyberspace** (New York, 1999); Joel R. Reidenberg "Lex Informatica: The Formulation of Information Policy Rules through Technology" 76 **Texas L. Rev.** (1997-1998) 553.

מתבססים על עקרונות אבטחת המידע המקובלים בקשר למערכות מידע. אטען, כי יש לאתר את הערך החברתי המוגן על ידי החוק בעקרונות האבטחה הטכנולוגיים. אפתח בשרטוט מסגרת הדיון, שהיא היחס שבין משפט לטכנולוגיה. מסגרת זו הכרחית בעיני כדי להבין את חוק המחשבים, לפרשו ולהפעילו בתבונה. אטען, כי בעת עיצוב מדיניות משפטית לטכנולוגיה, עלינו לאמץ נקודת מבט רחבה של **דיני מידע**: זו מסגרת שערה ליחס המורכב בין משפט, טכנולוגיה וחברה. יש לפרש את כללי המשפט הקיימים או לעצב כללים חדשים, תוך גזירתם מערכים חברתיים ותוך דו-שיח עם מאפייניה הייחודיים הרלוונטיים של הטכנולוגיה שבה מדובר. תפישה כזאת מקנה עדיפות עקרונית לערכים חברתיים ואתיים על פני הטכנולוגיה, ואינה נופלת ברשתה כדבר מובן מאליו, אך גם אינה מתעלמת ממנה. התפישה הזאת מדגישה את הדינמיות של היחסים שבין משפט, ערכים וטכנולוגיה. זו הטענה, וכעת אסביר אותה.

2. דטרמיניזם טכנולוגי או אימפריאליזם משפטי?

מהו, אם כן, היחס שבין משפט לטכנולוגיה? תשובה קיצונית אחת היא עמדת הדטרמיניזם הטכנולוגי.⁶ לפיה, למשפט אין ברירה אלא לסגת מפני הטכנולוגיה. לפי עמדה זו, ניסיונות ההתערבות של המשפט עלולים להזיק להתפתחות הטכנולוגיה, הם בגדר איוולת ובכל מקרה סופם להיכשל. כאן אתמקד בסביבה הדיגיטלית. המצדדים בעמדה הדטרמיניסטית מזכירים שרשת האינטרנט בנויה כרשת מבוזרת, כלומר, מבחינה טכנולוגית, שלטונית, ולמעשה מכל בחינה, אין לה מרכז. בהיעדר מרכז ששולט בכל קצות הרשת, אין למשפט מקום להניח את ידו. עוד מוזכר בהקשר הזה האופי הגלובלי של הרשת למשל, גם אם מדינה פלונית תטיל צנזורה על אתר אינטרנט בשטחה, יצוץ הטקסט המצונזר בנקודה אחרת בעולם.⁷ אבל הטענה אינה רק כי קשה לאכוף את המשפט ברשת. הטענה הדטרמיניסטית חזקה יותר, שכן היא מניחה שהטכנולוגיה נוצרת יש מאין, שהיא בלתי נמנעת, שהיא מתנהלת לפי "חוקים משלה", ואינה כפופה למשפט הקיים. מעמדה זו נובע כי למשפט אין בכלל מקום בהסדרת הטכנולוגיה.⁸

6 לדין ביקורתי ראו Langdon Winner *Cyberlibertarian Myths and the Prospects for Community* (CFP 1997) .available at, <http://www.langdonwinner.org/Cyberlib.html>

7 לדין בצנזורה ברשת ובתמורות שחלו בה, ראו קריין ברזילי-נהון וגד ברזילי "חופש הביטוי וחופש מדומיין באינטרנט על בטלותה והולדתה מחדש של הצנזורה" **שקט! מדברים התרבות המשפטית של חופש הביטוי בישראל** (עורך מיכאל בירנהק) (התשס"ו) 483 ואילך.

8 את העמדה הדטרמיניסטית אפשר למצוא בעיקר בשיח הפופולרי. הטקסט המובהק ביותר הוא "הצהרת העצמאות של האינטרנט", של ג'ון פרי בארלו. ההצהרה, שכל כולה נושבת רוח ליברטריאנית, מציעה הסדרה פרטית של הגולשים במקום משפט המדינה. ראו John Perry *Barlow A Declaration of the Independence of Cyberspace* (1996).

תשובה קיצונית הפוכה היא עמדה שאכנה אותה "עמדה משפטית טהורה". לפי עמדה זו, הטכנולוגיה החדשה היא, לכל היותר, עילה לבחון מחדש הסדר משפטי קיים ולעדכנו, אולם ידו של המשפט היא זו שצריכה להיות על העליונה. עמדה כזו מניחה שהטכנולוגיה היא תוצר של פעילות אנושית ככל פעולה אחרת. אין לה ייחוד מן הבחינה המשפטית וודאי שאין לקבל, לפי עמדה זו, שהטכנולוגיה מתנהלת לפי מערכת כללים עצמאית.⁹ בעיקר, מקפידים המחזיקים בעמדה זו על עקרונות יסוד של שיטת הממשל, כמו למשל ריבונות המדינה. העובדה שהרשת מאפשרת פעילות חוצת-גבולות אינה טעם, לשיטתם, לוותר על ריבונות המדינה.¹⁰

נדמה לי שהיחס בין המשפט לבין הטכנולוגיה מורכב יותר משתי אפשרויות הקיצון האלה, וכדי להבין את היחס המורכב הזה עלינו לפענח מעט יותר את "המשפט", ומעט יותר את "הטכנולוגיה". למשל, עלינו לשאול שאלות, כמו כיצד נוצרת טכנולוגיה? אני סבור שיש, כעניין מצוי, רב-שיח בין המשפט לבין הטכנולוגיה, כלומר בין המחוקקים, בתי המשפט ושאר יוצרי-משפט מצד אחד, לבין יוצרי הטכנולוגיה מצד שני, הפועלים במסגרת תאגידית או במסגרת עצמאית/פרטית, ולבין משתמשי הטכנולוגיה, מצד שלישי. השיח שבין המשפט לטכנולוגיה מורכב. לעיתים חוברים שני הכוחות לסייע זה לזה בהשגת יעד חברתי מסוים.¹¹ לעיתים הם רודפים זה אחר זה ומציעים חלופות המתנגשות זו בזו.¹² בדרך זו הם משפיעים זה על זה, ויש ביניהם יחס דיאלקטי.

9 לא מקרה הוא ששופטים מחזיקים בעמדה זו. ראו, למשל, את דברי השופט בעז אוקון בה"פ (י-ם) Ahava Inc USA 003137/04 **דבלין בע"מ** (10.10.04): "האינטרנט יכול להציב אתגרים לא פשוטים בכל הנוגע להפעלת הסמכות המקומית, העניינית והבינלאומית. ואולם, האינטרנט אינו הופך את המשפט לזר, כאילו אירע שבר או כאילו חדלו חוקי הכובד של המשפט לחול על כלי זה, באופן שהוא גורר אותנו למצב דמדומים של קיום מעשה או מחלל שאין עליהם תגובה משפטית מתאימה. השימוש באינטרנט טומן בחובו יתרונות גדולים, וכולל אפשרויות הנראות 'נארניות'. אך הוא אינו יכול לשבור את 'המצור' הרגיל של הדין. המתכון הנכון מצוי בהגיגה של הכללים הרגילים של הדין."

10 ראו: Joel R. Reidenberg "States and Internet Enforcement" 1 U. **Ottawa Tech. L.J.** (2003-2004) 213.

11 למשל, תוכנות המקדמות הגנה על הפרטיות (הנקראות PETs – Privacy Enhancing Technologies); מנעולים דיגיטליים המאפשרים לבעלי זכויות יוצרים לשלוט ביצירותיהם (DRM – Digital Rights Management), או תוכנות סינון, האמורות לחסום גישה של ילדים לאתרים פורנוגרפיים.

12 ראו, למשל, את המאבק בקשר לשיתוף מוסיקה ברשת: תחילה באה תוכנת נאפסטר, שנסגרה בעקבות תביעות משפטיות. **A&M Records Inc. v. Napster, Inc.** 239 F.3d 1004 (9th Cir. 2001). התוכנה הייתה מבוססת על מנגנון מרכזי של מאגר מידע דינמי שקישר בין המשתמשים. לאחר הפסיקה פותחו תוכנות שיתוף קבצים נטולות-מרכז, דוגמת eMule. תחילה הכשירו בתי

3. דיני מידע

כדי להכריע בתחרות שבין המשפט לטכנולוגיה, יש לתת את הדעת לגורם שלישי, והוא הערכים החברתיים והאתיים.¹³ הוספת הערכים לדיון הופכת את הציור "משפט-טכנולוגיה" למשולש: "ערכים-משפט-טכנולוגיה". אקרא לכך **המודל המשולש של דיני המידע**. הערכים עצמם אינם מקובעים. בחברה הדמוקרטית קיימים ערכים רבים המתגושים ביניהם. ערכים חדשים דוחקים ישנים. לעיתים חברה מאמצת ומעדיפה ערך אחד על פני אחר, ולעיתים חוזרת ומעדיפה את האחר על פני האחד. מובן גם שהערכים שונים ממקום למקום. במדינה אחת מקדשים את חופש הביטוי גם במחיר פגיעה ברגשות, למשל – כאשר נאמרים דברי שטנה נגד קבוצת מיעוט, ובמדינה אחרת מסרבים להגן על ביטויי שנאה שכאלה.

משפט וערכים

קודקודי המשולש וצלעותיו מוכרים וזכו לדיון נרחב. הצלע שבין משפט לערכים היא שאלת יסוד של תורת המשפט: האם המשפט כולל כללים פוזיטיביים בלבד או שהוא מקיף גם עקרונות וערכים? כיצד מגלמים הכללים הפוזיטיביים ערכים, וכיצד יש לפרשם כך ששיגו את תכליתם? בשיטת המשפט הישראלית העכשווית, הערכים הם שמכתיבים את פרשנות כללי המשפט.

טכנולוגיה וערכים

בצלע השנייה, זו שבין ערכים לטכנולוגיה, עוסקים בעיקר חוקרי המדיה, פילוסופים והיסטוריונים של הטכנולוגיה: האם וכיצד מעצב המדיום את המסר? איך משפיעה הטכנולוגיה על פרקטיקות אישיות, חברתיות, פוליטיות? עמדה אחת רואה בטכנולוגיה יישות עצמאית ונייטרלית, שאינה תלויה בדבר. לעמדה זו שני פנים: פן אחד הוא

המשפט את התוכנה, אולם בית המשפט העליון סייג. ראו **MGM v. Grokster, Ltd.** 125 S.Ct. (2005) 2764.

13 לסיג מציג מודל שונה, ומציב במרכזו את הפעילות אותה אנו מבקשים להסדיר. ראו לסיג, **לעיל** הערה 5. לשיטתו, הפעילות מוסדרת על-ידי ארבעה גורמים: משפט, קוד (טכנולוגיה), ערכים חברתיים והשוק. בטקסט אני מתייחס לשוק ולערכים החברתיים בצוותא, שכן ככל שאנו מייחסים חשיבות לשוק החופשי, הרי זהו ערך חברתי. נוסף לכך, המודל של לסיג מתעלם מהקשרים שבין הגורמים השונים המסדירים את הפעילות שבה מדובר. המודל המוצג בטקסט כאן מדגיש את היחסים שבין גורמי ההסדרה.

הטענה בדבר דטרמיניזם טכנולוגי, שהזכרתי קודם. הפן השני הוא, שהטכנולוגיה היא נטולת ערכים, אפשר לבחון את יעילותה, אבל היא מנותקת מנורמות מוסריות והתנהגותיות.¹⁴

בעיניי, עמדה זו, על שני פניה, שגויה. הטכנולוגיה אינה נוצרת יש מאין. היא נוצרת על ידי בני אדם, הפועלים במסגרות חברתיות, מסחריות ואקדמיות. גם אם הם פועלים באופן עצמאי הרי הם אזרחי מדינה כלשהי וכפופים לחוקיה. די בכך כדי לדחות את הטענות כי "לטכנולוגיה חוקים משלה". אין לה חוקים עצמאיים. היא חלק מהפרקטיקה האנושית, ולכן נמצאת בתוך המסגרת החברתית, ובכלל זה – כפופה למשפט.

נוסף לכך, כל טכנולוגיה באשר היא מגלמת ערכים מסוימים בדרכים מגוונות ומורכבות. בחיי היום-יום, אנו רגילים להשתמש בטכנולוגיות רבות מבלי לתהות יותר מדי אחר תכליתן, מהותן או משמעויותיהן. אנו פשוט משתמשים בהן. אבל פילוסופים והיסטוריונים של טכנולוגיה, כמו גם חוקרי תקשורת, טוענים מזה זמן כי למרות החזות הנייטרלית-פונקציונלית, יש גם יש ערכים בטכנולוגיה.¹⁵ סכין, למשל, יכולה לגלם אלימות, או דווקא ערך של הגנה עצמית, או של יעילות, אם נעשה בה שימוש לעיבוד מזון. Langdon Winner מביא דוגמה של גשרים שנבנו בדרך לאזורי נופש בניו יורק בגובה נמוך, באופן כזה שאוטובוסים אינם יכולים לעבור מתחתם. התוצאה היא הדרתם של משתמשי התחבורה הציבורית מאזורי הנופש, ובדרך כלל היו אלה תושבים שחורים.¹⁶ אמרו מעתה, הטכנולוגיה של הגשרים בניו יורק גילמה ערך של הדרה, אפליה וגזענות. בהקשר של הדיון פה, רשת האינטרנט גם היא מגלמת ערכים. בשיח הפופולרי שומעים לא אחת דוברים המציינים את "טבעה של רשת האינטרנט", בדרך כלל כרשת המעלה על נס את חופש הביטוי והדמוקרטיה. באותה מידה, שומעים בעלי אינטרסים שונים המדברים על אותה רשת כעל שטח הפקר, למשל בהקשר של זכויות יוצרים. הרשת יכולה, אם כן, להיות **רשת של חופש או רשת של אנרכיה**. לפיכך, ראוי לשאול, האם בכלל יש לרשת מהות, או אולי משמעותה נקבעת לפי השימוש שאנו עושים בה? במילים אחרות, גם כאשר אנו מקבלים את הטענה, שהטכנולוגיה מגלמת ערכים, יש לפצח כיצד בדיוק.

14 שני הפנים האלה אינם בהכרח מופיעים יחדיו. מי שמחזיק בעמדה הדטרמיניסטית עדיין עשוי לסבור שהטכנולוגיה היא מטבעה "טובה" או מטבעה "רעה" מן הבחינה הערכית.

15 ראו, למשל, Langdon Winner "Do Artifacts Have Politics?" in **The Whale and the Reactor – A Search for Limits in an Age of High Technology** (Chicago, 1986) 19; **Human Values and the Design of Computer Technology** (Batya Friedman, ed., 1997). ראו גם, יובל דרור, **הפוליטיקה של הטכנולוגיה** 2006.

16 Winner, **שם**, בע' 22 ואילך.

הצורה שבה הטכנולוגיה מגלמת ערכים מורכבת מאוד ותלויה בשאלות סבוכות של פרשנות, בעיקר שאלות בדבר הדרך בה נוצרת משמעות. האם משמעות הטכנולוגיה, כלומר הדרך שבה היא מגלמת ערכים, תלויה בכוונת יוצרי הטכנולוגיה? האם היא טבועה בטכנולוגיה בלי קשר לכוונת יוצריה? אולי משמעות הטכנולוגיה תלויה במשתמשים בה? ואולי המשמעות תלויה בהקשר החברתי, התרבותי, הכלכלי והפוליטי? שאלות אלה של פרשנות מוכרות לפרשני אמנות וספרות, כמו גם לפרשני המשפט, המתחבטים בשאלה אם המשמעות של יצירה או של חוק צריכה להיקבע לפי כוונת היוצר/המחוקק, לפי הטקסט בלבד או לפי הבנת הפרשן. נראה לי, שהתשובה (בספרות, באמנות, במשפט ובטכנולוגיה) אינה באף לא אחד מהגורמים האלה לבדם, אלא דווקא בקשר שביניהם. הטכנולוגיה נטענת במשמעות במרחב שבין מפתחיה של הטכנולוגיה לבין הטכנולוגיה עצמה, בין טכנולוגיה מסוימת לטכנולוגיות אחרות, ובינה לבין משתמשיה, והכול – בהקשר החברתי הנתון. זהו מרחב של דיאלוג על-זמני, אינטראקטיבי ודינמי.

לפי הדיווח הרווח, הארכיטקטורה הבסיסית של רשת האינטרנט נוצרה מתוך כוונה של צבא ארצות הברית להתגונן מפני מתקפה גרעינית גם אם יימחו אזורים נרחבים מעל לפני האדמה, יישמר המידע ברשת במקומות אחרים. הביזור המכוון הזה איפשר, שלא במכוון, את החופש הגדול שיש ברשת האינטרנט למשתמשיה. במילים אחרות, הטכנולוגיה פותחה כך שתשיג ערך של הגנה וביטחון, אבל בפועל היא מגלמת ערך אחר, של חופש. לטכנולוגיה עצמה יש מאפיינים שמדגישים ערכים מסוימים על פני אחרים. היעדר מרכז שליטה ברשת, ומתכונתה כרשת של "קצה לקצה" (end to end), מקנה מיידית כוח ל"קצוות". במדינה הפיסית יכול השלטון להזרים טנקים לכיכר העיר ולבלום מחאה נגד השלטון. בהיעדר כיכר מרכזית אחת, אי אפשר לשלוט ברשת בדרך הישנה הזו. אבל, העיקר אינו מה התכוונו המפתחים, או מה יש בטכנולוגיה, אלא העיקר הוא מה עושים המשתמשים. משמעותה של רשת האינטרנט נוצרת על ידי השימוש בפועל, כאשר השימוש מוכתב ונתחם על ידי הטכנולוגיה עצמה, דבר שהושפע בעתו מהמפתחים. הגולשים יכולים להשתמש באינטרנט "שימושים של חופש", כמו למשל להגביר את אפשרויות הביטוי, את ההשתתפות בשיח הציבורי, או "שימושים של אנרכיה", כמו למשל להפר זכויות יוצרים או לפגוע בפרטיות.

ועוד דוגמה: איש המחשבים לו מונטולי פיתח טכנולוגיה שתזכור את כל הסיסמאות הרבות שנדרש למסור באתרים השונים, וכך יילד את "העוגיה" – אמצעי המקל מאוד על הגלישה, אבל גם אמצעי למעקב ולפגיעה בפרטיות. הטכנולוגיה של "העוגיה" מגלמת תפישה "רזה" מאוד של פרטיות. משמעותה הערכית, החברתית והאתית של "העוגיה" נקבעת, אם כן, ביחס שבין כוונת המפתח לבין מאפייני הטכנולוגיה עצמה, ובשימושים שנעשים בה. בדרך מורכבת זו נוצרת המשמעות של הטכנולוגיה. המשמעות עשויה לפיכך להשתנות לפי השימושים בה. טכנולוגיה יכולה לשמש תחילה כאמצעי למטרה חיובית ולהפוך במרוצת הזמן לסימן שלילי.

