הטרור באינטרנט: תקיפות סייבר שמטרתן היא פגיעה בפרטיות

ברוריה פרידמן פלדמן

מאמר זה מציג את הצורך לעדכן את חוק המאבק בטרור כדי להתמודד עם תצורות אקטואליות של איומים קיברנטיים. החוק כיום כולל סוגים מסוימים של תקיפות רשת קיברנטיות (CNA) תחת הגדרת הטרור, אך אינו מתייחס לפעולות סייבר מסוג איסוף (CNE), חדירה למערכות וניצול המידע שמושג ללא גרימת הרס ישיר. מאחר שפעולות מסוג איסוף יכולות להוביל לפגיעה חמורה בפרטיות, בפרט בהקשר של פרטיות אישית וביטחון לאומי, מאמר זה טוען כי יש להרחיב את הגדרת הטרור בחוק הישראלי כך שתכלול הן פעולות איסוף והן פעולות שיבוש. עדכון כזה ישקף את מציאות האיומים הקיברנטיים בני זמננו ויחזק את יכולתה של המערכת המשפטית להתמודד עם תצורות חדשות של קיבר־טרור. המאמר קורא למחוקק להרחיב את הגדרת הטרור כך שתכלול פעילויות איסוף במטרה להתאים את המאבק בטרור של ישראל למציאות האיומים הקיברנטיים המודרניים ולחזק את עמידותה כנגד כל פעילות טרור באינטרנט.

מבוא

נהוג להגדיר פעולת סייבר כפעולת מניפולציה מכוונת של מחשב או רשת מחשבים אשר בעקבותיה נגרמת תוצאה רצויה מראש. נבחין בין פעולות שיבוש לפעולות איסוף. בעוד פעולות שיבוש מובילות להרס או השבתה של רכיבים או מערכות ברשת היעד, פעולות איסוף מוגבלות לאיסוף חשאי של המידע ושימוש בו על ידי הפורצים, בין אם באופן אישי ובין אם באמצעות פרסומו. פעולות סייבר אלו עלולות להוביל לחשיפה של הפורצים למידע אישי רב השמור על גבי מחשבים ושרתים ברשת שאליה חדרו. מידע זה יכול לשמש את הפורצים למגוון מטרות ויכול לכלול שימוש במידע הגנוב או פרסומו. בכל מקרה, הפגיעה בפרטיות היא עמוקה, קבועה וארוכת טווח.

כיום נראה שאין כלי חוקי המאפשר להגדיר פעולת סייבר מסוג איסוף כאקט טרור, למרות שיש לפעולה זו פוטנציאל נזק משמעותי שלפעמים עולה על הזנק הנגרם מפעולת שיבוש. חוק המאבק בטרור מגדיר שלושה תנאים מצטברים לסיווג של פעולה כמעשה טרור: הפעולה נעשתה ממניע אידאולוגי־לאומני, היא נועדה לעורר פחד בציבור, וגרמה, או יצרה סיכון ממשי, לנזק פיזי. יישום של תנאים אלו, בדגש על התנאי השלישי, על פעולות סייבר המבוצעות ממניעים אידאולוגיים ונועדו לזרוע בהלה בציבור, מוביל למסקנות סותרות. מצד אחד, פעולת סייבר מסוג שיבוש מייצרת פגיעה פיזית ולכן עומדת בתנאים של מעשה טרור. מצד שני, פעולות איסוף, שמהותן היא גנבה ופרסום של מידע שהושג באופן לא חוקי, על פי רוב נופלות מחוץ לגבולות ההגדרה, זאת חרף הפגיעה החמורה בפרטיות הנפגעים.

ברשימה זו אבקש לנתח את הפגיעה בפרטיות שנגרמת במסגרת פעולות טרור בסייבר. על בסיס ניתוח זה, אטען כי בחוק המאבק בטרור קיים פער בזיהוי של פעולות בסייבר כמעשי טרור. הדבר גורם לכך שתקיפות סייבר שמובילות לפגיעה עמוקה וארוכת טווח בפרטיות אינן זוכות להכרה כמעשי טרור בעיני החוק. על כן, אציג הצעות לתיקון פער זה וכן הצדקות לצמצומו.

מפת הדרכים למאמר זה היא כדלהלן: **א. פעולות סייבר והזכות לפרטיות.** א(1) פעולות סייבר וסיווגן. א(2) הזכות לפרטיות – מהי? א(3) פגיעה בפרטיות בפעולות סייבר. **ב. פעולות סייבר בראי חוק המאבק בטרור.** ב(1) מעשה טרור במשפט הישראלי. ב(2) סוגי הנזק המנויים בהגדרה של מעשה טרור. ב(3) סיווג פעולות סייבר כמעשה טרור בהתבסס על סוג נזק. ב(4) הפער בחוק המאבק בטרור באמצעות מקרה בוחן: שירביט. **ג. ממצאים ומסקנות.** ג(1) פתרון מוצע – אימוץ הפרשנות האירופית להגדרה של מעשה טרור. ג(2) הצדקות לשינוי ההגדרה של מעשה טרור בחוק באשר לפגיעה בפרטיות. **ד. ביקורות כנגד הרחבת ההגדרה של מעשה טרור בחוק המאבק בטרור.** ד(1) קושי בהעמדה לדין. ד(2) קביעת רף החומרה. ד(3) הרחבת אחריות המדינה. **ה. סיכום.**

א. פעולות סייבר והזכות לפרטיות

א.1 פעולות סייבר וסיווגן

<u>סוגי פעולות סייבר</u>

נהוג להגדיר פעולת סייבר כפעולת מניפולציה מכוונת (או רצף פעולות מסוג זה) של מחשב או רשת מחשבים אשר בעקבותיה נגרמת תוצאה רצויה מראש.[1] לרוב פעולות מסוג זה מוכוונות ומבוצעות על ידי ממשלות וצבאות, אך ישנם מקרים שבהם אנשים פרטיים או קבוצות פרטיות עומדים מאחורי פעולה זו או אחרת.

קיימות כמה שיטות לסיווג פעולות סייבר: על פי מטרת הפעולה ותוצאותיה, על פי הכלים הטכנולוגיים שבאמצעותם הפעולה הוצאה לפועל וכן על פי סוג הנזק שנגרם (פיזי, כלכלי, תדמיתי וכולי).[2] רשימה זו עוסקת בפעולות סייבר שנועדו לגרום לפגיעה בפרטיות, לכן אשתמש בסיווג המבוסס על תוצאות הפעולות.

בחלוקה גסה, ניתן לזהות שני סוגים של פעולות סייבר. הסוג הראשון הוא פעולות שיבוש (CNA),[3] פעולות שמובילות להשבתה או הריסה של היעד. כך למשל, השבתה של מערכות הניהול בנמל שהיד רג'אעי באיראן, השבתת צינור הולכת הגז המרכזי בארצות הברית ותקיפות נוספות.[4] הסוג השני הוא פעולות מסוג איסוף

---

[1] Tarun Yadav & Arvind Mallari Rao, *Technical Aspects of Cyber Kill Chain,* in SECURITY IN COMPUTING & COMMUNICATIONS 438–52 (2015).

[2] M. Uma & Ganapathi Padmavathi, *A Survey on Various Cyber Attacks and their Classification*, 15 INT'L J. OF NETW. SECUR. 390, 396–390 (2013); Ioannis Agrafiotis et al, *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding how they Propagate*, 4 J. OF CYBERSEC. (2018).

[3] Cyber Network Attack – CNA.

[4] "דיווח: מתקפת הסייבר האיראנית נועדה להעלות את רמת הכלור במים בישראל" **הארץ** (1.6.2020); https://www.haaretz.co.il/news/politics/2020-06-01/ty-article/.premium/0000017f-dbcb-df9c-a17f-ffdbb9e40000 Joseph Choi, *Regional Emergency Declaration Issued over Pipeline Shut-down after Cyberattack*, THE HILL (Sept. 5, 2021, at 10:30 ET), https://thehill.com/homenews/administration/552564-white-house-declares-state-of-emergency-over-cyberattack-that-shut/; Andy Greenberg, *Chinese Hacking Spree Hit an 'Astronomical' Number of Victims*, WIRED (May 5, 2021, at 6:56 ET), https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/; Ronen Bergman & David M. Halbfinger, *Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks*, N.Y TIMES (2020), https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html.

(CNE)[5] שמטרתן היא השגת נגישות למידע השמור ברשת המחשבים של היעד, באופן לא חוקי, לצורך שימוש במידע או פרסומו.[6]

עתה נחדד את מאפייני פעולת השיבוש לעומת מאפייני פעולת האיסוף באמצעות דוגמאות. אחת מפעולות השיבוש המפורסמות והמוקדמות ביותר היא נוזקת Stuxnet שהתגלתה ב־2011. מדובר בתולעת[7] שהתפשטה ברשתות רבות, אך יועדה לרשתות של צנטריפוגות במתקן העשרת אורניום בנתנז, איראן. התולעת הייתה מזהה כי יש צנטריפוגות ברשת ומשנה את ההגדרות שלהן כך שמהירות הסיבוב תעלה על המהירות המקסימלית המומלצת, מה שבסופו של דבר הוביל להרס והשבתה של הצנטריפוגות. מבצע זה עיכב את היכולת של איראן לפרוץ לגרעין וכן שינה את פניה של לוחמת הסייבר.[8] מטבען, פעולות סייבר מסוג שיבוש נועדו להיות "רועשות", ואין מניעה שיתגלה כי רכיב הושבת או נהרס כליל. כמובן שזה לא בהכרח אומר שממען התקיפה ייחשף או אפילו שיזהו כי השיבוש נגרם בעקבות פעולת סייבר.

באשר למבצע איסוף, אחת הדוגמאות הבולטות והדרמטיות מהשנים האחרונות היא פריצה לרשת המחשבים של המפלגה הדמוקרטית בארצות הברית (DNC) לפני הבחירות ב־2016. במסגרת הפריצה נגנבו אלפי מסמכים חסויים של המפלגה הדמוקרטית אשר עסקו בתוכניות האסטרטגיות של הקמפיין הנשיאותי של המועמדת דאז, הילרי קלינטון, וכן מידע רגיש על המפלגה הדמוקרטית. אין ספק כי פרסומים אלו השפיעו על המרוץ הנשיאותי והגדירו מחדש את הגבולות של מאמצי שינוי תודעה ומבצעי השפעה.[9] פעולות מסוג איסוף נועדו, לרוב, להישאר חשאיות גם אחרי שהפורצים עזבו את הרשת עם המידע שהם נדרשו לאסוף. בשל אופיין הסודי, פעולות אלו נחשפות רק בשל טעות אנוש או לחלופין החלטה מודעת של הפורצים, והפעולה מתגלה והמידע שנגנב מפורסם לכל מאן דבעי.

קווים לדמותה של פעולת סייבר

התפיסה הרווחת היא שפעולת סייבר, CNA או CNE, בנויה משבעה שלבים: (1) איסוף המל"מ, (2) חימוש, (3) העברה, (4) ניצול חולשה, (5) התקנה, (6) פיקוד ושליטה, (7) הוצאה לפועל.[10]

---

[5] Cyber Network Exploit – CNE; פעולה זו מכונה information content security / data confidentiality; European Union Agency for Network and Information Security, *Reference Incident Classification Taxonomy: Task Force Status and Way Forward,* 9–18 (2018).

[6] Charles Harry & Nancy Gallagher, *Classifying Cyber Events: A Proposed Taxonomy*, 5 CENTER FOR INT'L & SECURITY STUD. AT MD. 8–5 (2018); JOHN HOWARD & THOMAS LONGSTAFF, A COMMON LANGUAGE FOR COMPUTER SECURITY INCIDENTS (Sandia National Laboratories (1998); Maria Kjaerland, *A Classification of Computer Security Incidents based on Reported Attack Data,* 2 J.OF INVESTIGATIVE PSYCH. OFFENDER PROF., 120–105 (2005).

[7] נוזקה בעלת יכולת לחדור ובאופן עצמאי, ולשכפל, לעיתים ללא הכוונה, ברשת היעד.

[8] J.R. Lindsay, *Stuxnet and the Limits of Cyber Warfare*, 22 SEC. STUD. 404–365 (2013); J.P. Farwell & R. Rohozinski, *Stuxnet and the Future of Cyber War*, 53 SURVIVAL 40–23 (2011).

[9] Ellen Nakashima & Shane Harris, *How the Russians hacked the DNC and passed its emails to WikiLeaks*, WASH. POST (July 13, 2018, at 7:26 ET), https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

[10] להרחבה על מודל תקיפת סייבר גנרית ומבוא לפעולות סייבר ראו: Yadav & Rao, *Technical Aspects of Cyber Kill Chain*; לעיל ה"ש 1; Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, *Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, IN LEADING ISSUES IN INFORMATION WARFARE & SECURITY RESEARCH 1.1 80, 80-84 (2011).

מאמר זה טרם עבר עימוד סופי ומספרי העמודים ישתנו לכשיתפרסם הכרך המודפס. כן צפויים שינויים נוספים.

