אוניברסיטת תל-אביב

הפקולטה למשפטים ע״ש בוכמן

הפעלת אמצעי מעקב מקוונים לצרכי סיכול טרור - היבטים משפטיים

עבודה סמינריונית בקורס

״דיני אינטרנט: היבטים פליליים ואזרחיים״

בהנחיית ד״ר אלעד אורג

Copyright © 2012 www.all-free-download.com

מגיש: **חן מנצור**

שנה״ל תשע״ב

תל אביב, 11 ספטמבר 2012

תוכן עניינים

מס' עמוד

מבוא... **1**

1. **טרור ושימוש של ארגוני טרור ברשת האינטרנט ....** **2**

1.1. טרור - משמעות המונח ומאפייניו **2**

1.2. שימוש של ארגוני טרור ברשת **4**

1.2.1. שימוש ב"אתרי טרור" **5**

1.2.2. איסוף מל"מ (מודיעין לקראת מבצע) **7**

1.2.3. סייבר טרור (טרור מקוון) **8**

1.2.4. הרשת כאמצעי תקשורת בשירות ארגוני הטרור **9**

2. **המאפיינים המיוחדים של אמצעי המעקב המקוונים ברשת........................** **10**

2.1. מאפיינים ייחודיים של המודיעין המסכל.................................... **11**

2.2. המודיעין בעידן המידע **12**

2.3. האיומים על זכויות הפרט ביחס להפעלת אמצעי מעקב על תקשורת מקוונת **14**

3. **הגבלות משפטיות על מעקב אחר פעילות מקוונת - מערכת האיזונים הקיימת בין צורכי המודיעין לבין זכויות הפרט במסגרת הדין הקיים ....** **16**

3.1. **משפט משווה ....** **16**

3.1.1. האיחוד האירופי **16**

3.1.2. בריטניה **16**

3.1.3. קנדה **17**

3.1.4. ארה"ב **18**

3.2. **ישראל ....** **23**

3.2.1. מודיעין מסכל בישראל – שירות הביטחון הכללי **24**

3.2.2. חיפוש ותפיסת חומר במערכות מחשב **25**

3.2.3. האזנת סתר **26**

3.2.4. האזנת סתר מחוץ לגבולות ישראל **31**

מס' עמוד

3.2.5. מעקבים אלקטרוניים 32

3.2.6. אחריות ספקי שירות באינטרנט 32

3.2.7. ראיות חסויות 33

3.2.8. שיתוף במידע מודיעיני 33

4. **האם מערכת האיזונים הקיימת בדין הישראלי בין צורכי המודיעין לבין זכויות הפרט מתאימה להתפתחות הטכנולוגית בעידן המידע? 34**

4.1. חקיקה פרטנית ביחס לאמצעי מעקב מקוון או שימוש בכלים המשפטיים הקיימים? 34

4.2. "ביטחון המדינה" – סיכול טרור או גם מניעת פשיעה וקידום אינטרסים ממלכתיים חיוניים? 38

4.3. ביקורת ודיווח על הפעלת סמכויות מעקב מקוון 38

4.4. שיקול דעת שיפוטי, מיניסטריאלי או מינהלי באישור הפעלת מעקב מקוון? 40

סיכום, מסקנות ומבט לעתיד 41

רשימת מקורות 42

מבוא

"I can't wait to join you"* *

*** תגובתו של הקצין האמריקני, רב-סרן נידל מאליק חסן, לאימם המוסלמי אנוואר אל-קואיתי במהלך התכתבות דואר אלקטרוני בין השניים בהקשר של דיון על ה"חיים שאחרי המוות", חודשים ספורים לפני שנידל פתח בירי שהביא למותם של 13 חיילים אמריקנים ו- 29 פצועים, בבסיס צבאי בטקסס[1].*

הציטוט לעיל, הודעת דואר אלקטרוני פשוטה ותמימה, בתוך מבול אין סופי של תכתובות ומיליארדי משתמשים ברשת האינטרנט, נקראת עכשיו קצת אחרת. הטכנולוגיה המודרנית מאפשרת לנו לנתח בדיעבד שיחות שהתקיימו על גבי הרשת, ותמיד, כך נראה, ישאירו אחריהן עקבות דיגיטליות. קל כעת לראות כיצד תכתובות דוא"ל בין קצין אמריקני לבין מטיף דת בעל עמדות אסלאמיות קיצוניות צריכה להביא להרמת "דגל אדום" בדמות התרעה מודיעינית כלפי מי ששוטט בפורומים רדיקליים, התבטא בצורה חשודה ונראה שחצה את הקווים לקראת קבלת החלטה קיצונית לגבי גורלו. היעדר אותו "דגל אדום" משמעותו אחת - כישלון מודיעיני לסכל פיגוע טרור קטלני. עם זאת, כמו שכל מי שבהה מול הודעת דוא"ל מבלי להבין את "כוונת המשורר" יודע, אפשר גם לקרוא את המייל הזה אחרת. מדוע שנאפשר למדינה לחדור לפרטיותו של אזרח אמריקני, פסיכיאטר וקצין צבא בכיר בשיחה שלו מול איש דת? כיצד הגיעו הרשויות לתכתובת הדוא"ל הזו? האם הדבר מצביע על כך שפעילותנו המקוונת חשופה כולה בפני המדינה? האם אין גבול להתערבות המדינה בסוד שיחו של הפרט?

התקפת הטרור ב-11 בספטמבר 2001 הביאה את ארצות הברית לתחושה לפיה ייתכן שהאיזונים בין זכויות האדם אל מול צורכי הביטחון של האומה אינם במקומם[2]. בעקבות פיגועים אלו והתקיפה הצבאית באפגניסטן, התבטא נשיא ארצות הברית לשעבר בוש: "*...the only way to pursue peace is to pursue those who threaten it...*". למדינת ישראל, איום הטרור אינו חדש שכן היא נתונה להתקפות חוזרות ונשנות של ארגונים שונים מיום היוסדה. גם היא יודעת היטב כי בטרור יש להילחם בצורה עיקשת. מזמן כבר הביעו חשש ש"*בעת מלחמה מחרישים החוקים*"[3], אך מלחמה בטרור אינה מלחמה רגילה. זו מלחמה שיש לה אויב אבל לאויב אין כתובת. לאור זאת, בחקיקה נגד טרור קיימת תמיד סכנה של גלישה לפגיעה בערכים דמוקרטיים ליבראליים ובחירויות האדם והאזרח. על מורכבות המשימה המוטלת על המחוקקים ומערכת המשפט למציאת האיזון הנדרש במסגרת הדילמה הדמוקרטית ננסה להרחיב בעבודה זו, ככל שהדברים אמורים ביחס להפעלת אמצעי מעקב מקוונים בדגש על זירת האינטרנט.

הדיון להלן יעסוק בשאלה מהם ההגבלות המשפטיות על הפעלת אמצעי מעקב על פעילות מקוונת של הפרט לצרכי סיכול טרור לפי הדין הקיים בישראל, והאם המאפיינים הייחודיים של הרשת עשויים לחייב בחינה מחדש של דין זה או את התאמתו של מערך האיזונים הקיים במרחב הקיברנטי לצרכים, לאמצעים ולאיום החדש על זכויות הפרט.

העבודה מורכבת מארבעה פרקים. הפרק הראשון יתווה רקע כללי לגבי המאפיינים העיקריים של הטרור בן זמננו והשימוש של ארגוני הטרור ברשת. מאפיינים אלו יבהירו מדוע המרחב הקיברנטי הוא מרחב אשר גורמי מודיעין מסכל מקדישים לו תשומת לב רבה בשנים האחרונות ומפעילים אמצעי פיקוח שונים על מנת לאתר מודיעין שיוביל לסיכול טרור. הפרק השני יתמקד במאפיינים הייחודיים של אמצעי המעקב המקוונים שמפעילים ב- cyberspace גופי מודיעין שונים וינסה לתת תמונה ברורה ביחס לאיומים הקיימים על זכויות הפרט נוכח אמצעים אלו. רקע תשתיתי זה יעזור לנו להבין טוב יותר בפרק השלישי את האילוצים והמגמות שמשפיעים על ההסדרים הסטטוטוריים ביחס להפעלת אמצעי מעקב מקוונים על ידי רשויות מודיעין מסכל בישראל ובדמוקרטיות בעלות מסורת של הגנה על זכויות הפרט, כפי שהדברים משתקפים לאחר פיגועי ה- 11 בספטמבר והעלאת המלחמה בטרור הבינלאומי למוקד סדר היום. בפרק הרביעי נדון במערכת האיזונים שנקבעה בדין הישראלי אל מול המשפט המשווה והמאפיינים הייחודיים של הרשת ונתמקד במספר סוגיות בולטות שיעלו בדיון שנערך.

כמי ש"בילה" למעלה מעשור מחייו בתחום האינטנסיבי של המודיעין המסכל בישראל, אני מודה על ההזדמנות לחקור נושא מרתק זה וכולי תקווה שגם הקורא ימצא בעבודה זו עניין.

---

[1] Brian Ross and Rhonda Schwartz, *Major Hasan's E-Mail: 'I Can't Wait to Join You' in Afterlif*e, abc News, November 2009 *available at*: abcnews.go.com/Blotter/major-hasans-mail-wait-join-afterlife/story?id=9130339#.UEJZYsHN_kc

[2] עמנואל גרוס, **מאבקה של דמוקרטיה בטרור – היבטים משפטיים ומוסריים**, שער עשירי, נבו הוצאה לאור בע"מ, תשס"ד-2004, עמ' 633.

[3] "*Silent enim leges inter arma*", Cicero, Pro Milone (N.H. Watts trans., Harvard Univ. Press, 5th ed. 1972) 16

1. טרור ושימוש של ארגוני טרור ברשת האינטרנט:

1.1 טרור - משמעות המונח ומאפייניו

המונח טרור הוא מונח סבוך, טעון ובעייתי להגדרה. השימוש במונח זה לתיאור תופעות קיצוניות של אלימות פוליטית הוא מאוד שכיח בעולם, אך עצם הגדרת פעולה או ארגון מסוים כ"טרוריסטים" תלויה בהשקפת עולם פוליטית או אידיאולוגית. נהוג לזהות את המונח כשימוש שיטתי ומכוון, או איום להשתמש, באלימות כדי להשיג מטרות פוליטיות, אולם הגדרה זו היא כללית ואינה מתמודדת עם הבחנה אפשרית בין פעולות טרור לבין צורות אחרות של אלימות פוליטית. נדמה שהשאלה האם לסווג פעולה מסוימת כפעולת טרור תלויה בשאלה באיזה צד של המשוואה אנו נמצאים, כיוון שפעולות המכונות בצד אחד של המתרס פעולות טרור אלימות יכולות להיות מוגדרות בצידו האחר כמאבק לגיטימי לשחרור לאומי, ומי שמוגדר בעיני אחד כטרוריסט, הינו לוחם חופש בעיני האחר[4].

הגדרה משפטית של טרור על פי הדין הבינלאומי עשויה לסייע ללחימה בטרור וליצור תשתית לעיגון מערכת חוקית נורמטיבית שתגדיר את המותר והאסור בכל מאבק פוליטי[5], אך ככל הנראה, נוכח חוסר ההסכמה הבינלאומית בנושא, לא נחקקו אמנות בינלאומיות המפרטות הגדרה כוללת של התופעה ולכן קיים לעיתים קושי להגיע להגדרה מקובלת ולהבחין בין פעולות טרור לבין פשעים אחרים. כך נוצר לעיתים מצב אבסורדי בו רוב מדינות העולם מגנות את הטרור ומתחייבות לנקוט בפעולות מנע כנגדו אך הן אינן מסוגלות להסכים באשר להגדרתו.

החלטות של גופים בינלאומיים ובראשם מוסדות האומות המאוחדות מבטאות את העמדה הבינלאומית שלפיה הטרור פוגע בזכויות האדם ובחירויותיו, ובראשן הזכות לחיים, לחופש ולביטחון, מסכן את קיומן של מדינות ושל פוליטיקה דמוקרטית מתונה ומאיים על השלום והביטחון הבינלאומיים[6].

בשיח הביטחוני והציבורי בישראל, הגדרת מעשה טרור אינה תלויה בזהות הקורבנות או באופי מטרות הטרור (צבאיות, אזרחיות וכיוצא בכך) אלא בזהות המבצע[7]. נוכח הניסיון המצטבר של מדינת ישראל במלחמה בטרור המופעל כנגדה, מופיעים גם בדין הישראלי מספר דברי חקיקה המתייחסים באופן ישיר לטרור ומנסים להגדיר מונח זה. **פקודת מניעת טרור, התש"ח-1948** מגדירה את המונח "ארגון טרוריסטי" כ*"חבר אנשים המשתמש בפעולותיו במעשי אלימות העלולים לגרום למותו של אדם או לחבלתו, או באיומים במעשי אלימות כאלה"*[8]. **חוק איסור מימון טרור, תשס"ה-2005** מגדיר אדם שהוא פעיל טרור וארגון טרור כמי שפועלים לביצוע מעשה טרור או במטרה לאפשר או לקדם ביצוע מעשה טרור[9]. עם זאת וכפי שנראה בפרקים הבאים, חלקים ניכרים מהחקיקה הביטחונית בישראל אשר מקנה לרשויות הביטחון סמכויות מעקב, אכיפה וסיכול של טרור לא מתייחסים באופן ישיר למונח "טרור" אלא נוקטים שפה עמומה יותר של "ביטחון המדינה". כך הדברים אמורים למשל בעניין ההסמכה הניתנת לרשויות הביטחון בישראל בעניין האזנת סתר, סמכויות מעקב וחיפוש וסמכויות נוספות שנבחן בפרק השלישי לעבודה זו.

---

4 עמנואל גרוס, לעיל ה"ש 2, עמ' 29.

5 ראה בועז גנור **מבוך הלוחמה בטרור: כלים לקבלת החלטות** הרצליה: הוצאת מפעלות המרכז הבינתחומי, 2003.

6 דנה בלאנדר "טרור – כואב, אבל עמום" המכון הישראלי לדמוקרטיה, **פרלמנט**, כתב עת מקוון (גליון 59) 2008 זמין לצפייה ב-www.idi.org.il/Parliament/2008/Pages/59_2008/B_59/b_59.aspx.

7 דנה בלאנדר, לעיל ה"ש 6, שם.

8 ראה הגדרת המונח "ארגון טרוריסטי" בסעיף 1 בפקודת מניעת הטרור. סעיף 8 לפקודת מניעת טרור קובע שהממשלה יכולה להכריז על חבר אנשים מסוים כארגון טרוריסטי והדבר ישמש הוכחה בכל דיון משפטי.

9 "מעשה טרור" לפי חוק איסור מימון טרור הוא מעשה המהווה עבירה, או איום בעשיית מעשה המהווה עבירה, אשר נעשה או תוכנן להיעשות כדי להשפיע על עניין מדיני, אידיאולוגי או דתי והוא נעשה או תוכנן להיעשות במטרה לעורר פחד או בהלה בציבור או במטרה לכפות על ממשלה או רשות שלטונית אחרת, לרבות ממשלה או רשות שלטונית של מדינה זרה לעשות מעשה או להימנע מעשיית מעשה. ראה סעיף 1 לחוק איסור מימון טרור.

הטרור הוא צורת אלימות ייחודית לאור הפער הקיים בין הנזק שהוא גורם בפועל לבין השלכותיו מרחיקות הלכת על חיי האזרחים ועל הפוליטיקה והמדיניות של המדינות שהוא מופעל נגדן. עוצמתו של הטרור, בהיותו אמצעי של אלימות פוליטית, נובעת בעיקר מתחושת האיום (הפועל הלטיני Terrere משמעו לגרום לרעד, לפחד ולאימה) שהוא יוצר – שכן זהו אויב ללא גבולות וללא פנים אשר בוחר את קורבנותיו באופן שרירותי. יכולתה של המדינה הדמוקרטית להתמודד עם איום הטרור היא מבחן ליכולתה לעמוד בהתחייבות החשובה והבסיסית מול אזרחיה: הגנה על ביטחונם האישי. חוסר יכולת להתמודד עם איום זה עלול לערער את הלגיטימציה של השלטון בעיני הציבור[10].

לפי דוח של המרכז הלאומי לסיכול טרור בארה״ב (National Counterterrorism Center) בוצעו בשנת 2011 למעלה מ 10,000 תקיפות טרוריסטיות אשר פגעו בכמעט 45,000 אזרחים והובילו לרצח של למעלה מ- 12,500 בני אדם ב-70 מדינות ברחבי העולם[11]. בישראל, הלחימה המתמשכת בטרור היא איום אסטרטגי מזה שנים רבות ובמיוחד החל מספטמבר 2000 עת פרצה האינתיפאדה השנייה. לפי נתוני שירות הביטחון הכללי, בעשור שבין שנת 2000-2010 נהרגו בישראל 1,178 בני אדם ונפצעו 8,022 כתוצאה מפיגועי טרור שביצעו ארגונים ופעילי טרור פלסטינים[12].

היום, בעקבות תהליכים של גלובליזציה, לובש הטרור אופי בינלאומי אשר חוצה גבולות לאומיים וגיאוגרפיים. כיום, במידה רבה באמצעות האינטרנט, שמטשטש את הגבולות ומכווץ את המרחקים וקבועי הזמן, מיקומו הגיאוגרפי של ארגון הטרור מאבד מן המשמעות שהייתה לו בעבר. בעקבות אירועי ה- 11 בספטמבר 2001, הטרור נחשב כיום לאיום עולמי והלחימה בו עומדת בראש סדר היום הציבורי של דמוקרטיות רבות ובניהן ישראל, הרואה את עצמה בחזית המאבק העולמי כנגד הטרור. המאבק בטרור מציג לפני המדינה הדמוקרטית אתגרים שמעמידים במבחן את ערכי הדמוקרטיה ומחייבים את המדינה לנקוט פעילויות מנע, בכדי לאתר ולסכל פעילות טרור לפני שזו מגיעה לפסים מעשיים וגורמת לקורבנות, אך מנגד לשמור על זכויות הפרט.

מבנה ואופי הפעילות של ארגוני הטרור משפיעים רבות על האופן שבו תוכל להתמודד דמוקרטיה ליבראלית עם סיכול טרור כנגדה. מבנה שכיח של ארגון טרור מונה את הנהגת הארגון, שתפקידה קביעת מדיניות והחלטה על הדירקטיבה הכללית שלו; דרג מבצעי, אשר מוציא לפועל את פעולות הטרור; מעטפת מבצעית, המספקת תשתית לביצוע פעולות הטרור (סיוע בהעברת מסרים ואמצעי לחימה בין הפעילים, הסתרת מפגעים, איסוף מודיעין, ועוד); ומעטפת סיוע, המקיימת מערך של תשתית אזרחית, גופי תקשורת, מוסדות חינוך, תרבות ודת, וכן מערך לגיוס פעילים ומימון. נמצא אפוא כי רוב פעילי ארגון הטרור אינם נוטלים חלק ישיר בביצוע הפעולות החבלניות עצמן, ובכך, על מנת לסכל את הטרור המופעל כנגדה, תאלץ המדינה הדמוקרטית לא אחת גם להפעיל אמצעי פיקוח חודרניים כלפי מסגרת רחבה ביותר של בני אדם, שהקשר שלהם לטרור הוא לעיתים מרוחק וגובל בהתארגנות פוליטית או חברתית לגיטימית.

המציאות מראה כי מאבק בטרור דורש לעיתים הסטת הדגש מזכויות אדם לעבר אינטרסים של ביטחון המדינה והציבור. פעילויות לאיתור, יירוט ומעקב על מנת למנוע פעולות טרור הן אינטרס ציבורי, אך הסכנה בהן כמובן היא הפגיעה בזכויות האדם ובראשן הזכות לפרטיות, הזכות לסוד השיח, הזכות לצנעת הפרט והזכות לחופש ביטוי. גם אם נסכים כי זכויות אדם אינן במה לכיליון לאומי וכי בעיתות חירום יש לתת עדיפות לצרכי ביטחון, הרי שפגיעה בזכויות האדם בשם הביטחון צריכה להיעשות במידתיות

---

10 דנה בלאנדר, לעיל ה״ש 6.

11 The National Counterterrorism Center, *2011 Report on Terrorism* (2012), *available at* www.nctc.gov/docs/2011_NCTC_Annual_Report_Final.pdf.

12 שירות הביטחון הכללי **״סקירת מאפייני הפיגועים הבולטים בעימות הנוכחי – ניתוח מאפייני הפיגועים בעשור האחרון״** (2010) ניתן לצפייה באתר השב״כ www.shabak.gov.il/publications/decade/Pages/default.aspx.

ועקרונות המשטר הדמוקרטי מחייבים שלא פעם נלחמת הדמוקרטיה כאשר אחת מידיה קשורה לאחור[13]. הקושי המובנה בין שני האינטרסים המנוגדים הללו מתחדד ויוצר דילמות קשות בכל מה שקשור להפעלת אמצעי מעקב על ידי ארגוני ביון וביטחון בישראל בסביבה החדשה יחסית בה פועלים ארגוני הטרור לקידום פעילותם – זירת האינטרנט. זירה אשר תהיה במוקד עבודה זו.

1.2. **שימוש של ארגוני טרור ברשת:**

רשת האינטרנט, המקשרת בין מיליארדי מחשבים בכל העולם הפכה לגורם רב משמעות ולזירת התפתחות כלכלית ותרבותית אדירה. עם זאת, התפתחותה האדירה של הרשת, טכנולוגיות תקשורת חדשות והנגישות למידע יוצרים יחדיו מציאות חדשה וקרקע נוחה גם לתופעות של עבריינות וטרור במרחב הקיברנטי (Cyberspace). תופעות שמוצאות ברשת אכסניה נוחה למדי. כך באופן פרדוקסאלי, הרשת המבוזרת של תקשורת בין מחשבים, שנוצרה על ידי שירותי הביטחון של ארה״ב בתחילת שנות ה-70 של המאה הקודמת על מנת להתמודד עם החשש ממלחמה גרעינית, היא זו שמשמשת כיום כר פורה לארגוני הטרור הבינלאומיים אשר רואים בארצות הברית והמערב כיעד המרכזי לטרור[14].

