פרק ב

חלופות לאכיפה הפלילית המדינתית במרחב הסייבר

א. הקדמה

אחד מתפקידיה המסורתיים של המדינה הוא לנהל חקירות פליליות, לאסוף ראיות מספיקות להעמדה לדין, לשפוט, ובמקרה של הרשעה אף להעניש את הנאשמים. אחת הטענות המקובלות באשר ליחס שבין המשפט למרחב הסייבר הוא כי מעמדה של המדינה משתנה באינטרנט, וכי יכולתה לאכוף את הדין הפלילי ברשת נחלשת. גם מעמדה של המדינה כשחקן המרכזי בזירה של הסדר החברתי־מדיני הבין־לאומי נחלש. בעקבות זאת מתפתח דיון עשיר, נורמטיבי,[1] משפטי־פורמלי[2] וסוציולוגי[3] בדבר המשך אחריותה של המדינה לחקירה הפלילית. מהלך

---

1 ג׳ואל ריידנברג (Reidenberg) וג׳ק גולדסמית׳ (Goldsmith) וטים וו (Wu) הביעו עמדות נורמטיביות כי אל לה למדינה להפר את חובותיה להגן על תושביה גם כשמדובר בעבירות במרחב הממוחשב, וכי על המדינה לנסות ״לכבוש״ את האינטרנט ולהחזיר את שלטון החוק אליו. ראו Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. Pa. L. Rev. 1951 (2005); Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World 156 (2006). לעומתם, ניתן לציין את עמדתו של הפובליציסט ג׳ון פרי בארלו (Barlow) שלפיה האינטרנט צריך להיות משוחרר מכבלי האכיפה המדינתית או מכל אכיפה אחרת בעלת סממנים של כפיית ציות. ראו John P. Barlow, *A Declaration of the Independence of Cyberspace* (9.2.1996) http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration. עוד על העמדה האנטי־מדינתית, ראו הסקירה אצל Goldsmith & Wu, לעיל, בעמ׳ 13–27. ראו עוד את עמדתה של השופטת מיכל אגמון־גונן כפי שהובעה בשני פסקי דין מפורטים שנתנה בבית המשפט המחוזי בתל־אביב – האחד בנושא זכויות משדרים בטלוויזיה לעומת משדר באינטרנט, והשני בנושא לשון הרע באינטרנט – שבו היא צידדה בצמצום המעורבות המדינתית באינטרנט והגברת ההסדרה העצמית. ראו (בהתאמה) ה״פ (מחוזי ת״א) 541/07 **סבו נ׳ ידיעות אינטרנט (שותפות רשומה)**, בפס׳ 6–7 (פורסם בנבו, 11.11.2007); בש״א (מחוזי ת״א) 11646/08 **The Football Association Premier League Ltd. נ׳ פלוני**, בפס׳ 3 (פורסם בנבו, 2.9.2009). ראו גם מיכל אגמון־גונן ״האינטרנט כעיר מקלט?! הסדרה משפטית לאור אפשרויות העקיפה הטכנולוגיות וגלובליות הרשת״ **רשת משפטית: משפט וטכנולוגיות מידע** 207, 213–218, 221–227, 234–235 (ניבה אלקין־קורן ומיכאל בירנהק עורכים, 2011).

2 כך, למשל, ג׳ון דלקורט (Delacourt) הביע עמדה שלפיה המדינה תאבד מכוחה באינטרנט, כיוון שהדין אינו מאפשר לה לפתור את הסוגיות המתעוררות באינטרנט. לשיטתו, יש לראות בזירה האינטרנטית זירה בין־לאומית, וכך גם במודל האכיפה. ראו John T. Delacourt, *The International Impact of Internet Regulation*, 38 Harv. Int’l L.J. 207 (1997). לכתיבה נוספת ברוח זו ראו גם Gus Hosein, *International Co-operation as a Promise and a Threat*, *in* Cybercrime and Jurisdiction: A Global Survey 23 (Bert-Jaap Koops & Susan W. Brenner eds., 2008); Tonya L. Putnam & David D. Elliott, *International Responses to Cybercrime*, *in* The Transnational Dimension of Cyber Crime and Terrorism 35 (Abraham D. Sofaer & Seymour E. Goodman eds., 2001). לעומתם, ראו למשל את מיכאל בירנהק וניבה אלקין־קורן, אשר הציגו תיאור מצב עובדתי שלפיו האינטרנט עבר שינוי מהותי בין העשור הראשון לקיומו בשימוש הכלל לבין העשור השני לקיומו כאמור. העשור השני (החופף לעשור הראשון של המאה העשרים ואחת) מתאפיין ב״קאמבק״ של

nevo.co.il

הטיעון המרכזי של החוקרים בנושא האכיפה הפלילית במרחב המקוון הוא בדרך כלל כדלקמן: **ראשית**, הנחת מוצא שהמדינה אחראית לאכיפה הפלילית; **שנית**, תיאור השפעתו השלילית של המרחב המקוון על יכולת האכיפה הפלילית המדינתית; **שלישית**, הצגת חלופה לאכיפה הפלילית המדינתית במרחב המקוון. בפרק זה אציע מהלך טיעון מעט שונה, הניתן לתיאור כך: **ראשית** אעמוד על מקורותיה של אותה הנחת מוצא בדבר אחריותה של המדינה לחקירה הפלילית במרחב המקוון; **שנית** אציג טעמים ארכיטקטוניים־טכנולוגיים, משפטיים ומוסדיים להיווצרות קשיים ייחודיים לחקירה פלילית במרחב המקוון על בסיס המודל המדינתי הקיים; **שלישית** אעמוד על החלופות השונות לאכיפה הפלילית המדינתית תוך מיונן לשתי קבוצות: קבוצת החלופות לאכיפה הפלילית וקבוצת החלופות לאכיפה מטעם המדינה; **רביעית** אראה כי כל החלופות המוצעות אין ביכולתן להפחית את הפשיעה במרחב המקוון הפחתה ניכרת, ודאי לא כשהן עומדות לעצמן, בלא שהנטל המרכזי נותר באחריות המדינה על דרך של אכיפה פלילית. בהמשך, בפרקים ג ו־ד, אחזור אל המודל המדינתי לאכיפה פלילית במרחב המקוון, אפשיט את הדין הנוהג בעניינו מקליפתו החיצונית ואזהה את התפישות, השגויות לטעמי, שבבסיסו. תחתן אציע לשמר את מודל האכיפה הפלילית הקלאסית, שבאחריות המדינה, תוך עריכת שינוי תפישתי באשר לדיני איסוף הראיות במרחב המקוון.

ב. על תפקיד המדינה בביצוע חקירות פליליות

החקירה הפלילית מבוססת על שתי נקודות מוצא, ועליהן אבקש להרחיב להלן: **האחת**, האחריות הכוללת לביצוע החקירה הפלילית היא על המדינה; **השנייה**, החקירה הפלילית נערכת, על פי רוב, בדיעבד, לאחר ביצוע העברה. אפרט על שני יסודות אלה:

המדינה באינטרנט תוך ניסיונות לגייס את ספקיות השירות באינטרנט בפרט והסקטור הפרטי בכלל, ככל שאלה נמצאים בטריטוריה שלה, לטובתה. ראו Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003). עוד ראו לעניין זה Goldsmith & Wu, לעיל, בעמ' 49–85.

3 הכותבים הסכימו כולם שהסדר החברתי המדינתי מתערער באינטרנט, אך נחלקו בדעותיהם בדבר חליפיו. ניקולאס נגרופונטי (Negroponte) חזה בספרו תהליך, כמעט דטרמיניסטי לשיטתו, של מעבר ליחידניות (singularity) בעידן הדיגיטלי: הכוונה לתהליך שבו הפרט יהפוך ל"שחקן" המרכזי בזירה הבין־לאומית, ואילו המדינה תאבד מכוחה ומחשיבותה. ראו ניקולאס נגרופונטי **להיות דיגיטלי** (תרגום עמנואל לוטם, 1996). אסתר דייסון (Dyson), היו"ר הראשונה של ארגון ICANN (Internet Corporation for Assigned Names and Numbers), חזתה כי המדינה תאבד מכוחה לטובת האינטרנט עצמו, שיהפוך לאוטונומיה הסדרתית משל עצמה. ראו ESTHER DYSON, RELAESE 2.0: A DESIGN FOR LIVING IN THE DIGITAL AGE 105–106 (1997). עמדה אחרת, שהביע הווארד ריינגולד (Rheingold) ואחרים, גורסת כי באינטרנט עולה כוחן של הקהילות כ"שחקנים" משמעותיים שיכולים אף להפעיל סנקציות ואכיפה בקרבן. ראו HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY (1993). כן ראו Note, *Communities Virtual and Real: Social and Political Dynamics of Law in Cyberspace*, 112 HARV. L. REV. 1586 (1999); Yuval Karniel & Haim Wismonsky, *Pornography, Community and the Internet – Freedom of Speech and Obscenity on the Internet*, 30 RUTGERS COMP. & TECH. L. J. 105, 124–145 (2004).

nevo.co.il

1. אחריות המדינה לחקירה הפלילית

המדינה המודרנית צמחה מתוך הסדר הפאודלי ששרר במערב אירופה בימי הביניים. בתחילת המאה ה־17 פרצה "מלחמת 30 השנה", שהחלה כעימות דתי בין קתולים לבין פרוטסטנטים וסחפה את מרבית אירופה. המלחמה הסתיימה ב־1648 עם חתימת שתי אמנות שהן "הסכמי שלום וסטפליה" (The Peace of Westphalia). בהסכמים אלה נקבע עיקרון שכל מדינה יכולה לבחור לעצמה את דתה בלי התערבות של גורמים חיצוניים. כן נקבעו גבולות מדיניים בין משתתפות מלחמת 30 השנה. קודם להסכמי שלום וסטפליה נחשבה אירופה הנוצרית לחלק מהרפובליקה הנוצרית (Respublica Christiana), שבה לא הייתה סמכות עליונה בטריטוריה, והנצרות היא שנועדה לאחד את כל האנשים. המשפט הטבעי (בגרסתו הנוצרית) משל. הכנסייה הייתה הסמכות – מבחינה דתית, כמובן, אך גם מבחינה פוליטית.[4] השיטה הווסטפלית, המבוססת על הסכמי שלום וסטפליה, כללה חמישה יסודות:[5] **האחד**, האנושות מאורגנת לטריטוריות מוגדרות שבתוכן מתנהל ארגון פוליטי המכונה "מדינת הלאום" (Nation State); **השני**, בטריטוריות מוגדרות אלה המדינות הן בעלות הסמכות העליונה והבלעדית כלפי תושביהן; **השלישי**, המדינות אוטונומיות בפעולותיהן הפוליטיות, החברתיות והכלכליות המתנהלות בתוך גבולותיהן, תוך שמירה על הפרדה בין הספרה הפנימית של המדינות לבין העולם שמחוץ לגבולותיהן; **הרביעי**, המדינות הן השחקניות השולטות בזירה הבין־לאומית, משום שהן שולטות בטריטוריה שלהן ובמקורות הטבעיים, הכלכליים והאנושיים שבהן; **החמישי**, המדינות צריכות לדאוג לענייניהן הפנימיים ולהבטיח ביטחון לתושביהן הן כלפי פנים והן כלפי חוץ.

בשנת 1933 נחתמה אמנת מונטווידאו, שבה עוגנו זכויותיהן וחובותיהן של המדינות.[6] אמנה זו עיגנה את חמשת היסודות של השיטה הווסטפלית, והוסף יסוד שישי, שלפיו קיומה הפוליטי של מדינה אינו תלוי בהכרה מצד המדינות האחרות.

סמכויות איסוף הראיות בידי המדינה, שהן במוקד דיוננו, הן חלק מסמכויות החקירה הפלילית. סמכויות החקירה הפלילית הן חלק מסמכות השיטור. סמכות השיטור נועדה להבטיח ביטחון לאזרחים כלפי פנים, ואילו סמכויות הצבא נועדו להבטיח ביטחון לאזרחים כלפי חוץ. סמכות השיטור נגזרת מהיסוד השני לעיל של השיטה הווסטפלית. סמכות השיטור היא כה יסודית עד שהיא בבחינת אחד המאפיינים המגדירים מדינה.[7] סמכות החקירה, שנגזרת מסמכות השיטור, נתפשת כיום כחלק מהסמכויות המכוננות של המדינה המנהלית, בבחינת אחד המאפיינים לקיומה של מדינה.[8] הגם שסמכות השיטור היא של המדינה, אין זה ברור מאליו

---

4 ראו Daniel Philpott, Revolutions in Sovereignty: How Ideas Shaped Modern International Relations 76–79 (2001).

5 ראו David Held, A GLobalizing World? Culture, Economics, Politics 133 (2004).

6 ראו Montevideo Convention on Rights and Duties of States, 165 L.N.T.S 19 (1933). האמנה נתפשת כחלק מהמשפט הבין־לאומי המנהגי, ומכאן שאינה מחייבת רק את המדינות החתומות עליה (מדינות אמריקה הצפונית והדרומית) אלא את כל מדינות העולם. ראו רובי סיבל "המדינה" **משפט בינלאומי** 77 (רובי סיבל עורך, מהדורה שנייה, 2010).

7 Martin van Creveld, The Rise and Decline of the State 169 (1999).

8 ראו למשל יצחק זמיר **הסמכות המנהלית** כרך א 237–239, 295–300 (מהדורה שנייה מורחבת, 2010). זמיר מונה את תפקידיה וסמכויותיה של המדינה המנהלית: שירותים, מענקים, רישיונות, מסים,

nevo.co.il

שבפועל סמכות זו מרוכזת ומופעלת בידי המדינה במקום בידי גורמים פרטיים.[9] העברת כוחות השיטור לידי המדינה היא חלק מתהליך היסטורי של מונופוליזציה של השימוש בכוח בידי המדינה. המונופול על השימוש בכוח נחשב גם הוא לאחד ממאפייניה של המדינה.[10] לפי תהליך זה, בתחילה הפך הצבא למדינתי במקום מיליציוני־פרטי בשירות המדינה, ולאחריו הפך השיטור אף הוא למדינתי.[11] ניתן להסביר תהליך זה בהתמקצעות הצבא והשיטור וכן בהתפתחויות הטכנולוגיות ששינו את פני המלחמה (אבק השרפה, כלי נשק מתוחכמים יותר ויותר) והגבירו הן את עצמת הסיכון מכוחות זרים והן את הצורך בנאמנות מוחלטת של כוחות הצבא והשיטור לסמכות הריבונית.

מקובל לטעון כי המשטרה המודרנית, ששוטריה כולם עובדי מדינה המאורגנים בהיירכייה מסודרת ושכולם מאומנים למקצוע השיטור, נולדה באנגליה עם חקיקת ה־Metropolitan Police Act בשנת 1829.[12] חוק זה ייסד את משטרת לונדון, שמומנה בכספי משלם המסים והוכפפה ל־Home office הבריטי. החוק כלל את העקרונות האלה: המשטרה היא כוח נפרד ועצמאי, המאורגן באופן מעין־צבאי שבו היירכייה ומדים, ושוטריו מועסקים במשרה מלאה ללא יכולת להשתכרות נוספת בעיסוקים פרטיים. מודל זה חלחל במהלך העשורים הבאים למדינות אירופה השונות ולארצות הברית והשלים התפשטות בעולם המערבי עד סוף המאה התשע־עשרה.[13] משימות המשטרה המודרנית התרכזו תחילה בסיור ובשיטור קהילתי, ובהדרגה חל המעבר לאכיפה פלילית.[14] הנה כי כן, השיטור המודרני הוא תופעה מוסדית־חברתית חדשה יחסית.

עד כה תיארתי את התפתחות סמכות השיטור, כסמכות המשויכת למדינה ומופעלת על ידיה, בפרספקטיבה היסטורית. מבחינה משפטית ניתן להסביר את ייחודה של סמכות החקירה (והשיטור בכלל) למדינה משני כיוונים: האחד, מכיוון של **חובתה** של המדינה כלפי אזרחיה במסגרת חובתה לשמור על ביטחון הפנים;[15] השני, מכיוון **זכותם** של האזרחים שהחקירה

הפקעות, פיקוח, צווים, חקירות וחוזים. זמיר חילק את סמכויות החקירה לשני סוגים: **האחד**, סמכויות חקירה שהן בבחינת עזר לסמכות ראשית אחרת; **השני**, סמכויות חקירה שהן הסמכות הראשית. במקרה כזה אין רשות מנהלית מבצעת את החקירה כשלב מוקדם לצורך הפעלת סמכות מסוימת בידי אותה רשות, כגון מתן רישיון, אלא רשות אחרת, שאפשר לקרוא לה רשות חוקרת, מבצעת אותה לצורך קביעת עובדות כמטרה בפני עצמה.

9 ראו Van Creveld, לעיל ה"ש 7, בעמ' 173. ואן־קרפלד תיאר כי בעידן הפרה־וסטפלי הריבון נעזר בגופים פרטיים על מנת להשליט סדר בטריטוריה שלו.

10 הסוציולוג והפילוסוף מקס ובר (Weber) קבע כי: "...we have to say that a state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory". ראו Max Weber, *Politics as Vocation*, *in* From Max Weber: Essays in Sociology 77, 78 (H. H. Gerth & C. Wright Mills translators and eds., 1947).

11 ראו יהודה אלירם **משטרה וחברה – מבוא למדעי המשטרה** 42–61 (1996).

12 Metropolitan Police Act, 1928, c. 44 (Eng.).

13 ראו Nimrod Kozlovski, *A Paradigm Shift in Online Policing – Designing Accountable Policing* 120 (J.S.D. Dissertation, 2005).

14 ראו Kozlovski, שם.

15 ראו סעיף 3 לפקודת המשטרה [נוסח חדש], התשל"א–1971, המטיל על משטרת ישראל את התפקידים האלה: "משטרת ישראל תעסוק במניעת עבירות ובגילוין, בתפיסת עבריינים ובתביעתם לדין, בשמירתם הבטוחה של אסירים, ובקיום הסדר הציבורי ובטחון הנפש והרכוש". בית המשפט העליון הדגיש כי מדובר בחובה של המדינה, אשר לא ראוי שתופרט: בג"ץ 39/82 **הנפלינג נ' ראש עיריית אשדוד**, פ"ד

nevo.co.il

הפלילית, שנועדה לפגוע בזכויותיהם, תתייחד למדינה ולא לגוף פרטי, אשר בסיס הלגיטימיות שלו מוטל בספק.[16] סמכות השיטור, ובכללה סמכויות איסוף הראיות במסגרת חקירה פלילית, יש בה הפעלת כוח, במובן של ביצוע פעולות הפוגעות פגיעה ניכרת בזכויות יסוד מוגנות של אזרחי המדינה ולעתים אף במובן של הפעלת כוח פיזי של ממש.[17] מכאן שחובתה של המדינה היא להפעיל סמכויות אלה במידתיות ולתכלית ראויה.

סמכות השיטור (במרחב הפיזי) ניתנת לאפיון מבחינה מוסדית על פי הקריטריונים האלה:[18] **האחד**, מדובר בשיטור טריטוריאלי, בגבולות המדינה, גם אם סמכות השיפוט של המדינה יכולה לחול על עברות מסוימות שנעברו מחוץ לטריטוריה;[19] **השני**, כוחות השיטור מאורגנים במבנה היירכי, הדומה למבנה הצבאי, כשלכוחות יש פיקוד מרכזי עליון; **השלישי**, ככלל יבצעו את השיטור עובדי מדינה הנאמנים בלעדית למשימתם זו. יש למעט בהפרטה של פעולות השיטור; **הרביעי**, כפועל יוצא מהאפיון השלישי, ולצורך השלמתו, קיים איסור על שימוש בכוח בידי גופים פרטיים שאינם מכוחות השיטור, למעט בנסיבות מצומצמות של הגנה עצמית, צורך או צידוק.

2. החקירה הפלילית נערכת בדיעבד, לאחר ביצוע העברה

החקירה הפלילית נועדה לאתר את מבצע העברה או לחשוף את דבר קיומה של העברה לאחר מעשה ולספק ראיות מספיקות לצורך העמדה לדין, ומאוחר יותר – אם מושגת הרשעה – לצורך ענישת העבריין. בכוחה של החקירה הפלילית להרתיע את העבריינים בכוח, בהנחה שהם

לו(2) 537, 541 (1982); בג"ץ 5009/97 **חברת מולטימדיה בע"מ נ' משטרת ישראל**, פ"ד נב(3) 679, 692 (1998); ע"פ 4855/02 **מדינת ישראל נ' בורוביץ**, פ"ד נט(6) 776, 833 (2005).

16 וכך, ניתן לתאר את ייחוד סמכות השיטור למדינה בלבד כנגזר מתאוריות של אמנה חברתית. בהקשר זה יש לציין כי טליה פישר ניתחה את ההצדקות הרעיוניות לייחוד פונקציית האכיפה, כמו גם את פונקציית החקיקה והשפיטה, למדינה. לטענתה, תאוריות האמנה החברתית, מבתי היוצר של תומס הובס (Hobbes) ושל ג'ון לוק (Locke), אמנם מצדיקות את עצם התערבות המדינה במשפט ובאכיפה, אולם הן אינן מצדיקות את היותה של התערבות זו מונופוליסטית. פישר קושרת את טיעונה בהתפתחויות הטכנולוגיות, ובהן האינטרנט, שיצרו תופעות של גלובליזציה מחד גיסא והתפוררות הסדר החברתי בתוך המדינה מאידך גיסא. ראו טליה פישר "הפרטת המשפט" **עיוני משפט** ל 517 (2008). לא ארחיב עוד בכיוון זה, שכן בהקשרנו הנדון הטיעון שלי מבקש להתמקד בתיאור המצב הקיים, שלפיו המדינה אחראית לחקירה הפלילית, ובתיאור הכשלים המעשיים במצב הקיים, כשלים הנובעים מהתפתחות הזירה האינטרנטית.

17 הכוונה היא להפעלת כוח כלפי אדם במסגרת החקירה או להפעלת כוח כלפי רכוש במסגרת איסוף הראיות. כדוגמה להפעלת כוח מן הסוג הראשון ראו הסמכות לעצור חשוד לצורכי חקירה, גם כשעילה זו עומדת כשלעצמה בלי הוכחת מסוכנות לשלום הציבור או חשש מפני שיבוש מהלכי חקירה או הימלטות מן הדין (אם כי במגבלת זמן של הארכה לחמישה ימים בלבד): סעיף 13(א)(3) לחוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996. כדוגמה להפעלת כוח מן הסוג השני ראו הסמכות להיכנס בכוח לחצרים לצורכי ביצוע מעצר או חיפוש, כאשר אדם הגר במקום מסרב להרשות כניסה חופשית: סעיף 45 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969 (להלן – הפסד"פ).

18 ראו Kozlovski, לעיל ה"ש 13, בעמ' 128.

19 אעמוד בהרחבה על מאפיין זה ועל מושג סמכות האכיפה הנובע ממנו להלן בפרק 3(ב).

nevo.co.il

פועלים ממניעים רציונליים,[20] כיוון שהיא מגלמת פוטנציאל איתור ותפיסה, ומכאן, בנוסף – פוטנציאל ענישה. מכפלת סיכויי התפיסה בשיעור העונש (במקרה של הרשעה) מגלמת את ה"מחיר" של ביצוע העברה. כך יכול העבריין הפוטנציאלי (והרציונלי כאמור) לשקול את כדאיות ביצוע העברה.[21] ככל שהחקירה הפלילית תהיה יעילה יותר, במובן זה שהיא תצליח לאתר מבצעי עברות רבים יותר ולהגדיל את סיכויי התפיסה, כך משוואת ההרתעה תנוע לכיוון אי־כדאיות לביצוע העברה. במילים אחרות, החקירה הפלילית ex post עוזרת למנוע בסיבוב הבא התנהגות עבריינית מראש, ex ante.

נמרוד קוזלובסקי הסביר כי המשטרה המקצועית נמדדת לפי מספר התיקים הפליליים שפתחה ולפי המעצרים שביצעה, תוך בחינה של מספר תיקי החקירה שהבשילו לכדי כתבי אישום. מכאן שקיים תמריץ שלילי למשטרה לעסוק במניעת עברות פליליות מראש או בסיכול העברות תוך כדי התרחשותן,[22] הגם שהדבר מותר לה כמובן מבחינה משפטית־פורמלית. בשל התמקדות המשטרה באסטרטגיה תגובתית ולא מניעתית נוצר חוסר שיתוף פעולה ואף מתעוררת עוינות בקהילה כלפי המשטרה, ולכן הקרבנות הפוטנציאליים הופכים לפסיביים. תנאי לשיטור מניעתי הוא שיתוף פעולה, ואף יזמה, מצד הקהילה, ומשיסוד זה נגרע, הרי שבתהליך של היזון חוזר בין המשטרה לקהילה מתקיים שיעתוק של המודל התגובתי ודחייה של המודל המניעתי.[23]

במסגרת המודל התגובתי של המשטרה יש להבחין בין כמה אופני תגובה של המשטרה: **האחד**, חקירה פלילית בעקבות תלונה. יכול שאת התלונה יגיש נפגע העברה או עד לעברה; **השני**, חקירה פלילית בעקבות הוראה או המלצה לפתיחה בחקירה, שמתקבלת למשל על־ידי היועץ המשפטי לממשלה,[24] בית המשפט, מבקר המדינה, ועדת חקירה ממלכתית או אחרת; **השלישי**, חקירה פלילית בעקבות אירוע (חקירת זירה). במקרה זה אין פנייה מצד גורם כלשהו המניע את החקירה, אלא יש אירוע פלילי שמתרחש ו"קורא" לחקירה. כך הוא למשל במקרה של חקירת רצח הנפתחת בעקבות מציאת גופה במקום כלשהו; **הרביעי**, "עברות חשיפה" שבהן אין מתלונן ואין זירה, ובלא יזמה מצד המשטרה, היא לא תצליח לחשוף את העברה ולהרתיע מפני הישנותה.[25]

---

20 חלק מתחומי הפשיעה מוסברים ממניעים לא רציונליים, כגון דחף מיני, שאז אי אפשר לומר שענישה מרתיעה, וכן הגדלת סיכויי התפיסה של העבריין יוכלו לשמש כמונעי נזק יעילים.

21 למשוואת ההרתעה הזאת, ראו Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968); Dan M. Kahan, *Reciprocity, Collective Action, and Community Policing*, 90 CALIF. L. REV. 1513, 1521–22 (2002). בהקשר של פשיעה באינטרנט, ראו למשל Susan Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 2, 58–68 (2005); Susan Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, 9 INT'L J. COMM. L. & POL'Y 1, 40–49 (2004).

22 ראו Kozlovski, לעיל ה"ש 13, בעמ' 122.

23 ראו Kahan, לעיל ה"ש 21, בעמ' 1526.

24 היועץ המשפטי לממשלה יכול לקבל פניות מכל מיני גופים, למשל עמותות למען איכות השלטון, חברי כנסת, מבקר המדינה, אזרחים פרטיים, ויש בפניות אלה כדי לחולל הנחיה של היועץ לרשויות החקירה לפתוח בחקירה פלילית.

25 ראו The Attorney General's Guidelines for Domestic FBI Operations 16–18 (2008), *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf. כן ראו גדי אשד "החקירה המשטרתית והמודיעין האנושי" **משפט וצבא** 18 223, 228–229 (2005).

ניתן למצוא כמה הצדקות לשיטור שעוסק בחשיפה: **האחת**, יש עברות שבהן כל הצדדים הם בבחינת מעורבים בעסקת עברה,[26] ואין להם אינטרס לפנות למשטרה, שכן הם מעמידים גם את עצמם בסיכון של העמדה לדין, לדוגמה עברות של סחר בסמים (הן הקונה והן המוכר מעורבים בעסקת העברה) ומשחקים אסורים (הן המארגן והן המשחק מעורבים בעסקת העברה); **השנייה**, יש עברות אחרות, כגון זנות, תועבה וסחר בבני אדם, שבהן אמנם העוסק בזנות, מי שמופיע בתכנים המתועבים או מי שהוא קרבן לעברת סחר, אינם מעורבים בעסקת העברה, אולם ההנחה היא שקרבנות אלה מושתקים, וכמעט תמיד אין באפשרותם לפרוץ את מעגל האימה ולהתלונן במשטרה. מכאן שגם עברות אלה תסווגנה, קטגורית, כ״עברות חשיפה״; **השלישית**, יש מקרים שבהם קרבן העברה חושש מנקמה או מתיוג שלילי במקרה שיתלונן, ובמקרה שהעברה מתבצעת ברשות היחיד וללא עדים (או שגם העדים סובלים מאותם חששות של המתלונן), קיימת הסתברות גבוהה לאי־הגשת תלונה למשטרה. כדוגמאות למקרים אלה ניתן לציין עברות מין במקום העבודה או תוך ניצול יחסי מרות, עברה של הטרדה מינית, עברות אלימות במשפחה ועברות של סחיטה באיומים או בכוח. עברות החשיפה הן מורכבות יותר ויקרות יותר לחשיפה, כיוון שהחקירה מתחילה באופן שניתן להמשילו ל״ירייה באפלה״. גם התקדמות החקירה מסובכת יותר, כיוון שאין מתלונן, אין ראיות ה״מדברות״ מהזירה, ופוטנציאל איסוף הראיות קטן יותר. כפי שאראה להלן, עברות פליליות רבות בזירת הסייבר מחייבות פעולות חשיפה. פעולות חשיפה אלה מסובכות עוד יותר בזירה המקוונת.

ג. קשיי החקירה הפלילית במרחב הסייבר

כזכור, בתרשים 1.1 בפרק המבוא סיווגתי את עברות המחשב לשלושה סוגים: עברות נגד המחשב וחומר המחשב; עברות באמצעות מחשב שהועתקו במלואן אל המרחב הממוחשב; עברות מסתייעות־מחשב אשר הושלמו מחוץ למרחב הממוחשב והותירו עקבות דיגיטליות. סבורני כי בכל שלוש הקטגוריות הללו של עברות מחשב קיימת אכיפת חסר, כפי שאפרט להלן. אכיפת החסר מעודדת שגשוג של הפשיעה.[27] בעקבות זאת משתמשים רבים במרחב הממוחשב עלולים להימנע מהרחבת פעילותם או מהמשך פעילותם במרחב, כולה או חלקה, ובכך תיפגע התועלת המצרפית של השימוש במרחב זה.

את טיעון אכיפת החסר של העברות הפליליות במרחב הסייבר אציג כך: מצד אחד אביא נתונים בדבר ריבוי הפשיעה במרחב הסייבר, ומצד שני אציג מגוון הסברים — ארכיטקטוניים־טכנולוגיים, משפטיים ומוסדיים — לקיומו של קושי ממשי לאכוף את העברות במרחב הסייבר. איסוף נתונים כמותיים על העברות השונות במרחב הסייבר אינו משימה קלה, ולמעשה סביר להניח שהנתונים הקיימים חסרים. יש לכך כמה טעמים: **ראשית**, למעשה יש צורך באיסוף נתונים סטטיסטיים מכל מדינות העולם, שכן האינטרנט הוא גלובלי; **שנית**, את מרבית הנתונים

---

26 עוד על מיהותם ועל מעמדם של המעורבים בעסקת עברה, ראו יעקב קדמי על הראיות חלק ראשון 462–468 (2009).

27 כפי שכתב ארתור מילספאו (Millspaugh) עוד ב־1937, בהקשר של פשיעה במרחב הפיזי: "Crime tends to flourish in the legal categories and the geographical areas where enforcement is weak". ראו ARTHUR C. MILLSPAUGH, CRIME CONTROL BY THE NATIONAL GOVERNMENT 278 (1937).

nevo.co.il

אוספות עמותות פרטיות נושאיות (עמותות נגד פדופיליה מקוונת, נגד התמכרות להימורים באינטרנט וכדומה) או חברות מסחריות לאבטחת מידע. בכל הנוגע לנתונים שמוסרות חברות מסחריות לאבטחת מידע קיים חשש ממשי שבשל אינטרסים מסחריים למכירת אמצעים של אבטחת מידע והגנת סייבר, הרי שהאיום יוצג באור מוגזם. מנגד, נתונים רשמיים של המדינות כמעט שאינם זמינים,[28] אם כי לאחרונה נערך ניסיון יסודי ראשון, בחסות ה־UNODC (United Nations Office on Drugs & Crime), לשקלל נתונים מכלל המדינות על פי דיווח של גורמים רשמיים מתוכן;[29] **שלישית**, קיימת תופעה של דיווח חסר על עברות מחשב מצד הקרבנות, בין בשל הקושי שלהם לזהות כי נפגעו, בין בשל חשש שלהם לחשוף את דבר הפגיעה בהם,[30] ובין בשל חוסר אמון ביכולתן של רשויות אכיפת החוק לחשוף את מבצעי העברה ולהביאם לדין; **רביעית**, בכל הנוגע לעברות מסתייעות־המחשב שהושלמו מחוץ למרחב הממוחשב, על פי רוב לא יימצאו נתונים המתעדים קטגוריה זו בנפרד, שכן ההתייחסות לעברות אלה תהיה כאל עברות המבוצעות במרחב הפיזי (ואז המיון של הנתונים לא ייחתך על פי הקריטריון של האופן שבו בוצעה העברה, תוך הסתייעות במרחב הסייבר אם לאו, אלא לפי סוג העברה, סוג הקרבן וכיוצא בזה). על אף הקשיים האמורים אציג כמה נתונים על העלייה בפשיעה המקוונת. על מנת למתן את הקשיים המתודולוגיים אציג נתונים ממקורות שונים, מפרקי זמן שונים, בהתייחס לשאלות מחקריות שונות:

בכל הנוגע לעברות נגד המחשב וחומר המחשב, אלה פרחו בעידן האינטרנט ורשתות המחשב, אשר הקלו את ביצוען עד מאוד לעומת המצב טרם עידן האינטרנט. עוד לפני כעשור, כמעט כשני שלישים מהתאגידים בארצות הברית דיווחו על חדירות לא מורשות למערכות

---

28 David Wall, *Cybercrimes and the Internet*, *in* CRIME AND THE INTERNET 1, 7–10 (David Wall ed., 2001).

29 המחקר של ה־UNODC התבסס על קבוצת מומחים בין־מדינתית, שהתכנסה בינואר 2011 ובפברואר 2013 בניסיון להגדיר ולאמוד את פשיעת האינטרנט וכן להציע דרכי התמודדות עם התופעה. ראו United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (Draft – February 2013) http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

30 ראו UNODC, שם, בעמ׳ 259–263. הדוגמה המובהקת לכך היא במקרה של חברות המציעות שירותים פיסקאליים באינטרנט. עובדת היותם של אלה קרבנות לעברות מחשב עלולה לפגוע קשות במוניטין של חברות אלה, שכן הלקוחות הפוטנציאליים יחששו להשתמש בשירותיהן. בכמה מדינות בארצות הברית נחקקו חוקים המחייבים את אותן חברות לדווח על חדירה למחשביהן. החוק הראשון מסוג זה נחקק בקליפורניה בשנת 2002, ראו CAL. CIV. CODE, §§ 1798.29, 1798.80-.84. כן ראו בעניין זה דירקטיבה של האיחוד האירופי משנת 2009 שתיקנה את הדירקטיבה משנת 2002 להגנת מידע אישי: Directive 2009/136/EC of the European Parliament and of the Council (25.11.2009) amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337. עוד על חקיקה המחייבת יידוע במקרה של אירוע אבטחת מידע, ראו Jane K. Winn, *Are “Better” Security Breach Notification Laws Possible*, 24 BERKELEY TECH. L.J. 133 (2009).

המחשבים שלהן, ולכמחצית מהם גרמו החדירות הפסדים כספיים.[31] בשנת 2011 תועדו בארצות הברית בלבד יותר מ־300,000 תלונות על עברות נגד מחשב ונגד חומר מחשב.[32] חברת אבטחת המידע McAfee מציינת עלייה אקספוננציאלית בעשור הקודם בהתקפות של וירוסים, סוסים טרויאניים, התקפות DDoS (Distributed Denial of Service)[33] עד למספרים של אלפי זנים שונים של תוכנות זדוניות בשנים האחרונות (כאשר בכל הנוגע לסוסים טרויאניים נמנו יותר מ־100,000 סוגים שונים בשימוש).[34]

בכל הנוגע לעברות שהועתקו במלואן אל המרחב הממוחשב, מדובר בתופעה מעניינת במיוחד המוכיחה את כדאיות ביצוע העברות במרחב הסייבר. כיוון שקיימת מקבילה מלאה לעברות בקבוצה זו גם במרחב הפיזי, הרי שעצם העתקתן של העברות למרחב המקוון מוכיח את כדאיות ביצוע העברות במרחב זה. עוד בשנת 1997 הכריזו מדינות ה־G8 על חמישה תחומים של עברות באמצעות מחשב שהועתקו אל המרחב הממוחשב כתחומים שבהם מזוהה עלייה כמותית בפשיעה וסכנה גלובלית: ניצול מיני, סחר בסמים, הלבנת הון, מרמה וריגול תעשייתי ומדינתי.[35] עליות תלולות זוהו בתחומים נוספים שבעניינם קבעו מדינות רבות איסורים פליליים, ובהם פדופיליה באינטרנט,[36] עברות ביטחון כגון סיוע לאויב במלחמה ומסירת ידיעה לאויב,[37] פרסומי הסתה לגזענות, פגיעה בפרטיות ובזכות להגנה על מידע אישי והימורים מקוונים.[38]

---

31 ראו Cybercrime: Hearing Before the Subcomm. on Commerce, Justice, and State, the Judiciary, and Related Agencies of the S. Appropriations Comm., 106th Cong. 74 (2000) (statement of Mark Rasch, Vice President, Global Integrity Corporation).

32 ראו בנושא זה את דוח ה־IC3 (גוף שנוסד כשותפות בין ה־FBI וה־National White Collar Crime Center ועניינו בטיפול בתלונות הנוגעות לפשעי אינטרנט ברמה המדינתית והפדרלית): Internet Crime Complaint Center, 2013 Internet Crime Report (2014), https://www.ic3.gov/media/annualreport/2013_IC3Report.pdf/; http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf.

33 להגדרות של התקפות DDoS, וירוסים וסוסים טרויאניים, ראו לעיל בפרק המבוא, בה"ש 2–6.

34 ראו McAffee Virtual Criminology Report: Cybercrime Versus Cyberlaw 4 (2010), *available at* http://img.en25.com/Web/McAfee/mcafee_VCR_US_lowResFinal_REV.pdf. כן ראו למשל את Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1004–1031 (2001) (והמקורות המצוטטים שם). ראו עוד, למשל, את הסקירה אצל SUSAN BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE ch. 2 & 4 (2009); Commonwealth Cybercrime Initiative Proposal (presented at the Commonwealth Internet Governance Forum, 19.7.2011), *available at* http://www.commonwealthconnects.org/wp-content/uploads/2011/07/Cyber-Crime-Proposal-Ver-6-.pdf.

35 ראו: Clifford Krauss, 8 Countries Join in an Effort To Catch Computer Criminals, NY TIMES A12 (Dec 11, 1997).