נוזקה היא שם כולל לכל האמצעים שנועדו, יחד, לממש מניפולציה על הרכיבים ברשת[11] היעד על מנת להוציא לפועל את מטרת הפעולה. בזה נכלל גם סיוע לפורץ להשיג גישה לרשתות ומחשבים שבעליהם לא מעוניינים בכך. השלב הראשון הוא איסוף מל״מ (מידע לפני מבצע) הכולל אפיון של הרשת הרלוונטית והדרך הטובה ביותר לחדור אליה. כך למשל, בדומה לפורץ שמנסה לפרוץ דלת נעולה, תחילה יש לראות את הדלת ולהבין מהו סוג המפתח הנדרש. החימוש הוא יישום של תובנות שנאספו מתוך המל״מ הספציפי שנאסף על גבי הנוזקה כדי לסייע לפורץ להתגבר על ההגנות ברשת היעד. כך למשל, אם נחזור לדוגמת הפורץ המנסה לפרוץ דלת, שלב זה יהיה מקביל להתאמת כלי הפריצה המתאימים, בהתאם למידע שנאסף בשלב האיסוף.[12] שלב ההעברה מסמן את תחילת החדירה לרשת. בשלב זה הנוזקה מוכנסת לתוך הרשת של היעד. ישנן אין ספור דרכים לבצע מהלך זה, החל מפעולת פישינג[13] וכלה בהחדרת הנוזקה באמצעות חיבור של מדיה נתיקה ליחידת קצה ברשת. שלב ניצול החולשה כולל זיהוי של פרצה באופן ניהול הרשת, שבאמצעות ניצולה ניתן להגיע ליכולת לפעול בחופשיות ברשת מבלי לעורר את חשדם של אחראי האבטחה. לאחר ניצול החולשה יש לבסס את הגישה לרשת המחשבים באמצעות הנוזקה באופן שיאפשר גישה קבועה לנוזקה ולרשת. במסגרת שלב הפיקוד והשליטה, הפורצים מקימים ערוץ תקשורת עם הנוזקה שיאפשר להם לממש את שלב ההוצאה לפועל שבו מתחילים לבצע פעולות ברשת באמצעותה. בשלב זה הנוזקה תבצע סדרת פעולות אשר בדרך כלל כוללות איסוף מידע רב וכן ביצוע מניפולציות עד כדי גרימה להשבתה מוחלטת של רכיבים מסוימים ברשת.[14] השבתה של רכיב ברשת יכולה לקרות במגוון דרכים שכולם דומים בבסיסם – הכוונה היא לגרום לרכיב לבצע פעולה שתוביל לפגיעה ברכיב עד שלא יוכל לבצע את תכליתו. באופן מקביל, פעולת סייבר מסוג איסוף תוביל לגנבה של מידע רב שהפורץ יעשה בו שימוש. קיים סיכוי משמעותי כי הפורצים יחליטו גם לפרסם את המידע באינטרנט, ואת הנעשה לא יהיה ניתן להשיב מבחינת הפגיעה העמוקה בפרטיות.

<u>אתגר הייחוס של פעולות סייבר למבצעיהן</u>

חשוב לציין כי אתגר הייחוס באינטרנט הוא אחת הסוגיות המשפטיות־מדיניות המורכבות ביותר בעיצוב דיני הסייבר. אין הסכמה בקהילה הבין־לאומית באשר לאופן שבו ניתן לייחס אחריות מובהקת וחד־משמעית לגורם החשוד בביצוע פעולת סייבר. מאחר שהרשימה מתמקדת באתגר אחר בדיני סייבר, אשר במובן מסוים הוא בסיסי יותר מאתגר הייחוס, והוא הגנה על אזרחים מפני תקיפות סייבר, ועבור הסדר הטוב, ברשימה זו אניח

---

[11] רשת – הכוונה לקבוצה של מחשבים המנוהלים באופן מרוכז.

[12] מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 191–202, 217–244 (2011); עת״ם (מנהליים ת״א) 24867-02-11 **איי.די.איי חברה לביטוח בע״מ נ׳ רשם מאגרי המידע, הרשות למשפט טכנולוגיה ומידע במשרד המשפטים** (נבו 5.8.2012).

[13] פעולת הנדסה חברתית שנועדה לגרום לנמען, ללא ידיעתו, לאפשר כניסה לרשת באמצעות חשיפה של פריטים רגישים.

[14] Yadav & Rao, *Technical Aspects of Cyber Kill Chain*, לעיל ה״ש 1.

כי לא קיים אתגר ייחוס עבור המקרים הנדונים, כך שאין שאלה הנוגעת לכך שהפעולות בוצעו ממניעים אידאולוגיים, לאומניים או דתיים או שהתוקפים נתמכו באופן ישיר על ידי גוף מדינתי.
עד כה נתנו רקע טכני על מבצעי הסייבר, בדגש על ההבחנה בין מתקפת סייבר מסוג שיבוש למתקפת סייבר מסוג איסוף. לאחר ביסוס הרקע הטכני, נעבור עתה לסקירה על הרקע הנורמטיבי של הזכות לפרטיות ולהעמקה על 3 הגישות המרכזיות בהגדרת הזכות לפרטיות שלאחריהן נוכל לדון בזכות לפרטיות במתקפת סייבר.

א.2 הזכות לפרטיות – מהי?

הזכות לפרטיות ייחודית במובן הזה שעצם הגדרתה הבסיסית ביותר, של ליבת הזכות ממש, נתון למחלוקת. ככלל, הזכות לפרטיות נוגעת לזכותו של אדם לשמור את המידע האישי שלו, חייו וכן פעולותיו מפני פרסום פומבי או התערבות חיצונית ללא הסכמתו. במקרים רבים, הזכות לפרטיות מכילה גם הגנות על דאטה ונתונים אישיים, חופש ממעקב והאוטונומיה לקבל החלטות אישיות. יחד עם זאת, קיימות פרשנויות רבות הן בחקיקה והן בספרות באשר לגבולותיה ותכולותיה המדויקים של זכות זו. כך למשל, הזכות לפרטיות המוגדרת בסעיף 12 של ההכרזה לכל באי עולם בדבר זכויות אדם מתמקדת בזכותו של האדם לחיות בחופשיות מהתערבות שרירותית וכופה.[15]
במדינת ישראל הזכות לפרטיות מעוגנת בשני חוקים מרכזיים. ראשית בחוק־יסוד: כבוד האדם וחירותו וכן בחוק הגנת הפרטיות.[16] בחוק־היסוד מוגדרת הזכות לפרטיות בסעיף 7: "(א) כל אדם זכאי לפרטיות ולצנעת חייו. (ב) אין נכנסים לרשות היחיד של אדם שלא בהסכמתו. (ג) אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו. (ד) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו." בפרק א' של החוק להגנת הפרטיות ישנה הרחבה של ההגדרה של הזכות לפרטיות וכן התמקדות הגדרת הסוגים השונים של הפגיעות האסורות בזכות זו. בפרקים הבאים החוק עוסק בשמירה על פרטיות במסגרת מאגרי מידע וכן הנחיות למסירת מידע אישי וידיעות מגופים ציבוריים. מבחינת האיזון בין הזכות לפרטיות לזכויות אחרות, הפסיקה הישראלית פירשה את חוק הגנת הפרטיות כמעניק לזכות זו מעמד חוקתי על חוקי. עוד מודגשת החשיבות של זכות זו על מנת לקיים משטר דמוקרטי. על כן, עליה להתפרש באופן נדיב ורחב, אך מדויק.[17]
ישנו מגוון רחב של תפיסות בספרות באשר לאופן המשגת ליבת הזכות לפרטיות. לדוגמה, ג'ודית ת'ומסון (Judith Thomson) מגדירה את הזכות לפרטיות בתור מקבץ של זכויות המאפשרות אוטונומיה לאדם.[18] לעומת זאת, על פי הגישה הקונטקסטואלית של הלן ניסנבאום (Helen Nissenbaum), הדגש הוא על החלוקה בין פרטי לציבורי. ניסנבאום טוענת כי עבור כל קונטקסט וסוג של סיטואציה קיימות נורמות באשר לרמת אופן מימוש הזכות לפרטיות של אדם. כך למשל, בקונטקסט רפואי חוקי הפרטיות יהיו שונים מאשר בקונטקסט חינוכי. הקונטקסט מוגדר בהתבסס על השחקנים הפועלים בו, סוג המידע ואופן העברתו. הפרה של הזכות לפרטיות מתרחשת כשמועבר מידע, מסווג, באופן או לנמען אשר לא הולם את הנורמות הקונסקטואליות המסוימות.[19]

---

[15] The Universal Declaration of Human Rights, United Nations, art 12 Dec. 10, 1948.
[16] חוק-יסוד: כבוד האדם וחירותו; חוק הגנת הפרטיות, התשמ"א–1981.
[17] ע"א 8954/11 **פלוני נ' פלונית**, פס' 67–73 לפסק הדין של השופט סולברג (נבו 24.4.2014); בג"ץ 2109/20 **בן-מאיר נ' ראש הממשלה**, פס' 35–42 לפסק הדין של הנשיאה חיות (נבו 26.4.2020).
[18] Judith Thomson, *The Right to Privacy*, 4.9 PHIL. & PUB. AFF 314–295 (1975).
[19] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004).

גישת הפרטיות כזכות אדם דוגלת בכך שהזכות לפרטיות מהווה בסיס למימוש של חירויות דמוקרטיות חשובות כמו כבוד ואוטונומיה. הפרטיות היא אמצעי עבור האדם לנהל את חייו בפרטיות ללא התערבות חיצונית לא רצויה. החשש גובר בצל ההתפתחות הטכנולוגית, והאפשרויות למעקב ופיקוח מדינתי רוחבי גדלות ומשתכללות. ג׳פרי רוזן (Jeffery Rosen), אחד ממובילי גישה זו, קורא להתאמה של מחסומים משפטיים שנועדו לשמר את הזכות לפרטיות כזכות אדם בסיסית.[20] באופן מקביל, על פי התפיסה שמציע דניאל סולוב (Daniel Solove), אשר מכונה ״ארכיטקטורת פרטיות״, מערכות תקשורת ואינפורמציה מודרנית מייצרות אתגרי פרטיות חדשים. במקום לראות את הפרטיות כאפשרות של שליטה או הסכמה מצד אינדיבידואל מסוים, לדידו של סולוב הפרות של פרטיות נובעות מכשלים במערכות ומקור התיקון הוא מוסדי. כשלים אלו כוללים למשל פרופיילינג, מעקב מדינתי ופריצות למאגרי מידע.[21]

שלוש הגישות המרכזיות אשר נדון בהן במסגרת מאמר זה הן: פרטיות כשליטה, פרטיות כגישה והזכות להיעזב במנוחה. להלן ניתן סקירה קצרה על כל אחת מגישות אלה:

1. פרטיות כשליטה

גישת הפרטיות כשליטה מתמקדת בתפיסה שפרטיות בבסיסה היא היכולת של אדם לשלוט במידע הפרטי שלו ולהחליט עם מי, באילו סיטואציות ועבור אילו מטרות לשתף אותו עם אחרים. על כן, פרטיות היא לא רק היעדר התערבות, אלא זכות דינמית הכוללת כמה מרכיבים מרכזיים. ראשית, שליטה על שיתוף מידע, מבחינת היקף, פורום ונמענים. שנית, הבחירה לשתף מידע ופרטים אישיים נתונה בידי האדם. על כן, ברשותה הסמכות לחשוף חלקים או אלמנטים מתוך חייה הפרטיים. שלישית, הסכמה מהווה נדבך משמעותי של תפיסת הפרטיות כשליטה. לכל אישה צריכה להיות ההזדמנות לתת או לסרב להסכים לשיתוף מידע או פרטים אישיים. הדגש המשמעותי הוא על היכולת לסרב לספק מידע. גישה זו מחזקת את האוטונומיה של האדם. זאת אומרת ביכולתה של אישה להחליט, בכל אינטראקצייה, באמצעות איזה מידע לחשוף פרטים אישיים.[22]

2. פרטיות כגישה

תפיסת הפרטיות כגישה (access), אשר אותה הובילה רות גביזון, מתמקדת ביכולת של אדם להגביל את הגישה אליו, אל המרחב האישי שלו ואל המידע האישי. על כן, במסגרת תפיסה זו הדגש הוא על היכולת של אדם להגביל או לחסום לחלוטין מאחרים גישה לספרה הפרטית שלו. היכולת למנוע פלישה של זרים כוללת כמה נדבכים. קודם כול, גישה פיזית – הסמכות למנוע מאחרים לחדור למרחב הפרטי שכולל את מקום המגורים, מקום העבודה (במובנים מסוימים) ועוד. בנוסף, האפשרות למנוע מזרים גישה לאמצעי התקשורת ואגירת המידע של אדם היא נדבך משמעותי של פרטיות כגישה. לבסוף, פרטיות כגישה היא האפשרות להשאיר אחרים מחוץ לחיים הפיזיים והדיגיטליים של אדם. הייעוד הוא לשמר את האוטונומיה של האדם על ידי ויסות הגישה אל החיים הפיזיים והדיגיטליים המדוברים.[23]

3. הזכות להיעזב במנוחה

הזכות להיעזב במנוחה היא אחת הגישות הראשונות והיסודיות ביותר של היישום של הזכות לפרטיות. לתפיסה זו יש כמה עקרונות. ראשית, חופש מהתערבות לא רצויה – הכוונה היא לאפשר לאנשים לחיות ללא התערבות לא נדרשת ולא רצויה של אחרים, בין אם מדובר בממשלה, בתקשורת או באנשים פרטיים. שנית, יסוד של רעיון

---

[20] JULIE E. COHEN, PRIVACY, IDEOLOGY, AND TECHNOLOGY: A RESPONSE TO JEFFREY ROSEN (2001).