היום, יהא זה מפתיע מאוד למצוא ארגון טרור אשר לא מקיים נוכחות כל שהיא ברשת[15]. עם הסיבות לכך שהאינטרנט הוא מרחב אידיאלי לפעילות של ארגוני טרור נהוג למנות את הגישה הנוחה שהוא מאפשר לתקשורת מכל העולם ולהעברת מידע בהיקף אדיר; המבנה המעיין ״כאותי״ של הרשת, ללא גורם בעל שליטה מרכזית, מבנה שמחליש את כוחו של המרכז ומעניק כוח יתר לקצוות; מיעוט הרגולציה וההתערבות המדינתית; האפשרות שהוא מעניק לבעל תוכן לעצב את המסר בעצמו ללא תיווך של גופי תקשורת המונים, להגיע לקהל אדיר ולפרסם רעיונותיו בכל העולם; פרוטוקול התקשורת שהוא אנונימי במידת מה; העלות הנמוכה של קיום נוכחות ברשת וכמובן סביבת המולטימדיה שהוא מאפשר[16].

גם ישראל מתמודדת זה זמן רב עם התופעה ההולכת ונרחבת של שימוש שעושים גורמי טרור ברשת. שתי פרשיות שנחשפו על ידי שירות הביטחון הכללי בשנת 2008 יוכלו אולי להמחיש את הדברים.

בחודש יולי 2008 דיווח שירות הביטחון הכללי (להלן: השב״כ) על מעצרם של שני אזרחי ישראל וארבעה תושבי מזרח ירושלים בחשד שהיו חלק מקבוצה אסלאמית קיצונית שניסתה להקים תשתית של אל-קאעדה בישראל. ישאל השואל, כיצד הגיע השב״כ דווקא לאותם צעירים אשר ככל הנראה לא היה להם קשר קודם עם ארגוני טרור? התשובה טמונה ככל הנראה בעובדה שאחד הצעירים, סטודנט באוניברסיטה העברית בירושלים, פנה לפורום אינטרנטי המזוהה עם אל-קאעדה והתעניין לגבי האפשרות להפיל כלי טיס בו טס הנשיא האמריקני בוש, שביקר בישראל באותה תקופה. הסטודנט נעצר וחקירתו גילתה כי במקביל לגלישתו בפורום, אכן ביצע תצפית ממעונות הסטודנטים לעבר מנחת מסוקים סמוך ותיעד בטלפון הסלולארי שלו סרטים של נחיתות והמראות מהמנחת וכי במחשבי חבריו נמצאו הוראות להכנת מטעני חבלה וחומר נפץ וחומרי תעמולה של אל-קאעדה שהורדו מהאינטרנט. חודשים ספורים לפני כן, וללא קשר עם הפרשייה הקודמת ביצע השב״כ מעצר נוסף של שני תושבי רהט בחשד שהופעלו עלי ידי גורמי אל-קאעדה באמצעות האינטרנט. גם כאן, החקירה העלתה כי הקשר נוצר כשהשניים החלו לקרוא מאמרים בעלי אופי אסלאמי באינטרנט ולהיכנס לאתרים המזוהים עם אל-קאעדה והג׳האד העולמי. בין השאר

---

13 בג״ץ 5100/94 **הוועד הציבורי נגד עינויים בישראל נ׳ ממשלת ישראל**, פ״ד נג(4) 817, בעמ׳ 842 וגרוס, להלן ה״ש 2, עמ׳ 17-18, 25, 682.

14 Gabriel Weimann, www.terror.net *how modern Terrorism Uses the Internet*, United States Institute of Pace, Special Report 116 (2004), page 1-2.
ראה גם: יריב צפתי, גבריאל וימן **״טרור באינטרנט״** פוליטיקה 4 (1999), עמ׳ 45-64. ו- Tsfati, Yariv, and Weimann, Gabriel, *www.terrorism.com: Terror on the Internet,* Studies in Conflict and Terrorism (2002), 317-332.

15 Denning, D. E., *Terror's Web: How the Internet is Transforming Terrorism*, in Handbook on Internet Crime (Y. Jewkes and M. Yar, eds.), Willan Publishing (2010), page 3.

16 Weimann, לעיל ה״ש 14 בעמ׳ 2 ו- צפתי, י. וימן, ג., לעיל ה״ש 14 בעמ׳ 46.

גלשו השניים בפורומים סגורים (המאפשרים כניסה רק באמצעות שם משתמש וסיסמא) והכירו את מנהל הפורום מטעם אל-קאעדה ופעילים נוספים שביקשו להעביר לידם מידע על מקומות פוטנציאליים לביצוע פיגועים. כמענה לבקשות אלו העבירו השניים ידיעות אודות מועדון בילוי באילת, התחנה המרכזית בב״ש, תחנת הכוח של אשקלון, מרכז עזריאלי בת״א, ומקומות ריכוז של חיילים בנגב ואזורים מהם ניתן להכניס מפגעים לישראל. לבקשת מפעיליו הפיץ אחד הנאשמים ״תיקיות מידע״ באינטרנט המכילות חומרים ומדיה בנושאי ג׳האד עולמי באתרים שונים. עם מעצרם, נמצאו במחשבם של השניים תכנים רבים בנושא ייצור אמצעי לחימה שהורדו מהאינטרנט וחומר תעמולה של אל-קאעדה[17].

שתי הפרשיות הנזכרות לעיל מצביעות על השימושים השכיחים אשר מבצעים ברשת ארגוני טרור. בפרק זה ננסה למפות את שימושים אלו. באופן קטגורי נסווג את פעילות הטרור ברשת למספר ענפים אשר משיקים ולעיתים חופפים אחד עם השני: א. השימוש ב״אתרי טרור״; ב. איסוף מודיעין לפעילות טרור; ג. טרור קיברנטי (Cyber-terrorism); ד. נסיים את פרק זה בסקירת השימושים שעושים גורמי הטרור ברשת כאמצעי תקשורת בשירותיהם. סקירה זו תאפשר לנו לראות כי הרשת מהווה כיום אמצעי מרכזי להעברת מסרים בין גורמי הטרור וככלי לניהול מידע ובהמשך נראה כי מרכזיות זו הופכת את הרשת ליעד חשוב לאיסוף חומר מודיעיני על ידי גורמי מודיעין מסכל למטרות ביטחון ומאבק בטרור.

1.2.1. <u>שימוש ב״אתרי טרור״:</u>

הרשת מהווה בית חם לאלפי אתרים שכאלו אשר נבנו, מופעלים או ממומנים על ידי גורמי טרור[18]. בעלות מינימאלית, ארגון טרור יכול להקים אתר המזוהה או שאינו מזוהה איתו ודרכו להפיץ תכנים ומסרים בשפות שונות שככל הנראה בכל מדיום אחר לא הייתה לו דרך להפיץ, ולהגיע לקהל אדיר שלא הייתה לו דרך אחרת להגיע אליו אלמלא היה נעשה שימוש באינטרנט. לפי **פרופ׳ גבי וימן**, התופעה של שימוש באתרי אינטרנט על ידי ארגוני טרור היא דינאמית ביותר, כאשר אתרים חדשים צצים חדשות לבקרים, ״נעלמים״ או משנים כתובת URL בתכיפות גבוהה. כיום, כמעט כל ארגוני וקבוצות הטרור הפעילים מתחזקים אתר או מספר אתרים בשפות שונות אל מול קהלי יעד שונים[19]. מהזווית ״הישראלית״ ניתן לציין כי חלק מהאתרים של ארגוני הטרור האסלאמיים הרדיקאלים הינם בעלי אופי חדשותי מובהק ומהווים צינור מידע ביחס לפעילות ארגון הטרור אך גם מפיצים בגלוי מסרי שנראה כלפי ישראל והמערב, מטפחים את מיתוס השהידים ומשבחים את האלימות והטרור במסגרת הג׳האד[20]. נרחיב כעת בקצרה על השימושים אשר עושים ארגוני הטרור באתרי הטרור:

<u>א</u>. **לוחמה פסיכולוגית**. שימוש של גורמי טרור בלוחמה פסיכולוגית על מנת להפיץ מידע שגוי או מגמתי במטרה לאיים ולזרוע פחד ומורא בקרב האזרחים במדינת היעד לטרור ולסייע ללחץ על מקבלי ההחלטות אינו תופעה חדשה. עם זאת, ראויה לציון יכולתם של ארגוני טרור להצליח בעקביות לרתום לטובתם את המהפכה התקשורתית שהביאה ה- World Wide Web ולהשתמש במדיה החדשה במסגרת המלחמה על התודעה[21]. כך למשל, בעלות מינימאלית גורמים מספר אתרים המקושרים לאל-קאעדה לנזק עצום

---

17 מרכז המידע למודיעין ולטרור, **מבזק טרור ואינטרנט**, המרכז למורשת המודיעין (מל״מ), פורסם ב- 20 ביולי 2008.

18 לצורך עבודה זו נכנה אתרים אלו כ״אתרי טרור״ למרות שברשת קיימים גם אתרים אשר תומכים בתכנים ומסרים הקשורים לפעילות טרור אך אינם ממומנים, או מופעלים על ידי גורמי טרור.

19 Weimann, לעיל ה״ש 14 בעמ׳ 4-2. אתרים אלו, יספקו בד״כ היסטוריה של הארגון ופעילותו, סקירה מפורטת של הרקע החברתי והפוליטי שלו, ביוגרפיות של הנהגת הארגון, מייסדים ופעילים בולטים שלו ותיאור מטרותיו הפוליטיות והאידיאולוגיות.

20 להרחבה בעניין זה ראה הסקירות המעניינת - מרכז המידע למודיעין ולטרור, **האינטרנט בשימוש ארגוני הטרור: תשתית אתרי האינטרנט של הג׳האד האסלאמי בפלסטין וספקיות השירותים בהן מסתייע הארגון**, המרכז למורשת המודיעין (מל״מ), ספטמבר 2007, עמ׳ 2-1; מרכז המידע למודיעין ולטרור, **מבזק טרור ואינטרנט: חמא״ס שידרגה לאחרונה את אתר האינטרנט של גדודי עז אלדין אלקסאם**, המרכז למורשת המודיעין (מל״מ), יוני 2008.

21 מרכז המידע למודיעין ולטרור, **האינטרנט כזירת מאבק עם ארגוני הטרור: השימוש שעושים חזבאללה וחמאס באינטרנט במלחמה על התודעה ודרכי ההתמודדות עם התופעה**, המרכז למורשת המודיעין (מל״מ), יולי 2007, עמ׳ 3-1, 53. להרחבה, ראה גם לקט מרכז המידע למודיעין ולטרור, **המלחמה על התודעה במסגרת העימות בין ארגוני הטרור לבין ישראל כמקרה מבחן**, המרכז למורשת המודיעין (מל״מ), מאי 2007.

לארה״ב כאשר הם מעבירים ברשת הודעות אודות מתקפות מתוכננות על מטרות אמריקאיות. הודעות אלו יזכו לרוב לכיסוי תקשורתי נרחב, יצרו חשש בקרב אזרחים ומוסדות אמריקאים ויגרמו לנזק כלכלי[22].

ב. **פרסום ותעמולה**. האינטרנט הרחיב משמעותית את היכולת של טרוריסטים להשיג פרסום ולנהל את ״תיאטרון הטרור״ שלהם[23]. אם בתקופה שלפני האינטרנט היכולת של ארגון טרור להשיג פרסום לטענותיו היה תלוי במשיכת תשומת ליבם של גופי תקשורת המונים, שכפופים לרגולציה, צנזורה ושיקולי עריכה, הרי שבעידן האינטרנט, ארגון הטרור כבר לא זקוק לאותם מתווכים ויכול לעצב את המסר שלו בעצמו ולהעבירו בתפוצה אדירה באמצעות טכנולוגיה אינטראקטיבית כגון תמונות, סרטים, מולטימדיה ועיצובים גרפיים מיוחדים, וכמובן אפשרות ״לשוחח״ עם גולשים on-line[24] על מנת ליצור עניין ציבורי בפעילותו ולהגביר את האהדה והתמיכה למניעיו.

הרשת מאפשרת מדיום ישיר בין הטרוריסט לקהל היעד שלו, בין אם מדובר בגורמי תקשורת או צרכנים ישירים באזור הפעולה של הגורם הטרוריסטי או בקהילה הבינלאומית, ומקלה על הטרוריסטים להעביר את המסר שהם מבקשים להעביר וזאת תוך עקיפת המגבלות המוטלות על ארגוני הטרור לפעול באותן מדינות[25]. באופן זה ניתן לציין כי חלק גדול מאתרי האינטרנט הרשמיים והלא רשמיים של חזבאללה, חמא״ס, כהנא-חי וארגוני טרור נוספים הם בשפה האנגלית ובשפות נוספות (רוסית, צרפתית וגם עברית) על מנת לפנות באופן ישיר לקהל בינלאומי. כמו כן, ניתן למנות גם את השימוש שעושים ארגוני טרור אסלאמיים רדיקליים ברשתות חברתיות כגון Facebook, You-Tube ואתרים אחרים על מנת להעביר חומר תעמולה או מסרים התומכים באידיאולוגיה הטרוריסטית כגון פרסום מסרי שנאה נגד ישראל והמערב[26].

ג. **גיוס מימון ותרומות**. אתרים רשמיים ולא רשמיים של ארגוני טרור מכילים ברוב המקרים מספרי חשבונות בנק בהם ניתן להפקיד תרומות במסווה של צדקה או פעילות חברתית, אך בחלק מהמקרים גופי מודיעין מזהים כי הכספים המועברים אל אותם ארגוני צדקה מנוצלים באופן ברור לפעילות טרור[27]. גם הונאות רשת ופשיעה מקוונת מאפשרים לארגוני הטרור השונים לגייס כספים באמצעות האינטרנט[28].

ד. **גיוס תומכים ופעילים לשירות הטרור**. הגלובאליות של הרשת מאפשרת כיום לגורמי טרור להגיע בקלות לקהל יעד של תומכים בכל מקום על הגלובוס[29]. בהקשר הישראלי, גורמי מודיעין מודאגים יותר ויותר מחדירה של אידיאולוגיית הג׳יהאד העולמי לרצועת עזה, יהודה ושומרון ואף ערביי ישראל כמו גם

---

22 Weimann, לעיל ה״ש 14 בעמ׳ 5. בהקשר זה ראוי לציין גם את התופעה של פרסום צילומי זוועה שמועלים לרשת האינטרנט על ידי גורמים טרוריסטים שונים, כגון סרטי עריפת ראשים (כמו זו של העיתונאי האמריקני ניקולס ברג בעיראק) או תמונות שרידי גופות (כמו במקרה של החייל הישראלי איתמר איליה ז״ל לאחר אסון השייטת בלבנון).

23 לפי גבי ויימן המונח תיאטרון הטרור ממשיל את הטרור לתיאטרון ואת התקשורת כ״במה״ ומבטא את ההנחה כי פעולת טרור ללא הד תקשורתי משמעותי היא חסרת ערך. גבי ויימן ״תיאטרון הטרור: אתגרה הקשה של הדמוקרטיה״ בתוך: כהן אלמגור ר׳ (עורך) **סוגיות בדמוקרטיה הישראלית** (1999), עמ׳ 47.

24 Weimann, לעיל ה״ש 14 בעמ׳ 6. ראה גם מרכז המידע למודיעין ולטרור, הערה 26 לעיל, שם.

25 יצויין בהקשר זה כי ארגוני טרור איסלאמים כגון חזבאללה וחמא״ס מנצלים את הנגישות הגבוהה ולעיתים גם הבלעדית שיש להם על המידע המופץ מדרום לבנון או מרצועת עזה ולאור זאת המידע המופיע באתרים של אותם ארגוני טרור מהווה לעיתים מקור מרכזי בדיווח וסיקור חדשותי בזירה הבינלאומית, באופן זה משפיעים ארגוני הטרור גם על התוכן התקשורתי שיפורסם ביחס לנושאי הסיקור הרלוונטיים.

26 מרכז המידע למודיעין ולטרור, **טרור ואינטרנט: הכרזה על ״אנתיפאדה אלקטרונית״ נגד ישראל באמצעות רשת פייסבוק באינטרנט**, המרכז למורשת המודיעין (מל״מ), מרץ 2010, עמ׳ 1-4.

27 Weimann, לעיל ה״ש 14 בעמ׳ 7. ראה גם
Michael Jacobson, *Terrorist Financing and the Internet*, Studies in Conflict & Terrorism, 2010, page 356 *available at*: www.tandfonline.com/doi/pdf/10.1080/10576101003587184
בהקשר ״הישראלי״, ארגון הטרור חזבאללה עושה שימוש נרחב באתרי האינטרנט בבעלותו על מנת לעודד תרומות וגיוס כספים למוסדותיו. ראה גם לקט מרכז המידע למודיעין ולטרור, **מימון הטרור: חזבאללה מגייס תרומות עבורו ועבור מוסדות הקשורים עימו באמצעות אתרי האינטרנט שלו**, המרכז למורשת המודיעין (מל״מ), מאי 2008.

28 Denning, D. E., לעיל ה״ש 15, עמ׳ 19.

29 החוקרת Denning טוענת כי לאינטרנט תרומה משמעותית להפצת האידיאולוגיה של אל-קאעדה עד כדי כך שהתנועה האסלאמית הקיצונית שמזוהה עם הארגון לא הייתה יכולה להתקיים ללא האינטרנט אשר מאפשר לתומכי הרעיון לקיים ״רשת חברתית״ מבוזרת ברחבי העולם להפצת האידיאולוגיה ולגיוס תמיכה ומשאבים. Denning, D. E לעיל ה״ש 15, עמ׳ 13.

גיוס והפעלה על ידי גורמים אלו בעיקר באמצעות הפורומים באינטרנט[30]. דומני שהדוגמאות של שתי הפרשיות שחשף השב״כ בשנת 2008 אשר הובאו לעיל ממחישות את הדברים היטב.

ארגוני הטרור מפעילים באתריהם וברשתות חברתיות שונות פורומים ומנהלים חדרי שיחה מקוונים (צ׳אט) עם גולשים. דוח של הסנאט האמריקאי ממאי 2008[31] מצביע בהקשר זה על תהליך רדיקליזציה שעלול לעבור גולש באתרים אסלאמיים קיצוניים ומציין מספר מקרים בהם תכננו אזרחים אמריקאים פיגועי טרור בארה״ב בעקבות תהליך רדיקליזציה שעברו, בו מילא האינטרנט תפקיד מרכזי. לפי הדוח, גם במקרים בהם לא ניתנה למתכנני הפיגועים הוראה מפורשת מהארגון לבצע פיגועי טרור היוו האתרים השראה לפיגועים אלו. אותם פורומים מהווים גם מאתר של מגויסים פוטנציאליים לארגון הטרור. באופן זה, ארגוני טרור מבצעים מעקב אחר תנועת הגולשים באתריהם, מסבים תשומת לב למשתתפים פעילים במיוחד בפורומים ובאתרי הארגון ויוצרים איתם קשר אשר מוביל ברוב הפעמים לדרישות אופרטיביות לסיוע לארגון בין אם בפעילות הסברתית, תקשורתית, מבצעית או אחרת[32].

ארגוני טרור משתמשים גם ברשתות חברתיות כגון Facebook על מנת ליצור קשר באופן ישיר עם ישראלים בארץ ובחו״ל במטרה לגייסם לפעילות ארגוני טרור[33].

<u>ה</u>. **שיתוף במידע מבצעי**. דוח הסנאט האמריקאי מציין כי האינטרנט משמש מעין תחליף וירטואלי למחנות האימונים עבור ארגוני הטרור וכי דרכם נעשית הכשרה של פעילים חדשים ברמה האידיאולוגית והמבצעית. ואכן, ברשת ניתן למצוא אלפי אתרים המדריכים כיצד להכין מטעני נפץ, רקטות ורעלים שונים. חיפוש פשוט של מילות מפתח כמו ״מדריך״ ו-״טרור״ במנועי החיפוש מפנה בקלות למדריכים מקוונים הניתנים להורדה ללא כל הגבלה[34]. אתרי ארגוני החמאס ושאר ארגוני הטרור ברצועת עזה משתפים מידע באופן גלוי באתריהם בנוגע לייצור והפעלת רקטות ונשק תלול מסלול לעבר ישראל, מדריכים להקמת תאי טרור, שמירה על ביטחון הקבוצה מפני חדירה מודיעינית ישראלית ועוד[35]. המתעניין יכול למצוא קבצי הדרכה, מפות, תמונות, סרטוני וידאו ועוד. מידע זה מופיע לא אחת באופן גלוי לחלוטין, ללא שום הצפנה או קידוד.

1.2.2. <u>**איסוף מל״מ (מודיעין לקראת מבצע):**</u>

ארגוני הטרור מבצעים שימוש נרחב באינטרנט במטרה ללמוד על מטרות פוטנציאליות לתקיפה. ארגוני טרור יכולים ללמוד בקלות על המבנה הפנימי של מטרות לתקיפה כמו שדות תעופה, נמלים וכיוצא בכך באמצעות חיפוש פשוט באינטרנט, לאסוף מודיעין בזמן אמת באמצעות מצלמות אינטרנט במקומות הומי אדם (למשל ברחבת הכותל המערבי, בכיכר Times בניו-יורק, ועוד) ואף ללמוד את נקודות התורפה של אותם מטרות באמצעות תוכנות הזמינות לכל[36], כגון Google Earth ו- Google Street-view. המידע הזמין ברשת, מהווה נתח מרכזי מהמידע המשמש את ארגוני הטרור, ואלו יכולים להגיע אליו בקלות

---

30 אתר חדשות ערוץ 2 ״**יובל דיסקין: יכולות טרור אינטרנטי מאיימות על מדינות שלמות**״ גלובס 1.11.2010 www.globes.co.il/news/article.aspx?did=1000597974.

31 United States Senate Committee on Homeland Security and Governmental Affairs, *Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat* (2008) *available at:* hsgac.senate.gov/public/_files/IslamistReport.pdf.

32 Weimann, לעיל ה״ש 14 בעמ׳ 8. מקרה מפורסם, שמאוזכר אצל וימן הינו המקרה של זיאד חליל, אמריקני ממוצא פלסטיני, סטודנט למדעי המחשב במכללת קולומביה שבמיזורי. חליל הפך לאקטיביסט מוסלמי ובשנת 1995 ונוכח פעילותו הרבה באתרים איסלאמים קיצוניים אלו, פעילי אל-קאעדה יצרו קשר עימו ״גייסו״ אותו והפעילו אותו כ״קצין הרכש״ של אל-קאעדה בארה״ב.

33 ראה סקירת שירות הביטחון הכללי ״**גיוס אזרחים ישראלים על ידי גורמי טרור ברשת האינטרנט**״ מאי 2009, www.shabak.gov.il/publications/study/Pages/internetTerror.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93 וסקירת שירות הביטחון הכללי ״**פעילות חזבאללה מול ערביי ישראל**״ מאי 2010, www.shabak.gov.il/publications/study/Pages/hizballahdecade.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93.

34 Weimann, לעיל ה״ש 14 בעמ׳ 10. Denning, D. E לעיל ה״ש 15, עמ׳ 16.

35 מרכז המידע למודיעין ולטרור, לעיל ה״ש 21.