36 למצב בישראל, ראו דבריו של סנ"צ אבי אביב בפני ועדת המדע של הכנסת ה־17: פרוטוקול מס' 68 מישיבת ועדת המדע והטכנולוגיה בנושא "המאבק למיגור תופעת הפדופילים באינטרנט" (26.12.2007), המצוי ב: http://www.knesset.gov.il/protocols/data/html/mada/2007-12-26.html. אשר למצב בעולם, ההערכות של עמותת ה־Internet Watch Foundation מציירות תמונה עולמית עגומה של עלייה מתמדת ותלולה באתרים שמופצים בהם תכנים פדופיליים. ראו Internet Watch Foundation, Annual Report 2010, *available at* http://www.iwf.org.uk/accountability/annual-reports/2010-annual-report. על פי הדוח השנתי לשנת 2010, אותרו 16,739 אתרים בעלי שם (URL) שונה, אשר כללו תכנים פדופיליים אסורים על פי דין המדינה שבו נמצאו שרתי אותם אתרים. כמות זו שילשה את עצמה לעומת שנת 2008, השוו ל־ Internet Watch Foundation, Annual Report 2008, *available at* http://www.iwf.org.uk/accountability/annual-reports/2008-annual-report.

nevo.co.il

נוסף על האמור לעיל ניתן להצביע על קבוצת מחקרים שניסתה לכמת את הנזקים הכלכליים, בין הישירים ובין העקיפים,[39] שנגרמים מפשיעת הסייבר. מחקרים אלה רלוונטיים מראש רק לעברות המונעות ממוטיבציות כלכליות, כגון עברות מרמה מקוונות, התקפות סייבר שונות המסבות נזק למחשבים ולמידע, עברות על דיני הקניין הרוחני וכדומה. הנתונים ממחקרים אלה מצביעים על עלייה בהיקפי הנזק הכלכלי שנגרם מהפשיעה המקוונת.[40] לכאורה, נתונים אלה

---

37 ראוי לציין בהקשרנו את אמירותיו הלאקוניות, אך החשובות, של בית המשפט העליון בנוגע לעלייה בביצוע עברות ביטחון באמצעות האינטרנט. בע״פ 3417/10 **מדינת ישראל נ׳ פלוני** (פורסם בנבו, 31.1.2011) התקבל ערעור המדינה על קולת עונש של נאשם שהורשע בעברה של מסירת ידיעה לאויב. השופטת ארבל כתבה: ״יצירת קשר עם גורמים עוינים לישראל הפכה פשוטה יחסית בעידן האינטרנט ומקלה על אלה החפצים לפעול נגד המדינה״. ראו גם ע״פ 7430/10 **פלוני נ׳ מדינת ישראל** (פורסם בנבו, 5.2.2012), שם דובר על עברה של קשירת קשר לסיוע לאויב במלחמה, ובית המשפט העליון, מפי השופט גרוניס, קבע כי ״רשת האינטרנט מהווה כר פורה לביצוע פעילות עבריינית מסוגים ומינים שונים, ובין היתר פעילות המכוונת נגד ביטחון המדינה״. האמירה אינה נסמכת על נתונים אמפיריים, אך שימשה שיקול של בית המשפט העליון שלא להיעתר לערעור הנאשם נגד חומרת העונש שהוטל עליו.

38 ראו חיים ויסמונסקי ״על ענישה בעבירות מחשב״ **מחקרי משפט** כד 81, 87–93 (2008) וההפניות המובאות שם. המאמר מתייחס גם לעברות של פרסומי תועבה מיניים ופרסומים פדופיליים וכן לעברות של מרמה באמצעות מחשב, אשר ציינתי אותן קודם לכן כעברות שחלה עלייה תלולה בתפוצתן באינטרנט. לעלייה התלולה בהימורים המקוונים ראו למשל Edward M. Yures, *Gambling on the Internet: The States Risk Playing Economic Roulette as the Internet Gambling Industry Spins Onward*, 28 RUTGERS COMP. & TECH. L.J. 193 (2002); כן ראו Dana Gale, *The Economic Incentive Behind the Unlawful Internet Gambling Enforcement Act*, 15 CARDOZO J. INT'L & COMP. L. 533, 534 (2007).

39 בנזקים ישירים מעברות אינטרנט הכוונה היא, למשל, לאלה: סכום הכסף שנגנב, אבדן הזמן שנגרם לנפגע העברה, הפיצויים ללקוח של נפגע העברה ואבדן מידע בעל ערך כלכלי. בנזקים עקיפים הכוונה, למשל, להורדת דירוג האשראי של תאגיד שמחשביו נפרצו, לאבדן הזדמנויות עסקיות, להפסקת השימוש באמצעים אלקטרוניים מצד נפגע העברה או לקוחותיו, וכן להוצאות בגין התגוננות מפני עברות עתידיות והוצאות לצורך אכיפה (תביעות אזרחיות של הקרבן). ראו לעניין זה Ross Anderson et. al, *Measuring the Cost of Cybercrime*, ECONINFOSEC 4–6 (2012) http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

40 ראו למשל את הדוח של חברת Ponemon Institute בשביל HP Enterprise Security משנת 2012, שבדק את מידת הנזק של תאגידים עסקיים גדולים בארצות הברית בשל תקיפות סייבר ומרמה מקוונת. נמצא כי תאגידים עסקיים גדולים בארצות הברית סובלים בממוצע מנזק של 8,933,510 דולר לשנה לכל תאגיד, וכי נזק ממוצע זה גדל בכ־500,000 דולר לעומת הנתון המקביל שנה קודם לכן. ראו Ponemon Institute, 2012 Cost of Cybercrime Study: United States (2012), http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf. ראו עוד את הדוח של ממשלת בריטניה בשיתוף חברת Detica משנת 2011, אשר קבע כי עלויות פשיעת הסייבר בבריטניה מוערכות בכ־27 מיליארד ליש״ט בשנה. המחקר התמקד בנזק לשלושה מגזרים – משתמשי האינטרנט הפרטיים, המגזר הציבורי והמגזר העסקי – והוא הצביע על מגמת עלייה בהיקפי הנזק בשלושת המגזרים הללו. ראו Detica Report in Partnership With the Office of Cyber Security and Information Assurance in the Cabinet Office, The Cost of Cyber Crime 2011, https://www.baesystemsdetica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf. ראו גם דוח של איגוד הקמעונאים הבריטים (British Retail Consortium) לשנת 2012, הקובע כי סוג הפשיעה המזיק ביותר לסקטור הקמעונאי הוא תחום תקיפת המחשבים והמרמה המקוונת, הגורמים לנזק רב משגורמות גנבות של לקוחות, גנבות של עובדים, פריצות, שודים וכד׳. הערכת הנזק לסקטור הקמעונאי מתקיפת המחשבים והמרמה המקוונת בשנת 2012 בבריטניה היא 205,400,000 ליש״ט, כאשר סכום זה מבטא עלייה בהיקפי הנזק. ראו British Retail Consortium,

nevo.co.il

כשלעצמם אינם מצביעים על עלייה במספר העברות במרחב הסייבר, אפילו לא על עלייה במספר העברות בסייבר המונעות ממוטיבציות כלכליות, אלא מצביעים הם על עלייה בהיקפי הנזק הכלכלי שמסבה פשיעת הסייבר, וכך אם התלות של נפגעי העברות במרחב המקוון גדלה, ייתכן שהנזק שייגרם להם יגדל גם אם לא יגדל מספר העברות במרחב. כך או כך, יש בנתונים אלה כשלעצמם כדי להצביע למצער על גידול בהשלכות של פשיעת הסייבר. מחקר שנערך באוניברסיטת קיימברידג׳ הראה כי הנזקים העקיפים של העברות במרחב הסייבר, בעיקר עלויות ההתגוננות מפני עברות עתידיות, קשים מן הנזקים הישירים של עברות אלה, ומכאן שפרדיגמה של התגוננות בלבד אינה יעילה כלכלית, ויש לנסות להגביר את מאמצי החשיפה של מבצעי העברות והבאתם לדין.[41]

לסיכום, חרף קשיים מתודולוגיים לאמוד את שיעורי הפשיעה במרחב הקיברנטי, מגוון מחקרים מצביעים על עלייה בפשיעה במרחב זה. למול עובדה זו ניתן להצביע על קשיים בחקירה הפלילית במרחב הקיברנטי. מדוע החקירה הפלילית כאמור היא משימה קשה במיוחד? ניתן למנות כמה טעמים לכך, הנחלקים לשלוש קבוצות: טעמים ארכיטקטוניים התלויים במבנה האינטרנט ובטכנולוגיה המרכיבה אותו, טעמים משפטיים הנובעים מהארכיטקטורה הייחודית של המרחב המקוון וטעמים מוסדיים.

1. טעמים ארכיטקטוניים־טכנולוגיים

האחד, רשתות המחשב הפתוחות, ובראשן האינטרנט, מאפשרות **אנונימיות** יחסית, ולמשתמשים מתוחכמים מתאפשרת אנונימיות מוגברת. האנונימיות היחסית נובעת מן האפשרות להתייצג ללא זהות, בזהות בדויה קבועה (פסידונימיות)[42] או ארעית. היא מאפשרת גם התחזות לאדם אחר לצורך הפללתו או ביזויו בפומבי באמצעות כתיבת מסרים מבזים ״בשמו״.[43] הבסיס להסוואת הזהות באינטרנט נעוץ בכך שהזיהוי הבסיסי הוא על פי כתובת IP שמוענקת לכל מחשב באינטרנט. כתובת ה־IP מוקצה למשתמש בידי ספקי הגישה לאינטרנט, וכשמדובר במשתמש פרטי, הרי שהכתובת הניתנת לו משתנה מעת לעת. במילים אחרות, כתובת IP אינה מזהה חד־ערכי לזהות משתמש באינטרנט.[44] יתרה מזאת, גם אם ניתן לשייך את כתובת ה־IP למחשב מסוים, אין זה אומר שיהיה ניתן לשייך את המחשב לחשוד מסוים. זאת, כיוון שניתן לגלוש באמצעות שרתי proxy שאינם שומרים את נתוני הגלישה של המחשבים שהתקשרו

Retail Crime Survey 2012, *available at* http://www.brc.org.uk/downloads/brc_retail_crime_survey_2012.pdf. לניסיון להצביע על עלייה בנזקי פשיעת האינטרנט ברמה הגלובלית, ראו דוח של חברת נורטון Norton Cybercrime Report (2012), *available at* http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

41 ראו Anderson et. al, לעיל ה״ש 39, בעמ׳ 7 ו־26.

42 על ההבחנה בין אנונימיות לבין פסידונימיות, ראו למשל אלעד אורג **זכות לזהות אינפורמטיבית: עקרון משפטי חדש להגנת קיומה של זהות אינפורמטיבית ויישומו בסביבת מידע מודרני** 23–26, 123–143 (חיבור לשם קבלת תואר ״דוקטור למשפטים״, אוניברסיטת תל־אביב, 2008).

43 ראו, בהקשר זה, צ״א (שלום י־ם) 32145-07-13 **הוצאת עיתון הארץ בע״מ נ׳ משטרת ישראל** (פורסם בנבו, 12.8.2013).

44 ראו מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 338–348 (2010).

nevo.co.il

דרכם אל האינטרנט;[45] דרך רשת ביתית שמחוברים אליה כמה מחשבים (ואי אפשר לדעת מי מהמחשבים ביצע את הפעולה הנחקרת); דרך רשתות אלחוטיות wireless ציבוריות וכדומה. יתר על כן, משתמש יכול להשתמש בשירותי אנונימיזציה המגבירים את האנונימיות שלו באופן מיוחד.[46] כך למשל ניתן להשתמש בשירותים המציעים כתובת IP דינמית המשתנה מעת לעת ומעלימה את כתובת ה־IP האמתית של המחשב ברשת,[47] וכן ניתן להשתמש בשיטות של Onion routing כדוגמת פרויקט TOR המסווה את המסר המועבר מגולש מסוים באמצעות העברתו דרך שרשרת של מחשבים כאשר אי אפשר לאחזר בדיעבד את מקור ההתקשרות (לפחות מבלי לפקח לאורך זמן ומראש על כל שרשרת המחשבים).[48] אמצעי אנונימיזציה מתוחכמים אלה מאפשרים לגורמים עברייניים לפתח אזורים מחתרתיים ברשת המכונים Darknets שבהם רוחשת פעילות עבריינית ענפה.[49]

השני, האינטרנט, כרשת התקשורת הגלובלית, **פתוח לכלל הציבור**, וההצטרפות אליו כיום למעשה יכולה להיות חופשית ולא מבוקרת (לפחות במדינות דמוקרטיות).[50] נגישות האינטרנט גדלה מאוד, ובכמה מובנים: **ראשית**, עלויות הרכישה של מחשב ועלויות ההתחברות לאינטרנט הביתי והעברת המידע באינטרנט הוזלו עם השנים; **שנית**, האינטרנט עבר למקומות ציבוריים רבים (שדות תעופה, בתי קפה, בתי מלון ואף ערים שלמות) המציעים שירותי התחברות אלחוטית (Wireless) בתשלום או בחינם; **שלישית**, מספר וסוג המכשירים היכולים להתחבר לאינטרנט גדל בשיעור ניכר. האינטרנט אינו מחבר עוד בין מחשבים נייחים או אף ניידים. האינטרנט הסלולרי הנגיש את הרשת והעצים את השימוש במשאביה. "ניוד" האינטרנט אינו מאפשר עוד רק להגיע לכל "מקום", אלא להגיע לכל "מקום" מכל מקום שבו נמצא הגולש. כאשר החיבור לאינטרנט נעשה ממקומות ציבוריים, ללא דרישת הזדהות מוקדמת, הרי שיכולת הבקרה בדיעבד על זהות הגולש נפגעת מאוד, ומשכך הוא, קטנה היכולת לחשוף את מבצע העברה הפלילית.

השלישי, חלק ניכר מן העקבות הדיגיטליות שמותירה פעילות עבריינית במרחב הסייבר – **נדיף**. מקובל לטעון שהמידע ברשת נשמר לזמן ארוך, לעתים אינסופי, וכי בעיית הזיכרון ארוך

---

45 כדוגמה לאתר אינטרנט המספק מידע על שרתי proxy שונים אשר מהם ניתן לגלוש באינטרנט בלא שיהיה אפשר להסגיר את זהות הגולש, ראו http://proxy.org.

46 ראו Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. Miami L. Rev. 1301 (2004). במאמר זה ז'רסקי עורך בחינה נורמטיבית אם ראוי להכיר במודל של הגנה על אנונימיות ברשת. ז'רסקי מציג את בעיותיו של מודל האנונימיות, ועם הבעיות נמנית גם הבעיה של פגיעה ביכולת האכיפה הפלילית באשר לעברות ברשת. ראו שם, בעמ' 1334–1340. לסקירה של שיטות אנונימיזציה, ראו בירנהק, לעיל ה"ש 44, בעמ' 388–395.

47 כדוגמה לשירותים המספקים כתובת IP דינמית ומטשטשים עקבות IP בשרתים ובמחשבים אחרים שבהם גלש המשתמש, ראו למשל: www.anonymixer.com, www.no-ip.com.

48 ראו www.torproject.org.

49 ראו נמרוד קוזלובסקי "פדופיליה, סמים וחיסולים: עולם הפשע האפל של ה־Darknets" http://www.holesinthenet.co.il/archives/35228 (1.1.2012); רועי גודלשמיט "שימוש הרשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה" מרכז המחקר והמידע של הכנסת (1.1.2012).

50 ראו בירנהק, לעיל ה"ש 44, בעמ' 339.

nevo.co.il

הטווח יוצרת אפקטים לא פשוטים של פגיעה בפרטיות ובשמו הטוב של אדם.[51] עם זאת חלק ניכר מהמידע הדיגיטלי, אשר עשוי להיות יקר ערך לצורכי חקירה פלילית עתידית, אינו נשמר דרך קבע. תכנים רבים נשמרים בספריות "זמניות" או שהם מאוחסנים עד ל"דריסתם" על ידי מידע אחר שיתפוס את מקום האחסון לצורך השימוש הבא באותו שרת או מחשב המחובר לרשת. ככל שהמידע הדיגיטלי מנוהל בידי ספקי שירות שונים, וככל שאין מוטלת עליהם כל חובה שבדין לשמור את המידע הזה בשביל המדינה ולשימושה, הרי שניהול המידע נעשה לתועלת התאגיד המנהל את השירות ולתועלתו בלבד, ולא תמיד תועלת זו מצטלבת עם צורכי החקירה הפלילית. יש ששמירת המידע נעשית בידי ספק השירות לצרכיו שלו, למשל לצורך בקרת איכות השירות שלו, לצורך איתור תקלות ואבטחת מידע באמצעות בדיקות בדיעבד.[52] תכונת הנדיפות של העקבות הדיגיטליות מעוררת דיון בשאלת הצורך של המדינה להטיל על ספקיות השירות השונות חובות שימור מידע דרך קבע (Retention),[53] או מכאן ולהבא במקרה קונקרטי (Preservation),[54] כאשר לחובות אלה השלכות ניכרות על הזכות לפרטיות, על הזכות לאנונימיות, על האוטונומיה של הרצון הפרטי ועל חופש השימוש במחשב ובאינטרנט.[55]

הרביעי, בכל הנוגע לאינטרנט, הרי שחלק ניכר מאותן עקבות דיגיטליות **מבוזר** על פני כמה מחשבים באופן שאינו חופף את יעד ההתקשרות הסופי של המשתמש. הטעם לכך הוא

---

51 קיים דיון ציבורי ומשפטי בדבר "הזכות להישכח" (the right to be forgotten) באינטרנט, כשהכוונה היא לזכות שלפיה מידע אישי לא ייאגר ויעמוד לדיראון עולם במרחבי האינטרנט נגד אדם. לדיונים שיפוטיים וציבוריים בהקשר זה ראו למשל (ובהתאמה): ע"א (מחוזי ת"א) 2319/08 **פלוני נ' פלונית**, בפס' 19–39 (פורסם בנבו, 1.6.2011). משה גורלי "כנס ה־OECD בנושא הפרטיות ברשת: הזכות להישכח" **כלכליסט** (27.10.2010) http://www.calcalist.co.il/local/articles/0,7340,L-3421903,00.html.

52 לנוהג של ספקי השירות השונים באינטרנט לאגור נתוני תוכן ונתוני תקשורת רבים על אודות הגולשים השונים, ראו Kozlovski, לעיל ה"ש 13, בעמ' 88–93. מכאן מסיק קוזלובסקי שאותם ספקי שירות הם מוקד משמעותי ביותר במסגרת חקירות במרחב הקיברנטי. עם ספקי השירות שמציין קוזלובסקי נמנים אלה: ספקי גישה לאינטרנט, ספקי שירותי דוא"ל, אתרי אינטרנט המרכזים נתוני גלישה ואף מנועי חיפוש. כיום ניתן למנות גם את מנהלי הרשתות החברתיות. שמירה כזו של נתונים בידי ספקי השירות השונים צריכה כמובן להירשם בישראל כמאגר מידע לפי הוראת סעיף 8 לחוק הגנת הפרטיות, התשמ"א–1981.

53 עד לאחרונה הוכר משטר Retention באיחוד האירופי. ראו Directive 2006/24/EC of the European Parliament and of the Council (13.4.2006) on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105. על בסיס הדירקטיבה האמורה חוקקו מדינות האיחוד האירופי חוקי Retention במשפטן הפנימי. לדוגמה, מתוקף הדירקטיבה קובע חוק הביטחון היום־יומי בצרפת: Loi sur la sécurité quotidienne 2001 (LSQ) כי ספקי שירות באינטרנט ישמרו מידע למשך שנה. לאחרונה פסל בית הדין הגבוה לצדק של האיחוד האירופי את הדירקטיבה האמורה בטענה כי היא מציעה פגיעה לא מידתית בזכות לפרטיות. הפסיקה אינה בעלת כוח לבטל את החקיקה הפנימית של המדינות השונות, אך הדירקטיבה ככזו נפסלה. ראו Digital Rights Ireland Ltd. v. Minister of Communictaions, Marine and Natural Resources, ECJ C-293/12 [2014].

54 כדוגמאות להוראות preservation באשר לראיות דיגיטליות, ראו בארצות הברית את 18 U.S.C. § 2703(f). כן ראו באמנת מועצת אירופה בדבר פשעי מחשב: Council of Europe Convention on Cybercrime (Budapest 2001) בסעיפים 16–17.

55 ארחיב על פעולות האיסוף של שימור מידע דרך קבע (Retention) ושימור מידע מכאן ולהבא (Preservation) בפרק ד.ג.3. להלן.

nevo.co.il

שהאינטרנט בנוי כמערכת שהיא Packet-switched, שבה המידע מפוזר ל״חבילות״, המשוגרות עם כתובת יעד מסוימת המחוברת אליהן. רק בסוף המסלול מתחברות ה״חבילות״ יחדיו ונמסרות לנמען. במהלך הדרך ה״חבילות״ מתערבבות עם ״חבילות״ אחרות הממוענות ליעדים אחרים.[56] כך מתאפשר לנצל את משאבי התעבורה ברשת ביתר יעילות.[57] החלופה המרכזית לתקשורת שהיא מבוססת packets קיימת בעולם הטלפוניה, שהוא Circuit-switched, ובו על מנת ״להקים״ שיחה יש צורך ביצירת מעגל סגור בין שני המשוחחים באופן שחוסם משוחחים אחרים באותו חלק של הרשת. כל עוד מתקיימת השיחה בין השניים, החסימה נמשכת. ביזור העקבות הדיגיטליות אינו רק במובן של טכניקת העברת המידע, כמצוין לעיל, אלא גם בשיטת ההחזקה והשימוש במידע. רשתות מחשב שונות, ובראשן האינטרנט, מאפשרות לקיים שירותים של אגירת מידע במחשבים מרוחקים באופן המאיין את ההצמדה הפיזית בין המחזיק לבין הנכס שהוא מחזיק. שירותי דוא״ל Webmail, כגון Gmail, Yahoo!, מספקים, לצד עצם שירות התקשורת, גם שירות של תיבת אחסון מידע אישי בנפחים שונים אשר גדלו עם השנים.[58] שרתי FTP[59] רבים מציעים שירותי אחסון מידע לצורך החלפת קבצים מהירה ויעילה בין כמה גורמים. בשנים האחרונות הפכה שיטת ״מחשוב הענן״ (Cloud computing)[60] לשיטה מקובלת להחזקת שירותים, תכניות ומידע במחשבים מרוחקים תוך שמירה על שליטתו של המשתמש בהם.

---

56 הסיבה ההיסטורית לשיטת העברת הנתונים שהיא packet-switched נעוצה באב הטיפוס של הרשת הנוכחית, ה־Arpanet, אשר נועדה לשרת את הצבא האמריקני במקרה של מלחמה גרעינית. דייוויד קלארק (Clark) מנה את המטרות האלה של רשת ה־Arpanet: (1) הרשת צריכה להתאפיין בשרידות (survivability), ועליה להצליח להתקיים גם במקרה של אבדן חלק מהרשתות; (2) הרשת צריכה לתמוך בכמה סוגים של תקשורת בין מחשבים; (3) הרשת צריכה לאפשר קיום של כמה רשתות בתוכה (רשת המורכבת ממספר רב של תת־רשתות; (4) הרשת צריכה להתנהל בביזור. ראו David D. Clark, *The Design Philosophy of the DARPA Internet Protocol*, 18 COMP. COMM. REV. 106 (1988). כן ראו עוד JAMES GILLIES & ROBERT CAILLIAU, HOW THE WEB WAS BORN – THE STORY OF THE WORLD WIDE WEB (2000).

57 ה־packet מכיל את המידע שמבקשים להעבירו, את ה־header שאליו ממוען המידע, ולעתים גם את ה־trailer האוסף נתונים על שגיאות בהעברת המידע. נתבי הרשת (routers) בוחרים את המסלול המיטבי להעברת ה־packets ליעדם, וכן הם מריצים פרוצדורה של packet forwarding ובו מועבר ה־packet מנקודה לנקודה במהלך מסלולו אל יעדו. ראו עוד בנספח א׳ (רקע על ארכיטקטורת האינטרנט).

58 עד לפני זמן לא רב כלל חלק מהתחרות בין ספקיות שירותי הדוא״ל מסוג Webmail הגדלה של נפחי האחסון של התיבה. ראו למשל שירות בלומברג ״מייקרוסופט תציע נפח אחסון מוגדל של דואר אלקטרוני – במענה לגוגל ויאהו״ **גלובס Online (24.6.2004)** http://www.globes.co.il/news/docview.aspx?did=808555. אדר שלו ״שירות הדוא״ל Live Hotmail גדל ל־5 גיגה בייט״ **Ynet (14.8.2007)** http://www.ynet.co.il/articles/1,7340,L-3437367,00.html.

59 File Transfer Protocol: מדובר בפרוטוקול תקשורת מבוסס TCP להעברת קבצים בין מחשבים דרך שרת ייעודי שאליו מתקשרים המשתמשים השונים.

60 הכוונה ב״מחשוב ענן״ לשירות שבו משתמש הקצה מעביר את התוכנות היישומיות ואת המידע האגור ברשותו לאינטרנט, ומחשבו האישי הופך למעין מסוף בלבד. התוכנות והמידע מנוהלים בשביל משתמש הקצה בידי תאגיד המספק שירותי ״מחשוב ענן״. מבחינת משתמש הקצה, האינטרס להשתמש ב״מחשוב ענן״ הוא הוזלת עלויות הרכישה והתחזוקה של מחשבו האישי. משתמש הקצה על פי רוב אינו יודע (ואינו מתעניין בכך) מהו המקום הפיזי שבו אגור המידע השייך לו. ראו למשל http://epic.org/privacy/cloudcomputing/. כן ראו M. Taylor, J. Haggerty, D. Gresty & R. Hegarty, *Digital Evidence in Cloud Computing Systems*, 26 COMP.L.& SECURITY REV. 304 (2010).

nevo.co.il

לביזוריות העקבות הדיגיטליות כמה השלכות על אכיפת הדין הפלילי במרחב המקוון: **ראשית**, הביזוריות חוצה גבולות מדיניים, ובשל כך על החקירה להתייחס לראיות פוטנציאליות המבוקשות מטריטוריה זרה; **שנית**, הביזוריות מגדילה את מספר הגורמים שעמם יש לבוא במגע במסגרת החקירה הפלילית, ומטבע הדברים החקירה וההתדיינות הכרוכות בה (הגשת בקשות לצווים שיפוטיים שונים כלפי אותם גורמים, התדיינויות במקרה של התנגדות לאותם צווים שיפוטיים) – מתייקרות; **שלישית**, הביזוריות מקשה על חשיפת מבצעי העבירות, שכן לעתים עלול מקור ה־packet להצביע על "מחשב חשוד" שממנו בוצעה פעולה זדונית מסוימת, אך בפועל מחשב זה אינו אלא צומת תמים שדרכו עבר המידע.[61]

2. טעמים משפטיים

הטעמים המשפטיים להיותה של החקירה הפלילית במרחב המקוון משימה קשה במיוחד נובעים מהטעמים הארכיטקטוניים שמניתי לעיל, המייחדים את המרחב המקוון מהזירות האחרות של ביצוע עברות פליליות:

האחד, האינטרנט כאמור נולד, מבחינה היסטורית, כרשת מבוזרת, שהמידע בה אינו מצוי במקום אחד, והוא ניתן להעברה בלחיצת כפתור ממקום למקום. הביזור מאפשר למשתמש לנצל את **המולטי־טריטוריאליות** ולפעול דרך כמה מדינות ובאופן שיצריך – על פי המשטר המשפטי המקובל כיום במרבית מדינות העולם – בקשות מורכבות לעזרה משפטית.[62] מנגנון העזרה המשפטית אטי, מסורבל ותלוי בשיתוף פעולה ובהדדיות. על פי רוב, העזרה המשפטית מחייבת פליליות כפולה (Dual criminality) במובן זה שהמעשה שאותו מבקשים לאכוף ייחשב לאסור על פי דיני שתי המדינות – המדינה החוקרת והמדינה שלה הוגשה בקשת העזרה המשפטית. בעיית המולטי־טריטוריאליות האמורה מבוססת על התפישה הטריטוריאלית החולשת על דיני איסוף הראיות במרחב הסייבר, אשר עליה ארחיב בפרק ג. לצד בעיית העזרה המשפטית, המולטי־טריטוריאליות של המרחב המקוון עלולה ליצור תופעה של סחרור דינים: ככל שמיקום השרתים של אתר מסוים ישפיע על הגדרת מיקום הפעילות הפלילית, הנטייה של מנהלי האתרים תהיה להעתיק את פעילותם למדינות שבהן אין איסור פלילי על הפעילות, גם אם במדינות אחרות קיים איסור פלילי שכזה. כך, יוכלו אותן מדינות להימנע מחקירה ומהעמדה לדין בהיעדר "פליליות כפולה" במעשים הנחקרים.[63]

---

61 ראו Orin S. Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture and Civil Liability*, 1 J. L. ECON. & POL'Y 197, 205 (2005).

62 מנגנון העזרה המשפטית קבוע בחוק עזרה משפטית בין מדינות, התשמ"ח–1988 (להלן – חוק עזרה משפטית). לעומת המודל של העזרה המשפטית הקלאסית המגולם בחוק עזרה משפטית, אמנת מועצת אירופה בדבר פשעי מחשב (Convention on Cybercrime), שנחתמה בבודפשט בשנת 2001, מנסה להתמודד עם בעיות של הצורך ב־transborder search באינטרנט באמצעות פיתוח מנגנוני שיתוף פעולה מהירים בין שתי המדינות. אפרט על האמנה להלן בפרק ב.ה.2.א).

63 ראו, למשל, Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553, 577–580 (1998). כן ראו ב"ש (מחוזי ת"א) 90861/07 **קרלטון נ' היחידה הארצית לחקירות הונאה** (פורסם בנבו, 17.6.2007). באותו מקרה דובר על בעלי חברת הימורים באינטרנט (ויקטור־צ'נדלר), שהציעה שירותיה בין היתר לקהל בישראל, תוך העלאת תכנים בשפה העברית. שרתי אתר ההימורים מוקמו בגיברלטר, שם מותר על פי דין לארגן הימורים.

nevo.co.il

השני, מערך הדינים המסמיך את רשויות החקירה אינו מתאים לחקירה במרחב המקוון. החקיקה המסמיכה את רשויות החקירה בדרך כלל אינה מכוננת התפתחויות טכנולוגיות אלא מגיבה להן. כמוה גם פסיקת בית המשפט. כאשר ההתפתחות היא מואצת במיוחד, כבעידן האינטרנט, וכאשר ההתפתחות מאתגרת את עצם ההגדרה של המדינה כאוכפת החוק בטריטוריה שלה, הרי שהפיגור המשפטי (במובן של חקיקת המדינה ופסיקת בתי המשפט שלה) מחריף.

מן הטעמים המשפטיים שהצגתי לעיל נובע כי המשפט מפגר אחר ההתפתחות הטכנולוגית. הגם שהמודל הלסיגיאני, שאותו הצגתי בפרק א לעיל, מדבר על ארבעה כוחות מסדירים – משפט, ארכיטקטורה, ערכים חברתיים וכוחות השוק – הרי שבהתבוננות על הציר של משפט מול ארכיטקטורת המרחב המקוון, נראה כי המשפט, בכליו הקיימים, לוקה בקשיים ניכרים להתמודד עם השינויים שחוללה מהפכת המרחב המקוון, ולו מבחינה טכנולוגית בלבד. בפרק ו אציע תיקון לפער שנפער בין המשפט לבין המרחב המקוון כתופעה טכנולוגית־ארכיטקטונית.

3. טעמים מוסדיים

הטעם הראשון מבין הטעמים המוסדיים לקיומם של קשיי חקירה פלילית במרחב הסייבר הוא כי חקירות במרחב הממוחשב מצריכות **מומחיות טכנית גבוהה** בתחום הרשתות ותקשורת נתונים, ומומחיות זו אינה תמיד מצויה דייה בקרב רשויות החקירה.[64] בשל התפתחות המחשוב, ובעיקר בשל התפשטות האינטרנט, התפתח ענף חדש בתחום החקירה הפלילית שעניינו פורנזיקה של חקירות מחשב (Computer forensics או Cyber forensics).[65] המחוקק הישראלי הכיר למשל בדרישת מיומנות לחוקר המבצע פעולות של חדירה לחומר מחשב,[66] אולם החוק

בעת שהגיע בעל חברת ההימורים לביקור בישראל, עוכב לחקירה בגין ביצוע לכאורה של עברת ארגון הימורים. במקרה זה עוררה ההגנה את עניין הפליליות הכפולה וציינה כי כיוון שבמדינת מושבו של השרת מותרים ההימורים, הרי שאי אפשר לעכב את בעל החברה לחקירה. השאלה צפה במידה רבה בעקיפין, שכן לא דובר בהליך הסגרה ממדינה אחרת למדינת ישראל, כי אם בעיכוב לחקירה של החשוד בעת שהגיע לישראל. אולם בהליך הסגרה, כמו גם במסגרת הגשת בקשה לעזרה משפטית, או כאשר מבקשים להעמיד לדין נאשם בישראל על "עברת חוץ", נדרשת הוכחת פליליות כפולה, במובן זה שהמעשה ייחשב עברה על פי דיני המדינה הזרה. ראו סעיף 14(ב) לחוק העונשין, התשל"ז–1977 (להלן – חוק העונשין); סעיף 8 לחוק עזרה משפטית; סעיף 2(א) לחוק ההסגרה, התשי"ד–1954. על כן, ובהמשך לדוגמה בעניין קרלטון, אילו היו מבקשים להסגיר את החשוד מחו"ל לישראל בטענה שביצע עברות הימורים בישראל, היה אז מקום להוכיח "פליליות כפולה", ולבחירתו של החשוד למקם את שרתיו דווקא בגיברלטר הייתה השלכה ניכרת על תוצאת הבקשה.

64 ראו מחקר ה־UNODC, לעיל ה"ש 29, בעמ' 152–156. בנוסף, גם בקרב חוליות ההמשך בשרשרת האכיפה הפלילית – רשויות התביעה ולבסוף בתי המשפט – חסרה מומחיות טכנית בניתוח, בהגשה ובעיבוד של הראיות הדיגיטליות. ראו מחקר ה־UNODC בעמ' 172–178.

65 כדוגמה בלבד, ראו LINDA VOLONINO, REYNALDO ANZALDUA & JANA GODWIN, COMPUTER FORENSICS: PRINCIPLES AND PRACTICE 22–52 (2006), שם מתארים המחברים את התפתחות התחום כתחום פורנזי עצמאי בעבודת המשטרה. כדוגמה למדריכי שטח לחוקרי משטרה בזירה האינטרנטית, ראו BRUCE MIDDLETON, CYBER CRIME INVESTIGATOR'S FIELD GUIDE (2nd ed., 2005); ALBERT J. MARCELLA & ROBERT S. GREENFIELD (EDS.), CYBER FORENSICS: A FIELD MANUAL FOR COLLECTING, EXAMINING AND PRESERVING EVIDENCE OF COMPUTER CRIMES (2002).

66 ראו סעיף 23א(א) לפסד"פ. "בעל תפקיד מיומן" אינו מוגדר בפסד"פ או בשום חוק אחר. המשטרה, ובעקבותיה המשטרה הצבאית החוקרת (מצ"ח), הנהיגו קורס לחקירות מחשב.

nevo.co.il

אינו מתייחס למידת המיומנות הדרושה. הפסיקה פירשה את דרישת המיומנות כדרישה גמישה, התלויה בטיב פעולת האיסוף שביקש החוקר לבצע ובמידת מורכבותה.[67] בשל הקצב המואץ של ההתפתחות הטכנולוגית, המחייב את החוקרים הפליליים להכשרה מתאימה, ובשל ההכרח לאסוף ראיות מבלי לזהם את הזירה הממוחשבת, מבלי לשבש את טיב הראיה המבוקשת ומבלי להתערב בגרסתה המקורית, הרי שפער האכיפה רק הולך וגדל.[68]

הטעם השני הוא כי קיימת טענה שמבנה המשטרה ותפישת ההפעלה שלה אינם מתאימים לחקירות בזירת הסייבר. ההסבר לכך הוא שהמשטרה המקצועית־המודרנית פותחה להתמודדות עם עברות המרחב הפיזי, והיות שהפשיעה המקוונת היא בעלת כמה מאפיינים שונים מהפשיעה במרחב הפיזי, הרי שהמשטרה נדונה לכישלון מראש בנסותה להתמודד עמה. כך למשל סוזן ברנר (Brenner) טענה כי המשטרה המקצועית המודרנית מניחה כי הפשע ניתן למיקום פיזי, הוא מוגבל מבחינת היקפו ואופן ביצועו למגבלות העולם הפיזי, הוא מוגבל מבחינת מספר הנפגעים הפוטנציאליים לפי המגבלות הפיזיות, והוא מאופיין דמוגרפית וגאוגרפית (אזורי פשיעה). על כן המשטרה מתמקדת בפורנזיקה של ניתוחי זירה (CSI) ובמיקוד מראש של מאמצי השיטור לאזורים מסוימים.[69] הנחות אלה אינן מתקיימות במרחב המקוון, שבו הפשיעה אינה ניתנת למיקום, היא אינה ממוקדת גאוגרפית, היא אינה מוגבלת מבחינת ההיקף ומספר הנפגעים היות שהפשיעה היא אוטומטית ובעלת פוטנציאל לשכפל את עצמה ללא התערבות אנושית, ואין לה אפיון דמוגרפי או גאוגרפי מסוים. מכאן שאין מדובר רק בהכשרה טכנית של החוקרים אלא בשינוי מערכתי כולל יותר שנדרש לצורך שיטור במרחב הסייבר.

---

67 בעניין אריש נבחן מקרה שבו שוטר, שאינו חוקר מחשבים, חדר לטלפון סלולרי של חשוד לצורך עיון ותיעוד של מסרוני SMS שהיו שמורים במכשיר. ת"פ (מחוזי י-ם) 2077/06 **מדינת ישראל נ' אריש** (פורסם בנבו, 6.3.2007). השופטת בן־עמי כתבה: "...אף בהנחה כי טלפון סלולארי עונה על הגדרת מחשב, במישרין או בעקיפין, ברור כי לצורך הפקת מידע ממנו, כגון: רשימת שיחות נכנסות ויוצאות, מיסרונים שנשלחו וכו', אין צורך במיומנות מיוחדת מעבר למיומנות של אדם סביר... ובנסיבות אלו 'בעל תפקיד מיומן לביצוע פעולות כאמור' יכול להיות אף שוטר רגיל". למעשה, נובע מדבריה של השופטת בן עמי כי "בעל תפקיד מיומן" הוא מושג גמיש ולא קבוע, וכגודל המשימה הפורנזית בחומר המחשב, כך גודל המיומנות שתידרש מחוקר המחשבים. מכאן שקורס חקירות מחשב של המשטרה אינו בהכרח מקנה מיומנות לכל פעולות איסוף הראיות הדיגיטליות, כפי שאי־השתתפות בקורס אינה בהכרח שוללת מיומנות לכל הפעולות. בהמשך לכך, אם יידרש חוקר מחשבים לבצע פעולה חקירתית מתוחכמת, כגון התקשרות למחשב מרחוק, הורדת החומר, פיצוח הצפנתו ומיונו, ייתכן בהחלט שתעודת חוקר המחשבים המיומן לא תספיק כדי להוכיח מיומנות מספקת להתמודדות עם המשימה. "בעל תפקיד מיומן" ייחשב מי שיוכיח בבית המשפט שמומחיותו מתאימה למשימה, בדומה לנעשה לגבי עדים מומחים אחרים הבאים בפני בית המשפט, וכשלב מקדמי נדרשים להוכיח את מומחיותם לפי הפעולה שעליה הם מתבקשים להעיד. לעומת זאת דפדוף בספר טלפונים במכשיר טלפון נייד או קריאת תכתובות דוא"ל האגורות במחשב אינם פעולות המצריכות מיומנות מיוחדות, שכן הן פעולות המתבצעות כעניין שבשגרה בידי כל אדם, וייתכן ששוטר שאינו בעל תעודת "חוקר מחשבים מיומן" יוכל לבצעה כראוי.

68 ראו למשל YEE FEN LIM, CYBERSPACE LAW: COMMENTARIES AND MATERIALS 256–257 (2003); CHRIS REED & JOHN ANGEL (EDS.), COMPUTER LAW 585–586 (6th ed., 2007). כן ראו McAffee Virtual Criminology Report, לעיל ה"ש 34, בעמ' 14–16. עוד על הפיגור המובנה של המשטרה אחר התפתחות הפשיעה המקוונת, ראו Marc C. Goodman, *Why the Police Don't Care About Computer Crime,* 10 HARV. J. L. & TECH. 465, 482–488 (1997).

69 ראו Brenner, *Toward a Criminal Law for Cyberspace*, לעיל ה"ש 21, בעמ' 62.

nevo.co.il

קוזלובסקי התייחס גם הוא לתפישת ההפעלה של חוקרי המשטרה. הוא אפיין את מודל החקירה הפלילית הנוהג על פי המאפיינים האלה: **האחד**, הדגש מושם על מבצע העברה; **השני**, המשפט הפלילי נתפש כגורם המרתיע הבלעדי מפני ביצוע עברות פליליות; **השלישי**, הקרבן נתפש כפסיבי ואין לו מעמד בכל הנוגע לתגובה לעברה הפלילית שבוצעה כלפיו או למניעתה; **הרביעי**, החקירה מתבססת על ראיות, והמטרה היא לאספן על מנת להציגן בבוא העת לבית המשפט; **החמישי**, קיים שיקול דעת לגורמי החקירה והתביעה אם לפתוח בחקירה או להגיש כתב אישום בכל מקרה שמובא בפניהם; **השישי**, אם וכאשר הנאשם מורשע בעקבות החקירה הפלילית, מוטל עליו עונש.[70] לטענת קוזלובסקי, מודל זה אינו מתאים למאפייני הפשיעה בזירה המקוונת, שהיא כאמור דיגיטלית, אנונימית, מבוזרת, מודולרית, בין־לאומית, חשאית, מידית, אוטומטית ומתפשטת.[71] ברנר וקוזלובסקי הסיקו מניתוחיהם שיש לשנות את שיטת השיטור ולזנוח את המודל של חקירה פלילית לאחר ביצוע העברה, ההעמדה לדין והענישה.[72] לעומתם, אבקש להציג טענה שונה, ולפיה אין צורך לזנוח את מודל החקירה הפלילית הקלאסית אלא יש לשמרו תוך עריכת שינויים בתפישות של הדין המסדיר את החקירה הפלילית בזירה המקוונת.