4. עיצוב מדיניות טכנולוגית

אם המשפט מגלם ערכים, ואם גם הטכנולוגיה מגלמת ערכים, אפשר היה להסיק שעיצוב המדיניות לסביבה הטכנולוגית מוגבל רק לדיון בערכים עצמם, ובמונחי המשולש של דיני המידע שהוצג לעיל – רק לקודקוד של הערכים. האם בעת עיצוב מדיניות אפשר להתעלם מהטכנולוגיה שבה מדובר? אני סבור שהתשובה שלילית. לטכנולוגיה יש תפקיד מכשירני בעיצוב מדיניות. היא מהווה עילה טובה לבחון מחדש את ערכינו, היא מאתגרת אותנו ויוצרת מצבים חדשים שעלינו להתמודד עימם. מה תוכנם של הערכים ומה משמעותם? אולי יש מקום לשנות את סדרי העדיפות שלנו בקשר לערכים? לטכנולוגיה יש גם תפקיד מעשי. היא מהווה את המנוע של הפעילות האנושית שאותה אנו מבקשים להסדיר. זו נקודה בסיסית: המשפט מסדיר התנהגות אנושית, ולא טכנולוגיה כשלעצמה. גם אם נדמה לנו שיש הסדרה של הטכנולוגיה, הרי המטרה היא – או ראוי שתהיה – להשפיע על ההתנהגות של המשתמשים בה.

מהדיון עד כה עולה הנחיה כללית לעיצוב מדיניות בסביבה הדיגיטלית, ולפיה כללי המשפט הקיים הם תחילתו של דיון, שצריך להפנות אותו לערכים, שמהם נגזרים כללי המשפט, ולהזכיר לנו שגם הערכים ניצבים ביניהם ואינם מוחלטים. בין אלה יש למנות גם ערכים כמוכבן המוסרי וגם כמוכבן החברתי, ובכלל זה ערכים של שוק חופשי, במידה שבה אנו מחזיקים בהם. זו תפישה שמזכירה לנו שהטכנולוגיה אינה חסינה מפני הסדרה, אבל בד בבד, אין להתעלם ממנה. בעיצוב כללים משפטיים חדשים או בעת פרשנות כללים קיימים, יש להיות ערים לטכנולוגיה, ללמוד את מאפייניה הרלוונטיים ולחליץ את הערכים המגולמים בה. הטעם לכך הוא שהטכנולוגיה מאתגרת את הערכים. היא יוצרת מצבים חדשים, אשר אין לנו תשובה מן המוכן לגביהם. היא חושפת את קוצר ידם של ערכים מסוימים ואת עוצמתם של ערכים אחרים. נוסף לכך, רב השיח שבין הערכים, המשפט והטכנולוגיה נדרש כדי שהכלל המשפטי הנגזר מהערכים יהיה אפקטיבי. אין טעם או היגיון בכלל משפטי שאינו ישים לרשת, או שניתן לסכלו בקלות באמצעות טכנולוגיה מתאימה.

הלקח שנלמד מהדיון במודל המשולש של דיני המידע הוא שכדי לעצב משפט חדש, או לענייננו ברשימה זו, כדי לפרש את חוק המחשבים, על המשפט לנהל דו-שיח עם הטכנולוגיה. יוצרי המשפט חייבים ללמוד את הטכנולוגיה שאותה הם מבקשים להסדיר, אבל לא רק. אין די בלימוד הטכנולוגיה המונחת על השולחן, אלא צריך להבין תהליכים מורכבים יותר: כיצד נוצרת טכנולוגיה, כיצד היא מתקדמת, כיצד היא מושפעת או עלולה להיות מושפעת מכלל משפטי חדש. על המשפט להתערב רק כאשר הערכים המנחים אותו מגובשים וחזקים, רק כאשר הדבר אפשרי ורק כאשר תוצאות ההתערבות אינן מזיקות יותר משהן מועילות. גם תהליך זה הוא דינמי, ולמעשה, אינסופי. נוסף לכך, השיח הנדרש שבין המשפט לטכנולוגיה חייב להימשך כל העת. הטכנולוגיה משתנה, משמעותה משתנה, ולכן תוכן השיח משתנה, ובהתאם, נדרש שינוי בתוצאות השיח. ולענייננו, כדי לפרש את חוק המחשבים בצורה האופטימלית,

עלינו לערוך בירור ערכי, מהו הערך המוגן על-ידי החוק? זו פרשנות תכליתית, כמקובל במשפט הישראלי. אלא שיש ללמוד את הטכנולוגיה. לראות מה מאפייניה. לחשוב אלו מהם אנו מעוניינים להעצים ואלו אנו מעוניינים לצמצם. לאחר שנסיק מסקנות ערכיות מברור כזה ונלמד את הטכנולוגיה בה מדובר, אין לחשוש מהטלת הערכים על הטכנולוגיה, במגבלת תכונותיה.

הדיון שלהלן בחוק המחשבים נועד להמחיש כיצד מיושמת המסגרת הכללית של דיני המידע, כיצד הכלל המשפטי נגזר מתוך האינטראקציה המורכבת שבין המשפט לבין הטכנולוגיה, שמנהלים ביניהם שיח נמשך שיש בו היוון הדדי.

ג. על חוק המחשבים

חוק המחשבים כולל מספר עבירות פליליות שמקצתן מוגדרות גם כעוולות אזרחיות. החוק אוסר פעולות מסוימות הנתפשות כשליליות ומזיקות, הקשורות למחשב.¹⁷ כדי למקד את הדיון, אצביע על כמה הבחנות מוכרות.¹⁸ הבחנה ראשונה היא בין עבירות **באמצעות מחשב** לעבירות **נגד מחשב**, שהן פעולות שמטרתן היא הפגיעה במחשב עצמו או במערכות המחשב.¹⁹ כך, למשל, עבריינים הקושרים ביניהם קשר לבצע עבירה באמצעות חילופי דואר אלקטרוני משתמשים אמנם במחשב, אולם השימוש במחשב הוא אגבי ומקרי: באותה מידה היו יכולים להשתמש בטלפון, בשיחה פנים אל פנים וכדומה. העיקר כאן הוא קשירת הקשר. החוק קובע עבירה נפרדת, שעונשה חמור יותר, למי שמבצע חדירה לחומר מחשב כדי לעבור עבירה אחרת (סעיף 5). בכמה מקרים ציינו בתי המשפט את השימוש במחשב או ברשת האינטרנט כנסיבה מחמירה, למשל

17 חוקים דומים ניתן למצוא היום במדינות רבות. לדיון ראו Marc A. Goodman & Susan W. Brenner "The Emerging Consensus on Criminal Conduct in Cyberspace" 2002 *UCLA J.L. & Tech.* 3; Neal Kumar. Katyal "Criminal Law in Cyberspace" 149 *Pa. L. Rev.* (2001) 1003.

18 לניסיון לזהות את הייחוד שבפשעית מחשב, ראו Susan W. Brenner "Is There Such A Thing as Virtual Crime?" 4 *Cal. Crim. L. Rev.* (2001) 12.

19 ראו, גם, מיגל דויטש "חקיקת מחשבים בישראל" **עיוני משפט** כב (תשנ"ט) 427, 435. החוק הישראלי הוא תוצאה של מספר הצעות וועדות לאורך השנים. ראו Yoram Bar-Sela "Computer Legislation in Israel: A Proposal Being Developed by the Ministry of Justice" 21 *Isr. L. Rev.* (1986) 59. וראו עוד את הפרוטוקולים של דיוני ועדת המשנה של הכנסת להצעת חוק המחשבים, של ועדת החוקה, חוק ומשפט (להלן ועדת המשנה של הכנסת), ישיבות מיום 24.1.95, 14.2.95, 14.3.95, שייקראו בהמשך הפרוטוקול הראשון ואילך, בהתאמה. תודתי לעו"ד נעמי אסיא ולד"ר ויקטור בוגנים שהעמידו את הפרוטוקולים לעיון.

בהקשר של תרמית בניירות ערך שבוצעה באמצעות פרסום הודעות כוזבות באתר אינטרנט.²⁰

הבחנה שנייה, היא, שגם כאשר המחשב הוא היעד לפעולה האסורה, יש להבחין בין פעולות שנועדו לגרום נזק למחשב עצמו לבין פעולות שנועדו לגרום נזק מחוץ למחשב עצמו. למשל, טרוריסט המחבל במערכת מחשב של תשתיות לאומיות קריטיות, כמו מחשבי חברת החשמל, חברות הטלפון, מערכת בקרת רמזורים או בקרה אווירית. שיבוש פעולת המחשב במקרה כזה נועד לפגוע בתשתיות הקריטיות. השימוש במחשב אינו כאמצעי תקשורת לעבור עבירה אחרת, כמו בדוגמת הקשר הפלילי, אלא מטרתו היא לגרום לנזק ממשי בעולם המוחשי. במקרים כאלה, המקום המשפטי המתאים לבחון את הפעולה החשודה הוא דיני העונשין הכלליים, האוסרים רצח, חבלה וכיוצא בזה, וברור כי מבחינת חומרת המעשים, העבירה שלפי סעיף 5 לחוק, של עבירה באמצעות מחשב, מתגמדת לנוכח העבירה האחרת. כמו כן, אם נגרם נזק למחשב עצמו – הרי ניתן להעמיד לדין גם בגין עבירה לפי חוק המחשבים, אולם, שוב, ברור כי היא טפלה ביחס לעבירה העיקרית.

בהקשר זה, מטריד הזיהוי התכוף שיוצרים מחוקקים בעולם בין עבירות מחשב לעבירות טרור.²¹ הנזקים שגורמים הטרוריסט ועברייני המחשב שונים בדרך כלל וגם כוונתם והמניע שלהם שונה. הקושי הוא שלמפעיל המערכת הנפרצת אין בדרך כלל יכולת להבחין ביניהם.²² החשש בטישטוש הגבול שבין הטרוריסט לעברייני המחשב טמון בהחמרה הניכרת שאינה במקומה ביחס לפעולותיו של עברייני המחשב. לפחות

20 ראו ע"פ (ת"א) 070571/01 מדינת ישראל נ' טל פודים (23.3.02). בית המשפט המחוזי שם הדגיש כי עובדת השימוש באינטרנט אינה משנה את אופייה של העבירה, שכן רשת האינטרנט שימשה רק כאמצעי "הטכני המשוכלל" לביצוע העבירות, ויותר מכך, עובדה זו פועלת לחובת הנאשם. בקשת רשות ערעור לבית המשפט העליון נדחתה – רע"פ 5729/02 פודים נ' מדינת ישראל, תק-על 2002 (2) 1049.

21 דוגמה מובהקת להאחדת עבירות מחשב ופשעי טרור היא ה-Convention on Cybercrime, 2001 של מועצת אירופה. ראו <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. האמנה נדונה במשך כעשור, אולם הושלמה בורחות בחודש נובמבר 2001, בעקבות אירועי האחד-עשר בספטמבר. לביקורת על הטישטוש בין פשיעת מחשב לטרור, ראו Ariel T. Sobelman "Is Everyone an Enemy in Cyberspace?" 2(4) Strategic Assessment (2000), נמצא ב: <http://www.tau.ac.il/jcss/sa/v2n4p4.html>. לדיון בשינוי פניה של הסביבה הדיגיטלית לסביבה ביטחונית בעקבות אירועי 9/11 ראו אודי אינהורן ואח' לוחמה בטרור בזירת המידע (חיפה, המרכז למשפט וטכנולוגיה, ניבה אלקין-קורן ומיכאל בירנהק עורכים, 2002) במיוחד ע' 6-1.

22 אמנם יש אמצעים טכנולוגיים מתוחכמים המאפשרים להבחין בין השניים, למשל לפי ניתוח ההתנהגות, מועד ההפעלה, יעד התקיפה (מבחינת המרכיב בתוכנת המחשב המותקף) וכדומה. אולם, לפי שעה הם יקרים, אינם מושלמים ואינם בשימוש רחב. ראו Nimrod Kozlovski *A Paradigm Shift in Online Policing – Designing Accountable Policing* (SJD Dissertation, submitted to Yale Law School, June 2005).

חלק מאלה המהלכים על גבולו של חוק המחשבים אינם עבריינים, אלא חוקרי מחשבים, המבקשים ללמוד, לדעת, להבין. הדימוי הרומנטי של עברייני המחשב נכון לא אחת, ופעמים רבות מדובר בנערים סקרנים, אשר בהתבגרם הופכים להיות מובילים במחקר מחשבים או מומחים לאבטחת מידע. המחיר החברתי שאנו משלמים, כתוצאה מהאחדת היחס לטרוריסט והיחס לעבריין המחשב, הוא הרתעת יתר של חוקרי מחשב (נערים סקרנים או מיזמי אינטרנט) מפני ניסיון, לימוד ומחקר של מערכות מחשבים, הצפנה ומערכות אבטחה. אמנם, אפשר להבריל בין הטרוריסט לחוקר המחשבים באמצעות ענישה, אולם מאחר שבדרך כלל רק החוקר יתפס, ומאחר שהכוח המרתיע של האיסור משפיע עליו יותר מאשר על הטרוריסט, יש חשש להרתעת יתר כאמור. נוסף על כך, וכפי שאסביר בהמשך, פעולתו של החוקר הסקרן חיובית ורצויה מבחינת חברתית, שכן זהו אמצעי לימוד מרכזי ואמצעי בקרה ביטחונית יעיל מבחינה חברתית. המחיר של כלל מחמיר במיוחד הוא גם שאננות של מפעילי אתרים, העלולים לסמוך על החוק לבדו.²³

המוקד במאמר זה הוא, אם כן, בעבירות שיעדן הסופי הוא המחשב: נבחן את פעולתו של עבריין המחשבים המבקש להזיק למערכת המחשב עצמה. העבירות המרכזיות שבחוק המחשבים הן שיבוש או הפרעה למחשב (סעיף 2), העברת מידע כוזב או אחסונו (סעיף 3), חדירה לחומר מחשב (סעיף 4) ועריכת נגיף מחשב (וירוס) או הפצתו (סעיף 6). מבין אלה, ראויה לעיון מיוחד העבירה של חדירה לחומר מחשב. אמנם, כדי להרשיע בעבירה זו אין צורך להוכיח נזק, כלומר נזק אינו יסוד מיסודות העבירה, אולם חשוב לזהות את הערך המוגן על ידי העבירה, וזה אינו פשוט כלל וכלל לזיהוי: לא במקרה התעוררה מחלוקת בין פסקי הדין שיידונו בהמשך בקשר לעבירה זו דווקא, ולא במקרה יש הנחות רקע מנוגדות של השופטים בקשר לעבירה.

23 נקודה זו מעוררת שאלות בדבר השפעת כלל משפטי על התנהגות אנושית: במקרים רבים ניתן להשיג את התוצאה שהחוק מבקש להשיג, למשל הגנה על קניין, בדרך של נקיטת אמצעי הגנה עצמיים, כמו התקנת גדרות, הצבת שומרים וכדומה. הכלל המשפטי המגן על הקניין אמור לייתר את הצורך באמצעים עצמיים, ובכך להוויל עליות הגנה. אולם למרות שיש כלל קנייני, אנו נוקטים אמצעי אבטחה רבים. מדוע? גם לאכיפת החוק הקיים יש עלויות (שיטור, פנייה לגורמי אכיפת חוק, עורכי דין, סיכון להפסד בתביעה). לאזרח כדאי לנקוט אמצעי הגנה עצמיים רק כל עוד עלותם קטנה מעלות אכיפת החוק. בטקסט אני מתאר מצב שבו החוק מחמיר מאוד. במקרה כזה, עלות הפעלת החוק מבחינת האזרח נשארת אולי דומה (עדיין יש לפנות למשטרה, לעורכי דין ולבתי משפט), אולם, אם וככל שחוק מחמיר יותר כלפי העבריינים-לעתיד ומרתיע אותם יותר, הרי תוחלת הזכייה של האזרח המפעיל את החוק גבוהה יותר. במקרה כזה, רבים מאיתנו עלולים לסמוך על החוק ולהימנע מנקיטת אמצעי אבטחה פשוטים וזולים.

עוד הערה לסדר, איני מציע כאן ניתוח מלא של העבירה הפלילית. איני דן כאן במחשבה הפלילית הנדרשת להרשעה, או בשאלה של מרכיבי העבירות הנדרשים.²⁴ המטרה כללית יותר, לזהות ברמת חידוד גבוהה יותר, מזו הקיימת בהיסטוריה החקיקתית או בפסיקה, את הערך החברתי המוגן על ידי העבירות שבחוק המחשבים. הטענה המרכזית היא שראוי לזהות את הערך החברתי המוגן בחוק המחשבים עם עקרונות האבטחה המקובלים בעולם המחשבים ומערכות המידע. עמדה כזו תוכל לדייק יותר בשרטוט הקו שבין פעולות רצויות, אשר יש לעודדן, לבין פעולות שאינן רצויות, אשר יש להרתיע מפני ביצוען או להעניש בגינן. עמדה כזו תואמת גם את המודל של דיני מידע שהצגתי לעיל, בדבר עיצוב כללים משפטיים תוך כדי דיאלוג של המשפט עם הטכנולוגיה.

נראה, כי נסחי החוק פעלו מתוך מודעות לטכנולוגיה ולדו-שיח עימה.²⁵ ההיסטוריה החקיקתית, במבט של עשור לאחור, נראית אנכרוניסטית ואפילו משעשעת, אולם יש להעריך את קפיצת המדרגה שנעשתה בשעתה. נסחי החוק נדרשו להבהיר שהחוק מיועד להגן על הפעילות במחשב, ולא על המחשב הפיסי. לפיכך, תפישות קנייניות והגנות משפטיות מפני גזל, למשל, שהיו בדין הקיים לא היו רלוונטיות. כיום הבחנה זו, בין הגנה על המחשב להגנה על השימוש בו, נראית מובנת מאליה: זה ההבדל שבין אטומים לסיביות (ביטים).²⁶ חוק המחשבים מגן רק על הסיביות.²⁷

כיצד יש להבין את החוק לפי המודל של דיני המידע? או במילים אחרות, מהי תפישת החוק, כפי שהיא מגולמת בהוראותיו וכפי שפורשה על ידי בתי המשפט, באשר ליחס שבין משפט לטכנולוגיה? מקריאת החוק ומשמו ברור כי המחוקק היה מודע לכך שהוא מנסה להתערב ולהסדיר את השימוש בטכנולוגיה. החוק ודאי אינו מגלם עמדה של דטרמיניזם טכנולוגי. דברי ההסבר לחוק מונים מספר טעמים בקשר לצורך בחקיקת החוק, והראשון שבהם הוא "המקום המרכזי שהמחשב תופס בכל שטחי הפעילות של החברה המודרנית מחייב חקיקה כדי להגן כראוי על האינטרסים המגוונים המקודמים

24 לדיון בשאלות אלה, ראו יהונתן בר-שדה **האינטרנט והמשפט המסחרי המקוון** (תל אביב, תשס"ב-2002) 687-690.