[21] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. (2003).

[22] Julie E. Cohen, *What Privacy is For*, 126.7 HARV. L. REV. 1940–33 (2013); Andrei Marmor, *What Is the Right to Privacy?*, 43 PHIL. & PUB. AFF. 3 (2015).

[23] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421–7 (1980).

המרחב הפרטי והאישי וקידושו. מרחב זה חולש על הממד הפיזי והמנטלי ובשנים האחרונות גם הדיגיטלי. שלישית, אוטונומיה על החלטות אישיות. הכוונה היא לאפשר לאדם את האוטונומיה לקבל החלטות אישיות באשר לאורח חיים, הקשרים הבין־אישיים ועניינו הפרטיים ללא התערבות או כפייה של כוחות וגורמים חיצוניים.[24]

א.3 פגיעה בפרטיות בפעולות סייבר

זיהוי הנקודה הסינגולרית במהלך פעולת סייבר אשר מובילה לפגיעה (או פגיעות) בפרטיות הוא שאלה מורכבת הן בפן המשפטי והן בפן העובדתי. סוגיה זו לא נדונה באופן מפורש בספרות או הוכרעה במפורש בפסיקה. יחד עם זאת, מתוך הגישות התאורטיות השונות לפרטיות וכן הפסיקה הקיימת בנושא, ניתן להצביע על השלבים בפעולת הסייבר שעלולים לייצר פגיעה מסוג זה.[25] תחילה אסביר כיצד יכולה להיגרם פגיעה בפרטיות בפעולת סייבר, ולאחר מכן אסקור את ההתייחסות לפגיעה מסוג זה בפסיקה המצומצמת ובספרות.

<u>איך במסגרת פעולת סייבר יכולה להיגרם פגיעה בפרטיות</u>?

הן בפעולות סייבר מסוג שיבוש והן בפעולות סייבר מסוג איסוף קיים סיכון לפגיעה בפרטיות, מאחר שמדובר בגורם זר המשיג גישה לרשת ולכל המידע השמור על גבי רכיביה. פגיעה בפרטיות הייחודית לפעולת סייבר יכולה לקרות החל מרגע החדירה לרשת, משלב ההעברה והלאה. הפגיעה בפרטיות נגרמת כתוצאה מכך שלרשות הפורצים עומד מידע אישי רב אשר במובהק אינו ציבורי. סיכון זה לא נגמר אחרי שהפורצים עוזבים את הרשת מאחר שברשותם המידע האישי הגנוב. הפגיעה יכולה להיות מוגברת אם הפורצים יחליטו לפרסם את המידע. על כן, כל פרסום או שימוש במידע שהושג מתוך הרשת של היעד יהיה מבוסס על מידע שהושג מתוך הרשת אחרי היציאה ממנה.

באשר למושא הפגיעה, נבחין בין צד ב׳, בעל המחשב או הרשת, לבין צד ג׳, כל גורם שמידע על אודותיו שמור ברשת. תקיפה של מחשב ביתי תוביל בעיקרה לפגיעה בצד ב׳; לעומת זאת פריצה למאגר הלקוחות של חברה תהיה בעיקרה פגיעה בצד ג׳, הלקוחות עצמם.

<u>בראי הפסיקה</u>

התופעה של פעולות סייבר הולכת ומתרחבת, ולכן בשנים האחרונות ישנה מגמה של תביעות רשלנות כנגד מושאי תקיפות סייבר; חברות פרטיות וגופים ממשלתיים.[26] התביעות ברובן מתמקדות במחדל של החברות על כך שלא הגנו על רשתותיהן ומאגרי המידע שברשותן ובכך הפרו את חובתן להגן על המידע של לקוחותיהן. בשל הקושי בייחוס פעולת הסייבר לגורם מסוים ולזהותו, מעטים הם המקרים שבהם התוקף עצמו זוהה ונתבע, ומושאי תקיפות הסייבר הן התובעות. לכן קיימת פסיקה מצומצמת העוסקת בתביעות כנגד גורמים המואשמים בביצוע פעולות סייבר בכלל ותביעות הדנות בזיהוי השלב המדויק בפעולת סייבר שממנה נולדת הפגיעה בפרטיות הנפגעים בפרט. תביעות אלו התנהלו בעיקר בבתי משפט השלום, ולכן גם הפסיקות שהתקבלו אינן מעידות על

---

[24] Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 220–193 (1890).

[25] להרחבה ראו: שם, בפרק א.2.

[26] ליטל דוברוביקצי ״פשרה בפרשת פריצת הסייבר לשירביט: הראל תשלם פיצויים של 4.8 מיליון שקל״ **כלכליסט** (2.7.2023) https://www.calcalist.co.il/local_news/article/rketdjrd3; שירה יום טוב ״תביעת ענק נגד אפליקציית אטרף: זה הסכום שהמשתמשים דורשים״ **ICE** (4.11.2021) https://www.ice.co.il/law/news/article/834375;
Megan Kardona, *Frontier Communications hit with class action suit in Texas after massive data breach*, KERA NEWS (July 13, 2024, at 5:00 ET), https://www.keranews.org/government/2024-06-13/frontier-communications-hit-with-class-action-suit-in-texas-after-massive-data-breach; Ben Kesslen, The massive car dealership cyberattack already has lawsuits flying, **Quartz** (25.6.2024).

גיבוש של הלכה מחייבת בנושא. אתגר הייחוס גם הוא מקשה על גיבוש בסיס ראייתי על מנת להביא לכדי כתב אישום כנגד חשוד בביצוע פעולת סייבר מסוג איסוף. חרף זאת, ישנם כמה מקרים שבהם התוקפים כן זוהו ובית המשפט קבע כי, בין השאר, נגרמה פגיעה בפרטיות.[27]

בעניין קוריאה מוטורס נערך דיון באשר לשאלה האם עצם החדירה לרשת יכול בפני עצמו להיחשב פגיעה בפרטיות. בהכרעה נכתב כי "הנתבעים ידעו והיו צריכים לדעת שבכל תיבת דוא"ל, קיימת התכתבות פרטית, גם אם היא כרוכה בעסקים או נכתבה מתיבת דוא"ל עסקית. כל חדירה לתיבת דוא"ל היא פגיעה בפרטיות וכפועל יוצא הפגיעה נעשתה בחוסר תום לב ועל מנת להתחקות אחר התנהלות יאנג ואונגר. מדובר בעניינם הפרטי, כולל אסטרטגיות פרטיות, פגישות פרטיות, עניינים אישיים של אדם וכיוצ"ב שאינם נחלת הכלל."[28] לפיכך, ניתן להסיק כי עצם החדירה לרשת והנוכחות של גורם לא מורשה בתיבת הדואר של אדם עולה כדי פגיעה בפרטיות. על כן, הפעולה של החדירה, ועצם השהות ברשת ללא אישור, עולה כדי פגיעה בפרטיות.

יתרה מזו, בעניין פלוני,[29] שבו שני קטינים הורשעו בהקמה וניהול של אתר המציע שירותי תקיפה והשבתה של אתרי אינטרנט, באמצעות מתקפות DDOS,[30] מכלל הלאו אתה שומע הן – העובדה שהקטינים לא הורשעו בפגיעה בפרטיות בגין התקיפות שביצעו יכולה לנבוע מכך שתקיפות מסוג DDOS כלל אינן כוללות חדירה לרשת או למאגר המידע הנתקף, אלא מבוצעות מחוץ לרשת. על כן, ייתכן כי ניתן להסיק כי נדרשת חדירה לרשת במסגרת פעולת סייבר על מנת שהיא תעלה כדי פגיעה בפרטיות.

בעניין שלום ביליק, שהורשע בהפצה ללא אישור של מאגר הנתונים "אגרון" שהועתק מהרשת של משרד הפנים ומכיל פרטים אישיים של עשרות אלפי אזרחים, נקבע כי עצם פרסום של מידע פרטי, שהושג באופן לא חוקי באמצעות פעולת סייבר, עולה לכדי פגיעה בפרטיות.[31] זאת חרף העובדה כי ביליק הפיץ את המידע בלבד, ולא ביצע את פעולת הסייבר הבלתי חוקית על מנת להשיג את המאגר מלכתחילה.

<u>בראי הספרות</u>

לטובת הניתוח של הפגיעה בפרטיות, אציע סידור חדש המציג את הסכמה של הוצאה לפועל של פעולת סייבר:

1. טרום חדירה לרשת

פעולות המבוצעות ללא נגישות למידע אישי השמור בתוך הרשת כלל לא נחשבות לפעולות סייבר, אלא עולות כדי פגיעות בפרטיות "סטנדרטיות".

---

[27] פסקי דין כנגד העוסקים בגורמים המואשמים בביצוע של פעולות סייבר: ת"א (מחוזי ת"א) 8781-07-13 **קוריאה מוטורס ישראל בע"מ נ' אונגר** (נבו 10.3.2021); ת"פ (שלום ת"א) 19578-11-14 **מדינת ישראל נ' פלוני** (נבו 20.3.2016); ת"פ (מחוזי ת"א) 20098-06-16 **מדינת ישראל נ' מסארווה** (נבו 15.1.2017); ת"פ (שלום כ"ס) 16419-08-17 **מדינת ישראל נ' פלוני** (נבו 13.5.2020) (להלן: פרשת **פלוני**); ע"פ (שלום ת"א) 24441-05-12 **מדינת ישראל נ' ביליק** (נבו 5.6.2016); ע"ח (מחוזי ת"א) 25897-01-20 **עמותת ועשית הטוב והישר נ' נוה** (נבו 27.1.2020).

[28] ת"א (מחוזי ת"א) 8781-07-13 **קוריאה מוטורס ישראל בע"מ נ' אונגר**, פס' 236–237 לפסק הדין של השופטת צילה צפת (נבו 10.3.2021). דיון דומה התקיים גם בעניין ת"פ (שלום ת"א) 19578-11-14 **מדינת ישראל נ' פלוני** (נבו 20.3.2016).

[29] פרשת **פלוני**, לעיל ה"ש 27.

[30] distributed denial of service – DDOS. להרחבה על תקיפות שיבוש מסוג DDOS ראו: Christos Douligeris & Aikaterini Mitrokotsa, *DDoS Attacks and Defence Mechanisms: Classification and State-of-the-Art*, 44.5 COMP. NETS., 666–643 (2004).

[31] פרשת **ביליק**, לעיל ה"ש 27.

2. חדירה לרשת

אין עוררין על כך שכניסה לרשת היא פגיעה בפרטיות של צד ב׳, בדומה לפגיעה הנגרמת כתוצאה מחדירה פיזית למרחבו האישי של אדם אליבא דוויליאם פרוסר (William Prosser) – intrusion upon seclusion.[32] באשר לפגיעה בפרטיותו של צד ג׳, מצב הדברים פחות ברור.

גישת הפרטיות כשליטה מעמידה במרכז את היכולת של האדם לשלוט במידע על אודותיו והסכמתו, או התנגדותו, להעברתו לאחרים. השליטה היא ביטוי לאוטונומיה של האדם ונגזרת מזכותו לכבוד.[33] התוקף פועל ברשת מתוקף כך שהצליח להשיג עליונות טכנולוגית־תפעולית כלשהי ברשת. עצם הימצאותו ברשת מחליש את השליטה שיש לצד ב׳, אשר הוסמך לשמור על המידע עבור צד ג׳. אי לכך, החדירה לרשת מובילה לכך ששליטתו של צד ב׳ במידע נחלשת, ומאחר שהוא שליחו של צד ג׳, יש בכך לגרום לפגיעה בפרטיותו של צד ג׳ לאור ההתרופפות בשמירה על המידע שלו על ידי צד ב׳. מהותה של תפיסת הפרטיות כגישה היא שהפרטיות נאמדת על פי הגישה (access) של אחרים לאדם או למידע על אודותיו. ככל שהאדם יכול להיות פחות נגיש לחברה, פרטיותו נשמרת.[34] בראי סוגייתנו, תפיסה זו דומה לתפיסת הפרטיות כשליטה בכך שתתפוס את החדירה לרשת כפגיעה בפרטיותו של צד ג׳. זאת מאחר שמעגל הגורמים הנגישים למידע על אודותיו התרחב ובכך סודותיו, אחד המרכיבים של הזכות לפרטיות, חשופים.[35] לעומת זאת, על פי התפיסה של וורן וברנדייס (Warren & Brandeis), הממשיגה את הפרטיות בתור הזכות להיעזב במנוחה,[36] הנגישות של גורמים לא מורשים למאגר נתוני לקוחות אינה מחייבת פגיעה בזכות של הלקוחות לפרטיות. בנוסף, יש לאמוד זאת על פי הפעולות הבאות שיבצעו הגורמים.