הטעם השלישי הוא כי רשויות האכיפה והתביעה נאלצות **להזניח יחסית את החקירות בזירת הסייבר** אל מול שאר המשימות המוטלות עליהן.[73] זירת הסייבר נתפשת כווירטואלית, וקיימת נטייה לשוות לנזקים הנגרמים במרחב הסייבר משקל פחות. חלק מן העברות בזירה הממוחשבת נדחקות בתחתיתו של סולם סדר העדיפויות של רשויות האכיפה.[74] הבעיה מחריפה במיוחד כשמדובר בצורך בחקירת חשיפה בזירה האינטרנטית, כלומר חקירות שנערכות שלא על פי תלונה או הנחיה מגבוה לפתיחה בחקירה ושלא בעקבות התרחשות אירוע מסוים ש״זועק״ לחקירה (חקירת זירה). חקירות החשיפה הן מורכבות ויקרות יותר ואין הן מניבות תוצאות

---

70 ראו Kozlovski, לעיל ה״ש 13, בעמ׳ 106—107.

71 ראו שם, בעמ׳ 48—102. כן ראו התייחסותי לעיל בפרק המבוא, טקסט לה״ש 56.

72 ברנר הציעה לעבור למודל של אבטחה מבוזרת, מעין מנגנון של עזרה עצמית מגוננת בתמיכה ארגונית ומדינתית. ראו Brenner, *Toward a Criminal Law for Cyberspace*, לעיל ה״ש 21, בעמ׳ 80—110. קוזלובסקי הציע מודל מניעתי משולב, ראו Kozlovski, לעיל ה״ש 13, בעמ׳ 161—258. קוזלובסקי חזר מאוחר יותר על עיקרי המודל: נמרוד קוזלובסקי ״האם ניתן להתמודד עם הפשיעה ברשתות האפלות?״ **חורים ברשת** http://www.holesinthenet.co.il/archives/35306 (1.1.2012).

73 ראו McAffee Virtual Criminology Report, לעיל ה״ש 34, בעמ׳ 3. עוד ראו ביקורת על שאין מוקדשים מאמצים מספיקים לחקירת עברות פליליות בעולמות וירטואליים (Virtual worlds) באינטרנט (הכוונה לאתרים שקיימת בהם תקשורת בין־אישית בין כמה משתמשים העוטים על עצמם זהות פסידונימית ומנהלים אינטראקציות מורכבות ונמשכות כביקום מקביל), ראו Benjamin Tyson Duranske, Virtual Law: Navigating the Legal Landscape of Virtual Worlds 198–200 (2008). להתבוננות כללית על העומס על מערכת אכיפת החוק הפלילי בהקשר כללי והסיבות לו, ראו למשל אורן גזל־אייל **ענישה בהסכמה – חלופות להליכי משפט בפלילים** 37—43 (חיבור לשם קבלת תואר ״דוקטור לפילוסופיה״, אוניברסיטת חיפה, 2002).

74 ראו התייחסות אצל אסף הרדוף **הפשע המקוון** 266 (2010) וההפניות המובאות שם. ראוי לציין כי בעת האחרונה חל שינוי בנקודה זו מבחינת משטרת ישראל, בשל הקמתה של יחידה ארצית לחקירת פשעי סייבר תחת יחידת החקירות הארצית להב 433. מפכ״ל המשטרה הכריז על הקמת היחידה בסוף שנת 2012. ראו למשל חן מענית ״מוטב מאוחר: דנינו הכריז על הקמת יחידת סייבר במשטרה״ **גלובס Online** (12.11.2012) http://www.globes.co.il/news/article.aspx?did=1000797583. היחידה החלה לפעול בשנת 2014.

nevo.co.il

מהירות. עם זאת חקירות החשיפה חיוניות היכן שבהיעדרן יופקרו עברות פליליות מסוימות כלא מטופלות כלל או כעברות המטופלות חלקית בלבד (בנסיבות שבהן אין נדרשת חשיפה ביזמת המשטרה).

ניתן להניח כי במרחב הסייבר תהיינה חקירות החשיפה מורכבות עוד יותר בשל המאפיינים ה"מסבכים" הייחודיים של המרחב, הנוספים על המאפיינים ה"מסבכים" של חקירות החשיפה במרחב הפיזי: **האחד**, חלק מתופעות הפשיעה במרחב הסייבר כוללות פיזור הנזק שבהתנהגות העבריינית על פני מספר רב של קרבנות, כאשר מידת הנזק לכל קרבן בנפרד לא תהיה גבוהה מדי ולא תביאו לחצות את הסף של הגשת התלונה (בדומה למתרחש, למשל, במקרים של זיהום אוויר או במקרים המצדיקים תובענות ייצוגיות);[75] **השני**, לעתים הקרבן במרחב הסייבר אינו יודע שנפגע בפועל מעברה, כיוון שהעברה התבצעה ללא מגע כלשהו עמו ובאמצעים אוטומטיים;[76] **השלישי**, ספקי שירות רבים הנופלים קרבנות לעברות של האקינג, מתקפות DDoS וכדומה יחששו לחשוף את דבר פגיעותם על דרך של הגשת תלונה למשטרה מחשש לבריחת לקוחות.[77]

לסיכום, במצב המשפטי הקיים ניתן להגיע לכלל מסקנה כי הפשיעה במרחב המקוון גואה, וכי רשויות החקירה אינן מטפלות בה כדבעי. רשויות החקירה מוגבלות בפעולתן במרחב לעומת פעולתן במרחב הפיזי ממכלול של סיבות שעליהן עמדתי. מכאן שקמה לכאורה הצדקה לחיפוש חלופות לאכיפה הפלילית המדינתית הנוהגת כיום בעברות פליליות במרחב הסייבר. ההצדקה היא במישור של יעילות האכיפה. כאן המקום לציין כי ניתן בהחלט להעלות הצדקות לכאוריות אחרות לבדיקת חלופות לאכיפה הפלילית המדינתית. הצדקות אלה נובעות מפרדיגמת המחקר של משפט וטכנולוגיות מידע, שעליה עמדתי בפרק המבוא, ולפיהן ייתכן ששינויים בשיווי המשקל בין המשפט, הערכים החברתיים, כוחות השוק והארכיטקטורה יובילו לשינויים באופן ההסדרה של התנהגות הפרט. על פי קו טיעון אחד, בשל שינויים משמעותיים בארכיטקטורת הרשת, ניתן כיום לשקול חלופות אכיפה ארכיטקטוניות שיביאו למניעת ההתנהגות המזיקה מראש או לסיכולה במהלך התרחשותה.[78] על פי קו טיעון אחר, ארכיטקטורת הרשת והשלכותיה על התפתחויות כלכליות וחברתיות מאפשרת יצירת חלופות הפללה פוגעניות פחות. כיוון שהשימוש בכלי הפלילי צריך להיות המוצא האחרון, הרי שחלופות ההפללה מביאות

---

75 כדוגמאות ניתן לציין את התופעה של הפצת דוא"ז המגיע לרבבות משתמשי אינטרנט, או מקרה של השתלטות על מספר רב של מחשבים לצורך "גיוסם" למתקפות DDoS. ההשתלטות עצמה על אותם מחשבים היא עברה פלילית של חדירה לחומר מחשב שלא כדין כדי לעבור עברה אחרת, לפי סעיף 5 לחוק המחשבים, התשנ"ה–1995, כאשר דבר ההשתלטות אינו מורגש בפועל.

76 לאפיון זה ראו למשל, Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, 4 N.C.J.L. & Tech. 1, 26–27 (2002). כדוגמאות למצבים בהם הקרבן אינו מודע לפגיעה בו, ניתן לציין עברות של פגיעה בפרטיות, כגון ציתות לתקשורת אינטרנט, קריאת הודעות דוא"ל של אחר, הפעלת סוסים טרויאניים לצורך גנבת מידע.

77 ראו לעיל ה"ש 30.

78 ראו למשל Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 Yale L.J. 2261 (2003), שם מצביע קטיאל על האפשרויות החדשות שארכיטקטורת האינטרנט פותחת בפני מי שמבקשים למנוע עברות או לסכלן בעת הוצאתן אל הפועל. כן ראו Kozlovski, לעיל ה"ש 13, בעמ' 287–290.

nevo.co.il

לדה־קרימינליזציה של המעשה.[79] על אף האמור אני סבור כי למרבית העברות במרחב המקוון לא תימצאנה הצדקות רבות לדה־קרימינליזציה,[80] ולפיכך הטעם של מוגבלות רשויות החקירה ימשיך לעמוד כטעם המרכזי לאיתור חלופות לאכיפה הפלילית המדינתית.

אבחן להלן את החלופות המוכרות לאכיפה הפלילית המדינתית במרחב הסייבר. אחלק את החלופות לשתיים: חלופות **לאכיפה הפלילית** וחלופות **לאכיפה המדינתית**. החלופות מהקבוצה הראשונה מתייחסות לעצם הבחירה בהפללה, הכוללת איסור, העמדה לדין והטלת סנקצייה עונשית על המורשים, והחלופות מהקבוצה השנייה מתייחסות לזהות הגורם האוכף בפועל ומציעות גופים אחרים לביצוע עבודת החקירה (כחלק מהאכיפה הפלילית) זולת המדינה.

ד. הצעות לאכיפה לא־פלילית במרחב הסייבר

1. אי־אכיפה

א) הצגת החלופה

בתגובה לחקיקת ה־Communications Decency Act (CDA) ב־1996, החוק האמריקני הראשון שביקש להטיל חובות של סינון תכנים פוגעניים באינטרנט, פרסם הפובליציסט ג'ון פרי בארלו, מייסד ה־Electronic Frontier Foundation,[81] מאמר בשם "הכרזת העצמאות של מרחב הסייבר". מאמר עיתונאי זה הציע כי המרחב האינטרנטי יהיה מחוץ לגבולות המשפט, מכל סוג שהוא, וכי יחלשו עליו כללים של אתיקה תחת כללים משפטיים, אשר יש בהם משום כפייה.[82] במושגי הגישה הלסיגיאנית, שתיארתי בפרק המבוא, בארלו למעשה הציע שאת הריק המשפטי באינטרנט ימלאו כוחות השוק, הנורמות החברתיות והארכיטקטורה או הטכנולוגיה עצמה, כגורמי ההסדרה הנוספים להתנהגות הפרטים ברשת. מצדדי הגישה של אי־האכיפה נטו להדגיש את אלמנט השוק החופשי (laissez-faire) באינטרנט,[83] שלפיו משתמשי האינטרנט יעברו מאתר אינטרנט אחד למשנהו, ובכך יבחרו למעשה את מערכת הכללים שאליהם הם רוצים להיכפף.

---

79 ראו JEREMY BENTHAM, THEORY OF LEGISLATION 199 (reprinted, 1975). השימוש במשפט הפלילי נתפש כמוצא אחרון, "Ultima Ratio Regum". עוד על ההכרח בבחינת חלופות פוגעניות פחות מהמשפט הפלילי בטרם הפללה (Criminalization) של התנהגות מסוימת, ראו JONATHAN SCHONSHECK, ON CRIMINALIZATION: AN ESSAY IN THE PHILOSOPHY OF THE CRIMINAL LAW 63–99 (1994); DOUGLAS HUSAK, OVERCRIMINALIZATION – THE LIMITS OF THE CRIMINAL LAW 153–158 (2008); הרדוף, לעיל ה"ש 74, בעמ' 77—85, 100.

80 זו גם מסקנתו הכללית של הרדוף, לעיל, בספרו המוקדש לבחינה מעין זו של הפשע המקוון.

81 מדובר בארגון ללא מטרות רווח, שייסד בארלו בארצות הברית בשנת 1990 בשיתוף עם מיטש קאפור (Kapor) וג'ון גילמור (Gilmore). מטרות הארגון: עידוד חופש השימוש באמצעי טלקומוניקציה וחיזוק מעמדו של חופש הביטוי והזכות לפרטיות באמצעי הטלקומוניקציה, באמצעות הסברה, מימון פעילויות בתחום, התדיינויות משפטיות בנושאים אלה ועוד. כתובת אתר הארגון: https://www.eff.org.

82 ראו Barlow, לעיל ה"ש 1.

83 ראו DYSON, לעיל ה"ש 3, בעמ' 109. כן ראו Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. REV. 323, 350 (2003). יוער כי גייסט תיאר את גישת אי־האכיפה במונחים של גישה שחלפה מן העולם ונדונה בעבר עד אמצע שנות התשעים של המאה הקודמת. וראו גם את: Joel Reidenberg, *Choice of Law and*

מיקוד העדשה בגישת אי־האכיפה מלמד כי למעשה ניתן לבדל שני טיעוני אי־אכיפה השונים במהותם: **האחד**, טיעון נורמטיבי במהותו המבקש להגשים חזון ליברטריאני בזירה המקוונת. על פי עמדה זו, הזירה המקוונת אינה אלא הזדמנות נאותה להגשים מערכת אידאלית של חירות מפני התערבות כופה, ערך שהיה ראוי להגשימו ככל האפשר גם במרחב הפיזי;[84] **השני**, טיעון מעשי בעיקרו שלפיו ארכיטקטורת הרשת אינה מאפשרת אכיפה פלילית מדינתית יעילה. על פי טיעון זה, אי־אכיפה היא מצב דברים נתון ולאו דווקא מצב דברים ראוי.

ב) הערכת החלופה

ניל נתנאל (Netanel) כינה את טיעוני אי־האכיפה של האינטרנט "Cyberanarchism". נתנאל תקף את הטענה של מצדדי אי־האכיפה כי משתמשי הרשת עוברים בין האתרים השונים כאקט פוליטי של בחירת ה"משטר" הרצוי להם. לטענתו אין לראות בבחירה כזו של משתמשי האינטרנט אלא עניין פרוזאי הרבה יותר של צרכנות תקשורת ותכנים. נתנאל הוסיף וטען כי שוק הגישה לאינטרנט, החיפוש באינטרנט ותוכני האינטרנט מתחילים להתגבש בכיוונים של הגבלות על תחרות, מיזוגים וקרטלים, ומכאן שמעשית חירות הבחירה של משתמשי האינטרנט מוגבלת.[85]

הרעיון בדבר אי־אכיפה חיצונית במרחב המקוון מניח במידה רבה בידול של המרחב המקוון מהמרחב הפיזי. כפי שציינתי בפרק המבוא (תרשים 1.1), הפעילות העבריינית במרחב הסייבר אינה נותרת אך ורק בזירת הסייבר.[86] יש לה השלכות בעולם הפיזי כאשר מדובר בביצוע עברות מסתייעות־מחשב המושלמות מחוץ למרחב הממוחשב. מלבד זה יש לה השלכות בעולם הפיזי גם כאשר כל העברה בוצעה בתוככי המרחב הממוחשב, כיוון שנזק וירטואלי הוא נזק ממשי גם למשתמש המחשב. כך למשל הפסד כספי באתר הימורים וירטואלי הוא הפסד כספי אמתי למהמר; הטרדה מינית במסגרת צ'אט אינטרנטי היא הטרדה מינית של אדם העומד מאחורי המחשב. גם כאשר מדובר בעברות נגד מחשב ונגד חומר המחשב, אשר באו לעולם אך ורק בעידן המחשב והאינטרנט, לעברות אלה יש משמעות בעולם הפיזי: מדובר בגרימת הפסדים כלכליים למחשבים ולשרתים הניזוקים, וכשמדובר בפגיעה במידע אישי, זוהי עוולה בעלת השלכות לא־ממוניות. מכאן שהחתירה להוצאת המשפט מהמרחב המקוון מתעלמת מהמציאות המקוונת כהווייתה. היא מגלמת עמדה הנדמית כיום כשגויה באשר למשמעותו של המרחב המקוון בחיי המעשה. יתרה מזאת, הסדרה כופה במרחב הסייבר הולכת ומתרבה, ומכאן שאי־אכיפה, כמצב דברים נתון, הופכת ללא יותר מעמדה אוטופית, בבחינת סמן קצה לערכים של חופש הגישה, השימוש והביטוי במרחב המקוון.

Jurisdiction on the Internet: Technology and Internet Jurisdiction, 153 U. PA. L. REV. 1951, 1952 (2005).

84 ראו למשל Dan L. Burk, *Federalism in Cyberspace*, 28 U. CONN. L. REV. 1095 (1996); David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155 (1997).

85 ראו Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 433–443 (2000).

86 ראו גם Beryl A. Howell, *Real World Problems of Virtual Crime*, 7 YALE L.J. & TECH. 103 (2004–2005), שם מדגים המחבר כיצד פעילות מקוונת יכולה להסב נזק ממשי לקרבנות לא מקוונים.

nevo.co.il

2. אכיפה מגוננתית־וולונטרית

א) הצגת החלופה

התגוננות עצמית אינה ייחודית לפשיעה במרחב הסייבר, ולמעשה היא שכיחה גם בעולם הפיזי (לדוגמה, נעילת בתים וכלי רכב, בניית חומות שתקשינה על פריצה, הימנעות מהסתובבות מאזורים המועדים לפשיעה, לבישת אפוד מגן ועוד אין־ספור דוגמאות).[87] במרחב הסייבר פותח מגוון כלים של מיגון שמטרתם למנוע את הפגיעה מהתנהגות מזיקה, בין בדרך של הרתעה מראש של מבצע העברה מפני עצם ביצועה ובין בדרך של סיכול הנזק לאחר תחילת הביצוע של העברה. כלים אלה מנצלים את הארכיטקטורה של המרחב הקיברנטי לטובת התגוננות.[88]

במסגרת החלופה דנן יש למנות את כל הפעולות הוולונטריות למניעת נזקים מביצוע עברות פליליות במרחב הסייבר.[89] הפעולות הוולונטריות יכולות להיות עצמיות או קבוצתיות, הן יכולות להיות בשביל משתמש האינטרנט עצמו או בשביל אחרים כגון ילדיו, עובדיו (אם מדובר במקום עבודה) והבאים בשעריו (אם מדובר במוסד או בית עסק כלשהו המציע שירותי אינטרנט). בין הפעולות העצמיות והקבוצתיות הקלאסיות ניתן לציין פעולות של התקנת תוכנות אנטי־וירוס, "חומת אש" (Firewall), תוכנות לניטור עצמי על מנת לבדוק אם יש חדירה או

---

87 ראו Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039, 1046–1073 (2001). חיבורו זה של קטיאל נסמך בין היתר על עבודתה המוקדמת יותר של ג'יין ג'ייקובס (Jacobs), אשר תקפה את תכנון הערים והשיקום העירוני בארצות הברית. ראו ג'יין ג'ייקובס מותן וחייהן של ערים אמריקאיות גדולות (מתרגמת מרים טליתמן, 2008) (החיבור נכתב במקור בשפה האנגלית בשנת 1961). ג'ייקובס כתבה: "הדבר הראשון שיש להבין הוא ששלום הציבור בערים... אינו נשמר בעיקרו על ידי המשטרה, נחוצה ככל שתהיה. הוא נשמר בראש ובראשונה על ידי רשת מורכבת, בלתי מודעת כמעט, של בקרות ואיזונים וולונטריים, המופעלים על ידי התושבים עצמם" (שם, בעמ' 56). בקרימינולוגיה פותחו שתי גישות למניעת פשיעה באופן ארכיטקטוני: Crime Prevention Through Environmental Design (CPTED) וכן Crime Reduction Through Production Design (CRPD). לסקירת הגישה הראשונה ראו למשל TIM CROWE, CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (2nd ed., 2000), ולסקירת הגישה השנייה ראו למשל RONALD V. CLARKE & GRAEME R. NEWMAN, DESIGNING OUT CRIME FROM PRODUCTS AND SYSTEMS (2005). גישות אלה מתכתבות עם התאוריה הקרימינולוגית הנקראת Situational Crime Prevention. על פי תאוריה זו, שפיתח במקור רונלד קלארק (Clarke), ניתן להניח את המוטיבציות של העבריינים כנתונות, והמטרה היא לפתח כלים מוסדיים וחברתיים להפחתת האטרקטיביות של הפשיעה. בחינת הפשיעה מתמקדת בסיטואציות הספציפיות שבהן נעברות העברות, והמטרה היא לשנות את המרכיבים הפיזיים והחברתיים של הסיטואציות הללו על מנת להפחית את האטרקטיביות של ביצוע העברות במהלכן. ראו Ronald V. Clarke, *Situational Crime Prevention: Theory and Practice*, 20 BRITISH J. CRIM. 284 (1980). המתודולוגיה המקובלת במסגרת גישה זו היא של בחינה case-by-case, בגלל האופי הנסיבתי של הגישה. ראו למשל RONALD V. CLARKE (ED.), SITUATIONAL CRIME PREVENTION: SUCCESSFUL CASE STUDIES (2nd ed. 1997). לכתיבה ברוח גישה זו בעידן האינטרנט ראו GRAEME R. NEWMAN & RONALD V. CLARKE, SUPERHIGHWAY ROBBERY – PREVENTING E-COMMERCE CRIME (2003). הגישה של לסיג, שלפיה הארכיטקטורה של המרחב המקוון מעצבת את כללי ההתנהגות של הפרטים בה, למעשה דומה במהותה לגישות הארכיטקטוניות לפשיעה. להבחנה זו, ראו Richard Jones, *Cybercrime and Internet Security*, *in* LAW AND THE INTERNET 601, 611–612 (Lilian Edwards & Charlotte Waelde eds., 3rd ed. 2009).

88 ראו Katyal, לעיל ה"ש 78, בעמ' 2263–2282; Kozlovski, לעיל ה"ש 13, בעמ' 237–241.

89 פעולות מגוננתיות המבוצעות באמצעות הוראות דין מחייב תימנינה בתת־הפרק הבא.

nevo.co.il

זליגת מידע, התקנת תוכנות לסינון תכנים פוגעניים על פי הגדרת המשתמש או שימוש בשירותי חיפוש מסוננים,[90] שימוש בהצפנות ובהגנת ססמאות לצורך מניעת סיכול עברות של גנבת מידע ממוחשב באמצעות חדירה לא מורשה מרחוק ועוד.

באכיפה מגננתית־וולונטרית ה״שחקן״ המרכזי הוא משתמש המחשב הבודד. עם זאת, לצדו, גם ספקיות השירות יכולות להחליט על אכיפה מגננתית־וולונטרית המשליכה על כלל המשתמשים בשירותיהן. כך למשל ניתן לציין את המערכות של סינון דואר הזבל (דוא״ז – Spam) שמפעילות ספקיות השירות. האינטרס להתגונן כאן הוא של ספקיות השירות עצמן לא פחות משל לקוחותיהן. פעולתן נגזרת מאינטרס זה והיזמה לפעולה בעניין זה היא שלהן. עוד ניתן לציין את הכללים להסדרה עצמית של תוכן משתמשים באינטרנט, שנערכו בידי איגוד האינטרנט הישראלי בשיתוף עם אתרי האינטרנט הישראליים הגדולים הכוללים תוכן משתמשים (תגוביות (טוקבקים), פוסטים וכו׳).[91] כללים אלה קובעים קריטריונים לסינון תכנים פוגעניים של משתמשי אינטרנט. טל ז׳רסקי ציין כי ספקי השירות הגיעו למסמך כללים זה בשל חשש מהצעת חוק פרטית שהציעה לכפות עליהם בחקיקה חובות נרחבות לפיקוח על תוכני גולשים,[92] ומכאן שבמידה מסוימת מתערער יסוד הוולונטריות, וניתן להציג את המהלך כמהלך כופה, גם אם סמוי במידת מה, של המדינה.[93]

בתחום הפדופיליה המקוונת מוכרת תופעה של ארגונים ללא מטרת רווח ששמו להם למטרה לסרוק את הפעילות באינטרנט ולדווח לספקיות הגישה לאינטרנט על אתרי אינטרנט שמצוי בהם תוכן פדופילי.[94] במקרה כזה ספקיות הגישה לאינטרנט ייטו להסיר את התכנים הפוגעניים מבלי להידרש לשאלת חוקיות הפרסום. הדבר בר־ביצוע כשמדובר בתכנים פדופיליים מובהקים, שנמצאים מחוץ לגדרי חופש הביטוי אליבא דכולי עלמא, אולם אם ידובר בפרסומים

---

90 קיימות אפשרויות סינון תכנים במערכות הפעלה, ברמת ספק הגישה לאינטרנט וברמת המשתמש עצמו המתקין תוכנה במחשבו. לאפשרויות לפיקוח הורי (Parental control) במערכת ההפעלה ״חלונות ויסטה״, ראו http://windows.microsoft.com/en-US/windows7/products/features/parental-controls. כדוגמה לשירות סינון תכנים לא רצויים ברמת ספק הגישה לאינטרנט, ראו למשל מערכת Ynet ״נטוויז׳ן השיקה שרות סינון תכנים״ **Ynet** (30.6.2003) http://www.ynet.co.il/articles/0,7340,L-2675037,00.html; כן ראו שירות בקרת ההורים של Smile 012 ב: http://www.012.net/productslist.aspx?docID=8592&FolderID=188&lang=he&tabn=4. כדוגמאות לתוכנות סינון להתקנה עצמית, ראו www.netnanny.com; www.cybersitter.com; www.cyberpatrol.com. ראו גם את אופציית ה־Safe search for Google images של גוגל http://support.google.com/images.

91 ראו ״כללים להסדרה עצמית של תוכן משתמשים באינטרנט״ **איגוד האינטרנט הישראלי** (2008) http://www.isoc.org.il/docs/Rules-Self_regulation_users_content.pdf.

92 ראו טל ז׳רסקי ״שקיפות בסינון תכנים: הצעה לפעולה״ **חוקים** ב 133, 147 (2010). הצעת החוק הפרטית שעליה דיבר ז׳רסקי היא הצעת חוק בדבר אחריותן המשפטית של הנהלות אתרי האינטרנט על דברי הגולשים המגיבים באתריהן (תיקוני חקיקה), התשס״ח–2007, ה״ח פ/3171/17 (ח״כ ישראל חסון).

93 אדון באכיפה מגננתית־כופה להלן בפרק ב.ד.4..

94 לדיון בשיטת אכיפה זו, ראו למשל Yaman Akdeniz, *Controlling Illegal and Harmful Content*, *in* CRIME AND THE INTERNET 113, 121–124 (David S. Wall ed., 2002). לעמותות העוסקות בעזרה עצמית בנושאי פדופיליה מקוונת, ראו למשל Internet Watch Foundation באתר האינטרנט: http://www.iwf.org.uk/; Family Watchdog באתר האינטרנט: http://www.familywatchdog.us/; Enough is Enough באתר האינטרנט: http://www.enough.org/; International Association of Internet Hotlines (Inhope) באתר האינטרנט: http://www.inhope.org/gns/home.aspx.

nevo.co.il

פורנוגרפיים "רגילים", או בפרסומי הסתה, הימורים מקוונים וכיוצא באלה תופעות, שהאיסור בעניינם הוא גמיש ותלוי במקום, בזמן, בנסיבות הפרסום ובקהל היעד שלו, הרי ששיטת הדיווח של ארגונים ללא מטרת רווח עשויה להיתקל בקשיים משפטיים. ספק גישה לאינטרנט שיסיר את הקישורית לאתרים מסוג זה עלול למצוא עצמו כמי שגרם נזק לבעל האתר המוחרם, שיטען לפגיעה אסורה בחופש הביטוי שלו, ואם מדובר באתר מסחרי – תעלה טענה לפגיעה גם בחופש העיסוק שלו.

מלבד הדיווח על אתרים פוגעניים לצורך הסרתם בידי ספקיות הגישה לאינטרנט, ארגוני "עזרה עצמית" אלה מפרסמים מאגרי מידע הכוללים כתובות של אתרי אינטרנט המציגים תוכן פדופילי, וכן מאגרי שמות ופרטים מזהים נוספים של פדופילים מורשעים. בנוסף, הם מנהלים מעין "משמר אזרחי" בתוך חדרי צ'אט לזיהוי פדופילים הפועלים און־ליין. חלק מאותם ארגונים לא רק משגיחים על הנעשה בחדרי הצ'אט השגחה פסיבית, אלא הם אף פועלים כסוכנים באותם חדרים, ובמקרה של חשיפה להטרדה מינית מצד משתמש אינטרנט אחר, הם מבצעים פעולת חשיפה והשפלה פומבית (Shaming), בבחינת סנקציה חברתית לצד הסנקציה הפלילית, שיכולה לבוא בעקבות המעשה.

ב) הערכת החלופה

לדידה של המדינה, התגוננות עצמית תמיד רצויה. ניתן להצדיקה במונחים מקרו־כלכליים, שכן משמעה הפחתת הפשיעה והוזלת עלויות האכיפה שבאחריות המדינה. גם מבחינתו של נפגע העבירה הפוטנציאלי ניתן להצדיקה במונחים רציונליים פשוטים: נוסחת ההרתעה של דיני העונשין מכוונת למבצע העבירה הפוטנציאלי ולא לקרבן.[95] במקרים של עבירות פליליות שכוללות פגיעה גופנית או פגיעה בכבוד ובשליטה העצמית, כגון עבירות מין ועברות של פגיעה בפרטיות, אין בפיצוי העונשי, ואף לא בפיצוי בתביעת הנזיקין המקבילה למשפט הפלילי, כדי לשפות את הנפגע על מלוא נזקו. זאת כיוון שחלק מהנזק אינו בר־כימות או שאינו ממוני מטבעו. על כן התגוננות עצמית עשויה להשתלם מבחינתו של נפגע העבירה הפוטנציאלי, המבקש להקטין את סיכוייו ליפול קרבן לביצוע העברות. יתרה מזאת, אפשר לחשוב על מודל שבו המדינה מממנת את ההתגוננות העצמית, במסגרת שינוי פרדיגמת השיטור מדגש על מבצע העבירה לדגש על הקרבן.

ברנר הציגה הצדקה נוספת להטלת נטל על הקרבן הפוטנציאלי להתגונן מפני עברות במרחב המקוון. על פי הסברה, בשונה מפשיעה במרחב הפיזי, שבה לאי־ההתגוננות של הקרבן יש מחיר שבו נושא בדרך כלל הקרבן בלבד, הרי שכאשר הפשיעה מתבצעת במרחב המקוון, למחיר אי־ההתגוננות של הקרבן יש השלכה גם על משתמשים אחרים ברשת. כדוגמה מביאה ברנר את מקרהו של אדם שאינו מגן על מחשבו מפני חדירות לא מורשות, ואדם אחר משתלט על מחשבו

95 לא ארחיב כאן על נוסחת ההרתעה והניסוחים השונים שהוצעו לה. ככלל, בין מרכיביה היחס בין סיכויי התפיסה של העבריין הפוטנציאלי ומידת העונש שיקבל אם ייתפס לבין התועלת שהעבריין הפוטנציאלי מפיק מביצוע העברה. הנקודה המרכזית לענייננו היא שנוסחת ההרתעה מוטה לכיוון העבריין הפוטנציאלי ולא לקרבן. לביקורת על הטיה זו ולהצעת מודל המכליל את הקרבן במשוואת ההרתעה הפלילית, ראו Omri Ben-Shahar & Alon Harel, *The Economics of the Law of Criminal Attempts: A Victim-Centered Perspective*, 145 U. PA. L. REV. 299 (1996).

ומבצע דרכו עבירות באינטרנט. במקרה זה הנפגעים, נוסף על משתמש המחשב הלא מוגן, הם גם משתמשי האינטרנט האחרים שכלפיהם פעל מבצע העבירות לאחר ההשתלטות על המחשב הלא מוגן.[96]

הצדקות מקרו־כלכליות לאכיפה מגננתית יכולות לכאורה להוביל למסקנה בדבר הצורך בחיוב משתמשי המחשב בהתקנת אמצעי אבטחת מידע. במסגרת זו הכוונה תהיה להפעלת אמצעי התגוננות מן הסוג שמניתי לעיל בהקשר הוולונטרי, אלא שפעולות אלה לא תבוצענה לא מיזמת משתמש המחשב אלא על פי הוראה מחייבת בדין או על פי תמריץ כלכלי לפעול כאמור באמצעות קביעת משטרי אחריות נזיקית ופלילית המושפעים מאופן התנהלות הקרבן: פיצוי ועונש מלאים על קרבן שהתגונן ופעל על מנת למנוע את העבירה והפחתת הפיצוי והעונש על קרבן שנמנע מלהתגונן כאמור.[97]

עם זאת, כפי שאטען להלן, **התגוננות עצמית אינה יכולה לבוא במקום אכיפה פלילית** אלא היא יכולה להיות **שיטה משלימה בלבד** לאכיפה הפלילית המדינתית הקלאסית:

ראשית, תמיד יימצאו נגיפי מחשב מתוחכמים שתוכנות האנטי־וירוס ו״חומות האש״ של המחשב אינן מגלות אותם.

שנית, גם הקרבן המוגן ביותר אינו יכול להיות מחוסן מפני עבריין שיחדור, במצג שווא, את המסננות הטכנולוגיות. הנדוס אנושי (Social Engineering) עשוי ״להפיל בפח״ גם את משתמשי המחשב הזהירים, שנוהגים להתגונן באמצעות ״חומות אש״ ותוכנות אנטי־וירוס.[98]

---

96 ראו Brenner, *Toward a Criminal Law for Cyberspace*, לעיל ה״ש 21, בעמ׳ 90–92.

97 לדיון מעין זה בהקשר של פשיעה במרחב הפיזי, ראו למשל Omri Ben-Shahar & Alon Harel, *Blaming the Victim: Optimal Incentives for Private Precautions against Crime*, 11 J. L. ECON. & ORG. 434 (1995). לטענת בן־שחר והראל, יש להפחית את מידת העונש לעבריינים שביצעו עבירות כלפי קרבנות אשר לא פעלו להתגוננות עצמית. בקביעת כלל זה, של רשלנות תורמת של הקרבן בפלילים, יתומרץ הקרבן להתנהגות מניעתית, אשר תביא לתוצאה יעילה יותר של מניעת פשיעה ותמנע מצבים של Moral hazard הקיימים לטענתם כיום בהתנהלותם של קרבנות בפלילים. לדיון באפשרות זו בהקשר של פשיעה באינטרנט, ראו Brenner, *Toward a Criminal Law for Cyberspace*, לעיל ה״ש 21, בעמ׳ 90–93, 94–99. ביטוי דומה לגישתם של ברנר, בן־שחר והראל, אם כי בהקשר של הדין המהותי ולא של שאלת הענישה, ניתן למצוא בדיון סביב היקף הפרשנות הראוי לעברה של חדירה שלא כדין לחומר מחשב (העברה על סעיף 4 לחוק המחשבים, התשנ״ה–1995 ומקבילותיה במדינות אחרות). קיימת מחלוקת אם אדם שנכנס לאתר אינטרנט או למחשב לא מאובטח, ללא הרשאה מפורשת לכך, ביצע עברת חדירה לחומר מחשב, או שמא תנאי לקיומה של העברה הוא שבוצעה חדירה תוך פריצת ״מנעול״ טכנולוגי מסוים (כגון עקיפת ססמת הגנה, התחזות כמשתמש מורשה והקלדת ססמתו וכיוצא בזה). ראו למשל Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003); מיכאל בירנהק ״משפט המכונה: אבטחת מידע וחוק המחשבים״ **שערי משפט** ד 315, 337–345 (2006). העמדה הגורסת שעל הקרבן לאבטח את מחשבו / אתר האינטרנט שלו כתנאי לכינון עברה של חדירה לחומר מחשב שלא כדין, למעשה מתמרצת בעקיפין את הקרבן להתגונן מפני חדירה.
מבחינה סיווגית חיוב משתמשי האינטרנט בהתגוננות עצמית כאמור כלול בקטגוריה שתידון להלן, של אכיפה מגננתית־כופה, ולא בקטגוריה הנוכחית של אכיפה מגננתית־וולונטרית, אלא שהבאתי את הדברים כאן מטעמי נוחות ובהירות מתודית בלבד.

98 אחת הדוגמאות המובהקות לכך טמונה בפרשת הסוס הטרויאני, שנחשפה בישראל במאי 2005. באותו מקרה נחשף כי מספר רב של תאגידים וכמה גורמים פרטיים נפלו קרבן למזימה שיטתית של החדרת סוסים טרויאניים למחשביהם. הסוס הטרויאני שבו דובר היה משוכלל למדי, בעל יכולות לביצוע העתקות ״חכמות״ של המידע ממחשבו של הקרבן כמו גם בעל יכולות ליצירת תיעוד ממחשבו של

nevo.co.il

שלישית, שיטת ההתגוננות העצמית אינה רלוונטית במצבים שבהם אין הקרבן יודע מבעוד מועד על קרבניותו הפוטנציאלית (דהיינו במקרה שבו הוא טועה או משוטה בעניין זה). כך הוא למשל כאשר הקרבן נכנסת לצ׳אט אחד־על־אחד עם אדם נוסף, שבשלב מסוים מטריד אותה מינית.

רביעית, שיטת ההתגוננות העצמית אינה רלוונטית במצבים שבהם הפשע מתבצע בין שני מעורבים בעסקת עברה, למשל במקרים של סחר בסמים באמצעות האינטרנט, הימורים באינטרנט, שיתוף בקבצים פדופיליים וכו׳. מדוגמה זו ומהדוגמה שהובאה לעיל בדבר הטרדה מינית בצ׳אטים, ניתן להסיק ששיטת ההתגוננות העצמית מניחה, ולפיכך מתאימה, לקרבן רציונלי ואקטיבי, המיומן בשימושי המחשב והאינטרנט והמבקש להתרחק מכל פעילות לא נורמטיבית.

חמישית, מלבד היותה של שיטת ההתגוננות העצמית לא רלוונטית לכל תופעות הפשיעה ולכל סוגי הקרבנות, יש לציין גם את המחיר הכלכלי והחברתי הכרוך ביישומה. ההתגוננות העצמית כרוכה בעלויות המושתות על משתמש המחשב הפרטי. ככל שרמת ההתגוננות תעלה, כן תגדלנה העלויות.[99]

שישית, חלק ממרכיבי ההתגוננות העצמית, הכוללים סינון תכנים או הימנעות מכניסה לאתרים מסוימים מחשש ליפול קרבן לעברות מחשב, משמעם למעשה התנזרות מראש. בהתנזרות מראש יש משום פגיעה עודפת בחופש השימוש במרחב המקוון, בחופש המידע, בנסיבות מסוימות גם בחופש העיסוק ובאופן כללי בהתפתחות החופשית של העולם המקוון, שכן היא לעולם כוללת ויתור גם על נתחים של פעילות לגיטימית ברשת. שימת הדגש על התגוננות עצמית עלולה ליצור אפוא אפקט מצנן על כלל הפעילות ברשת ועל התפתחותה. כך למשל בדוגמת ההטרדה המינית בצ׳אט, משמעות ההתגוננות העצמית היא למעשה הימנעות מכניסה לצ׳אטים אלה, ובכך יש כדי לשלול את עיקר הפעילות בצ׳אט שהיא לגיטימית ורצויה.