25 הדיונים במליאת הכנסת אינם מלמדים רבות. ראו ד"כ התשנ"ד 9989 ואילך (קריאה ראשונה) וד"כ התשנ"ה 10817 ואילך (קריאה שנייה וקריאה שלישית). בדיוני ועדת המשנה של הכנסת התעוררה מדי פעם השאלה בדבר הערך המוגן על ידי החוק, וניתנו לה תשובות כלליות, שתכלית החוק היא "הגנה על הערך התיפקודי של המחשב" (פרוטוקול 1, ע' 3); האינטרס המוגן הוא השימוש הבלתי-מופרע במחשב ושלמות החומר (פרוטוקול 2, ע' 8); הגנה על המחשב (פרוטוקול 2, ע' 9, 19); והגנה על "פרטיות" של חומר מחשב (פרוטוקול 2, ע' 27).

26 להבחנה זו ראו ניקולאס נגרופונטי **להיות דיגיטלי** (תרגום עמנואל לוטם, 1995).

27 האינטרנט נזכר רק פעם אחת בוועדת המשנה של הכנסת, ובדרך אגב. במליאת הכנסת לא נזכר האינטרנט כלל.

על-ידי המחשב".²⁸ כלומר, המחשבים, וברמת הפשטה גבוהה יותר – הטכנולוגיה, נחשבים כאמצעי חיובי להשגת מטרת אחרות, רצויות כשלעצמן. התפקיד של הטכנולוגיה מוצג כאן כמכשירני. המחשב אינו יעד כשלעצמו. החוק, בתורו, כך עולה הן מההיסטוריה החקיקתית והן מלשונו, נועד לסייע לטכנולוגיה. אין מדובר כאן בחוק הנאבק בטכנולוגיה הנתפשת בעיני המדינה כשלילית,²⁹ מסוכנת,³⁰ או כמזיקה לאינטרס ציבורי חשוב אחר.³¹ להיפך, החוק נועד לתמוך ולחזק. מיד בהמשך, מזכירים דברי ההסבר את עבריינות המחשבים, תוך הערה כי קשה להתאים את הדין הקיים לעבירות החדשות,³² ובהמשך דברי ההסבר, מודגש הצורך להגן מפני שימוש לרעה במחשב.³³ מכל האמור עולה, כי תכלית החוק נוסחה באופן רחב יחסית, כהגנה על השימוש במחשבים. בחלוף עשור משפטי, ושנות דור טכנולוגיות, אפשר לנסח את תכלית החוק בדרך ממוקדת יותר: החוק נועד להגן על עקרונות אבטחת המידע.

ד. אבטחת מידע

את העבירות הקבועות בחוק המחשבים יש לפרש בתוך מסגרת כללית של דיני מידע, כלומר מתוך הבנה של היחס הדיאלקטי שבין משפט לטכנולוגיה. את הכלל המשפטי יש לעצב תוך לימוד הטכנולוגיה, יתרונותיה וחסרונותיה, תוך חילוץ הערכים, שעליהם אנו מבקשים להגן, ובחינה חוזרת אם ואיך ניתן לממשם. לפיכך, יש לפרש את העבירות

- 28 הצעת חוק המחשבים, התשנ"ד-1994, ה"ח התשנ"ד, ע' 478.
- 29 כמו למשל האיטורים בדין האמריקני על פיתוח, שימוש והפצה של טכנולוגיה שנועדה לעקוף מנגנוני גישה טכנולוגיים המגינים על יצירות המוגנות בזכויות יוצרים. ראו 17 U.S.C. §§ 1201-1205.
- 30 טכנולוגיה של הצפנה נתפשת בעיני המדינה כמסוכנת, אם תגיע לידיהם של טרוריסטים או פושעים, שאז יהיה קושי לעקוב אחריהם. הדיון סביב הסדרתה של הצפנה עורר ויכוחים עזים. לדיון בהקשר האמריקני ראו – Stephen Levy *Crypto: How the Code Rebels Beat the Government* (New York, 2001) *Saving Privacy in the Digital Age* (New York, 2001). בישראל: אינהורן, **לעיל** הערה 21, בע' 7 ואילך.
- 31 למשל טכנולוגיות מעקב מסוימות הנתפשות כפוגעות בפרטיות, לפחות במדינות האיחוד האירופי. ראו Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
- 32 לקושי זה ראו, גם, אליעזר לדרמן "פעילות פסולה המסתיעת במחשבים ודיני העונשים בישראל" **עיוני משפט יג** (תשמ"ח-תשמ"ט) 499. נושא זה הובהר גם בדיוני ועדת המשנה של הכנסת.
- 33 הדברים חזרו גם בהצגתו של שר המשפטים דאז, דוד ליבאי, את הצעת החוק בכנסת. ראו ד"כ התשנ"ד 9989 ואילך.

שבחוק המחשבים על רקע עקרונות אבטחת מידע. הנורמה החברתית המוגנת שאותה מבקש החוק לקדם, כלומר תכלית החוק, חופפת את עקרונות אבטחת המידע.³⁴ "אבטחת מידע" הוא מושג-סל בתחום מערכות המידע, שנעשה בו שימוש בהקשרים שונים שאינם תמיד אחידים,³⁵ והוא גם משתנה לאורך השנים, ככל שהטכנולוגיה משתכללת והעבריינים מתעדכנים גם הם. מתוך הספרות המקצועית ניתן לחלץ גרעין מרכזי:³⁶

המטרה הכללית של אבטחת המידע ומערכות המידע היא לוודא שהמחשב או מערכת המחשבים יבצעו את הפעולות והמשימות שאותן יועדו לבצע, ללא התערבות או הפרעה חיצונית, וכל זה בסודיות, ככל שהיא נדרשת.

אבטחת מידע אינה עוסקת בכשלים ("באגים") במערכת עצמה, אלא בסיכול שיבושים מכוונים. הסיכונים האלה יכולים לבוא "מבחוץ", כלומר מגורמים שהמערכת לא נועדה לשימושם, או "מבפנים", כלומר מגורמים המורשים להשתמש במערכת ברשות

34 האם בכלל יש מקום להתערב משפטית כדי להגן על המידע? איני כופר בהצדקת קיומו של חוק המחשבים, וחותר לפרשנותו הראויה. ייתכן שבהיעדר חוק היה השוק מגיב, והיו ננקטים אמצעי אבטחה חזקים מאלה הקיימים. לאמצעי אבטחה חזקים מדי יש מחיר כלכלי, טכנולוגי, ומחיר של הכבדת הגלישה ברשת. בספרות יש הצעות מגוונות להסדרה לא-משפטית. למשל, נקיטת אמצעים התקפיים. לדין ראו **Curits E.A. Karnow Launch on Warning: Aggressive Defense of Computer Systems** (Yale Law School, 2004), available at: http://islandia.yale.edu/isp/digital%20cops/papers/karnow_newcops.pdf. מלומד אחד הצביע על אמצעים פשוטים המקובלים להפחתת פשיעה בעולם הפיסי, ובחן את אפשרות יישומם ברשת: ליצור ניראות של הרחוב, תחושת קהילה אצל השכנים וכדומה. ראו Neal Kumar Katyal "Digital Architecture" *as Crime Control* 112 **Yale L. J.** (2003) 2261.

35 הדבר בולט בהתייחסות לאבטחת המידע הכלולה ב"מדיניות הפרטיות" של אתרים רבים. ממחקר אמפירי שבחן אתרים ציבוריים בישראל (אתרי ממשל, רשויות מקומיות, מוסדות אקדמיים וכדומה) התברר שאתרים רבים מתייחסים למדיניות אבטחת המידע שלהם, גם כאשר נראה שהם בכלל אינם כפופים לדרישה כזו. ראו ניבה אלקין-קורן ומיכאל בירנהק "הגנת הפרטיות באתרים ציבוריים באינטרנט" **ביטאון אוניברסיטת חיפה** (אביב 2004) 7. במדיניות אבטחת המידע, במקרים שבהם היא מופיעה, ניתן למצוא בדרך כלל התייחסות לשמירת המידע, המקרים בהם יימסר לצדדים שלישיים, וכן פטור מאחריות למפעילי האתר במקרים של פעולה עוינת.

36 הדיון שלהלן מבוסס על קשת מקורות. ראו במיוחד: Donald L. Brinkley & Roger R. Schell, "Concepts and Terminology for Computer Security", in *Information Security: An Integrated Collection of Essays* 40 (Marshall D. Abrams, Shushil Jajodia, Harold P. Podell, eds., Ca. 1995); Simon Garfinkel, **Web Security, Privacy and Commerce** (2nd ed., O'Reilly, Sebastopol, Ca. 2002).

ובסמכות, אולם לא בדרך בה הם עושים זאת בפועל. זהו אם כן עקרון-העל של אבטחת מידע: **לוודא שהמערכת ממלאת את ייעודה ללא הפרעה**. השיבושים מפניהם מבקשים עקרונות אבטחת המידע להתגונן הם הפרעה לתיפקוד התקין של המערכת ונטילה של מידע הנמצא במערכת. מניעת הפרעה לפעילות משמעה למנוע התערבות זרה, כמו למשל של וירוסים או סוסים טרויאניים, למנוע סילוף של המידע שבמערכת, ושאר אמצעים העלולים לשבש את פעילותה. מניעת נטילת מידע הנמצא במערכת באה להגן על אינטרסים המוגנים בדינים אחרים, כמו דיני זכויות היוצרים המגינים על קוד התוכנה, דיני הגנת הפרטיות המגינים בדרך כלל על תוכן המידע, חובות חיסיון על מחזיקי מידע, והגנה על סודות מסחריים כאשר מדובר על מערכות מחשב של גורמים עסקיים, או סודות מדינה כאשר מדובר במערכות מחשב ממשלתיות. תכליתו של עקרון-העל של אבטחת המידע, ברורה. מערכות מחשב חשופות לסיכונים רבים. תפקידם של המחשבים בחיינו מתחזק כל העת ואנו הופכים להיות תלויים בהם. משום כך חיוני שנבטיח שהמערכות יפעלו כפי שיועדו לפעול, בעוד אנו עמלים לפתח מערכות מתוחכמות יותר שיציעו אותנו ואת האנושות צעד נוסף אחד קדימה.

עקרון-העל של אבטחת מידע נפרט לכמה עקרונות או כללים פרטניים. מובן שהפירוט הטכני הוא תלוי-מחשב ותלוי-מערכת. שלושת עקרונות אבטחת המידע המרכזיים הם: שלמות המידע ומהימנותו (integrity), זמינות המערכת (availability) וסודיות המידע (confidentiality). עקרונות כלליים אלה נפרטים לכללי משנה, ובעיקר – אימות זהות המשתמש (authentication), בקרת גישה חיצונית (access control) ובקרת שימוש פנימית (authorization). אדון בהם בקצרה, ואציג כיצד העבירות שבחוק המחשבים מתאימות לעקרונות אלה וכיצד עקרונות אבטחת המידע הם תכליתו של החוק.³⁷

1. אימות זהות

כלל אבטחת מידע ראשון, שנועד להבטיח את שלמות המידע, את אמינותו וסודיותו, הוא הכלל בדבר אימות זהות: לפיו, יש לוודא שהגורם המבקש להשתמש במערכת אינו גורם עוין ושהוא מורשה להשתמש בה.³⁸ בשיח של אבטחת מידע מקובל לדבר על

37 דברים אלה אמורים במערכת שבה נמצא המידע. אבטחת המידע מתפרשת גם על דרך ההתקשרות. על סודיות התקשורת ניתן להגן באמצעים טכנולוגיים, למשל באמצעות העברת נתונים בפרוטוקול מוצפן. ראו Garfinkel, ibid, at 107. גם המשפט מגן על התקשורת, בחוק האונת סתר, התשל"ט-1979. לצד אלה, מוזכרים בספרות המקצועית גם אבטחה פיסית של המחשבים, יצירת גיבוי ואפשרויות שיחזור של המערכת והמידע שבה. לאלה אין ביטוי בחוק המחשבים, ולא אדון בהם כאן.

38 עיקרון נספח הוא של אי-הכחשה (non repudiation), כלומר, שהאימות אינו רק לזהות, אלא גם לפעולות, בדרך שמקשה או מונעת מהמשתמש להתכחש לפעולתו. מובן שלאימות פעולה יש

שלושה אמצעי אימות, שניתן לצרפם כדי להגביר את רמת האבטחה:³⁹ (א) דבר מה שהאדם יודע (דוגמת סיסמא) (ב) דבר מה שיש לאדם (דוגמת כרטיס אשראי, מחולל סיסמאות) (ג) דבר מה של האדם (דוגמת טביעת עין, טביעת אצבע או טביעת כף יד הנקוטה בנמלי תעופה). הזיהוי יכול להיות גם של **המחשב** שבאמצעותו מבקשים להתקשר עם המערכת או של המערכת האוטומטית המבקשת "לפנות" למחשב המוגן. דוגמה מוכרת היא השימוש בכרטיס אשראי למשיכת כסף מכספומט, המחייב שימוש בסיסמה ושימוש בחפץ פיסי.⁴⁰ גם הפרוטוקולים הטכנולוגיים של תקשורת בין מחשבים מסוגלים לוודא את זהות המתקשרים ולהצפין את שיחתם (פרוטוקול SSL).⁴¹ חוק המחשבים אינו מגן במישרין על עקרון אימות הזהות,⁴² אולם, קיימת בחוק העבירה של "חדירה שלא כדין לחומר מחשב" (סעיף 4). מי שאינו מורשה וזהותו אינה מאומתת, ובכל זאת מצליח להיכנס למערכת, מפר את העיקרון הזה, והמסגרת המשפטית לבחון זאת היא קורת הגג של העבירה שנוכרה ותידון בהמשך. עם זאת, אני סבור שיש להביא את עקרון אימות הזהות בחשבון, במקרים המתאימים, גם בהיעדר הגנה משפטית ישירה על העיקרון. כך, למשל, ראוי היה להביא זאת בחשבון במקרה שבו עובד לשעבר של חברה, שסיפקה שירותי מרכזיה ללקוחות, השתמש באמצעי הגישה שנתרו בידו כדי לחדור למרכזיה ולשבש את פעולתה.⁴³ לבד מפגיעה בעקרונות אבטחת מידע נוספים (עקיפת בקרת גישה ופגיעה בשלמות המערכת – ואכן, הנאשם במקרה זה הורשע בעבירות של שיבוש והפרעה למחשב וחדירה שלא כדין לחומר מחשב) – הייתה שם פגיעה בעקרון אימות הזהות: הנאשם השתמש באמצעי זיהוי שנתרו בידו לאחר סיום עבודתו כדי להשתמש במערכת. אין בחוק איסור ישיר על פעולה זו, אולם אני סבור שזהו שיקול ראוי בהערכת חומרתה של העבירה ובגזירת הדין.

חשיבות משפטית רבה בהקשר של סחר אלקטרוני, למשל הצעה וקיבול חוזיים. לדיון בעיקרון זה, ובפער שבין המושג המשפטי של הכחשת פעולה (למשל, התכחשות לחתימה על חוזה) למושג המקובל אצל אנשי מחשבים, ראו Adrian McCullagh & William Caeli "Non-Repudiation in the Digital Environment" **First Monday** Vol. 5(8) (August 2000), available at: http://firstmonday.org/issues/issue5_8/mccullagh/index.html. אמצעי מרכזי לממש את עקרון אי היכולת להתכחש לפעולה משפטית מושג על ידי חתימה אלקטרונית. ראו חוק חתימה אלקטרונית, התשס"א-2001.

39 ראו, למשל, הגדרת "authentication" ב-<http://en.wikipedia.org/wiki/Authentication>.

40 ראו <http://he.wikipedia.org>, בערך "אבטחת מידע".

41 הכשל המרכזי בקשר לעקרון אימות הזהות הוא הגורם האנושי: איבוד סיסמאות, שימוש בסיסמאות שקל לנחשן ("QWERT", "1234"), הפקרת האמצעי הפיסי המשמש לזיהוי, וכדומה.

42 השוו לחוק הקנדי Criminal Code, R.S.C. 1985, c. C-46, s. 342.1, הקובע עבירה של שימוש לא מורשה במחשב, למשל באמצעים טכנולוגיים או שימוש בסיסמה של אחר.

43 ראו ע"פ (ת"א) 71832/02 **ואטורי נ' מדינת ישראל** (26.11.03).

במקרה אחר הורשע נאשם, לפי הודאתו, בעריכת וירוס מחשב שנשלח לעובדיה של חברה מסוימת. הווירוס פעל כך שחשף בפני שולח הווירוס את שמות המשתמשים ואת סיסמאותיהם.⁴⁴ ההרשעה הייתה, כמובן, בעבירה של עריכת נגיף מחשב (סעיף 6), אולם, פרשנות ראויה של החוק ויישומו צריכים לגרור הבנה של חומרת המעשה. נוסף להפצת הווירוס, החומרה היא פעולתו של הווירוס – הפגיעה בעקרון אימות הזהות. זהו ערך המוגן בחוק המחשבים ולכן ראוי להביאו בחשבון בעת גזירת הדין.

2. בקרת גישה וחזירה שלא כדין לחומר מחשב

מערכות מחשב משמשות בו-זמנית משתמשים רבים. מטעמים שונים מבקשים מפעילי המערכת להגביל את אפשרות הגישה והפעולה של המשתמשים השונים לאזורים מוגדרים במערכת ולפעולות מוגדרות מראש. בקרת הגישה נועדה לפעול הן כלפי פנים והן כלפי חוץ.