3. פעולה בתוך הרשת

על פי חוק הגנת הפרטיות, עצם ההעתקה של תוכן ללא רשות נתפס כפגיעה בפרטיות.[37] לפיכך, האקרים שמטרתם לאסוף מידע ברשת גורמים לפגיעה בפרטיות באופן מנותק מהמטרה שלשמה המידע נאסף. על פי גישות פרטיות כגישה ושליטה, עצם העתקת המידע, בעודו נמצא בתוך הרשת, מהווה המשך ישיר של הפגיעה בפרטיות הנובעת מהחדירה לרשת, ואינו עומדת בפני עצמו.[38] לעומת זאת, על פי תפיסתם של וורן וברנדייס, ביצוע פעולות בילוש הכוללות האזנת סתר או קריאה של טקסט פרטי וכן העתקת המידע האישי של צד ג׳ הם הפעולות אשר מפירות את הזכות שלה להיעזב במנוחה.[39] מנגד, פעולת השיבוש, שלא כוללת העתקת תוכן, לא תייצר פגיעה חדשה בפרטיות מעבר לחדירה לרשת עצמה, על פי גישות הפרטיות כשליטה וכגישה.[40]

---

[32] בירנהק **מרחב פרטי**, לעיל ה״ש 12, בעמ׳ 57–88; William Prosser, *Privacy,* 48 CAL. L. REV. 383, 423–383 (1960).

[33] מיכאל בירנהק ״שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות״ **משפט וממשל** יא 9, 41–45 (תשס״ח).

[34] Ruth Gavison, *Privacy and the Limits of Law*, לעיל ה״ש 23.

[35] רות גביזון ״הזכות לפרטיות ולכבוד״ **זכויות אדם בישראל – קובץ מאמרים לזכרו של חמן שלח** 61 (רות גביזון עורכת 1989); בירנהק ״שליטה והסכמה״, לעיל ה״ש 33 בעמ׳ 40.

[36] Warren Samuel D. & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 220–193 (1890).

[37] ס׳ 2(5) לחוק הגנת הפרטיות, התשמ״א–1981.

[38] Julie Cohen, *What Privacy is For*, לעיל ה״ש 22; Andrei Marmor, *What Is the Right to Privacy?*, לעיל ה״ש 22.

[39] ס׳ 2(1), 17 לחוק הגנת הפרטיות; תקנות הגנת הפרטיות (אבטחת מידע), התשע״ז–2017.

[40] ״דיווח: מתקפת הסייבר האיראנית נועדה להעלות את רמת הכלור במים בישראל״, לעיל ה״ש 4; KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2014); Bergman & Halbfinger, *Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks*, לעיל ה״ש 5.

4. פעולה מחוץ לרשת

שלב זה קיים בשימוש במידע לאחר סיום פעולת הסייבר ויציאה מהרשת, זאת אומרת שימוש ופרסום של מידע פרטי שהושג שלא כדין או שהושג כדין אך עבור מטרה שונה, לרבות עבור פרסומו, מכירתו או הנגשתו לציבור כולו או לחלקים ממנו. מסתמן כי מדובר בפגיעה בפרטיות של צד ג׳ על פי שלוש התפיסות של פרטיות שמניתי: פרטיות כגישה, כשליטה, ובתור הזכות להיעזב במנוחה.[41] שימוש במידע הוא התכלית של ביצוע פעולות איסוף בסייבר. זאת בשונה ממטרתה של פעולת שיבוש שנועדה להשבית או לפגוע במערכת, וכשהתוקפים יוצאים מהרשת, הפגיעה בפרטיות מסתיימת.

בתת־פרק זה ניסינו לזהות ולהגדיר את נקודות הזמן במסגרת ההוצאה לפועל של תקיפת סייבר אשר עלולות להוביל לפגיעה בפרטיות. ניתן לסכם כי הכניסה לרשת היא פגיעה בפרטיות לפי כל הגישות. לכן יש בסיס לטעון שכל פעולת סייבר, שבשורשה יש חדירה של גורם לא מורשה לרשת, גורמת לפגיעה בפרטיות, הן של צד ב׳ והן של צד ג׳. עם זאת, בניתוח יותר מדויק נראה שבפעולות איסוף ישנה פגיעה נוספת הן בשלב הפעולה בתוך הרשת והן בשלב של שימוש במידע מחוץ לרשת, אשר לא קיימת בפעולות מסוג שיבוש. לכן, בפעולות איסוף, שייעודן שימוש במידע אישי ללא רשות, הפרת הפרטיות היא משולשת והיא הנזק המרכזי, בעוד בפעולות שיבוש הפגיעה בפרטיות היא תוצר לוואי בלבד.

ב. פעולות סייבר בראי חוק המאבק בטרור

ב.1 מעשה טרור במשפט הישראלי

לחקיקתו של חוק המאבק בטרור בשנת 2016 ישנן שתי תכליות בלשון החוק וכן בדברי ההסבר. ראשית, מניעת הקמתם, קיומם ופעילותם של ארגוני טרור, ושנית, סיכול פעולות טרור.[42] הטרור הוא אויב רב־פנים, ופעילי טרור משתמשים במגוון אמצעים, פלטפורמות ודרכי פעולה. החוק עוצב כך שהוא נותן בידי המדינה את הכלים להתמודד עם איום הטרור תוך איזון עם מחויבותה לשמירה על זכויות אדם וערכי הדמוקרטיה.[43] בהקשר זה יפים דבריו של נשיא בית המשפט העליון (בדימוס) אהרן ברק: ״האיזון הראוי בין הביטחון לחירות הוא פרי עמדה ברורה המכירה בחיוניותו של הביטחון ובנחיצותן של זכויות אדם״.[44]

הרקע לחקיקה של חוק המאבק בטרור הוא הרצון להסדיר את מגוון המקורות של דברי החקיקה והתקנות בנושא. החוק נועד להיות מותאם למציאות המורכבת של השנים שקדמו לחקיקתו, ואשר במידה רבה ממשיכה עד היום, ולהעניק כלים ליצירת ודאות תוך התמודדות אפקטיבית ומידתית עם גל הטרור שהתרחש בשנה שקדמה לחקיקתו. מנגד עלו קולות על היעדר המידתיות של החוק ועל הצורך לדייק ביתר שאת בהגדרת הכוח הכופה שהמדינה יכולה להפעיל על מנת להתמודד עם תופעות של טרור.[45]

---

[41] ס׳ 6(א)(6) לחוק המחשבים, התשנ״ה–1995; ס׳ 2(9), 2(10) לחוק הגנת הפרטיות.

[42] ס׳ 1 לחוק המאבק בטרור, התשע״ו–2016.

[43] דברי הסבר להצעת חוק המאבק בטרור, התשע״א–2011, ה״ח 611, 1408.

[44] אהרן ברק ״שפיטה, דמוקרטיה וטרור״ **מנשה שאוה: מחקרים במשפט לזכרו** 43, 48–51 (2006).

[45] טל שלו ״רק בהרתעה ננצח את הטרור״ הכנסת אישרה את חוק הטרור״ **וואלה** (15.6.2016) https://news.walla.co.il/item/2970430; יהונתן ליס ״ביקורת על חוק הטרור: כמעט בלתי אפשרי להתגונן בפניו״ **הארץ** (7.6.2013) https://www.haaretz.co.il/news/politics/2013-06-07/ty-article/0000017f-e86c-dc7e-adff-f8edd7250000

על מנת שפעולה תיחשב כמעשה טרור, על פי חוק זה, היא צריכה לעמוד בשלושה תנאים מצטברים: (1) הפעולה נעשתה ממניע אידאולוגי, דתי, לאומני או מדיני; (2) המעשה נועד על מנת לעורר פחד בציבור, או להשפיע על רשות ממשלתית, מעשיית או הימנעות מעשיית מעשה; (3) המעשה או אי־עשייתו גרמו, או היה סיכון ממשי לכך שיגרמו, לפגיעה פיזית חמורה לאדם או לחירותו, לביטחון המדינה או הציבור, לרכוש, לקודשי דת או לשירותים חיוניים.[46] נציין כי הגדרה זו של מעשה טרור היא אימוץ, לצד שכלול, של פרשנות הפסיקה את גלגוליו הקודמים של החוק,[47] ובעלת מאפיינים דומים להגדרות משפטיות של טרור במדינות שונות בעולם.[48]

בדברי ההסבר של התיקון הודגש שהתנאי הראשון מתייחס למניע לפעולה, ולא למעשה עצמו, מה שמרחיב את התנאי.[49] על המניע האידאולוגי ניתן ללמוד לא רק מהכוונה לזרוע פחד, אלא גם מהרקע של הפעולה, המבצע והמעשים עצמם.[62] הודגש בדברי ההסבר שעל מנת שהתנאי הראשון והשני יתממשו, אין דרישה שהמניע, בין אם הוא אידאולוגי, דתי, לאומני או גזעני, או הייעוד של הפעולה, לעורר פחד ובהלה בציבור, יהיו הבלעדיים.[48] במקרה שבו ניתן לזהות כמה מניעים או תכליות, בנוסף לאלו העומדים בתנאי החוק, הפעולה עדיין תיחשב למעשה טרור. לפיכך, ניתן לגזור שהרכיבים בחוק שעוסקים במטרת הפעולה (התנאי הראשון) ובממדי ההשפעה (התנאי השני) הם הדומיננטיים מבין תנאי החוק, ולכן יש לפרש את סעיף הנזק לאורם (התנאי השלישי).[50]

התנאי השלישי עוסק בדרישת הנזק. בהגדרה של מעשה טרור מנויים שלושה סוגי נזק.[51] הראשון הוא נזק פיזי הכולל פגיעה חמורה בגופו של אדם, בבטיחות הציבור או ברכוש, אשר מוביל לנזק חמור לאדם או לציבור. הסוג השני הוא פגיעה בקודשי דת והסוג האחרון הוא פגיעה חמורה בתשתיות קריטיות. אם מעשה מוביל לאחד, או יותר, מהנזקים הללו, או גורם לסיכון ממשי להתממשות אחד מהם, הוא עומד בתנאי השלישי של הגדרת מעשה טרור.

בחלק זה דנו בצורה מעמיקה בחוק המאבק בטרור. תחילה עסקנו בתכליות החוק ולאחר מכן הצגנו וניתחנו את ההגדרה של מעשה טרור כפי שנקבע בחוק המאבק בטרור וכן התנאים המצטברים הנדרשים על מנת לסווג פעולה כמעשה טרור. בחלק הבא נתמקד בתנאי השלישי בתור התנאי המבחין בין פעולת סייבר מסוג שיבוש לפעולת סייבר הגורמת "רק" לפגיעה בפרטיות.

ב.2 סוגי הנזק המנויים בהגדרה של מעשה טרור

בחלק זה יוצגו גבולות ההגדרה של סעיף הנזק, התנאי השלישי והאחרון שנדרש כדי שפעולה תסווג בתור מעשה טרור. אבאר את סוגי הנזק הנכללים בדרישת הנזק בהגדרת החוק הישראלי למעשה טרור. יתבהר במהלך הפרק כי הנזק הנכלל בהגדרה של מעשה טרור הוא פגיעה חמורה בגופו של אדם, חירותו או רכושו, ולכן מדובר בהגדרה בעלת מאפיינים פיזיים מובהקים. באשר לפגיעה בבטיחות הציבור או תשתית חיונית, האומדן הוא לא נזק פיזי, אך במקרים אלה רף החומרה הוא גבוה.

---

[46] ס' 2 לחוק המאבק בטרור.

[47] חוק איסור מימון טרור, התשס"ה–2005; פקודת מניעת טרור, התש"ח–1948, אשר בוטלו בהמשך; ע"פ 3793/18 **פלוני נ' מדינת ישראל** פס' 11, 37 לפסק הדין של השופט מזוז (נבו 3.5.2020) (להלן: פרשת **פלוני נ' מדינת ישראל**).

[48] דברי ההסבר להצעת החוק, לעיל ה"ש 43, בעמ' 1413; Criminal Code, C-46, R.S.C. 1985, 83.01; Terrorism Act 2000, c. 11, s 1(102).1 (Austl.) *Criminal Code 1995* (Cth); 5(3).

[49] דברי הסבר להצעת חוק המאבק בטרור, התשע"ה–2015, ה"ח הממשלה 1066, 1066.

[50] ס' 2(א)(3)(ג)(2)(ג)(3)(ד) לחוק המאבק בטרור. כלומר, סייג ד להגדרת "מעשה טרור".

[51] ס' 2 לחוק המאבק בטרור.

<u>פגיעה חמורה בגופו של אדם או בחירותו</u>

יש להבחין בין שני החלקים של הגדרה זו. הרישא עוסקת בפגיעה פיזית חמורה הנגרמת לגופו של אדם, ואילו הסיפא עוסקת בפגיעה ממשית בחירותו. אתייחס לשני החלקים בנפרד. למרות שלא הוגדר רף מינימלי לפגיעה פיזית חמורה בגופו של אדם בפסיקה, ניתן להסיק ממנה שפגיעה חמורה היא כזו שעשויה להוביל לסיכון חיים או פגיעה בלתי הפיכה לנפגע.[52] פגיעה בגוף היא דרישת הנזק האינטואיטיבית ביותר עבור עמידה בהגדרה של מעשה טרור, אותה קל להסביר ולהגדיר באופן יחסי.