36 Weimann, לעיל ה״ש 14 בעמ׳ 7.

באמצעות מנועי חיפוש ואפשרויות תרגום שמציעה הרשת לכל גולש. בזירה הישראלית, ארגוני הטרור סורקים באופן שוטף את האתרים הישראלים הבולטים, הפורומים בנושאי צבא וביטחון ורשתות חברתיות בהם פועלים ישראלים, במטרה לאסוף מידע מסווג אודות מטרות ויעדים ביטחוניים בישראל[37].

1.2.3. סייבר טרור (טרור מקוון):

רשת האינטרנט יכולה לשמש לא רק ככלי עקיף לארגוני הטרור לקידום מטרותיו במרחב הפיזי אלא גם ככלי נשק ישיר במימד הקיברנטי באמצעות תקיפות של טרור מקוון (Cyber-terrorism). כמעט כל מערכת הקשורה לתפקיד תקין של משטר מבוססת כיום על תקשורת בין מחשבים, ובכלל זאת מערכות של תשתיות חיוניות כגון תחבורה, חשמל, מים, נפט וגז, לוויינים, גופי תקשורת ומערכות ביטחוניות וממשלתיות. מדינות אשר תלויות יותר בתשתית המבוססת על תקשורת בין מחשבים יהיו חשופות יותר לחדירה למערכות אלו, לשיבושם ואף לשיתוקם המוחלט על ידי גורמים בלתי מורשים, ובכלל זה גורמי טרור.

סייבר טרור הוא מונח שסובל מחוסר בהגדרה מובחנת ומוסכמת, אך באופן כללי, המינוח מתייחס למתקפה של קבוצות לאומיות או ארגוני טרור כנגד מערכות מידע אשר מביא לתוצאות אלימות כנגד מטרות אזרחיות ופגיעה בתשתיות קריטיות[38]. ארגוני הטרור החלו לפתח יותר ויותר התעניינות בתקיפה במימד זה לאור היתרונות היחסיים שהוא מקנה כמו היכולת לשנות את מאזן הכוחות הא-סימטרי בין ארגוני הטרור ליריביהם[39]. כך, מדינות מפותחות, כמו ארצות הברית או ישראל, נמצאות במציאות בעייתית כשהיתרון נמצא כמעט תמיד בצד של התוקף וכש"מחיר הכניסה" לעולם המלחמה המקוונת הינו נמוך מאוד וההרתעה היא חלשה אם בכלל קיימת נוכח האפשרויות המוגבלות להגיב עליה[40].

החסרונות היחסיים של תקיפה קיברנטית הם מגבלות הפעילות במרחב הקיברנטי הגלוי של רשת האינטרנט אשר מאפשרים לגורמי המודיעין לזהות התנהגויות חשודות ברשת ולהתגונן מפני איומים ספציפיים[41].

גם בישראל, השיח בנושא תופעת הסייבר טרור לא ניזון רק מדיונים תיאורטיים אלא גם מכורח המציאות בה מתרחשות באופן תדיר תקיפות כנגד אתרי אינטרנט ישראלים וחברות אשראי[42]. פרסומים גלויים גם הצביעו על מעורבות אקטיבית של ישראל בלוחמת הסייבר בפרשת תולעת הסטקסנט (Stuxnet) ששיבשה את פעילות הגרעין באיראן[43] ותוכנת הריגול "להבה" שנועדה לאסוף מידע מקוון ממחשבים איראנים[44].

---

37 סקירת שירות הביטחון הכללי, לעיל ה"ש 33.

38 קרין תמר שפרמן "**פני הטרור העתידיים – סייבר-טרור**" המכון הישראלי לדמוקרטיה, כתב עת מקוון (גליון 59) 2008, עמ' 1-2 www.idi.org.il/Parliament/2008/Pages/59_2008/G_59/g_59.aspx. ראה גם: Denning, Dorothy E., *Cyberterrorism*, 2000 available at: www.cs.georgetown.edu/%7Edenning/infosec/cyberterror-GD.doc
יצויין כי בשיח האקדמי נעשה שימוש במספר מושגים והגדרות המבחינים בין סייבר טרור לבין סוגי תקיפות אחרים של מאגרי מידע ומחשבים, כגון סייבר-ונדליזם (Cybervandalism), פשיעת סיבר (Cyber-Crime), לוחמת סיבר (Cyberwar), סייבר ריגול (Cyberespionage), אך בפועל, כשמתרחשת תקיפת מחשבים קשה מאוד לקבוע באיזו תופעה מדובר. ראה מרים דאן קוולטי "על המשכיות ושינוי בשיח על איומי הסייבר" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 11, עמ' 13-14. לסקירה מקיפה של מושגים מרכזיים על לוחמה במרחב הקיברנטי ראו: טבנסקי ליאור "לחימה במרחב הקיברנטי: מושגי יסוד" **צבא ואסטרטגיה**, כרך 3, גיליון 1 (2011), עמ' 65-80.

39 אמיר לופוביץ "לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 41, עמ' 43.

40 זאת משום שמאפייני המרחב הקיברנטי מקשים על ההבחנה בין פגיעה מכוונת לתקלה, ועל האפשרות לזהות את התקיפה, את מקורה ואת זהות התוקף ולייחס פעולה לגורם מסוים (attribution). רם לוי "מרחב הלחימה החמישי" **אתר IsraelDefence**, 16 לדצמבר 2011, www.israeldefense.co.il/?CategoryID=512&ArticleID=1470. ראה גם אמיר לופוביץ, להלן ה"ש 39, עמ' 43.

41 יורם שוייצר, גבי סיבוני ועינב יוגב "המרחב הקיברנטי וארגוני הטרור" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 33, עמ' 34-37. להרחבה ראה גם: שמואל אבן ודוד סימן-טוב "**לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**" המכון למחקרי ביטחון לאומי, מזכר 109, יוני 2011, עמ' 18-23.

42 כגון תקיפת אתר האינטרנט של עיריית ת"א על ידי גורמים תורכיים בעקבות אירועי משט המרמרה לעזה בשנת 2011, או הפצחן (האקר) 0xOmar שהקפיץ את מדינת ישראל בתחילת 2012 כשפרסם את פרטי כרטיסי האשראי של ישראלים רבים.

43 ראה מרטין ס' ליביקי "השימושים האסטרטגים בעמימות במרחב הקיברנטי" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 3, עמ' 4-5.

1.2.4. **הרשת כאמצעי תקשורת בשירות ארגוני הטרור:**

מבנה חלק מארגוני הטרור - תאים עצמאיים נטולי שרשרת פיקוד מקשרת או תיחום גיאוגרפי - מתאים ככפפה ליד למבנה המבוזר והאנרכיסטי של הרשת ומאפשר לתאים או לקבוצות מבודדות לקבל הנחיות, להעביר מסרים וליצור קשר עם מפעיליהם ועם תאים מקושרים ומסונפים אחרים[45]. האינטרנט מהווה אמצעי תקשורת מרכזי במבנה מרושת מעין זה. באמצעות השימוש באינטרנט יכולים ארגוני הטרור לדלג מעל מחסומים גיאוגרפיים ואחרים ולעשות שימוש ברשת כגורם לתקשורת מבצעית תוך שימוש בכלים מגוונים ובהם כלי הצפנה זמינים. היום תקשורת מבוססת מחשבים מאפשרת לפעילי טרור לשוחח באמצעות טלפוניית רשת (VoIP), לבצע שיחות וידאו ולתקשר באמצעות מסרים מידיים (IM) במהירות ובאופן אפקטיבי ולקבל או להעביר תכנים מורכבים ומגוונים (קבצי מידע, אודיו, וידאו, תוכנות ועוד). דוגמאות בהקשר זה ישנן למכביר: תאום המתקפה של אל-קאעדה ב-11 בספטמבר 2001 נשען כמעט באופן בלעדי על האינטרנט[46], וכך גם הקשר והאכוונה של אל-קאעדה עם המורדים בעיראק ובאזורים נוספים בעולם. האינטרנט יכול לשמש גם פלטפורמה נוחה להעברת פקודות מוצפנות באתרים ודפי אינטרנט תמימים לכאורה תוך שימוש באמצעי הצפנה נגישים לשוק או במילות קוד שהוסכמו בין הפעילים.

דוחות שפרסם השב״כ מצביעים על כך שמספר לא מבוטל של אזרחי ישראל או תושבי השטחים הורשעו לאחר שהופעלו באמצעות האינטרנט על ידי מפקדות ארגוני הטרור ב״חוץ״ לאסוף מודיעין לפעילות טרור, לצילום אתרים צבאיים ואזרחיים, כשהכוונת הטרור, והקשר המבצעי עם תאי הטרור בשטח, נעשה כיום באמצעות האינטרנט[47]. כך למשל ראוי פואד סולטאני תושב טירה שגויס לחזבאללה והעביר למפעיליו מידע על הרמטכ״ל גבי אשכנזי, עימו נהג להתאמן בחדר הכושר, התבקש לאסוף מידע על אישים בכירים נוספים ועל בסיסי צה״ל ולהעביר את המידע באמצעות האינטרנט דרך הרשת החברתית Facebook[48].

האינטרנט, אם כן, תופס מקום מרכזי ביותר כאמצעי להעברת מסרים וניהול מידע גם אצל ארגוני הטרור. בפרק הבא נראה כיצד מרכזיות זו הופכת את הרשת ליעד חשוב המהווה מקור לחומר מודיעיני הנאסף על ידי גורמי מודיעין מסכל. הפרקים הבאים יבחנו כיצד מגיבים גורמי מודיעין מסכל בישראל ובעולם המערבי לאיומים השונים שהוצגו לעיל ובמיוחד בכל הקשור בניתור ובפיקוח על התקשורת בין מחשבים באינטרנט והלחימה בטרור בזירה זו. לצד הדיון הטכנולוגי והמשפטי, ננסה לעמוד בקצרה גם על השאלה החשובה של המחיר שמדינת ישראל משלמת בהקשר של הגנה על זכויות וחירויות הפרט שעה שהיא מקיימת מעקב וניטור שכזה. השאלות המשפטיות שמעוררת הלחימה בטרור ביחס לזכויות אדם אינן חדשות, וגם לפני עידן האינטרנט הגבילו ממשלות מערביות זכויות אדם נוכח הצורך להילחם באיומי הטרור. הדיון שנקיים בפרקים הבאים ינסה להתמקד בעיקר בשאלה האם הטכנולוגיה המתקדמת בעידן המידע, אשר מאפשרת למדינה לנטר, לסקור ולנתח אינפורמציה בהיקף חסר תקדים, משנה את מידת האיזון הנהוגה כיום בין זכויות הפרט לבין זכות הדמוקרטיה להגן על עצמה.

---

44 ״מטרת וירוס להבה: השגת רישומים טכניים מאיראן״ **YNET** 5 ליוני 2012, www.ynet.co.il/articles/0,7340,L-4238369,00.html, ו ״ישראל וארה״ב ביחד: מלחמת סייבר נגד איראן״ **YNET** 1 ביוני 2012 www.ynet.co.il/articles/0,7340,L-4236972,00.html.

45 Weimann, לעיל ה״ש 14 בעמ׳ 9.

46 Weimann, לעיל ה״ש 14 בעמ׳ 9 ו- 11. וימן מאזכר את הודעת הדוא״ל האחרונה ששלח מוחמד עט׳ה ל- 18 פעיליו שהשתתפו עימו בפיגועי הטרור ב- 11 בספטמבר כדוגמא למסר מקודד תמים לכאורה שנועד לחמוק מתחת לעיניהם הפקוחה של גורמי המודיעין האמריקאים: ״The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering״. האזכור של הפקולטות השונות מצביע לכאורה על יעדי התקפת הטרור.

47 להרחבה ראה גם מרכז המידע למודיעין ולטרור, להלן ה״ש 20, עמ׳ 1.

48 סקירת שירות הביטחון הכללי, להלן ה״ש 33.

2. המאפיינים המיוחדים של אמצעי המעקב המקוונים ברשת

בפרק הקודם סקרנו את השימושים השונים של ארגוני הטרור ברשת האינטרנט אשר מחייבים את ארגוני המודיעין לעמוד על משמרתם בניטור ופיקוח מודיעיני על מנת לאתר ולסכל פעילות טרוריסטית מקוונת. הדיון בעבודה זו יתמקד בהיבטים המשפטיים של אמצעי המעקב המקוון ברשת לצרכי ביטחון וסיכול טרור. כפי שראינו, חלק מפעילות הטרור ברשת נעשית "בתווך הגלוי" של רשת האינטרנט ובכלל זאת, גורמי טרור, המפעילים לוחמה פסיכולוגית, מקדמים גיוס תומכים ומימון ופועלים לשיתוף ידע מבצעי באמצעות אתרים הנגישים לכל. המעקב המודיעיני אחר פעילות טרור שכזו מכונה "אוסינט" (Open Sources Intelligence) – איסוף מודיעין ממקורות גלויים, והוא איננו מאתגר במיוחד מבחינה מודיעינית, שכן אופן הפקת המידע הוא פשוט יחסית ונוכח העובדה שככלל הוא אינו מעורר סוגיות ייחודיות אינני סבור כי ראוי להקצות לו דיון נפרד במסגרת עבודה זו. לאור מרכזיות הרשת כאמצעי תקשורת בשירות ארגוני הטרור, אבקש לשים את הדגש במקום בו מתחוללת עיקר המלחמה המודיעינית במרחב הקיברנטי. במלחמה זו, מנסים ארגוני המודיעין להתחקות אחר הפעילות המקוונת של פעילי טרור, אשר עוסקים בתכנון, הכוונת וביצוע פעילות חבלנית עוינת קטלנית. בפרק זה נסקור את המאפיינים המיוחדים של אמצעי המעקב המודיעיני המקוון שיהוו בסיס לדיון חשוב בנוגע לזכויות האדם שעומדות מנגד בדמוקרטיה ובנוגע למערכת האיזונים הקיימת בדין הישראלי ובמדינות מערביות נוספות בין צורכי המודיעין לבין זכויות הפרט.

כאמור לעיל, האינטרנט הוא אמצעי מרכזי להעברת מסרים וניהול מידע. כפועל יוצא, ארגוני המודיעין, אשר בשגרה מבססים את עיקר תוצריהם על השגת חומר מודיעיני באמצעים טכנולוגיים ובעיקר בסיגינט[49] מסבים בשנים האחרונות יותר ויותר תשומות להפקת מודיעין איכותי לסיכול טרור באמצעות ניטור ומעקב של מסרים המועברים ברשת מתוך ידיעה שיעדי המודיעין, ככל האדם, עושים גם הם שימוש ניכר באמצעי התקשורת האינטראקטיביים אותם הרשת מאפשרת, ומשתמשים במחשבים לנהל מידע.

המאפיינים המיוחדים של איסוף מודיעיני בסביבה הטכנולוגית המודרנית מאפשרים לארגוני המודיעין מספר יתרונות בולטים: ראשית, כל פעולה מקוונת מותירה "עקבות דיגיטאליים". משלוח דוא"ל, גלישה, העלאת/הורדת קבצים, כתיבת מסמכים או תוכנות וכו', כל פעולות אלו נרשמות בקבצים שונים של המחשב ושל השרתים המעורבים בתקשורת. כך למשל דיון בצ'ט או דוא"ל יוצר תרשומת של תוכן השיחה, המועד בו התקיימה, מיהם הדוברים, המחשבים והשרתים שדרכם בוצעה השיחה וכדומה. שנית, ברשות ארגוני מודיעין אמצעי איסוף מקוונים המאפשרים עושר והיקף מידע חסר תקדים: דוא"ל, מסרים מיידים, וידאו, גישה לשיחות שמבצע היעד באמצעות האינטרנט (VoIP), נתונים על גלישה ופעילות באתרי אינטרנט, נתוני מחקר תקשורת על הרשתות בהן נעשה שימוש המאפשרים לבצע כריית מידע (Data Mining) שתחשוף דפוסי התנהגות שהגולשים אינם מודעים אליהם, ועוד[50].

מנגד, יתרונות אלו עלולים ליצור איום חדש על חירויות הפרט. איום זה נובע מכך שאמצעי האיסוף החודרניים מופעלים כלפי הציבור בכללותו ובפועל מעמידים את הפרט ומעשיו במצב של שקיפות (או שקיפות בפוטנציה) ועלולים ליצור פגיעה בפרטיות בהיקפים חסרי תקדים. דמינו לעצמכם מה יוכל ללמוד עליכם מאן דהוא אילו הייתה ניתנת לו גישה לכל מסמך, תמונה או סרטון השמור אצלכם במחשב האישי

---

[49] מודיעין אותות אלקטרוניים (Signals Intelligence). קטגוריה של מודיעין ובה נכללים גם מודיעין התקשורת (קומינט - Communication intelligence - מידע המתקבל מתעבורה של אותות כגון שיחות טלפון, פקס, דואר אלקטרוני, מסרים מידיים וכיוצא באלו המכילים תוכן), המודיעין האלקטרוני ומודיעין האותות. סיגינט נחשב למקור המודיעיני הנפוץ ולרוב גם האיכותי ביותר בעקרב ארגוני מודיעין מובילים בעולם. מובא בשמואל אבן ודוד סימן-טוב, להלן ה"ש 41, עמ' 79.

[50] אודי איינהורן ואח', נייר עמדה "**לוחמה בטרור בזירת המידע**", המרכז למשפט וטכנולוגיה, עורכים: ניבה אלקין-קורן, מיכאל בירנהק, תשס"ב-2002, עמ' 53-54.

ואפשרות לתפעל בעצמו את המצלמות והמיקרופונים של אותו מחשב, לתעד את כל הקלדותיכם, לעיין בכל תכתובת דוא״ל, מסר מיידי, צ׳אט או פורום ולבחון באלו אתרים גלשתם. נוכח העובדה שתמסורות של יעדים מודיעיניים עלולות להיבלע בתמסורות תמימות של גורמים שאינם קשורים לפעילות בלתי חוקית (שהרי דוא״ל בין פעילי טרור לא תמיד נושא את הכותרת – *״תזכורת לגבי פיגוע התאבדות של אל-קאעדה בטווח הזמן המיידי״*), הרי שמעקב מקוון כרוך במקרים רבים גם באיסוף מידע על מי שאינם חשודים כלל, וחיפוש במחשב ובתכתובותיו המקוונות של אדם כרוך בפגיעה חמורה בפרטיות גם בשל העובדה שמסמכים רלוונטיים לחקירה ומסמכים אישיים נמצאים זה לצד זה. יתרה מכך, פעילות מודיעינית מבוצעת לא אחת על גבי ציוד ושרתים של גורמים מסחריים ולעיתים אף באמצעותם. במיוחד הדברים אמורים ביחס לפעילות גולשים באינטרנט אשר ניתן לזהות בה פער משמעותי בין הציפייה לפרטיות לבין המציאות הפולשנית אליה הפרט חשוף יותר מבעבר באמצעות מערכות תוכנה וחומרה שאינן בולטות לעין למשתמש הקצה[51].

פעילות מודיעינית בעולם הקיברנטי היא דינאמית ביותר. על גופי המודיעין לעקוב באופן צמוד אחר הפיתוחים הטכנולוגים והמגמות במרחב ולפתח אמצעי מעקב מתוחכמים ביותר. בהמשך נראה כי בארצות הברית עיגנה המדינה בחקיקה את החובה של חברות תקשורת לפתח את מוצריהן תוך שהן מאפשרות את האפשרות להאזין ולנטר את התקשורת דרכן וזאת בכדי לוודא שהטכנולוגיה בעידן הרשת, המתפתחת באופן תדיר, לא ״תעקוף״ את היכולות המודיעיניות הקיימות. טרוריסטים הפועלים ברשת האינטרנט הגלויה לכל נעשים מודעים יותר ויותר לאותם ״עקבות דיגיטאליים״ וליכולות הניטור וההאזנה של גורמי המודיעין ועם השנים למדו להסוות את פעולותיהם ברשת, למשל באמצעות שימוש ברשתות אינטרנט פומביות, רשתות Wifi פתוחות ואינטרנט קפה, שימוש ב Proxy כדי להסוות את כתובת ה-IP, שימוש והחלפה תדירה של חשבונות דוא״ל מבוססות Web, שימוש בנקודות משלש[52] וירטואליות כגון קבצים מוסתרים, מוגנים באמצעות סיסמא או מוצפנים, וכמו כן העברת פקודות מוצפנות באתרים ודפי אינטרנט תמימים לכאורה תוך שימוש באמצעי הצפנה נגישים לשוק או מילות קוד שהוסכמו בין הפעילים. אחת הדוגמאות הבולטות למודעות ההולכת וגוברת של פעילי הטרור לאמצעי המעקב המקוון יכולה להילמד מהמודוס האופרנדי[53] שבו השתמשו מתכנני הפיגועים במערכת הרכבות במדריד בשנת 2004: העברת מסרים בין גורמי טרור באמצעות שמירת טיוטות של דוא״ל בתיבת דוא״ל מבוססת רשת (Gmail, Yahoo, Hotmail וכו׳) מבלי שהודעות אלו נשלחו לאף נמען[54].

2.1. __מאפיינים ייחודיים של המודיעין המסכל:__

למדינה ישנם מספר גורמי אכיפה, מודיעין וביון אשר עוסקים באיסוף, ניתוח וסיכול פעילות עוינת. כך למשל בישראל פועלים זה לצד זה *אגף המודיעין בצה״ל* (אמ״ן) שתפקידו לאסוף ולנתח מודיעין לשם התרעה או לשם מתן ייעוץ לדרג המדינה; *המוסד למודיעין ותפקידים מיוחדים* המופקד על איסוף מידע, מחקר מודיעין וביצוע פעולות חשאיות מיוחדות מחוץ לגבולות המדינה וכמובן *משטרת ישראל*. לצד אלו, האחריות המרכזית של המודיעין המסכל בישראל הוטלה על *שירות הביטחון הכללי* (השב״כ), וככזה -

---

51 איינהורן ואח׳, לעיל ה״ש 50, עמ׳ י-יא׳, 54.

52 דרך של תקשורת חשאית ללא קיום קשר ישיר בין הצדדים, באמצעות הטמנת דבר מה בנקודה שנקבעה בהסתר ובכיסוי כלפי הסביבה, וריקונה על ידי גורם אחר, כאמור תוך בידול בין הצדדים. שירות הביטחון הכללי, פורטל הטרור, **מילון מושגים**, תאריך פרסום לא זמין, ניתן לצפייה באתר השב״כ www.shabak.gov.il/publications/Pages/dictionary-terms.aspx

53 שיטת הפעולה ואופן הביצוע או המתווה. מונח השגור בהקשר של תיאור מאפייני הפיגועים שמבצעים ארגוני הטרור. שירות הביטחון הכללי, לעיל ה״ש 52, שם.