בקרת הגישה הפנימית מבוססת על מערכת של הרשאות (authorization) וקובעת היכן יכולה המשתמשת לגלוש ומה הפעולות המותרות לה. המקרה הפרדיגמטי הוא של עובד, שמורשה לבצע פעולות מסוימות במערכת, אך חורג מההרשאה. בקרה פנימית מיועדת להשיג מידור בתוך הארגון, כדי שעובדים לא ייחשפו למידע סודי, למידע רגיש, לסודות מסחריים של המעסיק שיש חשש שידליפו אותו או למידע של צדדים שלישיים המוחזק במערכת ומוגן בדיני הגנת הפרטיות. כלומר, כלל אבטחה העוסק בבקרת גישה פנימית נועד להגן על שלמות המערכת ועל סודיות המידע. חשיבותם של כללי מידור בארגון באה לידי ביטוי בפסיקה אחרונה של בג"ץ: היעדרם של כללי מידור בקשר לבקרת הגישה היה טעם מרכזי לקבלת עתירה נגד משרד הפנים ולהוצאת צו מוחלט שבו הורה בית המשפט להפסיק את העברת המידע לידי גופים ציבוריים דוגמת רשות השידור, שבהם לא היו כללי מידור מספיקים.⁴⁵ לפיכך, מטרתה של בקרת הגישה הפנימית היא הגנה על אינטרסים של מפעילי המערכות (המדינה, המעסיק) והגנה על אינטרסים של צדדים שלישיים (פרטיות).⁴⁶

בקרת הגישה החיצונית (access control) מכוונת למנוע ממי שאינם מורשים להשתמש במערכת, מלהשתמש בה בכלל או מלבצע בה פעולות מסוימות. המערכת שמורה לבעליה, המבקש לשלוט בה ובמידע הנמצא בה, בין מטעמים מסחריים של

44 ראו ע"פ (ת"א) 2591/04 מדינת ישראל נ' אנור (31.10.04).

45 ראו בג"ץ 8070/98 האגודה לזכויות האזרח נ' משרד הפנים, פ"ד נח(4) 842.

46 ראו, לדוגמה, הנחיות מערכת המחשב של המינהל הבית ספרי, המיועדת לשימוש בתי ספר, המגדירות אלו בעלי תפקידים או אחרים רשאים לעשות אילו פעולות: http://cms.education.gov.il/EducationCMS/Units/Manbas/maarechet/avtachat_meyda/nehelim/Midur.htm.

שמירה על סודות מסחר, בין מחמת חובה שהדין מטיל, למשל על אבטחת "מאגר מידע" כהגדרתו בחוק הגנת הפרטיות, או מטעם לגיטימי אחר. אדון בשני פניה של בקרת הגישה לפי סדרם. במהלך הדיון אבחן את העבירה של "חדירה שלא כדין" שבחוק המחשבים, אטען שיש לפרשה בצמצום, ושאין מקום להרחיבה למישור האזרחי.

א. בקרת גישה פנימית

האם ראוי להגן על עקרון אבטחת המידע של בקרת הגישה הפנימית באמצעות הגדרתה של עבירה פלילית בחוק? ההקשר, כזכור, הוא של עובד החורג מתחום ההרשאה. אני סבור שאין מקום לקבוע חריגה כזו כעבירה פלילית. האינטרסים והזכויות המוגנים על ידי עיקרון זה נהנים כבר עתה מהגנה משפטית רחבה: המידע על אזרחים המוחזק אצל המעסיק מוגן במסגרת דיני הגנת הפרטיות.⁴⁷ האינטרסים של המעסיק בשמירת סודותיו העסקיים ומניעת ריגול תעשייתי מוגנים במסגרת דיני העוולות המסחריות ודיני סודות מסחר.⁴⁸ אינטרסים של המדינה מוגנים בחובות אמון של עובדיה. למעסיקים (בין המדינה ובין מעסיק פרטי) יכולת לקבוע כללי התנהגות המגובים בתקנון משמעת או בסנקציות אחרות, עד כדי פיטורים. אם נעשה שימוש לרעה במידע – הרי הפעולה תהיה בדרך כלל גם עבירה פלילית וגם עבירת משמעת.⁴⁹

במילים אחרות: האינטרסים השונים המוגנים כאן, בין שהם של הציבור, של המעסיק או של צד שלישי כלשהו, נהנים ממבנה הגנה רב-שכבתי: **הסדרה ציבורית ישירה** (בדרך של חקיקה פלילית) המגינה על הסוד, המידע וכדומה.⁵⁰ בנוסף לכך,

47 ראו חוק הגנת הפרטיות, התשמ"א-1981, במיוחד סעיפים 2(9), 8(ב), ובקשר לגופים ציבוריים גם סעיף 23ב.

48 ראו חוק עוולות מסחריות, התשנ"ט-1999 (להלן: "חוק עוולות מסחריות"). כאשר "הריגול התעשייתי" כרוך בהאזנת סתר, בהעתקת יצירות המוגנות בזכויות יוצרים, עומדות לרשות התובע גם עילות אלה.

49 ראו, למשל, רע"פ 10225/01 **כהן נ' מדינת ישראל**, תק-על 2002(1) 216. באותו מקרה הורשע מפעיל מחשב בעיריית נתניה בעבירות של קבלת דבר במרמה בנסיבות מחמירות, זיוף ועוד עבירות, בקשר עם שורת מקרים בהם נכנס הנאשם לבסיסי נתונים של בעלי מקרקעין, הזין נתונים כוזבים ובכך הביא להפחתת תשלומי המס של הבעלים. ראו גם עש"ם 6348/01 **בן דוד נ' הנציבות**, פ"ד נו(2) 918.

50 במונח "הסדרה ציבורית" כוונתי לנורמה משפטית שמקורה ברשויות ציבוריות, דוגמת הכנסת או בתי המשפט. הסדרה ציבורית יכולה להיות ישירה – כאשר היא מגדירה במפורש את המותר ואת האסור, או עקיפה, כאשר היא יוצרת תמריצים חיוביים או שליליים לפעולה. הסדרה פרטית מקורה ב"שטח" והיא צומחת "מלמטה", בין בדרך של קוד אתי, קביעת מדיניות, וכדומה. לדיון, ראו מיכאל בירנהק "הסדרה פרטית – מסמך עקרונית" **איגוד האינטרנט הישראלי** (2004), נמצא ב: http://www.isoc.org.il/hasdara/hasdara_code.html.

הסדרה פרטית הנהנית מגיבוי ציבורי, בדמות חוזי עבודה ותקנוני משמעת, שייאכפו במידת הצורך ובמקרים המתאימים לפי דיני החוזים ודיני העבודה. ונוסף על כך, **הסדרה פרטית-טכנולוגית** שיכול המעסיק או מפעיל המערכת לנקוט, כלומר, אותם אמצעים שנדונו לעיל של אימות הזהות ואמצעים טכנולוגיים להגבלת גישה.⁵¹ הצעת חוק המחשבים כללה בשעתה איסור על "שימוש במחשב תוך חריגה מהרשאה", אלא שהאיסור הושמט מהנוסח הסופי.⁵² כיצד ניתן להסביר את ההשמטה הזו? הסבר אפשרי אחד הוא שאין צורך באיסור כזה, משום שהוא כלול ממילא בעבירה של חדירה שלא כדין לחומר מחשב, למשל, במקרה שבו אדם המורשה להשתמש במחשב חדר לקובץ שאליו לא היה מורשה לחדור (מה שמוגדר כאן כחריגה מהרשאה ובקרת גישה פנימית).⁵³ סעיף 4 לחוק קובע כי:

החודר שלא כדין לחומר מחשב הנמצא במחשב, דינו – מאסר שלוש שנים; לעניין 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, תשל"ט-1979.⁵⁴

גם בכמה פסקי דין הביעו בתי משפט את עמדתם, כי חריגה מהרשאה היא עבירה פלילית או הניחו זאת כמובן מאליו, כאשר המסגרת לכך נמצאה בעבירה של חדירה שלא כדין לחומר מחשב. כך, למשל, בעניין אחד הורשע עובד לשעבר של חברה, לפי הודאתו, בעבירה זו.⁵⁵ בית המשפט גזר עליו שנת מאסר על-תנאי וקנס, מבלי שנדונה כלל השאלה אם התמלאו יסודות העבירה (כאמור, הנאשם הודה באישום). האם היה מקום להרשיע בעבירות אלה? האם יש לראות בחריגה מהרשאה משום "חדירה שלא כדין לחומר מחשב"? אני סבור שצדקה הכנסת כאשר סירבה לחוקק את האיסור וכי יש לפרש את סעיף 4 הנ"ל בצמצום, כך שלא יוחל על חריגה מהרשאה. נימוק אחד לפרשנות המצמצמת של סעיף 4 נגזר מהמסגרת של דיני מידע שהוצגה לעיל. המשפט מציע מספר מעגלי הגנה כדי להבטיח את בקרת הגישה הפנימית: הסדרה ציבורית ישירה, הסדרה פרטית בגיבוי ציבורי והסדרה פרטית, בין משמעתית ובין טכנולוגית. די באמצעים אלה. לטעמי, לא רצוי שפעילות מסוימת תיאסר בו-זמנית בכמה דינים נפרדים. בכל אחד מהדינים הנזכרים יש מערכת של איזונים פנימית

51 למשל תוכנות ניטור המתעדות את השימוש במערכת, המכוננות באופן כולל בשם audit-trail. ראו הגדרה: http://www.webopedia.com/TERM/A/audit_trail.html.

52 בדברי הכנסת אין הסבר להשמטה. הפרוטוקולים של ועדת המשנה של הכנסת אינם ברורים בעניין זה.

53 בועז גוטמן "חקיקת מחשבים ויישומה" **משפט וצבא** 13 (התשנ"ט) 175, 180.

54 בשונה מהעבירות שבסעיף 2, הרי חדירה שלא כדין לחומר מחשב אינה מוגדרת כעוולה. ראו סעיף 7 לחוק.

55 ת"פ (ת"א) 123670/97 **מדינת ישראל נ' שפירא**, דינים שלום יח 863.

המביאה בחשבון שיקולי-נגד.⁵⁶ דיני זכויות יוצרים, למשל, מאזנים בין היוצר לבין הציבור. פעולות מסוימות בדיני זכויות יוצרים, למשל, מותרות, בהיותן "טיפול הוגן".⁵⁷ דיני העבודה מאזנים בין האינטרסים והזכויות של המעסיק לאלו של העובדים. כאשר המהות העיקרית של הפעולה הבעייתית מוסדרת בחוק אחר, ובכל זאת אנו פונים לעבירה של "חדירה שלא כדין לחומר מחשב", הרי אנו מתעלמים מכל אותם שיקולי-נגד המצויים בדינים העוסקים בפעילות האסורה ממש. אנו עשויים למצוא עצמנו אוסרים בחוק המחשבים את שהתרנו בחוק זכות יוצרים. זאת ועוד, כפל האיסורים עלול לגרום סתירות בין החוקים, מה שמותר בחוק אחד (שימוש הוגן) ייאסר בחוק אחר (חוק המחשבים). התוצאה תהיה אי-בהירות, ומאחר שאנו נמצאים בהקשר הפלילי, יש בכך פגיעה בעקרון החוקיות. אולם זהו רק נימוק אחד לפרשנות מצמצמת של העבירה. נימוק שני הוא, שאת האיסורים על שימוש במחשב יש להטיל במשורה. ריבוי איסורים פליליים יוצר אווירה עוינת בקשר לשימוש במחשב. הוא משרד מסר לאנשי הטכנולוגיה כי מדובר במכשיר שהשימוש בו מסוכן, ולעיתים הוא על סף הפלילי. מסר כזה בעייתי במיוחד בהקשר של יחסי העבודה. יש בו הרתעת-יתר שאינה רצויה. עובד כפוף לשורת חובות בדין הכללי ובדין המשמעותי, ומחויב להישמע להוראות הממונים עליו. הכבדה נוספת מצד החוק הפלילי מתערבת שלא לצורך ביחסי העבודה ומציידת את המעסיק בכלי רב עוצמה שמחירו גבוה מתועלתו. דיני העבודה מושגתים על העיקרון של צמצום פערי הכוח שבין העובד למעסיק, ואם נפנה למסלול של חוק המחשבים, נימצא עוקפים אותם איזונים מורכבים שבדיני העבודה.

מכאן עולה מסקנה פרשנית, במקרה שבו זוהתה חריגה מהרשאה (בקרת גישה פנימית), וככל שגרמה לנזקים, הרי זהו עניין שיש לבחון ולהכריע בו לפי הדין הכללי הקיים (פגיעה בפרטיות, הפרת זכויות יוצרים, הפרת סוד מסחרי, דיני חוזים ודיני העבודה), או לפי דין משמעותי, והיא ניתנת למניעה גם באמצעים טכנולוגיים פשוטים וזולים למדי. די בשילוב של הדין הכללי על רבדיו השונים, בדין המשמעותי ובאמצעי ההסדרה הפרטית. אין לפרש את עבירת החדירה שלא כדין שבחוק המחשבים כאוסרת חריגה מהרשאה. כך ניתן משקל פרשני ראוי להיסטוריה החקיקתית של חוק המחשבים, כמו גם לתכליתו.

56 גם בית המשפט העליון מחזיק בגישה כזו, למשל בקשר לחוק הגנת הפרטיות. בית המשפט סבור שכאשר פעילות אסורה בחוק איסור לשון הרע, די בעבירה שם, ואין לפרש את חוק הגנת הפרטיות כך שישתרע גם הוא על אותה פעילות. ראו רע"פ 9818/01 **ביטון נ' סולטן** (טרם פורסם), בפסקה 40 לפסק דינו של הנשיא ברק. לטעמי, דווקא שם טעה בית המשפט בנקודה זו, אולם זהו עניין למאמר אחר.

57 ראו סעיף 1(2) לחוק זכות יוצרים, 1911.

ב. סודיות ובקרת גישה חיצונית

מהי, אם כן, הפרשנות הראויה של העבירה שעניינה חדירה שלא כדין לחומר מחשב? לטעמי, העבירה מגלמת את עיקרון אבטחת המידע של סודיות (confidentiality), שנועד להגן על המידע הנמצא במערכת המחשב מפני עיניים זרות. עקרון זה נפרט לכלל האבטחה של בקרת גישה חיצונית. יחד עם זאת, גם כאן, פרשנות העבירה של חדירה שלא כדין צריכה להיות זהירה, ממספר טעמים:

(1) עמימות הגדרתה של העבירה (2) הבנת דרך התפתחותה של הטכנולוגיה (3) שימוש זהיר במטפורות קנייניות (4) הבנת עולם המחשבים הנוכחי **כרשת** מחשבים ולא כמחשבים נפרדים.

(1) הטעם הראשון לפרשנות המצמצמת קשור להגדרת העבירה. עבירה זו כוללת מרכיב פעולה (אקטוס פאוס) עמום להפליא: מהי "חדירה"? מה בדיוק נחדר כאן? ומהי חדירה כדין או "חדירה שלא כדין"? סעיף 4 לחוק, שצוטט לעיל, מגדיר חדירה לחומר מחשב כ"חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר". זו הגדרה טאוטולוגית, שאינה מועילה במיוחד. כדי להבין מה כלול בה, ניתן להראות מה אין כלול בה.

פרופ' Orin Kerr מנתח את הביטוי "unauthorized access", המקביל לביטוי הנקוט בחוק הישראלי.⁵⁸ זהו ביטוי מרכזי המופיע ברבים מחוקי המחשבים בארצות הברית ובמדינות אחרות. קר מצביע על היעדר אחידות בפרשנות הביטוי ומציע להבחין בין גולש, שניגש למחשב תוך הפרת תנאי החוזה (המשתמע או המפורש) שבינו לבין מפעיל האתר, לבין גישה לחומר מחשב הכרוכה בעקיפת מנגנונים טכנולוגיים. לשיטתו, העבירה הפלילית אוסרת רק את המצב השני (או ליתר דיוק, כך ראוי שיהיה). פרשנות כזו, כך הוא מסביר, מאזנת בין שני ערכים מנוגדים, חירות השימוש ברשת מול פרטיות הגולשים שמידע אודותיהם מוחזק אצל האתרים בהם הם גולשים. אם יפורש הביטוי "גישה שלא כדין" כך שיקיף גם הפרת חוזה, טוען קר, משמעות הדבר היא שיופקד כוח רב מדי בידי בעלי אתרים על חשבון הגולשים.⁵⁹

58 Orin S. Kerr "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Fraud and Abuse Act, codified as 18 U.S.C. §1030 and Abuse Act, codified as 18 U.S.C. §1030. ראו גם, Computer Misuse Statutes" 78 NYU L. Rev. (2003) 1596
הביטוי illegal access.

59 שם, בע' 1649-1650.

אני מצטרף לעמדתו של קר. אתרים רבים נוהגים לפרסם הודעה, שתוקפה החוזי אינו ברור תמיד,⁶⁰ כי בגלישתו מסכים הגולש לתנאים שמפורטים אי שם באתר (ובדרך כלל מנוסחים בשפה משפטית עמומה ומעורפלת להפליא). פעמים רבות תנאים אלה מתיימרים לצמצם את זכויותיו של הגולש, למשל בקביעת סמכות שיפוט וברירת דין במקומות שאינם נגישים לגולש, או בתניות גורפות של פטור מאחריות. תניות שימוש אחרות אוסרות לעיתים הנדסה חוזרת של האתר, הגם שזו מותרת לפי דיני סודות המסחר ופורשה בפסיקה האמריקנית כ"שימוש הוגן" במסגרת דיני זכויות יוצרים.⁶¹ האם גולשת שהפרה תנאי מהתנאים (גם אם מעמדם הוא של חוזה תקף), למשל בקשר למטרת השימוש באתר, הנדסה חוזרת וכיוצא באלה פעולות, אשמה בעבירה של "חדירה שלא כדין"? אני סבור שהתשובה שלילית. נזק שייגרם כתוצאה מהפרת חוזה כזה, בהנחה שהחוזה תקף והוא הופר, צריך להיבחן במשקפי דיני החוזים, ואם נגרם נזק – גם במשקפי הדין הרלוונטי (למשל הפרת זכות יוצרים, אם פעולת המשתמש מגיעה לכדי כך). כל אחד מהאפיקים האפשריים שמציע הדין הכללי מושתת על איזון מורכב בין אינטרסים. עקיפתם ופנייה לחוק המחשבים מבטלת את השיקולים היריבים ואת האיזון שנערך שם. לפיכך, פרשנות ראויה של עבירת החדירה שלא כדין לחומר מחשב אינה מקיפה מצב של הפרת חוזה גלישה.

התוצאה היא, כי העבירה של חדירה שלא כדין לחומר מחשב, תחול רק על מי ש"פורץ" "מנעול" טכנולוגי שהגן על הגישה החיצונית לאתר (וכפי שאסביר מיד, יש להיזהר במטפורות אלה, השאלות מהעולם הפיסי). כך למשל, כניסה לאתר דרך "פורט" (ולא "סריקת פורטים" לבדה)⁶² שלא נועד לכך, היא לכאורה חדירה שלא כדין לחומר מחשב. הפרת תנאי שימוש האוסרים גלישה באתר פלוני אינם מקימים אשמה בעבירה זו.