על מנת להבין מה נחשב לפגיעה ממשית בחירותו של אדם אפנה לחקיקה ולפסיקה, שמהן ניתן להסיק שתי פרשנויות אפשריות. הפרשנות המרכזית היא ששלילת חירותו של אדם היא הגבלת האדם באמצעות כליאתו או מאסרו, כפי שמוגדר בסעיף 5 לחוק־יסוד: כבוד האדם וחירותו.[53] אין בפסיקה מקרה שבו עבירה סווגה כמעשה טרור על בסיס פגיעה חמורה בחירותו של אדם. יחד עם זאת, בפסיקה אוששה הפרשנות שפגיעה חמורה בחירותו של אדם היא כליאתו.[54] פרשנות זו מתיישבת גם עם דיני זכויות אדם במשפט הבין־לאומי. סעיף 9 לאמנה הבין־לאומית בדבר זכויות פוליטיות ואזרחיות קובע זכות אוניברסלית לחירות (liberty) וביטחון אשר באה לידי ביטוי באיסור על מעצר או כליאה של אדם באופן שרירותי או ללא הסמכה בחוק.[55]

פרשנות אחרת לפגיעה חמורה בחירותו של האדם היא כפייה, כלומר שלילה מרחיבה של כוחו המשפטי של אדם, במסגרת המשפט הציבורי, באמצעות פסילת כשרות משפטית, או הפרטי, באמצעות כפייה חוזית.[56] אחד מהעקרונות של אפוטרופסות, כפי שמוגדר בחוק הכשרות המשפטית והאפוטרופסות, הוא שיש לשמור על כבודו של האדם בדרך שתגביל את זכויותיו וחירותו במידה הפחותה ביותר.[57] ניתן להסיק מכך שפגיעה חמורה בחירותו של אדם היא שלילה משמעותית של זכויותיו המשפטיות הבסיסיות באמצעות כפיית מימוש חוזה או אפוטרופסות המותירות את האדם ללא יכולת לשלוט על חייו. פרשנות זו נסמכת על אחד משניים: קיום של קשר חוזי בין המפגע לבין הקורבן או התבססות על כוח כפייה מדינתי על מנת להוציא לפועל את מעשה הטרור, מה שלא מתקיים במקרה של פעולות הסייבר.

לפיכך, מהסמיכות לרישא העוסקת בפגיעה פיזית חמורה, ניתן לשער כי כוונת המחוקק הייתה לפגיעה בחירות אשר יש בה אלמנט פיזי. לכן סביר להניח כי פרשנות של פגיעה בחירותו של אדם במסגרת דרישת הנזק במעשה טרור היא חטיפה או ניסיון חטיפה של אדם.

<u>פגיעה חמורה בבטיחות הציבור או בבריאותו</u>

---

[52] פרשת **פלוני נ' מדינת ישראל**, לעיל ה"ש 47, בפס' 38 לפסק הדין של השופט מזוז; שם, בעמ' 13 "מה שנראה כמו טרור ועושה פעולת טרור אז זה טרור"; אסף הרדוף **הפשע המקוון**, 31–94 (2010); David E. Graham, *Cyber Threats and the Law of War*, 4 J. OF NATIONAL SEC. L. & POLICY 87, 87 (2010); J. A. GREEN, CYBER WARFARE: A MULTIDISCIPLINARY ANALYSISch. 3 (2015).

[53] ס' 5 לחוק-יסוד: כבוד האדם וחירותו.

[54] ע"פ 5338/17 **אבוטבול נ' פיליפ** (נבו 1.11.2018); בש"פ 5312/00 **מזרחי נ' מדינת ישראל** (נבו 9.8.2000); ת"צ (מחוזי חי') 58915-03-17 **דראושה נ' צ'מפיון מוטורס בע"מ** (נבו 29.9.2020); עפ"ת (מחוזי י-ם) 38497-04-18 **ענים נ' מדינת ישראל** (נבו 15.5.2018).

[55] International Covenant on Civil and Political Rights, art. 9, Dec. 16, 1966, 999 U.N.Doc. 171.

[56] ע"א 5587/93 **דניאל נחמני נ' רותי נחמני**, מט(1) 485 (12.9.1996); ת"א (שלום ת"א) 53189-04-15 **אברהם (אברימי) ישעיהו ליזרוביץ נ' אלחנן (חנן) רפאל ליזרוביץ**, פס' 48 לפסק הדין של השופט גיא הימן (נבו 29.4.2020).

[57] ס' 67ה(א)(1) לחוק הכשרות המשפטית והאפוטרופסות, התשכ"ב–1962.

בדברי ההסבר של חוק המאבק בטרור, וכן בגלגול הקודם של החוק, חוק איסור מימון טרור, אין התייחסות ספציפית למה ייחשב כפגיעה בבטיחות הציבור. עולה מהפסיקה כי כל פעולה או התנהגות שנועדו לזרוע פחד, חרדה וטרור בלבבות הציבור עולה כדי פגיעה מסוימת בבטיחות הציבור.[58]

<u>פגיעה חמורה ברכוש</u>

על פי חוק המאבק בטרור, פגיעה חמורה ברכוש תעמוד בדרישת הנזק אם בנסיבות ביצועה הייתה אפשרות ממשית שתוביל לפגיעה חמורה בגופו של אדם או לחירותו או לחלופין לפגיעה בביטחון או בבריאות הציבור. לכן לא אתייחס לקטגוריה זו בנפרד, אלא כשלב מקדים או מאפשר עבור שתי הקטגוריות האמורות.

<u>פגיעה בתשתיות, במערכות ובשירותים חיוניים או פגיעה בכלכלת המדינה</u>

סוג פגיעה זה כולל שני אלמנטים: הראשון הוא פגיעה בתשתיות או מערכות חיוניות והשני הוא פגיעה בכלכלת המדינה. מדברי ההסבר לחוק עולה כי ההרחבה לפגיעה בכלכלת המדינה כך שתכלול פגיעה גם אם אינה בעלת השפעה מיידית וישירה על הציבור תתאפשר אם היקף הנזק שנגרם עלול להיות חמור ביותר.[59] גישה זו מהדהדת רכיבים דומים בפסיקה הבין־לאומית העוסקת בהגדרת עבירות טרור.[60]

<u>רף החומרה</u>

על מנת לאמוד את חומרת הפגיעה בבטיחות הציבור, בתשתיות קריטיות או בכלכלת המדינה עוצב בפסיקה מבחן הסכנה החמורה והמיידית לאזרחי המדינה ותושביה או לסדרי השלטון שלה. מבחן זה מורכב משני רבדים, הראשון מהותי והשני כרונולוגי. ברובד המהותי נדרש רף גבוה של סכנה לאזרחי המדינה ותושביה. הכוונה היא לא בהכרח לאיום קיומי, אך איומים שגרתיים שעימם מתמודדות המשטרה ורשויות האכיפה מדי יום הם מתחת לרף החומרה. באשר לרובד הזמן, נדרש חשש להתממשות הסכנה באופן מיידי.[61] הדרישה המחמירה נועדה על מנת שלא להרחיב יתר על המידה את ההגדרה של מעשה טרור.

הדיון ברשימה זו עוסק בתקיפת סייבר גנרית, כשמושא היעד אינו ספציפי. לכן לצורך הדיון, פגיעה בבריאות הציבור תיחשב למקרה פרטי של פגיעה בבטיחות הציבור וכן פגיעה בקודשי דת תיחשב כמקרה פרטי של פגיעה בתשתיות ושירותים חיוניים.

לסיכום, בניתוח של סוגי הנזק הנכללים בהגדרה של מעשה טרור עולה כי פגיעה חמורה בגופו של אדם, חירותו או רכושו היא בעלת מאפיינים של נזק פיזי. באשר לפגיעה בבטיחות הציבור (ובבריאותו) וכן במערכת או תשתית חיונית, לא נדרשת פגיעה פיזית, אך כפי שהוצג לעיל, רף החומרה לעמידה בדרישת הנזק הוא גבוה.

ב.3 סיווג פעולות סייבר כמעשה טרור בהתבסס על סוג הנזק

תחילה נציין כי שאלת הסיווג של פעולה כמעשה טרור כמעט ולא עלתה בפסיקה הישראלית. ברוב מוחלט של המקרים בית המשפט לא עסק בשאלה זו מאחר שלא הייתה שאלה עובדתית או משפטית האם העבירה נשוא

---

[58] ע"פ 5536/18 **עמאר אלבייאע נ' מדינת ישראל**, פס' 27 לפסק הדין של השופט אלרון (נבו 13.6.2019).

[59] דברי הסבר להצעת חוק המאבק בטרור, 1415.

[60] Draft Comprehensive Convention on International Terrorism, Aug. 28, 2000 art. 2(1)(b), U.N.Doc. A/59/894.

[61] בג"ץ 2109/20 **עו"ד שחר בן מאיר נ' ראש הממשלה**, פס' 22 לפסק הדין של הנשיאה (בדימוס) חיות (נבו 26.4.2020).

התביעה עומדת בתנאים של מעשה טרור.[62] על כן, לצערנו, לא נוכל לבחון את סיווג פעולות סייבר באמצעות עזרים מהפסיקה.

נזכיר כי כדי שפעולה תיחשב כמעשה טרור, על פי חוק המאבק בטרור, היא צריכה לעמוד בשלושה תנאים מצטברים: (1) הפעולה נעשתה ממניע אידאולוגי, דתי, לאומני או מדיני; (2) המעשה נועד על מנת לעורר פחד בציבור או להשפיע על רשות ממשלתית מעשיית, או הימנעות מעשיית, מעשה; (3) המעשה או אי־עשייתו גרמו, או היה סיכון ממשי לכך שיגרמו, לפגיעה פיזית חמורה לאדם או לחירותו, לביטחון המדינה או הציבור, לרכוש, לקודשי דת או לשירותים חיוניים.[63] כעת, נחיל תנאים אלו על פעולות סייבר. במקרה של התנאי הראשון והתנאי השני, לא קיים הבדל מהותי בין פעולות החשודות כמעשי טרור במרחב הפיזי לבין במרחב הסייבר.[64] על כן, נתמקד בהבדל המהותי בין הפעולות אשר בא לידי ביטוי בתנאי השלישי – תנאי הנזק.

בפרק נבחין בין סוגי הנזק שיכולים להיגרם, נזק פיזי לעומת נזק שאינו פיזי. מדינת ישראל אימצה את הגישה המקובלת כיום בקהילה הבין־לאומית בנוגע לאופן סיווג הנזק הפיזי שנגרם כתוצאה מפעולת סייבר, לפיה רק פעולת סייבר שגרמה לנזק פיזי תיחשב לתקיפה.[65] גישה זו מיושמת על פעולות סייבר בין־לאומיות ולאומיות כאחד.[66] לפיה, נזק פיזי כתוצאה מפעולת סייבר הוא כזה שהיה יכול להיגרם כתוצאה מפעולה בממד הקינטי בלבד. לפיכך, תקיפת סייבר היא פעולה אשר קיימת צפיות סבירה שתגרום פגיעה פיזית לאנשים או לרכוש, בין אם בממד הפיזי ובין אם בווירטואלי.[67] למשל, נזק הנגרם למידע עצמו, כמו מחיקתו או הצפנתו, ייחשב בגדר פגיעה פיזית כי הפצצת השרת הייתה מייצרת תוצאה דומה.[68] כדי לבחון את החלת תנאי הנזק על פעולות סייבר נסקור את הנזק הנגרם מפעולות סייבר.

<u>פעולות סייבר המולידות נזק פיזי</u>

על פי הטקסונומיה של פעולות סייבר שהוצגה לעיל, פעולות סייבר מסוג שיבוש נועדו להרוס או לפגוע במערכת, בין אם בממד הפיזי ובין אם בווירטואלי. לפיכך, פעולת שיבוש יכולה להוביל לפגיעה פיזית בגופו או חירותו של אדם, בבטיחות הציבור או להשבתה של שירות חיוני, ולכן מהווה תקיפת סייבר שעומדת בדרישת הנזק. לעומת זאת, פעולות סייבר מסוג איסוף, שייעודן הוא השגת מידע מהיעד והן מבוצעות תחת מעטה חשאיות, אינן גורמות לשיבוש חומרתי או וירטואלי העולה כדי נזק פיזי, זאת בהתאם לפרשנות המונח כפי שנתפס בדין הישראלי והבין־לאומי.

<u>פעולות סייבר המולידות נזק שאינו פיזי</u>

---

[62] פרשת **פלוני נ' מדינת ישראל**, לעיל ה"ש 47, בפס' 38 לפסק הדין של השופט מזוז.

[63] ס' 2 לחוק המאבק בטרור.

[64] זאת למעט שינוי קטן באשר לזיהוי המניע של הפעולה, התנאי הראשון של ההגדרה של מעשה טרור, קיים אתגר בפעולות סייבר שלא בהכרח קיים במקרה של פעולות פיזיות. במעשי טרור פיזיים אפשר ללמוד על המניע של המבצע גם מנסיבות עקיפות. לעומת זאת, לא ניתן באותה הקלות לייחס מעשים שמבוצעים בתווך האינטרנטי לאדם, ואף לגוף, מסוים.