54 Denning, D. E., לעיל ה״ש 15, עמ׳ 20. תופעה נוספת שניתן להצביע עליה היא ניסיונות הולכים וחוזרים של פעילי טרור הנמצאים תחת מעקב מודיעיני לבחון את יכולות ההאזנה של גורמי המודיעין העוקבים אחר פעילותם ברשת. באופן זה פעילי טרור החושדים שהם נמצאים תחת מעקב לעיתים שולחים הודעות כוזבות המרמזות על פעילות טרור מתוכננת במקום הומה אדם, ובוחנים את התנהגות גורמי הביטחון.

תפקידו העיקרי הינו לאסוף מידע שישמש לסיכול עבירות ביטחון. גופי מודיעין שפועלים מחוץ לשטח מדינתם פטורים בדרך כלל מהדילמה של אפשרות הפרת חוקיה ומחובת הנאמנות לכיבוד עקרונות שלטון החוק במקומות פעילותם הייעודית. הפרת חוקיה של מדינה זרה היא בגדר סיכון מחושב אשר מהווה חלק ממארג היחסים הבין-מדינתיים. המודיעין הצבאי עוסק בדרך כלל באיסוף לשם התרעה למלחמה והיערכות לה ולשם מתן חוות דעת לדרג המדיני והמודיעין המשטרתי נועד לקדם את החקירות הפליליות.

לעומתם, תפקידו של המודיעין המסכל הוא לתרגם את המידע שנאסף לפעילות סיכול מיידית. כל מערכת הארגון בנויה לתכלית זו, ואם לפעילות המודיעין המסכל יש תוצרים נוספים כמו איסוף ראיות שיביאו להעמדה לדין, הריהם תוצרי לוואי נגזרים בלבד. תכלית זו מחייבת את ארגון המודיעין המסכל להתמקד בכוונות יותר מאשר במעשים המוכחים, ולעיתים הדבר נוגד ערכים בסיסיים של דמוקרטיה שאינה מגבילה את חירותו של אדם לחשוב ולהתכונן, כל עוד אין הדברים מגיעים לכדי עבירה[55].

לשירותי מודיעין מסכל ניתנים לרוב סמכויות ואמצעים שמטבע הדברים טמון בהם פוטנציאל רב לפגיעה בצנעת הפרט בחירותו, בגופו, וכן בערכים חברתיים ופוליטיים שונים. מכיוון שפעילות המודיעין המסכל היא מטבעה חשאית, הרי שמנגנוני הבקרה, ההרתעה והאיזון הקיימים בחברה דמוקרטית להגנה מפני שרירות השלטון ושימוש לרעה בכוחותיו, הם מוגבלים מאוד ביחס לשירותים אלו[56]. בפרקים הבאים נבחן את ההסדר הסטטוטורי שמסמיך את גופי המודיעין המסכל במשפט המשווה ובישראל להפעיל אמצעי איסוף מודיעיניים במרחב המקוון ונשאל האם הסדר זה מאזן באופן ראוי את הפגיעה בזכויות הפרט.

2.2. <u>**המודיעין בעידן המידע:**</u>

עבודת המודיעין לצרכי סיכול טרור דורשת איסוף מודיעין, עיבודו, ניתוחו (תוך הצלבתו עם מקורות מודיעיניים אחרים), הערכתו והפצתו במטרה לאסוף מידע תשתיתי על ארגון הטרור, פעיליו, מטרותיו וכיוצא בכך, להתריע על פעילות טרור מתוכננת ולהביא מודיעין נקודתי על מנת להכווין את סיכולה של פעילות זו. מודיעין לסיכול טרור אמור להצביע על השלבים השונים של גלגול הפיגוע[57] ולאתר סימנים מעידים שעשויים להצביע על כוונה של אדם או של תשתית טרור. שלב איסוף המודיעין לסיכול טרור הוא הרלוונטי יותר לדיון שלנו כאן, אך נשאלת השאלה כיצד ניתן להגיע בזמן אמת לאותה תכתובת דואר אלקטרוני או לקובץ המצוי במחשבו של פעיל טרור המכיל מידע מקודד אודות תכנון פיגוע, מבין עשרות מיליארדי המסרים המועברים ברשת מדי יום? ננסה לסווג את אמצעי המעקב המקוון בהתאם לאופן בו נאסף המידע, דהיינו על ידי ניטור – רישום פעולות המתבצעות ברשת על ידי משתמשים, או על ידי חדירה לשרת או למחשב עצמו ורישום הפעולות המתבצעות שם.

<u>א. ניתור מידע</u>: פרסומים גלויים מצביעים כי המערכת "אשלון" (Echelon) אותה מפעיל ה- NSA (National Security Agency) האמריקני, מסוגלת ליירט בזמן אמת מסרים שמועברים באמצעי תקשורת ברחבי העולם ובכלל זאת מסרים המועברים דרך רשת האינטרנט. המערכת עושה שימוש בתוכנות "רחרחן" (Sniffers) שעוברות על שרתים מרכזיים באינטרנט ומנטרת את הפעילות בהם. פעילות תקשורתית חשודה נשלפת ומועברת להמשך טיפול מודיעיני[58]. המערכת היא בעלת אלגוריתם מורכב המאפשר לה לאתר ולזהות מילים מסוימות בטקסט/מלל (כגון: "חומר נפץ", "מטען", "רקטה", "מתאבד" וכיוצא בכך) וגם מילות קוד תמימות לכאורה המוכרות בקרב גורמי הביטחון, כמו גם כתובות

---

[55] אריה רוטר "**חוק שירות הביטחון הכללי – אנטומיה של חקיקה מהתהליכים הפנים ארגוניים ועד לחוק הכנסת, ביטוי לשינוי התפיסה ביחסים שבין חוק לביטחון בישראל**" מרכז המחקר המכללה לביטחון לאומי, מרץ 2010, עמ' 15-16.

[56] **הצעת חוק שירות הביטחון הכללי**, התשנ"ח-1998, ה"ח תשנ"ח מס' 2689, 244, עמ' 245. להלן הצעת חוק השב"כ.

[57] תהליך התכנון וההכנות עד להוצאה לפועל של פיגוע. שירות הביטחון הכללי, לעיל ה"ש 52, שם.

[58] איינהורן ואח', לעיל ה"ש 50, עמ' 56 מול הערת השולים 206.

ואמצעי תקשורת ש"הוכללו" והוחשדו נמצאות תחת מעקב שוטף. נוכח היעדר המידע הגלוי בנושאים אלו, נצא מנקודת הנחה, לשם הדיון, כי מערכות האזנה בעלות מאפיינים דומים לאלו המאוזכרות בפרק זה מצויות גם הן בקרב גורמי מודיעין מערביים אחרים וביניהם גורמי מודיעין ישראלים.

הרחרחן הידוע והמתוקשר ביותר הוא ה**"קרניבור" – Carnivore** (או DC1000). הכינוי ניתן לתוכנה ע"י ה FBI שכן לדברי הארגון התוכנה "לועסת" את כלל המידע אך "בולעת" ו"מעכלת" רק מידע ספציפי רצוי. התוכנה עוברת בצורה פאסיבית על כלל התקשורת בשרת ועל גבי המערכות של ספקי האינטרנט כחלק בלתי נפרד מהפעלת הרשת, ודולה את המידע הספציפי בו היא מעוניינת. המערכת מאפשרת שני שימושים עיקריים: **(1) ציטוט תוכני (Content Wiretap)** – כלומר האזנה לסיגנאלים המשודרים מטעם היעד המודיעיני בדומה להאזנה לתוכן של שיחת טלפון. באופן זה ייורטו למשל הודעות דואר אלקטרוני שנשלחו מאת היעד המודיעיני ואליו. **(2) זיהוי המתקשרים (Trap and Trace / Pen Register)** – איתור וזיהוי של כל יוצרי הקשר אל הידע המודיעיני או ממנו. אלו כוללים זיהוי כתובת IP, כתובת דואר אלקטרוני, זיהוי שרתים אליהם ליעד המודיעיני גישה, זמן משלוח ההודעה, מעקב אחר משתמשים בדף אינטרנט ספציפי (כך ניתן ללמוד גם על אתרי האינטרנט בהם ביקר) ועוד[59].

כאמור לעיל, נניח כי בידי גורמי מודיעין מערביים אחרים אמצעים דומים במאפייניהם ל"רחרחן" ומכאן יש לתת את הדעת גם על האפשרות שמערכות כאלו יפגעו בפרטיותם של גורמים רבים אחרים אשר אינם קשורים לפעילות טרור כל שהיא. כך למשל סטודנט המקיים קשרי דואר אלקטרוני עם סטודנט אחר אשר מעורב בפעילות טרור יעלה גם הוא ברשת הקשרים שיצביע עליה ה"רחרחן". באופן דומה, מי שמתכתב ברשת על אמצעי לחימה לצרכי עבודת מחקר או לשם עניין אישי, גם אם אין לו שום מעורבות בפעילות טרור, יחזה בפני המערכת כמי שחשוד בטרור, וגורמי המודיעין יצטרכו להזים חשד זה.

<u>ב. חדירה ואיסוף מידע מהשרת או המחשב אישי</u>: לאחר שאותר גורם טרוריסטי, ינסה ארגון המודיעין למצות את כלל המודיעין שניתן להפיק ממנו באמצעים שונים, כגון:

1. **אמצעים חודרניים הנשתלים במחשב האישי לשם איסוף מידע**. למשל Cookies המהוות רכיב אינטגראלי בדפדפני האינטרנט, תוכנת מחשב השותלת קובץ טקסט במחשבו של הגולש, המתעד את כניסותיו לאתר אינטרנט ומאפשר לאסוף עליו מידע, כגון: פרטי ספק שירותי האינטרנט של המשתמש (ISP), סוג המחשב והתוכנות בהן הוא עושה שימוש, פרטי האתרים אליהם הגיע כתוצאה מקישורו לאתר, הזמן ששהה בכל אחד מהם ועוד[60]. כיום, דפדפני אינטרנט מאפשרים לחסום קבלת Cookies, אולם חסימה שכזו מגבילה את חווית הגלישה ואת היקף האתרים שניתן יהיה להיכנס אליהם. בעיה חמורה יותר בהיבט הפרטיות היא כמובן העובדה שכל האינפורמציה שמתועדת באמצעות ה- Cookies תיאסף יחד ממספר אתרים ותוצלב כדי להרכיב פרופיל של פעילות המשתמש, אשר יכלול מידע אישי רב על אותו משתמש וכמובן תפגע במעטה ה"אנונימיות" שקיים לכאורה בגלישה ברשת[61].

2. **חיפוש ותפיסה פיזית במחשב** - בין אם מדובר בחיפוש "גלוי" במעברי גבול או כחלק ממעצר פעילי טרור והחרמת רכושם, ובין אם מדובר בחיפוש "סמוי" הנעשה באמצעות החדרת תוכנה זדונית.

---

59 איינהורן ואחי, לעיל ה"ש 50, עמ' 56-57, 80. ישנן טענות לפיהן ההגבלות המשפטיות החלות על איסוף מודיעין המפר זכויות לפרטיות מצומצמות יותר כשמדובר במעקב מסוג Trap and Trace בלבד, אך עם זאת יש לתת את הדעת על כך שמערכות כמו ה"קרניבור" סורקות בפועל כמות גדולה מאוד של מידע על מנת למצוא פיסת מידע נקודתית שרק לגביה ניתן אישור לביצוע איתור, ובנוסף כי לא ניתן להפריד בין התוכן לבין מידע אודות היעד, משום שהם מועברים יחד וקיים חשש שמערכות אלו אוספות גם מידע תוכני ולא רק את מקור המסר ויעדו. ראה גם הדיון בפרק 4 להלן בנושא זה.

60 משרד המשפטים, **הוועדה לבדיקת בעיות משפטיות הנובעות ממסחר אלקטרוני**, דוח חלקי, מאי 2004, עמ' 81 .www.justice.gov.il/NR/rdonlyres/989CB3C8-BFEC-49C6-A689-433181BED312/0/electroniccommerce.pdf

61 יעל און ואחי "**פרטיות בסביבה הדיגיטלית**" המרכז למשפט וטכנולוגיה, עורכים: ניבה אלקין-קורן, מיכאל בירנהק (2005), עמ' 59-60.

3. **תוכנות זדוניות (Malware) ותוכנות ריגול (Spyware)** שניתן להחדירן למחשבי היריב, תוך הסתייעות בגורמים אנושיים, סוכנים או מקורות מודיעין הפועלים בארגון, או דרך "הדבקת" מחשב היעד המודיעיני באמצעות רשת האינטרנט כאשר היעד המודיעיני יפתח דוא"ל מסוים ממחשבו. Spyware הוא שם גנרי המתייחס לתוכנות השונות המושתלות במחשבו של המשתמש במטרה לאסוף מידע על הרגלי הגלישה שלו וליצור פרופיל של משתמש הקצה לצרכים מסחריים או אחרים[62]. במשפחת התוכנות הזדוניות ניתן למנות את תולעי המחשב ו"סוסים טרויאנים" (Trojan horse).

סוסים טרויאנים הם סוגים שונים של תוכנות המיועדות להתקנה במחשב היעד, וליצור לשולחיהם "דלת אחורית" (Backdoor) דרכה הם יכולים להמשיך ולהיכנס לאותו מחשב. סוס טרויאני מופיע בדרך כלל כקובץ המצורף לדואר אלקטרוני או כתוכנה חופשית להורדה[63]. ישנם סוסים טרויאנים היוצרים 'דלת אחורית' שתפקידה לתת הרשאות למשתמש אחר להיכנס למחשב הנפגע מרחוק לצורך ביצוע מגוון פעולות במחשב זה (Remote Access Trojans) כגון שיבוש פעילותו, מחיקת קבצים, השתלטות ופעולה באמצעותו על מנת לחדור למחשבים נוספים.

סוסים טרויאנים אחרים כגון Data-Sending Trojans או Proxy Trojans מאפשרים איסוף מידע (למשל, מספרי כרטיסי אשראי, מסמכים, קבצים, תמונות, בחינת מאפייני הגלישה של המשתמש במחשב, העברת צילומי מסך ועוד) מהמחשב "הנגוע" ושליחה ליעד מוגדר מראש. בהקשר זה, פרסומים גלויים וטכנולוגיה קיימת בשוק הפרטי מצביעים על קיומן של תוכנות אשר מאפשרות לשמור את כל הקשות המקלדת אשר מקליד היעד המודיעיני שבמחשבו הושתלה התוכנה (key-loggers). מכאן, הדרך פשוטה וקצרה לחשיפת כל חומר מוצפן על המחשב[64]. שימושים נוספים בתוכנות הזדוניות יכולים לאפשר לגורם החודר למחשב להשתמש במערכותיו כמו מצלמות המחוברות אליו, מיקרופונים או רמקולים ולבצע בעצמו צילומים או האזנת נפח לסביבתו של אותו מחשב. עניינו הרואות, ברצותו של גוף מודיעין לנבור במידע האגור ברשת או במחשבו של החשוד בטרור, היקף החדירה הוא בלתי נתפס בהיקפו ובעומקו.

2.3. <u>האיומים על זכויות הפרט ביחס להפעלת אמצעי מעקב על תקשורת מקוונת:</u>

בשנים האחרונות השימוש באינטרנט, בתקשורת מקוונת בכלל ובדוא"ל בפרט הפך נפוץ בקרב משתמשי האינטרנט ומשמש ככלי מרכזי להעברת מידע ותקשורת בין הפרטים בחברה. גישה להודעות דוא"ל ותקשורת מקוונת של חשוד מהווה אמצעי יעיל לגורמי מודיעין מסכל לשמור על בטחון המדינה. בדרך זו ניתן לנהל מעקב וחקירה סמויה ולהשיג ראיות מבלי שהחשוד יודע על דבר קיום החקירה. אולם מנגד, ניצבות זכויותיהם של המשתמשים המצפים לשמירה על פרטיותם; האינטרס החברתי לעודד שימוש בתקשורת מקוונת, בהיותה אמצעי זמין, מהיר נוח וזול; והצורך לאפשר חיי מסחר תקינים בעידן הטכנולוגי[65].

אחת הטענות לעניין הצורך בהגבלת כוחה של המדינה בהקשר של פגיעה בפרטיות היא שהזכות לפרטיות משפיעה גם על אפשרות מימוש אינטרסים אחרים וזכויות אזרח אחרות ובראשן חופש הביטוי. כשהאזרח יודע כי כל פעולותיו ברשת נרשמות, וכי רשויות המדינה מאזינות או מפעילות מערכות המסוגלות ליירט כל סוג של תשדורת מקוונת, יחשוש הפרט מהתבטאות חופשית ויימנע מאיתור וחיפוש מידע שמא הדבר

---

62 יעל און ואח', לעיל ה"ש 61, עמ' 72-73.

63 שמואל אבן ודוד סימן-טוב, לעיל ה"ש 42, עמ' 29.

64 דוגמא לכך ניתן למצוא במערכת "פנס הקסם" אשר פורסמה בתקשורת האמריקאית, ככזו המשמשת את ארגון ה FBI. איינהורן ואח', לעיל ה"ש 50, עמ' 60.

65 ת"פ (ת"א) 40206/05 **מדינת ישראל נ' אליעזר פילוסוף ואח'**, תק-מח 2007(1) 4872 (החלטה מיום 5.2.2007), עמ' 12. להלן: פס"ד פילוסוף.

עלול לפגוע בו. לעיתים די בעצם הידיעה בדבר השימוש באמצעי מעקב גם אם לא נעשה בהם שימוש בפועל, על מנת לגרום לצנזורה עצמית. האפשרות של גולש לפעול ברשת מבלי לחשוף את זהותו האמיתית הינה היבט של הזכות לפרטיות, אשר מאפשרת לנהוג בביטחון, בפתיחות ובחופשיות ללא עכבות או חששות מביקורת עוינת ממקורבים ומלחצים אחרים[66]. בהקשר זה, מנגנוני מעקב מודיעיניים אשר "מפצחים" את אותה אנונימיות על מנת לשרת את אינטרס הציבור, עלולים לגרום לפגיעה חמורה בחופש הביטוי ברשת וכן לפגיעה בפרטיותו של מעביר המסר[67].

כאמור, זכותה של המדינה הדמוקרטית לשמור על הסדר הציבורי מקימה את הצידוק להפעלת אמצעי האזנה, חיפוש ותפיסה ברשת או בחומר מחשב על ידי גופי מודיעין מסכל. ראינו גם, כי כנגד זכות זו עומדות זכויות היסוד של האדם וביניהן הזכות לפרטיות ולחופש הביטוי. איזו גישה של איזון ניתן לנקוט בין אותם אינטרסים מתחרים?

האם עלינו לנקוט בגישה שמאפשרת למדינה ליירט את כל המידע ללא סינון ולנתח רק את המידע החשוד? במקרים רבים בהם אין התרעה מודיעינית לפני פעילות טרור קטלנית, היכולת לחזור אחורה אל מידע שנקלט אך לא עובד מודיעינית מאפשרת להגיע למבצעי הפיגוע ולמסייעיהם[68], אך כמובן שלגישה זו יש השפעות עקיפות רבות על זכויות הגולשים.

האם נקבל גישה אחרת לפיה נאפשר למדינה ליירט רק את המידע בו היא חושדת, גישה שעלולה להביא פגיעה לציבור? באופן זה לא יהיה ניתן לשחזר בעתיד מידע שלא יורט גם אם יהיה רלוונטי בשלב מאוחר יותר. המצב הזה יביא ככל הנראה להרחבת המונח "חשוד" אצל גורמי המודיעין והסיכול (למשל במתן אפשרות ליירט ביטויים של קרובי משפחה או מכרים של יעד מודיעיני רק נוכח החשד שאינו מגובה במידע ממשי כי ייעשה בצינור זה שימוש כדי להעביר מידע שעלול להזיק לאינטרס הציבורי). גישה זו תפגע בחופש הביטוי ובפרטיותם של קרובים בדרכים עקיפות ליעד מודיעיני גם במצבים שבהם אין כל אינדיקציה לפעילות טרור מצידם[69].

גישה נוספת של איזון תשאל את השאלה היכן יופקד שיקול הדעת לפגיעה בפרטיות באמצעות המעקב המודיעיני ברשת? האם עלינו להפקיד שיקול דעת זה אצל גוף המודיעין המסכל עצמו, נוכח המומחיות המבצעית והמודיעינית שלו? האם עלינו להפקיד את שיקול הדעת בידי הרשות המבצעת הרלוונטית המפקחת על אותו שירות חשאי? או שמא עלינו לדרוש שכל פגיעה בפרטיות באמצעות מעקב מודיעיני ברשת תחייב הפעלת שיקול דעת שיפוטי בערכאות של בית המשפט.

בדיון בפרק הבא נבחן כיצד באות לידי ביטוי הגישות השונות שנסקרו לעיל, במסגרת ההסדרים המשפטיים הקיימים, בנוגע לפעולות מעקב וחיפוש באינטרנט במשפט המשווה ובישראל. כן נראה כיצד קבעו שיטות משפט שונות ושיטת המשפט הישראלית איזונים בין האינטרסים המנוגדים ובעלי החשיבות שהוצגו לעיל.

---

66 יעל און ואח', לעיל ה"ש 61, עמ' 6-7.

67 איינהורן ואח', לעיל ה"ש 50, עמ' 64-65

68 כך למשל בדוגמא של הקצין האמריקני, רב-סרן נידל מאליק חסן, ראה ה"ש 2 לעיל.

69 איינהורן ואח', לעיל ה"ש 50, עמ' 64-66

3. הגבלות משפטיות על מעקב אחר פעילות מקוונת - מערכת האיזונים הקיימת בין צורכי המודיעין לבין זכויות הפרט במסגרת הדין הקיים

3.1. משפט משווה:

בפרק זה נסקור את הדינים הרלוונטיים במישור הבינלאומי, במספר דמוקרטיות ליבראליות, בדגש על חקיקה שנכנסה לתוקף לאחר אירועי ה- 11 בספטמבר 2001, על מנת להסיק לגבי גישות שונות למתן סמכויות לרשויות מודיעין מסכל ביחס למעקב מקוון, אל מול הצורך לשמור על זכויות האדם.