הקרבן באמצעות לכידת הקלדות המקלדת (Keylogging) וצילום עקיב של תמונת המסך (Screenshot) שלו. לצד שכלול זה, השיטה שבה הוחדרו הסוסים הטרויאניים הייתה אנושית ולא ממוחשבת. כך, למשל, השתמשו משתילי הסוס הטרויאני בזהות בדויה ושלחו פנייה לקרבן המיועד בשמו של איש עסקים מקנדה שמבקש כביכול להציע הצעה עסקית סודית לקרבן. עוד הוסיפו כי לצורך ההתקשרות עם ״איש העסקים״ מתבקש הנמען לחתום תחילה על הסכם סודיות שנשלח כצרופה לפנייה. תחת מצג שווא זה פתחו קרבנות רבים את הקובץ המצורף לדוא״ל, אשר כלל את קובץ הסוס הטרויאני. על מנת להבטיח כי מי שפותח בפועל את הדוא״ל הוא האדם המסוים שאל מחשבו רצו לחדור, חסמו משתילי הסוס הטרויאני את הקובץ המצורף, הנחזה להיות הסכם סודיות כאמור, באמצעות ססמה. הססמה נמסרה טלפונית בידי משתילי הסוס הטרויאני לאדם שבמחשבו רצו להשתיל את הסוס הטרויאני, וכך הוגבר מאוד הסיכוי שאותו אדם יפתח את הקובץ בעצמו ולא יעביר את הודעת הדוא״ל לעובדי לשכתו, למשל, על מנת שיקראו אותו בשבילו (כמקובל לא אחת בלשכות של מנהלי חברות). בחלק מהמחשבים נחסמו הודעות הדוא״ל הללו באמצעות ״חומות האש״ שהותקנו במחשבי החברות. אולם היות שמצג השווא היה משכנע במיוחד, הסכימו הקרבנות להסיר זמנית את ״חומת האש״ כדי לעקוף את ההגנה שלה ולפתוח את הקובץ. לפרטים על אודות שיטת המרמה שהופעלה בפרשת הסוס הטרויאני, ראו למשל, ת״פ (מחוזי ת״א) 40061/06 **מדינת ישראל נ׳ האפרתי**, בפס׳ 2—8 (פורסם בנבו, 27.3.2006); בש״פ 7368/05 **זלוטובסקי נ׳ מדינת ישראל**, בפס׳ 2—3 (פורסם בנבו, 4.9.2005).

99 כאמור לעיל, Anderson et. Al, לעיל ה״ש 39, הראו בנתונים מספריים שעלויות ההתגוננות מפני פשיעת אינטרנט גבוהות בהרבה מן הנזקים הישירים של פשיעה זו.

nevo.co.il

בסיכומו של דבר, התגוננות עצמית היא התנהגות רצויה של קרבנות פוטנציאליים, אך אין היא בבחינת תחליף לאכיפה הפלילית המדינתית הקלאסית. גם התגוננות עצמית יקרה ומשולבת, גם אם תהיה במימון המדינה, לא תוכל למנוע, או להפחית, באופן סביר חלק ניכר מתופעות הפשיעה במרחב המקוון.

3. אכיפה קהילתית

א) הצגת החלופה

חלק מהמרחב המקוון הוא קהילתי באופיו. האינטרנט כולל אתרים בעלי מאפיינים קהילתיים מובהקים, החל מהקהילות שנפוצו בשנות התשעים של המאה העשרים כ־WELL[100] או LambdaMOO[101] וכלה בעולמות הווירטואליים התלת־ממדיים כ־Second Life,[102] שהחל את דרכו בשנת 2003 והמציאות המדומה שבו קרובה יותר למציאות הפיזית, ומתקיימים בה מאפיינים קהילתיים מובהקים.

בשנת 1993 פרסם העיתונאי ג׳וליאן דיבל (Dibbell) מאמר בעיתון הניו־יורקי *The Village Voice* על מקרה של אכיפה קהילתית שהופעלה כלפי מפר סדר בתוך קהילת ה־LambdaMOO באינטרנט.[103] באותו מקרה הפעיל חבר בקהילה המכנה עצמו "Mr. Bungle", בתוך הקהילה הווירטואלית תוכנה זדונית כלשהי שאפשרה לו להתבטא בשמם של חברים אחרים בקהילה. לאחר "השתלטות" זו על זהותם, החלו אותם חברים "נשלטים" להשתמש בשפה מינית בוטה באופן קיצוני. שלושה ימים לאחר קרות האירועים נערך דיון וירטואלי ממושך בין משתתפי הקהילה כדי לבחון סנקציות נגד Mr. Bungle. בשום שלב לא נבחנה הפנייה לרשויות אכיפת החוק, בבחינת הוצאת האירוע מגדרי הקהילה הווירטואלית. בעקבות אירועים אלה אפשר מייסד קהילת ה־LambdaMOO והאדמיניסטרטור שלה לחברי הקהילה להעלות עצומות נגד התנהלות חברים אחרים בקהילה ולפנות – על פי רוב דמוקרטי – לאדמיניסטרטור על מנת שיתכנת בהתאם את הפלטפורמה שעליה מתנהלת הקהילה. בעקבות זאת פנו חברי הקהילה וביקשו

---

100 WELL פירושו "Whole Earth `Lectronic Link", רשת מחשבים פופולרית בשנות השמונים של המאה הקודמת, עוד טרם עידן ה־World Wide Web. ה־WELL החלה לפעול כרשת של ועידות וחילופי מידע באמצעות דוא"ל, ומשלב מסוים – גם באמצעות התקשרויות מקוונות.

101 LambdaMOO הוא אתר של קהילה וירטואלית בשם Lambda. MOO פירושו MUD Object Oriented, והמילה MUD פירושה Multi-User Dungeon. ה־MOO הוא סוג של MUD המנסה לייצר מציאות מדומה (עולם וירטואלי) נוסף על ההתקשרות המילולית בין המשתתפים. לתיאור הפעילות ב־LambdaMOO על בסיס התנסות חווייתית יום־יומית של לפחות 30 שעות בשבוע, ראו למשל Julian Dibbell, My Tiny Life (1999).

102 Second Life הוא אתר אינטרנט המדמה עולם וירטואלי מרובה־משתתפים בגרפיקה תלת־ממדית, שבו כל "שחקן" בונה לעצמו דמות (Avatar). ה"שחקן" פוגש דמויות אחרות, שמנהלים אותן שחקנים אחרים, משוחח אתן ויוצר אינטראקצייה עמן בדומה לפעילויות שבעולם האמתי. העולם הווירטואלי ב־Second Life הוא סימולציה של המציאות האמתית, ואין מדובר במשחק שבו צריך לבצע משימות או לעבור שלב. ראו http://secondlife.com.

103 ראו Julian Dibbell, *A Rape in Cyberspace*, The Village Voice (23.12.1993), *available at* http://www.juliandibbell.com/texts/bungle_vv.html.

nevo.co.il

שתהיה אפשרות למנהל הקהילה להרחיק חברים שהוגשו נגדם תלונות על־ידי חברים אחרים. סיפורו של Mr. Bungle בתוך ה־LambdaMOO מייצג דוגמה לאכיפה קהילתית של הפרת סדר.

הווארד ריינגולד (Rheingold) טבע את המושג "קהילות וירטואליות"[104] בספרו שבו תיאר את חוויותיו כמשתתף קבוע בקהילת ה־WELL בשנים 1985–1993, על בסיס של שעתיים גלישה ביום בממוצע לאתר זה. בניסיונו להמשיג את המונח "קהילה וירטואלית" הציע ריינגולד הגדרה רחבה, שלפיה כל אימת שנוצר באתר אינטרנט כלשהו דיון ציבורי, ממושך, אשר במהלכו מובעים רגשות ומתהווים קשרים בין־אישיים בין הגולשים, הרי שלפנינו קהילה וירטואלית.[105] ההכרה בקהילות וירטואליות, על בסיס הגדרה זו, משמעה פירוק המרחב האינטרנטי לתתי־מרחבים אוטונומיים.[106] לעומת זאת קיימת גישה שלפיה האינטרנט מכונן קהילה וירטואלית אחת, ותתי־המרחבים שבה הם בבחינת מקומות מפגש קבועים בתוך הקהילה האחת.[107] דומני כי גישה זו חוטאת במידה רבה בהתבוננות מרוחקת מדי על האינטרנט. האינטרנט למעשה אינו אלא שם כולל של מופעים שונים, שרובם לא קהילתיים, בין מכיוון שהם ארעיים ("גלישה" לאתרי אינטרנט שונים), בין מכיוון שהם דו־צדדיים בלבד (למשל צ'אט דו־צדדי או שליחת דוא"ל פרטי), ובין מכיוון שהם חד־כיווניים בלבד ולא אינטראקטיביים (למשל קריאת תוכן מסוים באתר חדשות).

נראה כי על מנת שתתגבש קהילה וירטואלית באינטרנט, יש צורך בכמה קריטריונים, ובהם קיומה של קבוצת אנשים שחלה אינטראקצייה בתוכה, שיש בה תחושת שייכות וערבות הדדית ברמה מסוימת והכוללת כמה ערכים משותפים. לא אנסה כאן לעמוד על המאפיינים לקהילה בכלל או על המאפיינים לקהילה וירטואלית בפרט.[108] כמו כן לא אדרש לדיון הנורמטיבי בדבר

---

104 Howard Rheingold, The Virtual Community (1993).

105 ראו לעיל, בעמ' 23–25.

106 ראו Ann W. Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 Yale L. J. 1639, 1640 (1995). ראו גם יובל קרניאל וחיים ויסמונסקי "חופש הביטוי, פורנוגראפיה וקהילה באינטרנט" מחקרי משפט כג 259, 281–282, 291–292 (2006).

107 ראו Amber J. Sayle, *Note and Comment: Net Nation and the Digital Revolution: Regulation of Offensive Material For A New Community*, 18 Wis. Int'l L.J. 257, 281–84 (2000). למעשה, ניתן למצוא ניצנים לגישה זו במטאפורת "הכפר הגלובלי" שטבע מרשל מקלוהן (McLuhan) בקשר לעולם הטלקומוניקציה של שנות השישים של המאה הקודמת. ראו Marshal McLuhan, Understanding Media: The Extensions of Man 16 (1964).

108 ג'ורג' הילרי (Hillery) מנה 94 הגדרות שונות למונח "קהילה". ראו George Hillery, *Definitions of Community: Areas of Agreement*, 20 Rural Sociology 111 (1995). בין ההגדרות ניתן למצוא התייחסות לאלמנטים פיזיים (קיום גאוגרפי במקום מסוים לאורך זמן), אלמנטים חברתיים (אמצעי תקשורת בין חברי הקהילה ויצירת קריטריונים להצטרפות לקהילה), אלמנטים תרבותיים (ערכים ומנהגים משותפים) ואלמנטים פסיכולוגיים (תחושת השתייכות סובייקטיבית לקבוצה). חוקרים שונים הפחיתו בחשיבות האלמנט הפיזי של קהילה המגודרת טריטוריאלית. כך למשל ברי ולמן (Wellman), פטר קרינגטון (Carrington) ואלאן הול (Hall) הציגו תפישה של "קהילות משוחררות" (Liberated Communities), שבהן אין משמעות לקרבה הגאוגרפית, וזאת בין השאר בשל הטכנולוגיה שמאפשרת את קיומם והתפתחותם של קשרים עמוקים בין החברים בקהילה, וראו Barry Wellman, Peter Carrington & Alan Hall, *Networks as Personal Communities*, *in* Social Structures: A Network Approach 130–184 (Barry Wellman & S.D. Berkowitz eds., 1988). בכל הנוגע לקהילות וירטואליות, במאובחן מקהילות במרחב הפיזי, אלעד אורג הדגיש את חשיבותה של הזהות הווירטואלית כזהות קבועה כתנאי לקיומה של יציבות בסיסית אשר מדביקה יחדיו את הקבוצה

nevo.co.il

ההכרה העקרונית שעל המשפט לתת לאוטונומיה הקהילתית, בעיקר בתחום הסדרת ההתנהגות של חברי הקהילה בידי הקהילה עצמה.[109] הדיון הנורמטיבי רלוונטי בעיקר כאשר המדינה **עודה בעלת כוח אכיפתי**, ונשאלת השאלה אם המדינה **צריכה** לרסן את עצמה אל מול הקהילה ולהעניק לה אוטונומיה הסדרתית. בהקשר שאני דן בו כעת, נקודת המוצא היא שהמדינה **איבדה מכוחות האכיפה הפלילית** שלה, ונשאלת השאלה אם הקהילה הווירטואלית **יכולה** להיות לה חלופה, ואם כן — עד כמה. רק אם יימצא שהאכיפה הקהילתית יכולה להיות חלופה לאכיפה הפלילית המדינתית, תשוב ותישאל השאלה הנורמטיבית במלוא עצמתה — האם ראוי להתיר לקהילות הווירטואליות להיות גורם מסדיר ואוכף?

עניינו כאמור בשאלת הזיהוי של הקהילות הווירטואליות כגורמים אוכפי חוק. ניתן להצביע על הקהילות הווירטואליות ככאלה שנוצרה בהן תופעה של שיעתוק המוסדות והפרקטיקות מהקהילות המסורתיות. גם בקהילות הווירטואליות מחפשים השחקנים סטטוס ומעמד, מופעלת שם סמכות וסנקצייה, ונוצרת הכפפה למערכת חוקים ומשמעת.[110] בקהילה הווירטואלית לאדמיניסטרטור (מנהל הפורום) יש סמכות־על באופן אינהרנטי־ארכיטקטוני.[111] בסמכותו להסמיך מנהלי משנה, בסמכותו להרחיק אנשים מהקהילה (על בסיס כינויים, כתובת ה־IP שלהם והססמה שלהם בכניסה לפורום). בשל כך נגזרת הסמכות ליצור היירכייה בתוך הקהילה וכן אכיפה בעלת אלמנטים של כפייה. בצד יצירת ההיירכייה יכולה הקהילה ליישם עקרונות של דמוקרטיה ישירה. ארכיטקטורת הרשת, המאפשרת קישוריות, יצירת פלטפורמות נוחות ויעילות להעלאת נושאים והכרעה בהם ב"לחיצת כפתור הצבעה", מעוררת מחדש את הטיעון

המסוימת של משתמשי האינטרנט לכדי קהילה וירטואלית. ראו אלעד אורג **זכות לזהות אינפורמטיבית: עקרון משפטי חדש להגנת קיומה של זהות אינפורמטיבית ויישומו בסביבת מידע מודרני** 109–112 (חיבור לשם קבלת תואר "דוקטור למשפטים", אוניברסיטת תל־אביב, 2008). אניטה בלנצ'ארד (Blanchard) הדגישה את חשיבות התחושה הסובייקטיבית של שייכות נמשכת לקהילה וירטואלית כקריטריון להבחנת קהילות וירטואליות אמתיות מקהילות וירטואליות מדומות. ראו Anita Blanchard, *Sense of Virtual Community*, *in* 1 VIRTUAL COMMUNITIES: CONCEPTS. METHODOLOGIES, TOOLS AND APPLICATIONS 101 (Mehdi Khorsow-Pour ed., 2011).

109 לדיון זה הצדקות מכיוון קהילתני (Communitarianism), ראו למשל Michael Walzer, *The Communitarian Critique of Liberalism*, 18 POL. THEORY 6 (1990); AMITAI ETZIONI, THE SPIRIT OF COMMUNITY: RIGHTS, RESPONSIBILITIES, AND THE COMMUNITARIAN AGENDA (1993). לחלופין, יש גם הצדקה מכיוון ליברלי להכרה בקהילות, וראו למשל WILL KYMLICKA, LIBERALISM, COMMUNITY AND CULTURE 164 (1989); Stephen A. Gardbaum, *Law, Politics, and the Claims of Community*, 90 MICH. L. REV. 685 (1992). מנגד, לניתוח אנטי־קהילתני, המבקש להחיל את הדינים הקיימים על הקהילות הווירטואליות באינטרנט, ראו ANDREW SPARROW, THE LAW OF VIRTUAL WORLDS AND INTERNET SOCIAL NETWORKS (2010).

110 ראו למשל ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTES FOR COLLECTIVE ACTION 89 (1991) בהקשר של קהילות ברשת ה־Usenet; יובל דרור **קהילות בעידן הווירטואלי** 55–76 (חיבור לשם קבלת תואר "מוסמך אוניברסיטה", אוניברסיטת תל־אביב – הפקולטה למדעי החברה, 2001) בהקשר של קהילות ב־IRC.

111 ראו קרין ברזילי־נהון וגד ברזילי "חופש הביטוי המעשי והמדומיין באינטרנט" **שקט, מדברים! התרבות המשפטית של חופש הביטוי בישראל** 483, 492–493 (מיכאל בירנהק עורך, 2006).

nevo.co.il

בעד בחירה אישית של כל משתמשי האינטרנט באשר לעיצוב הנורמות בתוככי הקהילה.[112] הקהילה, בין בדרך של כפייה והיירכייה ובין בדרך של בחירה ישירה, יכולה להפעיל סנקציות ובכך לכונן מערכת אכיפה. הסנקצייה החריפה ביותר היא הרחקה מן הקהילה. סנקציות כופות אחרות יכולות להיות השפלה פומבית, הרחקה זמנית מן הקהילה, נטילת אפשרות של חבר הקהילה החשוד לבצע פעולות מסוימות בתוך הקהילה ועוד.[113]

בנוסף, הקהילה הווירטואלית יכולה להפעיל כלי אכיפה רבים הזהים לכלי האכיפה המוכרים מאכיפה מגננתית־וולונטרית, כאשר ההבדל המרכזי הוא בזהות הגורם האוכף: במקום הפרט זו הקהילה המטמיעה את כלי האכיפה האמורים בקרבה. כך, למשל, ניתן להתקין תוכנות סינון תכנים פוגעניים, תוכנות אנטי־וירוס ו"חומות אש" למיניהן.[114]

חשוב לציין מאפיין אחד ההופך את הקהילה הווירטואלית לפגיעה במיוחד, יותר ממשתמש המחשב הבודד: בשל המספר הרב של המחשבים המקושרים בקהילה ובשל מידת האמון הבסיסית שבין חברי הקהילה, הרי שמדובר ברשת מחשבים הפגיעה במיוחד לתוכנות זדוניות התלויות בהתפשטות מהירה. כך למשל אדם המבקש "לגייס" מספר גדול של מחשבים ולהפכם ל"צבא" Zombies שישמש לו כלי לצורך מתקפות DDoS, יעדיף לנסות ולהדביק מחשבים בקהילה וירטואלית על פני הדבקה פרטנית של מחשבים בודדים. לכן הקהילה הווירטואלית ככזו צריכה לחתור להטמעת כלי אבטחת מידע מיוחדים לאיתור רכיבים זדוניים המנסים לנצל את חולשות הקהילה הווירטואלית מבחינת אבטחת מידע.

ב) הערכת החלופה

כפי שציינתי לעיל, איני סבור כי ניתן לראות באינטרנט קהילה וירטואלית אחת. ניתן לראות בחלק מהמופעים באינטרנט קהילתיים על פי טיבם. מכאן שהאכיפה הקהילתית היא ממילא מוגבלת ביחס להיקף תחולתה האפשרית. יתרה מזאת, על המדינות שמהן מגיעים חברי הקהילה להכיר בסמכויותיה של הקהילה הווירטואלית לשמור על הסדר בקרבה ולנקוט סנקציות, שאם לא כן, עצמאות הקהילה תיפגע.

בעיה מכיוון אחר נוגעת לגבולותיה של הקהילה ולאופן הגדרתה. כיוון שההגדרה של קהילה, בעיקר של קהילה וירטואלית, היא עמומה למדי, הרי שאין ודאות מתי קבוצה וירטואלית מסוימת נכנסת לגדר קהילה ומתי לא. כמו כן ייתכנו מצבים שבהם תכנים מסוימים יחצו את גבולות הקהילה אל המרחב המדינתי של אחד מן החברים, ובמקרה כזה הפעפוע בין הווירטואלי לבין הפיזי ייצור סטנדרט משפטי כפול. להמחשת נקודה זו נניח כי משתמש אינטרנט תושב איראן מצטרף לקהילה וירטואלית ששרתיה מצויים בגרמניה וחברי הקהילה הם

---

112 ראו Netanel, לעיל ה"ש 85, בעמ' 412–433. נתנאל כינה את שיטת הדמוקרטיה הישירה באינטרנט כשיטה מוצעת לעיצוב הנורמות ברשת ואכיפתן, בשם "Cyberpopulism".

113 ראו David S. Wall & Matthew Williams, *Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities*, 7 CRIMINOLOGY AND CRIMINAL JUSTICE 391, 402–408 (2007).

114 ראו Georgios Michaelides & Gabor Hosszu, *Privacy and Security for Virtual Communities and Social Networks*, *in* 2 VIRTUAL COMMUNITIES: CONCEPTS, METHODOLOGIES, TOOLS AND APPLICATIONS 1051, 1058–1060 (Mehdi Khorsow-Pour ed., 2011). כן ראו ברזילי־נהון וברזילי, לעיל ה"ש 111, בעמ' 493–502.

nevo.co.il

תושבי מדינות רבות אחרות בעולם. נניח שבמסגרת הקהילה הווירטואלית שבה מדובר מוחלפות תמונות וסרטים פורנוגרפיים בין החברים, וחבר הקהילה האיראני הוריד למחשבו את התכנים המיניים האמורים. אפילו אם הדין האיראני מעניק אוטונומיה לקהילה הווירטואלית, נראה כי אין זה רֵאלי לדרוש שהאוטונומיה תישמר גם משבחר חבר הקהילה האיראני להוריד למחשבו את המידע אליו.

בעיה נוספת היא החשש מהיווצרות קהילות "מקלט" לעבריינים שבהן חברי הקהילה יבחרו להחיל סטנדרט קיצוני האסור על פי דיני כל המדינות שמהן הגיעו חברי הקהילה. ניתן לצפות שקהילות ה"מקלט" תפרחנה במקום שבו כל החברים מעוניינים לבצע עברה משותפת, כגון במקרה של עברות ביטוי, הפצת חומרי תועבה וחומרים פדופיליים והימורים. הדרך היחידה למנוע היווצרות קהילות "מקלט" שכאלה, שאינה כוללת התערבות מדינתית בפעילות הגולשים בקהילות הווירטואליות, היא להגיע לכלל הסכמה בין־לאומית (שהיא בין־מדינתית) בדבר חסמים כלליים באשר למעשים מסוימים, שייאסרו גם במסגרת הקהילה הווירטואלית. במקרה כזה תתעוררנה ביתר שאת כל הבעיות הקשורות להסכמה בין־מדינתית, אשר אליהן אתייחס בנפרד בהמשך פרק זה.

בעיה מכיוון אחר נעוצה ביעילות האכיפה הקהילתית. ניתן להניח שהסנקציות החריפות ביותר הנתונות בידי הקהילה הן השפלה פומבית והרחקה מהקהילה לאלתר. לא תמיד יהיה בסנקציות אלה כדי להרתיע את כל סוגי העבריינים הפוטנציאליים. סנקציות אלה תיחשבנה לאפקטיביות אם, ורק אם, נניח שהמשך החברות בקהילה חשוב מאוד לחבר הקהילה הסורר. לעומת זאת אם מדובר במי שמתחזה לחבר קהילה מן השורה ורוכש את אמון החברים בטרם ביצע את העברה, אין משמעות לחשיפתו ולהרחקתו מהקהילה, כיוון שיוכל לנסות לצוד את קרבנותיו בקהילות אחרות.[115] עוד יש לציין כי העובדה שבמרבית הקהילות הווירטואליות מזדהים החברים בפסידונים, מקשה על חשיפת זהותו האמתית של מבצע עברה בתוך הקהילה. לפיכך יוכל החשוד לעטות על עצמו זהות פסידונימית אחרת ובכך לעקוף את פעולות האכיפה הקהילתיות שיופעלו כלפיו.

שיטת ה"משטר" הקהילתית מעוררת קשיים ניכרים נוספים. אם מנהל האתר הוא ששולט בקהילה, הרי שמדובר למעשה בשלטון יחיד על כל מגרעותיו המוכרות משלטון יחיד מדיני: פוטנציאל לעריצות, שרירות, אי־שקיפות וכיוצא בזה. מנהל הקהילה עלול להכפיף עצמו לשיקולים מסחריים ועריכתיים שיעצבו את הנורמות בקהילה באופן הנסתר מעינם של חברי הקהילה. אם הקהילה תישלט בדמוקרטיה ישירה, עלולות להתעורר כל הבעיות המוכרות בדמוקרטיה ישירה: עריצות הרוב, המחסור בידע מקצועי לכלל הציבור באופן שעלול לעוות את התוצאות המבטאות ביתר דיוק את רצון הכלל.[116]

בסיכומו של דבר, ברור שהחלופה הקהילתית מוגבלת מאוד בהיקפה העקרוני, שכן היא תחומה בגדרי הקהילה הווירטואלית עצמה. כמו כן יכולת האכיפה של הקהילה הווירטואלית מוגבלת מאוד על פי טיבה, ולא בטוח שהיא תוביל למניעת ההתנהגות המזיקה בעתיד.

---

115 כדוגמה לחבר קהילה מתחזה שכזה ניתן לציין את מקרהו של אדם המבקש להטריד מינית משתמשות אינטרנט אחרות. יצירת האמון בינו לבין הקורבנות, תוך הסוואת כוונותיו האמיתיות של מבצע העבירה, יכולה להיחשב כחלק מהמהלך של ביצוע העבירה.

116 ראו Netanel, לעיל ה"ש 85, בעמ' 415–422.

nevo.co.il

4. אכיפה מגננתית־כופה

א) הצגת החלופה

צורת ההתמודדות עם עברות במרחב הסייבר, המוצגת כאן, היא באמצעות התגוננות, אלא שיישום אמצעי ההתגוננות אינו עוד פרי רצון טוב וחופשי של המתגונן, כבמקרה של האכיפה המגננתית־הוולונטרית שפירטתי לעיל, אלא פרי הוראה כופה המחייבת ביישום ההתגוננות כאמור. מכאן שהביטוי שבחרתי לתאר קטגוריה זו – "אכיפה מגננתית־כופה" – הוא אוקסימורוני. בתוך קטגוריה זו אתייחס לשתי פעולות שונות ברמה הטכנית:[117] **האחת**, חסימת גישה לאתרי אינטרנט; **השנייה**, סינון תכנים אסורים. הפעולות אינן מכוונות במישרין לאתרים החשודים, ומטרתן לספק מערכת שתמנע את חשיפתו של ציבור משתמשי המחשב במדינה האוכפת לתכנים או פעולות אסורות המבוצעות באתרים האמורים.

בכל הנוגע לחסימת גישה לאתרי אינטרנט ניתן, מבחינה טכנית־אופרטיבית, לדבר על כמה סוגים של חסימה:[118] **האחת**, חסימה לפי כתובת IP (IP Blocking). כל אתר אינטרנט נמצא בשרת כלשהו, ולשרת יש כתובת IP מזוהה וקבועה באינטרנט. ספקי הגישה לאינטרנט יכולים לחסום את הגישה לכתובת IP מסוימת, וכך כל אימת שמשתמש אינטרנט המחובר לשירותיהם יבקש להתקשר לכתובת ה־IP האסורה, תימנע היכולת לבצע את ההתקשרות האמורה; **השנייה**, הסרת רישום של אתר פוגעני (Deregistration). ניתן לקבוע בשרתי ה־DNS המדינתיים המנהלים את כל שמות המתחם בסיומת של המדינה (למשל, il של ישראל; fr של צרפת), כי יוסר הרישום של שם מתחם מסוים שמצוי בו תוכן שמבקשים לחסום את הגישה אליו;[119] **השלישית**, חסימה לפי שרת ה־DNS הספציפי הממען את משתמש האינטרנט ליעדו. על פי שיטה זו, כל אימת שיוקלד שם מתחם של אתר אסור, תופסק פעולת שרת ה־DNS למשתמש המבקש, והשם לא יתורגם לכתובת ה־IP המובילה אל האתר; **הרביעית**, חסימה באמצעות סינון באמצעות פרוקסי (Http Proxy Filtering). שיטת חסימה זו מבוססת על כך שמשתמשי האינטרנט יחויבו "לגלוש" באמצעות שרת פרוקסי. אותו שרת יפעיל אצלו סינון תכנים ויעביר אל המשתמשים אך ורק

---

117 כאמור, בתת־הפרק הקודם התייחסתי לאפשרות לחיוב משתמשי המחשב לבצע פעולות של התגוננות עצמית. אפשרות זו כלולה באכיפה מגננתית־כופה כמובן ולא באכיפה המגננתית־הוולונטרית, והדברים צוינו בתת־הפרק הקודם מטעמים מתודיים בלבד.

118 ראו Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 57, 59–63 (Ronald Deibert, John Palfrey, Rafal Rohozinski & Jonathan Zittrain eds., 2008).

119 ה־DNS הם ראשי תיבות של Domain Name System. מדובר בפרוטוקול שנועד להקל את השימוש ברשתות תקשורת. התקשורת האינטרנטית מבוססת־כתובות־IP, שהן כתובות מספריות. לעומת זאת ה־DNS הוא שֵמי. על מנת שיתאפשר למשתמשי האינטרנט להגיע לאתרים שהם מבקשים להגיע אליהם, מתנהלת מערכת של תרגום שמות המתחם המילוליים לכתובות ה־IP המספריות. זו מהותה של מערכת ה־DNS. מערכת ה־DNS היא היררכית: מרמת ה"שורש" הגבוהה ביותר (הכוללת כיום 13 שרתים, Root servers, שחלקם מבוזרים פיזית ומופעלים באמצעות ראוטרים מיוחדים הנקראים "anycast"), דרך הרמה המתייחסת לסיומת המדינה שבה מצוי אתר האינטרנט, דרך רמת המשנה (המתייחסת לסוג השירות בתוך המדינה – אם מדובר בסיומת gov ממשלתית, או ב־co מסחרית, ב־org של ארגונים לא־ממשלתיים ועוד), ועד לרמה הפרטנית (המתייחסת לשם האתר עצמו בתוך המדינה הנתונה ובתוך סוג השירות הנתון).

nevo.co.il

תכנים מסוננים; **החמישית**, חסימה באמצעות מנועי החיפוש. על פי שיטה זו, מנועי החיפוש, המהווים את נתיב הכניסה המקובל למרבית אתרי האינטרנט, יחויבו למחוק אתרים פוגעניים מוגדרים מראש מתוצאות החיפוש שיספקו למשתמשי האינטרנט.

בכל הנוגע **לסינון תכנים אסורים**, ניתן מבחינה אופרטיבית לדבר על שני מנגנונים: **האחד**, כשמדובר בספקיות גישה או בספקיות תוכן, ניתן להתקין תוכנות סינון אשר מתיימרות לאתר את התכנים המוגדרים כאסורים עוד בטרם הגיעם למשתמשי הקצה ולחסום את הגישה אל הדפים המציגים תכנים אלה או למחוק תכנים אלה מתוך הדפים. הזכרתי לעיל בתת־הפרק המתייחס לאכיפה מגננתית־וולונטרית, כי יכול שמשתמש הקצה עצמו יתקין תוכנות סינון בשביל עצמו, בשביל ילדיו או בשביל עובדיו. השימוש בתוכנות סינון תכנים במסגרת אכיפה מגננתית־וולונטרית הוא בבחינת צנזורה עצמית, ואילו במקרה של אכיפה מגננתית־כופה, הכוונה להתקנה בכפייה של תוכנות סינון לתכנים האסורים. המנגנון **השני** לסינון תכנים הוא זה: כשמדובר במנועי חיפוש, ניתן להסיר תוצאות חיפוש מסוימות או לשנות את סדר הצגת תוצאות החיפוש באופן שאתרים מסוימים הכוללים תוכן לא רצוי לא ייחשפו, או יידחקו לשוליים. יש לזכור כי ה״גלישה״ באינטרנט או ברשתות מחשב גדולות תלויה בשני גורמים: מנועי החיפוש והקישוריות. הקישוריות מאפשרות נדידה מדף לדף לפי בחירתו של עורך התוכן באתר שאליו נכנס הגולש, בעוד שמנועי החיפוש מאפשרים הגעה לתכנים לפי בחירתו החופשית של המשתמש עצמו (בהנחה שמנוע החיפוש עצמו אינו מוטה בתוצאותיו).[120]

אציג להלן כמה דוגמאות מעשיות לחסימת גישה ולסינון תכנים: בישראל נעשה לאחרונה ניסיון ראשון מסוגו לחסום גישה לאתרי אינטרנט המציעים הימורים לא חוקיים והנגישים למשתמשי אינטרנט מישראל. משטרת ישראל השתמשה בסעיף 229(א)(1) לחוק העונשין, התשל״ז–1977, אשר נחקק עוד טרם עידן האינטרנט וקובע כי ״מפקד משטרת מחוז במשטרת ישראל רשאי להורות על **סגירתו** של **מקום** **משחקים אסורים** או מקום לעריכת הגרלות או הימורים״. ״מקום משחקים אסורים״ מוגדר בסעיף 224 לחוק העונשין כדלקמן: ״׳מקום משחקים אסורים׳ — **חצרים** שרגילים לערוך בהם משחקים אסורים, בין שהם פתוחים לציבור ובין שהם פתוחים לבני אדם מסוימים בלבד...״ (ההדגשות שלי — ח׳ ו׳).

ספקיות הגישה לאינטרנט ניאותו לציית להוראות משטרת ישראל. לעומת זאת איגוד האינטרנט הישראלי הגיש עתירה מנהלית נגד ההוראה, ובית המשפט המחוזי, בשבתו כבית משפט לעניינים מנהליים, קיבל את העתירה וקבע כי לא קמה למשטרה סמכות להורות על חסימת גישה לאתרי הימורים מכוח סעיף זה.[121] ערעור המדינה על פסק הדין נדחה ברוב

---

120 עוד על הדומיננטיות של מנועי החיפוש במסגרת ה״גלישה״ באינטרנט ראו Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 DAYTON L. REV. 179, 180–185 (2001).

121 עת״מ (מחוזי ת״א) 45606-10-10 **איגוד האינטרנט הישראלי נ׳ מפקד משטרת מחוז תל־אביב** (פורסם בנבו, 2.4.2012). השוו גם עם פסיקת בית המשפט העליון של אוסטרליה בדבר שאלת אחריותם של ספקי הגישה לאינטרנט לתכנים מפרי זכויות יוצרים. נפסק כי כיוון שהאחריות לסינון התכנים אינה נקובה במפורש ב־Copyright Act האוסטרלי משנת 1968, אי אפשר לקרוא סמכות מעין זו יש מאין, שכן יש לה מאפיינים מובהקים של צנזורה על אתרים. ראו Roadshow Films Pty Ltd v. iiNet Ltd., [2012] HCA 16 (2012) (Austl.).

nevo.co.il

דעות.[122] שופטי הרוב בבית המשפט העליון לא שללו עקרונית את הסמכות להורות על חסימת גישה לאתרי אינטרנט פוגעניים,[123] ועיקר ההנמקה בוססה על כך שסעיפי החוק הקיימים אינם יכולים "לסבול" קריאה מכללא של סמכות לחייב צדדים שלישיים – ספקיות הגישה לאינטרנט – לבצע פעולת חסימה בשביל משטרת ישראל. הנשיא גרוניס כתב כי בסוגיה זו "למחוקק הפתרונים".[124] ואכן, לאחר פרסום פסק הדין של בית המשפט העליון פורסמה הצעת חוק, ובה הוצע לקבוע לראשונה סמכות מפורשת לסגירת אתרי אינטרנט המשמשים לניהול הימורים אסורים הקשורים בפעילות של ארגוני פשיעה, ובנוסף הוצע להכיר בסמכות מעין זו גם באשר לאתרים המציגים תכנים פדופיליים ובאשר לאתרים המציעים ממכר של סמים קשים.[125]

נוסף על ניסיון זה, הועלו בעבר כמה הצעות חוק לסינון תכנים פוגעניים באמצעות ספקי הגישה לאינטרנט. הצעות החוק לא הבשילו לכדי מהלך חקיקה מתקדם. ההצעות ביקשו לקבוע ברירת מחדל של סינון תכנים בידי ספק הגישה לאינטרנט, עם אפשרות של גולש האינטרנט לבטל את מגבלת סינון התכנים. מכאן שמבחינת הטקסונומיה שהצעתי לסוגי אכיפה לא פלילית, ניתן למקום הצעות אלה כהצעות לאכיפה מגננתית־כופה עם ריכוך לכיוון הוולונטרי.[126]

בארצות הברית נחקקו כמה חוקים לחיוב בסינון תכנים פוגעניים ובחסימת גישה לאתרי האינטרנט המציגים אותם תכנים. שניים מהם — ה־CDA (Communications Decency Act) מ־1996 וה־COPA (Child Online Protection Act) מ־1998 — נפסלו בבית המשפט העליון האמריקני כלא חוקתיים, בהטילם מגבלות עמומות ורחבות מדי על חופש הביטוי של אתרי האינטרנט.[127] חוק נוסף, ה־CIPA (Children's Internet Protection Act) מ־2000, נפסל תחילה

---

122 עע"מ 3782/12 **מפקד מחוז תל־אביב־יפו במשטרת ישראל נ' איגוד האינטרנט הישראלי** (פורסם בנבו, 24.3.2013).

123 כאן המקום לציין כי במסגרת הליכים אזרחיים, במסגרת בקשה לסעד זמני בתביעת נזיקין בגין הפרת זכות יוצרים, נעתר בעבר בית המשפט לבקשת התובעות והורה לספקיות הגישה לאינטרנט לחסום גישה לאתר אינטרנט של הנתבע, אשר הפר לטענתן את זכות היוצרים שלהן. ראו ת"א (מחוזי ת"א) 20205-12-12 **זיר"ה (זכויות יוצרים ברשת האינטרנט) בע"מ נ' בוסני** (פורסם בנבו, 26.12.2012).

124 שם, בעמ' 40 לפסק הדין.

125 ראו סעיף 6 להצעת חוק הגבלת שימוש במקום לשם מניעת ביצוע עבירות (תיקון מס' 2), התשע"ד–2014, ה"ח הממשלה 839. יוער כי תזכיר החוק פורסם עוד בטרם יצא פסק דינו של בית המשפט העליון.

126 ראו למשל את הצעת חוק הגבלת גישה לאתרי אינטרנט למבוגרים, התשס"ו–2006, ה"ח פ/892/17 (ח"כ אמנון כהן). ההצעה נדונה בוועדת הכלכלה של הכנסת בתאריכים 21.5.2007, 16.7.2007, 4.2.2008, 13.2.2008. הצעת החוק הוגשה שוב, לאחר ביצוע כמה שינויים, בידי שר התקשורת אריאל אטיאס מש"ס. ראו הצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 41) (שירות סינון של תכנים בלתי הולמים לקטינים באינטרנט), התשס"ח–2008, ה"ח פ/892/17, אשר נדונה בישיבת ועדת הכלכלה של הכנסת ביום 30.6.2008. להצעת חוק עדכנית יותר ראו הצעת חוק התקשורת (בזק ושידורים) (תיקון – חובת סינון אתרים פוגעניים), התשע"ד–2013, ה"ח פ/1733/19. כדוגמה להצעת חוק מרוכבת עוד יותר, של הטלת חובות על ספקיות הגישה לאינטרנט ליידע את משתמש האינטרנט בדבר אתרים ותכנים פוגעניים באינטרנט ואפשרויות ההגנה מפניהם, לרבות סינון תכנים או מניעת גישה אל האתרים, ראו הצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 47) (אתרים ותכנים פוגעניים באינטרנט), התשע"א–2011, ה"ח פ/456/18, אשר נדונה אף היא כמה פעמים בוועדת הכלכלה של הכנסת.