מצב מעניין אחר הוא כאשר למשתמש אחד ניתנה רשות לגלוש באתר, למשל באמצעות סיסמת זיהוי, ונאסר עליו להעביר את ההרשאה (והסיסמה) לאחר, ובכל זאת הוא העבירה. מצב זה מתעורר לדוגמה בקשר לאתרים "סגורים", המאפשרים גישה מבוקרת לאתר ולתכנוני בכפוף להתחייבות לשימוש שאינו מסחרי בלבד, או בכפוף לתשלום. ברור, כי למפעילי האתר עילת תביעה טובה נגד המורשה הראשון שהעביר את ההרשאה לאחר ללא רשות, שהרי המורשה הפר את התחייבות החוזית. האם יש למפעילי האתר עילת תביעה לפי חוק המחשבים נגד מקבל הסיסמה השני, הנעבר, אם זה גלש באתר תוך עשיית שימוש בסיסמה שקיבל מחברו? האם מדובר בחדירה שלא

60 לסוגי חוזים ברשת ולתוקפם, ראו Specht v. Netscape Communications Corp., 150 F.Supp. 2d 585 (S.D.N.Y. 2001).

61 לדין, ראו Pamela Samuelson & Suzanne Scotchmer "Law and Economics of Reverse Engineering" 111 Yale L. J. (2002) 1575; ניבה אלקין-קורן "זכויות יוצרים ותחרות: משוק עותקים למשטר רישוי" **דין ודברים** ב (תפרסם בתשס"ו).

62 ראו הדיון בעניין מזרחי, **להלן**, פרק ה.3.

כדין לחומר מחשב? נראה לי כי המבחן לתשובה הוא צורת החדירה. אם באתר יש חוזה, שבלי לקבלו קיבול משפטי אין אפשרות לגלוש (למשל מסך המחייב אישור קריאה, בטרם מתאפשר המשך הגלישה), הרי עשויה לקום עילה חוזית, וכאמור לפי עמדתו של קר, שאליה אני מצטרף, אין מקום להפליה גם בחוק המחשבים.⁶³ אם מדובר באתר שבלעדי הסיסמה אי אפשר לגלוש בו, או שננקט אמצעי טכנולוגי אחר המגביל גישה, הרי יש לראות בכך אתר "סגור", ומי שעוקף את האמצעי הטכנולוגי "חודר" אליו שלא כדין.⁶⁴

ניתן להקשות: גם חוזה וגם טכנולוגיה המגינה על הגישה לאתר הם אמצעים של הסדרה פרטית, כלומר אמצעים שנוקט בעל האתר בעצמו. מדוע, אם כן, להתייחס באופן שונה לחוזה ולטכנולוגיה? הנה שתי תשובות: הראשונה, היא שמנעול טכנולוגי נהיר יותר לגולש מאשר חוזה. "החוזה" אינו תמיד נגיש, הוא "קבור" פעמים רבות במקום סמוי באתר, תוכנו מנוסח בשפה משפטית, מעורפלת ולא ברורה. "מנעול טכנולוגי", לעומת זאת, מציב תמרוך ברור לגולשת: אם אינך יודעת את סיסמת הכניסה לאתר, לא תוכלי להיכנס אליו בדרך המלך. האיתות מובן יותר לגולש מאשר תנאי השימוש המעורפלים. תשובה שנייה, נסמכת על בדיקה כלכלית של עלויות ההגנה של בעל האתר. הוספת "חוזה" אינה עולה למפעיל האתר כמעט דבר, במיוחד אם החוזה מועתק מאתר אחר. מפעיל אתר המבקש להסתפק בהגנה חוזית מאותת בכך כי הגנת האתר אינה בראש מעייניו. לעומת זאת, שימוש באמצעי טכנולוגי מאותת את ההיפך: מפעיל האתר מבקש להגביל את השימוש באתר, מסיבה זו או אחרת.⁶⁵

63 יש לבחון את החוזה, שבין האתר למקבל הסיסמה המורשה, בקפדנות, מפני שאולי העברת הסיסמה והרשות מותרות.

64 השוו למקרה שנדון בארצות הברית: עובד לשעבר הקים אתר ביקורת על מעסיקו הקודם, שהגישה אליו התאפשרה רק באמצעות סיסמה. המעסיק השיג סיסמה מגולש מורשה, גלש באתר ותבע על לשון הרע. בית המשפט קבע שמדובר בחדירה שלא כדין. ראו, **Konop v. Hawaiian Airlines, Inc.**, 302 F.3d 868, 879 (9th Cir. 2002), cert. denied 537 U.S. 1193 (2003).

65 יש להבדיל בין האיסור שבחוק המחשבים על פריצת מנעול טכנולוגי לבין איסור על עקיפת מנעולים טכנולוגיים המגינים על יצירות המוגנות בזכויות יוצרים (Digital Rights Management). איסורים מעין אלה, המכונים anti-circumvention, נחקקו בארצות הברית במסגרת ה-Digital Millennium Copyright Act 1998, בסעיפים 1201-1205 שם, ואף נכללו ב-WIPO Copyright Treaty 1996. בישראל עדיין לא נחקק חוק מקביל, אם כי הנושא נדון במשרד המשפטים. לעמדתו, יש לפרש סעיפי ה-anti-circumvention כך שתותר "פריצה" של "מנעול טכנולוגי" כאשר היא מיועדת לאפשר שימוש הוגן ביצירה, לפי דיני זכויות יוצרים, מטעמים שביסוד דיני זכויות יוצרים. יש להקפיד, שחוק המחשבים לא ייצור מסלול העוקף את האיוון המורכב שבדיני זכויות יוצרים.

גם כאשר מדובר בעקיפת מנגנונים טכנולוגיים מתעוררים קשיים. למשל, עם התרחבות השימוש בחיבור אלחוטי לרשת האינטרנט, עולות שאלות בדבר התחברות גולשים למשרדים (hotspot) של משתמשים אחרים. הטכנולוגיה הנוכחית מאפשרת לבעל המשרד לבחור אם ברצונו לאפשר גישה פתוחה או לסגור את השימוש לבעלי סיסמה בלבד. ברירת המחדל הטכנולוגית היא שהרשת פתוחה. כאשר גולש מצליח לעקוף סיסמה ולהשתמש ברשת סגורה, הרי ניתן לראות בכך חדירה שלא כדין לחומר מחשב (אם כי נדרשת פרשנות גמישה וכלל לא מובנת של המונח "חומר מחשב" כדי שיקיף גם את החיבור האלחוטי לאינטרנט). כאשר נעשה שימוש ברשת שהושארה פתוחה, בין בכוונה תחילה ובין מחמת אי שינוי ברירת המחדל הטכנולוגית, אין לראות בכך חדירה שלא כדין לחומר מחשב. להיפך. במקרה כזה מגלמת הרשת ערך של פתיחות ושיתוף.⁶⁶

(2) הטעם השני לפרשנות המצמצמת של סעיף 4, הוא חשש מהרתעת-יתר. בסביבה הטכנולוגית הדינמית יש ערב-רב של שחקנים שקשה להבחין ביניהם. החוקרים הממוסדים והחובבים מחד גיסא, ועברייני המחשב מאידך גיסא. המשפט הפלילי מנסה להבחין בין הראשונים לאחרונים. כאשר הכלל המשפטי מופעל בבתי המשפט, יש לקוות שהשופטים יידעו להבחין בין "הטובים" ל"רעים". אולם, הכלל המשפטי פועל גם מחוץ לבתי המשפט. בעצם קיומו הוא משרד מסר לציבור הרלוונטי. בכלל רחב מדי יש הרתעת-יתר, שמחירה בצידה. המחיר הוא פגיעה במחקר, בחופש לנסות, "לשחק" עם המחשב, ללמוד את דרך פעולתו ולהכיר את יתרונותיה ואת חסרונותיה של מערכת המחשב. ה"משחק" במערכת המחשב הוא הדרך שבה נרכש ידע טכנולוגי. כך נוצר ידע חדש. כך, במידה רבה, מתוך ניסוי וטעייה מתפתחת טכנולוגיה חדשה.

הדבר דומה בעיניי למגבלות על מחקר רפואי, דמו מנהלי מעבדת מחקר אוניברסיטאית האוכפים אכיפה קפדנית את חוקי הסמים במעבדות. ודאי שאסור לייצר סמים, ויש לכך איסורים מפורשים בדין הפלילי.⁶⁷ כיצד תנהג סטודנטית החוקרת במעבדה ומנסה תרכובות שונות כדי ללמוד את התנהגות החומרים, ואגב הניסוי מייצרת סם אסור? לכלל משפטי פלילי רחב יהיה אפקט מצנן על המחקר, והחוקרת עלולה להימנע ממנו מלכתחילה. השוני בהקשר של המחשבים הוא שהמעבדה שקולה כאן לכלל המחשבים בעולם. כל גולש ברשת שקול לחוקרת במעבדה. אם תפורש עבירת החדירה שלא כדין לחומר מחשב בפרשנות מרחיבה, הרי הניסוי התמים במחשבים עלול להסתיים בעבירה פלילית (כפי שאירע לאבי מזרחי, שבעניינו אדון

66 לדין בחשיבות השיתוף וביתרונות הכלכליים שלו גם בהקשר של רשת אלחוטית, ראו Yochai Benkler "Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production" 114 *Yale L. J.* (2004) 273, 344-348.

67 פקודת הסמים המסוכנים [נוסח חדש], התשל"ג-1973, אוסרת ייצור סמים וקובעת חריג (בסעיף 6), שלפיו הדבר מותר ברישיון של המנהל הכללי של משרד הבריאות.

בהמשך). מובן, שאת ההבחנה בין החוקרת לבין עברייני הסמים, או בהקשרנו – בין הנערה המבקשת ללמוד כיצד פועלת מערכת מחשבים לבין עברייני המחשבים, ניתן להשיג באמצעות הקפדה על המרכיב הנוסף הנדרש להרשעה, המחשבה הפלילית. אלא, כפי שעולה מהתנהגות רשויות האכיפה בעניין **אבי מזרחי**, ההבחנה הזו לא תמיד היא מספיקה.⁶⁸

רעיון זה, בדבר חשיבות הניסוי והטעייה בפיתוח טכנולוגי, אינו זר למשפט. דיני סודות מסחר, למשל, מתירים במפורש את הפעולה של הנדסה חוזרת, ולא בכדי.⁶⁹ ההיתר בא מתוך מחשבה תחילה ומתוך כוונה ברורה לעודד מחקר בדרך של "לימוד על ידי פירוק" של הטכנולוגיה, ומתוך הבנה כי רעיונות ועובדות צריכים להישאר בנחלת הכלל. על ידי פירוק מוצר ניתן ללמוד כיצד הוא פועל ומה העיקרון הטכנולוגי שביסודו. הרעיון עצמו, הנמצא ביסוד המוצר, אינו מוגן, ולכן יש לאפשר למעוניינים לחקור ולחשוף אותו. במילים אחרות, הטכנולוגיה מתפתחת, בין היתר, בדרך של תהייה, ניסוי וטעייה, ובדרך של שימוש ברעיונות קיימים ויישומם למצבים חדשים. הטכנולוגיה מתקדמת כפרייקט כלל-אנושי מורכב, שבו כל משתתף מניח את תרומתו על גבי ידע קיים, אבן על אבן, נדבך על נדבך. זו גם עמדת-יסוד של דיני זכויות יוצרים.⁷⁰ את התובנה הפשוטה והחשובה עד מאוד בדבר דרך התפתחותה של הטכנולוגיה, ראוי לקלוט גם לתוך פרשנות חוק המחשבים. עמדה כזו מושגת מתוך הבנת היחס הדיאלקטי שבין משפט לטכנולוגיה. מכאן נדרשת פרשנות זהירה של סעיף 4.

(3) שני הטעמים הבאים לפרשנות מצמצמת, שימוש זהיר במטפורות והבנת עולם המחשבים כרשת, כרוכים זה בזה. מסעיף 4 לחוק עולה, כי מטרתו היא למנוע פריצות חיצוניות למחשבים ולמערכות מידע, בין אם אלה נועדו להשיג יעדים אחרים (טרור או פשיעה בעולם הפיסי), ובין אם נועדו לפגוע בשלמות המידע ובזמינות המערכת (שני עקרונות של אבטחת מידע שיידונו בהמשך). הכניסה הלא-מורשית למערכת נתפשת כפריצה – בדומה לפריצה בעולם הפיסי. זהו גם המקום שבו המטפורה של העולם הפיסי מושלכת במלוא עוצמתה לעולם הווירטואלי, ופעמים רבות ללא תשומת לב

68 יש להיזהר במטפורות, וההיקש כאן אינו מלא. חיים רביה מעיר לי, כי פרוץ המחשבים אינו שקול לחוקר העורך ניסיונות במעבדה שלו, אלא לחוקר המנסה לחבל במעבדה אחרת. תשובתי היא שהרשת היא כולה מעבדה אחת, כפי שאסביר גם בהמשך, ולכן אין לראות כאן "מעבדות" נפרדות.
69 ראו סעיף 6(ג) לחוק עוולות מסחריות, התשנ"ט-1999. מובן שאפשר להסביר את הכלל המתיר הנדסה חוזרת גם בדרכים אחרות, למשל כאיתות לבעלי הסוד לשקול את הכדאיות של הגנה באמצעות דיני הפטנטים.

70 ראו סעיף 7 לפקודת זכות יוצרים, 1924. ככל שמדובר ברעיון מופשט, שאינו מגולם בהמצאה חדשה, מועילה, ושיש בה התקדמות המצאתית, גם דיני הפטנטים אינם מגינים על רעיונות בעלמא. ראו סעיפים 3-5 לחוק הפטנטים, תשכ"ז-1967.

למשמעות השימוש במטפורה.⁷¹ כך, למשל, דו"ח של מדינות חבר העמים הבריטי הדגיש את מרכזיות האיסור והעיר: "The offence is important in several respects. It is analogous to an offence of 'break and enter' as it involves accessing private premises' without excuse or justification".⁷² לפי גישה זו, האיסור על חדירה שלא כדין נתפש כמגן על הקניין הפרטי.

האומנם שקולה מערכת המידע הממוחשבת למקרקעין או מיטלטלין? האם ראוי לראות במחשב המחובר לרשת מחשבים – לאינטרנט – משום קניין פרטי? ברור שהאטומים – המחשב הפיסי – הם קניין פרטי של בעליו. אולם האם ראוי לראות גם את הסיביות כקניין פרטי?⁷³ ההיסטוריה החקיקתית של חוק המחשבים מעלה שהגישה הקניינית נדחתה, ולטעמי – בצדק נדחתה. העבירה של חדירה שלא כדין הוגדרה בצמצום ונקבעו בה מגבלות: האחת היא הביטוי העמום "שלא כדין",⁷⁴ הקורא כמובן לפרשנות, והשנייה היא דרישת המחשבה הפלילית (גם אי הגדרתה של החדירה שלא כדין כעולה במשפט האזרחי אינה מקרית). פרופ' מיגל דויטש, שהיה פעיל בניסוח טיוטות החוק, מעיד שהעבירה נועדה למנוע עבירות באמצעות מחשב, ולא עבירות נגד מחשב.⁷⁵ כמובן זה, תכליתה של העבירה היא מכשירנית, וחריגה בנוף המשפט הפלילי, העבירה קובעת עבירת הכנה כעבירה פלילית.⁷⁶ הטעם שדויטש מביא להצדקת הצעד החריג, של הפללת פעולת הכנה והגדרתה כעבירה בפני עצמה, הוא הקושי להוכיח את העבירות המבוצעות באמצעות מחשב, כמו מרמה.⁷⁷ מטעם זה, גם לא נקבעה עוולה מקבילה. מובן, שלעדוהו של דויטש אין מעמד מחייב בפרשנות חוק, אולם, אני סבור שהפרשנות הראויה של החוק (ותכלית החוק) תואמת את הכוונה ההיסטורית שהוא מעיד עליה. אין זה ראוי לפרש את העבירה בדרך הקיצונית המרחיבה כך שתקיף כל חדירה למחשב.

71 למטפורות תפקיד מכריע בעיצוב החשיבה, והיא אינה רק פיוט טקסטואלי. לדיון ראו Dan Hunter "Cyberspace as a Place and the Tragedy of the Digital Anticommons" 91 Cal. L. Rev. (2003) 439.

72 ראו 33 Law in Cyber Space (Commonwealth Secretariat, 2001).

73 למונחים "אטומים" ו"סיביות", ראו נגורפונטי, לעיל הערה 26.

74 לדיון ראו נעמי אסיא דיני מחשבים – הלכה למעשה (תשס"ג, כרך א) 345.

75 דויטש, לעיל הערה 19, בע' 440.

76 המשפט הפלילי נמנע, בדרך כלל, מקביעת מעשי הכנה כעבירות עצמאיות. ראו מרים גור-אריה "על ההבחנה בין הכנה לבין ניסיון" משפטים לב (תשס"ב) 505. לכלל זה חריגים בודדים, למשל סעיף 497 לחוק העונשין, התשל"ז-1977, הדין ב"הכנת עבירה של חומרים מסוכנים".

77 דויטש, לעיל הערה 19, בע' 441.

גם הרחבתו של האיסור לתוך השדה האזרחי אינה ראויה בעיניי.⁷⁸ כלומר, יש לדחות את העמדה הקניינית הרואה בכל כניסה לחומר מחשב משום הסגת גבול במיטלטלין. הפרשנות המוצעת כאן נסמכת על זהירות בשימוש במטפורות, על עיון זהיר בטכנולוגיה שבה מדובר, מתוך העמדה הכוללת בדבר היחס הראוי שבין משפט לטכנולוגיה. טעמים אלה שפורטו מצטרפים לזהירות הנדרשת בעת פרשנות עבירה של הכנה, שגם היא כשלעצמה חריגה ובעייתית בנוף המשפטי.

(4) כאמור, המחשב הפיסי הוא מושא לבעלות קניינית. אלא שהסיביות שבמחשב נמצאות "שם" רק במידה מוגבלת. הן "שם" והן בכל מקום ברשת. מחשב המחובר לאינטרנט הוא חלק מרשת. ערכה של רשת האינטרנט הוא בדיוק במאפיין זה, בחיבור שבין המחשבים. בכך שערכו של כל אחד מהם לבדו קטן מאוד, והשלם – הרשת – גדול מסכום חלקיו. על מפעיל מחשב המחובר לרשת להבין כי המחשב אינו עומד בוד, הוא חלק ממערכת, חלק מרשת. על מפעיל המחשב לדעת כי פעולת הגלישה הטבעית ברשת מחייבת דו-שיח בין המחשבים, ועל כן, "ביקורים" הדדיים של המחשבים זה אצל זה. אי הכרת הטכנולוגיה כשלעצמה אינה מצדיקה את השלכתן של המטפורות הפיסיות על הסביבה הווירטואלית. עמדה קניינית, המבקשת לקבוע כל כניסה לחומר מחשב כעבירה, משעתקת את התפישה האינטואיטיבית הפיסית שלנו לתוך סביבה שאינה פיסית. עמדה זו מתייחסת לאינטרנט כאל עוד מושא להסדרה משפטית רגילה, ומחילה עליו כללים משפטיים קיימים כמות שהם, מבלי לבחון את הטכנולוגיה בה מדובר, מבלי לעיין בערכים המגולמים בה, מבלי לבדוק את היתכנות ההסדרה. עמדה קניינית זו מחמיצה את הייחוד של הרשת, שאין היא צירוף מקרי של יחידות בודדות ונפרדות, אלא יחידה שלמה אחת מרובת מרכיבים.