3.1.1. האיחוד האירופי:

לאחר אירועי ה-11 בספטמבר 2001 נחתמה "**האמנה הבינלאומית לפשעי מחשב**" (Convention on Cybercrime, Budapest 2001)[70] מבית היוצר של מועצת אירופה. האמנה נועדה להקנות סמכויות פרוצדוראליות לאומיות הנדרשות לדין הפלילי בגין עבירות מחשב, עבירות שבוצעו באמצעות מערכות מחשב ועבירות שהראיות עליהן הגיעו מאמצעים אלקטרוניים. האמנה מקנה שורה של סמכויות לרשויות האכיפה, ובניהן: צווי הפקת מידע (ס' 18), חיפוש ותפיסה של מידע ממוחשב (ס' 19), איסוף בזמן-אמת של מידע תקשורתי (ס' 20), ויירוט בזמן-אמת של מידע תוכני (ס' 21). כל הסמכויות שניתנו לרשויות כפופות לסעיפים 14-15 לאמנה, לפיהם יש לתחום את הסמכויות בתנאים ספציפיים ומוגדרים בחוק. האמנה גם מטילה חובות על ספקי שירותי אינטרנט במסגרת הכוללת של הסמכויות המוקנות לרשויות האכיפה. אמנה זו מגדירה באופן רחב ביותר את המונח "ספק שירות" כך שגם גופים פרטיים וגם גופים ציבוריים כלולים בהגדרה וכוללת שירותים של אירוח או חיבור לרשת. בסעיף 18 מחייבת האמנה חקיקה מדינתית, לפיה תוכלנה הרשויות לכפות על ספק שירות להעביר מידע על לקוח שבאמצעותו ניתן יהיה לקבוע את סוג ההתקשרות, זהות המשתמש ומיקומו הגיאוגרפי. בסעיפים 20-21 נקבע כי ספקי השירות גם יחויבו לספק לרשויות מידע תוכני והתקשרותי בזמן-אמת על התקשורת שמתנהלת על גבי שרתיהם[71].

בשנת 2002 קבע האיחוד האירופי את **הדירקטיבה בנושא עיבוד מידע ופרטיות בסקטור התקשורת האלקטרונית**[72]. דברי המבוא וסעיף 15 לדירקטיבה מעניקים למדינות החברות אפשרות להגביל את הוראותיה לפי צורכי ביטחון ואכיפה, וקובעים כי מעקב על תשדורת זו חייב להיות הכרחי, מתאים, מידתי ומוגבל בזמן. אמצעי המעקב חייבים להיות מעוגנים בחוק ומאושרים על בסיס פרטני על ידי רשות מתאימה בכפוף למחויבות לאמנה האירופית בדבר זכויות האדם ולפסיקת בית הדין לזכויות אדם[73].

3.1.2. בריטניה:

<u>האזנת סתר ואיסוף נתוני תקשורת</u>: החוק **Regulation of Investigatory Powers Act 2000**[74] (RIPA) המהווה דבר חקיקה כולל המרכז את סמכויות השימוש באמצעי חקירה מיוחדים לרבות אמצעי מעקב מקוונים, מסדיר גם את נושא האזנת הסתר בבריטניה ובכלל זאת האזנה לתשדורת מקוונת. לפי ה- RIPA האזנת סתר על ידי רשות ביטחונית תתבצע רק לאחר הגשת בקשה על ידי בעלי תפקידים מוסמכים

---

70 נוסח האמנה נמצא באתר מועצת אירופה conventions.coe.int/Treaty/en/Treaties/Html/185.htm. על האמנה שנחתמה בשנת 2004 חתומות בעיקר מדינות החברות במועצת אירופה אך גם מדינות אחרות כמו ארצות הברית, קנדה ויפן. ישראל אינה חתומה על אמנה זו.

71 יצויין כי האמנה מאפשרת גם לדרוש מספק השירות לשמור על סודיות גם במסגרת שיתוף הפעולה עם הרשויות.

72 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

73 יצויין כי באיחוד האירופי התקבלה גם בשנת 1995 הדירקטיבה האירופאית להגנה על מידע אישי (EU Directive on Data Protection) המחייבת את המדינות החברות לחוקק חוקים שיחולו על המגזר הפרטי להגנה על הזכות לפרטיות ביחס לאיסוף, עיבוד, אחסון והעברה של מידע אישי. דיון מעמיק בתחולת האמנה והשפעתה על נושא המחקר שלנו חורג מגדרי עבודה זו.

74 2000 c.23 www.legislation.gov.uk/ukpga/2000/23/contents להלן: "RIPA".

באותה רשות כגון המנהל הכללי של שירותי הביטחון, ראש שירותי המודיעין, מפכ"ל המשטרה וכדומה[75] וקבלת צו מתאים משר ממונה. שר הפנים הבריטי פרסם קוד התנהגות בדבר ההליכים לקבלת צו האזנת סתר, ואלה קיבלו את אישור הפרלמנט בשנת 2002[76]. הקוד קובע כי בבקשת צו האזנת סתר צריכים להיכלל פרטי מידע רבים: (1) הרקע לפעולה הרלוונטית; (2) מידע על האדם או המקום אליו הבקשה מתייחסת; (3) תיאור התקשורת שמבקשים להאזין לה, ספק התקשורת והערכת מידת הישימות של פעולת ההאזנה; (4) הסבר מדוע ההאזנה נדרשת לפי תנאי RIPA; (5) הסבר בדבר הפרופורציונאליות בין ההאזנה המבוקשת לבין מטרתה; (7) שקילתן של נסיבות שיש בהן סכנה לפגיעה יוצאת דופן בפרטיותם של מי שאינם נושא הצו, ובפרט נסיבות שבהן תיגרם פגיעה בחיסיון רפואי, דתי, משפטי או עיתונאי; (8) אם מדובר בבקשה דחופה, פירוט ההצדקה לדחיפות; (9) הבטחה כי השימוש וההחזקה במידע המופק מההאזנה ייעשו בהתאם להוראות RIPA ביחס לשמירה על זכויות האדם.

בקשה להאזנת סתר מוגשת לשר ממונה שבסמכותו להוציא צו בנושא, במידה והוא מאמין כי הפעולה המותרת על פי הצו היא פרופורציונאלית למטרתה וכי הצו דרוש לאחת ממטרות אלו: פעולה לטובת ביטחון המדינה, למניעה או גילוי של פשע חמור או להבטחת אינטרסים כלכליים של בריטניה. החוק מחייב את השר לבחון אם יש דרך סבירה אחרת להשיג את המידע אשר לשמו נדרש הצו[77]. במקרים דחופים מוסמך גם פקיד בכיר להוציא צו האזנת סתר. נתוני תקשורת יועברו לרשויות ביטחוניות על ידי אישור מגורם זוטר יותר במשרדו של השר הממונה. תוקפו של צו האזנת סתר הוא שלושה חודשים ממועד הוצאתו. צו שהוצא על ידי פקיד בכיר במקרה דחוף יהא בתוקף למשך 5 ימים[78]. ה- RIPA קובע מספר כללי ביטחון שנועדו להגן על זכויות האדם בכל הקשור להאזנת סתר ומחייב את השר לוודא כי הם נשמרים[79]. בין הכללים:שמירה על היקף מינימאלי של חשיפת המידע שהושג בהאזנה (הגבלת מספר האנשים שנחשפים למידע, הגבלת היקף העתקת המידע), הצבת כללים לטיפול בחומר, שמירתו והשמדתו של החומר כאשר אין בו צורך.

<u>אחריות ספקי שירות באינטרנט</u>: כחודשיים לאחר מתקפת ה- 11 בספטמבר הוצג בפרלמנט הבריטי ה- **Anti Terrorism Crime and Security Act 2001**[80] ונכנס לתוקפו בדצמבר 2001. החוק מרחיב את סמכויות הסיכול והאכיפה של רשויות השלטון ובין השאר מאפשר לרשויות המדינה לקבוע רגולציה כלפי חברות טלקומוניקציה וספקי אינטרנט במטרה לשמור ולהעביר לרשותם חומר בנושאי ביטחון לאומי, לשמור מידע תקשורתי לתקופה ממושכת ולקבוע הוראות לגילוי מידע לרשויות.

<u>חיפוש בחומר מחשב</u>: ה- **Terrorism Act, 2000**[81], המהווה את דבר החקיקה המרכזי נגד טרור בבריטניה, קובע כי חיפוש בחומר מחשב יעשה לפי צו שופט בלבד.

3.1.3. <u>קנדה:</u>

בקנדה קבועות הוראות שונות ביחס להאזנת סתר בחוקים שונים, על פי מטרות ההאזנה. הוראות שעניינן האזנת סתר למטרות מודיעין זר מצויות ב-**National Defense Act**[82] והוראות שעניינן האזנת סתר למטרות הגנה על ביטחון המדינה מצויות ב-**Canadian Security Intelligence Service Act**[83].

---

75 ראה סעיף 8 לRIPA .

76 Regulation of Investigatory Powers (Interception of Communications: Code of Practice), Order, 2002, No. 1693.

77 דפנה בן-פורת "**מסמך רקע בנושא: חקיקה בעניין האזנת סתר בבריטניה ובקנדה**" הכנסת, מרכז מחקר ומידע, מוגש לועדת החוקה, חוק ומשפט (2004), עמ' 5-4.

78 ראה סעיפים 7 ו- 9 ל-RIPA.

79 ראה סעיפים 15-16 ל-RIPA.

80 www.legislation.gov.uk/ukpga/2001/24/contents.

81 www.legislation.gov.uk/ukpga/2000/11/contents.

ה- NDA מסמיך את שר הביטחון הקנדי להתיר לרשויות הביטחון האזנה לתקשורת פרטית (ובכלל זאת לתקשורת מקוונת) לצורכי מודיעין בהתקיים התנאים המצטברים הללו: (1) האזנה מכוונת כלפי ישויות זרות מחוץ לקנדה; (2) אין דרך סבירה אחרת להשיג את המידע; (3) ערכו המודיעיני הצפוי של המידע שיופק מההאזנה מצדיק אותה; (4) ננקטו אמצעים מספיקים להגנה על פרטיותם של אזרחי ותושבי קנדה. שר הביטחון מוסמך להתיר לרשויות הביטחון האזנה לתקשורת פרטית גם בכל הקשור לפעילות למטרת הגנה על מערכות מחשב או על רשתות ממשלתיות מפני נזק, שימוש לא מורשה או הפרעה[84]. היתר האזנה מידי שר הביטחון נשאר בתוקפו במשך התקופה המצוינת בו וניתן לחדשו לתקופה שאינה עולה על שנה[85].

האזנות סתר למטרות ביטחון לאומי לפי ה- CSIS מוסדרות על ידי צו שופט. מנהל שירות הביטחון והמודיעין הקנדי או עובד שהוסמך לכך מוסמכים להגיש בקשות לצווים, כשיש יסוד להאמין כי הצו דרוש כדי לאפשר לשירות הביטחון לחקור איום על ביטחון המדינה או כדי לאפשר לו לבצע את תפקיד איסוף המידע הקשור למדינות זרות או לזרים. הבקשה לצו תלווה בתצהיר שיפורטו בו: (1) העובדות שהמבקש מסתמך עליהן לביסוס הצורך בצו כאמור; (2) מידע על דחיפות העניין ועל ניסיונות לשימוש באמצעי חקירה אחרים; (3) זהות האדם לו מבקשים להאזין; (4) פירוט על מיקום ההאזנה, מבצעי ההאזנה ותקופת הצו המבוקשת; (5) מידע על בקשה קודמת ביחס לאותו אדם לו מבקשים להאזין[86]. צו האזנת סתר יישאר בתוקפו לתקופה שתצוין בו ושלא תעלה על שנה אחת.

הצעת חוק שהוגשה בשנת 2012 בקנדה מבקשת לחייב בחקיקה את כל חברות התקשורת, ובכלל זאת ספקי אינטרנט, להשיג ולתחזק יכולת טכנית להקליט, לפקח ולנטר כל פעילות ברשת האינטרנט לפי דרישה של רשויות הביטחון הקנדיים ולפי היתרים שיינתנו לרשויות לאיסוף מידע זה. הצעת החוק מחייבת את ספקיות התקשורת להעביר גם נתוני תקשורת (כגון, שם המנוי, כתובתו, מספר הטלפון, כתובת הדוא"ל וכתובת ה IP) לרשויות ללא צו[87]. נשים לב לגישה זו, המאפשרת לגורמי הביטחון להפעיל אמצעים למעקב מקוון אחר אזרחים באמצעות "זרוע ארוכה" בדמותן של חברות פרטיות, כאשר נסקור את הדין הישראלי.

3.1.4. **<u>ארה"ב:</u>**

התיקון הרביעי לחוקה בארצות הברית מגדיר את ההגנה על הזכות לפרטיות ומגביל את סמכויות הממשל לא לפגוע בזכויות אלו ללא עילה חוקית בקובעו סטנדרט של "probable cause" שעל פיו יינתן צו שיפוטי אשר יתיר ביצוע פעולות אשר יפגעו בפרטיות. את העילות להוצאת הצו יש לפרט בתצהיר וכן נקבעו בהקשר זה מערכות בלמים ואיזונים בחקיקה ובפסיקה האמריקאית. ב- 26 באוקטובר 2001 התקבל החוק **USA Patriot Act**[88] בקונגרס האמריקאי ונכנס לתוקף ב-1 בפברואר 2002. החוק, בין השאר, צמצם בצורה דרמטית את המגבלות שהוטלו על רשויות אכיפת החוק בפעילות לאיסוף מודיעין בין אם מדובר ברשויות הממונות על אכיפת החוק או של סוכנויות לביטחון העוסקות באיסוף מודיעין בינלאומי. החוק

---

82 National Defence Act (R.S.C., 1985, c. N-5), להלן NDA. laws-lois.justice.gc.ca/PDF/N-5.pdf

83 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23), להלן ה- CSIS laws-lois.justice.gc.ca/PDF/C-23.pdf

84 ראה סעיף 273.65 (3) ב- NDA. שר הביטחון יוציא היתר להאזנת סתר כאמור, רק בהתקיים מספר תנאים מצטברים ובניהם כי אין דרך סבירה אחרת להשיג את המידע, כי ננקטו אמצעים כדי לוודא שייעשה בהאזנה שימוש חיוני בלבד ושיתקבל ממנה אך ורק מידע חיוני למטרות ההאזנה; וכי ננקטו אמצעים מספיקים להגנה על פרטיותם של אזרחי ותושבי קנדה.

85 ראה סעיף 273.68 ב- NDA.

86 ראה סעיפים 27-28 ב CSIS, מובא גם בדפנה בן-פורת, לעיל ה"ש 91, עמ' 15-16.

87 An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts (Bill C-30). Available at: www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5380965

88 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, P.L. 107-56, 115 Stat. 272 (2001). להלן USA Patriot Act.
כמה מתת הסעיפים ב- Patriot Act היו אמורים לפקוע ב-31 בדצמבר 2005, אולם הוסכם שגם אותם תת-סעיפים שתוקפם אמור לפקוע בתאריך זה, יוסיפו להתקיים לגבי חקירות שנמצאות בעיצומן כנגד גורמי מודיעין חוץ, כך שניתן יהיה למצות את החקירות עד תומן. ב- 26 במאי 2011 חתם הנשיא אובמה על הארכה לארבע שנים של מספר הוראות המפתח בחוק.

שינה ללא הכר את יכולתו של השלטון לחדור לתחום הפרט, לרבות במרחב המקוון. נראה כי אחת מהמטרות הבולטות של ה-Patriot Act היא להתאים את הסמכויות שמקנה החקיקה האמריקאית לזרועות המודיעין ללחימה בטרור בסביבה אינטרנטית[89]. בקרב ארגוני זכויות אדם ומשפטנים קיימת ביקורת כנגד החוק , לפיה המהלך נעשה שישה שבועות בלבד לאחר המתקפה על ארצות הברית ב-11 בספטמבר וללא התנגדות של ממש[90] במיוחד לנוכח המהירות שבה נעשה שינוי כה מהותי במערכת האיזונים והבלמים הקיימת ביחס לזכות לשמירה על הפרטיות לאור המציאות שאחרי התקפת הטרור על ארצות הברית[91] ולאור ההסמכה הרחבה שהוא מעניק לרשויות, הכוללת, בין השאר, גם את היכולת לנטר פעילות באינטרנט. נבחן כעת כיצד מערך הדינים בארצות הברית הושפע מה- Patriot Act ביחס לסמכויות רשויות ביטחון לאסוף מידע מקוון מול האיזונים שהתקיימו ערב חקיקתו.

<u>1. האזנה וניטור מחוץ לגבולות ארה"ב</u> - רשויות המודיעין כמעט ואינן מוגבלות בהפעלת אמצעי האזנה, ובכלל זאת לתשדורת מקוונת, מחוץ לארצות הברית. אין כל חיקוק בנושא, למעט הנחיה של הנשיא רייגן, התקפה עד היום, הקובעת כי במקרה שאזרח או תושב אמריקני הוא נשוא ההאזנה, יש לקבל את אישור התובע הכללי, אם קיימת עילה מסתברת שהיעד הוא סוכן זר[92]. בעניין **Truong**[93] נקבע שרשויות החקירה והאכיפה לא זקוקות לצו מבית המשפט אם מטרת הציטוט היא איסוף מודיעין זר, אלא שה- Patriot Act מרחיב היתר זה על ידי ביטול ההבחנה בין ציתות לצרכי חקירה לבין ציתות לצורך איסוף מודיעין זר, דבר שעומד בניגוד להגנה שניתנה לפרטיות על ידי התיקון הרביעי לחוקה האמריקאית[94].

בהקשר זה יצוין כי החוק **Protect America Act**[95] שהיום כבר פקע תוקפו, התיר לגורמי המודיעין האמריקנים, תחת תנאים מסוימים, לאסוף מידע (גם באמצעות האזנה לדוא"ל ולאמצעים נוספים של תשדורת אלקטרונית) בנושאי מודיעין זר ביחס לאנשים אשר גורמי מודיעין חושדים כי הם מחוץ לגבולות ארצות הברית ללא צו או פיקוח שיפוטי, למעט אישור התובע הכללי שנדרש לצורך כך.

<u>2. האזנה וניטור בגבולות ארצות הברית</u> - שני חוקים מסדירים את הנושא. האחד הוא **Omnibus Crime Control and Safe Streets Act of 1968**[96] אשר Title III שלו מאפשר הפעלת אמצעי פיקוח והאזנה לתקשורת אלקטרונית, כולל תכתובות דוא"ל, ללא הסכמת או ידיעת הגורם הנתון להאזנה, באמצעות צו בית משפט, לאחר שזה מצא, על סמך תצהיר המדינה, כי יש עילה מסתברת ("probable cause") שפשע בוצע, מבוצע או עתיד להתבצע. בעוד שחוק זה לא התייחס תחילה לאמצעים מודרניים יותר של תקשורת כגון האזנה לתשדורת פקס, דואר אלקטרוני, ונתוני תקשורת אלקטרונים, תיקון הקונגרס את החסר באמצעות ה- **Electronic Communications Privacy Act of 1986**[97] על מנת להסמיך את הרשויות

---

89 ראה דברי הנשיא גורג' ו. בוש בנאומו בבית הלבן במעמד החתימה על ה- Patriot Act. מובא באלעד אורג **אנונימיות, משפט ואינטרנט, על חשיבה משפטית בנוגע לפעילות אנונימית באינטרנט ובכלל** (עבודה מסכמת לצורך קבלת תואר "מוסמך במשפטים") אוניברסיטת תל-אביב, הפקולטה למשפטים (2002), עמ' 123 ליד הערת השולים 489.

90 ארגון זכויות האדם בארצות הברית ה- America Civil Liberties Union טוען שממשל בוש הפעיל לחץ כבד על המצביעים ורמזו שמי שיצביע נגד קבלת החוק יהא "אחראי" לכל תקיפה עתידית כנגד ארצות הברית. היה זה איום קשה, במיוחד נוכח החשש הציבורי הכבד מתקיפה נוספת כנגד ארצות הברית בשבועות ובחודשים שלאחרי פיגועי ה- 11 בספטמבר. ראה America Civil Liberties, *Surveillance Under the USA Patriot Act* (2010) page 1, available at: www.aclu.org/national-security/surveillance-under-usa-patriot-act.

91 איינהורן ואח', לעיל ה"ש 50, עמ' 78. עמנואל גרוס, לעיל ה"ש 2, עמ' 634.

92 .Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. §401 note

93 United States v. Truong Dinh Hung, 629 F. 2d 908 (4th Cir. 1980). מבוא בעמנואל גרוס, לעיל ה"ש 2, עמ' 661.

94 עמנואל גרוס, לעיל ה"ש 2, עמ' 662.

95 .Pub.L. 110-55, 121 Stat. 552

96 Pub. L. No. 90-351, 82 Stat. 197, codified as 18 U.S.C. §2510-2522; (להלן: "Title III").

97 .18 U.S.C. §§ 2701-2710, 3121-3126

להאזין גם באמצעים אלו. החוק מכיל רשימה סגורה של פשעים בגינם ניתן לבקש צו במסגרת חוק זה וב-Patriot Act הוספו לרשימה פעולות טרור, "cybercrime" ועבירות לפי חוק הונאה במחשבים[98].

הבקשה והצו להאזנה מכוח Title III יכללו מידע רב אודות ההאזנה המתוכננת, כגון: זהות המואזן והגורם המאשר, מיקום ההאזנה, פירוט של אמצעי ההאזנה והצהרה שהמידע לא יוכל להיות מושג בדרכים אחרות שלא דרך האזנה, המאמצים שנעשו ביחס להאזנה בכדי למנוע פגיעה בזכויות האדם של אזרחים ותושבים אמריקנים, המטרה הדרושה למשימות ההאזנה, היסטוריה של בקשות האזנה קודמות ביחס לגורם המואזן, למתקן או לתשתית התקשורת, משך ההאזנה וכל מידע נוסף אחר שידרוש השופט. צו בית משפט המתיר האזנת סתר לפי Title III יישאר בתוקף למשך פרק הזמן שכתוב בצו אך לא מעבר ל-30 יום כאשר ניתן להאריך את הצו בתקופה נוספת של 30 יום[99].

החוק השני הינו **The Foreign Intelligence Surveillance Act of 1978**[100] (FISA) המאפשר הוצאת צווי האזנה על-ידי בית-דין מיוחד לסוכנים זרים, וזאת נוכח הרגישות הגבוהה בחשיפת ראיות אלו והצגת מידע מודיעיני מסווג בפני ערכאות שיפוטיות אמריקניות "רגילות". FISA נועד לאפשר לרשויות לחקור ולהפעיל אמצעי מעקב על איומים פוטנציאליים של סוכנים זרים של מדינות וגופים זרים ("agents of foreign power") ובכלל זאת גורמי טרור שונים. גם פה בית המשפט המיוחד ייתן צו כאשר דרישות החוק יתמלאו ואולם על-מנת להוציא צו לאזרח או לתושב קבע אמריקני יש להוכיח שהמידע הכרחי לביטחון הלאומי. לגבי מי שאינו אזרח, יש להראות שהמידע קשור לביטחון הלאומי. הבקשה והצו להאזנה מכוח ה- FISA יפרטו גם הם מידע רב אודות ההאזנה המתוכננת בדומה למצב המתואר ב Title III [101].