127 ה־CDA הופיע כ: 47 U.S.C. § 223(a)-(h). החוק אסר על פרסום תכנים הנחשבים ללא מהוגנים ("indecent") ופוגעניים ("patently offensive"), ולא צמצם את תחולתו רק על פרסום תכנים מתועבים ("obscene"), הנחשבים ככאלה המקימים עברה פלילית של פרסומי תועבה. כשנה וארבעה חודשים

nevo.co.il

בבית המשפט לערעורים והוכשר לבסוף בבית המשפט העליון האמריקני.[128] ניסיונות אלה מעידים על הקושי, בעיקר בעברות ביטוי, לחסום גישה לאתרים בשל החשש שיהיה בכך משום אפקט מצנן על הפעילות באינטרנט, על מפרסמי התכנים ברשת ופיתוח השיח בו. כן ניתן לציין כמה ניסיונות חקיקה, שלא הבשילו לכלל חקיקה, שמטרתם הייתה לפגוע בענף שיתוף הקבצים באינטרנט, לדוגמה ה־SOPA (Stop Online Piracy Act),[129] הצעת חוק משנת 2011 שביקשה לקבוע כמה סמכויות: סמכות להורות למנועי חיפוש למחוק תוצאות של הפנייה לאתרי אינטרנט המאפשרים פגיעה בזכויות יוצרים; סמכות להורות לספקיות הגישה לאינטרנט לחסום גישה לאתרים מעין אלה; סמכות להורות על איסור הצגת פרסומות בתשלום באתרים אלה. ההצעה

לאחר חקיקתו של ה־CDA פסל בית המשפט העליון את הגדרות החוק באשר לתכנים האסורים בפרסום באינטרנט, בהיותם עמומים ורחבים מדי באופן הסותר את התיקון הראשון לחוקה האמריקנית המעגן את חופש הביטוי. ראו Reno v. ACLU, 521 U.S. 844 (1997). ה־COPA הופיע כ: 47 U.S.C. § 231. על פי ה־COPA, אתרי אינטרנט מסחריים בגבולות ארצות הברית בלבד חויבו להימנע מהעלאת תכנים המזיקים לקטינים ("harmful to minors"), כאשר התוכן המזיק לקטינים ייקבע על פי הסטנדרט הקהילתי הלוקאלי בכל מקום ומקום בארצות הברית. החוק חולל סדרה של דיונים משפטיים בכמה סבבים, ובסיומם נקבע כי החוק אינו חוקתי בהיותו פוגע בחופש הביטוי. נקבע כי החוק נקט מונח עמום כקריטריון לחסימת אתרים פוגעניים, הוא לא היה יכול להשיג תוצאה אפקטיביות בשל תחולתו המוגבלת לאתרים מסחריים בתוככי ארצות הברית בלבד, וכן יש קושי טכני ליישם סטנדרט קהילתי לוקאלי באינטרנט. ראו פסק הדין של בית המשפט הפדרלי לערעורים: ACLU v. Reno, 217 F. 3d 162 (3rd Cir., 2000); בבית המשפט העליון האמריקני הוחלט על החזרת הדיון לערכאה דלמטה, וראו Ashcroft v. ACLU, 122 S. Ct. 1700 (2002). החוק שוב נפסל: ACLU v. Ashcroft, 322 F. 3d 240 (3rd Cir., 2003). בית המשפט העליון שוב השיב את התיק לערכאה הדיונית על מנת לבחון אם ניתן כיום לבצע סינון אפקטיבי של גולשים לפי גיל. ראו Ashcroft v. ACLU, 542 U.S. 656 (2004). בסבב הבא שוב נפסל החוק: ראו ACLU v. Mukasey, 534 F. 3d 181 (3rd Cir., 2008). בית המשפט העליון לבסוף דחה את הבקשה לדון בערעור (ראו Mukasey v. ACLU, cert. denied, 129 S. Ct. 1032 (2009)), ובכך החוק נותר בטל.

128 החוק מופיע כ: 17 U.S.C. § 1701–1703, 1711–1712, 1721, 1731–1733, 1741. מדובר בחוק מימוני המוחל על ספריות ציבוריות ובתי ספר במימון ציבורי. במסגרת החוק חויבו מוסדות אלה – כתנאי למימון פדרלי – בהתקנת תוכנות סינון לתכנים מתועבים, פדופיליים או "מזיקים לקטינים" ("harmful to minors"). עתירה נגד חוקתיותו של החוק התקבלה בתחילה בבית המשפט הפדרלי של מחוז פנסילבניה (American Library Association v. United States, 201 F. Supp. 2d 401 (2002)) אך בסופם של ההליכים נדחתה העתירה בבית המשפט העליון. ראו United States v. American Library Association, 539 U.S. 194 (2003). הטענה המרכזית נגד חוקתיותו של החוק הייתה כי אי אפשר לבצע מבחינה טכנולוגית סינון תכנים אפקטיבי אשר לא יביא להכללת יתר (יסוננו גם תכנים שהם "ביטוי מוגן") או להכללת חסר (לא יסוננו כל התכנים האסורים). כיוון שהנטייה של הספריות ובתי הספר תהיה להימנע מהכללת חסר (שאז ייחשבו למי שלא עמדו בדרישות החוק, ולא ייהנו מן התמריץ הכלכלי המוצע למי שמיישם את החוק), הרי שהנטייה תהיה לכיוון הכללת יתר וחסימת ביטויים מוגנים. נפסק כי ניתן לרפא את הפגם האמור אם יוכל בגיר שגולש בספרייה או בבית הספר, לבקש את הסרת הסינון במקרה מסוים, והמוסד שבו מותקנת תוכנת הסינון יבצע את הדרישה ללא דיחוי. לדיון עקרוני בשאלת סינון תכנים במסגרתו של מוסד ציבורי בפרט ובאינטרנט בכלל, ראו מיכאל בירנהק "החופש לגלוש בספריות ציבוריות" משפט וממשל ו 421 (2003) (המאמר מתייחס לפסיקת הערכאה הראשונה של בית המשפט הפדרלי, שכן פסיקת בית המשפט העליון ניתנה לאחר פרסום המאמר).

129 Stop Online Piracy Act, H.R. 3261 (112th Congress, 2011).

nevo.co.il

הושעתה בינואר 2012 בשל מחאה ציבורית רחבה, אשר במסגרתה הועלו טענות נגד חוקתיות ההוראות המנויות בה.[130]

בבריטניה מאפשר ה־Digital Economy Act משנת 2010 לרגולטור (המאסדר) להורות על חסימת גישה לאתרי אינטרנט המפרים בקביעות זכויות יוצרים.[131] החוק דורש כי חסימה שכזו תבוצע תוך התחשבות בעקרונות של חופש הביטוי (של האתר שאליו נחסמת הגישה), במידתיות ובפגיעה אפשרית בזכויות מוגנות של גורמים נוספים. בנוסף, הפסיקה הכירה באפשרות להורות בצו שיפוטי על חסימת גישה לאתר אינטרנט המפר זכויות יוצרים, וזאת על בסיס עקרונות ממשפט האיחוד האירופי והוראות הדין המקומי בנושאי מסחר אלקטרוני.[132] במילים אחרות, בבריטניה, אמנם בהקשר קונקרטי של הפרת זכויות יוצרים באינטרנט, הוכרו מנגנוני חסימת גישה לאתרים בסמכות בית המשפט (מכוח הסקה פרשנית של הסמכות) ובסמכות הרגולטור (מכוח הסמכה חוקית מפורשת לכך). ועוד בהקשר הקונקרטי של הפרת זכויות יוצרים, לאחרונה הכיר **בית המשפט הגבוה לצדק של האיחוד האירופי** (ECJ – European Court of Justice) בסמכות להורות לספקיות גישה לאינטרנט לחסום תכנים המפרים זכויות יוצרים, וכי על הספקיות יהא, לפי הדירקטיבה האירופית הדנה בזכויות יוצרים, לנקוט אמצעים סבירים למנוע גישה כאמור.[133]

בצרפת צו שהוצא בפברואר 2015 (מכוח חוק מסמיך שנחקק באוקטובר 2014) קובע כי בסמכותו של מנהל יחידת הסייבר המשטרתית הצרפתית להורות לספקיות הגישה לאינטרנט לחסום גישה של משתמשי רשת בצרפת לאתרים הכוללים תוכן פדופילי ולאתרים המסיתים לביצוע פעולות טרור או המקדמים זאת.[134] על ספקיות הגישה לציית לצו המנהלי תוך 24 שעות. הספקיות תוכלנה לקבל החזר הוצאות מהמדינה אם חסימת הגישה תשית עליהן עלויות. באתרים החסומים תופיע הודעה מטעם משרד הפנים הצרפתי, המסבירה כי הגישה אליהן

130 לנוסח דומה של הצעת החוק האמורה אשר הוצג בסנאט, ראו גם ה־ PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, S. 968 (112th Congress, 2011)) או בשמו הקצר ה־PIPA. גם הצעה זו הושעתה. הצעה נוספת ברוח זו, מוקדמת יותר, הושעתה אף היא בסנאט. ראו Combating Online Infringement and Counterfeits Act, S. 3804 (111th Congress, 2010).

131 ראו Digital Economy Act, 2010, c. 24 §§ 17–18 (Eng.). הוראות החוק בוקרו, ובאוגוסט 2011 הכריזה הממשלה הבריטית על זניחת תכניתה ליישם את הוראות ה־Digital Economy Act ולפעול למטרת חסימה של אתרי אינטרנט מפרי זכויות יוצרים. ראו Andrew Orlowski, *Ofcom Says No to Web-Blocking*, THE REGSITER (3.8.2011) http://www.theregister.co.uk/2011/08/03/ip_policy_roundup/.

132 ראו Twentieth Century Fox Film Corporation v. British Telecommunications PLC, [2011] EWHC 1981 (Eng.).

133 ראו UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, ECJ C-314/12 [2014]. הפסיקה עסקה בצו שיפוטי שנתן בית המשפט באוסטריה, על סמך חקיקת זכויות היוצרים האוסטרית. לדירקטיבת האיחוד האירופי הדנה בזכויות יוצרים, אשר נבחנה בפסיקה האמורה, ראו Directive 2001/29/EC of the European Parliament and of the Council (22.5.2001) on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167.

134 ראו Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique 2015 (Fr.).

nevo.co.il

נחסמה על פי חוק, וכן מסבירה כיצד ניתן להשיג על ההחלטה בדבר חסימת הגישה אל התכנים שבאתרים החסומים.[135]

בצד האמור, נמצא שבארצות הברית, וכן במדינות נוספות באירופה, קיימת מערכת של לחצים משפטיים בדמות מכתבי התראה משפטיים המועברים למנועי חיפוש כדוגמת גוגל. במכתבים אלה הכותבים עומדים על כך שמנוע החיפוש לא יציג דפי אינטרנט מסוימים בתוצאות החיפוש שלו, שכן בדפים אלה יש משום עברה פלילית או הפרה של קניין רוחני. ג׳ונתן זיטריין (Zittrain) ובנג׳מין אדלמן (Edelman) הראו, נכון לשנת 2002, ש־Google.de (גרמניה) ו־Google.fr (צרפת) אינם מציגים יותר מ־100 דפי אינטרנט שונים בעלי תכנים גזעניים ופרו־נאציים אשר פרסומם עולה לכאורה כדי עברה פלילית על פי הדין הגרמני והצרפתי.[136] גם גוגל האמריקנית ניאותה לסנן דפי אינטרנט מתוצאות החיפוש שלה, לאחר קבלת כמה וכמה מכתבי התראה משפטיים על שדפים אלה כוללים תכנים המפרים זכויות יוצרים והגנה של סימני מסחר לפי הדין האמריקני.[137]

בסין נהוגה מערכת קבועה של סינון תכנים לא נאותים, הפועלת במידה לא מבוטלת של הצלחה אופרטיבית.[138] מדובר במערכת סינון תכנים הנחשבים לא נאותים על פי הסטנדרט הסיני, ובכללם תכנים פוליטיים, מיניים ואף כלכליים. תוכנת הסינון מותקנת אצל ספקיות הגישה לאינטרנט, המפוקחות בידי המדינה. את התוכנה פיתחה חברת Cisco האמריקנית, והיא מבוססת על יישום של סינון תכנים שפיתחה החברה בשביל מעבידים בארצות הברית שביקשו לאפשר לעובדיהם גישה לאינטרנט, אם כי גישה שאינה כוללת תכנים שעלולים להסיטם מעבודתם. הממשל הסיני מעביר ומעדכן את רשימת האתרים שיש לחסמם, וספקיות הגישה לאינטרנט מעדכנות בהתאם את התוכנה לצורך ביצוע בפועל של החסימה הנדרשת. זיטריין ואדלמן כינו שיטה זו ״החומה הסינית״ המודרנית, שנבנתה בלבנים אמריקניות.[139] ״חומה״ זו יעילה בחסימת אתרים שבהם התקשורת היא על דרך של שידור one-to-many, מה שמכונה הדור הראשון של האינטרנט. גם בכל הנוגע לאינטרנט דור 2.0, דהיינו אתרי אינטרנט שבהם התקשורת היא many-to-many והתכנים מועלים בידי הגולשים עצמם (בלוגים, פורומים, צ׳אטים, רשתות חברתיות ועוד), מפעילה סין מערכת מפותחת של סינון תכנים, הן אוטומטית והן אנושית. המערכת האוטומטית כוללת סריקת תכנים אסורים בפורומים ובלוגים וסינון החוצה, עוד בטרם העלאתם לדף הציבורי (באמצעות עיכוב העלאתם לצורך ביצוע סריקה מקדימה זו) או בסמוך לאחר העלאתו. בנוסף, קיימת מערכת של צנזורים שסורקת את כל אותם

---

135 לסקירה נוספת של מהלכי חקיקה בעולם לחסימת גישה, ראו רועי גולדשמיט ״מידע לקראת דיון בנושא ׳בריונות ברשת והשימוש באפליקציית סיקרט׳״ **מרכז המחקר והמידע של הכנסת** (29.9.2014).

136 ראו Jonathan Zittrain & Benjamin Edelman, *Localized Google Search Result Exclusions* (2002), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399920.

137 ראו Goldsmith & Wu, לעיל ה״ש 1, בעמ׳ 74—75.

138 ראו שם, בעמ׳ 87—102.

139 ראו Jonathan Zittrain & Benjamin Edelman, *Empirical Analysis of Internet Filtering in China*, IEEE INTERNET COMPUTING 70 (Mar.-Apr. 2003).

nevo.co.il

מרחבים של תוכן גולשים ומסמנת את כל התכנים האסורים שחמקו מרשת הדיג של תוכנות הסינון. מנהלי האתרים מוחקים את התוכן שסימנו הצנזורים.[140]

ב) הערכת החלופה

האכיפה המגוננתית־הכופה במרחב הסייבר נהנית מיתרון ניכר על פני האכיפה הפלילית הקלאסית: היא מציעה פתרון שאינו כרוך בפעולה אקסטרה־טריטוריאלית אלא בהוראה לספקיות השירות המדינתיות. בהנחה שביכולתן של הספקיות לבצע חסימת גישה או סינון תכנים אפקטיביים, הרי שמדובר בפתרון בעל פוטנציאל לחיסון מפני סכנות ברשת. עם זאת יש כמה ביקורות לא מבוטלות – משפטיות, טכנולוגיות ופרקטיות – נגד שיטת אכיפה זו, ואביאן להלן:

ראשית, האכיפה המגוננתית־הכופה מוגבלת לסוג מסוים של אתרים ולסוג מסוים של עברות. אשר לחסימת גישה, השיטה רלוונטית כמעט רק לאתרים פומביים באינטרנט המציעים שירות פסול לציבור לא מסוים של גולשים. היא אינה נוגעת לאתרים המציעים את אותו שירות לקבוצה סגורה של גולשים, תופעה המוכרת למשל באתרי הימורים, באתרים של פדופילים המשתפים בקבצים אסורים או באתרים לממכר סמים מסוכנים. אתרים אלה קשים לחשיפה, ומלבד זאת, גם אם הם ייחשפו וייחסמו, יוכלו מנהלי האתרים להחליף בנקל את כתובתם וליידע את קבוצת הגולשים המצומצמת בכך. מלבד זאת, חסימת האתרים אינה רלוונטית, כשיטת אכיפה, לעברות המתבצעות במעמד של אחד־על־אחד, או במופעי אינטרנט בעלי מאפיינים "פרטיים", לדוגמה: עברות מרמה או העברת נגיף מחשב באמצעות הדוא"ל, או הטרדה מינית בצ'אטים פרטיים. מן הפרט אל הכלל ניתן לומר ששיטת אכיפה זאת מוגבלת מראש לעברות פליליות המתבצעות בגלוי, כשמן העבר האחד יש מבצע עברה ומן העבר השני – נפגעי עברה. עברות חשיפה, שבהן אין נפגע עברה מזוהה, או עברות שאינן מתבצעות בערוץ גלוי ונגיש – אינן רלוונטיות לשיטת אכיפה מגוננתית־כופה. אשר לסינון תכנים, הטכניקה מוגבלת בעיקר לתוכני טקסט. סינון על בסיס תמונות וסרטי וידאו ככלל אינו אפשרי באופן אוטומטי, בוודאי לא ביעילות.

שנית, האכיפה המגוננתית־הכופה סובלת מאפקטיביות מוגבלת מבחינה טכנולוגית. בכל הנוגע לחסימת גישה, אתרי האינטרנט, מן העבר האחד, ולפחות חלק ממשתמשי האינטרנט, מן העבר השני, ימצאו דרכים לעקוף את החסימה המבוססת על כתובת IP של האתרים האסורים.[141] גם תוכנות הסינון אינן מושלמות מבחינה טכנית. הן לעולם עלולות לגרום להכללת יתר של ביטויים מוגנים ולהכללת חסר של ביטויים פוגעניים שלא יילכדו ברשת

---

140 לדיווחים שוטפים על מערכת הצנזורה הסינית על האינטרנט ראו באתר "עיתונאים ללא גבולות": http://en.rsf.org/china.html. עם זאת ברי כי מערכת הסינון והצנזור של תכנים אסורים במופעים אינטרנטיים של many-to-many, כמו גם ההתערבות בתכנים במופעים אינטרנטיים של one-to-one, כגון דוא"ל, צ'אטים וכדומה, אינה מושלמת.

141 כך למשל אתרי האינטרנט יוכלו לשנות את כתובת ה־IP שלהם. משתמשי האינטרנט יוכלו לגלוש באמצעות שרת פרוקסי מחו"ל, וכך, מבחינת ספק הגישה הישראלי, הגלישה תהא לכאורה אל כתובת חוקית (כתובת הפרוקסי). ראו בהקשר של סגירת אתרי ההימורים בישראל: עמ' 7 לפרוטוקול מס' 417 של ועדת החוקה, חוק ומשפט של הכנסת מיום 14.1.2008, ניתן לצפייה ב־www.knesset.gov.il (אגב דיון בהצעת חוק העונשין (תיקון – משחקים אסורים, הגרלות והימורים ברשת האינטרנט), התשס"ז–2007, ה"ח פ/1923/17 (ח"כ רונית תירוש)).

nevo.co.il

הסינון.[142] יתרה מזאת, קיימים קשיים טכנולוגיים מוגברים כאשר מבקשים ליישם את סינון התכנים יישום ממוקד. כך למשל כשמעוניינים לסנן תכנים מסוימים כלפי קטינים בלבד ולא כלפי כלל משתמשי האינטרנט, אין יכולת טכנית יעילה לערוך סינון תכנים על בסיס זהות המשתמש, בוודאי אם הקטין מתחזה לבגיר ומשתמש בנתונים מזהים של הוריו למשל.[143] כמו כן אם ספק גישה לאינטרנט מתבקש לסנן תכנים מסוימים מתוך אתר אינטרנט מסוים, להבדיל מחסימת עצם הגישה לאתר האינטרנט, הרי שמדובר, מבחינת ספק הגישה לאינטרנט, בפעולה מורכבת ויקרה.[144]

שלישית, הפעולה של חסימת גישה לאתרים היא למעשה הפעלה של סנקצייה מעין־עונשית (משטרה או רגולטור) בידי בעל סמכות מנהלית ולא שיפוטית, והדבר מעורר קשיים במישור של הפרדת רשויות.[145] כמו כן מנגנון זה של הפעלת הסנקצייה בידי גורם מנהלי עלול לפגוע בזכות להליך הוגן, שבו תבורר האחריות של מבצע העבירה.

רביעית, לאכיפה המגננתית־הכופה יכולות להיות השלכות על חופש השימוש באינטרנט ובמחשב, באוטונומיה של הרצון החופשי וחופש המידע.[146] ככל שמדובר בחסימת גישה

---

142 ראו לעיל ה"ש 128.

143 ככלל החקיקה הפלילית ממעטת להפליל ביטויים אשר כלפי בגירים ייחשבו מותרים וכלפי קטינים – ייאסרו. בדין הישראלי ההוראה היחידה מסוג זה מצויה בסעיף 3(א)(6) לחוק למניעת הטרדה מינית, התשנ"ח–1998, הקובע כי הצעות חוזרות בעלות אופי מיני או התייחסויות חוזרות המופנות לקטין מתחת לגיל 15, המתמקדות במיניותו תיחשבנה לעברה של הטרדה מינית. הוראה זו הוספה בתיקון לחוק מיום 8.8.2007. תיקון זה נועד במפורש, כך על פי דברי ההסבר להצעת החוק, להתמודד עם פניות בעלות תוכן מיני המופנות לקטינים במופעים שונים של האינטרנט, כדוגמת ערוצי צ'אט ופורומים שונים שאליהם קטינים רבים נוהגים לגלוש. ראו הצעת חוק לתיקון חוק למניעת הטרדה מינית (תיקון מס' 4) (הטרדה מינית של קטין שטרם מלאו לו 14 שנים), התשס"ז–2006, ה"ח הכנסת 123. בכל הנוגע לסינון תכנים על פי קריטריון של גיל, יש תוכנות המציעות מנגנונים של וידוא גיל (Age verification), כדוגמת www.adultcheck.com. תוכנות מעין אלה נועדו לשרת את ספקיות התכנים באינטרנט ולא את משתמשי האינטרנט. לכן האוריינטציה של תוכנות אלה היא להציב רף סינון שיפטור את ספק שירותי התוכן מאחריות, גם אם המסננת לא תמנע בפועל מקטינים להיחשף לתכנים פוגעניים.

144 טענה זו נטענה במפורש והתקבלה בבית משפט בצרפת, שבו חויבו ספקיות הגישה לאינטרנט לחסום גישה לאתר אינטרנט בשם "Copwatch Nord Paris I-D-F", שנועד להציג מקרים שבהם הפעילו שוטרים צרפתים את סמכותם לרעה. קצין משטרה צרפתי התלונן למשרד הפנים הצרפתי, לאחר שקיבל איום בדמות קליע שהושם בתיבת הדואר הפרטית שלו, בעקבות פרסום שהועלה לאתר האינטרנט. משרד הפנים עתר לבית המשפט (Tribunal De Grande Instance De Paris) להוצאת צו לסינון תכנים מסוימים מתוך אתר האינטרנט המדובר אשר מסגירים פרטים אישיים ורגישים אחרים של אנשי המשטרה המצולמים באתר. איגוד האינטרנט הצרפתי התנגד לבקשה זו בטענה שאינו יכול לבצע את הסינון המבוקש מבחינה טכנית, כיוון שאין באפשרותו לאתר את שרת האירוח של האתר ולהרכיב עליו את הסינון המבוקש. בעקבות זאת הורה בית המשפט הצרפתי על החלטה גורפת יותר של חסימת גישה לאתר האינטרנט כולו באמצעות ספקי הגישה הצרפתיים. ראו Ministre de l'Interieur à la société Free, No. RG 11/58052 (Tribunal De Grande Instance De Paris, 14.11.2011), *available at* http://dl.free.fr/rdghZJ7Os.

145 בעבר צומצם בפסיקה אופן הפעלת סמכותו של מפקד מחוז במשטרה להורות על סגירת חצרים פיזיים שנחשדו כמשמשים למשחקים אסורים. ראו, למשל, עת"מ (מחוזי י-ם) 1709/09 **ראזם נ' מפקד מחוז ירושלים** (פורסם בנבו, 30.12.2009); עת"מ (מחוזי י-ם) 1666/09 **קאזם נ' משטרת ישראל** (פורסם בנבו, 14.12.2009).

146 ראו Organization for Security and Cooperation in Europe (OSCE), Freedom of Expression on the Internet: Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow

nevo.co.il

לאתרים המבוססת על כתובת ה־IP של אתר האינטרנט, ייתכן שעם חסימת הגישה לכתובת ה־IP ייחסמו גם אתרי אינטרנט נוספים המתארחים באותו שרת הנושא את כתובת ה־IP המדוברת.[147] בכל הנוגע לסינון תכנים, במקרה של הכללת יתר של תכנים מותרים, תיגרם פגיעה עודפת בחופש הביטוי.

חמישית, ככל שהאכיפה המגננתית־הכופה מתבצעת בפועל בידי ספקיות השירות, וכשמשימת האכיפה הזאת מוטלת על כתפיהן מכוח חוק או הוראה מחייבת אחרת של אורגן של המדינה, מתעוררת השאלה הכללית בדבר אפשרותה של המדינה לבצע פעולה של מעין מיקור חוץ של אכיפת הדין הפלילי.[148]

שישית, אכיפה מגננתית־כופה אין באפשרותה להרתיע את עברייני האינטרנט מלשוב ולבצע את מעשיהם, בעיקר אם העלויות של ניסיון ביצוע העברות אינן גבוהות מבחינתם. במקרה כזה, ככל שאין חשש לתפיסה ולענישה של העבריין הפוטנציאלי, הרי שאין תמריץ שלילי כבד משקל לחדול מביצוע העברות.

5. אכיפה התקפית

א) הצגת החלופה

הכוונה הכללית באכיפה התקפית היא למניעת שימוש, או כפי שריידנברג כינה זאת: הטלת סנקציות אלקטרוניות (Electronic Sanctions).[149] באכיפה התקפית ניתן לסמן שני יעדי תקיפה: **אתרי האינטרנט החשודים** מחד גיסא **ומשתמשי המחשב החשודים** מאידך גיסא. אתייחס תחילה לאכיפה התקפית כלפי אתרי האינטרנט. בקטגוריה זו ניתן לכלול אמצעים טכנולוגיים ומשפטיים שהרשות משתמשת בהם על מנת לפגוע באתר האינטרנט בעל התכנים האסורים בעצמה או בחיוב מנהל האתר או מנהל השרת שבו מאוחסן האתר לסגור אותו או לשנות

---

of Information and Media Pluralism on the Internet in OSCE Participating States 31–34, 136–180 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1906717. הארגון התנגד לחקיקה מדינתית הכופה סינון תכנים וחסימת גישה לאתרי אינטרנט פוגעניים, ומציע להכיר אך ורק במנגנונים אלה כשהם על בסיס וולונטרי ושקוף למשתמשי האינטרנט, היכולים לערער על החלטותיהם.

147 ראו: Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 5, 14 (Ronald Deibert, John Palfrey, Rafal Rohozinski & Jonathan Zittrain eds., 2008).

148 טענה זו קשורה לנושא העברת חובות האכיפה לספקיות שירות באינטרנט, נושא שיידון בחלק נפרד להלן.

149 ראו Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. TECH. J. 213, 228–229 (2003–2004). ריידנברג התייחס להטלת סנקציות שכאלה בידי המדינה. ההנחה הכוללת היא שסנקציות מעין אלה תטיל המדינה או שיוטלו מכוח הוראה מחייבת של המדינה. קיימת עמדה הגורסת כי גם תאגידים יכולים ליזום הפעלת סנקציות אלקטרוניות נגד מחשבים ש"תקפו" אותם, בבחינת עזרה עצמית התקפית, ראו Michael E. O'neil, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237 (2000); Curtis E. A. Karnow, *Counterstrike*, *in* CYBERCRIME – DIGITAL COPS AND LAWS IN A NETWORKED ENVIRONMENT 135, 140–148 (Jack M. Balkin et al. eds., 2007). כן ראו Brenner, *Distributed Security*, לעיל ה"ש 21, בעמ' 15–18. לביקורת על עמדה זו, ראו Kerr, לעיל ה"ש 61, בעמ' 209–213.

nevo.co.il

מתכניו. האכיפה ההתקפית כלפי אתרי אינטרנט חשודים יכולה להתבצע בכמה אופנים: **האחד**, באמצעות מתקפות של מניעת שירות (Denial of Service). התקפות אלה יכול שיבוצעו באמצעות מחשב אחד, אם מדובר במחשב אחד חזק ובפס־תקשורת רחב במיוחד, ומנגד מדובר באתר אינטרנט היושב על שרת קטן שקל להציפו בתעבורה ובכך לחסום את הגישה אליו. לחלופין, יכול שהתקפות אלה יבוצעו בידי קבוצת מחשבים המכונים "zombies", אשר "יגויסו" לשמש לביצוע התקפות מבוזרות למניעת שירות (DDoS); **השני**, באמצעות חדירה לאתר האינטרנט הנדון ושינוי תכנים או מחיקתם; **השלישי**, מתן הוראה ישירה למנהל אתר האינטרנט או בעל השרת המאחסן את האתר "לסגור" אותו; **הרביעי**, תפיסת השרת שבו שוכן האתר וניתוק או מחיקה של המידע האסור.[150]

בכל הנוגע לאכיפה התקפית כלפי משתמשי האינטרנט, ניתן לציין פעולות לניתוק הגישה לאינטרנט של משתמשים חשודים. עד כה התפתח הדיון בשיטת אכיפה זו בכל הנוגע למשתמשי אינטרנט המפרים בשיטתיות זכויות יוצרים מוגנות באתרים לשיתוף קבצים באינטרנט. בכמה מדינות בעולם נחקקו חוקים המטמיעים מודל של "שלוש פסילות" (Three Strikes Policy), ולפיו משתמש אינטרנט שנתפס שלוש פעמים בפרק זמן נתון בהפצה של חומר המפר זכויות יוצרים מוגנות ינותק מכל ספקי הגישה לאינטרנט במדינתו. חקיקה מעין זו התקבלה בצרפת, בטאיוואן, בדרום קוריאה, בניו זילנד ובבריטניה, והיא נשקלת במדינות נוספות.[151] באירלנד ובארצות הברית קיים מנגנון דומה שאינו פרי חקיקה אלא פרי הסכם בין ספקיות הגישה לאינטרנט לבין נציגי תעשיית המוזיקה והסרטים.[152]

---

150 למען שמירה על הקוהרנטיות בטקסונומיה שאני מציג בפרק זה, אציין כי התייחסתי לעיל בפרק ב. ד.4 לפעולות של חסימת גישה לאתרי אינטרנט או סינון תוכניהם כפעולות של אכיפה מגננתית כופה ולא אכיפה התקפית. פעולות אלה מכוונות במישרין לציבור גולשי האינטרנט וסותמות את צינור התקשורת שלהם אל אתר האינטרנט. כך בעקיפין, ולא במישרין כבמקרה של אכיפה התקפית, נפגע אתר האינטרנט החשוד. פעולות של הפלת אתרים או הוראה לסגירתם משליכות על כל ציבור גולשי האינטרנט בעולם. לעומת זאת חסימת גישה לאתר אינטרנט או סינון תכניו בדרך ממנו אל ציבור הגולשים – אלה הן פעולות החלות על גולשי האינטרנט במדינה האוכפת, בעוד שאר גולשי האינטרנט בעולם יכולים להמשיך ולהיכנס לאתר האינטרנט האמור.

151 לסקירת המדינות שאימצו את המודל בחקיקתן, ראו Eldar Haber, *The French Revolution 2.0: Copyright and the Three Strikes Policy*, 2 HARV. J. SPORTS & ENT. J. 297, 300–306 (2011).

152 ההסדר באירלנד הוא פרי הסכם בין ספקית הגישה לאינטרנט הגדולה באירלנד, Eircom, לבין נציגי תעשיית המוזיקה האירית. על פי ההסכם, Eircom תספק פרטים מזהים על משתפי־קבצים העוברים על דיני זכויות היוצרים לפדרציית התקליטים האירית (Irish Recorded Music Association – IRMA) תוך יישום, במקביל, של מודל "שלוש הפסילות". בארצות הברית נחתם הסכם בין מרבית ספקיות הגישה הגדולות לאינטרנט לבין נציגי תעשיית הסרטים והמוזיקה ליישום של מודל "שש הפסילות", המאפשר, על פי שמו, להטיל סנקציות אלקטרוניות על מי שהפר לכאורה בפרק זמן נתון זכויות יוצרים מוגנות בשש הזדמנויות. על פי ההסכם, מדובר לא רק בסנקצייה של ניתוק הגישה לאינטרנט באמצעות הספקיות החתומות על ההסכם, אלא גם בסנקציות מרוכבות יותר, כגון האטת קצב הגלישה, העלאת דף בדפדפן האינטרנט הדורש ליצור קשר עם ספקית השירות וכד׳. ראו Fahmida Y. Rashid, *ISPs Agree to Six Strikes System Warning Users of Suspected Online Piracy*, EWEEK (8.7.2011) http://www.eweek.com/c/a/Messaging-and-Collaboration/ISPs-Agree-to-Six-Strikes-System-Warning-Users-of-Suspected-Online-Piracy-668389.

nevo.co.il

ב) הערכת החלופה

פעולות אכיפה התקפיות הן אטרקטיביות למדי במישור יעילותן: **ראשית**, הן זולות, קלות יחסית לביצוע ומהירות לביצוע; **שנית**, הן מאפשרות להתגבר, ולו חלקית, על האנונימיות של משתמשי האינטרנט החשודים, שכן לכאורה די בכתובת ה־IP שממנה פעל החשוד על מנת להפעיל נגדו את הסנקציות ההתקפיות, ואין צורך ב"הרמת המסך" אל זהות המשתמש המצוי מאחורי כתובת ה־IP. אל מול נימוקים אלה יש לבחון את המשמעויות של שימוש באכיפה התקפית, בעיקר כאשר שימוש זה בא כחלופה ממשית לאכיפה הפלילית המסורתית:

ראשית, אכיפה התקפית כלפי אתרי אינטרנט או משתמשי אינטרנט המצויים בחו"ל משמעה ביצוע פעולה אקסטרה־טריטוריאלית היכולה להיתפש, במשקפי תפישה טריטוריאליסטית, כפגיעה בריבונותה של המדינה שבה נמצא משתמש האינטרנט או שממנה הוא פועל. בשונה מהאכיפה המגננתית־הכופה, שבה נחסמת הגישה מתוך גבולות המדינה אל אתרי אינטרנט זרים, כאן הפעולה מבוצעת ישירות כלפי משתמש האינטרנט או אתר האינטרנט, וככל שאלה מצויים מחוץ לטריטוריה של המדינה האוכפת, הרי שעלול הדבר לעלות כדי חריגה מסמכות האכיפה במישור הבין־לאומי.[153]

שנית, לעתים פעולות האכיפה ההתקפית לא תהיינה אפקטיביות, אם המידע האגור באתר, שאותו מבקשים "לתקוף", כבר פרש כנפיים והופץ ברחבי הרשת. כדוגמה לשני הטיעונים האחרונים שמניתי – טיעון הסמכות וטיעון האפקטיביות – ניתן להביא את פרשת **ויקיליקס (Wikileaks)**.[154] מבחינתן של המדינות שסודותיהן נחשפו, ככל שמוגדרת עברה של איסור גילוי סודות רשמיים או עברה דומה, מדובר לכאורה בעברה פלילית על פי דיני מדינתן. היות שאתר ויקיליקס שכן בשרתים מחוץ לתחום שיפוטן, והיות שסודה של מדינה פלונית אינו סודה

---

153 לעומת זאת כשאתר האינטרנט מצוי בשטחה של המדינה האוכפת, ייתכן שניתן להחיל הוראות חוק מסוימות על הסיטואציה ולחייב את סגירתו. כך, למשל, סעיף 229(א)(1) לחוק העונשין מסמיך מפקד מחוז במשטרה להורות על סגירת מקום הימורים, הגרלות או משחקים אסורים. כזכור, הראיתי לעיל בפרק ב.ד.4., כשהצגתי את האכיפה המגננתית־הכופה, כי משטרת ישראל ביקשה להשתמש בסעיף 229(א)(1) לחוק העונשין כעוגן להורות על חסימת גישה לאתרי אינטרנט. ניסיונה זה של המשטרה נדחה בבית המשפט העליון בעילה של חוסר סמכות. על פי מילות סעיף החוק, דווקא פרשנות של סגירת אתר הימורים בידי המשטרה מוקשה פחות מפרשנות הקוראת לתוך סעיף זה גם את הסמכות להורות לספקיות הגישה על חסימת גישה לאתר הימורים (הגם שבעיית הפרשנות של אתר אינטרנט כ"מקום" נותרת בעינה).

בנוסף, אפשר לשקול שימוש בסמכות ההפסקה המנהלית שבסעיף 20 לחוק רישוי עסקים, התשכ"ח–1968. על פי סמכות זו, אם עסק מסוים מתנהל באינטרנט, ומופרים תנאים מסוימים של הרישיון, או שהעסק התנהל ללא רישיון כמתחייב, רשאי הממונה על המחוז במשרד הפנים (או גורמים אחרים הנקובים בחוק) – "לצוות בכתב על הפסקה ארעית של העיסוק בעסק, אם בסגירת החצרים ואם בכל דרך אחרת הנראית לו מתאימה בנסיבות הענין כדי להביא לידי הפסקה של ממש בעיסוק". כיוון שהחוק מאפשר לא רק מתן הוראה ל"סגירת החצרים" אלא גם הפסקת העיסוק "בכל דרך אחרת", נראה כי מילות החוק פתוחות לפרשנות שלפיה ניתן להורות על סגירת אתר אינטרנט יותר ממילותיו של סעיף 229(א)(1) לחוק העונשין, אשר דיבר כזכור על "מקום משחקים אסורים או מקום לעריכת הגרלות או הימורים".

154 לפרטי הפרשה ראו לעיל בפרק המבוא, בה"ש 13.

nevo.co.il

של מדינה אלמונית.[155] ניתן להניח שיקשה על כל מדינה להשיג שיתוף פעולה בחקירה ובהסגרה של מפעיל האתר, אסאנג׳, בגין פרסומיו באתר. אף מדינה אחת לא הודתה בכך רשמית כמובן, אבל שרתי ויקיליקס ספגו מתקפות מבוזרות של מניעת שירות (DDoS).[156] במקרה של שרתי ויקיליקס נודע כי הם הקימו יכולת לנייד את המידע ממקום למקום באמצעות אתרי מראה (Mirror sites), הכוללים שכפולים של המידע בכמה שרתים, ומכאן שבפועל גם התקפות של DDoS אין בכוחן להביא למניעת הגישה אל המידע הסודי. יתרה מזאת, המידע הסודי ניתן להעתקה בידי גורמים שונים הצופים בו, ואם המידע כבר הועתק והגיע ליעדים רבים בטרם מוּפלים השרתים, הרי שהוא ימשיך ״לחיות״ ברשותם של הצרכנים שהספיקו להיחשף אליו ולהעתיקו לרשותם. על כן האפקטיביות של הפלת שרתי ויקיליקס כפעולת אכיפה נגד פרסום המידע הסודי, נתונה בספק.

שלישית, אם האכיפה ההתקפית מכוונת כלפי אתר האינטרנט החשוד (ולא כלפי המשתמש עצמו), ניתן לטעון כי האכיפה ההתקפית מביאה לפגיעה רחבה יחסית, השוללת מאתר האינטרנט החשוד גם פעילות לגיטימית שלו. בכך נפגע חופש הביטוי וחופש העיסוק של מפעילי אתר האינטרנט.[157] ועוד, יש לזכור כי הפלה או שיבוש של פעילות אתר אינטרנט זר פוגעת לא רק בגישה של משתמשי האינטרנט מהמדינה האוכפת אלא גם בגישה של כלל משתמשי האינטרנט בעולם. ייתכן מצב שבו מדינות שונות תחלנה סטנדרט שונה באשר לשאלת

---

155 השוו למשל לפרשת מרדכי ואנונו, שהורשע ונידון ל־18 שנות מאסר בפועל בגין ביצוע עברות של סיוע לאויב במלחמה, ריגול חמור, לפי סעיפים 99(א) ו־113(ב) (בהתאמה) לחוק העונשין, לאחר שחשף בפני עיתונאי בריטי של ה״סאנדי טיימס״ נתונים רבים על פעילות הקריה למחקר גרעיני בדימונה, נתונים שאליהם נחשף במסגרת עבודתו שם. ראו ע״פ 172/88 **ואנונו נ׳ מדינת ישראל**, פ״ד מד(3) 265 (1990). העיתונאי שפרסם את הדברים בכתבת שער של העיתון הבריטי ב־5.10.1986, פגע בעצמו אף הוא בסודותיה של מדינת ישראל, אלא שהוא ביצע את מעשהו במקום שבו מותר לפרסם תכנים אלה, שכן סודותיה של מדינת ישראל אינם סודותיה של בריטניה. מכאן שמדינת ישראל לא הייתה יכולה לבקש את הסגרתו מבריטניה. יתר על כן, גם ואנונו עצמו ביצע פיזית את עברותיו באוסטרליה ובבריטניה, כשפגש שם עיתונאי ה״סאנדי טיימס״. מכאן ניתן להניח כי אילו הייתה מדינת ישראל מבקשת את הסגרתו של ואנונו מבריטניה או מכל מדינה אחרת, הרי שהיתה נענית בשלילה מן הטעם שלא הוכחה במעשהו ״פליליות כפולה״. בפועל, על פי הפרסומים, הובא ואנונו לישראל בפעולה חד־צדדית חשאית. ראו, למשל, יוסי מלמן ״מאוסטרליה ועד לפיתוי ע״י ׳סינדי׳: כך נחטף ואנונו״ **הארץ Online** (21.4.2004) http://www.haaretz.co.il/hasite/spages/417896.html.