78 ההרחבה לתחומי המשפט האזרחי אפשרית על ידי חקיקת עוולה מפורשת של חדירה שלא כדין, או על ידי פרשנות שיפוטית שתחייב את העוולה הנושנה והמיושנת של השגת גבול במיטלטלין. להצעה ברוח זו, ראו מאמרם של שרון אהרונ-גולדנברג ואריה רייך "חדירה למחשב כעוולה נזיקית" בחוברת זאת. לעוולה של השגת גבול המיטלטלין בדין הישראלי, ראו סעיף 31 לחוק המיטלטלין, תשל"א-1971. הסעיף הופעל לאחרונה, ככל הידוע, בשנת 1973, בקשר לגניבת כבשה. ראו ע"פ 2/73 סלע נ' מדינת ישראל, פ"ד כח(2) 371. העוולה האחרונה מופעלת בשנים האחרונות בארצות הברית בסביבה הדיגיטלית. ראו, למשל, eBay, Inc. v. Bidder's Edge, Inc., 100 F.Supp. 2d 1058 (N.D. D. Cal., 2000) Dan L. Burk "The Trouble With Trespass"; ניבה אלקין-קורן, "המתווכים החדשים/בכיכר השוק הווירטואלית" משפט וממשל 1 (תשס"ג) 381. גם בישראל נזכרה העוולה בפסק דין של בית משפט לתביעות קטנות, אולם הדיון שם חסר מאוד. ראו ת"ק (ת"א) 00600/03 אבן-חן נ' סריסה (בית משפט לתביעות קטנות, 15.9.03). פסק הדין נהפך בר"ע (ת"א) 002542/03 סריסה נ' בן חיים (9.10.05).

אחד ממאפייני הטכנולוגיה הוא החיבור בין המחשבים. החיבור מאפשר זרימה של מידע מכל מי שמחובר לכל מי שמחובר. הרשת מאפשרת הזדמנויות ביטוי והשתתפות בשיח, אינטראקטיביות (הידודיות), שיתוף במידע, ועוד. במילים אחרות, הרשת מגלמת ערכים חיוביים. העמדה הקניינית מחמיצה אותם. עמדה קניינית כאמור תהפוך פעולות יומיומיות ברשת לבלתי חוקיות. כעניין טכנולוגי, הרשת בנויה על "דיאלוג" נמשך בין מחשבים. כאשר גולשת מבקשת לצפות באתר אינטרנט, לכתוב הודעה בפורום או צ'אט וכדומה, יש אוסף של "שיחות" בין מחשב הקצה של הגולשת לבין אתרי היעד. התקשורת עוברת דרך אינספור מחשבים אחרים. כך בנויה הרשת המבוזרת. העמדה הקניינית המשעתקת תפישה פיסית לרשת עיוורת לטכנולוגיה. כפי שטענתי קודם, עיצוב כללי המשפט בסביבה הטכנולוגית צריך לבוא מתוך דיאלוג עם הטכנולוגיה. לפיכך, אין מקום לעמדה קניינית המבקשת להרחיב עד בלי די את האיסור של חדירה לחומר מחשב.

הפרשנות המוצעת, הדוחה את העמדה הקניינית והמעדיפה את העמדה הנובעת מתוך הדיאלקטיקה של המשפט והטכנולוגיה והבנת המחשב כחלק מרשת של מחשבים "המשוחחים" זה עם זה, משיגה איזון ראוי בין תכלית החוק של שמירה על עקרונות אבטחת המידע לבין המחיר הכרוך בהרתעת-יתר.

* * *

כל הטעמים שנמנו, ובהם עמימות העבירה, הבנת הרשת כרשת, הזהירות בשימוש במטפורות ודחיית העמדה הקניינית, אינם מאיינים את העבירה של חדירה שלא כדין. הם רק מכתיבים שיש לפרשה בצמצום. פרט לתיחום שהוצע לעיל, הרי האמצעים לפרשנות המצמצמת הם הקפדה על הרכיב של "שלא כדין" ועל המחשבה הפלילית הנדרשת, כמו גם אי הרשעה במקרה של זוטי דברים.⁷⁹ נוסף לכך, אני סבור שיש מקום להבחין בין חדירה לחומר מחשב שלא גרמה נזק לכזו שהזיקה. אם נגרם נזק, הרי שחומרת המעשה רבה יותר, שכן יש פגיעה גם בעקרון שלמות המידע ובזמינות המערכת. אבל חדירה כשלעצמה אינה מזיקה. היא עלולה אולי להטריד את מפעילי האתרים והמחשבים. במקרים רבים, לחדירה הלא-מזיקה דווקא יש שכר בצידה, ודווקא למפעילי האתרים, זו דרך לאתר פגמים באבטחת המידע שלהם. מובן שהם יכולים לחפש פגמי אבטחה בעצמם, אולם יכולתם לעשות כך – מוגבלת. "פורצי המחשבים" תמי הלב הם בבחינת עיניים נוספות הבוחנות את המערכת. אריק ריימונד ניסח רעיון זה

79 ראו, למשל, את החלטת האיחוד האירופי המאפשרת למדינות האיחוד לצמצם את העבירה רק למצבים בהם הופר אמצעי אבטחה Council Framework Decision on Attacks Against Information Systems (Jan. 17, 2005) <http://register.consilium.eu.int/pdf/en/04/st15/st15010.en04.pdf>

בפשטות: "given enough eyes, all bugs are shallow".⁸⁰ עדיף שמפעילי האתרים יגלו את הפגמים באמצעות חובבי מחשבים המצביעים על כשלי האבטחה, מאשר באמצעות גורמים עוינים שלא יסתפקו ב"חדירה" למחשב, אלא יפגעו בשלמות המידע, בזמינות המערכת ואולי אף יעשו במידע שימוש פלילי או חבלני.⁸¹

בהקשר זה ולהשלמת התמונה יש להעיר, שלפי הדין הישראלי מוטלת חובה על בעלי מאגרי מידע, כפי שאלה מוגדרים בחוק הגנת הפרטיות (וכן על מחזיקים ומנהלים של מאגרי מידע), לנקוט אמצעי אבטחה.⁸² המטרה היא להגן על פרטיות מושאי המידע (data subjects). התקנות הנלוות מפרטות מעט יותר, אך עדיין מותירות עמימות רבה בקשר לרמת האבטחה הנדרשת.⁸³ במילים אחרות, בעלי מאגרי מידע אינם יכולים להסתפק באמצעי אבטחה מינימליים, ואינם יכולים לבוא בטרוניה למי שחושף את דלות האמצעים שנקטו או שחדלו מלנקוט. בכך דווקא משרתת פעולת אלה החודרים לחומר מחשב את האינטרס הציבורי, כל עוד אין הם משבשים את המחשב אליו הם חודרים. למצער, נראה שלא כך פורש החוק עד כה.⁸⁴

3. שלמות המידע

עקרון אבטחת מידע זה מכונן להבטיח את אמינותו של המידע המאוחסן במערכת המחשב, או של המידע העובר בין המחשבים ברשת. מובן שבלעדי שמירה על המידע, המערכת כולה אינה אמינה ושימושיה לא יועילו ואף יזיקו. לפיכך, עקרון שלמות המידע נועד להבטיח כי המידע לא שונה על ידי מי שאינו מורשה לכך. העיקרון מתייחס למניעת סילוף חיצוני של המידע, למשל – על ידי הזנת נתונים שגויים, בין ככוונת עבריינין ובין בטעות. העיקרון מאפשר גם וידוא פעולות צדדים למשא ומתן או

- 80 ראו Eric S. Raymond *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (O'Reilly, 1999) 41.
- 81 חברות האבטחה מתגאות בחשיפת פרצות אבטחה אצל אחרים. ראו, למשל, גליה ימיני "פינג'אן זיהתה פרצת אבטחה בגוגל שאפשרה גניבת זהות משתמשים; תוקנה תוך ימים" **הארץ – The Marker**, (11.10.05) ע' 18.
- 82 סעיף 7 לחוק הגנת הפרטיות מגדיר: "אבטחת מידע" – הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כד"ן; סעיף 17 לחוק קובע אחריות לאבטחת מידע.
- 83 ראו תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986.
- 84 חוק המחשבים מספק תמריץ נוסף לבעלי מחשבים לנקוט אמצעי אבטחת מידע מפני חדירה למחשביהם. בלי נקיטת אמצעים כאלה לא יקבל בית משפט את פלטי המחשב כראיה. ראו סעיף 36 לפקודת הראיות [נוסח חדש], התשל"א-1971, שתוקן באמצעות סעיף 10 לחוק המחשבים, ודין אצל נמרוד קוזלובסקי **המחשב וההליך המשפטי – ראיות אלקטרוניות וסדרי דין** (2000) 219.

עסקה, וכך להקשות על התכשורתם לעסקה.⁸⁵ עיקרון זה נפרט לכללים בדבר אימות זהות המשתמש ובקרת הגישה (החיצונית), וגם לאמצעים טכניים כמו חתימה דיגיטלית המקודדת את המידע. כאשר המידע מגיע למחשב אחר ברשת ניתן להשוות את המידע לחתימה האלקטרונית וכך לדעת אם חלו שינויים. גם הצפנת המידע היא אמצעי להבטיח את שלמות המידע.

חוק המחשבים, כמו גם חוקים מקבילים בעולם,⁸⁶ מגן במישרין על עקרון שלמות המידע, ובעת פרשנות החוק ויישומו יש לזהות את הערך החברתי המוגן הזה. סעיף 2 אוסר את שיבוש פעולתו התקינה של המחשב או הפרעה לשימוש בו, כמו גם מחיקת חומר מחשב או שינוי בו.⁸⁷ סעיף 3 אוסר העברה או אחסון של מידע כוזב, וסעיף 6 אוסר עריכת נגיף מחשב. וירוס כזה עלול לשבש את המערכת, כמו גם את זמינותה.⁸⁸ ראוי לציין כאן גם את חוק האזנת סתר, המספק הגנה משלימה לסודיות המידע המועבר.⁸⁹ כל אלה הם אמצעים משפטיים שתכליתם להגן על עקרון השלמות של המידע.

4. זמינות המערכת

עקרון אבטחת המידע של זמינות המערכת מכוון לסכל הפרעה חיצונית לשימוש האופטימלי במשאבי המערכת הקיימים, ובכך לאפשר לבעלי המערכות ליהנות ממערכותיהם. מערכת מחשב צריכה להיות זמינה למשתמשיה המורשים. אחד האתגרים הטכנולוגיים הוא לבנות מערכת אשר למרות משאביה המוגבלים של הטכנולוגיה תוכל להיות זמינה לכל המשתמשים ולמלא את ייעודה. המגבלה המרכזית היא טכנולוגית, אולם מערכות מחשב חשופות לגורמים עוינים המבקשים לפגוע בזמינותן. במונח זה, כפי שמציינים ניסנבאום, פרידמן ופלמן, עקרון הזמינות הוא ביטוי לרעיון של שליטת האדם במערכת שלו – כלומר רעיון קנייני וביטוי לאוטונומיה של בעלי המערכת.⁹⁰ כידוע, מערכות מחשב נתונות למתקפות רבות מצד גורמים עוינים: וירוסים, סוסים טרויאניים, מתקפות סירוב-שירות (denial of service) ושאר מרעין

85 ראו לעיל הערה 38.

86 ראו, למשל, את האמנה האירופית, לעיל הערה 21, בסעיף 4.

87 בדברי ההסבר להצעת החוק נאמר שהערך המוגן הוא שלמות המידע. ראו גם דויטש, לעיל הערה 21, בע' 438.

88 ראו, למשל, ת"פ (חי') 8243/97 מדינת ישראל נ' גיל פז, דינים-שלום יב 153, שבו הורשע עובד לשעבר של רפא"ל בהחדרת וירוס למחשב הארגון.

89 חוק האזנת סתר, התשל"ט-1979, וכן ראו את דו"ח חבר העמים הבריטי, לעיל הערה 72, בע' 38.

90 Helen Nissenbaum, Batya Friedman, Edward Felten "Computer Security: Competing Conceptions" (2001), available at <http://arxiv.org/html/cs.CY/0110001>

בישין⁹¹ גם כאן, התשובה לבעיה היא במידה רבה טכנולוגית – תוכנות בקרה וסינון, שאמורות לחסום גורמים עוינים, ובדיקות חוזרות באמצעות תוכנות אנטי-וירוס למיניהן. גם כאן חוזר המבנה שראינו – המשפט מציע רובד הגנה נוסף על רובד ההגנה העצמי-טכנולוגי.

חוק המחשבים מתגייס לסייע לעקרון זמינות המערכת, בכך שהוא אוסר על עריכת נגיף מחשב או על הפצתו (סעיף 6).⁹² בתי המשפט, כך נראה, מבינים את העיקרון הזה, גם אם באופן אינטואיטיבי. כך למשל, נקט בית משפט השלום בתל-אביב לשון חריפה במיוחד נגד נאשם שהודה (והורשע) כי כתב וירוס מחשב שנועד למחוק קבצים במחשב הנגוע, והחדירו למחשבים בבסיס צבאי בו שירתה חברתו.⁹³ בגזר הדין הכביר השופט מילים כלליות על כך ש"עבירות המחשב הן עבירות של העת האחרונה, העידן המודרני", ולענייננו, "ככל שמדינה מתקדמת בשימושים בטכניקות המחשב, כך גם הסיכונים לשיבוש מערכות בעת הפגיעה בהן". אפשר להבין דברים אלה כזיהוי הערך המוגן על ידי העבירה, הפצת הווירוס פגעה בזמינות המערכת (וממילא – בשלמות המידע).

ה. הנועזים (עברייני המחשב) והאמיצים (השופטים)

כיצד מיישמים בתי המשפט את חוק המחשבים? מהי עמדתם בקשר ליחס שבין משפט לטכנולוגיה? בעשור האחרון, עיקר הניסיון השיפוטי היה בקשר לגזירת הדין, ופחות מכך בקשר להכרעתו. ברוב המקרים שבאו לפני השופטים הודו הנאשמים בביצוע העבירות, כך שהשאלה שהתעוררה הייתה האם ניתן להסתפק בעונש ללא הרשעה (כאשר המגמה הכללית היא שיש להרשיע), ובשאלת העונש עצמו. משום אופיים של גזרי דין בכלל, המעמתים את הנסיבות האישיות של הנאשמים עם האינטרס הציבורי, נחשפת שם עמדת השופטים באשר למהות החוק. בחלוף עשור לחוק, מצטיירת התמונה הכללית הבאה: עמדת בתי המשפט נוטה להיות כוללנית, ולעיתים אף

91 לדיון מפורט במתקפות אלה, ראו יעל און ואח' פרטיות בסביבה הדיגיטאלית (המרכז למשפט וטכנולוגיה, עורכים: ניבה אלקין-קורן, מיכאל בירנהק, 2005). ראו עוד את סעיף 5 לאמנה האירופית.

92 ראו, למשל, ע"פ (חי') 002864/92 מדינת ישראל נ' קטין (17.2.03), בו הורשעו מספר קטינים בעריכת וירוס המחשב goner, שגרם לנזקים רבים למערכות מחשב ברחבי העולם. לפי כתב האישום, נועד הווירוס להציף ערוצי הידברות ברשת ולהפיל תוכנות אנטי-וירוס ותוכנות הגבלת גישה (firewall). בית המשפט המחוזי הדגיש את חומרת העבירות "שנעשו בתחכום רב וגרמו לנזק כבד לאנשים תמימים". במונחי עקרונות אבטחת המידע, הנזק שנגרם כפול: נזק לזמינות המערכות ופגיעה במערכות שנועדו להשיג את שאר עקרונות האבטחה, כמו בקרת גישה וחדירה עוינת.

93 ת"פ (ת"א) 005177/99 מדינת ישראל נ' גרינברג, דינים מחוזי לבן (9) 363 (11.4.00).

שבלונית, וקשה למצוא בה אותו דיאלוג נחוץ כל כך שבין המשפט לבין הטכנולוגיה. נדמה לי שראוי לשופטים לדייק יותר בשאלה מהו בדיוק הנזק שנגרם כתוצאה מפעילות הנאשם שלפניהם. את הנזק יש לנסח לא רק במונחי נזק כספי, אם זה ניתן לכימות, אלא במונחים של הפגיעה בעקרונות אבטחת המידע, שהרי זו התכלית של חוק המחשבים. לימוד פסקי הדין מעלה שיש בהם שני נרטיבים מרכזיים. בכל אחד מהם יש מספר שחקנים – הנאשם, הטכנולוגיה, הציבור ובית המשפט, ויש ליהוק ברור בקשר לתפקידו של כל אחד. הנרטיבים מגולמים בשני פסקי דין מרכזיים – זה שדן את אהוד טננבאום, המכונה "האנלייזר", וזה שזיכה את אבי מזרחי, שבסך הכול רצה להצטרף לשורות המוסד.

1. האנלייזר הנועז

לפי כתב האישום, שבו הודה טננבאום, הוא קשר קשר עם אחרים לחדור שלא כדין למחשבים בארץ ובחול, וכך עשה, תוך שימוש בשמות משתמשים ובסיסמאות של גולשים, ללא ידיעתם. בכמה מקרים חדר למחשבי NASA, משרד ההגנה האמריקני, שינה קבצים במחשבים אלה, השתיל סוס טרויאני ותוכנות מעקב (sniffer). הוא גם חדר למחשבי אתר נשיא המדינה, אתר הכנסת ואתר של מדרשת שדה בוקר. בחלק מהמקרים שינה את דפי הבית באתרים ובעקבות זאת הושבתו האתרים לכמה ימים. לדבריו, בחלק מהמקרים תיקן חורי אבטחה, כמו באתר הכנסת.

בכל שלוש הערכאות שדנו בעניינו של טננבאום ניכר שהן נפעמו, מי יותר ומי פחות, מהחדשנות שבעבירות. אלה בוצעו בשנים 1997-1998, כתב האישום הוגש כשנתיים לאחר מכן, גזר הדין ניתן בשנת 2001, והערעור בשנת 2002. גזרי הדין ראויים לעיון מפורט.