ה- FISA מתיר במצבי חירום גם לנשיא, באמצעות התובע הכללי, לאשר שימוש באמצעי מעקב אלקטרונים ללא צו שיפוטי, במטרה להשיג מידע מודיעיני זר במגבלות מסוימות[102]. ה- Patriot Act תיקן את ה- FISA כך שבקשות המוגשות לצו שיפוטי לאישור האזנה לא צריכות לציין שהמידע על המודיעין הזר הינו מטרת ההאזנה, אלא מספיק שיהיה חלק ממנה[103].

כמו כן, לבית משפט של FISA יש סמכות לאשר מעקב מודיעין אלקטרוני ללא ציון אמצעי הקשר שלו יאזינו או הצדדים שהם יעד ההאזנה. ארגוני הביון האמריקאים מצביעים כמובן על הצורך החיוני להמשיך ולפקח על פעילות טרור פוטנציאלית בעולם בו טרוריסטים מחליפים מחשבים, חשבונות דוא"ל, טלפונים סלולארים ורשתות במהירות. מנגד, יכולים המבקרים להצביע על הפגיעה הלא מידתית בהגנה הניתנת לפי התיקון הרביעי לחוקה האמריקנית בצווים מסוג זה.

סעיפים 201-202 של ה- Patriot Act מרחיבים את רשימת הפשעים החמורים שיכולים להיחקר באמצעות הפעלת אמצעי פיקוח, ציטוט, והאזנה לפי Title III, גם למעקב אחר שימוש בנשק להשמדה המונית, שימוש בנשק כימי, פעולות אלימות של טרור במעברי גבול, עסקאות פיננסיות עם מדינות התומכות בטרור, ופעילויות נוספות שקשורות לטרור ולסיוע לו[104].

---

98 .18 U.S.C. § 1030

99 .18 U.S.C. § 2518(1),(2) § 2518(a),(b)

100 .Pub.L. 95-511, 92 Stat. codified as amended at 50 U.S.C. §1801-1811

101 .50 U.S.C. §1804

102 (4) ,U.S.C. 50 §1805(f), 1802(a)(1)(4), 1822(a)(1). בהקשר זה יצויין כי ממשל הנשיא גורג' ו. בוש הורה לסוכנות ה- NSA לבצע שימוש בהאזנה ללא צו בתוך ארצות הברית על מנת למנוע פיגועי טרור לאחר הפיגועים ב- 11 בספטמבר 2001. פרשייה זו נחשפה בתקשורת והובילה לביקורת ציבורית קשה על הפגיעה בתיקון הרביעי לחוקה ביחס לפעולות אלו.

103 .USA Patriot Act Sec 218

104 .USA Patriot Act §201-202

על מנת לבצע מעקב מקוון באמצעות ה FISA לא נדרש להוכיח שפשע עתיד להתבצע ואין צורך בדרישת "probable cause". ראינו כי ה- Patriot Act משנה את האיזונים שהתקיימו בעבר לעניין הפגיעה בזכויות האדם ביחס לציטוט ולחדירה למערכות מקוונות שבידי הפרט. חוק ה- Patriot Act דורש אמנם צו מבית משפט כדי לאפשר פגיעה בזכות לפרטיות של אדם, אך מסתפק בצו משופט שלום או שופט של FISA. לפני ה- Patriot Act הצו היה ניתן גם ללא הוכחה של "probable cause" ואילו לאחריו הצווים יינתנו על בסיס של רמת חשד פחותה, כשמבית המשפט ניטל שיקול הדעת המהותי ומה שנותר בידיו הוא שיקול דעת טכני בלבד. תוצאה זו יכולה לפגוע באופן חסר תקדים בזכויות אדם[105].

יש לציין גם בהקשר זה כי ה- **Intelligence Reform and Terrorism Prevention Act of 2004**[106] מרחיב את הסמכויות הניתנות לרשויות לפי ה FISA לאתר ולנהל מעקב אלקטרוני ואחר ביחס לחשודים בפעילות טרור אשר אינם קשורים לאף מדינה זרה או לארגון טרור, המכונים "זאבים בודדים", כלומר טרוריסטים הפועלים לבדם ללא תמיכת ארגון טרור.

יצוין כי הרשויות להן ניתן אישור להאזנה וחיפוש על פי ה FISA נתונות לפיקוח של הקונגרס האמריקאי ומחויבות בדיווח חצי שנתי ביחס לאמצעי המעקב אשר הן מפעילות[107].

3. <u>צווי איתור וזיהוי (Pen Register/Trap and Trace Order)</u>- צווים אלה נועדו לאתר את המיקום בו נקלטה או שוגרה תשדורת מסוימת ביעד המודיעיני הנתון תחת מעקב. בקשות לצווים אלו יכללו מידע מאוד בסיסי בהשוואה למידע שיכללו בקשות להאזנה כאמור לעיל, ובמסגרת זו יכללו בהם פרטים אודות האדם מושא ההאזנה, נתונים אודות מיקום הקו או אמצעי התקשורת הניתן לאיתור וזיהוי, ופירוט בסיסי של הפשע או החקירה הרלוונטית לאיתור ולזיהוי[108]. צווים אלו יכולים להורות לנותני שירותים ולספקי אינטרנט להעביר מידע אודות מנויים[109] וכמו כן, במקרים דחופים החקיקה מתירה לתובע הכללי לאשר התקנת חירום של אמצעי ניטור שכזה כל עוד הבקשה מוגשת לבית המשפט בתוך 48 שעות[110].

סעיף 216 ל- Patriot Act מרחיב את ההיתר לביצוע איתורים מתקשורת קווית ומוסיף תקשורת אלקטרונית ובכך מאפשר לצווים אלו לכלול גם מידע אודות שולח ההודעה וכתובת האינטרנט שלו ומידע נוסף ביחס לדוא"ל או אמצעי התקשורת האלקטרוניים. ה- Patriot Act קובע שעל בית המשפט לאשר צו מסוג זה גם ביחס לאמצעי תקשורת אלקטרונים כגון דוא"ל, במידה והוא יכול לספק מידע רלוונטי בגין עבירה פלילית. שיקול הדעת שבידי בית המשפט הוא טכני בלבד ולא מהותי ומתייחס לאופן הגשת הבקשה ואינו מתייחס למידת הוודאות הנדרשת שאכן מתן צו שכזה יספק מידע לגבי עבירה[111]. במובן זה שינה ה- Patriot Act את האיזון הקיים בדין האמריקאי וקבע כי התקנים אלו באינטרנט לא מהווים חיפוש ולכן לא חל הסטנדרט של probable cause שבעבר נדרש מהרשויות בארה"ב אלא סטנדרט מקל יחסית של רלוונטיות לחקירה פלילית[112]. למשל, לאור התיקון רשויות יכולות לבצע מעקב של איתור וזיהוי של פרטי התקשורת כלפי גולש תמים שהקיש מושג "מעורר חשד" במנוע חיפוש באינטרנט, וכל שנדרש מהרשויות הוא להצהיר בפני בית המשפט שהמעשה עשוי להוביל למידע רלוונטי לחקירה שמתנהלת באותה העת.

105 עמנואל גרוס, לעיל ה"ש 2, עמ' 661, 665-664.
106 Pub.L. 108-458, 118 Stat. 3638
107 50 U.S.C. §1808, 1826.
108 18.U.S.C 3123. ביחס לאמצעי הניטור מסוג Pen Register/Trap and Trace ראה גם פרק 2.2 לעיל.
109 50 U.S.C. §1842(d)(2)(c).
110 50 U.S.C. §1843.
111 עמנואל גרוס, לעיל ה"ש 2, עמ' 641.
112 USA Patriot Act §214, 216.

אותו אדם שמצותתים למחשבו, אינו צריך להיות מושא החקירה או חשוד בעבירה כלשהי[113]. סעיף 214 ל-Patriot Act אף הרחיב את אפשרויות הוצאת הצו במסגרת מודיעין נגדי (FISA) למקרי טרור, אולם אוסר פתיחת חקירה נגד אזרח רק בגין מידע המוגן בתיקון הראשון לחוקה (חופש הביטוי).

4. <u>צווי חיפוש ותפיסה</u> - צווי חיפוש מוצאים באישור שופט כאשר קיימת עילה מסתברת שבוצעה עבירה. בעת ביצוע החיפוש או אחריו יש להודיע לבעל המקום שבוצע חיפוש, אולם ה-Patriot Act הרחיב את הסמכות לביצוע חיפושים חשאיים בהם בעל המקום לא יודע שבוצע חיפוש[114]. גם כאן, בתי המשפט לא נדרשים למצוא probable cause אלא מסתפקים בסטנדרט מקל יחסית של רלוונטיות לחקירה פלילית כאמור[115]. צווי חיפוש משמשים לתפישת מידע תוכני שהתקבל ומאוחסן ("stored") באמצעים אלקטרוניים לרבות דוא"ל שטרם נקרא. ה- Patriot Act מתיר ליירט מידע מאוחסן של תקשורת קווית לרבות תא קולי באמצעות צו חיפוש[116] ואף מאפשר עיון במידע שנתפס תוך כדי השגת גבול במחשבים ללא צורך בצו בית משפט[117]. תחת FISA ניתן גם לבצע חיפושים, ללא פיקוח שיפוטי, באישור התובע הכללי[118].

<u>5. קבלת מידע שנאסף בידי ספקי גישה</u>- רשויות האכיפה רשאיות להזמין ולקבל מידע מספקי גישה לאינטרנט לצורך ביצוע חקירות כאשר הזמנת המידע אינה כפופה לביקורת שיפוטית. ה- Patriot Act מסמיך את רשויות האכיפה להזמין ולקבל מספקי גישה ותקשורת מידע רב יותר מבעבר, לרבות זמן ומשך השיחה/גלישה ברשת, כתובת המנוי, כתובת IP, אופן התשלום ופרטי המשלם[119]. הרשויות יכולות להזמין רשומות עסקיות דוגמת מידע בגין עסקאות שבוצעו בחברת התקשורת וכל מידע לא תוכני הקשור למנויי ספקיות גישה[120]. ה- Patriot Act מאפשר לספק השירות למסור מידע לא תוכני, ללא צו, במקרה של סכנת חיים או פגיעה חמורה[121]. דבר חקיקה אמריקני מעניין במיוחד הינו ה- **Communications Assistance for Law Enforcement Act**[122] הדורש מחברות התקשורת שתתאמנה את מערכותיהן להפעלת אמצעי פיקוח על ידי רשויות האכיפה לטובת השגת מודיעין בזמן אמת מניטור תקשורת אלקטרונית. באופן זה מנסה החקיקה האמריקנית לוודא שהטכנולוגיה בעידן הרשת, המתפתחת באופן תדיר, לא "תעקוף" את היכולות המודיעיניות הקיימות. כך אנו רואים שגם טכנולוגיה המפותחת בשוק האזרחי ומאפשרת לבני אדם לתקשר בצורה פרטית ומאובטחת (כגון הצפנת הדוא"ל של Blackberry), באמצעות מסרים מיידים ברשתות חברתיות (כגון שירות ה Messenger של הרשת החברתית Facebook) או באמצעות תוכנות המאפשרות העברת מסרים ישירה "peer to peer" (כגון זו של חברת Skype), מתפתחת יחד עם חיוב סטטוטורי להשתיל בה מעיין "סוסים טרויאניים" המאפשרים את ההאזנה והניטור מניה ובה.

יצוין כי לספקי תקשורת וביניהם ספקי אינטרנט ישנו פטור מהאיסור הפלילי על האזנת סתר כאשר הם משתפים פעולה עם חקירה של רשות פדראלית או מדינתית מוסמכת[123]. ה- FISA מקנה לתובע הכללי ולמנהלי שירותי המודיעין האמריקניים סמכות להורות לספקי תקשורת אלקטרונית, וביניהם ספקי

---

113 איינהורן ואח', לעיל ה"ש 50, עמ' 78-80.

114 USA Patriot Act §213. יצוין כי כלי נוסף שנותן ה Patriot Act בידי רשויות האכיפה הוא ביטול הצורך בצו המפרט והמזהה את המקומות, החפצים והיעדים הספציפיים לחיפוש – USA Patriot Act § 219. כמובן שלעניין זה נשמעת ביקורת נרחבת בטענה שצווים מסוג זה עומדים בסתירה להוראות התיקון הרביעי לחוקה.

115 18 U.S.C. §2703(b), (c).

116 USA Patriot Act, §209.

117 USA Patriot Act, § 217.

118 USC §1822 50.

119 USA Patriot Act § 210.

120 18 U.S.C. §2703 (c).

121 USA Patriot Act § 212.

122 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010; 18 U.S.C. §2522 .

123 18.U.S.C 2511(2)(a)(ii).

אינטרנט לסייע באיתור והשגת מידע ביחס לאמצעי תקשורת של גורם הנמצא תחת האזנה. ספקי תקשורת שמשתפים פעולה עם הרשויות זכאים לתגמול, וה-Patriot Act אף מקנה להם הגנה כאשר הם שומרים על המידע והתכתובות ביחס ליעד האזנה מסוים לבקשת הרשויות וזאת עד שיושג צו בנושא[124]. יצוין גם כי לתובע הכללי יש סמכות לפעול בהליכים נגד ספקי תקשורת שלא משתפים פעולה עם הרשויות[125].

6. <u>שיתוף פעולה מודיעיני</u>- כחלק מלקחי פיגועי ה-11 בספטמבר 2001 בארצות הברית, הדגישו גורמים ביטחוניים את החשיבות הרבה בשיתוף פעולה מודיעיני בין גורמים שונים של אכיפת חוק בארצות הברית במאבק כנגד הטרור[126]. בהקשר ישיר לכך, ה- Patriot Act הרחיב את האפשרויות לשיתוף מידע בין הרשויות השלטוניות השונות, ובכלל זאת ביחס למידע שהושג באמצעות האזנה לאמצעים אלקטרונים. שיתוף המידע לצרכי מניעת טרור אפשרי כיום ללא הגבלה על זהות הרשות המוסרת או מקבלת המידע או זהות העובדים שייחשפו למידע וללא כל פיקוח שיפוטי לגבי ההצדקות לחשיפה זו[127]. בהקשר זה יצוין כי לאחרונה הוצג החוק [128] **Cyber Intelligence Sharing and Protection Act** אשר מציע מתן אפשרות לרשויות ממשלתיות נוספות ואף לחברות טכנולוגיה פרטיות בארצות הברית לשתף מידע ביניהם בכדי להילחם בפשיעה מקוונת ואיומים קיברנטיים. החוק אושר בבית הנבחרים האמריקאי ב-26 באפריל 2012, והביקורת הרבה שספג מתייחסת כמובן לאפשרות של עקיפת המגבלות השונות המוטלות על הרשויות והחברות האמריקאיות באיסוף נתונים על תושבי ואזרחי ארצות הברית תוך פגיעה בפרטיותם.

7. <u>עבירות ביטחוניות אחרות</u>- כהערה כללית עלינו לזכור כי Title VIII של ה-Patriot Act מגדיר סייבר טרור, חדירה למחשבים של רשויות ממשלתיות, ופעולות אחרות שאינן בהכרח בעלות גוון טרוריסטי מובהק, כמעשה טרור[129], ומכוח זאת מאפשר הפעלת אמצעי מעקב מקוונים גם כלפי פעילויות אלו.

לסיכום, ראינו בפרק זה כי ה- Patriot Act מחיל הוראות חוק העוסקות במודיעין ובריגול זר גם על אזרחי המדינה. הוראות אלה מתאפיינות במידה פחותה של איזונים ובלמים ומעניקות לרשות החוקרת כר פעולה נרחב לחדור לצנעת הפרט. ה- Patriot Act מדגיש את סמכויות השלטון על חשבון חירות הפרט. הסטה זו נעשתה בשמה של המלחמה בטרור אך היא מקיפה הרבה יותר, חולשת על פעילויות רבות שאינן קשורות ישירות למאבק בטרור ופוגעת קשות בזכות לפרטיות של אזרחים שאינם מעורבים בטרור. הדבר ממחיש את הצורך בהפרדה ברורה בין איזונים ובלמים שקובע החוק ביחס להפעלת אמצעי מעקב על ידי שירותים חשאיים ביחס למלחמה בטרור, לבין הפעלת אמצעים אלו על ידי רשויות חקירה ואכיפת חוק אחרת ביחס למניעת פשיעה או שמירה על אינטרסים לאומיים אחרים – צורך אשר נדון בו בפרק הרביעי בעבודה זו.

בפרקים הבאים ננסה לבחון, מול המודלים השונים במשפט המשווה שסקרנו לעיל, האם האיזונים והבלמים שנקבעו בדין הישראלי בהקשר הפעלת המעקב המקוון על ידי גורמי מודיעין מסכל הם ראויים.

3.2. <u>ישראל - הדין המצוי:</u>

אמצעי סיכול ואכיפה המופעלים על ידי רשויות השלטון בישראל ובהם גורמי מודיעין מסכל, תחומים מבחינה פורמאלית על ידי כללים ועקרונות מהמשפט הציבורי. ראשית, רשויות המדינה כפופות למשפט החוקתי ולזכויות היסוד שהוכרו כמסגרת על נורמטיבית. שנית, הרשויות כפופות לעקרונות המשפט

---

124 USA Patriot Act § 815, § 222, 50 U.S.C. §1881(h)(1)-(3).

125 50 U.S.C. §1881(h)(5).

126 Charles Doyle, *The USA PATRIOT Act: A Legal Analysis*, Congressional Research Service, The Library of Congress, CRS Report for Congress, April 15, 2002, page 19.

127 USA Patriot Act § 203.

128 H.R.3523, available at: thomas.loc.gov/cgi-bin/query/z?c112:H.R.3523 .

129 USA PATRIOT Act, Title VIII, Sec. 814. Amended 18 U.S.C. § 1030(e).

המנהלי, המתווים מסגרת של פעולה לפי עיקרון החוקיות, הסמכות, שיקול הדעת (פעולה בסבירות, הגינות מהותית ודיונית ומידתיות) ולבסוף כפופות הרשויות לביקורת שיפוטית[130].

הזכות לפרטיות הינה זכות יסוד חוקתית המעוגנת ב**חוק יסוד: כבוד האדם וחירותו**. כל פגיעה בזכות זו חייבת להיעשות בהתאם לתנאי פסקת ההגבלה, כלומר להיעשות בחוק, או מכוחו, עליה להלום את ערכיה של מדינת ישראל כמדינה יהודית ודמוקרטית, להיות לתכלית ראויה ובמידה שאינה עולה על הנדרש[131]. עוד טרם עיגונה החוקתי של הזכות לפרטיות, חוקקה הכנסת את **חוק הגנת הפרטיות, התשמ"א-1981**. לפי החוק, פגיעה בזדון בזכות לפרטיות הינה עבירה פלילית, אך אם נעשתה הפגיעה בפרטיות בנסיבות בהן מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה הוא יזכה להגנה מפני תביעה אזרחית או פלילית[132]. חוק הגנת הפרטיות קובע בסעיף 2 כי האזנה אסורה מהווה פגיעה בפרטיות אך איסוף מידע באמצעות מחשב אינו מנוי על סעיף זה כפגיעה אפשרית בפרטיות, אולם רשימה זו הינה רשימה פתוחה, הניתנת להשלמה על-ידי בית המשפט. בפסיקה הישראלית אין הגדרה אחידה לזכות לפרטיות. על פי רוב בוחרת הפסיקה שלא להגדיר את הזכות לפרטיות, אלא לקבוע בכל מצב לגופו האם האינטרס הנדון כלול בזכות לפרטיות. בדרך זו, אינטרסים רבים ומגוונים נכנסו אל גדרי הזכות לפרטיות[133]. עם זאת, הזכות לפרטיות אינה זכות אבסולוטית, והיקף ההגנה שתינתן לה תלוי בהתחשבות באינטרסים אחרים. בתת-פרק זה נסקור את ההסדרים המשפטיים המאפשרים פגיעה בפרטיות בישראל בתחום המעקב המקוון של גורמי ביטחון ביחס לסיכול טרור.

3.2.1. <u>מודיעין מסכל בישראל - שירות הביטחון הכללי</u>

שירות הביטחון הכללי של מדינת ישראל, הוקם בסמוך לקום המדינה, אולם תפקידיו, מבנהו וסמכויותיו, לא נקבעו עד שנת 2002 בחוק, אלא בהחלטות ממשלה בלבד, ובאופן חלקי[134]. במהלך השנים ניתן ביטוי בחקיקה לסמכויות שונות של השב"כ[135], אך למעט הסדרים נקודתיים אלו, מעמדו של השב"כ, תפקידיו, סמכויותיו ודרכי הפיקוח על פעילותו, לא זכו עד לכניסתו לתוקף של **חוק שירות הביטחון הכללי**[136] להסדרה כוללת בחקיקה. חוק השב"כ קובע כי השירות מופקד על שמירת ביטחון המדינה, סדרי המשטר הדמוקרטי ומוסדותיו מפני איומי טרור, חבלה, חתרנות, ריגול וחשיפת סודות מדינה. כן קובע החוק כי השירות ימלא בין השאר את התפקידים של סיכול ומניעה של פעילות בלתי חוקית שמטרתה לפגוע בביטחון המדינה, בסדרי המשטר הדמוקרטי או במוסדותיו. כמו כן יפעל השירות לקידום של אינטרסים ממלכתיים חיוניים אחרים לביטחון הלאומי של המדינה ואף לאסוף ולקבל מידע לשמירה ולקידום מטרות ותפקידים אלו[137]. החוק גם מסמיך את השירות לקבל ולאסוף מידע מודיעיני ולחקור חשודים וחשדות בתחומי פעילותו ולצורך מילוי תפקידיו[138]. למעט תקנות מכוח חוק השב"כ, כללי השירות, הוראותיו

---

130 איינהורן ואח', לעיל ה"ש 50, עמ' 67.

131 סעיפים 7 ו- 8 לחוק יסוד: כבוד האדם וחירותו.

132 ראה ס' 5 וס' 18(2)(ב) לחוק הגנת הפרטיות.

133 יעל און ואח', לעיל ה"ש 61, עמ' 7-6.

134 הצעת חוק השב"כ, לעיל ה"ש 56, עמ' 244.

135 **חוק האזנת סתר**, התשל"ט – 1979, ס"ח 938, **חוק הגנת הפרטיות**, התשמ"א – 1981, ס"ח 1011.