156 ראו למשל שי ענבל ״האקרים תקפו את ויקיליקס, המסמכים החסויים פורסמו בעיתונות״ **כלכליסט** (29.11.2010) http://www.calcalist.co.il/internet/articles/0,7340,L-3436302,00.html; John Leyden, *Lone Hacker Theory in Wikileaks DDoS Attack: Well Obviously it was the Governments etc.*, THE REGISTER (29.11.2010) http://www.theregister.co.uk/2010/11/29/wikileaks_ddos/.

157 בארצות הברית נדונה החלטתה של רשות ההגירה והמכס (ICE) לתפוס שני שמות מתחם Rojadirecta.com ו־Rojadirecta.org. מדובר באתרי אינטרנט שאוחסנו פיזית בשרתים אמריקניים והציעו שירות של קישוריות לשידורי ספורט באינטרנט ממקורות מחוץ לארצות הברית אשר מפרים זכויות משדרים בארצות הברית. במסגרת התנגדות לתפיסת שמות המתחם נטען לפגיעה בחופש הביטוי של אתרי האינטרנט, ובית המשפט הפדרלי במדינת ניו יורק דחה את הטענה. ראו Puerto 80 Projects, S.L.U. v. United States, Case No. 11 Cv. 3983 (PAC) (S.D.N.Y., 2011), *available at* http://www.eff.org/files/RojadirectaOrder.pdf. כן הועלתה הטענה שאתר האינטרנט יכול להעתיק את מיקומו לשרתים מחוץ לארצות הברית תוך שינוי שם המתחם שלו, ובכך לעקוף את סמכותה של ארצות הברית לתפוס את שרתי האתר. בפועל, אתר Rojadirecta אכן שינה את שם המתחם ל־Rojadirecta.es, Rojadirecta.in ו־Rojadirecta.me והעתיק פיזית את מקום האירוח שלו למדינות מחוץ לארצות הברית.

nevo.co.il

חוקיותו של אתר האינטרנט האמור, ובמקרה של אכיפה התקפית, למעשה תְּכפה המדינה האוכפת את הסטנדרט שלה על המדינות האחרות שמהן מתבצעת גלישה לאתר.

רביעית, כשהאכיפה ההתקפית מכוונת כלפי משתמש אינטרנט חשוד (ולא כלפי האתר עצמו), יש באכיפה ההתקפית כדי לפגוע בזכותו להשתמש באופן כללי באינטרנט. זכות זו יכולה להיגזר מהזכות לחופש המידע, לחופש ביטוי, מכבוד האדם במובן של אוטונומיה של הרצון, וכן ניתן לתפוש אותה כזכות חוקתית עצמאית.[158]

חמישית, האכיפה ההתקפית היא למעשה אקט של ענישה[159] לא שיפוטית, והיא מעוררת למעשה את הקשיים שמעוררות – להבדיל – פעולות כגון סיכול ממוקד, שבהן הרשות המנהלית מוציאה לפועל עונש שלא על בסיס הליך בירור משפטי מוסדר.

שישית, עבריין אינטרנט עדיין יוכל להסתתר מאחורי מערכות אנונימיזציה או מאחורי שרתי Proxy, ובמקרה כזה עלולות פעולות האכיפה ההתקפית להתבצע כלפי המחשבים המתווכים ולא כלפי המחשבים המשמשים במישרין את מבצע העבירה.[160] בעקבות זאת תיגרם תוצאה לא רצויה, בשני מובנים: הן במובן של היעדר אכיפה כלפי מבצע העבירה והן במובן של פגיעה במשתמשי מחשב אחרים תמימים.

בסיכומו של דבר, נראה כי פעולות אכיפה התקפית יעילות ומסוגלות לכאורה להציב חלופה כוללת לאכיפה הפלילית המדינתית, שכן היא מתפרשת על קשת רחבה של פעילויות עברייניות. אולם פגיעתה של השיטה גדולה, וככל הנראה אינה ישימה מבחינת המשפט הבין־לאומי, שכן יש בה משום התערבות ממשית ורחבה בזכויות של זרים וכן בריבונות של מדינות זרות, וכן היא אינה ראויה מבחינה חוקתית־פנימית, שכן יש בה משום פגיעה לא מידתית בזכות להליך הוגן ובזכויות הנלוות לשימוש באינטרנט (ביטוי, עיסוק, חופש מידע וכו׳).

6. אכיפה כלכלית – סיכול אמצעי התשלום

א) הצגת החלופה

חלק מהפעילות העבריינית במרחב הסייבר, גם אם לא כולה, מטרתה השגת רווח כספי. בחלק מאותן תופעות פשיעה מבצע העבירה מציע שירות כלשהו, בתשלום, לקהל לקוחות שעמו הוא מתקשר, וקהל הלקוחות משלם עבור השירות הפלילי. במיוחד אמורים הדברים באתרי הימורים מקוונים ובאתרים המציעים תכנים מתועבים ופדופיליים תמורת תשלום. בכל הנוגע לאותם אתרים, התשלום מהלקוחות למבצעי העברות כמעט תמיד מתווך בידי ספק שירותי תשלום. התשלום המקוון יכול להתבצע באמצעות כרטיסי אשראי, באמצעות שירותי העברת כספים באופן מקוון, באמצעות כרטיסי חיוב ספציפיים הנרכשים במקום אחר ושפרטיהם מוזנים באתר האינטרנט החשוד ועוד. רעיון האכיפה על דרך של סיכול אמצעי התשלום נועד לחסום

158 למעמדה של זכות השימוש באינטרנט, ראו בירנהק, לעיל ה״ש 128, בעמ׳ 435–443.

159 ריצ׳רד ג׳ונס (Jones) המשיל את האכיפה ההתקפית הכוללת השבתה של אתר אינטרנט ל״מאסר וירטואלי״ (Virtual imprisonment). ראו Richard Jones, *Digital Rule: Punishment, Control and Technology*, 2 PUNISHMENT & SOCIETY 5 (2000).

160 ראו Kerr, לעיל ה״ש 61, בעמ׳ 212–213.

nevo.co.il

את "צינור החמצן" של ספקיות השירותים הפליליים בתשלום. בלי אפשרות לממש את התשלום אין כל מניע להמשך ביצוע אותן עברות פליליות.

בכל הנוגע לאכיפה פלילית באמצעות ספקיות שירותי התשלום, אפשר לחשוב, רעיונית, על כמה מודלים: **הראשון**, חקיקה האוסרת על ספקיות שירותי התשלום להעניק שירותי סליקת תשלומים לבתי עסק המספקים שירותי הימורים מקוונים. החקיקה תצטרך להגדיר מהם הנטלים המוטלים על ספקי שירותי התשלום, לוודא את טיב השירות שמעניק בית העסק על מנת לאפשר לספקיות שירותי התשלום להיערך כדבעי מראש ולהימנע מהטלת אחריות עליהן; **השני**, קביעת משטר רישוי לספקיות שירותי התשלום, ובו התחייבות להימנע מסליקה של רשימת בתי עסק שתועבר על ידי המדינה. לפי מודל זה, נטל איתור השירותים המקוונים האסורים הוא על המדינה, ואת הפיקוח יעשה רגולטור; **השלישי**, הטלת אחריות פלילית על ספקיות שירותי התשלום כמסייעות לביצוע העברה המיוחסת לספקי השירותים האסורים. על פי מודל זה, ייאמר כי ספקיות שירותי התשלום מאפשרות את ביצוע העברה ומקלות אותו, כעולה מהגדרת ה"מסייע" בחוק העונשין.[161]

בישראל אין חקיקה האוסרת על סליקת תשלומים באינטרנט עבור שירותים פליליים. כמו כן עד כה לא הועמדו לדין חברות שהעמידו אמצעי תשלום עבור אתרי אינטרנט שהציעו שירותים אסורים כגון הימורים, הגם שלפחות חקירה פלילית אחת התנהלה נגד חברת כ.א.ל.[162] עם זאת קיימת הוראה של המפקח על הבנקים[163] המחייבת חברות כרטיסי אשראי ישראליות להימנע מאישור עסקה שנעשתה באמצעות כרטיסי אשראי שהן הנפיקו, אם קיים חשש כי החיוב הוא בגין משחקים אסורים, הגרלות או הימורים, האסורים על פי דיני העונשין בישראל, ואם השירות ניתן בישראל או בכל מדינה אחרת שבה אסורה הפעילות האמורה. יתר על כן, חברות אשראי המתקשרות בהסכם לסליקת עסקאות במסמך חסר עם בתי עסק שתחום פעילותם בענפים עתירי סיכון – **הימורים, פורנוגרפיה ושיווק תרופות**[164] – תחויבנה, טרם ההתקשרות, להצטייד בחוות דעת משפטית המכשירה את פעילות בית העסק במדינתו של בית העסק ושל המתווכים הפועלים

---

161 סעיף 31 לחוק העונשין: "מי אשר, לפני עשיית העבירה או בשעת עשייתה, עשה מעשה כדי לאפשר את הביצוע, להקל עליו או לאבטח אותו, או למנוע את תפיסת המבצע, גילוי העבירה או שללה, או כדי לתרום בדרך אחרת ליצירת תנאים לשם עשיית העבירה, הוא מסייע".

162 ראו דיווח על החקירה אצל חן מענית "בועז צ'צ'יק, מנכ"ל כ.א.ל. לשעבר, נחקר בחשד להלבנת הון" **גלובס Online** (25.12.2011) http://www.globes.co.il/news/article.aspx?did=1000709866. באותו מקרה כללה החקירה גם חשד לעברות של הלבנת הון ורישום כוזב במסמכי תאגיד, שכן יוחס לחברת כ.א.ל. חשד כי ניסתה להסוות את עסקאות הסליקה הללו כעסקאות תמימות, באמצעות שינוי רישומן.

163 ראו "מניעת הלבנת הון ומימון טרור וזיהוי לקוחות" **הוראות המפקח על הבנקים** מס' 411 (ינואר 2011). הפרת הוראות המפקח יכולה לשאת תוצאות במישור הרגולטורי, לרבות קנס כספי, ועלולה להוביל לפגיעה ברישיון הבנק.

164 נושא שיווק התרופות הוכנס לגדר המונח "ענפים עתירי סיכון" בשל ריבוי אתרי האינטרנט המציעים תרופות מזויפות כדוגמת ויאגרה. בכמה מקרים נפתחו חקירות פליליות בגין עברות על סעיף 60(א)(3) לפקודת סימני מסחר [נוסח חדש], התשל"ב–1972, סעיפים 26(א), 42(א), 47 ועוד לפקודת הרוקחים [נוסח חדש], התשמ"א–1981, עברות על סעיף 212(א)(13) לפקודת המכס, 1937 וכן עברות של מעשה פזיזות ורשלנות וזיוף בנסיבות מחמירות לפי סעיפים 338 ו־418 סיפה (בהתאמה) לחוק העונשין. ראו, למשל, את ב"ש (שלום ראשל"צ) 7461/04 **מדינת ישראל נ' חברת הרדוף** (פורסם בנבו, 14.11.2004); ת"פ (שלום ת"א) 7987/07 **מדינת ישראל נ' אוריאל** (פורסם בנבו, 3.7.2011).

nevo.co.il

בשבילו, עם חברת האשראי; כן תידרש חברת האשראי לבדוק, במעמד ההתקשרות עם בית העסק, כי הלה אינו פועל להתקשרות עם לקוחות ממדינות שבהן אסורה פעילותו; כן תידרש חברת האשראי לבדוק תקופתית את פעילות בית העסק על מנת לבחון אם לא שינה את אופני התנהלותו מבחינת תכניו ומבחינת התקשרותו עם לקוחות במדינות שבהן פעילותו אסורה.

בארצות הברית נודע המקרה שבו הרגולטור בנושא אלכוהול, טבק ונשק (The Federal Bureau of Alcohol, Tobacco and Firearms) הורה לחברות האשראי שלא לסלוק תשלומים באינטרנט של הזמנת סיגריות. זאת לאחר שהתפשטה תופעה של אתרי אינטרנט שהתמקמו במדינות בארצות הברית שבהן המיסוי על סיגריות נמוך יותר, וכך משתמשי אינטרנט ממדינות שבהן המיסוי גבוה גלשו לאותם אתרים והזמינו אצלם סיגריות במחירים מופחתים (גם בתוספת עלות המשלוח לבית הלקוח). בלחצן של המדינות שהפסידו כספים בשל פערי המיסוי הללו על הרגולטור הפדרלי, הוציא זה הנחיה להימנע מסליקת עסקאות של הזמנת סיגריות באינטרנט. בשל הוראה זו נכרת הענף שעליו ישבו וצמחו אתרי האינטרנט הללו, ותופעת הפסדי המיסוי פסקה כמעט מיד.[165]

בכל הנוגע להימורים באינטרנט, המדיניות בארצות הברית משולבת: חקיקה פדרלית אוסרת על אתרי הימורים לקבל תשלומים ממהמרים המשתמשים באמצעי תשלום אמריקניים,[166] בעוד שאיסור ישיר על חברות התשלומים אינו נקוב בחקיקה אלא בהוראות של ה־Federal Reserve האמריקני, שהוא בעל סמכות רגולטורית כופה כלפי כל סוגי החברות (האמריקניות) המספקות שירותי תשלום (חברות אשראי, חברות המספקות שירותי תשלום באמצעות חשבון אינטרנטי כדוגמת pay-pal וכיוצא בזה).[167] על המדיניות האמריקנית נמתחה ביקורת שלפיה מדיניות זאת מוצגת כביכול באור של הגנה מפני הלבנת הון כתופעת פשיעה בין־לאומית והגנה מפני נזקי ההימורים באינטרנט (התמכרות, גישת קטינים להימורים ועוד), אך בפועל המטרה האמיתית של הרשויות האמריקניות היא למנוע בריחת הכנסות ממיסוי הימורים באינטרנט.[168] כיוון שאתרי ההימורים באינטרנט יושבים מחוץ לגבולות ארצות הברית, המיסוי על רווחיהם אינו מגיע לקופת ארצות הברית. זו, כך הטענה, המטרה האמתית של האכיפה הכלכלית האמריקנית להימורים באינטרנט. איני מתכוון להיכנס לשאלת נכונותה של ביקורת זו, כיוון שמטרתי כאן היא לבדוק את האמצעי האכיפתי של סיכול אמצעי התשלום כאמצעי אכיפה חלופי לאכיפה הפלילית המדינתית. לכן אתנתק מההקשר האמריקני הספציפי ואף מההקשר הספציפי של הימורים באינטרנט ואנסה להעריך להלן את החלופה האכיפתית עצמה.

---

165 ראו Bob Tedeschi, *Now That Credit Card Companies Won't Handle Online Tobacco Sales, Many Merchants Are Calling it Quits*, N.Y. TIMES (4.4.2005), http://query.nytimes.com/gst/fullpage.html?res=9800E3DD1E3FF937A35757C0A9639C8B63.

166 ראו Unlawful Internet Gambling Enforcement Act 2006, 31 U.S.C. § 5363.

167 ראו Code of Federal Regulations, Prohibiting on Funding of Unlawful Internet Gambling, 12 C.F.R. § 233, *available at* http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=%2Findex.tpl.

168 ראו Gale, לעיל ה״ש 38, בעמ׳ 545–549. ראו עוד בהמשך התייחסותי לבוררות בין ארצות הברית לבין אנטיגואה בנוגע למדיניות האכיפה הכלכלית של ארצות הברית בנוגע להימורים באינטרנט, להלן בפרק 2(ה)(2)(א).

nevo.co.il

ב) הערכת החלופה

החלופה המתמקדת בסיכול אמצעי התשלום מוגבלת מעצם טיבה אך ורק לחלק מסוים של הפעילות הפלילית המקוונת, קרי לחלק שבו שני מעורבים בעסקת העברה מתקשרים ביניהם, והאחד מעניק לשני שירותים פליליים תמורת תשלום. בכל המקרים שבהם העברה הפלילית אינה כרוכה בפעילות כספית, הרי שחלופה זו מראש אינה רלוונטית.

מלבד זאת, גם בנוגע לעברות הרלוונטיות לענייננו, נראה כי החלופה מוגבלת ביעילותה הטכנית. כיוון שמדובר בהוראה הניתנת (בחקיקה או באמצעות הרגולטור) לספקיות שירותי התשלום המקוון, אשר פרנסתן תלויה בהספקת שירותים אלה, וכיוון שיש חשש משלילת עסקאות לגיטימיות, אין מנוס מהגדרה צרה וברורה (ברמת קטגוריות ברורות) של העסקאות האסורות לסליקה בידי ספקיות שירותי התשלום. מנהלי השירותים האסורים יוכלו לנסות לחמוק מכניסה לקטגוריות הפסולות לסליקה באמצעות הירשמות אצל ספק שירותי הסליקה כשירות תמים של בידור או כדומה. כך יתאפשר לחמוק מה"רדאר" של ספקיות שירותי הסליקה.[169] יש לזכור כי האינטרס הצר של ספקיות שירותי הסליקה הוא להצליח לציית להוראה הכופה מבלי לפגוע יתר על המידה בהכנסותיהן, ועל כן ודאי שלא יהיה להן אינטרס להפעיל אמצעים וולונטרית על מנת לאתר עסקאות פליליות המוסוות כעסקאות לגיטימיות. יתר על כן, יכול מנהל אתר המציע שירותים אסורים לפתוח עסק נוסף, עם אתר אינטרנט משלו אשר ישמש מתווך תמים לצורך העברת הכסף לאתר האסור. כל תפקידו של האתר המתווך יהיה למעשה להלבין את מהלך העברת התשלום תוך עקיפת ההוראה האוסרת על סליקת הפעילות האסורה. אין יכולת מעשית או חוקית לעקוב אחר הטרנסאקציות שיבוצעו מהאתר המתווך לאתר האסור, שכן משמעות הדבר היא למעשה ניטור של כל הפעילות העסקית המקוונת, מה שבוודאי אינו מתקבל על הדעת.

בסיכומו של דבר, החלופה הכלכלית של סיכול אמצעי התשלום לטרנסאקציות פליליות מציעה פתרון אכיפתי חלקי ביותר, הן מבחינת היקף פרישתו והן מבחינת יעילותו המעשית בתוך תחומי הפרישה שלו.

7. המודל המניעתי המשולב של קוזלובסקי

א) הצגת החלופה

הראיתי לעיל[170] כיצד אפיין קוזלובסקי את מודל החקירה הפלילית הנוהג בעולם הפיזי: התמקדות במבצע העברה, המשפט הפלילי נתפש כגורם המרתיע הבלעדי, הקורבן נתפש כפסיבי,

---

169 ראו את הטענה למשל אצל: Michael Blankenship, *The Unlawful Internet Gambling Enforcement Act: A Bad Gambling Act? You Betcha!*, 60 RUTGERS L. REV. 485, 496–497 (2008). כן ראו בהקשר זה את דוח החשב הכללי האמריקני משנת 2002, עוד טרם הכניסה לתוקף של הוראות החוק והרגולטור בנושא, שבו צוין החשש מפני אי־יעילותה של השיטה הכופה של ספקיות שירותי התשלום להימנע מסליקת עסקאות הימורים: UNITED STATES GENERAL ACCOUNTING OFFICE REPORT TO CONGRESSIONAL REQUESTERS, INTERNET GAMBLING: AN OVERVIEW OF THE ISSUES 26–27 (Dec. 2002), *available at* http://www.gao.gov/new.items/d0389.pdf.

170 ראו לעיל בפרק ב.ג.3..

nevo.co.il

מטרת החקירה הפלילית היא איסוף ראיות להצגה בבית משפט, האכיפה תלויה בשיקול דעתם של גורמי החקירה והתביעה, ותוצאתה העמדה לדין, הרשעה וענישה פלילית. לטענת קוזלובסקי, במרחב המקוון מתרחש (וצריך להתרחש) שינוי מגמה בדבר האופן שבו נאכף החוק ונשמר סדר. החקירה הפלילית, ובעקבותיה התביעה הפלילית, נדחקות לשוליים. שיטת האכיפה צריכה להשתנות מן הקצה אל הקצה: יש לנקוט טקטיקות אכיפה פרו־אקטיביות, יזומות ולא תגובתיות; יש להגביר את ההסדרה הארכיטקטונית של התנהגות הפרטים כאמצעי למניעה מראש של פשיעה;[171] המודל המניעתי צריך להיות אוטומטי, וככזה – חסר שיקול דעת מתי לאכוף ומתי להימנע מאכיפה;[172] הסנקציות שיוטלו צריכות להיות לא־משפטיות, דהיינו לא יוטל עונש על פורע החוק, אלא סנקציות אוטומטיות של חסימת גישה או הפלת אתר וכן פרסום והוקעה בפומבי באינטרנט; הקרבן הפוטנציאלי צריך להיות אקטיבי, למגן את עצמו מפני עברות באינטרנט; הדגש במודל האכיפה המוצע לא יהיה עוד על מבצע העברה אלא על הגורמים המתווכים, ספקי השירות השונים, שמכיוון שהם מרכזים בידיהם צמתים מרכזיים בתעבורה המקוונת, הם יחויבו במניעה ובבקרה של פעולות עבריייניות ברשת.[173]

כפי שניתן לראות, המודל של קוזלובסקי הוא מעין קונפיגורציה של כמה מן ההצעות שפורטו לעיל לעניין אכיפה לא פלילית לאינטרנט, בדגש על עיתוי האכיפה: מניעה מראש במקום הטלת סנקצייה בדיעבד. קוזלובסקי הציג במחקרו את טענתו בשתי רמות: תיאורית ונורמטיבית. הוא תיאר שינוי מגמה המתרחש לטענתו לנגד עינינו, ובד בבד הצדיק את המודל משיקולים של כורח המציאות, של יעילות ומידתיות בהפעלת כוח.

ב) הערכת החלופה

לטעמי, עמדתו של קוזלובסקי אינה ישימה במלואה, הן טכנולוגית והן משפטית: במצב הטכנולוגי הקיים אין מתאפשר יירוט של מרבית העברות טרם התרחשותן. מבחינה משפטית, הצעת קוזלובסקי מוקשה מכמה טעמים:

האחד, היא הופכת את ספקי השירות בעל כורחם לרשות חוקרת, תובעת ושופטת, בעוד בפועל מדובר בגורם פרטי שאינו מעוניין ואינו מוכשר לעסוק בתחום האכיפה.

---

171 אסף הרדוף הראה שהארכיטקטורה של הרשת יכולה למנוע מראש את העברה עוד בטרם תחילת ביצועה ("קטיעת סיבתיות קדם־התנהגותית", כהגדרתו), במהלך ביצועה ("קטיעת סיבתיות התנהגותית") ואף לאחר ביצועה, ובטרם נגרם הנזק בפועל לקרבן ("קטיעת סיבתיות פוסט־התנהגותית"). ראו הרדוף, לעיל ה"ש 74, בעמ' 167–178 וסקירת המקורות המובאת שם.

172 הכוונה במודל מניעתי אוטומטי היא למודל הקוטע את ההתנהגות המזיקה במהלך הוצאתה אל הפועל ובטרם גרימת הנזק בפועל לקרבנות, ברוח הסרט "דו"ח מיוחד" משנת 2002 שבכיכובו של טום קרוז ובבימויו של סטיבן שפילברג (Minority Report). על פי עלילת הסרט, מפותחת "מערכת קדם־פשע" המאפשרת למנוע מעשי רצח בטרם התרחשותם. לפירוט על עלילת הסרט ראו http://www.imdb.com/title/tt0181689/plotsummary. מבחינה טכנית, הכוונה לביצוע מעין packet interception (ציתות מתמיד לתקשורת באינטרנט לפי נוסחאות קבועות החוזות התנהגות עבריינית) ויירוט כל ההתקשרויות החשודות במהלך התרחשותן.

173 ראו Kozlovski, לעיל ה"ש 13, בפרק 2, בפרט בעמ' 109–110.

nevo.co.il

השני, מניעה מוקדמת עלולה לכלול ex ante התנהגויות אשר תישפטנה ex post ותיקבענה כהתנהגויות מותרות. במיוחד אמורים הדברים לנוכח טענתו של קוזלובסקי כי יש ליטול את שיקול הדעת מגורמי המניעה המוקדמת באינטרנט.[174]

השלישי, מודל מניעתי מלא משמעו מעקב תדיר אחר הרגלי גלישה, בבחינת פן־אופטיקון אינטרנטי שיצנן את פעילות הגולשים במרחב הסייבר. אכיפה מניעתית יעילה מחייבת פגיעה מקיפה בכלל משתמשי המחשב והאינטרנט על מנת לסרוק, לנטר ולמנוע פעילות לא רצויה.[175] לעומת זאת במודל של חקירה פלילית לאחר ביצוע העבירה יש מיקוד טבעי של פעילות הרשות החוקרת בקבוצה מסוימת, רלוונטית בכוח, של חשודים. על כן מרבית משתמשי המחשב והאינטרנט יימצאו מחוץ לתמונה. להתמודדות עם בעיית הפגיעה הקולוסאלית, גם אם האוטומטית (ולא אנושית), בפרטיות משתמשי האינטרנט, הציע קוזלובסקי לפתח פרקטיקות של **אחריותיות** (accountability) בפעולת הרשות האוכפת, ובראשן חובות תיעוד אוטומטיות רציפות של פעולות הרשות האוכפת וכן חובות יידוע של משתמשי המחשב והאינטרנט בדבר פעולות שונות שביצעה הרשות האוכפת, הכנסת פרקטיקות אדוורסריות גם לשלבי הפעולה המקדמיים של הרשות החוקרת ועוד.[176] איני בטוח שרעיון זה של קוזלובסקי יכול לרפא את הבעייתיות החוקתית שבמודל מניעתי. אמנם פיתוח האחריותיות בפעולת הרשות החוקרת הוא רעיון מבורך,[177] אולם רעיון האחריותיות מתאים לטעמי להקל את הקשיים שבבקרה אפקטיבית על פעולת הרשות החוקרת. אין הוא מרפא את הקשיים שבשינוי מודל האכיפה ממודל ex ante של חקירה בדיעבד למודל מניעתי, כפי שמציע קוזלובסקי. העובדה שמשתמשי המחשב והאינטרנט ידעו בדיעבד מתי נעקבו, וכן יוכלו לבקר את הרשות האוכפת על סמך תיעוד מלא של פעולתה, אינה יכולה לנטרל את האפקט המצנן הנגרם בעקבות המודל המניעתי.

---

174 התנגדות זו למניעה מוקדמת מקובלת במשפט הפלילי, בעיקר בקשר לעברות ביטוי, אף בלא קשר לזירה האינטרנטית. ראו למשל בג"ץ 399/85 **כהנא נ' הועד המנהל של רשות השידור**, פ"ד מא(3) 255 (1987) (בהקשר של הסתה לגזענות); ע"א 214/89 **אבנרי נ' שפירא**, פ"ד מג(3) 840 (1989) (בהקשר של לשון הרע); בג"ץ 4804/94 **חברת סטיישן פילם בע"מ נ' המועצה לביקורת סרטים ומחזות**, פ"ד נ(5) 661 (1997) (בהקשר של פרסומי תועבה); ע"א 409/13 **שידורי קשת בע"מ נ' קופר**, בפס' 16 לפסק דינו של הנשיא גרוניס (פורסם בנבו, 11.4.2013) (בהקשר של סוב יודיצה); רע"א 4783/13 **כהן נ' יצחק** (פורסם בנבו, 7.7.2013); אריאל בנדור "עבירה פלילית ומניעה מוקדמת" **פלילים** ג 240 (1993); אהרן ברק "המסורת של חופש הביטוי בישראל ובעיותיה" **משפטים** כז 723, 732 (1996).

175 את הפן־אופטיקון האינטרנטי, לפי המודל של קוזלובסקי, ייצרו ספקיות השירות האינטרנטיות, להבדיל מהמדינה. אמנם באופן מסורתי קיים איום מתמיד על הזכות לפרטיות מצד המדינה, אך יש הכרה גם באיום הנשקף מצד תאגידים חזקים באינטרנט. ראו בירנהק, לעיל ה"ש 44, בעמ' 149, 167.

176 ראו Kozlovski, לעיל ה"ש 13, בעמ' 352—429. כן ראו Nimrod Kozlovski, *Designing Accountable Online Policing*, *in* Cybercrime – Digital Cops and Laws in a Networked Environment 107, לעיל ה"ש 149. עוד על הכנסת פרקטיקות אדוורסריות להליכים ex parte בשלב הוצאת הצווים המסמיכים את הרשות החוקרת לאסוף ראיות דיגיטליות, ראו שרון גולדנברג־אהרוני "חדירה למערכות מחשב – היקפה הרצוי והמצוי של העברה" **ספר דיוויד וינר** 429, 450 (2009).

177 חלק מרעיונות אלה באו לידי ביטוי בהצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד–2014, ה"ח הממשלה 867. לענייננו, ראו בעיקר את סעיף 96, המפרט את האופן שבו ייערך דוח החדירה לחומר מחשב. כן ראו סעיף 84(ב)(7) להצעת החוק, המחייב את הרשות החוקרת, בעת הגשת בקשה למתן צו חדירה, לפרט בפני השופט את יכולת התיעוד של פעולת החדירה.

nevo.co.il

לאחריותיות בוודאי יכולה להיות השפעה מיטיבה על התנהלות הרשות האוכפת,[178] אולם לא כך הוא, לטעמי, כשמדובר בהשפעה על התנהלותם של משתמשי המחשב והאינטרנט.

8. סיכום ביניים

הצגתי לעיל כמה חלופות לאכיפה הפלילית הקלאסית, המבוססת על חקירה, על פי רוב בדיעבד, של עברה פלילית, כאשר מטרת החקירה היא לאסוף ראיות קבילות לצורך העמדה לדין, הרשעה וענישה. שללתי את כל אלה כחלופות מלאות לאכיפה הפלילית, בהיותן חלקיות מעצם טבען ובהיות חלק מהן פוגעניות מן השיטה הפלילית בזכויות מוגנות. גם מודל משולב של כמה מהפתרונות החלופיים הללו אין בו כדי להציב חלופה ממשית, ישימה משפטית וטכנולוגית, לאכיפה הפלילית.

ה. הצעות לאכיפה לא־מדינתית במרחב הסייבר

עד כה בחנתי חלופות לשיטת האכיפה הפלילית הנוהגת. מצאתי כי השיטה הנוהגת לא נדחתה מפני שיטת אכיפה חלופית. עתה יש מקום לבחון אם זהות הגורם האוכף צריכה להידחות מפני זהות אחרת. אעבור אפוא לבחון חלופות למדינה כגורם האוכף במרחב המקוון.

1. העברת חובות החקירה מהמדינות לספקיות השירות

א) הצגת החלופה

הצורך המעשי להטיל את חובת האכיפה הפלילית על ספקיות השירות נובע מן העובדה שהן אוצרות בקרבן מידע יקר ערך לצורכי חקירה. אותן ספקיות שירות הן מוקדי הכוח המרכזיים במרחב המקוון. כך, התקשורת האינטרנטית היא לעולם מתווכת מבחינה ארכיטקטונית. "גלישה" באינטרנט מחייבת הקצאת תשתית גלישה מספקית שירותי התשתית (תשתית כבלים, ADSL, רשת לוויינית או סלולרית) והקצאת כתובת IP לצורך הזדהות והתקשרות בין מחשבים ברשת על ידי ספקית שירותי הגישה (Internet Service Provider – ISP).[179] חיפוש מידע מחייב תיווך של מנוע חיפוש או פורטל נושאי. לאחר מכן, ברמת התוכן עצמו, מתחייבת התחברות עם אתר מסוים המספק את התוכן בעצמו (כדוגמת אתרי החדשות) או את הפלטפורמה לצפייה בתכנים, לשיתוף בתכנים (כדוגמת הרשתות החברתיות, הפורומים) או לשיחה (באמצעות תוכנות להעברת מסרים מידיים, Instant Messaging – IM). לכל הספקיות הללו יש נקודות שליטה על מידע תוכני ועל מידע על אודות התוכן (metadata) המאפשר זיהוי של מקור המידע והנמען שלו, זיהוי מועד מסירת המידע ועוד.

---

178 ראו בעניין זה את Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J. L & TECH. 257, 280–290 (2002). עציוני כתב גם הוא על מנגנון האחריותיות כמנגנון לאיזון פעולתה של הרשות החוקרת באינטרנט. לטענתו, קיימות טכנולוגיות מעודדות חירות מחד גיסא וטכנולוגיות הפוגעות בחירות מאידך גיסא. האחריותיות היא מנגנון לאיזון הטכנולוגיות מן הסוג השני.

179 ראו עוד בנספח א (רקע על ארכיטקטורת האינטרנט).

nevo.co.il

הטלת חובות אכיפתיות על ספקי שירות כבר נדונה בפרק זה בשלושה הקשרים: במסגרת הסוגיה של חסימת גישה לאתרים פוגעניים, שהיא ביטוי למנגנון של אכיפה מגוננתית־כופה; במסגרת אכיפה מגוננתית־וולונטרית שמפעילה ספקית השירות מיזמתה שלה; בהקשר של המודל המניעתי המשולב שהציע קוזלובסקי. בשלושת ההקשרים האלה דנתי בשיטת האכיפה, ועתה אני מבקש להתייחס לנושא בהקשר של זהות הגורם האוכף בפועל.

כאשר עניינו בזהות הגורם האוכף, יש להבחין תחילה בין זהות האוכף בפועל לבין זהות מחולל האכיפה. אבהיר את כוונתי: כשמדובר באכיפה מגוננתית־וולונטרית בידי ספק שירותי תוכן באינטרנט, המחליט מיזמתו לסנן תכנים הכוללים גסויות, ניתן לומר שספק השירות הוא האוכף בפועל וגם מחולל או יוזם האכיפה. לעומת זאת כאשר על פי חוק ספקיות השירות מחויבות לסנן תכנים מסוימים, הרי שהאוכפת בפועל היא ספקית השירות, אבל מחוללת האכיפה היא המדינה, אשר חוקקה את החוק המטיל אחריות כאמור על הספקית.

ברי כי למדינה יהיה קל לגלגל את חובות האכיפה בפועל אל ספקיות השירות יותר משיקל עליה לאכוף ישירות את החוק על ציבור משתמשי המחשב העצום. ספקיות השירות הן מעטות יותר ויציבות יותר מקהל משתמשי המחשב והאינטרנט, האנונימי והמפוזר בכל העולם.[180] בירנהק ואלקין־קורן הראו כי המדינה הבינה את הפוטנציאל הגלום בספקיות השירות הפרטיות לביצוע האכיפה בשבילה, ובהטלת חובות על הספקיות המדינה חוזרת לזירה המקוונת תוך עקיפת מגבלות משפטיות, דיפלומטיות וטכנולוגיות שהיא נתונה בהן.[181]

ארחיב עתה על האופן שבו המדינה יכולה להניע ביזמתה את ספקיות השירות לבצע בפועל את האכיפה. הטלת חובות אכיפה על ספקיות השירות, נוכח המעמד המיוחד שלהן בזירה המקוונת, יכולה להיעשות בשלוש דרכים עיקריות: **האחת**, הטלת חובות ישירות לביצוע פעולות בשביל הרשות החוקרת; **השנייה**, הטלת אחריות נזיקית או פלילית על ספקיות השירות השונות באופן שיתמרץ אותן לשמור על הסדר ב"טריטוריה" שלהן במידה שתאפשר להן לצאת מגדר האחריות שהטילה עליהן המדינה. דרך זו של הטלת אחריות משפטית לפעולות המבוצעת ב"שטח" של ספקית השירות מביאה בדרך עקיפה את ספקית השירות לסייע למדינה באכיפת הדין הפלילי בזירה המקוונת; **השלישית**, הפעלת לחץ כלכלי על ספקית השירות לבצע ביזמתה את ההסדרה שמבקשת המדינה.

אביא להלן שלוש דוגמאות להטלת חובות ישירות על ספקיות השירות בקשר עם איסוף ראיות בחקירה פלילית:

1) הטלת חובות שימור מידע דרך קבע (Retention). הכוונה לחיוב ספקיות שירות, בחקיקה או במשטר של רישיונות של המדינה, לשמר מידע שנאגר ברשותן במסגרת פעולתן,

---

180 ראו Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries and the Problem of the Weakest Link*, U. PA. L. REV. 11 (2006); Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 410–413 (1999).

181 ראו Birnhack & Elkin-Koren, לעיל ה"ש 2. בירנהק ואלקין־קורן טענו כי האינטרס של המדינה הוא להותיר את ספקיות השירות במעמדן המיוחד באינטרנט, על מנת שתוכלנה להמשיך להחצין את חובות האכיפה עליהן. כן ראו גם GOLDSMITH & WU, לעיל ה"ש 1, בעמ' 68–84; Reidenberg, לעיל ה"ש 149, בעמ' 222—225. ריידנברג, גולדסמית' ו־וו טענו כי באמצעות העברת חובות לספקיות השירות הפועלות בתוך שטחי המדינה, מתאפשר למדינה לאכוף את הדין באינטרנט, כולל אכיפה בעלת השפעות אקסטרה־טריטוריאליות, מבלי לפעול בעצמה ב"מקומות" באינטרנט שהם מחוץ לטריטוריה שלה.

nevo.co.il

לפרקי זמן שונים על פי דרישת המדינה. שימור המידע יכול להתייחס לנתוני תוכן או לנתונים על אודות התוכן (נתוני metadata כגון פרטי בעלות של לקוחותיהם, מועדי ההתקשרות של הלקוחות עם ספקית השירות, משך ההתקשרות, נפח זיכרון של המידע שהלקוח קיבל או העביר, כתובות IP שמהן התחבר הלקוח אל ספקית השירות וכיוצא בזה). משטר Retention מקובל במדינות האיחוד האירופי, הגם שלאחרונה נפסלה הדירקטיבה של האיחוד האירופי בנושא.[182] בישראל, ככלל, אין משטר שימור מידע דרך קבע וכך גם בארצות הברית.

2) הטלת חובה ליצירת תשתית טכנולוגית לשימוש עתידי בידי הרשות החוקרת במקרה קונקרטי. בארצות הברית מוכר חוק ה־CALEA (Communications Assistance for Law Enforcement Act) משנת 1994, המחייב ספקיות תקשורת לבנות תשתית טכנולוגית בצורה שתאפשר ביצוע האזנות סתר על ידי רשויות החקירה.[183] חקיקה זו מחייבת ספקיות שירות שונות להתקין תוכנות ורכיבי חומרה כנדרש על פי החוק, שאותם יהיה עליהן לרכוש מצדדים שלישיים המוגדרים אמינים לדידה של המדינה.[184] גם בבריטניה יש הוראות חוק המתייחסות לסוגיית החיוב של ספקיות תקשורת לבנות תשתית טכנולוגית שתאפשר האזנת סתר על ידי רשויות החקירה.[185] בשונה מבארצות הברית, החקיקה חלה במפורש גם על ספקיות גישה לאינטרנט, הכלולות בהגדרה של "מערכות טלקומוניקציה" שעליהן מוחל החוק. החוק קובע מנגנון שלפיו דרישה לבנות תשתית טכנולוגית מסוימת תעבור תחילה אישור פרלמנטרי. בחקיקה הישראלית אין חובה כללית ליצירת תשתית טכנולוגית לשימוש רשויות החקירה. הוראת סעיף 13(ב)(2) לחוק התקשורת (בזק ושידורים), התשמ"ב–1982 מסמיכה את ראש הממשלה לדרוש מכל בעלי רישיון בזק, ומהן בלבד, לבצע "התאמה טכנולוגית למתקן בזק", ככל שהדבר דרוש לצורך הפעלת סמכויותיהם של "כוחות הביטחון", כאשר "כוחות הביטחון" כוללים את משטרת ישראל, לפי סעיף 13(א) לחוק. השירותים הנדרשים לכוחות הביטחון מוגדרים בנספח סודי לרישיון הבזק.[186] צורה אגרסיבית יותר של דרישה ליצירת תשתית

---

182 מדינות האיחוד האירופי קבעו הוראות שימור מידע לפרקי זמן שבין 6 ל־24 חודשים של נתוני תקשורת באינטרנט ובתחום הטלפוניה, על בסיס דירקטיבת האיחוד האירופי משנת 2006, לעיל ה"ש 53. כאמור שם, לאחרונה נפסלה הדירקטיבה בפסיקת בית הדין הגבוה לצדק של האיחוד האירופי, אלא שחוקי ה־retention הפנימיים של המדינות באיחוד נותרו בעינם.