תחילה לגזר הדין של בית משפט השלום.⁹⁴ בית המשפט העיר כי "דיני המחשבים עושים צעדים כמעט ראשוניים בכל הנוגע לאכיפת החוק ותוצאותיו". פסק הדין מדבר על "מהפכה חדשה", "עידן חדש", ועל כך ש"חדשנותו של חוק המחשבים רודפת אותו". במילים אחרות, נוכח קיומו של החוק, ברור, כי בית המשפט סבור שהטכנולוגיה והשימוש בה כפופים למשפט וניתנים להסדרה משפטית, גם אם יש בכך קושי מעשי, לנוכח קצב השינויים המהיר. בהמשך גזר הדין נכתב עוד, כי "התיאורים שמסר הנאשם לגבי האופן בו בוצעו החדירות והכלים הווירטואליים בהם השתמש לקוחים מעולם אחר". הנאשם מתואר במאפיינים שחוזרים ועולים פעמים רבות בגזרי דין אחרים שלפי חוק המחשבים. הנאשם האופייני, וטננבאום הוא אב-טיפוס של הנאשם הזה, הוא גבר, צעיר, בעל ידע במחשבים, מתוחכם מאוד. כלומר, מאפיינים של "בן טובים". כך, למשל, נכתב שם על טננבאום, שהיה כבן 18 בעת ביצוע המעשים

94 ראו ת"פ (כפר סבא) 003709/00 מדינת ישראל נ' טננבאום (14.6.01).

שיוחסו לו: "למיטב ידיעתי הנאשם הוא פורץ המחשבים הנועז ביותר שנודע עד כה. הוא לא הסתפק באתרי המחשב בגבולותיה של המדינה וחצה יבשות. הוא חדר ל'קודש הקודשים' של מדינה ידידותית" [הכוונה למחשבי הפנטגון – מ' ב']. בהמשך, מציינת השופטת את עיסוקו של טננבאום בעת המשפט – מנהל פיתוח בחברת סטארט-אפ המתמחה באבטחת מידע – ומעירה על האירוניה בקשר ל"מי שהפיל חיתתו" וכעת עבר לצד השני של המתרס. כמובן, כל אלה מתמצים בכינוי שדבק לטננבאום – בעקבות אחד הכינויים בהם השתמש – האנלייזר, שם הנשמע כלקוח היישר מתסריט הוליוודי מצוי.⁹⁵ בית המשפט מעיר עוד כי הנאשם הפך לסלבריטי. לצד תכונות חיוביות אלה, מתואר הנאשם הטיפוסי כצעיר מבולבל, כזה שסובל מקושי לתפקד בסביבה האנושית ומצא מפלט בסביבת המחשב. שם נותן הנאשם הטיפוסי דרוור ליצריו האפלים. על טננבאום נכתב, בהתבסס על איבחון פסיכולוגי שנערך ועל איבחון דידקטי שנערך כשהיה בכיתה ט', כי "הקשר שלו עם החברה היה מוגבל... בעיות אלה העצימו עם הגיל, וככל הנראה הם אלה שהביאו לקשר שלו עם עולם המחשב, כאשר הוא מבין שהוא יכול לתקשר עם אנשים ללא הגבלה". ובהמשך: "מהאמור בחוזה"ד [שהוגשה לבית המשפט – מ' ב'] ניתן להגדיר את התעסקותו עם המחשב כתחליף לתקשורת הולמת. האובססיה עם המחשב נוצרה כתוצאה מליקויים בקומוניקציה ובמעורבות הבין אישית". מול דימוי זה של עבריין המחשבים כבן סורר, ברור מה תפקידו של בית המשפט: למלא את מקום ההורה המחנך שאינו חוסך את שיבטו.⁹⁶

95 כינויים רבי עוז המעוררים דימוי של גיבורי-על נפוצים בקרב האקרים. כתב הניו-יורק טיימס מעיר כי בדרך כלל מאחורי הכינוי הנועז מסתתר לכל היותר חנון-על (super geek). ראו Matt Richtel "Nicknames on the Net Bigger Bark than Bite" *New York Times*, March 12, 2000, available at: <http://www.nytimes.com/library/review/031200hacker-handles-review.html>

96 ראו, גם, ת"פ (ת"א) 005476/03 **מדינת ישראל נ' אורן לוי** (2.3.04): "עבירות כמו אלה שביצע הנאשם הן עבירות המתבצעות על ידי עבריינים כמותו. לא מדובר בעבריינים ערלי ראש ונפוחי זרוע, לא מדובר בפוחזים ובבריוני רחוב... מדובר באנשים משכילים ואינטליגנטים שצווארונם נקי ויגיעתם מוחית ולא שרירית. עבירות באמצעות מחשב הן עבירות שנולדו וכאו לעולם בשנים האחרונות. ההתפתחות הטכנולוגית, קפיצת הדרך הנחשונת בעולם המחשבים הביאו עימם עבירות שלא הכרנו וידענו קודם לכן. מדובר בעבירות המתבצעות מחדרים ממוזגים, עבירות המרחיקות לקצווי עולם בזמנים קצרים ונשלטות בידי בודדים המפעילים את כישורונותיהם ומכמני ראשם לפיצוח וחדירה אל תוככי מגירות אישיות, קבצים נסתרים וספריות חשאיות של אנשים פרטיים, חברות ענק ומוסדות ממשלתיים... עבריינות המחשב עלולה לפגוע ולשבש מערכות חיים. עבירות המחשב עלולות לגרום נזקים לבתי חולים, שדות תעופה, מתקני בטיחות ובטחון, תוך סיכון חיי אדם, פגיעה בסביבה ובסדר הציבורי. עבירות המחשב הן עבירות נואלות וקשות. חומרתן אינה פחותה מעבירות פליליות אחרות. אדרבא, שכולן ותחכומן מקנות להן נופך חומרה...".

מול האנגלייזר הנועז, מוצגים הנפגעים, מפעילי האתרים והמחשבים שנחדרו, כחסרי אונים, שלקו ב"מבוכה ובהלה", חשו "כאילו פרצו אליך הביתה". חלקם נאלץ לסגור את האתרים למספר ימים ולזמן כוח אדם מיומן לתקן את הבעיה. בית המשפט אינו מזכיר כלל אם טרחו לנקוט אמצעי אבטחה, כיצד מנוהלים האתרים, על ידי מי וכדומה. נראה, כי מתחת לפני השטח רוחשת כאן תפישה קניינית – כאילו האתר והמחשבים המחוברים לרשת הם יחידה קניינית נפרדת. הסברתי קודם מדוע עמדה כזו אינה משקפת את ההיסטוריה החקיקתית של חוק המחשבים, ומדוע היא אינה ראויה גם כעניין נורמטיבי. כך או כך, הקצנת התיאור של שני הצדדים – הנאשם והנפגעים – היא מרכיב חשוב בסיפור השיפוטי.

עוד שני מרכיבים יש בסיפור השיפוטי: הנזק שנגרם ומקומו של בית המשפט. תחילה הנזק. יש נזקים ישירים שנגרמו לאתרים שהושבתו, ו"ברור שיש לראות בחומרה עבירות אלה שתכליתן פגיעה במערכות מחשבים. החדירות למחשבים נעשו לתופעה וככל שגוברת התלות במחשב, בעיקר במדינות מתקדמות, כך מתעצמים נזקיה בעת הפגיעה במאגרי המחשב שלה." בית המשפט נסמך גם על עמדת התביעה, שהדגישה את הנזק התדמיתי לישראל בגלל החדירה למחשבים בממשל האמריקני, והקשיים באכיפת עבירות מחשבים. נזק נוסף, תמוה משהו, שנזכר בגזר הדין, הוא כי עבירות המחשב יחייבו השקעה כספית רצינית במערכות מיגון ופיתוח תוכנה. חוששני, בכל הכבוד, שאיזכור נזק אחרון זה מעיד על חוסר הבנה של מהותן של עבירות המחשב ושל תפקידיו של המשפט ביחס לטכנולוגיה, כמו גם היחס הכללי שבין איסור פלילי לנקיטת אמצעי הגנה פרטיים, כלומר היחס שבין הסדרה ציבורית להסדרה פרטית.⁹⁷ עברייני המחשב רבים ופזורים ברחבי העולם. ברובם הם אינם כפופים לחוקי המדינה. לפיכך, ממילא יש צורך להגן על מערכות המחשב ואי אפשר לסמוך על טוב ליבם של אזרחיה הנאמנים של המדינה. כך שהשקעה במערכות אבטחה חיונית ממילא – ובעיקר כדי להבטיח את הגשמתם של עקרונות אבטחת המידע שנדונו לעיל. ההגנה הטכנולוגית היא סעד עצמי, אמצעי של הסדרה פרטית. המשפט אינו מתיימר להיות תחליף לרובד זה, אלא תוספת אליו. מפעיל מערכת מחשב הנסמך רק על האיסורים שבחוק שימנעו פריצות למחשביו, ללא נקיטת כל אמצעי זהירות נוסף, פועל, לטעמי, ברשלנות. אם יש אצלו מידע על אזרחים, הרי הדבר עולה כדי הפרה של חובת האבטחה הקבועה בחוק הגנת הפרטיות בקשר להגנת מאגרי מידע, כפי שהם מוגדרים שם.⁹⁸

וכאן, לאחר שעמדנו על "הרעים" שבסיפור, על הנזק שהם גורמים לתמימים, וכל זה בליווי אווירה דרמטית של הטכנולוגיה החדשה, מגיעה כניסתו של בית המשפט לבימה, זהו תפקיד ה-Deus ex Machina, "האל מן המכונה", שבא להתיר את סבך

97 ראו לעיל הערות 23, 34.

98 ראו סעיף 17 לחוק הגנת הפרטיות.

העלילה ולהשיב את הסדר על כנו. את זאת משיג בית המשפט בענישה. אולם, לפני כן נדרש עוד מהלך אחד, שחזור ועולה בגזרי דין רבים: בית המשפט משווה את עבירות המחשב לעבירות פריצה וגניבה. כך בית המשפט: "אני תוהה האם אותו נאשם, ששם לעצמו מטרה להיכנס לפנטגון, היה רוכש לשם כך כרטיס טיסה, שם פעמיו לשדה התעופה, מגיע לארה"ב ומנסה להיכנס. האם גם אז היה פורץ מנעולים, מפיל את המאבטח ושועט לעבר היעד?"⁹⁹ וכך מלהק בית המשפט את עצמו בדרמה שהוא גם מחברה. בית המשפט מתגייס למען הציבור, כדי לסכל את הנזקים או להשיב את המצב לקדמותו, ובעיקר, כדי להיות מגן הטכנולוגיה החדשנית. לבית המשפט תפקיד לחנך את הבן הגאון הטוב שסטה לסימטאות אפלות, ולהרגיע את אלה הנבוכים מפני החדשנות הטכנולוגית. המשפט יכול לטכנולוגיה, שהרי אין הוא נאבק בה אלא דווקא מסייע בעדה בכך שהוא מרחיק ממנה את המזיקים. ובא למחשב גואל.

במקרהו של טננבאום, שילוב התפקידים – בית המשפט כמגן הטכנולוגיה, הקידמה והציבור, וכמחנך הנער הסורר ומגן החלשים – מביא לעונש. בית משפט השלום גזר שישה חודשי עבודות שירות. בית המשפט המחוזי שדן בערעור המדינה הקצין עוד יותר את הנרטיב, כבמאי הוליוודי המזהה חומרים לסרט מצליח. בערעור בבית המשפט המחוזי נחלקו הדעות באשר לעונש, אולם יש אהידות בנרטיב שנוקטים השופטים, והוא מעצים את הנרטיב שבפי בית משפט השלום. טננבאום מוצג כמי ש"פעל בדרך חסרת מעצורים", וכמי ש"שום דבר אינו קדוש בעיניו ואינו מעבר לתחום עבורו". השופטת דבורה ברלינר ערה להילה של הנאשם – וקשה להשתחרר מהרושם שההילה נוצרה, במידה לא מועטה בזכות ההתנהלות התקשורתית של המשטרה והתביעה בעניין, וכמובן התקשורת ששמחה "להצהיב" את הסיפור. השופטת מתארת את הדימוי הציבורי של הנאשם ל"סופרמן או אולי רובין הוד מודרני", ובנשימה אחת מזכירה את גאונותו, אם כי הביטוי מופיע במירכאות – רמז לבאות. גם כאן יש שרטוט סטריאוטיפי של הנאשם כמייצג את עברייני המחשב: "דומה שהכישורים השכליים, ה'גאונות' שמוצאת ביטויה ביכולת לחדור לכל אותם מחשבים מאפילה על כל שיקול אחר, ומסנוורת את הציבור הרחב ובמיוחד, כפי שאמרת, את השכבה הטיפוסית של העבריינים הפוטנציאליים, דהיינו צעירים אינטליגנטיים ומוכשרים שדמיונם הולך שבי אחרי ההרפתקה".

ועוד, השופטת מאמצת את התווית שהציעה התביעה – "ונדליזם אלקטרוני". ביטוי זה ראוי לעיון. הוא משקף קו חשוב במבנה הנרטיב השיפוטי: עבירת המחשב כמוה כעבירות של אחרון הפושעים הבזויים. בית המשפט מבקש לנתן את הילת

99 ראו במקרים נוספים: "מדובר בעבירות שלהן השלכות הרסניות. הנאשם חדר למקומם של אזרחים תמימים, ועשה ברכושם כרכושו. אין הבדל בין פעילותו לבין פעילות עבריינים אחרים הפורצים לדירות ובתי עסק ונוהגים מנהג בעלים במקום שאליו התפרצו". – ת"פ (ת"א) 005476/03 **מדינת ישראל נ' יוסף שי** (5.1.05).

הגאונות הנכרכת סביב עברייני המחשב, ודרכו לעשות זאת היא להציגם כעבריינים פשוטים, אלימים, לא-מתוחכמים. הביטוי עצמו חדש, אינו טריוויאלי, והוא על כן בגדר "ציטטה טלוויזיונית שיפוטית" (judicial sound bite), כלומר אמירה הנקלטת היטב בתקשורת הלהוטה לכותרות מסקרנות.¹⁰⁰ לא במקרה זכה הביטוי להבלטה בדיווחים אודות גזר הדין.¹⁰¹ בהמשך פסק הדין מופיע רעיון זה במפורש: "טננבאום איננו שונה ממי שעומד בראש כנופיה הפורצת לבתייהם של אנשים".

ומה באשר לנזק? השופטת מקבלת את הנזקים שפירט בית משפט השלום, ומציגה באופן כוללני משהו את עקרון אבטחת המידע היסודי: "בעולם שבו כל הידע שנצבר, בכל תחום שהוא, כל האינפורמציה, בין האינפורמציה הקשורה לנאס"א ולמערכות חלל, ובין אינפורמציה הקשורה לחשבון הבנק או לפרטיו של כל אדם שהוא, מצויה במחשבים, הצורך הראשון במעלה הוא להגן על מאגרי המידע העצומים המצויים במחשבים". מסקנתה הייתה חדה: שנת מאסר בפועל. אולם זו הייתה העמדה המקילה. השופט זכריה כספי הוסיף תיאורים משל עצמו, כאשר הקו המרכזי דומה: צורך להרתיע את דור העתיד של המחשבים ולעקף את ההערכה לטננבאום. הצעתו הייתה לגזור שנה וחצי מאסר. שופט הערעור השלישי, השופט המר, הציע להחמיר עוד יותר: שנתיים וחצי מאסר. בית המשפט העליון דחה את בקשתו של טננבאום לרשות ערעור.¹⁰²

2. על האקרים, קראקרים ובתי המשפט

האם אהוד טננבאום גיבור? נראה (והדברים מבוססים על קריאת פסקי הדין לברדם) שטננבאום ניסה, למעשה, לכוון לדימוי אחר, זה המבחין בין ה"האקר" ל"קראקר". להאקרים דימוי עצמי שונה מזה שבו הם נתפשים ומוצגים על ידי בתי המשפט והחברה בכלל. ההאקרים רואים עצמם כחלק מאלטיה חברתית בלתי מאורגנת הנמצאת פעמים רבות מחוץ לטווח החוק, אולם הם פועלים לפי חוקים בלתי כתובים משל עצמם בקשר

100 השופט האמריקני פייר לבאל כותב "Like politicians, [judges] sense the value of sound bite. Long, complicated sentences do not play well on Main Street. Therefore, judges, including the greatest of them, gave devised quotable quips" – Pierre N. Leval, "Judicial Opinions as literature" in *Law's Stories: Narrative and Rhetoric in the Law* (Peter Brooks and Paul Gewirtz eds., 1996) 208.

101 ראו, למשל, משה ריינפלד "העליון לא התיר ל"אנלייזר לערער"; היום הוא ייכנס לכלא "הארץ" (18.06.2002); צבי הראל "עונש מאסר לא וירטואלי" **הארץ** (16.06.2002); עמי בן דוד "סטארטאפ במטרה" **מעריב** (15.06.2002); "הפרקליטות עירערה למחוזי על קולת עונשו של ה"אנלייזר" **הארץ** (14.09.2001).

102 רע"פ 5147/02 **טננבאום נ' מדינת ישראל** (טרם פורסם).

למותר ולאסור.¹⁰³ מטרתם היסודית היא לצבור מידע ולהופכו לידע.¹⁰⁴ האתיקה ההאקית כוללת אמונה מוחלטת כמעט בזרימה חופשית של מידע ללא מגבלות, בחוסר אמון מוחלט בשלטון המרכזי, ובעיקר, ההאקרים רואים עצמם חופשיים להפר חוקים שבעיניהם הם טיפשיים. ההאקר אינו פועל למטרת רווח, ועיקר סיפוקו הוא מטפיחת השכם הווירטואלית מחבריו. ההאקר המצוי אינו מתכוון להזיק, אלא ללמוד, לשחק, לבדוק ולאתגר. הוא שש אלי מערכות מחשב מתוחכמות, וככל שהאבטחה חזקה יותר – האתגר נמרץ יותר. ההאקר מבחין עצמו מהקראקר. האחרון הוא "האקר רע", שמנסה להזיק לשם הנזק. הקראקר מוציא שם רע להאקרים.¹⁰⁵

מובן שמערכת המשפט והרשויות לאכיפת החוק אינן מסוגלות להכיל ולקבל את הדימוי של ההאקר המצוי.¹⁰⁶ לשלטון ולרשויות האכיפה חשוב להציב דימוי מתחרה לדימוי העצמי של ההאקר.¹⁰⁷ אכן, נראה שבמידה רבה דימוי המצוי של ההאקר השתנה, ומהדימוי הפוחז הפך ההאקר לבריון אלקטרוני. השינוי בא על ידי סוכנים שונים, כמו רשויות האכיפה, בתי המשפט והתקשורת.¹⁰⁸ בעיני המשפט נמצאים ההאקר והקראקר באותה קבוצה. ההבדל יבוא לידי ביטוי, אולי, רק בעונש. בעיני המשפט, איש אינו נמצא מחוץ לחוק, ודאי לא כאשר המעשים נעשים במודעות

103 ראו Steven Levy **Hackers: Heroes of the Computer Revolution** (New York, 1984) 27.

104 ראו את ההגדרה שמובאת במגזין האקרים נפוץ: "Hacking encompasses all sets of things, the basic common denominator being the desire to obtain information out of something or someone in order to gain knowledge" **2600: The Hacker** 30 (2004-2005) Quarterly.