136 **חוק שירות הביטחון הכללי** תשס"ב-2002, ס"ח 1832 (להלן: חוק השב"כ).

137 ראה סעיף 7(א) לחוק שירות הביטחון הכללי וכמו כן הצעת חוק השב"כ, לעיל ה"ש 56, עמ' 245. בהקשר זה יש לציין כי ניתן בהחלט להעלות ביקורת כלפי הגדרת תפקידי השירות לקידום "אינטרסים ממלכתיים חיוניים אחרים לביטחון הלאומי של המדינה" שכן תפקיד זה משאיר פתח רחב להרחבת סמכויות השירות ולהפעלת אמצעים חודרניים של מעקב פולשני הפוגע בפרטיות כלפי מטרות שונות שלאו דווקא עומדים בקנה אחד עם סיכול טרור. לביקורת בהקשר זה ראה האגודה לזכויות האזרח "**הצעת חוק השב"כ – הערות האגודה לזכויות האזרח**" (2002), פורסם ב www.acri.org.il/he/?p=5634 .
וראה גם צימרמן אריאל "**הצעת חוק השב"כ : ניתוח משווה - הערות מרכזיות להצעת החוק לאור המשפט המשווה**" המכון הישראלי לדמוקרטיה , נייר עמדה מס' 3, ירושלים , התשנ"ז 1997.

138 ראה סעיף 8(א) לחוק השב"כ. כאמור, איסוף מידע הינו בין התפקידים המרכזיים של כל שירות בטחון. בישראל, כמו באנגליה, קיימת חקיקה נפרדת, המסדירה את נושא איסוף המידע ודבר זה לא מוסדר בחוק המקים את השירות החשאי. בהקשר זה הועלתה ביקורת על סעיף 8(א) לחוק אשר נטען כלפיו שהוא סוטה מהאיזונים, שנקבעו בחקיקה מוקדמת יותר, ומרחיב מעבר לקיים את סמכות השב"כ לאסוף מידע באמצעות האזנת סתר או קבלת מידע מגורמים אחרים. בישיבת הוועדה לחוץ וביטחון בוועדת חוק, חוקה ומשפט של הכנסת ביום 25/6/98 נאמר, כי אין בכוונת יוזמי הצעת החוק להרחיב את הסמכות של אנשי השב"כ מעבר לקיים את ביחס לאיסוף מידע באמצעות האזנת סתר או קבלת מידע מגורמים אחרים, אלא רק לעגן בחוק השירות את מהותו של השב"כ כארגון, המופקד על

ונהליו לפי חוק זה אינם טעונים פרסום ברשומות או פרסום פומבי אחר[139]. בהיעדר פומביות של הנחיות פנימיות הרי שקשה מאוד לדעת כיצד נוהג ארגון זה במידע המודיעיני שהוא אוסף ובכלל זה המידע המופק כתוצאה ממעקב מקוון. למעשה, המסמך הפומבי היחיד בהקשר זה הינו הקוד האתי של השירות[140] אשר אושר בשב״כ בשנת 1998. חזון השירות קובע שפעילות השב״כ תתבצע באורח ממלכתי, בכפיפות לחוק ובנאמנות לערכי הדמוקרטיה והשירות. ערכי השב״כ כפי שהם משתקפים במסמך זה מציינים כי עובד השירות מחויב לפעול בכפיפות למערכת החוק והשלטון ותוך כיבוד המשטר הדמוקרטי והקפדה על עיקרון ״ריסון הכוח״ אשר לפיו, יפעיל עובד השירות סמכויות שהוקנו לו לצורך מילוי תפקידו, באורח מושכל , מבוקר והוגן, תוך התחשבות בזכויות היסוד ובכבוד האדם.

3.2.2. <u>**חיפוש ותפיסת חומר במערכות מחשב:**</u>

על החדירה למחשבו של אדם כבר נאמר כי היא *״גרועה לא פחות מן הפריצה לביתו. ביתו של אדם הוא מבצרו, ומחשבו האישי הוא פינת הסתר החבויה במבצר, הוא המגירה האישית של בעליו, והוא אוצר בתוכו, תכופות, מידע פרטי, אישי, ולעיתים כמוס. החדירה אל המחשב האישי כמוה כחיטוט בחפציו האינטימיים״*[141].

חיפוש ותפיסה מותרים בדין על מנת להגן על אינטרסים של ביטחון המדינה, על הזכות לחיים, וכן כדי לאפשר מניעת פשעים וענישה. מנגד, עלולות פעולות אלו לפגוע כמובן בזכות לפרטיות. בישראל הכלל לעריכת חיפוש הוא בצו שופט לפי הוראות **פקודת סדר הדין הפלילי (מעצר וחיפוש)**[142]. מאחר והוראות החיפוש בפסד״פ לא כללו חיפוש בחומר מחשב, הן תוקנו עם חקיקת **חוק המחשבים תשנ״ה-1995**, כך שמתאפשר גם חיפוש מידע או תוכנה המצויים במחשב או שייכים לו כשנוספו להגדרת ״חפץ״ המונח ״חומר מחשב״, וכמו כן התווספו הגדרות המונחים ״מחשב״ ו״פלט״ לפסד״פ כהגדרתם בחוק המחשבים[143]. שופט בית משפט שלום יכול להתיר צווי חיפוש וחדירה לחומר מחשב מכוח הפסד״פ וצו חיפוש כאמור יכלול גם את ההיתר לחדור לחומר מחשב ופירוט ביחס למטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש[144].

על אף שחיפוש בידי רשויות הביטחון ואכיפת החוק מהווה חדירה משמעותית לפרטיות האדם, ככלל, הוצאת צווי חיפוש היא עניין שבשגרה. כאמור, שופט שלום הוא שמוסמך להתיר את החיפוש וזאת מבלי שמתקיים דיון משפטי של ממש או בחינה מעמיקה בדבר היקף הפגיעה בפרטיות. בישראל מוגשות מידי יום מאות בקשות להוצאת צווי חיפוש ואין כל אפשרות פרקטית לבחון כל בקשה ובקשה לגופה ולקיים דיון מעמיק באשר למטרות החיפוש, לקיומה של דרך חלופית להשגת תכלית החיפוש אשר פגיעתה בחשוד פחותה, לבחינת היקף החיפוש ונוהל חיפוש שיקטין את הפגיעה ואת החדירה לרשות היחיד[145].

בעניין פילוסוף, נקבע גם כי כל תכתובות הדוא״ל הנמצאות במחשבו של החשוד ובכלל זאת התכתבויות צ׳אט או מסרים מיידים השמורים על המחשב, מכל סוג שהוא, מהוות ״חפץ״ בר תפיסה ולא ״שיחה״, בין אם אלו נקראו או לאו. כלומר, עם תפיסתו של מחשב קצה או מכשיר סלולארי השייך לחשוד, כל תכתובת שכזו, בין אם הגיעה אחרי התפיסה או לפניה, בין אם נקראה או לא, היא חפץ ומצריכה צו חיפוש ולא את ההסדר המחמיר יותר של צו או היתר האזנה[146] עליו נדון בהמשך. בעניין פילוסוף ציין גם בית המשפט

איסוף וניתוח מידע וכי חיקוקים אלו מהווים הסדר ספציפי, הגובר על ההוראה הכללית שבחוק השב״כ. לביקורת בהקשר זה האגודה לזכויות האזרח, לעיל ה״ש 136, שם.

139 ראה סעיף 22(א) לחוק שירות הביטחון הכללי.

140 ״**יעוד, ערכים וחזון השירות**״, מפורסם באתר שירות הביטחון הכללי www.shabak.gov.il/about/pages/values.aspx.

141 דברי השופט א׳ ריבלין, כתוארו אז, בבש״פ 7368/05 **זלוטובסקי ואח׳ נ׳ מדינת ישראל** (פורסם בנבו), פסקה 7 לפסק הדין.

142 **פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש]**, תשכ״ט-1969. להלן: הפסד״פ.

143 ראה סעיף 1 לפסד״פ, ראה גם סעיף 11 לחוק המחשבים.

144 ראה סעיפים 23 ו-23א לפסד״פ. יצויין כי ניתן גם לתפוס חומר במערכת מחשב מכוח סעיף 43 לפסד״פ (הזמנה להשיג חפץ).

145 עניין פילוסוף, לעיל ה״ש 65, עמ׳ 13.

146 עניין פילוסוף, לעיל ה״ש 65, עמ׳ 15, כנסת ישראל, **סיכום דיוני ועדת החקירה הפרלמנטרית לחקר האזנות הסתר**, ינואר 2009, עמ׳ 27.

המחוזי בהחלטתו כי הפרקטיקה הנוהגת כיום מלמדת כי לא נשתנה שינוי של ממש עם תיקון הפסד"פ לעיל ביחס לחיפוש בחומר מחשב. אומנם נדרש כי צו החיפוש יציין במפורש את ההיתר לחדור לחומר מחשב ואת תנאי החיפוש ומטרותיו, אולם בפועל מוספת הוראה כללית לטופס צו החיפוש בדבר מטרת החיפוש והסמכות לחפש ולתפוס גם חומר מחשב. אין בהוראה זו כדי להנחות ולהוסיף תוספת של ממש בדבר העילות והשיקולים שיש לשקול בבקשת צו חיפוש או במתן היתר לחיפוש בחומר מחשב[147].

יש לזכור כי הפסד"פ וחקיקה נוספת כגון **הפקודה למניעת טרור, תש"ח-1948** ו**תקנות ההגנה (שעת-חירום), 1945** מתייחסות לחיפוש בהקשרו הפלילי או הביטחוני-מניעתי בלבד לצורך חקירה פלילית, איסוף ראיות להעמדה לדין או הרתעה מפני החזקת אמצעי לחימה. חוק השב"כ מקנה גם סמכות ביחס לחיפוש למטרת מודיעין גרידא לצרכי סיכול. הבעייתיות בכך היא שהסמכות לחיפוש למטרות מודיעין אינה צריכה להיות כרוכה בהכרח בקיומו של חשד פלילי כלשהו ביחס לאדם מסוים, אלא בהערכה כי מצוי ברשותו מידע חיוני[148]. חוק השב"כ מתיר לבעלי תפקידים מבין עובדי השירות לערוך חיפוש, לתפוס חפץ או לאסוף מידע בתחנות גבול של ישראל, וכן קובע כי ראש הממשלה רשאי להתיר בכתב עריכת חיפוש ואיסוף מידע בכלי רכב ובחצרים שלא בנוכחות בעליהם או המחזיק בהם וללא ידיעתו, אם שוכנע כי יש במקומות אלו מידע חיוני לשם מילוי תפקידי השירות. ראש השירות רשאי להתיר בכתב ביצוע חיפוש סמוי כאמור גם ללא היתר מראש הממשלה במקרים דחופים[149]. חוק השב"כ אינו מתייחס מפורשות לחיפוש בחומר מחשב או באמצעות חדירה לחומר מחשב למרות שחוקק לאחר חוק המחשבים. הצעת חוק השב"כ לא שופכת אור על הנושא למעט הסמכת אנשי השב"כ להפעיל סמכויות שוטר, ובהקשר זה יש להניח כי אנשי השירות יכולים לבצע חיפוש וחדירה לחומר מחשב לפי הוראות הפסד"פ.

בהיעדר מידע גלוי אודות אמצעי המעקב שיכול להפעיל השב"כ על אזרחי ישראל במסגרת תפקידו לשמירה על ביטחון המדינה מאיומי טרור, ניתן רק להניח כי השב"כ מבצע גם הוא, כמו ארגוני ביון מערביים אחרים, פעילויות חדירה סמויות למחשבים במטרה להשיג מידע שיכול להביא לסיכול טרור, גם באמצעים חודרניים כגון רוגלות וסוסים טרויאניים. לכאורה, חיפוש מסוג זה באמצעות חדירה מרחוק לרשת מחשב מהווה האזנה, אך סעיף 23א(ג) לפסד"פ קובע שקבלת מידע מתקשורת בין מחשבים אגב חיפוש, לא תיחשב להאזנת סתר וחדירה לחומר מחשב. מכאן ניתן להסיק כי מקום שניתן צו חיפוש המתיר חדירה לחומר מחשב יכולה חדירה זו להתבצע גם מכוח התקשרות עם המחשב ולא יידרש היתר להאזנת סתר (ראה הדיון בפרק 3.2.3 להלן). לאור זאת, ניתן בהחלט לטעון כי הסמכה לביצוע חיפוש סמוי במחשב באמצעות רוגלה או סוס טרויאני מכוח פרשנות מרחיבה לדבר חקיקה כללי ביחס לחיפוש בחומר מחשב לא מקנה משקל מספק לפגיעה החמורה בפרטיות (במיוחד נוכח חיפוש סמוי וחדירה לחומר מחשב של אדם ללא ידיעתו) כאשר הטכנולוגיה המתקדמת מטשטשת את הגבולות בין "חיפוש" ל"האזנה".

בפרק הבא ננסה לעמוד על נקודה זו ונשאל האם אכן יש צורך של ממש להתייחס באופן פרטני לאפשרויות ההאזנה והניטור השונות בדברי החקיקה שמסמיכים את המודיעין המסכל בישראל לבצע פעולות מעקב מקוון.

3.2.3. <u>האזנת סתר:</u>

חוק האזנת סתר, *תשל"ט*-1979[150] מסתמך על המודל האמריקני, בו קיימת אבחנה בין האזנת סתר אסורה, לבין האזנה לשיחה והקלטתה בהסכמת אחד מבעלי השיחה, שהיא מותרת[151]. מטרתו של חוק

---

147 להרחבה בנושא זה ראו נמרוד קוזלובסקי, **המחשב וההליך המשפטי**, הוצאת לשכת עו"ד, התשס"א 2000, עמ' 54 - 65.

148 אריה רוטר, לעיל ה"ש 55, עמ' 47.

149 ראה סעיפים 9 ו- 10 לחוק השב"כ.

150 **חוק האזנת סתר**, תשל"ט-1979, ס"ח תשל"ט 938, להלן: "חוק האזנת סתר" או בסעיף זה "החוק".

האזנת סתר היא כפולה: לתת בסיס משפטי ברור וישיר להגנת הפרט מפני התערבות בצנעתו המבוצעת על ידי האזנה לשיחותיו ללא ידיעתו ולהבטיח את ההגנה על ידי הוראה האוסרת האזנה אסורה[152].

לפי חוק האזנת סתר, האזנה לשיחת הזולת, קליטתה או העתקתה, באמצעות מכשיר וללא הסכמה של אף אחד מבעלי השיחה היא האזנת סתר אסורה[153]. חוק האזנת סתר הגדיר בראשיתו "שיחה" כ"בדיבור או בדרך תקשורת אחרת". כשנחקק החוק לא חזה המחוקק לנגד עיניו אפשרות לציתות ומעקב אחר הפרט במדיה הדיגיטלית, אך כיום, לאחר תיקון תשנ"ה-1995 לחוק האזנת סתר בעקבות חוק המחשבים, "שיחה" מוגדרת ככוללת "תקשורת בין מחשבים"[154]. אמנם חוק האזנת סתר אינו מגדיר את המונחים "תקשורת בין מחשבים" או "מחשב", אך ההתייחסות לנושא בפסיקה מצביעה על כך שהמושג כולל בין היתר גם קליטת מידע מתקשורת בין מחשבים כגון דואר אלקטרוני או התכתבות בצ'ט או תוכנת מסרים מיידים. על כן, בהיעדר הסכמה של המשוחחים זוהי האזנת סתר המהווה עבירה פלילית לפי סעיף 2 לחוק האזנת סתר[155]. עם זאת, ספק אם גלישה ברשת האינטרנט נחשבת שיחה לצורך חוק האזנת סתר[156]. יש לציין כי האזנה לתקשורת בין מחשבים אינה מהווה "חדירה לחומר מחשב", כאמור בסעיף 4 לחוק המחשבים. סעיף 2(2) לחוק הגנת הפרטיות קובע, כי "האזנה אסורה על-פי חוק" מהווה פגיעה בפרטיות[157].

חוק האזנת סתר מסייג את תחולת האיסור על האזנת סתר בקובעו שני חריגים הרלוונטיים לעניין האינטרס של שמירה על ביטחון המדינה:

<u>א. האזנה ברשות הרבים</u>- החריג הראשון, מתייחס למקרים בהם ההאזנה מותרת מלכתחילה ללא צורך בהיתר. סעיף 8(1)(א) לחוק האזנת סתר קובע כי כאשר השיחה נערכת ברשות הרבים, האזנה לה על-ידי מי שהסמיכו ראש רשות ביטחון – כלומר, ראש השב"כ וראש אמ"ן - מטעמים של ביטחון המדינה, אינה האזנת סתר שלא כדין ואינה טעונת היתר לפי החוק. סעיף 8 לחוק מגדיר את המונח "רשות הרבים" כ"*מקום שאדם סביר יכול היה לצפות ששיחותיו יישמעו ללא הסכמתו, וכן מקום שבו מוחזק אותה שעה עצור או אסיר*". על אף שהאזנות אלו טעונות הסמכה, נמנע החוק מלקבוע כיצד תוקנה הסמכה זו, ובפועל הכירו בתי המשפט במתן הסמכה כללית לרשויות המוסמכות לביצוען של האזנות ברשות הרבים[158]. עם זאת, נראה כי ההסמכה חייבת להיות שמית, להתייחס לעניין מסוים, וככל שניתן להיות מוגבלת בזמן ובמקום. מהפסיקה מסתמנת ההלכה, לפיה כל שימוש באמצעי תקשורת, המאפשר נגישות לציבור הרחב, חשוף להאזנת סתר שאינה טעונת היתר לפי חוק האזנת סתר, וכי אין למשוחח בשיחת רשת צפייה סבירה לפרטיות או יסוד לסברה שלא יאזינו לדבריו[159]. ככל הנראה התכתבות דוא"ל איננה רשות הרבים, אך כתיבה בפורומים ושיחה בצ'אט יוכלו בהחלט להיראות כרשות הרבים. על כן רשויות הביטחון בישראל יכולות להאזין לתכתובות אלו של אדם, גם אם זה ניסה לנקוט באמצעים על מנת לשמור על פרטיותו באמצעים הזמינים לו. האזנה זו אינה מחייבת השגת צו מבית משפט אלא ניתנת לביצוע באמצעות הסמכה של ראש רשות ביטחון ללא ביקורת של בית משפט על הליך ההסמכה.

---

152 איינהורן ואח', לעיל ה"ש 50, עמ' 87-86.

153 ע"פ 1497/92 **מדינת ישראל נ' אלי בן משה צוברי**, פ"ד מז (4) 177.

153 ראה הגדרת "האזנה" ו"האזנת סתר" בסעיף 1 לחוק האזנת סתר.

154 ראה הגדרת "שיחה" בסעיף 1 לחוק האזנת סתר. בדברי ההסבר בהצעת חוק המחשבים התשנ"ד-1994 נאמר כי אחת ממטרות החוק היא "התאמת החקיקה הקיימת בתחום האזנת הסתר למציאות המיוחדת בתחום המחשבים".

155 יצויין כי סעיף 2 לחוק האזנת סתר קובע שתי עבירות פליליות נוספות: עבירת השימוש במידע ועבירת הצבת מכשירים.

156 משרד המשפטים, לעיל ה"ש 60, עמ' 86.

157 עם זאת, בעוד שהאזנת סתר מהווה עוולה לפי חוק הגנת הפרטיות, היא אינה מהווה עבירה פלילית לפי אותו חוק ראה סעיף 4 וסעיף 5 לחוק הגנת הפרטיות.

158 ראו לעניין זה: תקנה 2 לתקנות האזנת סתר, התשמ"ו 1986- , ק"ת התשמ"ו 111 אשר קובעת כי הסמכה לעניין החוק והתקנות תהיה מראש ובכתב, אולם רשות ביטחון תוכל לתת הסמכה בדיעבד, מטעמים מיוחדים שיירשמו, אם לא היה סיפק בנסיבות הענין לגבי מתן הסמכה מראש.

159 נמרוד קוזלובסקי, לעיל ה"ש 147, עמוד 91.

ב. האזנת סתר למטרות ביטחון המדינה- החריג השני הרלוונטי לענייננו, חל על מקרים בהם יינתן היתר להאזנת סתר, שלא ברשות הרבים. החוק מציב מחסומים מהותיים ודיוניים חמורים יותר בפני האזנה לרשות היחיד והאזנה שכזו תותר לשם הגנה על ביטחון המדינה או מניעת עבירות וגילוי עבריינים. פרק ב' של חוק האזנת סתר עוסק בהאזנה למטרות ביטחון המדינה וניכר כי המחוקק בחר במודע להעדיף את ביטחון המדינה על פני זכות האזרח לפרטיות[160]. ואכן לפי פרק ב' אין צורך בצו שופט להאזנה למטרות ביטחון המדינה ותחת זאת מסתפקים בהיתר בכתב מאת ראש הממשלה או שר הביטחון, ובמקרים דחופים בהיתר מאת ראש השב"כ או ראש אמ"ן[161]. לשם ביצוע האזנה לצרכי ביטחון על ראש רשות ביטחון להגיש בקשה בכתב לשר הביטחון או לראש הממשלה. אם שוכנע השר או ראש הממשלה, שהדבר דרוש מטעמי ביטחון המדינה, לאחר ששקלו גם את מידת הפגיעה בפרטיות יכולים הם להתיר את האזנת הסתר בכתב וללא צו בית משפט[162].

למרות החשש הברור לפגיעה בפרטיותו של אדם אשר מתבצעת האזנה על תכתובותיו ושיחותיו, המחוקק לא הגדיר את המונח "ביטחון המדינה", וכך השאלה מה נופל לגדרי מונח מעורפל זה הופכת למהותית שכן זהו מרכיב מרכזי בהחלטתם של ראש הממשלה או שר הביטחון להתיר האזנת סתר[163]. **בפרשת פלונים**[164], ציין בית המשפט העליון מפי הנשיא ברק ביחס ל"ביטחון המדינה" כי מושג זה סובל פירושים ומשמעויות רבות. קיימת גישה בספרות המשפטית, לפיה באיזון שבין ביטחון המדינה לבין זכותו של האדם לפרטיותו ושמירת סוד שיחתו, יהיה נכון להעדיף את ביטחון המדינה באותם מקרים שהפעולה בקשר אליהם תביא למניעת פגיעה בנפש של אזרחי המדינה[165]. במובן זה, הפסיקה הישראלית הכירה בשורה ארוכה של מקרים במצבים שבהם ביטחון המדינה ושלום הציבור יצדיקו פגיעה והגבלה על זכויות האדם[166]. המונח ביטחון המדינה נשאר עמום למדי ומאפשר פרשנות רחבה, וביחס לפגיעה בזכויות האדם בביצוע פעולות מעקב והאזנה באמצעים אלקטרונים הרי שהחשש הוא שאמצעים אלו לא יופנו רק לטיפול באיומי טרור אלא גם באינטרסים אחרים שלא מצדיקים את רמת האיזונים שקבע חוק האזנת סתר בהקשר זה.