[65] תקיפת סייבר – לצורכי רשימה זו אשתמש במונח זה עבור פעולה העולה כדי תקיפה על פי דיני השימוש בכוח במשפט הבין־לאומי, ולא כמילה נרדפת לכל פעולת סייבר לא חוקית.

[66] Roy Schondorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 NAVAL WAR COLL.REV. (2020).

[67] MICHAEL SCHMITT, CONDUCT OF HOSTILITIES IN TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, at 401–511 (2017); Katharine Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J.INT'L L. 11, 13–14 (2017).

[68] MICHAEL SCHMITT, CONDACT OF HOSTILITIES IN TALIIN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATION, שם.

ייתכן כי כתוצאה מפעולת סייבר מסוג איסוף ייגרם נזק שאינו פיזי אשר כלול במסגרת דרישת הנזק. כך למשל, אם גורם עוין ישיג נגישות ויפרסם פרוטוקולים של ישיבות ממשלה או תוכניות צבאיות אופרטיביות, אין ספק כי פעולה זו עולה כדי פגיעה בביטחון הציבור. יחד עם זאת, על מנת שפעולת איסוף תוביל לפגיעה, לא פיזית, הנכללת בדרישת הנזק, עליה לעבור את רף החומרה הגבוה שהוגדר בפסיקה. כתוצאה מכך, מספר מזערי, אם בכלל, של פעולות האיסוף יעבור את רף החומרה עבור פגיעה לא פיזית לטובת מימוש דרישת הנזק.

במקרים רבים, פרסום של מידע רגיש, במסגרת פעולת איסוף, גורם לנזק פיזי באופן עקיף ובחומרה נמוכה ביחס לרף הנקבע בחוק. למרות זאת, לא ניתן לקרוא את החוק הישראלי כך שההגדרה של מעשה טרור חלה גם על פעולות סייבר שגורמות לפגיעה בפרטיות. אין שאלה שחשיפה של מידע רגיש תגרור נזק פיזי, למשל נזק פסיכולוגי־נפשי, תדמיתי ואף כלכלי, רחב היקף לנפגעים. עם זאת, מדובר בנזק מסדר שני בלבד, ואילו הנזק הראשוני והישיר אינו פיזי.[69] בקריאה לשונית של החוק, לא ניתן להתעלם מהדרישה המפורשת של החוק שהמעשה בעצמו יגרום לנזק, או סיכון לנזק, פיזי־ממשי. לפיכך, הפרשנות הסבירה של החוק היא שפגיעה שאינה גורמת נזק פיזי לא תיחשב לפעולת טרור.

במסגרת הפרק לעיל נבחנו התנאים המצטברים לקיומה של פעולת טרור, תוך התמקדות בתנאי השלישי. ראינו כי על מנת לעמוד בהגדרה של פעולת טרור על פי חוק המאבק בטרור נדרש קיומו של נזק פיזי, ולפיכך פעולות סייבר הגורמות לפגיעה בפרטיות אינן נכללות בהגדרה זו. בפרק הבא נציג דוגמה הממחישה את הפער הזה בחוק.

ב.4 הפער בחוק המאבק בטרור באמצעות מקרה בוחן: שירביט

ב־1.12.20 הודיע מערך הסייבר הלאומי על פריצה לשרתי חברת הביטוח שירביט. ההאקרים השיגו נגישות למידע רגיש ורב על לקוחות החברה.[70] חלק מהמידע פורסם, והשאר נעלם בנבכי הרשת האפלה.[71] חברות האנטי־וירוס ייחסו את התקיפה לקבוצת האקרים איראנית[72] וסברו כי הפריצה לא הייתה תקיפת כופרה[73] פלילית גרידא, אלא אקט על רקע לאומני.[74] על פי הטקסונומיה המדגישה את תוצאות הפעולה שהוצגה לעיל, חדירה זו תסווג כפעולת סייבר מסוג איסוף. הייעוד של הפריצה היה השגת מידע ופרסומו. בנוסף, ישנו קונסנזוס

---

[69] M. Nofer et al., *The Economic Impact of Privacy Violations and Security Breaches,* 6 BUS. INFO. SYS. ENG'G 339 (2014); Loannis Agrafiotis et al., *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding how they Propagate*, 4 J. OF CYBERSEC. (2018); John Kleinig, *Crime and the Concept of Harm,* 15 N.Ill.U.L.Rev., 27 (1978); MICHAEL SCHMITT, CONDACT OF HOSTILITIES IN TALIIN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATION, לעיל ה"ש 67.

[70] "אירוע דלף מידע בחברת שירביט" **מערך הסייבר הלאומי** (1.12.2020) https://www.gov.il/he/pages/bp_info_leak; *Ransomware Alert: Pay2Key,* CHECK POINT RESEARCH (Nov. 6, 2020) https://research.checkpoint.com/2020/ransomware-alert-pay2key/.

[71] רשת אפלה (darknet) היא רשת נפרדת שמתקיימת על פני תשתית האינטרנט ומהווה מוקד לתקשורת של קבוצות מחתרתיות ועברייני מחשב.

[72] הקבוצה שביצעה את התקיפה הזדהתה בתור Blackshadow והיא קושרה לקבוצת Fox Kitten אשר מוציאה לפועל תקיפות סייבר נגד יעדים ישראליים באופן סדרתי. ראו: *Fox Kitten – Widespread Iranian Espionage-Offensive Campaign*, CLEARSKY CYBER SECURITY (Feb. 16, 2020) HTTPS://WWW.CLEARSKYSEC.COM/FOX-KITTEN/.

[73] המכונה גם ransomware היא נוזקה המגבילה גישה למידע ומשמשת לסחוט את הנתקף לשלם דמי כופר על מנת לאפשר את הגישה לאותו המידע.

[74] רפאל קאהאן "הפריצה לשירביט: ההאקרים פרסמו מידע חדש - כולל צילום של דרכון המנכ"ל" **כלכליסט**, (15.12.2020) https://www.calcalist.co.il/internet/articles/0,7340,L-3882054,00.html; יוסי הטוני "תם האולטימטום: נמשכת ההדלפה של מסמכי שירביט" **אנשים ומחשבים** (6.12.2020) https://www.pc.co.il/general/327230/; *Pay2Key – The Plot Thickens,* CHECK POINT RESEARCH (Nov. 12, 2020) HTTPS://RESEARCH.CHECKPOINT.COM/2020/PAY2KEY-THE-PLOT-THICKENS/.

שהפעולה לא גרמה לנזק פיזי מסדר ראשון למערכות החברה או ללקוחותיה. אומנם, נוהל משא ומתן לפדיון המידע, אך חברות האנטי־וירוס סברו כי רווח כלכלי או שימוש בפרטי המידע שנגנבו לא היו תכליות הפעולה. בנוסף, אין אינדיקציות לכך שההאקרים תכננו להשתמש במידע שהושג.[70] לפיכך, דרישת הנזק הפיזי אינה מתקיימת במקרה דנן, אך ניכר שהתרחשה פגיעה חמורה ועמוקה בזכותם הבסיסית לפרטיות של לקוחות החברה, העומדת בבסיס הנזק. למרות שהתפיסה הרווחת היא שהפעולה בוצעה על רקע לאומני ונועדה לזרוע פחד בציבורי הישראלי, מאחר שלא נגרם נזק פיזי, פעולה זו אינה נחשבת למעשה טרור על פי החוק הישראלי.
יתרה מזו, על פי חוק המחשבים, אדם החודר למחשב או לתוכנה שלא כדין בצורה הגורמת לפגיעה בפרטיות מבצע עבירה פלילית שדינה מאסר שלוש שנים.[75] בנוסף, אם אדם מבצע עבירה שנחשבת למעשה טרור, עונשו מוכפל.[76] לפיכך נוצר מצב אבסורדי שבו אם האקרים פורצים לשרתי חברה פרטית ומוחקים אותם, פעולה הנחשבת שיבוש, מעשיהם ייחשבו לעבירה פלילית שתוחמר למעשה טרור. לעומת זאת, אם ההאקרים היו מעתיקים את המידע, ולא משבשים את פעילות הרשת, פעולה המסווגת כאיסוף, מעשיהם ייחשבו "רק" לעבירה פלילית. זאת מבלי להתחשב במניעים לפעולה, ממדי ההשפעה שלה והאפקטיביות שבה זרעה טרור ובהלה בקרב הציבור. נזכיר כי חשיפה של מידע אישי קבוע, כמו תעודות זהות ותמונות, מובילה לפגיעה עמוקה, קבועה וארוכת טווח בנפגעים מאחר שהם עלולים להיות בסכנה לגנבת זהות וניצול של פרטיהם האישיים לדיראון עולם ולכן הדבר אפקטיבי מאוד למימוש של בהלה בקרב הציבור.
נראה אם כן, כי פעולת סייבר מסוג שיבוש שבמסגרתה הפורצים מוחקים כליל רכיבים ברשת היעד היא עבירה פלילית על פי חוק המחשבים ויתרה מזו נחשבת לפעולת טרור. לעומת זאת, פעולת סייבר מסוג איסוף גם אם תגרום לפגיעה חמורה, קבועה וארוכת טווח אינה נחשבת לנזק פיזי ולכן לא תסווג כמעשה טרור למרות הפגיעה המשמעותית.

ג. ממצאים ומסקנות

ג.1 פתרון מוצע – אימוץ הפרשנות האירופית להגדרה של מעשה טרור

התפיסה הישראלית מהדהדת את החקיקה בארצות הברית. בחוק האמריקאי ישנן כמה הגדרות שונות של מעשה טרור אשר נוסחו על ידי גופים ממשלתיים שונים כך שתכליותיהן שונות. עם זאת, המשותף להגדרות אלו הוא אימוץ של תנאים דומים לאלו המנויים בחוק למאבק בטרור. אין התייחסות ספציפית בחקיקה האמריקאית לפעולות סייבר העולות כדי פעולת טרור.[77] לעומת זאת, התפיסה באיחוד האירופי בעניין זה היא שונה. הפרלמנט האירופי זיהה את העלייה בשימוש בפעולות סייבר ככלי בידי גורמי טרור. לאור זאת, נחקק תחילה חוק נקודתי שנועד לסכל את פעולת "מחנות האימונים הווירטואליים".[78] חוק זה הוחלף ב־2013 בחוק שמטרתו להתמודד עם פשע וטרור באינטרנט באופן גורף. ההגדרה של מעשה טרור בחוק זה היא כוללנית ורחבה

---

[75] ס' 4, 6(א)(6) לחוק המחשבים, התשנ"ה–1995.

[76] ס' 37 לחוק המאבק בטרור.

[77] 22 U.S.C. § 2656f(d)(2); 18 U.S.C. § 2331; 28 C.F.R. § 0.85; USA Patriot Act, 2001; Terrorism Risk Insurance Act § 102(1)(a) (2002).

[78] European Parliament and Council, No. 919/2008 of 28 November 2008; Argomaniz, Javier, *European Union Responses to Terrorist Use of the Internet,* 50(2), COOPERATION AND CONFLICT 261–264 (2015).

יותר, כך שלא ניתן משקל משמעותי להבדל בין מעשה טרור לבין פשע פלילי. אולם, החוק כן מתייחס באופן ספציפי לפעולות שיבוש ואיסוף בסייבר ומסווג את שתיהן כמעשי טרור.[79]

על כן, אציע לאמץ בחקיקה את הפרשנות האירופית, שהיא סיווג של פעולות סייבר, הן מסוג שיבוש והן מסוג איסוף, כפעולות טרור אם בוצעו ממניעים לאומניים ונועדו לזרוע טרור בקרב הציבור. הדרך המומלצת להטמיע פרשנות זו היא באמצעות הוספת ראש נזק של פגיעה בפרטיות להגדרה של מעשה טרור מתוך חוק המאבק בטרור. נזכיר כי חוק המאבק בטרור מגדיר שלושה תנאים מצטברים לסיווג של פעולה כמעשה טרור: (1) הפעולה בוצעה ממניעים לאומניים, (2) נועדה לזרוע פחד בקרב הציבור, (3) וגרמה לנזק פיזי. אציע כי במסגרת דרישת התנאי הפיזי, תתווסף האפשרות כי הנזק שנגרם הוא פגיעה חמורה בפרטיות.

חלופה אפשרית היא, בדומה לאופן ניסוח החוק האירופי, סיווג מפורש של פעולות סייבר, הן מסוג שיבוש והן מסוג איסוף, בתור פעולות טרור במסגרת פרק ג': עונשין של חוק המאבק בטרור. לחלופין, ניתן לכלול הגדרה זו תחת חוק המחשבים משיקולים נושאיים.[80] יחד עם זאת, מאחר שההגדרות של מעשי ארגוני טרור ופעילי טרור בחוק המאבק בטרור מהוות בסיס עבור חוקים ותקנות אחרים, אני סבורה כי דידקטית ראוי לשנות את ההגדרה של מעשה טרור בגופו של חוק המאבק בטרור.