105 על הדימוי של ההאקרים, ראו Bruce Sterling **The Hacker Crackdown: Law and Disorder on the Electronic Frontier** (New York, 1992) 50-59. לניתוח מרתק של המעבר מדימוי ההאקר לדימוי הקראקר, ראו יעקב הכט "האקרים: בין טכנולוגיה לפשיעה וירטואלית", **מגזין איגוד האינטרנט הישראלי** (נובמבר 2004) נמצא ב: http://isoc.org.il/magazine/magazine5_2.html. ראו גם את ההסברים הבהירים של ויקיפדיה, בערכים "האקרים" ו"קראקרים".

106 למתח שבין ההאקרים ורשויות האכיפה, ולהתנגשות הדימויים, ראו Douglas Rushkoff **Cyberia – Life in the Trenches of Hyperspace** (New York, 1994) 208-211. לעמדת המשטרה, ראו את הערותיו של מפקד מפלג עבירות מחשב במשטרה, מאיר זוהר "ההאקר" **מראות המשטרה**, גיליון 178, נמצא ב: www.police.gov.il/persumim/kitvey_et/01_178/01_178.asp.

107 דברה האלברט טוענת כי הבניית זהות "ההאקר הרע" חיונית כדי להגדיר את היפוכו של הרע – את האזרח הישר. ראו Debra J. Halbert **Intellectual Property in the Information Age** (1999) 102-103.

108 לדיון ראו Helen Nissbenaum "Hackers and the Contested Ontology of Cyberspace" **New Media and Society** 195 (2004) 6(2).

וביורה. במובן זה, הערות השופטים, על כך שטנבאום הוא כאחרון הפושעים זבי החוטם, הן דקירה עמוקה וכואבת להאקר המצוי. זו הצהרה שיפוטית שאין כאן הילה ואין אתיקה נפרדת, לא כבוד ולא הדר, אלא רק שוליים עלובים. ההערות האלה שבגזרי הדין, יש להניח, נופלות על אוזניים ערלות, הן תסווגנה על ידי ההאקר המצוי באותה קטיגוריה של חוקים שבעיני ההאקר מותר לו להפר, חוקים שאין להם תוחלת והם בניגוד ל"חוקי הטכנולוגיה".

האם טנבאום אכן דומה לעבריין רחוב? האווירה התקשורתית שנוצרה סביב הפרשה לא הועילה לו. היא מיקדה אליה תשומת לב ציבורית, וחוששני שאין מנוס מלהסיק שבית המשפט מילא, ולא כמי שכפאו שד, תפקיד בדרמה התקשורתית. טנבאום ניסה להציג את מעשיו באור חיובי. הוא פרץ גם לאתרי פדופילים ולאחרים אנטישמיים. הוא תיקן פרצות באתר הכנסת. כוונתו, במילים אחרות, לא הייתה להזיק, אלא אפילו להועיל. טנבאום ניסה ליצור קטגוריה חברתית-תרבותית משל עצמו, ההאקר הציוני.¹⁰⁹ למעשה, בית המשפט השיב לו, אמנם בשפה משפטית ובדרך שתוארה, כי הוא אינו האקר אלא סתם קראקר.

נדמה לי שיש לבחון את מעשיו של טנבאום לאור תכליתן של העבירות הקבועות בחוק המחשבים, כפי שהצעתי לעיל, כלומר, לאור עקרונות טכנולוגיים של אבטחת מידע. במקומות בהם השתמש בשמות של גולשים תמימים ובסיסמאותיהם, הוא פגע בעקרון אימות הזהות. במקרים בהם שיבש את פעולת האתרים בליווי רכיב המחשבה הפלילית הנדרשת – הרי פגע בעקרון שלמות המידע, ובחלק מהמקרים פגע בעיקרון זמינות המערכת. בגין כל אלה היה ראוי לעונש. אולם נראה, כי מרכיב משמעותי בחומרה שייחסו השופטים למעשיו נבע מ"פריצתו" לאתרי הפנטגון ונאס"א. ברור, כי הוא לא היה מורשה להיכנס למחשבי גופים אלה, ובכך שנכנס הוא פגע בעקרון בקרת הגישה החיצונית. אלא שבלי שיבוש המערכות או פגיעה בזמינותן, כל שעשה היה לחדור לחומר מחשב. כאמור, הצעתי שעבירה זו – כאשר היא ניצבת לבדה, ללא פגיעה בשלמות מידע או בזמינות המערכת – יש לפרש בצמצום. אכן, לפי הדין הקיים, היה מקום להרשיעו בעבירה לפי סעיף 4 לחוק. אולם לא היה מקום לייחס לכך את החומרה הרבה שיוחסה לו על ידי בתי המשפט. טנבאום רכש ידע רב, יש להניח, בניסיונות הפריצה שלו. ניסוי וטעייה הם דרך לימוד מרכזית בענף זה. מתוך ידע כזה נוצרת טכנולוגיה חדשה. בדרך זו הסב את תשומת לב בעלי האתרים לדלות האמצעים שנקטו כדי לאבטח את המידע. בדרך זו אפילו שירת את האינטרס הציבורי – של הגנת הפרטיות. חברות אבטחה מתמחות באיתור פרצות אבטחה באתרים של אחרים, גם

109 טנבאום אינו לבד בקטיגוריה הזאת. קבוצות האקרים ישראלית נוהגות לפרוץ לאתרים העוינים את ישראל. ראו, למשל, ערן טל "האקרים ישראלים 'נקמו' בטורקיה השחיתו מאות אתרים" [http://www.ynet.co.il/articles/0,7340,L-3058112,00.html] (14.03.05) **ynet מחשבים** (14.03.05). (נצפה לאחרונה במאי 2005).

כאשר לא נתבקשו לעשות כן.¹¹⁰ פעולתן נתפשת כבקרה חשובה. הדבר דומה לעיתונאי החושף שחיתות ברשות שלטונית. מדוע, אם כן, להתייחס בדרך שונה למי שפעולתו דומה, ואפילו מניע כספי אין לו? ככל שהעונש שהוטל עליו היה גם בגין מעשים אלה, של "חדירה נטו" ללא נזקים נלווים, נדמה לי שבתי המשפט החמירו יתר על המידה.

3. "באין תחבולות יפול עם ותשועה ברוב יועץ"¹¹¹

אבי מזרחי התעניין באפשרות להצטרף למוסד. הוא גלש לאתר הבית של המוסד, אשר כלל בשעתו רק שאלון למועמדים, ותו לא. מזרחי, כך מדווח בפסק הדין שדן בעניינו, תהה על סדרי האבטחה של האתר, חשדנות אשר נדמה לי שהיא במקומה ממי שמבקש להצטרף לארגון ביון חשאי. מזרחי לא התעצל ומצא באינטרנט תוכנה הבודקת את אבטחתם של אתרים, פעולה המכונה port scanning, כלומר, בדיקה אם יש "פתחים" דרכם ניתן "להיכנס" לתוכנה. הוא הפעיל את התוכנה וקיבל פלט בקשר לאבטחה של אתר המוסד. מזרחי לא הבין את הפלט, תהה על כך בפורומים אחרים, לא נענה, ובכך תמה הבדיקה מבחינתו. לא כך סברו במוסד, שלא אהבו, בלשון המעטה, את הבדיקה שערך מזרחי. הוא הועמד לדין באשמת ניסיון חדירה לחומר מחשב. כאמור, בית המשפט זיכה אותו.¹¹² העמדתו לדין של מזרחי תמוהה בעיניי, ונדמה שאת הסיפור כולו יש להבין ברוח טענתה של ההגנה, כפי שהיא מובאת בהכרעת הדין המפורטת מאוד של השופט אבי טננבאום: "רצה מאן דהוא להפגין שרירים ולהראות כי עם ישראל חי וכל המתעסק עם המוסד מרה תהיה אחריתו, ונפל הפור על הנאשם דווקא...". התביעה השיבה כי החליטה לתבוע דווקא משום שהנאשם ישראלי, קל היה לאתרו ומשום שמדובר באתר ביטחוני.¹¹³

הנרטיב המקופל בהכרעת הדין שונה מאוד, עד כדי היפוך, מגזר הדין והערעור בעניין **טננבאום**. ההשוואה אינה בין הנסיבות – אלה ודאי היו שונות. בעניין **טננבאום** דובר בגזר דין, לאחר הסדר טיעון. כאן מדובר בהכרעת דין. בעניין **טננבאום** דובר גם במעשים אקטיביים שבוצעו, כמו שינוי אתרים. בעניין **מזרחי** מדובר רק בבדיקה. עם זאת, נדמה לי שאפשר להשוות את הנרטיב הכללי. הנאשם אינו מתואר כצעיר מבולבול ססר מדרך הטוב, אלא כאזרח תמים שהתעניין בהצטרפות למוסד – פעולה שהיא ציונית לעילא ולעילא, במרכז החברה ולא בשוליה. מזרחי מוצג, בניגוד להאקר המצוי, כמי שאינו מבין דבר במחשבים ובאבטחת מידע.¹¹⁴ בדיקת האבטחה של האתר, מבהיר

110 ראו לעיל הערה 81.

111 משלי, יא, יד. זו הסיסמה שאימץ לעצמו המוסד למודיעין ולתפקידים מיוחדים. ראו <http://www.mohr.gov.il>

112 ת"פ (י-ם) 003047/03 מדינת ישראל נ' מזרחי (29.2.04).

113 שם, בפסקאות 109-110.

114 שם, בפסקאות 93, 104.

השופט, אינה בהכרח חלק מפריצה למחשב. לעיתים, הבדיקה היא שלב מקדים, הכנה לפריצה, אולם הבדיקה כשלעצמה אינה בגדר חדירה או ניסיון לחדירה כזו. כלומר, בספור השיפוטי שמתווה בית המשפט בעניין **מזרחי** אין "רעים". גם נזק אין, להיפך. בבדיקת אבטחתם של אתרים, כותב השופט, יש תועלת חברתית. הטעם הוא שהדבר יהיה תמריץ לאחראים על אבטחת המחשבים לפעול לתיקון חורי האבטחה.¹¹⁵ עמדה זו נסמכת על הבנת האינטרנט כרשת מחשבים: אין זה מקום שבו כל מחשב בודד ישכון, אלא המחשבים מחוברים זה לזה. לפיכך, עוצמתה – או חולשתה – של הרשת תלויה בקשר שבין המחשבים: "שרת שאינו מאובטח כיאות מהווה סיכון לשרתים אחרים מאובטחים", ומכאן מסיק השופט: "כל המשתמשים באינטרנט תלויים זה בזה וערבים זה לזה".¹¹⁶ במילים אחרות, במקום התפישה הקניינית הרוחשת מתחת לפני השטח בעניין **טנבאום**, או אצל אלה המצדדים בהכרה בעוולה של הסגת גבול במיטלטלין או עוולה של חדירה שלא כדין לחומר מחשב, יש בהכרעת הדין תפישה של רשת שמרכיביה קשורים ותלויים זה בזה.¹¹⁷

גם האווירה הדרמטית שמלווה את פסקי הדין בעניין **טנבאום** אינה כאן. במקומה ישנה ראייה מפוכחת וניסיון שיפוטי כן ומוצלח להתמודד עם הטכנולוגיה. פסק הדין ער, באופן יוצא דופן, להשפעת המטפורות על החשיבה השיפוטית. בפסק הדין מנהל השופט את הדיאלוג הנחוץ כל כך שבין המשפט לטכנולוגיה. אין כאן החלה חד-צדדית של כלל משפטי קיים על הטכנולוגיה, אלא פרשנות הנסמכת על לימוד זהיר של מערכות המחשב, של הטכנולוגיה שביסודן ושל המשמעות הערכית של הטכנולוגיה. מסקנתו של השופט נסמכת, לפחות באופן אינטואיטיבי, על זיהוי הערך המוגן על ידי העבירות שבחוק המחשבים עם עקרונות אבטחת המידע. פעולתו של מזרחי נתפשה והוצגה בעיני בית המשפט ככזו שבאה דווקא להגן על עקרונות האבטחה: לא לפרוץ הוא בא, אלא לבחון ולבדוק. הבדיקה – כאשר אין היא מלווה בניסיון פריצה – אינה פסולה. להיפך. ההערה השיפוטית שבעניין **טנבאום**, כאילו האקרים גורמים להוצאות מיותרות על אבטחת מידע, מתנפצת כאן לרסיסים.¹¹⁸ ההאקר (להבדיל מהקראקר), ובמקרה **מזרחי** – "הטרומ-האקר הזוטר" – אינו מזיק, אינו גורם להוצאות, אלא להיפך, הוא מסייע באבטחה.

נראה שהנרטיב השונה משקף גם תפישה שונה של אבטחת מידע. בעוד שבעניין **טנבאום** תפישת האבטחה של בית המשפט היא של ביטחון בדרך עמימות (security) by (obscurity) הרי שתפישת הביטחון של בית המשפט בעניין **מזרחי** היא של ביטחון בדרך

115 שם, בפיסקה 72.

116 שם, בפיסקאות 77, 80, בהתאמה.

117 ראו לעיל חלק ד.2.ב.

118 ראו והשוו לעיל טקסט להערה 97.

של שקיפות (security by openness). לפי תפישת האבטחה בדרך של עמימות, מושגת האבטחה על ידי הסתרת כשלי אבטחה, כדי להקשות על התוקפים הפוטנציאליים למצוא אותם.¹¹⁹ עמדה זו משלימה עם קיומם של פגמים שונים, למשל דרכים בהן ניתן לחדור למערכת המחשב, לשבשה, להפעילה כדי לפגוע במחשבים אחרים וכדומה, אולם מניחה שהתוקפים לא יצליחו לאתר את הפגמים. לפיכך, אין לבעלי מערכת כזו עניין לפרסם את דבר קיומם של פגמים וכשלי אבטחה. תפישת האבטחה הנגדית, של ביטחון בדרך של שקיפות, כופרת בעמדה הקודמת. לפי מצדדי השקיפות, הרי העמדה של אבטחה על ידי עמימות צפויה להיכשל. כשלי האבטחה סופם להיחשף, ואז הנזק שייגרם רב מאוד, מה גם שהשגת העמימות עצמה כרוכה בהשקעת משאבים לא מועטה. מנגד, מצדדי השקיפות סבורים שחשיפת הפגמים, ובעיקר בדרך של חשיפת קוד התוכנה, תאפשר בקרה של רבים גם מחוץ לארגון בו מדובר. ככל שעניינם רבות יותר יביטו, יבחנו ויבדקו את המערכת, ייחשפו הפגמים והכשלים יתוקנו מהר יותר. בין שתי העמדות ניטש ויכוח עז, והוא משקף במידה רבה עמדות יריבות בהקשר אחר – היקף ההגנה הקניינית הראויה לתוכנות מחשב. עמדת העמימות מתיישבת עם תפישה קניינית, לפיה תוכנות מוגנות דיני זכויות יוצרים בדרך שמאפשרת לבעליה שליטה מלאה. עמדה כזו משמעה "קוד סגור", כלומר תוכנה שניתן להשתמש בה, אולם לא לראות את קוד המקור שלה. מנגד, העמדה של שקיפות נסמכת על "קוד פתוח". לפיה, ראוי שתוכנות מחשב יהיו נגישות לכל ושכל המעוניינת תוכל לראות, ללמוד ולהשתמש ברעיונות המגולמים בתוכנה. לשקיפות הקוד נלווית, יד ביד, תפישת אבטחה של שקיפות.

המסקנה של הכרעת הדין בעניין **מזרחי** נכונה. היא אפשרית רק בתוך מסגרת חשיבה שערה למורכבות היחס שבין משפט לטכנולוגיה, בשילוב הערכים שמנחים את שני הקודקודים האלה. מסקנת השופט בדבר זיכויו של מזרחי אך מתבקשת.¹²⁰

ו. סיכום

במאמר זה טענתי שאת חוק המחשבים יש לפרש על רקע עקרונות אבטחת המידע המקובלים אצל מפעילי מערכות מידע, כלומר, לפי עקרונות טכנולוגיים. הטענה הזו נסמכת על עמדה כוללת יותר, של דיני מידע, בדבר הקשר המורכב שבין משפט לטכנולוגיה. הקשר הזה אינו חד-צדדי, אלא הוא קשר דיאלקטי. המשפט והטכנולוגיה אינם זרים זה לזה, אינם עוינים זה לזה; הם יכולים וצריכים לשתף פעולה, והכול לפי

119 ראו ההגדרה בויקיפדיה.

120 הערעור על הכרעת הדין נדחה מהטעם שמעשיו של מזרחי היו בגדר "הכנה גרידא" וכי לא היה למזרחי היסוד הנפשי הנדרש. ראו ע"פ (י-ם) 008333/04 **מדינת ישראל נ' מזרחי** (22.8.04).

ערכיה של החברה שבה אנו פועלים. הדיאלוג הזה צריך להתנהל תוך תשומת לב לטכנולוגיה, לאפשרויות ולקשיים הגלומים בה, תוך עירנות לקשיי אכיפה אפשריים ולתגובה הטכנולוגית האפשרית.

מתוך העמדה העקרונית הכללית הזו בחנתי את העבירות שבחוק המחשבים והראיתי כיצד הן מגינות על עקרונות אבטחת מידע שונים. הדיון העלה גם כמה מסקנות פרשניות, בעיקר בקשר לפרשנות מצמצמת של העבירה של "חדירה שלא כדין לחומר מחשב", ולדחיית הטענה בדבר הרחבת האיסור גם לתחום האזרחי.

בעשור החולף נתקלו בתי המשפט בחוק המחשבים בכמה מקרים. הניסיון מעלה שני נרטיבים מרכזיים שנוצרו בפסיקה: זה המיוצג בעניין **טננבאום** ("האנלייזר"), ובו מלהק בית המשפט את עצמו כגיבור שנועד להציל את החברה ואת הטכנולוגיה ולהגן עליה מפני נערים שסרחו, ושאותם יש להחזיר לדרך המוטב. הנרטיב השני מיוצג בעניין **מזרחי**, ובו מלהק עצמו בית המשפט בתפקיד מורכב יותר, שבלוני פחות, של תומך במערך האבטחה של רשת מערכות המידע. הנרטיב הראשון, המיוצג בעניין **טננבאום**, מתלהם יתר על המידה, ומחטיא את הדו-שיח הראוי שבין המשפט לטכנולוגיה. הנרטיב השני, שבעניין **מזרחי**, טוב בהרבה. הוא מפוכח, זהיר ומעמיק בהבנת הקשר הזה. הוא גם מגלם תפישה עדכנית וטובה יותר של אבטחת מידע. הדרך הראויה ליצור את משפט המכונה אינה ליהוק של בית המשפט כ"אל מן המכונה", אלא כבן-שיח של המכונה.

שערי משפט ד(2) התשס"ו

מיכאל בירנהק