183 חוק זה מופיע כ־47 U.S.C. § 1001–1010.

184 בשנים האחרונות נבחנת בארצות הברית האפשרות להרחיב את דרישות ה־CALEA גם אל שיחות ב־VoIP, ראו Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L. 409 (2009).

185 ראו Regulation of Investigatory Powers Act, 2001, c. 23 § 12 (Eng.).

186 בעניין הנספחים הסודיים לרישיונות הבזק הוגשה לבית המשפט המחוזי בירושלים עתירה של התנועה לחופש המידע. במסגרת העתירה נתבקש משרד התקשורת לחשוף את תוכנם של הנספחים הסודיים. במהלך הדיון בעתירה נחשף כי הנספחים הסודיים מחייבים כי עובדים מסוימים בחברות הטלפוניה יהיו בעלי סיווג ביטחוני גבוה, וכן עלה כי לשב"כ יש גישה ישירה למחשבי חברות הטלפוניה. לאחר חשיפת נתונים אלה, ובהמלצת בית המשפט, העתירה נמחקה. ראו עת"מ 890/07 **התנועה לחופש המידע נ' משרד התקשורת** (לא פורסם, 5.11.2007).
לצד האמור, ברישיונות הבזק המוצאים מכוח חוק התקשורת ניתן למצוא חובות מסוימות המוטלות לטובת "כוחות הביטחון". כך הוא באשר להספקת שירותי טלפון קווי וסלולרי. ראו למשל רישיון כללי לפרטנר תקשורת בע"מ למתן שירותי רדיו טלפון נייד בשיטה התאית (רט"ן) (נוסח משולב מיום 13.5.2013), סעיפים 1, 66א–66ב, המצוי ב: http://www.moc.gov.il/sip_storage/FILES/6/626.pdf;

nevo.co.il

לשימוש הרשויות מצויה בדמות תקנות בסין משנת 2011, המחייבות ברים, מסעדות, מלונות וחנויות ספרים להתקין תוכנות יקרות (בעלות של כ־3,100 דולר) שיאפשרו לפקידי הממשל גישה למידע על זהות המשתמשים המתחברים לרשתות ואפשרות לנטר את פעילותם ברשת.[187]

3) חובות שמירת מידע במקרה נתון מכאן ולהבא (Preservation). חובת ה־Preservation, בשונה מחובת ה־Retention, מתייחסת למקרה מסוים אגב חקירת חשד מסוים. עניינה של חובה זו בשמירת מידע ללא עיון בו וללא מסירתו (בינתיים) לגורם כלשהו, אלא רק הקפאת מצבו, על מנת שלא יתנדף או ישתנה, כמקובל בנוגע למידע דיגיטלי באינטרנט.[188]

בכל הנוגע להטלת אחריות פלילית או נזיקית על ספקיות השירות שנועדה לתמרץ אותן לבצע אכיפה בתחום השליטה שלהן על מנת לצאת מגדר האחריות הרובצת לפתחם, אציין שני ניסיונות מעניינים מישראל בעשור האחרון ולאחריהם כמה דוגמאות מארצות הברית:

1) החקירה הפלילית נגד מנועי חיפוש ופורטלים שהציגו קישוריות לאתרי הימורים באינטרנט בחשד לביצוע עבירות של פרסום "הודעה על הגרלה או על הימור", כקבוע בסעיף 227 לחוק העונשין. משטרת ישראל עיכבה לחקירה כמה מנהלי אתרי אינטרנט שונים, ובהם הפורטל "וואלה", אתר הספורט One, הרשת החברתית "חבר'ה" ועוד,[189] על שאפשרו הצגת קישוריות ופרסומות לאתרי אינטרנט המציעים הימורים אסורים על פי הדין הישראלי. בחלק מהמקרים תוצאת החקירה האפקטיבית הייתה הסרה של אותן קישוריות ופרסומות המגלמות עבירה פלילית לכאורה של פרסום הודעה על הגרלה או על הימור. בגין חקירה זו לא הוגשו כתבי אישום נגד מי ממנהלי אתרי האינטרנט.

2) העלאתה של הצעת חוק מסחר אלקטרוני.[190] פרק ה להצעת החוק מנה תנאים שונים לפטור של ספקי שירות מאחריות בנזיקין או בתביעת קניין רוחני. מהוראות הפטור האמורות

רישיון כללי ל"בזק", החברה הישראלית לתקשורת בע"מ למתן שירותי בזק פנים־ארציים נייחים (נוסח משולב מיום 3.7.2012), סעיפים 1, 33—35 המצוי ב: http://www.moc.gov.il/sip_storage/FILES/2/622.pdf. בכל הנוגע לרישיונות משרד התקשורת לספקיות גישה לאינטרנט, לא מופיעה דרישה דומה להספקת תשתית טכנולוגית לשימוש "כוחות הביטחון". ראו דוגמה לרישיון מיוחד למתן שירותי אינטרנט ספק ראשי (27.5.2013), המצוי ב: http://www.moc.gov.il/sip_storage/FILES/1/651.pdf.

187 ראו Andrew Jacobs, *China Steps Up Web Monitoring, Driving Many Wi-Fi Users Away*, N.Y. TIMES (25.7.2011) http://www.nytimes.com/2011/07/26/world/asia/26china.html?_r=1.

188 התייחסות נוספת לשלוש החובות הללו, המוטלות על ספקיות השירות, ראו בפרק 4(ג)(3) להלן, בבואי לדון בסמכויות איסוף הנחסרות מהתפישה הפיזית החולשת על דיני איסוף הראיות באינטרנט.

189 ראו אפרת וייס וגל מור "המשטרה פשטה על אתרים המפרסמים הימורים" **Ynet** (19.12.2005) http://www.ynet.co.il/articles/0,7340,L-3186855,00.html; אפרת וייס "מנהלי אתר One נחקרו בחשד לפרסום הימורים" **Ynet** (10.7.2006) http://www.ynet.co.il/articles/0,7340,L-3273489,00.html; שלומי דיאז "עוכבו לחקירה מנהלי אתר חבר'ה" **מחלקה ראשונה** (10.8.2006) http://www.news1.co.il/archive/001-D-107813-00.html?tag=20-46-21. עוד על האפשרות להטיל אחריות על מנועי חיפוש המציגים קישוריות לאתרי הימורים באינטרנט, ראו חיים ויסמונסקי "הימורים באינטרנט — דין ישן וחדש" **רשימות בנתיב קנייני הרוח — השנתון למשפט, תקשורת וטכנולוגיה** 1, 291, 319 (2004).

190 הצעת החוק מבוססת על עבודת ועדת שפניץ, שמסרה את המלצותיה במאי 2004. ראו דין וחשבון הוועדה לבדיקת בעיות משפטיות הכרוכות במסחר אלקטרוני (דוח חלקי), התשס"ד—2004. הצעת החוק הוצגה לראשונה לכנסת ה־17 ועברה בקריאה ראשונה. ראו הצעת חוק מסחר אלקטרוני, התשס"ח—2008, ה"ח הממשלה 356. על הצעת החוק לא הוחל דין רציפות במעבר לכנסת ה־18, ועל

nevo.co.il

עולה כי הנחת המוצא היא כי חלה אחריות אזרחית על ספקי השירות השונים בגין תכנים פוגעים של צדדים שלישיים.[191] אמנם ההתייחסות בהצעת חוק מסחר אלקטרוני הייתה לאחריות ספקי השירות לעוולות ולהפרות של קניין רוחני המבוצעות בידי משתמשי האינטרנט הנעזרים בשירותיהם, אולם איני רואה טעם ממשי להבחין בין אחריות זו לבין אחריות לעברות פליליות של ממש בתחום לשון הרע, פגיעה בפרטיות ועברות על דיני הקניין הרוחני שיבוצעו בידי המשתמשים.[192] מנגנון הטלת האחריות על ספקי השירות בהצעת חוק מסחר אלקטרוני הוא מנגנון מדורג, שלפיו ספקי גישה לאינטרנט נהנים מחסינות מוגברת, ספקי אחסון זמני נהנים מחסינות מצומצמת יותר, ואילו ספקי שירותי אירוח (hosting) וחיפוש באינטרנט נהנים מחסינות מצומצמת עוד יותר.[193] מכאן שעל פי הצעת החוק, ספקי שירותי האירוח והחיפוש הם המתומרצים ביותר לבצע אכיפה בעצמם: הם יופטרו מאחריות רק אם לא ידעו, במועד העלאת המידע לאינטרנט, שתוכן המידע או הפצתו מהווים עוולה או הפרת קניין רוחני, אם מפיץ המידע לא פעל מטעמו או בשליטתו של הספק, ואם פעל על פי מנגנון של ״הודעה והסרה״. מנגנון זה קובע את שיטת האכיפה שלפיה על ספק שירותי האירוח או החיפוש לפעול במקרה של קבלת תלונה על מידע מסוים שהפיץ.[194] מנגנון זה, של ״הודעה והסרה״, אומץ בפסיקה הישראלית כשיטת פעולה הרצויה לספקי שירותי אירוח באינטרנט,[195] הגם שהצעת החוק לא עברה עד כה בכנסת.

3) הזכרתי לעיל[196] בפרק זה את הדוגמאות לחקיקה פדרלית בארצות הברית המחייבת בסינון תכנים מיניים העלולים לפגוע בקטינים ובחסימת גישה אליהם: ה־COPA (Child Online Protection Act) מ־1998 וה־CIPA (Children's Internet Protection Act) מ־2000. ה־COPA חל על כל ספקי התוכן המסחריים באינטרנט, ונקבעו בו הוראות המטילות אחריות פלילית ונזיקית

כן היא הוסרה מסדר היום. ב־25.7.2011 הניח ח״כ מאיר שטרית את הצעת החוק שוב על שולחן הכנסת. ראו הצעת חוק מסחר אלקטרוני, התשע״א–2011, ה״ח פ/3418/18 (ח״כ מאיר שטרית).

191 ראו דוח ועדת שפניץ, לעיל, בעמ׳ 56–66.

192 המשותף לתחומים אלה שאותו יסוד התנהגותי יכול להקים הן אחריות אזרחית והן אחריות פלילית.

193 ראו סעיף 7 להצעת חוק מסחר אלקטרוני המבחינה בין ספק שירות גישה (Mere Conduit), לספק שירות אחסון זמני (Caching) ולספק שירות אירוח (Hosting). בהגדרת ספק שירותי אירוח הוכללו גם מנועי החיפוש. אל מול מודל החסינות של הצעת חוק מסחר אלקטרוני ראו את פסק דינו של בית המשפט העליון של קנדה, שם נקבע כי ככלל אתר אינטרנט (לאו דווקא מנוע חיפוש) הכולל קישוריות לאתרי אינטרנט אחרים שתוכנם הוא בבחינת לשון הרע, פטור מאחריות בעצמו בגין לשון הרע, אלא אם הקישורית כללה תוכן שהוא כשלעצמו לשון הרע: Crookes v. Newton, [2011] SCC 47 (Ca.).

194 ראו סעיף 10(א)(3) להצעת חוק מסחר אלקטרוני. מנגנון ״הודעה והסרה״ קובע את האופן שבו על ספק שירותי האירוח (לרבות החיפוש) לפעול במקרה של קבלת תלונה כי תוכן המידע ה״מתארח״ אצלו או הפצתו עולים כדי עוולה נזיקית או הפרת זכות קניין רוחני. הכלל הוא שעל ספק השירות לפנות מיד אל מחזיק / מפיץ המידע הפוגע ולהודיעו כי בכוונתו להסיר בתוך שלושה ימי עסקים את המידע הפוגע או לחסום את הגישה אליו. אם לא יחלוק מחזיק/מפיץ המידע הפוגע על תוכן ההודעה, יסיר ספק השירות את המידע או יחסום כאמור את הגישה אליו. המנגנון כולל התייחסות למצבים נוספים, שבהם המחזיק / מפיץ המידע לא מאותר או שהמחזיק/המפיץ מציין כי בכוונתו לחלוק על המתלונן ולהתדיין עמו בבית המשפט.

195 ראו ת״א (מחוזי מר׳) 567-08-09 **א.ל.י.ס. אגודה להגנת יצירות סינמטוגרפיות (1993) בע״מ נ׳ רוטר.נט בע״מ** (פורסם בנבו, 8.8.2011).

196 ראו לעיל ה״ש 127–128.

nevo.co.il

על ספקי שירות שהפרו את הוראותיו, ואילו ה־CIPA חל על ספריות ציבוריות ועל מוסדות לימוד בכובעם כספקי שירותי גישה לאינטרנט, ונקבעה בו התניה כספית של היעדר מימון למי שלא יתקינו תוכנות סינון וחסימת גישה. מעניין לציין כי החוק הראשון שנועד להתייחס לחסימת תכנים מיניים פוגעניים, ה־CDA (Communications Decency Act) מ־1996, דווקא קבע בסעיף 230 שלו הוראת פטור לספקי שירות מאחריות על פרסום תכנים מיניים במסגרת השירות שלהם. כן נקבעה הוראת פטור הפוכה באותו החוק לספקי השירות על כך שאם בחרו לסנן תכנים מסוימים לא ייתבעו כמי שגרמו נזק למי שביקש לפרסם אותם תכנים או למי שביקש לגלוש לאותם תכנים.

בכל הנוגע **להפעלת לחצים כלכליים** על ספקיות השירות לאכוף את הדין המדינתי, כאן מדובר למעשה בשיטה שאינה כוללת הטלת אחריות משפטית, כבשתי השיטות הקודמות, אלא באיום של מדינה במישור המסחרי לפגוע כלכלית בספקית שירות שלא תיאות להתאים עצמה לדרישות החוק של אותה מדינה. הדוגמה המובהקת ביותר לשיטה של הטלת חובות על ספקיות השירות על דרך של הפעלת לחצים כלכליים מצויה בניסיונותיה של סין לצנזר את תוכני האינטרנט. סין דרשה מגוגל להסיר תכנים מסוימים ממנוע החיפוש שלה, כמו גם מדפי החדשות שלה (Google News). בתחילה סירבה גוגל להיעתר לדרישות אלה, ובתחילת שנת 2002 חסמה ממשלת סין, באמצעות ספקיות הגישה לאינטרנט במדינה, את הגישה לגוגל. כעבור כשנתיים החלה גוגל לספק אתר חדשות לקהל הסיני תוך סינון תכנים אסורים לשיטת הממשל הסיני. כעבור כשנתיים נוספות נערך מנוע חיפוש ייעודי לשוק הסיני (Google.cn) ובו סינון תוצאות מסיבי – כל זאת בשל חששה של גוגל מהינתקות השוק הסיני ממנה.[197] בדצמבר 2010 בוצעה מתקפת האקרים משולבת על גוגל, כמו גם על יותר מעשרים חברות אינטרנט אמריקניות נוספות. גוגל גילתה כי חשבונות Gmail של כמה פעילי זכויות אדם סיניים נפרצו במהלך המתקפה, זאת לצד פריצה לתשתיות מרכזיות של תפעול החברה. בתגובה הכריזה גוגל כי תפסיק את סינון התכנים ב־Google.cn, ובשלב מסוים העתיקה את שרתיה להונג קונג עם הוראת redirection מ־Google.cn ל־Google.com.hk.[198] גוגל אינה היחידה שהייתה נתונה ללחצים כלכליים מצד

---

197 להשתלשלות העניינים, ראו Ted Bridis, *Google Compromised its Principles in China, Founder Says*, USA Today (6.6.2006) http://www.usatoday.com/tech/news/2006-06-06-google-china_x.htm; Clive Thompson, *Google's China Problem (and China's Google Problem)*, N.Y. Times (23.4.2006) http://www.nytimes.com/2006/04/23/magazine/23google.html?pagewanted=1&ei=5090&en=972002761056363f&ex=1303444800. מהלכה זה של גוגל בוקר כשיתוף פעולה של תאגיד אמריקני עם העריצות הסינית. ראו, למשל, Human Rights Watch, *"Race to the Bottom": Corporate Complicity in Chinese Internet Censorship* (10.8.2006), *available at* http://www.hrw.org/reports/2006/china0806/index.htm.

198 ראו David Drummond, *A New Approach to China*, The Official Google Blog (12.1.2010) http://googleblog.blogspot.com/2010/01/new-approach-to-china.html; David Drummond, *A New Approach to China: An Update*, The Official Google Blog (22.3.2010) http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

nevo.co.il

סין. גם יאהו! האמריקנית הסכימה להציג תוכני חיפוש מסוננים באתר הסיני שלה,[199] וכמותה גם סקייפ[200] ואחרים.

ב) הערכת החלופה

ספקיות השירות מניעות את הרשת. הן חולשות על תעבורת המידע ועל אגירתו. הן פועלות במרחב הסייבר באופן שאינו מגביל אותן לטריטוריה או לסמכות (Jurisdiction) של מדינה אחת בלבד. מכאן שהן בעלות פוטנציאל לשמש אוכפות החוק במרחב הסייבר תוך התגברות לכאורה על בעיית הבין־לאומיות של הרשת.[201]

לצורך הערכת החלופה של אכיפה בידי ספקי השירות אציע שלוש נקודות מבט שונות המשלימות זו את זו: **האחת**, נקודת מבט ברזולוציה של **זהות כללית של הגורם האוכף בפועל**: האם זו המדינה או ספקית השירות? **השנייה**, נקודת מבט ברזולוציה קרובה יותר של **סוג ספקית השירות** שבה מדובר; **השלישית**, נקודת מבט ברזולוציה פרטנית של **סוג החובה המוטלת על ספקית השירות**:

1) בכל הנוגע לשאלה הכללית בדבר זהות הגורם האוכף בפועל – המדינה או ספקית השירות – ניתן לטעון שהעברת הנטל מהמדינות לספקיות השירות השונות יכולה להביא לתופעה של החצנה שלילית של העלויות מהמדינה לאותם גורמים פרטיים. נטל השמירה והאיסוף של הראיות יועבר לספקיות השירות, חובת האיתור של מבצעי העברות תוטל עליהן וחובת הניתוק של משתמש מחשב מפר או חסימת גישה לאתר מפר תוטל עליהן (אם זו שיטת האכיפה שתיושם).[202] בראייה כלכלית, ספקיות השירות – לפחות אלה שגובות תשלום על שירותיהן (כגון ספקיות גישה לאינטרנט או ספקיות תשתית) – יכולות לגלגל את עלויות האכיפה אל לקוחותיהן. לחלופין, המדינה תוכל ליצור מנגנון של החזר הוצאות בגין איסוף

---

199 ראו למשל Mark Maginer & Joseph Menn, *As China Censors the Internet, Money Talks*, L. A. TIMES (17.6.2005) http://articles.latimes.com/2005/jun/17/world/fg-censor17.

200 ראו למשל John Leyden, *Skype Uses Peer Pressure Defense to Explain China Text Censorship*, THE REGISTER (20.4.2006) http://www.theregister.co.uk/2006/04/20/skype_china_censorship_row.

201 אכן, חוקרים רבים צידדו בהסדרת המרחב המקוון, לרבות אכיפת הדין הפלילי בה, באמצעות ספקיות השירות. ראו Jonathan L. Zittrain, *Internet Points of Control*, 44 B.C. L. R. 653 (2003); Reidenberg, לעיל ה"ש 149. כן ראו סקירה אצל הרדוף, לעיל ה"ש 74, בפרק השלישי. ראו גם ניבה אלקין־קורן "המתווכים החדשים ב'כיכר השוק' הוירטואלית" **משפט וממשל** ו 365 (2003). לניתוח כלכלי המצדד בהעברת חובות האכיפה לספקיות השירות מן הטעם שהם מונעי הנזק הזולים ביותר, ראו למשל Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003); Douglas Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006); Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WILLIAM & MARY L. REV. 239 (2005).

202 לביקורת על החצנת הנטל מהמדינה לספקיות שירותי אינטרנט לאסוף ולהמציא חומר מחשב של לקוחותיהם למשטרה במסגרת צו להמצאת מסמכים, ראו ב"ש (מחוזי ת"א) 90868/00 **חב' נטוויז'ן נ' צבא ההגנה לישראל**, בפס' 9 (פורסם בנבו, 22.6.2000); ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף**, בפס' 8(ב) (פורסם בנבו, 5.2.2007). לביקורת כללית, לאו דווקא בהקשר האינטרנטי, על החצנת האכיפה הפלילית באמצעות שימוש בצווים לפי סעיף 43 לפסד"פ (צווי המצאה/הצגת חפץ), ראו ע"פ 1761/04 **שרון נ' מדינת ישראל**, פ"ד נח(4) 9, 23–24 (2004).

nevo.co.il

הראיות בידי ספקי השירות בשביל המדינה,[203] ובכך לצמצם את נטל גלגול האחריות אל ספקיות השירות.

גם אם יתאפשר להתגבר על אלמנט ההחצנה, עדיין תיוותרנה שאלות חוקתיות קשות בדבר האפשרות לכפות על גופים פרטיים לבצע פעולות שנתייחדו למדינה: האם אין בהעברה רחבת היקף של החובות מהמדינה לספקיות השירות משום התפשטות של המדינה מאחת הסמכויות המגדירות אותה כמדינה? האם אין בכך משום פגיעה בעיקרון חוקתי המחייב את המדינה להיות זו שתפעיל אכיפה פלילית?[204] האם אין בהטלת חובות על ספקיות השירות לאסוף מידע או לבצע אכיפה בפועל משום התערבות פסולה בחופש העיסוק שלהן? האם אין בכך כדי לפגוע ביחסי האמון בין משתמשי המחשב לבין ספקיות השירות? האם לא יהיה בכך כדי להביא לאפקט מצנן על המשך פעילותן של ספקיות השירות, או שלחלופין הן תחלטנה לצנן יתר על המידה את פעילות משתמשי המחשב והאינטרנט הנסמכים על שירותיהן?

---

203 חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת) קובע בסעיף 10 הוראה של החזר הוצאות לבעלי רישיון הבזק בגין ביצוע פעולות הנדרשות מהן על פי חוק זה, בין במסגרת צו לנתוני תקשורת (מכוח סעיף 3), בין במסגרת היתר לקבלת נתוני תקשורת במקרים דחופים (מכוח סעיף 4) ובין במסגרת דרישה להעברת המאגר (מכוח סעיף 6). הוראת החזר ההוצאות אמנם מכוונת במישרין לשיפוי בעל רישיון הבזק, אולם היא עשויה להשיג תוצאה נוספת – ריסון הרשות החוקרת מלבצע פעולות איסוף ראיות מכוח חוק נתוני תקשורת. במילים אחרות, מתוך שלא לשמה בא לשמה, והזכויות החוקתיות של הנחקרים תזכינה בהגנה עקיפה. מעניין לציין כי הוראה מקבילה אינה קיימת בכל הנוגע לשיפוי גורמים אחרים הנמענים לצווי המצאת מסמכים מכוח סעיף 43 לפסד״פ, אפילו אם הם ״שחקנים חוזרים״ ואפילו אם הם גורמים פרטיים. הדוגמה המובהקת ביותר היא של בנקים, הנדרשים להמציא תדפיסי חשבון של לקוחותיהם. ראו בע״פ (מחוזי חי׳) 496/96 **מדינת ישראל נ׳ בנק המזרחי המאוחד בע״מ** (פורסם בנבו, 27.3.1997) שם נדונה דרישתו של בנק לקבל החזר הוצאות עבור פעולותיו שנדרשו לצורך ביצוע צו המצאה לפי סעיף 43 לפסד״פ. בית המשפט המחוזי קבע כי הבנק אינו זכאי להחזר הוצאות, תוך שימת דגש על מעמדו של הבנק כגוף מעין־ציבורי שעובדיו חייבים בחובת נאמנות לציבור, ומכאן ההצדקה לחייבם בביצוע צו ההמצאה אפילו אם הוא כרוך בעלויות.

204 לביקורת חוקתית נגד סמכותה של המדינה להחצין את החקירה הפלילית בתחום ההגבלים העסקיים לחוקרים פרטיים, ראו למשל עניין **בורוביץ**, לעיל ה״ש 15, בעמ׳ 824–836. בין השאר נקבע שם כי ״בהענקת הסמכות לקיים חקירה פלילית גלום כוח, וממילא כרוכה סכנה, לפגיעה בפרטיות הנחקרים, בכבודם, בחירותם ובקניינם... מטעם זה מתחייב שככלל, יש לפרש סמכות... לחקור חשד לביצועה של עבירה, כמתייחסת למינויו של עובד ציבור הנתון למרותה ולפיקוחה של הרשות השלטונית... ומשום אופייה המיוחד של הפונקציה החקירתית, שהפעלתה כורכת חשש לפגיעה בזכויות יסוד של הפרט, מן הראוי להפקידה בידי עובדי ציבור״ (שם, בעמ׳ 833–834). עוד ראו בג״ץ 2605/05 **המרכז האקדמי למשפט ולעסקים (ע״ר), חטיבת זכויות האדם נ׳ שר האוצר**, פ״ד סג(2) 545 (2009). במקרה זה, שנודע כבג״ץ **הפרטת בתי־הסוהר**, פסל בית המשפט העליון תיקון לפקודת בתי־הסוהר שאפשר הקמת בתי סוהר פרטיים. חלקים ניכרים מפסק הדין יצאו מהבחינה הקונקרטית והשקיפו מלמעלה על שאלת התפרקותה של המדינה מסמכות הכליאה שלה. בית המשפט העליון עמד בהרחבה על חובותיה של המדינה לקבוע את הנורמות הפליליות ולאכפן. בית המשפט עמד על חשיבות אי־הפרטת האכיפה הפלילית בשל האיזון החוקתי המוטמע בפעולת הרשות המנהלית לעומת פעולתם של גופים פרטיים שמונעים ממטרות עסקיות. השופטת פרוקצ׳יה כרכה בפסק דינה במפורש את סמכות החקירה הפלילית עם סמכות הכליאה, כשתי סמכויות של אכיפת חוק פלילית, אשר לא ראוי לה למדינה להתפרק מהן. ראו שם, בעמ׳ 2453–2457. למעשה, האמור נכון במידה רבה באשר לכל סמכות של הרשות השלטונית, לאו דווקא באשר לרשויות אכיפת החוק. ראו בג״ץ 2303/90 **פיליפוביץ נ׳ רשם החברות**, פ״ד מו(1) 410, 420 (1992); עניין **איגוד האינטרנט הישראלי**, לעיל ה״ש 122, בעמ׳ 33–35; דפנה ברק־ארז **משפט מנהלי** 178–179 (2010).

nevo.co.il

2) בכל הנוגע לביקורת מנקודת המבט של סוג ספקית השירות שבה מדובר, נדרשת הבחנה בין סוגים שונים של ספקיות שירות. המונח ״ספקיות שירות״ רחב מאוד, ולמעשה כולל כמה קבוצות שונות של ״שחקנים״ המספקים שירותים באינטרנט, ובהן אלה: (1) ספקיות גישה לאינטרנט (הן ספקיות גישה ישירה והן ספקיות Wi-Fi המאפשרות ״גלישה״ משותפת דרך נתב (Router) פתוח); (2) ספקיות תשתית פיזית לחיבור אינטרנט; (3) שרתי Proxy המאפשרים גלישה באינטרנט דרכם, תוך רכישת קבוצת ההרשאות של שרת ה־Proxy;[205] (4) ספקיות שירותי אחסון מידע ואירוח אתרים; (5) מנועי חיפוש; (6) מנהלי אתרי האינטרנט עצמם, כאשר גם כאן המונח ״אתר אינטרנט״ מתפרק לשני סוגים אלה: (א) אתרי תוכן מסוג יחיד־אל־רבים (One-to-Many או web 1.0); (ב) ספקיות פלטפורמות להעלאת תכנים בידי אחרים (Many-to-Many או web 2.0). בין ספקיות הפלטפורמות להעלאת תכנים אפשר להמשיך ולהבחין בין ספקיות פלטפורמות לתקשורת מידית (Instant Messaging), לספקיות פלטפורמות לתקשורת מתווכת פרטית (E-mail) ולבין ספקיות פלטפורמות לתקשורת מתווכת ציבורית. גם התקשורת המתווכת הציבורית מתפרקת לתת־קבוצות: פלטפורמות הפתוחות לכולי עלמא (למשל אתרי חדשות שבהם ניתן לפרסם טוקבקים), פלטפורמות הפתוחות לקבוצה סגורה של משתמשים המנויים על השירות (דהיינו ספקית השירות מגדירה את הקבוצה, כפי שנעשה לדוגמה בקבוצות דיון שונות) ופלטפורמות הפתוחות לקבוצה סגורה של חבריו של משתמש האינטרנט (דהיינו משתמש האינטרנט מגדיר את הקבוצה, לדוגמה ברשת חברתית כ״פייסבוק״).[206]

השונות בין ספקיות השירות השונות היא בראש ובראשונה ברמה הטכנולוגית, הנובעת ממהות השירות שהן מעניקות, וכנגזר מזה – האופן שבו תוכנת השירות. כמו כן ספקיות השירות ממלאות פונקציות חברתיות שונות. הטלת חובות אכיפה עליהן צריכה להיבחן על בסיס שונות זו. במילים אחרות, גם אם נצדיק העברה של חובות האכיפה אל ספקיות שירות ברמה העקרונית, אין זאת אומרת שההצדקה תחול אוטומטית, ודאי לא באותה עצמה, על כל סוגי ספקיות השירות. מנגד, עצמת הטיעונים החוקתיים נגד אכיפה בידי ספקיות השירות גם היא תשתנה בין הספקיות השונות.

3) בכל הנוגע לביקורת מנקודת המבט של סוג החובה המוטלת על ספקית השירות, גם כאן יש להבחין בין החובות השונות מבחינת עצמת הפגיעה בזכויות המשתמשים מחד גיסא וכובד הנטל על ספקית השירות מאידך גיסא. בכל הנוגע לפגיעה בזכויות המשתמשים, ברי כי יש פעולות איסוף מידע שקטגורית ניתן לסווגן כפוגעניות יותר מפעולות אחרות. כך למשל

---

205 כך, למשל, שרתי אוניברסיטאות רבות מאפשרים לאנשי הסגל ולסטודנטים להתקשר אליהם מרחוק ולגלוש דרכם אל האינטרנט, כאשר שרתים אלה ישמשו כ־Proxy. הגלישה לאינטרנט דרך שרתי האוניברסיטה מאפשרת כניסה לאתרי אינטרנט מסוימים בחינם, במקום בתשלום, היות שלשרתים אלה הוענקו הרשאות גישה לאותם אתרים.

206 השוו לסעיף 7 להצעת חוק מסחר אלקטרוני, לעיל ה״ש 190, שם הוצע להבחין בין הקטגוריות של שירותי אירוח (כולל שירותי חיפוש), לשירותי אחסון זמני, לשירותי גישה. כעולה מהצעת חוק מסחר אלקטרוני, הסטנדרט המשפטי לספקיות שירותי חיפוש מאוחד עם הסטנדרט לספקיות שירותי אירוח, שכן מנסחי הצעת החוק הכלילו שירותי חיפוש בתוך ״שירותי אירוח״. חלוקה זהה, להוציא השמטה של החלופה השלישית של הגדרת ״שירותי אירוח״ (החלופה הכוללת מנועי חיפוש בגדר ספקי שירותי אירוח), הועתקה גם לתזכיר חוק חשיפת פרטי מידע של משתמש ברשת תקשורת אלקטרונית, התשע״א – 2011 (תזכיר העוסק בחשיפת טוקבקיסטים שפרסמו הודעות מכפישות ובחשיפת משתמשי אינטרנט שהפרו זכויות יוצרים).

nevo.co.il

נראה כי ניתן לקבוע שהטלת חובה כללית של שימור כל המידע העובר דרך ספקית השירות תיחשב לאקט פוגעני בזכויות המשתמשים יותר משתיחשב הטלת חובה לשמר מידע מכאן ולהבא במקרה נתון על פי דרישת הרשות החוקרת. בכל הנוגע להכבדת הנטל על ספקיות השירות, יש להבחין בין שלוש: (1) הטלת חובות איסוף של מידע הנאגר בכל מקרה ברשות הספקיות כחלק אינטגרלי מהשירות שהן מספקות; (2) הטלת חובות איסוף של מידע העובר ברשות ספקיות השירות אך מחייב אותן לייצר תיעוד של המידע האמור לצורך מילוי החובה שהטילה עליהן המדינה; (3) הטלת חובות איסוף של מידע שפוטנציאלית היה יכול להגיע לרשות ספקיות השירות, אולם המידע לא נדרש להן, ואך ורק בשל החובה שהטילה המדינה עליהן הן נאלצות לעצב את המערכת שלהן מחדש על מנת לאסוף את המידע כנדרש מהן. ברי כי הסיטואציה השלישית היא הקיצונית ביותר מבחינת הפגיעה בחופש העיסוק של ספקיות השירות ומבחינת הפגיעה הפוטנציאלית ביחסי האמון בין הספקיות לבין לקוחותיהן במסגרת השירות שלהן, ואילו הסיטואציה הראשונה היא המתונה ביותר.

לסיכום, בבואנו לבחון את המרת זהות הגורם האוכף מהמדינה לספקיות השירות יש להבחין בין שניים: **האחד**, מצב שבו ספקיות השירות יוזמות את ההסדרה בקרבן מיזמתן הפרטית; **השני**, מצב שבו המדינה כופה — בין במישרין ובין בעקיפין — על ספקיות השירות לבצע את מטלות האכיפה הפלילית במקומה. במצב הראשון מתעוררות השאלות והבעיות של הסדרה פרטית־וולונטרית שדנתי בהן לעיל. במצב השני מתעוררים קשיים במישור חוקתי כפול: מצד אחד סמכותה של המדינה להיפרד מחובתה, שהיא חלק מבסיס הלגיטימיות שלה בעיני תושביה, ולהפריטה; מצד שני, הגברת החשש לפגיעה לא מידתית בזכויות מוגנות בשל הפעלת גוף פרטי מוּנע־רווח לשמש בתפקיד ציבורי מוּנע־ערכים. עצמת החששות משתנה לפי סוג ספקית השירות וסוג החובה שמבקשים להטיל על הספקית. חרף האמור איני מציע לפסול את החלופה של העברת החובות לספקיות השירות כליל. בפועל אין למדינה ברירה אלא להחצין חלק מפעילות האכיפה שלה לספקיות השירות. זאת, בגלל ארכיטקטורת המרחב המקוון המבוססת על ביזוריות ותיווכיות בידי ספקיות השירות. עם זאת השימוש בספקיות השירות צריך להיכלל במסגרת החקירה הפלילית באחריות המדינה ולא להחליף אותה. המדינה צריכה לחולל חלק מפעולות האכיפה בידי ספקיות השירות ולהיוותר האחראית להן.

2. החלופה הבין־לאומית

א) הצגת החלופה

כיוון שמרחב הסייבר אינו כפופה לגבולות מדיניים, וה"גלישה" מאפשרת הגעה בלחיצת כפתור לשרתי מחשב ולתכנים שמקורם במדינות זרות, מתבקש הדיון בשאלת האכיפה הבין־לאומית. אכיפה פלילית בין־לאומית היא עניין מורכב, אשר במידה רבה תלוי בשיתוף פעולה בין מדינות. שיתוף הפעולה בין המדינות הוא על פי רוב אטי, מסורבל ופורמליסטי. נראה כי מנגנוני שיתוף הפעולה הבין־מדינתי המקובלים במרחב הפיזי עומדים בתוקף מלא גם במרחב

נבו nevo.co.il

המקוון. לפיכך האמנות הבין־לאומיות לעזרה משפטית,[207] שיתוף הפעולה במסגרת האינטרפול[208] וכמובן האמנות הקובעות איסורים פליליים בין־לאומיים[209] – כל אלה תקפים במרחב המקוון.[210]

בשל הסרבול של מנגנוני שיתוף הפעולה הקיימים באשר לאכיפה פלילית במרחב הפיזי, בשני העשורים האחרונים הצביעו חוקרים שונים על הצורך בכינון אמנות ומנגנונים בין־לאומיים לאכיפה פלילית במרחב המקוון. הטיעון המרכזי של חוקרים אלה מניח את כישלון האכיפה הפלילית המדינתית כמעין נקודת מוצא לדיון ומצביע על הזירה הבין־לאומית כזירה הטבעית והמתאימה ביותר להתמודדות עם הפשיעה המקוונת. ההצדקות לכינון מערכת אכיפה בין־לאומית במרחב המקוון נחלקות לשניים: האחת, תפישה שלפיה המרחב המקוון אינו שייך לשום מדינה. נובע מתפישה זו כי המרחב המקוון אנלוגי לים הפתוח או לחלל החיצון,

---

207 ראו לדוגמה את European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959). אמנה זו נחתמה ואושררה ב־49 מדינות, ובהן מדינת ישראל, שאישררה אותה בשנת 1967. כן ראו, כדוגמה להסכמי עזרה משפטית בי־לטרליים, את ההסכם בין ישראל לבין אוסטרליה: Treaty Between the Government of Australia and the Government of the State of Israel on Mutual Legal Assistance in Criminal Matters (1994); ההסכם בין ישראל לבין ארצות הברית: Treaty Between the Government of the United States of America and the Government of the State of Israel on Mutual Assistance in Criminal Matters (1998); ההסכם בין ישראל לבין הונג קונג: Agreement Between the Government of the Hong-Kong Special Administrative Region of the People's Republic of China and the Government of the State of Israel Concerning Mutual Legal Assistance in Criminal Matters (2005). יתרה מזאת, חוק עזרה משפטית בין מדינות, התשנ"ח–1988, מותאם להתמודדות עם חקירות בעברות מחשב. זאת כיוון שהגדרת "חפץ", הניתן לתפיסה ולבדיקה במסגרת עזרה משפטית, כוללת גם "חומר מחשב" כהגדרתו בחוק המחשבים, התשנ"ה–1995. כמו כן בהגדרת "האזנת סתר", הניתנת לביצוע במסגרת בקשה לעזרה משפטית, נכללת גם האזנה ל"תקשורת בין מחשבים", כמוגדר בסעיף 1 לחוק האזנת סתר, התשל"ט–1979. במילים אחרות, כל פעולות החקירה הניתנות לביצוע בנוגע למחשב או לחומר מחשב בישראל, ניתנות – על פני הדברים – לביצוע גם במסגרת בקשות לעזרה משפטית בין מדינות. ראו חיים ויסמונסקי "עזרה משפטית בין מדינות ועזרה עצמית בחקירת עבירות אינטרנט" (פורסם בנבו, פברואר 2008).

208 האינטרפול מאגד 188 מדינות כיום. הארגון נוסד בשנת 1923 ופועל על בסיס חוקה שנחתמה בשנת 1956. ראו Constitution of Interpol (Vienna, 1956). האינטרפול נמנע מעיסוק בעברות על רקע גזעי, פוליטי, צבאי או דתי, על מנת להפחית מחלוקות פוטנציאליות בין המדינות החברות בארגון. עיקר פעילות האינטרפול עניינה באיסוף מודיעין בנוגע לביצוע עברות של פשיעה מאורגנת, טרור, פשעי מלחמה, עברות על איכות הסביבה, עברות סמים, פיראטיות בים, הברחת נשקים, סחר בבני אדם, הלבנת הון, עברות צווארון לבן, פורנוגרפיית קטינים, עברות מחשב, עברות קניין רוחני ושחיתות. לשותפויות אזוריות בתחום השיטור הבין־מדינתי, ראו גם את ה־ Treaty on European Union (Maastricht, 1992), שבה כוננה ה־Europol בין מדינות הקהילה האירופית.

209 ראו, להמחשה בלבד, את אמנת פלרמו נגד פשע מאורגן בין־לאומי משנת 2000: United Nations Convention Against Organized Crime (2000). אמנה זו נחתמה בידי מדינת ישראל ואושררה בשנת 2006. כן ראו עוד Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (2000), שנחתם בידי מדינת ישראל ב־2001 ואושרר ב־2008; United Nations Convention Against Corruption (2005), שנחתמה בידי מדינת ישראל ב־2005 ואושררה ב־2009.