ג.2 הצדקות לשינוי ההגדרה של מעשה טרור בחוק באשר לפגיעה בפרטיות

<u>כוונת המחוקק – התאמת החוק לאיומים אקטואליים</u>

פעולה תוך איום בנשק הוגדרה בחוק כחריג של ההגדרה למעשה טרור. קרי, גם אם הפעולה אינה עומדת בתנאים של מעשה טרור, אם נעשתה תוך איום בנשק היא יכולה להיחשב לפעולת טרור.[81] בתיקון 12 לחוק העונשין, שנחקק ב־1991, נשק הוגדר ככלי שפולט חומר שנועד להזיק לאדם, לרבות נשק קר.[82] בשנת 2016 החוק למאבק בטרור תוקן, וההגדרה הורחבה לכלול גם נשק כימי, ביולוגי או רדיואקטיבי.[83] ניתן ללמוד מתיקונים אלו שהמחוקק הכיר בכך שמנעד האמצעים שבהם נעשה שימוש על מנת לבצע פעולות טרור מתרחב ומשתנה. יתרה מזו, בדיונים בנושא תיקון החוק הוסיף נציג השב"כ שנכח כי "החוק (חוק המאבק בטרור, התשע"א–2011) שאנו עובדים איתו היום, מתאים לאיומים שהיו לפני 50 שנה ולא לעידן הטכנולוגי והרשתות החברתיות".[84]

מכך נסיק כי כוונת המחוקק היא להתאים את החוק כדי להיטיב את התמודדותו עם איומים אקטואליים.

ההזדמנויות שמביאה עימה רשת האינטרנט שיפרו את חיינו בצורה דרמטית. עם זאת, התלות של החברה באינטרנט הפכה פלטפורמה זו ליעד לפגיעה ומניפולציה. כיום, גורם המעוניין לבצע אקט של אלימות ולפגוע באחרים יכול לעשות זאת בהינף מקלדת, בעודו ספון בביתו שעשוי להיות בכל מקום בעולם. יש המנצלים את האינטרנט ככלי להפחדה, להפצת שנאה ולאלימות. על פי פרשנות תכליתית של התנאי השני בהגדרת מעשה

---

[79] European Parliament and Council, No. 919/2008, שם.

[80] חוק המאבק בטרור; חוק המחשבים.

[81] ס' 2 לחוק המאבק בטרור ("נעשה המעשה או האיום כאמור בפסקה (3)(א) תוך שימוש בנשק או בסכין, יראו אותו כמעשה טרור גם אם לא התקיים בו האמור בפסקה 2").

[82] ס' 144(ג)(1–3) לחוק העונשין, התשל"ז–1997.

[83] ס' 1 לחוק המאבק בטרור.

[84] פרוטוקול ישיבה ועדת החוקה, חוק ומשפט, הממשלה ה־34 (12.10.2015).

טרור,[85] הפעולה נועדה לזרוע פחד בציבור, אין ספק כי ישנן פעולות סייבר המבוצעות ממניע זה.[86] פעולת סייבר היא כלי אפקטיבי בידי גורמים הפועלים ממניעים אידאולוגיים אשר מעוניינים לזרוע טרור ופחד בקרב הציבור או להשפיע על התנהלות ממשלתית.[87]

לפיכך, ראוי לדחות את הפרשנות הקיימת למעשה טרור ולאמץ את גישת האיחוד האירופי כך שפגיעה בפרטיות במסגרת הנזקים האפשריים עולה כדי טרור. הוספת ראש נזק של פרטיות תחת התנאי תיישב את חוסר העקביות בסיווג פעולות שיבוש ופעולות איסוף. במקרה שבו פעולת סייבר עומדת בתנאי החוק, בין אם מסוג שיבוש או איסוף, היא תיחשב למעשה טרור.

<u>עיבוי האפקט ההגנתי על זכות לפרטיות</u>

הזכות לפרטיות היא זכות יסוד אשר מהווה אמצעי משמעותי להגנה ומימוש זכותו של האדם לכבוד, המעוגנת בחוק־יסוד: כבוד האדם וחירותו.[88] מטרתה היא להבטיח את האינטרס האישי של האדם לאוטונומיה ואת חירותו.[89] תפיסה זו קיימת גם בגישות משפט מקבילות.[90] במסגרת זאת, החוק להגנת הפרטיות נועד למנוע מצב שבו מידע אישי של אדם חשוף לעיני הציבור כולו, ללא הצדקה וללא אישורו.[91] הזכות לפרטיות היא הגבול שנמתח בין נחלת הכלל לבין רשות הפרט וכך היא מאפשרת לאדם מרחב שבו מניחים לו לנפשו והוא חופשי לפתח את ה"אני" שלו.[92]

בעידן הנוכחי, הזכות לפרטיות נתונה לאיום מוגבר ומועצם בממד האינטרנטי. זאת לאור העובדה שמרב פעולות הסייבר כיום הן פעולות איסוף, ולא שיבוש.[93] ניכר שאיום הטרור פלש לממד האינטרנטי וכולל גם פעולות סייבר.[94] מציאות זו מדגישה את החשיבות של מציאת פתרון משפטי עבור התמודדות עם פעולות מסוג זה. כיום, שיתוף של פרטים אישיים עם חברות פרטיות או גופים ממשלתיים עבור קבלת שירות ושמירה על אורח חיים מסוים הוא אקט המלווה בחשש רב. לקוחות ומשתמשים רבים חוששים מפני שימוש לא מורשה במידע או נגישות של גורמים לא מורשים למידע והם נתפסים כלקיחת סיכון ממשי.[95] על כן, ניכר שהחוק לא ממלא את ייעודו במניעת טרור במרחב זה, וראוי לעבות את האפקט ההגנתי של זכות זו באמצעות חוקי הטרור לאור אופי האיום על הזכות.

---

[85] ס' 2 לחוק המאבק בטרור.

[86] OECD ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT, at 22-30 (2017).

[87] ICT CYBER DESK. CASE STUDY – OPISRAEL 2014, INTERNATIONAL INSTITUTE FOR COUNTER-TERRORISM, at 46–62 (2014).

[88] ס' 7 לחוק-יסוד: כבוד האדם וחירותו.

[89] ע"פ 1302/92 **מדינת ישראל נ' מרדכי בן ריימונד נחמיאס**, פ"ד מט(3) 309 (21.6.1995).

[90] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948), art. 12; Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8; U.S. Const. art. 4 § 4.

[91] הצעת חוק הגנת הפרטיות, התש"ם–1980, ה"ח 1453, בעמ' 206; ס' 2(5, 10-8) לחוק הגנת הפרטיות.

[92] בג"ץ 2481/93 **יוסף דיין נ' ניצב יהודה וילק, מפקד מחוז ירושלים**, פ"ד מח(2) 456 (9.2.1994).

[93] Charles Harry & Nancy Gallagher, *Classifying Cyber Events: A Proposed Taxonomy*, CENT. FOR INT'L & SEC. STUD. AT MARYLAND 2 (2018); *Cyber Security Report 2021*, CHECK POINT SOFTWARE TECHNOLOGIES (Apr. 12, 2021).

[94] דוד סימן טוב "מגמות אסטרטגיות בתחום הסייבר" **INSS** (6.1.2021) https://www.inss.org.il/he/publication/strategic-survet-cyber/.

[95] Ron Hill & Lisa Penaloza, *Understanding and Interpreting Consumer Vulnerability*, in *Advances in Consumer Research* Vol. 33, 212, 212-218 (Connie Pechmann & Linda Price eds., Ass'n for Consumer Rsch. 2006); Ereni Markos, George R. Milne & James W. Peltier, *Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil*, 36(1) JOURNAL OF PUBLIC POLICY & MARKETING 79, 79–96 (April 2017).

על כן, בעידן שבו הזכות לפרטיות נמצאת תחת מתקפה מתמשכת וקשה, מן הראוי להקים הגנות וסייגים נוספים על מנת למנוע את הפגיעה בזכות בסיסית זו אשר עלולה להשפיע ולהדהד שנים רבות לתוך העתיד.

<u>פרשנות טקסטואלית של ההגדרה המהותית של מעשה טרור – היכללות של פעולות סייבר מסוג איסוף</u>

מטרתן של פעולות טרור, כפי שעולה מדברי ההסבר, היא לעורר פחד ובהלה בציבור.[96] תכליתן אינה פגיעה אסטרטגית, אלא פגיעה תודעתית ורעיונית רחבה שאינה מחייבת פגיעה פיזית בהכרח, אלא מייצרת חשש משמעותי ונרחב.[97] אותן פעולות טרור נועדו לערער את עמודי התווך של חיי הנפגעים כך שיטילו ספק באורח חייהם, בביטחונם האישי ובתפיסות עולמם: הנסיעה באוטובוס מעוררת חשש, צבע העור או הזהות האתנית, דתית או מגדרית הופכים למקור לחשש, והטיסה הבין־לאומית היא סיכון מחושב.[98] בממד האינטרנטי הטשטוש בין המרחב האזרחי לציבורי מועצם וכך גם החשש מפגיעה בפרטים במטרה לזרוע טרור.

האפקטיביות של פעולת טרור אינה נאמדת רק על פי הנזק הפיזי שהפעולה גורמת, אלא גם בהתבסס על האדוות של הפעולה והשפעתה על המורל הציבורי. במקרים רבים, האפשרות שתושג נגישות למאגרי עתק שמכילים פרטים רבים על אנשים רבים, ושתוכנם ייחשף במסגרת פעולת סייבר, תייצר אפקט דומה ואף רחב יותר מאשר פעולה פיזית. אי לכך, יש להרחיב את ההגדרה של מעשה טרור כך שיכלול גם פעולות סייבר שנועדו להשליט טרור באמצעות פגיעה חמורה בפרטיות.

ד. ביקורות כנגד הרחבת ההגדרה של מעשה טרור בחוק המאבק בטרור

קיימים כמה מחסומים פוטנציאליים למימוש של מהלך מסוג זה המוצע במאמר. ראשית, סיווג פעולות איסוף כמעשי טרור הוא בעל משמעות דקלרטיבית במישור הפנימי וכן במישור הבין־לאומי. יחד עם זאת, לרוב, החשודים אינם נתונים תחת ריבונות המדינה שאזרחיה נפגעו, ולכן הרחבה זו לא בהכרח תגביר את הסיכוי להעמדתם לדין. שנית, יש לתת את הדעת לגבי רף החומרה של פגיעה בפרטיות המצדיקה זיהוי של הפעולה כמעשה טרור. לבסוף, ייתכן כי שינוי החוק ירחיב את אחריות המדינה להגן על אזרחיה באמצעות התערבות במנגנוני אבטחת הרשת והמידע של חברות פרטיות גדולות. בפרק זה ארחיב על טענות נגד אלו ואנסה להציג התמודדויות אפשריות עימן.

ד.1 קושי בהעמדה לדין

סיווג של עבירה כמעשה טרור אוטומטית מחמיר את העונש הפוטנציאלי לנאשמים, מה שיכול להגביר את ההרתעה כנגד מפגעים פוטנציאליים. יחד עם זאת, ניתן לטעון כי לא מדובר בעבירה פיזית שבה המפגע בהכרח נמצא בקרבת מקום ולכן נתון למנגנוני הריבונות והאכיפה של ממשלת ישראל. במקרים רבים האקרים לא מבצעים פעולות טרור בסייבר כאשר הם נמצאים בתוך שטחי המדינה או נתונים לריבונותה. לכן, בנדבך זה,

---

[96] דברי ההסבר להצעת חוק המאבק בטרור.

[97] מישל פוקו **לפקח ולהעניש** 244–310 (דניאלה יואל מתרגמת 2015).

[98] Martha Crenshaw, *Theories of terrorism: Instrumental and organizational approaches*, 10(4) J.STRAGIC STUD., 13 13–31 (1987); Donald Holbrook & John Horgan, *Terrorism and Ideology: Cracking the Nut,* 13 PERSPECTIVES ON TERRORISM 1 (2019).

כשאין בנמצא גופי אכיפה בין־לאומיים,[99] ההשלכות של הוספת ראש נזק של פרטיות לחוק המאבק בטרור הן דקלרטיביות בעיקרן.

לטענה זו כמה חלקים שונים שעבור כל אחד תהיה התמודדות אחרת. ראשית, לא מן הנמנע כי אזרחי ישראל או אנשים הפועלים בשטחה ותחת ריבונותה יבצעו פעולות סייבר מסוג איסוף, לרבות טרור יהודי, אשר יוכלו להיחשב על פי התיקון המוצע פעולות טרור. עבור מקרים אלו, התיקון המוצע אינו דקלרטיבי כלל וכלל. שנית, יש ערך משמעותי לפעולה דקלרטיבית. ספר החוקים של מדינת ישראל הוא גם מערך של מצוות עשה ואל תעשה המכווינות את האדם והמדינה איך לפעול. בנוסף לייעוד זה, ספר החוקים משקף את ערכיהן של מדינת ישראל והחברה הישראלית. יש משמעות חינוכית וערכית רחבה להוקיע פעולות אשר נתפסות בעיני הציבור כפסולות. על כן, ייעודו של התיקון המוצע הוא לשקף את התפיסה החברתית כי פעולת סייבר שמובילה לפגיעה עמוקה בפרטיות ונעשית ממניעים לאומניים ועל מנת לזרוע טרור היא פעולת טרור.

לבסוף, סיווג של קבוצת פעולות כמעשי טרור הוא בעל השלכות פרקטיות משמעותיות ומרחיקות לכת באשר לפיצוי הנפגעים ושיפויים. כיום, נפגעי צד ג׳ יכולים לתבוע פיצוי על הפגיעה שנגרמה להם באמצעות תביעת החברה שהותקפה. פתרון זה הוא חלקי בלבד משום שהוא מותנה בהוכחת התנהלות רשלנית מצד החברה. נפגע צד ג׳ לא יקבל פיצוי אם בית המשפט יפסוק שהחברה עשתה כל שביכולתה למנוע את התקיפה, לשמור על המידע ולמזער נזק פוטנציאלי,[100] כך שהדגש הוא על התנהגות החברה, וכפי שצוין לעיל, במקרים שמדובר בפעולה המגובה על ידי גוף מדינתי, לא ניתן לצפות מהחברה למנוע את התקיפה בהצלחה ללא סיוע.[101] מציאות זו עלולה להעמיד את הנפגעים בפני שוקת שבורה. לעומת זאת, במקרה של נזקים שנגרמו בעקבות מעשה טרור, קיימת תשתית משפטית מבוססת לטיפול בנפגעים באמצעות תביעת פיצויים מהמדינה לאור חומרת הפגיעה שנגרמה.[102] בשל הדמיון במטרת הפעולה ובמוטיבציות לביצועה בין פעולת טרור פיזית לבין פעולת סייבר ממניע אידאולוגי־לאומני, סיווג פעולות איסוף כמעשה טרור יקים לנפגעים אפשרות לתבוע פיצויים מהמדינה בגין הפגיעה.

ד.2 קביעת רף החומרה

יש לתת את הדעת לגבי אופן קביעת רף החומרה של פגיעה בפרטיות המצדיקה זיהוי של הפעולה כמעשה טרור. הרי לא כל פעולת סייבר המבוצעת ממניעים לאומניים ועל מנת לזרוע פחד בציבור שמובילה לחשיפה של מידע גורמת לפגיעה חמורה מספיק בכדי להיות מסווגת כפעולת טרור.

---

[99] Fausto Pocar, *New Challenges for International Rules against Cyber-Crime*, EUR. J. CRIM. POL'Y & RSCH. 10, 27–37 (2004).

[100] ליטל דוברובצקי ״שעות לאחר דליפת פרטי הלקוחות: בקשה לאישור תביעה ייצוגית נגד שירביט״, **כלכליסט** (1.12.20) https://www.calcalist.co.il/local/articles/0,7340,L-3878371,00.html; עידו גביש ״ייצוגית נגד שירביט? לתובעים תהיה משימה לא פשוטה, **וואלה!** (8.12.20) https://finance.walla.co.il/item/3403634; שלומי דיאז, ״בשל הפריצה: תביעות ייצוגיות נגד שירביט״, **ישראל היום** (6.12.20) https://www.israelhayom.co.il/article/826985.

[101] ראו למשל עניין (*The Right to Privacy*) Warren Samuel D. & Louis D. Brandeis, לעיל ה״ש 24. בית המשפט האנגלי צמצם את האפשרות של נפגעים לקבל פיצוי מחברה שנתקפה במסגרת פעולת סייבר.
ראו גם: Steven Baker et al., *English High Court Clarifies Appropriate Causes of Action in Data Claim Where Defendant Was a Victim of Third-Party Cyber-Attack*, PRIVACY LAW BLOG (Oct.4, 2021) https://privacylaw.proskauer.com/2021/10/articles/data-breaches/english-high-court-clarifies-appropriate-causes-of-action-in-data-claim-where-defendant-was-a-victim-of-third-party-cyber-attack/.

[102] חוק התגמולים לנפגעי פעולות איבה, התש״ל–1970; ס׳ 35 לחוק מס רכוש וקרן פיצויים, התשכ״א–1961; רע״א 6904/97 **ס׳ ת׳ ו׳ בקעות בע״מ נ׳ מנהל מס רכוש וקרן**, פ״ד נב(4) 1 (1.9.1998).

זהו אתגר הקיים בממד הסייבר כמו בממד הפיזי, על אף שלדאבוננו הניסיון הנרחב בממד הפיזי הוביל לקביעת רף ברור וחד־משמעי ברוב המוחלט של המקרים. יחד עם זאת, אציע כי עבור פעולות סייבר שמובילות לפגיעה בפרטיות יש לייצר רף חומרה באמצעות קביעת פרמטרים לבחינה. רק הפרה של הזכות לפרטיות אשר גורמת לפגיעה עמוקה, קבועה וארוכת טווח תהיה מסווגת בתור פעולת טרור. יתרה מזו, יש לשקול גם כמה הפגיעה היא מכוננת עבור הנפגעים: ככל שהמידע הוא יותר מרכזי לקיום חיים תקינים, כך הפגיעה תיחשב לעמוקה. כך למשל, חשיפה של תעודת הזהות או תמונה של אדם היא פגיעה מכוננת וקבועה, משום שמדובר בפרטים שאינם ניתנים לשינוי, ולכן חשיפתם תגרום לפגיעה ממושכת. זאת לעומת חשיפה של פרטי גישה לחשבון לקוח של שירות אינטרנטי כמו מועדון לקוחות, אשר ניתן לשינוי, כך שהפגיעה אינה מכוננת ובעלת אופי זמני. בנוסף, גם היקף הפעולה הוא שיקול משמעותי, כמו כמות הנפגעים ואופיים (פגיעה בקטינים היא חמורה יותר, למשל).

ד.3 הרחבת אחריות המדינה

ייתכן כי שינוי החוק יוליד הרחבה כלשהי של אחריות המדינה להגן על אזרחיה מפני פגיעה בפרטיות באמצעות סיוע לחברות פרטיות גדולות שאין בכוחן להתמודד עם איומי סייבר מעצמתיים. החשש במקרה זה הוא כפול. תחילה, הטלה של נטל גדול מדי על המדינה להגן על פרטיות אזרחית. שנית, ישנו חשש מפני התנגשות בין החובה של המדינה להגן על אזרחיה מפני פגיעה מהותית בליבת הזכות לפרטיות לבין פגיעה במרכזה של הזכות לקניין של בעלי החברות הפרטיות, אשר כוללת בתוכה את הזכות לאוטונומיה בשימוש של אדם בקניינו הפרטי.

כיום, ההגנה הממשלתית שלה זוכות חברות פרטיות בממד הפיזי ובממד הסייבר כאחד היא מצומצמת, כוללת בעיקר הגנה על תשתיות קריטיות ולרוב אינה מספקת. ראו למשל את עניין "אטרף" כשיקוף של מצב הדברים הנוכחי. אומנם, הרשות להגנת הפרטיות הוציאה תקנות אבטחת מידע לחברות פרטיות שמחזיקות מידע על אזרחי המדינה, אך התקנות הן גמישות ואמורפיות, ואכיפתן חלקית בלבד.[103] למרות שהרשות לפרטיות זיהתה מחדלים במנגנון האבטחה ובתצורת השמירה של לקוחות "אטרף" והתריעה על כך בפני חברת Cyberserve, חברת האם, החברה לא שעתה לאזהרות ולא תיקנה את פגמי האבטחה. מכאן ניתן להסיק כי המנגנון עצמו חסר שיניים ועל כן יעילותו לוקה בחסר, בלשון המעטה.[104]

סיווג של פעולות איסוף כטרור ירחיב את אחריות המדינה להגנה מעבר לגופים ממשלתיים ותשתיות קריטיות לחברות פרטיות. ייתכן כי מדובר בנטל יותר משמעותי, אך מאחר שמאמציה של המדינה כיום, כפי שניתן לראות, אינם מספקים, ראוי שמערך זה יעובה. הגדלת הנטל אינה מובילה בהכרח להגברת השליטה הממשלתית ברשתות המחשבים של חברות פרטיות. ההפך הוא הנכון, המטרה היא לספק יותר אמצעי הגנה ודרישות חיצוניות.

באשר לחשש השני שהוזכר לעיל, אין הכוונה להפקיע את האחריות מהחברות הפרטיות, אלא להגיע להסדר של חלוקת אחריות כפי שקיים בממד הפיזי.[105] אין שאלה כי התנגשות זו מחייבת שרטוט זהיר ומדויק של גבולות הגזרה של ההתערבות של המדינה בסיוע בהגנה על רשתותיהן של חברות פרטיות.[106] יחד עם זאת, מפריזמה

---

[103] תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017.

[104] עדכון בהמשך לאירוע אבטחה בחברת CyberServe שכולל את דליפת המידע מאתר האינטרנט "אטרף", הרשות להגנת הפרטיות (3.11.21); אסף גלעד ואופיר דור, "מפרשת שירביט ועד הפריצה לאטרף: לרשות הפרטיות אין כוח, המשתמשים חשופים, וההאקרים חוגגים" **גלובס** (1.11.21) https://www.globes.co.il/news/article.aspx?did=1001389255.

[105] ס' 1–2 לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998.

[106] ס' 3 לחוק יסוד: כבוד האדם וחירותו; יהושוע ויסמן **דיני קניין** חלק כללי (1993); Kenneth J. Vandevelde et al,. *The New Property of the Nineteenth Century: The Development of the Modern Concept of Property* BUFF.L.REV., 325 (1993);

פרגמטית־ריאליסטית, מבחינת צד ב', אומנם כל חברה נדרשת להציב מנגנוני אבטחה מסוימים על מנת להתגונן מפני תקיפות,[107] אך פעולות סייבר רבות, מקורן בארגוני טרור הנתמכים ואף מוכוונים על ידי מעצמות מדינתיות.[108] מדובר באיום מעצמתי, שלרוב החברות אין את המשאבים או את היכולת להתמודד עימו באופן עצמאי. זאת, לעומת תקיפות סייבר שמקדמים גורמים פליליים הפועלים באופן עצמאי ובמעט משאבים נגד חברות, מולן יכולה החברה לאבטח את עצמה ביתר קלות באופן יחסי. בהקבלה לממד הפיזי, מצופה מחברות להעמיד שומר בכניסה לבניין כדי למנוע גישה מגורמים לא מורשים, אבל לא מצופה מהן להדוף מתקפת טרור מאורגנת ללא סיוע של כוחות משטרה או צבא. מכך עולה המסקנה שבתחומים שבהם חברות פרטיות לא מצליחות לשאת לבדן בנטל של שמירה על זכות היסוד של משתמשיהן, לרבות הזכות לפרטיות, בבחינת "גזרה שהציבור לא יכול לעמוד בה", ראוי שהמדינה תסייע, בהינתן הסדרה סבירה ומידתית.[109]

ה. סיכום

סיווג של פעולת סייבר כמעשה טרור בדין הישראלי כיום מבוסס על הנזק שהפעולה גורמת, כך שפגיעה שלא מולידה נזק פיזי לא תיחשב למעשה טרור. תפיסה זו מובילה להבחנה בעייתית בין פעולות סייבר שנועדו לשיבוש לבין כאלו שנועדו לאיסוף. ניתן ליישב מתח זה באמצעות אימוץ הפרשנות האירופית להגדרה של מעשה טרור, הכוללת גם פגיעה בפרטיות כראש נזק.

מפרשנות תכליתית של החוק למאבק בטרור ניתן להסיק כי התוצאה של פגיעה בפרטיות, במקרים רבים, מייצרת אפקט ציבורי, פיזי ותודעתי דומה למעשה טרור. לפיכך ראוי להמשיג מעשים כאלו כמעשי טרור. הרחבה זו מתיישבת עם כוונת המחוקק, אשר ניכר כי ביקש להתאים את החוק לאיומים אקטואליים. כאמור, אין ספק שפעולות סייבר מהוות איום משמעותי שהולך וגדל בשנים האחרונות.

חשוב לציין כי להרחבה זו יש השלכות משפטיות, נורמטיביות וחברתיות שיש לבחון במסגרת שינוי עתידי של החוק. מובן מאליו שתיקון החוק יגרור שאלות והתאמות טכניות להן יש לתת מענה. במסגרת העבודה יש לדון בסוגיות מרכזיות ומרתקות אלו ועוד, על מנת לצמצם את הפער הקיים כיום בחוק המאבק בטרור.

Hanoch Dagan, *Autonomy and Property* in RESEARCH HANDBOOK ON PRIVATE LAW THEORY 185 (Hanoch Dagan & Benjamin C. Zipursky ed. 2020).

[107] תקנות הגנת הפרטיות (אבטחת מידע); Daniel Benoliel, *Law, Geography and Cyberspace: The Case of On-Line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125 (2005).

[108] Kenneth Geers, Darien Kindlund, Ned Moran & Rob Rachwald, *World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks*, FireEye (2014).

[109] בג"ץ 7846/19 **עדאלה המרכז המשפטי לזכויות המיעוט הערבי בישראל נ' פרקליטות המדינה יחידת הסייבר** (נבו 12.4.2021).