210 כפי שאראה בפרק ג להלן, התוקף של מנגנונים אלה מניח ומנציח את התפישה הטריטוריאלית באשר לזירת הסייבר.

nevo.co.il

המוסדרים במסגרת הסכמית בין־לאומית;[211] השנייה, המרחב המקוון שייך לכל המדינות, והפשיעה בו היא סוג מפותח ומשוכלל במיוחד של פשיעה חוצת־גבולות (transnational crime), בדומה להלבנת הון, עברות סמים, הברחת כלי נשק, טרור ועוד.[212]

ההצדקה הראשונה עשויה להוביל למסקנה כי האכיפה בזירה הקיברנטית צריכה להיות גלובלית, מנותקת מסמכותן של המדינות, בבחינת סמכות שיפוט ואכיפה נפרדות (אכיפה גלובלית חוץ־מדינתית). לעומת זאת ההצדקה השנייה מובילה למסקנה כי האכיפה בזירה הקיברנטית צריכה לינוק את סמכותה מן המדינות, בדרך של שיתוף פעולה בין־מדינתי, בין פורמלי מחייב (דיני אמנות) ובין על בסיס הסכמה אד הוק שלא על בסיס אמנה מחייבת.

בכל הנוגע לאכיפה על בסיס גלובלי חוץ־מדינתי, הכוונה לכך שמוסדות האכיפה הם עצמם בין־לאומיים ולא מדינתיים. ניתן למנות שתי דוגמאות למוסדות רגולטיביים בין־לאומיים שבפעולתם יש משום אכיפה (גם אם לא פלילית) בזירה הקיברנטית: ICANN (Internet Corporation for Assigned Names and Numbers)[213] וה־WTO (World Trade Organization).[214]

מבחינת הסדרת הפעילות באינטרנט, ICANN מנהלת פעילות חשובה אך מצומצמת בהיקפה, המתייחסת להסדרת נושא שמות המתחם (מניעת כפילויות, הקצאת סיומות נושאיות וכדומה) ולהתאמה בין שם המתחם לכתובת ה־IP של אתרי האינטרנט (מניעת מצב שבו הקלדת שם מתחם מסוים לא תוביל לכתובת המבוקשת). שיא פעילות ההסדרה של ICANN בא לידי ביטוי בכינון מנגנון בוררות (UDRP – Uniform Domain-Name Dispute-Resolution Policy) בנוגע לרישום שמות מתחם העלול לפגוע בזכויות מוגנות של צדדים שלישיים, כגון שמות מתחם הפוגעים בסימני מסחר מוגנים של צדדים שלישיים.[215] ICANN הוקמה ביזמת הממשל

---

211 ראו למשל HENRIK SPANG-HANSSEN, PUBLIC INTERNATIONAL COMPUTER NETWORK LAW ISSUES 9–11 (2006); Anna Maria Balsano, *An International Legal Instrument for Cybersapce? A Comparative Analysis With the Law of Outer Space*, 1 THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 127 (UNESCO Pub. 2000).

212 ראו למשל Henry H. Perritt, *Jurisdiction in Cyberspace: The Role of Intermediaries*, *in* BORDERS IN CYBERSPACE 164 (Brian Kahin & Charles Nesson eds., 1998). פריט הציע מודל אכיפה בין־מדינתית באינטרנט, שלפיו המדינות תתפקדנה כאוכפות בתיווך או בתיאום של גורם בין־לאומי. כן ראו דברי ההסבר (Explanatory report) לאמנת מועצת אירופה בדבר פשעי מחשב (Convention on Cybercrime): http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm; Sean Selin, *Governing Cyberspace: The Need for an International Solution*, 32 GONZ. L. REV. 365 (1996–1997); Ellen S. Podgor, *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. DAVIS L. REV. 267 (2002); Yoachim Vogel, *Towards a Global Convention against Cybercrime*, presentation at First World Conference of Penal Law (Guadalajara 2007), *available at* http://www.penal.org/IMG/Guadalajara-Vogel.pdf.

213 ICANN הוא ארגון ללא מטרת רווח שהוקם בשנת 1998 בקליפורניה. הארגון אחראי לניהול כתובות ה־IP וחלוקתן לארגונים האזוריים לפי מדינות. הארגון מחזיק ומנהל את שרתי ה־DNS הבסיסיים ביותר (DNS Root level) ואחראי למעשה לניהול שיטת ה־DNS של האינטרנט (ראו עוד על השיטה לעיל בה"ש 119). הסמכות לשלוט ב־Root level הופכת את ICANN למתווכת שדרכה עוברת כל תעבורת הרשת, ומשכך הוא, הופך הארגון לבעל פוטנציאל לשמש גוף בין־לאומי לאכיפת הדין באינטרנט. ראו עוד להלן בנספח א, המוסיף רקע על ארכיטקטורת האינטרנט.

214 WTO הוא ארגון שהוקם בשנת 1995, וחברות בו כיום 159 מדינות.

215 להרחבה על המנגנון ראו למשל Laurence R. Hefler & Graeme B. Dinwoodie, *Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy*, 43

האמריקני כדי להפריט את פעילות ההסדרה והתחזוקה הטכנית של הקצאת כתובות ה־IP ושמות המתחם. אולם הארגון פעל מכוח הסמכה של משרד התעשייה והמסחר האמריקני, והאמריקנים סירבו לשחרר אחיזתם המשפטית ב־ICANN. הדבר עורר טרוניות מצד מדינות רבות על שארצות הברית למעשה שומרת על מעמדה כמעצבת־העל של ארכיטקטורת הרשת.[216]

אשר ל־WTO, הארגון מסונף לאו״ם ואמון על הסכמי הסחר הבין־לאומי. בהקשרנו, ה־WTO נדרש לברוֹר בין ארצות הברית לבין מדינת אנטיגואה שבאיים הקריביים, בעקבות מהלכים אמריקניים נגד חברות כרטיסי האשראי שסלקו עסקאות הימורים של תושבי ארצות הברית שנעשו באתרי ההימורים באנטיגואה. אנטיגואה הגישה תלונה לארגון הסחר העולמי בטענה כי פעולות האכיפה האמריקניות פוגעות בסחר החופשי בין המדינות, ערך שהארגון הבין־לאומי נועד לקדמו. מנגנון הבוררות הבין־לאומי פסק נגד ארצות הברית, ובערכאת הערעור נהפכה ההחלטה, אם כי נקבע כי ארצות הברית אינה יכולה לפסול גלישה לאתרי הימורים באנטיגואה ובה בעת להתיר הימורים באתרי אינטרנט המצויים בשטחה.[217]

אעבור עתה להתייחס למישור האכיפה הבין־מדינתי, להבדיל מהגלובלי, החוץ־מדינתי. במישור הפרקטי נעשו כמה מהלכים בניסיון להתמקד קונקרטית באכיפת הפשיעה הבין־לאומית במרחב הסייבר. אסקור כמה מהמהלכים הבולטים להלן, תוך חלוקה למהלכים בעלי פוטנציאל משפטי מחייב (כגון אמנה או דירקטיבה) ולמהלכים לא מחייבים משפטית. תחילה למהלכים המחייבים:

1) הניסיון הבין־לאומי המעשי החשוב ביותר מצוי בדמות אמנת מועצת אירופה בדבר פשעי מחשב (Convention on Cybercrime). האמנה נחתמה בבודפשט בשנת 2001 במסגרת מועצת אירופה (Council of Europe), אולם היא נפתחה להצטרפות של מדינות מחוץ לאיחוד האירופי. עד כה 54 מדינות, כולל מדינות מחוץ לאירופה, כגון ארצות הברית, קנדה ויפן, חתמו על האמנה, ו־47 מתוכן אשררו אותה.[218] נכון לעת הזאת, מדינת ישראל אינה חתומה על האמנה, אך זה זמן מה שהיא בוחנת הצטרפות אליה.[219] סעיפים 2—10 לאמנה מתייחסים לכמה עברות מחשב: חדירה לא מורשה לחומר מחשב, האזנת סתר לתקשורת בין מחשבים, שיבוש חומר מחשב ומחיקתו, שיבוש מערכות מחשב, זיוף ומרמה באמצעות מחשב, עברות הקשורות

WILLIAM & MARY L. REV. 141 (2001). המחברים טענו כי מנגנון ה־UDRP אינו יכול לשמש מודל לאכיפה בין־לאומית חוץ־מדינתית לגבי סוגיות אחרות באינטרנט.

216 ראו סקירת המאבקים הפוליטיים הבין־לאומיים סביב השליטה ב־ICANN אצל GOLDSMITH & WU, לעיל ה״ש 1, בעמ׳ 167—171.

217 ראו סקירה אצל Anupam Chander, *Trade 2.0*, 34 YALE J. INT'L L. 281, 287–290 (2009); GOLDSMITH & WU, לעיל ה״ש 1, בעמ׳ 172–173.

218 לנוסח האמנה המלא, ראו http://conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm. לפירוט המדינות החתומות על האמנה, ראו http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. לאמנה גם פרוטוקול נוסף שנחתם בשנת 2003: Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (Strasbourg, 2003) http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm. על הפרוטוקול הנוסף חתמו 35 מדינות, מתוכן 20 אשררו אותו.

219 חיים ויסמונסקי ״על תיקון סעיף 6 לחוק המחשבים״ (29.7.2012) http://law.co.il/articles/criminal-law/2012/07/29/amendments-to-the-israeli-computer-law.

nevo.co.il

להפצת תכנים פדופיליים ועברות הקשורות להפרות של זכויות יוצרים מוגנות. על המדינות שהן צד לאמנה לחוקק בחוקיהן הפנימיים איסורים על המעשים הללו, למעט בנסיבות שבהן האמנה מתירה התניה על חלק מהעברות או על חלק מהנסיבות המקימות את העברות. האמנה קובעת עוד כי המדינות, שהן צד לה, תגבשנה כלים מסוימים לאיסוף ראיות, כגון שימור מידע (Preservation), הפקת מידע (Production), תפיסה וחיפוש במחשבים, איסוף בזמן אמת של נתוני תעבורה (Real-time collection of traffic data) ואיסוף בזמן אמת של נתוני תוכן (Interception of content data). הפרק השלישי של האמנה מכונן מנגנונים מיוחדים לעזרה משפטית לצורך ייעול האיסוף וההעברה של המידע במסגרת חקירת עברות באינטרנט. כך למשל גובשו פרוצדורות מהירות למתן הוראה מהמדינה החוקרת למדינה האחרת לשמר את המידע שאגור בשטחה (סעיף 29); הקמת מנגנון בירוקרטי יעיל, שיפעל 24 שעות ביממה ושבעה ימים בשבוע, לצורך מתן עזרה משפטית דחופה על מנת למנוע מחיקת מידע נדיף באינטרנט. מנגנון זה מכונה "24/7 network" (סעיף 35). כן ניתנה הרשאה לחדירה לחומר מחשב האגור במדינה אחרת, ובלבד שמדובר בחומר שהגישה אליו חופשית או שניתנה הסכמה כדין של המחזיק במידע (סעיף 32). גם בכל הנוגע לדיני איסוף הראיות, נוסף על החלק המתייחס לעברות הפליליות עצמן, ניתנה באמנה אפשרות לכל מדינה להסתייג מחלק מההסדרים המוסכמים.

2) בצד מועצת אירופה, גם האיחוד האירופי (EU) פעיל בנוגע לאכיפה הפלילית הבין־לאומית באינטרנט. בשנת 2005 פורסמה החלטה הדורשת ממדינות האיחוד האירופי לחוקק חוקים בנוגע ל"מתקפות" על מערכות מידע, לרבות חדירה לא מורשה למחשב ולחומר מחשב; שיבוש, הפרעה או מחיקה של חומר מחשב. כמו כן המדינות התבקשו לכונן מנגנוני עזרה משפטית בין־מדינתיים בסגנון ה־"24/7 network".[220] החלטות נוספות של האיחוד האירופי, הדנות בפרסומים פדופיליים, בפרסומי הסתה לגזענות ובעברות זיוף ומרמה, התייחסו בין היתר גם לביצוע עברות אלה באינטרנט וקראו למדינות החברות באיחוד לאסור עליהן ולפעול במשותף לאכיפת האיסורים.[221] האיחוד האירופי הקים קבוצת מומחים שמטרתה לחקור את עברות האינטרנט ולעודד שיתוף פעולה בין מדינות האיחוד בהתמודדות עם עברות אלה.[222] בנוסף, ה־Eurojust, ארגון האיחוד האירופי לשיתוף פעולה משפטי, הצטרף למאמצים לעודד שיתוף פעולה בין מדינות האיחוד בנושא פשיעה באינטרנט.[223] בכל הנוגע לנושא של הגנת מידע אישי, קבוצת העבודה הקבועה שהוקמה מכוח הדירקטיבה להגנת מידע אישי[224] דנה

---

220 ראו EU Framework Decision 2005/222/JHA (16.3.2005) on Attacks Against Information Systems, OJ L 69, p. 67.

221 ראו Council Framework Decision 2004/68/JHA (20.1.2004) on Combating the Sexual Exploitation of Children and Child Pornography, OJ L 13, p. 44; EU Framework Decision 2008/913/JHA (6.12.2008) on Combating Racism and Xenophobia, OJ L 328, p. 55; EU Framework Decision 2001/413/JHA (2.6.2001) on Combating Fraud and Counterfeiting of Non-Cash Means of Payment, OJ L 149, p. 1.

222 קבוצה זו היא אחד ממוסדותיו הרשמיים של האיחוד האירופי: European Network and Information Security Agency (ENISA). על פעילות הקבוצה ראו http://www.enisa.europa.eu/.

223 ראו לעניין זה חומרים המפורסמים באתר האינטרנט של ה־EuroJust: http://www.eurojust.europa.eu/.

224 ראו Directive 95/46/EC of the European Parliament and of the Council (23.11.1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281.

nevo.co.il

בשיתוף פעולה בין־מדינתי במקרה של עברות על חוקי הגנת הפרטיות והגנת מידע אישי אשר חוצות גבולות מדינתיים. בשלב זה לא גובשו המלצות מחייבות בנושא.[225]

3) הליגה הערבית (Arab League) ניסחה בשנת 2010 אמנה בדבר מאבק בעברות במרחב הממוחשב.[226] אמנה זו קובעת עברות מחשב שעל מדינות החברות באמנה לקבען: חדירה לחומר מחשב, האזנת סתר בין מחשבים, גרימת נזק למידע ממוחשב או למחשבים, עברות זיוף ומרמה באמצעים ממוחשבים, עברות של הפצה או מסחר (לרבות קנייה) של תכנים פורנוגרפיים, עם נסיבות מחמירות באשר לפורנוגרפיית קטינים, פגיעה בפרטיות, טרור באמצעים מקוונים, עברה במסגרת ארגון פשיעה באמצעים מקוונים, עברות קניין רוחני באינטרנט ושימוש לרעה באמצעי תשלום מקוונים. בנוסף כוללת האמנה כמה סמכויות איסוף שצריכות להיות בידי כל המדינות שהן צד לאמנה, וכן היא קובעת מנגנוני עזרה משפטית מהירים בין החברות באמנה, בדומה לאלה הקבועות באמנת מועצת אירופה בדבר פשעי מחשב.

4) מדינות ה־OECD[227] פרסמו בשנת 2002 קווים מנחים לאבטחת מידע ורשתות מחשבים. קווים מנחים אלה נועדו למדינות החברות בארגון הכלכלי הבין־מדינתי והם מחייבים אותן. הקווים המנחים נועדו להגן על מערכות מידע ורשתות מחשבים, לעורר מודעות לסכנות באינטרנט ולדרכי ההתמודדות הראויות, לעודד אמון והסתמכות על מידע מוגן ולכונן פרוצדורות של שיתוף פעולה בין המדינות לצורך אבטחת המידע.[228]

---

225 ראו Article 29 Data Protection Working Party, Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments (5.4.2011), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf. ראו גם Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMP. L. & SEC. REP. 508 (2008), שם טוען בירנהק להתגבשות מודל בין־לאומי של הגנת מידע אישי דרך דירקטיבת האיחוד האירופי. הדירקטיבה היא דין מחייב למדינות האיחוד האירופי וכן משמשת מודל מוצע למדינות אחרות ולארגונים בין־לאומיים שהם "שחקנים" בזירה הבין־לאומית. מוסדות האיחוד האירופי אף בוחנים את המדינות החברות באיחוד אם הן עומדות בסטנדרטים של דירקטיבת האיחוד בדבר הגנת מידע אישי. ראו Michael Birnhack, *Reverse Engineering Data Protection Law*, 15 YALE J. LAW & TECH. 24, 63–66 (2013).

226 ראו League of Arab States Convention on Combating Information Technology Offences (2010), נמצא ב: http://www.era-comm.eu/Cybercrime/library.html. כן ראו דוח ה־UNODC, לעיל ה"ש 29, בעמ' 64, 66–67. על האמנה חתומות 19 חברות בליגה הערבית, ושלוש מדינות טרם חתמו עליה: לבנון, סומליה וג'יבוטי.

227 ראשי תיבות של Organization for Economic Cooperation and Development.

228 ראו OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002), *available at* http://www.oecd.org/dataoecd/16/22/15582260.pdf. הקווים המנחים קבעו תשעה עקרונות: מודעות (Awareness); אחריות (Responsibility); שיתוף פעולה לצורך מניעה, חשיפה ותגובה לפגיעות באבטחה (Response); התחשבות באינטרסים לגיטימיים של מדינות אחרות (Ethics); התחשבות בעקרונות של חברה דמוקרטית במסגרת יישום עקרונות של אבטחת מידע (Democracy); המדינות תנסינה לערוך מחקר מקדים בדבר סיכוני אבטחת מידע עתידיים (Risk Assessment); אבטחת המידע תוטמע כחלק אינטגרלי מכל מערכות המחשב החדשות (Security Design and Implementation); נושא אבטחת המידע יהיה תחום ניהול עצמאי ומקצועי תוך גיבוש נהלים והנחיות בנושא (Security Management); המדינות תערֵכנה מחדש את סיכוני אבטחת המידע (Reassessment).

nevo.co.il

5) ארגון שנחאי לשיתוף פעולה (Shanghai Cooperation Organization)[229] חתם בשנת 2009 הסכם לשיתוף פעולה בתחום אבטחת המידע, ובו התחייבות להעניק סיוע הדדי למדינות הארגון בתחום הגנת מרחב הסייבר, לרבות בהקשר של אכיפה פלילית.[230]

ועתה בכל הנוגע למהלכים הבין־לאומיים הלא מחייבים:

1) מדינות ה־G8 הגיעו להסכמות מסוימות ביניהן בנוגע לאופן איסוף הראיות הדיגיטליות בחקירות פליליות באינטרנט.[231] המסמך משנת 1999 כונן חלק מההסכמות שגובשו לאחר מכן באמנת מועצת אירופה בדבר פשעי מחשב: קביעת מנגנון יעיל לשימור מידע על פי בקשה דחופה של מדינה אחרת החברה בארגון, קביעת מנגנון עזרה משפטית בסגנון ה־"24/7 network", קביעת מנגנון יעיל ולא פורמלי לעזרה משפטית בין המדינות החברות בארגון, הסכמה כי מותר לחוקרי מדינה א לחדור לחומרי מחשב האגורים בשרתים במדינה ב, אם מדובר בחומרים הפתוחים לציבור הרחב או אם התקבלה הסכמה כדין של מחזיק במידע. מדינה א במקרה כזה תשקול יידוע של מדינה ב בדבר פעולת חדירה שכזאת. יצוין כי מנגנון ה־"24/7 network" של מדינות ה־G8 הוא מנגנון וולונטרי, שההצטרפות אליו אינה מחייבת חתימה על אמנה בין־לאומית, כבמקרה של אותו מנגנון המופיע בהוראות אמנת מועצת אירופה בדבר פשעי מחשב. מדינות רבות, שאינן חלק מה־G8, הצטרפו למנגנון זה, ובהן גם מדינת ישראל, ונכון להיום מספרן גדול מ־50.

2) במסגרת ארגון הטלקומוניקציה הבין־לאומי (ה־ITU) פורסם בשנת 2010 מודל מוצע לחקיקה מדינתית בנושא פשיעה באינטרנט.[232] מטרת המודל לעודד האחדה בין־מדינתית של הדין המהותי והפרוצדורלי בנוגע לעבירות אינטרנט. למודל אין תוקף מחייב, שכן ה־ITU הוא גוף להתוויית מדיניות בלבד (ובתחומים מצומצמים).[233] מסמך ה־ITU מתייחס לעבירות האלה בלבד (סעיפים 2—9): חדירה לא מורשה למחשבים ולמערכות מחשב, חדירה לא מורשה לחומר המחשב ונטילה לא מורשה של חומר המחשב, האזנת סתר לתקשורת בין מחשבים, זיוף ומרמה באמצעות מחשב, סחיטה באמצעות מחשב והעברת נגיפי מחשב. כמו כן מציע המסמך למדינות לכונן סמכות שימור מידע, סמכות להפקת מידע, סמכות לציתות לנתוני תעבורה ולנתוני תוכן

---

229 מדובר בארגון שהוקם בשנת 1996 וכולל את המדינות האלה: סין, רוסיה, טג׳יקיסטן, קזחסטן, קירגיסטן ואוזבקיסטן.

230 ראו UNODC, לעיל ה״ש 29, בעמ׳ 63—68.

231 ראו G8 Justice and Interior Ministerial, Principles on Transborder Access to Stored Computer Data (1999), *available at* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/.

232 ראו International Telecommunication Union Toolkit For Cybercrime Legislation (2010), *available at* http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf. השיטה של מודל חקיקתי המשמש כלי עזר למדינות המעודד אותן לאמץ סטנדרט חוקי אחיד, יושמה בעבר במקרים של חתימה אלקטרונית וסחר אלקטרוני. ראו United Nations Commission on International Trade, Model Law on Electronic Signatures with Guide to Enactment (2001), *available at* http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf; United Nations Commission on International Trade, Model Law on Electronic Commerce with Guide to Enactment (1996), *available at* http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

233 הארגון הוקם על מנת להסדיר שימוש בתדרי רדיו, הצבה מתואמת בחלל של לוויינים, שיפור תשתיות טלקומוניקציה בין־לאומית בקביעת תקני איכות ושיפור ההנגשה לאמצעי טלקומוניקציה. ראו http://www.itu.int/en/about/Pages/default.aspx/.

nevo.co.il

וסמכות לתפיסה ולחיפוש בחומר מחשב. במישור שיתוף הפעולה הבין־מדינתי מציע המסמך של ה־ITU פתרונות דומים לפתרון של אמנת מועצת אירופה בדבר פשעי מחשב: כינון מנגנון עזרה משפטית 24/7 והכרה בתנאי האמנה האירופית לחדירה לחומר מחשב האגור במדינה אחרת.

מודלים מוצעים נוספים לחקיקה מדינתית בנושא פשיעה באינטרנט נוסחו במדינות חבר העמים הבריטי (The Commonwealth of Nations) בשנת 2002[234] ובשוק המזרח־אפריקני המשותף והדרום־אפריקני (Common Market for Eastern and Southern Africa).[235]

3) במסגרת האו"ם נעשה ניסיון לערוך מחקר בין־מדינתי מקיף בדבר הפשיעה באינטרנט. המחקר עסק בנושאים האלה: הגדרת בעיית הפשיעה באינטרנט, נתונים סטטיסטיים בדבר הפשיעה באינטרנט, כיצד ניתן להגיב משפטית ולא־משפטית לפשיעה באינטרנט, כיצד על הקהילה הבין־לאומית להתמודד עם פשיעה באינטרנט, אם וכיצד יש לסייע טכנולוגית למדינות מתפתחות על מנת לאפשר להן לאכוף עברות באינטרנט והתמודדות עם תפקידו של המגזר הפרטי באכיפה הבין־לאומית של הפשיעה באינטרנט. בשלב זה אין מהלך במסגרת האו"ם אשר נועד להיות בעל ערך מחייב מבחינה משפטית.[236]

4) מדינות ה־OAS[237] הכריזו בשנת 1999 על הקמת צוות עבודה קבוע לנושא המלחמה בפשיעה האינטרנטית. קבוצת העבודה נפגשה עד כה שש פעמים והוציאה כמה המלצות כתובות למדינות הארגון כדי לאחד את אופן פעולתן לחקירת עברות באינטרנט ולמניעתן, וכן כדי לייסד מנגנוני שיתוף פעולה ביניהן בחקירת עברות אלה בדומה לאלה שנקטו הארגונים הבין־לאומיים שמניתי לעיל. בעיקר, קרא צוות העבודה למדינות הארגון להצטרף למנגנון ה־"24/7 network" של מדינות ה־G8.[238]

נמצאנו למדים כי במהלך השנים האחרונות נעשו כמה מהלכים, חלקם מחייבים משפטית וחלקם לא, רובם ברמה האזורית, לכינון מערכת חוקית בין־מדינתית הרמונית לאכיפה פלילית במרחב הסייבר. חלק מהניסיונות עוסקים בהאחדת ההגדרות לעברות במרחב הסייבר, חלק מהניסיונות מבקשים לייצר מנגנוני איסוף ראיות בין־מדינתיים, וחלק מהניסיונות עניינם בפיתוח

---

234 ראו Commonwealth Cybercrime Initiative, לעיל ה"ש 34. ב־2011 החל הארגון לפעול לעדכון מודל החקיקה.

235 ראו Common Market for Eastern and Southern Africa (COMSEA) Cybersecurity Draft Model Bill (2011), also *available at* http://www.era-comm.eu/Cybercrime/library.html.

236 ראו לעיל בה"ש 28. יצוין כי הדיונים ב־UNODC סביב בחינה של אכיפה בין־לאומית בזירה האינטרנטית החלו בשנת 2009. עוד קודם לכן, במסגרת הקונגרס ה־11 של האו"ם בנושא Crime Prevention and Criminal Justice, שנערך בבנגקוק בשנת 2005, נוסחה הצהרה שאושרה בעצרת האו"ם לאחר מכן, ולפיה על המדינות החברות באו"ם לפתח מנגנונים מדינתיים וכן מנגנוני שיתוף פעולה בין־מדינתיים להתמודדות עם פשיעה באינטרנט, לרבות מניעה, חקירה פלילית והעמדה לדין בעברות מחשבים (High-tech and computer-related crime). ראו GA Resolution 60/177 of 16.12.2005, para. 2. כן ניתן לציין שתי הצהרות מוקדמות יותר של העצרת הכללית של האו"ם לעידוד תרבות ושיתוף פעולה בין־מדינתי בנושאי אבטחת מידע (Cybersecurity). ראו United Nations GA Resolution 57/239 of 20.12.2002 וכן United Nations GA Resolution 58/199 of 23.12.2002.

237 Organization of American States, המאגד 35 מדינות של צפון אמריקה ודרום אמריקה.

238 ראו OAS Sixth Meeting of the Working Group on Cyber-crime (2010), *available at* http://www.oas.org/juridico/english/cyb_VIrec_en.pdf.

nevo.co.il

דיני אבטחת מידע אחידים ושיתופיים בין המדינות. האסטרטגיה שבבסיס ניסיונות אלה היא למנוע היווצרות "מדינות מקלט" ברמת הדין המהותי או ברמת דיני איסוף הראיות, היינו מדינות שבהן תותר פעילות פלילית מסוימת ששאר המדינות אינן מעוניינות בה ומנסות למנוע אותה, או שתיאסר באותן מדינות פעולה מסוימת של איסוף הראיות אשר מדינות אחרות מעוניינות לאפשרה בנסיבות המקרה הנחקר.[239]

ב) הערכת החלופה

אין ספק כי היותו של מרחב הסייבר חוצה גבולות מדיניים, החלופה הבין־לאומית נתפשת כחלופה טבעית לאכיפה הפלילית המדינתית הקלאסית. כפי שניתן לראות, מבחינה מעשית נעשו ניסיונות ניכרים להגברת האכיפה הבין־לאומית במרחב הסייבר. אולם הפתרון הבין־לאומי, בין הגלובלי ובין הבין־מדינתי, סובל מכמה בעיות אינהרנטיות שמגבילות את כוחו לשמש חלופה ממשית לאכיפה הפלילית המדינתית במרחב הסייבר:[240]

ראשית, קצב הגיבוש של אמנות בין־לאומיות מחייבות הוא אטי במיוחד בשל הצורך בכינוס ישיבות רבות־משתתפים ממדינות שונות, בשל הצורך בגיבוש קונצנזוס על נוסח האמנה, ולאחר מכן בשל הצורך של כל מדינה ומדינה לאשרר את האמנה תוך התאמה, במידת הצורך, של חוקיה הפנימיים לדרישות האמנה. כשמדובר בפשיעה במרחב המקוון, המתבצעת על פלטפורמה טכנולוגית המשתנה בקצב מסחרר והמעוררת סוגיות חדשות כל העת, נדרשת תגובה משפטית מהירה הרבה יותר.[241]

---

239 ראו, לעניין זה Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. Chi. L. Rev. 1199, 1230–1232 (1998).

240 מלבד פירוט אותן בעיות להלן, יש לזכור כי קיים ויכוח עקרוני מקדמי בכל הנוגע לעצם כוחו של המשפט הבין־לאומי לאכוף ציות. לא ארחיב את הדיון בנושא זה ואניח, לצורך הדיון, כי ביכולתו העקרונית של המשפט הבין־לאומי לקבוע כללים מחייבים ואף לאכפם. אציין רק כי מצד אחד העמדה הראליסטית גורסת כי המשפט הבין־לאומי מוחלש ואינו יכול לכפות ציות הסותר את האינטרס של המדינות שעליהן מופעלת האכיפה. ראו Robert H. Bork, *The Limits of "International Law"*, National Interest 3 (Winter 1989–1990); Francis A. Boyle, *The Irrelevance of International Law: The Schism Between International Law and International Politics*, 10 Cal. W. Int'l L.J. 193 (1980). כן ראו ניתוח דומה, בהתבסס על תורת הבחירה הרציונלית (Rational Choice Analysis) אצל: Jack L. Goldsmith & Eric A. Posner, The Limits of International Law (2005). מנגד גורסת העמדה הקונסטרוקטיביסטית כי אין תפקודו של המשפט הבין־לאומי אינסטרומנטלי בלבד בשביל המדינות, אלא הוא משפיע על הנורמות והאינטרסים של המדינות ומעצב אותם, ובכוחו אף להיות כוח מסדיר בעל שיניים אכיפתיות. ראו למשל Abram Chayes & Antonia Handler Chayes, The New Sovereignty: Compliance With International Regulatory Agreements (1995); Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 Yale L.J. 2599 (1997); John Gerard Ruggie, *What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge*, 52 Int'l Org. 855 (1998).

241 ראו Goldsmith & Wu, לעיל ה"ש 1, בעמ' 167. גולדסמית' ו־וו הוסיפו וטענו שגם אמנת מועצת אירופה בדבר פשעי מחשב, שנפתחה להצטרפות של מדינות מחוץ לאיחוד האירופי, אינה מצליחה להביא להצטרפות כלל מדינות העולם, ומכאן הם הסיקו שגם ניסיון זה, הנחשב לבולט ביותר מבין הניסיונות הבין־לאומיים לאכוף את הדין הפלילי באינטרנט, הוא בבחינת כישלון. ראו גם Susan W.

nevo.co.il

שנית, מבחינת הדין הפלילי המהותי שיכוסה במסגרת מנגנוני האכיפה הבין־לאומיים, קיימת מגבלה ניכרת בשל השונות בתפישת האיסורים הפליליים בין המדינות השונות. הראיתי בפרק הקודם כי במסגרת העברות הפליליות במרחב הסייבר נכללות למעשה כל העברות הפליליות, בין שחלק מביצוע העברה עובר במרחב המקוון ובין שכל העברה מתבצעת בתוככי המרחב.[242] על מנת לחלוש על האכיפה הפלילית במרחב הסייבר במסגרת בין־לאומית, נדרש למעשה להגיע לקונצנזוס באשר לכל דיני העונשין. משימה זו היא בלתי אפשרית ברמה הגלובלית, כיוון שחלק ניכר מההתנהגויות הן בבחינת mala prohibita, ולא mala in se, דהיינו קביעתן כאיסור הוא תלוי־מדינה. ההסכמה בין המדינות בדבר האיסורים השונים צריכה לחול לא רק על כותרת האיסור אלא גם על תנאיו המפורטים של האיסור, מבחינת ההתנהגות האסורה, הנסיבות, התוצאה והיסוד הנפשי. אם השאיפה תהיה ליצור הסכמה כלל־מדינתית, לא יהיה מנוס מלחתור למכנה משותף, והמכנה המשותף שייווצר יהיה מינימליסטי מבחינת היקף תחולתו.

שלישית, עלולות להיווצר "מדינות מקלט" סוררות, שלא תסכמנה לשתף פעולה עם המנגנונים הבין־לאומיים. כיוון שההבדלים הגאוגרפיים נטולי משמעות בזירה הקיברנטית, הרי שהיעדר הסכמה של כלל המדינות על האיסורים הכלולים בהסכם הבין־לאומי ועל הצורך באכיפתם, משמעו יצירת תמריץ חזק להעתיק את הפעילות העבריינית אל המדינות שאינן צד לאותה הסכמה. העתקה זו זולה למדי ובת־ביצוע מרחוק, "בלחיצת כפתור".

רביעית, מבחינת הדינים הפרוצדורליים שיוסכמו בין המדינות במסגרת מנגנון האכיפה הבין־לאומי נדרשת הסכמה על רמת החשד המצדיקה פתיחה בחקירה בין־לאומית, הגדרה אחידה של סמכויות הרשות החוקרת (אילו פעולות מותר לה ואילו לא), תנאים בדבר העברת המידע שנאסף בין המדינות וכיוצא בזה. נובע מן האמור כי ניסיון ליצור מודל אכיפה פלילית בין־לאומי מחייב הסכמה לא רק על האיסור המהותי אלא גם על היבטים רבים של פרוצדורה פלילית, שבה קשת האפשרויות מתרחבת עוד יותר.[243]

חמישית, ניתן לצפות שיקשה להשיג קונצנזוס רחב באשר ל"גבולות הגזרה" של מנגנון האכיפה הבין־לאומי. כבר ציינתי לעיל כי העברות הפליליות במרחב הסייבר, אפילו המובהקות שבהן שנותרות כולן בתוככי המרחב הווירטואלי – גורמות לנזק ממשי במרחב הפיזי.[244] במקרה כזה יהיה צורך לקבוע אם העברה תיאכף בידי המדינה בלבד או בידי המנגנון הבין־לאומי. סביר להניח שהמדינות תתקשינה מאוד להסכים מראש, קטגורית, אימתי תיאכף עברה בידי המדינה בלבד ואימתי בידי המנגנון הבין־לאומי.

Brenner, *The Council of Europe's Convention on Cybercrime*, CYBERCRIME – DIGITAL COPS AND LAWS IN A NETWORKED ENVIRONMENT 207, 216–219, לעיל ה"ש 149.

242 ראו לעיל בפרק המבוא את תרשים 1.1.

243 ראו הניתוח של הרדוף באשר ל"מתקלי דינים" שונים בין מדינות באכיפת פשיעה חוצת־גבולות באינטרנט: הרדוף, לעיל ה"ש 74, בעמ' 246–256. יוער כי הרדוף דיבר על מתקל דינים מהותי, פרוצדורלי ועונשי. אשר למתקל הדינים העונשי (שבו מדינה א קובעת עונש X לעברה מסוימת, ואילו מדינה ב קובעת עונש Y לאותה עברה), לא ראיתי לנכון להתייחס אליו בניתוח כאן, שכן מתקל זה מהווה חסם לשלב אחר של האכיפה הפלילית: שלב ההסגרה ממדינה למדינה ושלב הענישה בפועל, ולא שלב החקירה הפלילית שבו אני מתמקד כאן.

244 ראו לעיל בפרק ב.ד.1.ב).

nevo.co.il

בסיכומו של דבר, ממבט ראשון החלופה הבין־לאומית היא אטרקטיבית ביותר. מצד אחד, היא בין־מדינתית, דהיינו היא שומרת על מעמדה הריבוני של המדינה ועל סמכותה כאוכפת חוק פלילית. בנוסף, היא יכולה תאורטית לכסות את כלל הזירה המקוונת. אולם מצד שני, בשל הקשיים המהותיים והקשיים בארגון שיתוף הפעולה בין המדינות באשר לזירה המקוונת, שאותם מניתי לעיל, הזירה הבין־לאומית לא תוכל לספק מענה כולל לאכיפה הפלילית במרחב הסייבר. זאת אף שניתן להניח שלכלל המדינות אינטרס למגר את פשיעת הסייבר המסבה להן נזק. לכל היותר, "איים" משפטיים מסוימים, שבהם ניתן להשיג קונצנזוס גלובלי, יוכלו להיות מטופלים בזירה הבין־לאומית, וגם במקרים אלה הביצוע בפועל של ההסכמות יהיה תלוי בפעולתה האוטונומית של המדינה שתתבקש לבצע את פעולות האכיפה כפועל יוצא מן ההסכם הבין־לאומי. ככל שמספר המדינות השותפות להסכם הבין־לאומי יקטן, כך יהיה ניתן להרחיב את ההסכמים לעברות פליליות נוספות ולפעולות איסוף ראיות נוספות, אולם כתוצאה מהקטנת מעגל המדינות השותפות להסכם תיווצר לעברייני הרשת האפשרות לפעול ממדינות זרות שהן מחוץ להסכם.

ו. מסקנת הדיון

בפרק זה בחנתי את שאלת ההצדקה לכך שהמדינה תמשיך להיות הגוף המרכזי באכיפה פלילית במרחב הסייבר. תחילה עמדתי על ההצדקות העקרוניות לכך שהמדינה אוכפת את החוק הפלילי במרחב הפיזי. בשלב הבא הצגתי שורה של קשיים – ארכיטקטוניים, משפטיים ומוסדיים – לאכיפה הפלילית המדינתית במרחב הסייבר. לאחר מכן עמדתי בהרחבה על החלופות השונות לאכיפה הפלילית המדינתית במרחב. הצגתי חלופות לשיטת האכיפה, דהיינו חלופות אכיפה שאינן כוללות חקירה פלילית בדיעבד, לאחר קרות העברה, ההעמדה לדין והענישה. כן הצגתי חלופות לזהות הגורם האוכף, דהיינו חלופות שבהן הנושאת באחריות לאכיפה אינה המדינה כי אם גורמים אחרים – ספקיות שירות מתווכות או הקהילה הבין־לאומית. הראיתי כיצד החלופות הללו, כשהן עומדות לעצמן ומתיימרות להחליף את האכיפה הפלילית המדינתית, מוגבלות ליישום בשל שלל בעיות משפטיות, טכנולוגיות ובעיות מתחום כיבוד ריבונותן של מדינות זרות.

מכאן שאי אפשר לראות בחלופות אלה משום תחליף לפרדיגמת החקירה הפלילית המדינתית. אשר לחלק מחלופות אלה, למשל האכיפה המגוננתית־הוולונטרית, או ההעברה של חלק מהחובות לספקיות השירות, וכמובן גם המאמצים לשיתוף פעולה בזירה הבין־לאומית – כבודן במקומן מונח, ואין לבטלן ברמה העקרונית. אולם מסקנתי בשלב זה של הדיון היא כי חלופות אלה לאו חלופות הן, אלא תוספות משלימות בלבד.

משלילת כל החלופות המוכרות לאכיפה הפלילית המדינתית במרחב הסייבר נובעת המסקנה שיש לשוב ולבחון לעומק את יכולתה של המדינה לספק מענה לצורכי אכיפה פלילית במרחב הסייבר. ניכר על החוקרים שבחנו חלופות לאכיפה הפלילית המדינתית כי הם הניחו כאקסיומה את כישלון האכיפה הפלילית המדינתית במרחב הסייבר, הן מבחינה מעשית והן מבחינה עיונית. בהמשך הדיון אבקש לחזור לאקסיומה זו ולערער אותה. בפרקים ג–ה להלן אציג ואציע לבחון מחדש שתי תפישות יסודיות, החולשות כיום על תחום איסוף הראיות לחקירת עבירות פליליות במרחב הסייבר: תפישה טריטוריאלית ותפישה פיזית. תפישות אלה הן העומדות לטעמי בבסיס

nevo.co.il

הכישלון של דיני איסוף הראיות לשרת את מטרתם המשולשת: הן הספקת כלים יעילים למדינה להוכחת עברות פליליות והוכחת זהות מבצעיהן, הן הגנה על הביטחון האישי, הכלכלי והלאומי במרחב המקוון והן שמירה על זכויות מוגנות של החשוד והצדדים השלישיים הבאים עמו במגע, ואשר זכויותיהם עלולות להיפגע במסגרת איסוף הראיות. התנערות מן התפישה הטריטוריאלית ומן התפישה הפיזית תאפשר למדינה – כך אטען – להשיב את מעמדה כאוכפת חוק פלילית במרחב הסייבר.

nevo.co.il