חוק האזנת סתר קובע שהיתר להאזנת סתר למטרת ביטחון המדינה יתאר את זהות האדם אשר ההאזנה לשיחותיו הותרה, או זהות הקו או המיתקן המשמשים או המיועדים לקליטה, להעברה או לשידור והאזנה אליהם הותרה, מקום השיחות או סוגן, אם אלו ידועים מראש וכמו כן יפורטו דרכי ההאזנה שהותרו. היתר לביצוע האזנת סתר למטרת ביטחון המדינה ניתן לתקופה שלא תעלה על שלושה חודשים, וניתן להאריכו מפעם לפעם[167]. ניתן לראות שהסדר זה מאפשר לרשויות הביטחון בישראל מרחב פעילות לא מבוטל כשהחשש הוא ששר הביטחון או ראש הממשלה לא יקיימו ביקורת על הליך מתן האישורים ויטו לאשר את רובם, במיוחד נוכח היקפם הגדול של בקשות אלו. עוד אנו רואים שבקשה להיתר להאזנת סתר עשויה להכיל את דרך ההאזנה שהותרה בלבד, מבלי שצוינו זהות החשוד, המתקן המהווה מטרה להאזנה, מקום השיחות וסוגן. החשש לפגיעה בפרטיות של צדדים שלישיים תמי לב בהקשר זה הוא ברור.

במקרים דחופים, כשראש רשות ביטחון שוכנע כי ביטחון המדינה מחייב האזנת סתר שאיננה סובלת דיחוי, ראשי הוא להתיר האזנת סתר למשך 48 שעות גם ללא אישור השר. על היתר זה יעדכן בדיעבד ראש

---

160 **הצעת חוק דיני העונשין (האזנת סתר)**, תשל"ח-1978, מציינת: *"הסעיף מבוסס על ההנחה שצרכי ביטחון המדינה גוברים על שיקולי חופש הפרט, ולפיכך יש להבטיח שרשות בדרג רם שעניינה בכך אכן תשוכנע שהמדובר הוא בצורכי ביטחון המדינה".*

161 ראה הגדרת "שר" בסעיף 1 וסעיף 4 לחוק האזנת סתר והגדרת "רשות ביטחון" בסעיף 1 וכן את סעיף 5 לחוק האזנת סתר.

162 ראה סעיף 4(א) לחוק האזנת סתר.

163 שופט בית המשפט העליון לשעבר חיים כהן, אמר על המונח "טעמים של ביטחון המדינה" בעת שדיבר בפני וועדת חוקה חוק ומשפט של הכנסת כשזו הכינה את חוק האזנת סתר לקריאה שנייה ושלישית: "אינני יודע מה זה בדיוק ואני מעז לומר שאיש מכם לא יודע מה זה". מובא בדן חי, **ההגנה על הפרטיות בישראל**, מילגה הוצאה לאור בע"מ (תשס"ו-2006), עמ' 666.

164 עמ"מ 94 / 10 **פלונים נ' שר הביטחון**, נג (1) 97.

165 דן חי, לעיל ה"ש 163, עמוד 667.

166 ראה בג"צ 73/53 **חברת "קול העם" בע"מ נ' שר-הפנים**, פ"ד ז(2) 871, בג"צ 16/48 **ברון נ' ראש הממשלה ושר הבטחון**, פ"ד א 109, בג"צ 951/06 **עזרא שטיין נ' רב ניצב משה קראדי**, דינים עליון 2006 (26) 755.

167 ראה סעיפים 4(ב) ו- 4(ג) לחוק האזנת סתר.

רשות ביטחון את השר בכתב והשר רשאי לבטל את ההיתר[168]. בישראל לא קיים מידע פומבי אודות בקשות להיתרים להאזנת סתר של השב"כ או אמ"ן, ועל כן קשה לבחון את הנפקות של האפשרות לביטול ההיתר, במיוחד במצבים שבהם היתר בוטל בדיעבד, לאחר שבוצעה האזנת סתר דחופה.

חוק האזנת סתר מאפשר גם לרשות ביטחון להאזין לתקשורת בין מחשבים שהעדות עליה חסויה לפי **פקודת הראיות [נוסח חדש], תשל"א-1971** כגון שיחות עם עורך דין, רופא, פסיכולוג, עובד סוציאלי או כהן דת. באופן זה יכול ראש רשות ביטחון לפנות בכתב, באישור היועץ המשפטי לממשלה, לנשיא בית משפט מחוזי, בעבירות מסוג פשע שיש בהן סכנה לביטחון המדינה והאזנת הסתר דרושה מטעמי ביטחון המדינה[169]. סעיף 5(ג) לחוק האזנת סתר מאפשר במקרים דחופים גם לראש רשות ביטחון להתיר בעצמו, ללא צורך בפניה לבית משפט, האזנת סתר לשיחה חסויה לפי פקודת הראיות כאשר הדיווח על היתר זה יינתן לאחר מכן בכתב ליועץ המשפטי לממשלה.

חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007 (להלן: חוק נתוני תקשורת) הוביל גם לתיקון לחוק האזנת סתר כשהוסיף לו בשנת 2007 את סעיף 9ג המאפשר לנותן ההיתר לביצוע ההאזנה, להתיר גם הפקת נתוני תקשורת כמשמעותם בחוק נתוני תקשורת, של המנוי או מיתקן הבזק שההאזנה הותרה לגביהם, למשך תקופת תוקפו של ההיתר. חוק האזנת סתר מסמיך את מי שמוסמך להתיר האזנת סתר להתיר כניסה למקום לצורך התקנת אמצעים הנדרשים להאזנה, פירוקם וסילוקם[170].

אם נשווה את ההסמכה להאזנת סתר לעומת סמכויות החיפוש במחשבים בפסד"פ, נראה כי היתר האזנה לצורכי ביטחון המדינה טומן פגיעה קשה בפרטיות, אף קשה מזו הנובעת מצו חיפוש. בעוד החיפוש מבוצע באורח חד-פעמי ובידיעתו של החשוד, האזנת סתר נמשכת לאורך זמן, נעשית ללא ידיעתו של החשוד, ואף עלולה לפגוע בפרטיותם של צדדים שלישיים תמי-לב[171]. כל זאת כאשר בחלק גדול מהמקרים ההיתר להאזנת הסתר לא ניתן על ידי רשות שיפוטית אלא על ידי שר בלבד שיכול אף לאשר את ההיתר בדיעבד, ומעבר לכך במקרים דחופים מאשר זאת ראש רשות ביטחון בלבד. במצב זה, בו די שראש שירות החליט כי ההאזנה היא חיונית ואינה סובלת דיחוי, החשש כאן הוא שהחריג (היתר על ידי ראש השירות בלבד) יהפוך לכלל והבעייתיות בהיעדר מוחלט של פיקוח על ההיתרים ברורה לכל[172].

סעיף 2ב לחוק האזנת סתר מתיר לרשויות המדינה לעשות שימוש גם בהאזנת סתר שנעשתה שלא כדין ומאפשר ליועץ המשפטי לממשלה, לפרקליט המדינה או לפרקליט הצבאי הראשי, להקשיב או לעיין בדברים שנתקבלו בהאזנת סתר שנעשתה שלא כדין למטרות מניעה או חקירה של פשע חמור או למניעה או חקירה של כל פשע מטעמים מיוחדים של חומרת העניין. חריג זה לא יחול על האזנת סתר שנעשתה שלא כדין על ידי מי שרשאי לקבל היתר לפי חוק האזנת סתר, אלא אם כן האזנת הסתר נעשתה בטעות בתום לב, תוך שימוש מדומה בהרשאה חוקית. אנו רואים שגם אם רשות ביטחון לא קיבלה היתר להאזנה ובכל זאת ביצעה האזנת סתר, ניתן לעשות שימוש בהאזנה זו וכי המרווח שהושאר לרשויות הביטחון רחב מאוד ויכול לאפשר גם פגיעה בפרטיות[173].

יצוין כי בשנת 2001 תוקנו **תקנות האזנת סתר** באופן ניכר, והוענקו סמכויות להאזנת סתר גם למספר רשויות שאינן רשויות ביטחוניות. סמכות זו כוללת האזנות סתר הן למניעת וגילוי עבירות והן מטעמי

---

168 ראה סעיפים 5(א) ו-5(ב) לחוק האזנת סתר.

169 ראה סעיף 9א לחוק האזנת סתר.

170 ראה סעיף 10א לחוק האזנת סתר.

171 איינהורן ואח', לעיל ה"ש 50, עמ' 88.

172 צימרמן אריאל, לעיל ה"ש 137, עמ' 33.

173 יצויין כי לפי ס' 13(א) לחוק האזנת סתר ראיות שתושגנה באמצעות האזנת סתר, בניגוד להוראות חוק האזנת סתר, תהיינה, ככלל, בלתי קבילות בכל הליך משפטי שהוא, זולת אם נתקיימו התנאים הנדרשים לקבלת הראייה. כיום, רשאי בית-המשפט, בנסיבות מסוימות ולפי שיקול-דעתו, לקבל כראייה האזנת סתר גם אם הושגה שלא כחוק.

ביטחון המדינה. רשויות אלו יכולות להגיש בקשה לצו האזנת סתר באמצעות פניה לנשיא בית משפט מחוזי ואם אכן ניתן הצו, תבוצע ההאזנה על ידי מי שרשות מוסמכת הסמיכה אותו לבצע האזנת סתר[174]. התקנות קובעות כי רשויות אלו יכולות גם להפיק מידע מודיעיני מחומר המושג בהאזנת סתר זו וכן יכולות הן להעביר את המידע שהושג בהאזנת הסתר לרשות מוסמכת אחרת, כשהחומר שהושג מגלה מידע העשוי לשמש למניעת פגיעה בביטחון המדינה, או לשמש למניעת עבירות או גילוי עבריינים בעבירות מסוג פשע[175].

<u>חומר מחשב והודעות דוא״ל המאוחסנות אצל ספק האינטרנט – חיפוש או האזנת סתר</u>

כידוע, תעבורת דוא״ל אינה נעשית במישרין מהשולח לנמען אלא בתיווכם של ספקי האינטרנט של השולח והנמען. בדרכה מהשולח לנמען, מאוחסנת תעבורת הדואר האלקטרוני באורח זמני אצל ספק השירות. **בעניין נטוויזן**[176] התעוררה השאלה האם רשאית המדינה לחייב ספקי גישה לאינטרנט לבצע פעולות מעקב וציתות לצורכי חקירה פלילית. הגם שעניין זה לא עסק בהאזנת סתר בהקשר ביטחוני, הדיון הרלוונטי לענייננו נסב סביב השאלה האם חדירה להודעות דואר אלקטרוני של מנויי ספק שירותי אינטרנט היא האזנת סתר או חיפוש בחומר מחשב. לשאלה זו יש חשיבות לעניין קבלת היתרים לביצוע האזנת סתר למניעת עבירות שכן לפי סעיף 6 לחוק האזנת סתר יש צורך בצו מאת נשיא או סגן נשיא מוסמך של בית משפט מחוזי לבקשת קצין בכיר, שיתיר זאת; לעומת זאת כדי להתיר חיפוש במחשב ניתן להסתפק בצו חיפוש לפי הפסד״פ שיוציא כל שופט של בית משפט השלום. בעניין נטוויזן נתן בית משפט השלום, לבקשת המשטרה הצבאית, צו חיפוש מכוח הפסד״פ שחייב את חברת נטוויזן למסור תכתובות דוא״ל שישבו בשרתיה הנוגעות למנויים מסוימים ודחה את טענת נטוויזן, כי דוא״ל שהגיע לשרתיה באמצעות תקשורת בין מחשבים, ואשר מצוי בהם בהמתנה שהנמען ימשוך אותו, נכנס לגדר ״שיחה״, כהגדרתה בחוק האזנת סתר. הדיון בערעור בבית המשפט המחוזי בשאלה זו לא נתקיים לאור עמדת פרקליטות המדינה, בעקבות פרשת נטוויזן **ועניין בדיר**[177], לנהוג להבא במקרים מסוג זה כאילו מדובר בהאזנת סתר[178]. לאחר ההכרעה בפסק הדין בעניין נטוויזן, פרסמה בספטמבר 2003 פרקליטת המדינה דאז, כב׳ השופטת עדנה ארבל, הנחיות חדשות בנוגע לסוגיה ואלה ביטלו את ההנחיה שהוצאה בשעתו בעקבות פרשת בדיר. על פי ההנחיה החדשה נקבע כי לצורך שליפת מידע האגור במחשב, ובכלל זה הודעות דוא״ל והודעות קוליות, אין צורך עוד להצטייד בצו האזנת סתר אלא בצו חיפוש. יחד עם זאת, מסייגת פרקליטת המדינה את ההנחיה בכל הנוגע לתפיסת מסרי דואר אלקטרוני ״עתידיים״ בהם יש צורך בהיתר על פי חוק האזנת סתר[179].

ההתפתחות המרכזית של הפסיקה הישראלית בהקשר זה נעשתה **בעניין פילוסוף** אשר למרות שגם הוא מתייחס להאזנה בחקירה פלילית, הדיון בו חשוב לענייננו. גם כאן נסב הדיון סביב השאלה האם דוא״ל האגור בשרת מחשב ספק השירות בדרכו לנמען הוא בבחינת ״חפץ״ אשר ניתן לתפיסה מכוח הוראות הפסד״פ, או שמא מדובר ב״שיחה״ אשר לצורך יירוטה נדרש היתר כדין להאזנת סתר. בית המשפט

---

174 ראה הגדרות ״האזנת סתר״ ו״רשות חוקרת אחרת״ ״רשות מוסמכת״ ״מזמין״ ו-״מבצע האזנה״ בתקנה 1 וכן את תקנה 3 לתקנות האזנת סתר, תשמ״ו-1986. הרשויות אלו הן הרשות להגבלים עסקיים, הרשות לניירות ערך ואגף מס הכנסה ומיסוי מקרקעין, אגף המכס ומס ערך מוסף, משטרה צבאית חוקרת והמחלקה לחקירת שוטרים במשרד המשפטים.

175 ראה תקנות 8 ו- 9 לתקנות האזנת סתר.

176 ב״ש 090868/00 **חב׳ נטוויזן בע״מ נ׳ צבא ההגנה לישראל ואח׳** (פורסם בנבו) (22.6.2000) (להלן: עניין נטוויזן).

177 ת״פ (ת״א) 40250/99 **מ״י נ׳ מונדיר בן קאסם בדיר** (פורסם בנבו) (4.9.2001).

178 **״תפישת הודעות קוליות האגורות בתא קולי ומסרים בדואר אלקטרוני האגורים במחשבי ספק השירות״**, הנחיות פרקליטת המדינה 14.15 (2004).

179 עניין פילוסוף, לעיל ה״ש 65, עמ׳ 4, 8. בעניין פילוסוף נדרש ספק שירותי האינטרנט למסור למשטרה את הדוא״ל הקיים בשרת בעת הוצאת הצו וכל דוא״ל שיגיע לאחסון אצל הספק במשך 30 ימים מיום הוצאת הצו. הצו הדגיש כי ״לא מדובר בהאזנת סתר, אלא בדוא״ל שמאוחסן בחברה״. הדבר מלמדנו על הפרקטיקה הנוהגת באותה תקופה לקבל מידע אודות תכתובות דוא״ל באמצעות צו מכוח הפסד״פ ולא על פי האיזונים שנקבעו בחוק האזנת סתר. כמו כן, טענות המבקשים בפסק הדין בעניין פילוסוף יכולות גם הן לשפוך אור על הפרקטיקה להוצאת צווים לפי הפסד״פ לספקי אינטרנט - נטען כי צווי החיפוש כוללנים ונדרשת בהם תפיסת כל הדוא״ל של בעל תיבת הדוא״ל, מבלי לערוך אבחנה בין דוא״ל אישי או עסקי, הרלוונטי לחקירה הפלילית או הבלתי רלוונטי, לא צוין בצו מי רשאי לבצע הצו, האם כל אדם או שמא ״בעל תפקיד מיומן״, כמו כן הצו הורה כי החיפוש לא יערך בפני עדים מבלי שניתן שום נימוק להוראה זו. נוסף על כך הצווים ציינו כי יש לתפוס ״דוא״ל״ מבלי שניתן להבין לאיזו תקופה, האם הכוונה לדוא״ל אגור בשרת או שמא דוא״ל עתידי, איזה סוג של דוא״ל וכיוצא בכך.

המחוזי קבע בהקשר זה כי תפיסת המסר על מחשב ספק השירות מהווה תפיסה ב"זמן אמת" במהלך תהליך ההעברה של תכתובת הדוא"ל ולפני שהסתיימה ה"תקשורת בין מחשבים" כהגדרת חוק האזנת סתר ל"שיחה". לפי בית המשפט, הדרך המגשימה את האיזון הראוי בין הזכות לפרטיות לבין האינטרס הציבורי, היא לאפשר לרשויות החקירה גישה להודעות דוא"ל של חשוד באמצעות צווי או היתרי האזנת סתר. מסקנה זו תקפה גם לגבי הודעות הדוא"ל שהיו מצויות בשרתי ספק האינטרנט בעת הוצאת צו החיפוש, וגם לגבי הודעות הדוא"ל העתידיות שנתבקשו בצו החיפוש במקרה זה[180].

לעניין זה אני נוטה להסכים עם הטענה המושמעת בספרות כי אין זה ראוי להטיל על ספק השירות, ללא הוראה מפורשת בחוק, לבצע הוא עצמו את האזנת הסתר לתעבורה עתידית של דוא"ל למנויו גם אם פרקטיקה זו תבוצע באמצעות צו או היתר שיוצא מכוחו של חוק האזנת סתר. האזנת סתר כזו צריכה להיעשות על ידי גופי החקירה והביטחון ובמשאביהם[181].

גם בספרות המשפטית ישנה נטייה לחלק את קו הגבול בין חדירה או חיפוש בחומר מחשב לבין האזנת סתר, באמצעות הפרדה בין שלבי התקשורת השונים בין המחשבים[182]. **אהרוני-גולדנברג** מציינת כי כניסה למחשב ויירוט מידע המאוחסן בו (כולל טיוטת דוא"ל, או קבצי מידע המכילים תרשומת שיחות שקיים אדם בתוכנת מסרים מיידים שהוריד למחשבו) לא תיחשב האזנת סתר. לעומת זאת, קליטת מידע הנמצא בתחנות הביניים בדרכו למחשב היעד, לרבות קליטת מידע הנמצא בשרת ספק האינטרנט או ספק ה-WebMail, תיחשב אקט של האזנת סתר, שכן תפיסה זאת של המסר בשרת ספק השירות יכולה להיראות כחלק בלתי נפרד מהליך תקשורת בין מחשבים. מקרה של חדירה למחשב וקריאת הודעות שכבר הגיעו ליעדן במחשב היעד לא יחשבו האזנת סתר אלא פעולת חיפוש מכוח הפסד"פ. עם זאת ולמרות שבית המשפט המחוזי הגיע למסקנה דומה בעניין פילוסוף, הנחיית פרקליט המדינה לאחר פס"ד זה היא שאין לראות בתפיסת הדוא"ל במצב דברים זה משום האזנה כי אם חיפוש סמוי או המצאה סמויה[183]. הנה כי כן, סעיף 23א(ג) לפסד"פ הקובע כי ביחס לחיפוש המבצעות רשויות הביטחון והאכיפה, קבלת מידע מתקשורת בין מחשבים אגב חיפוש לפי סעיף זה לא תיחשב כהאזנת סתר לפי חוק האזנת סתר, והתוצאה היא שאם במהלך חיפוש שלטוני במחשב מתקבל מסר אלקטרוני כמו דוא"ל, ניתן יהיה להעתיקו כדין, אף שמלכתחילה צו החיפוש התיר חיפוש במחשבים ולא האזנת סתר לתקשורת בין מחשבים[184].

בפרק הבא נרחיב על הביקורת אשר ניתן להעלות כנגד האיזונים שיוצר חוק האזנת סתר וכנגד הפסיקה בנושא ונשאל את השאלה האם איזונים אלו הם ראויים.

3.2.4. __האזנת סתר מחוץ לגבולות ישראל:__

התחולה הטריטוריאלית של חוק האזנת סתר הינה לשטח מדינת ישראל והיא אינה תקפה מחוץ לגבולות המדינה, לרבות בשטחי יהודה, שומרון ועזה, למעט הקלטות של שיחות שנעשו בשטחים אלו על ידי אזרחי ישראל. תוקפן של האזנות סתר שבוצעו מחוץ לישראל, נבחן בהתאם לחוק החל במקום בו בוצעו ההאזנות וככל שאותו דין אינו עומד בסתירה לעקרונות שנקבעו בחוק. בעניין ***מ"י נ' אל מצרי***[185] נקבע, כי האזנות סתר מחוץ לגבולותיה של מדינת ישראל אינן חייבות היתר מראש של בית-המשפט. בעניין ***עסאף נ' מ"י***[186] דן בית-המשפט העליון בחוקיות האזנה לשיחות בין תושב דרום לבנון לתושב ישראל, כאשר ההאזנה

---

180 עניין פילוסוף, לעיל ה"ש 65, עמ' 22-20.

181 ראה דברי בית המשפט המחוזי בעניין נטוויזן, פיסקה 9 להחלטה וכמו כן, נמרוד קוזלובסקי, לעיל ה"ש 147, עמ' 108.

182 ראה למשל נמרוד קוזלובסקי, לעיל ה"ש 147, עמ' 108-95, שרון אהרוני-גולדנברג "חדירה למערכות מחשב – היקפה הרצוי והמצוי של העבירה" **ספר דיויד וינר**, (2009) עמ' 429.

183 כנסת ישראל, ה"ש 146, עמ' 27.

184 שרון אהרוני-גולדנברג, לעיל ה"ש 182, עמ' 482.

185 ע"פ 4211/91 ***מ"י נ' אל מצרי***, פ"ד מז (5) 624. מאוזכר באיינהורן ואח', לעיל ה"ש 50, עמ' 91.

186 ע"פ 568/99 ***עסאף נ' מ"י***, תק-על 2001(2) 242, 246.

בוצעה בו זמנית בישראל ובלבנון. בית המשפט פסק כי חוק האזנת סתר אינו דורש היתר האזנה לשיחותיו של כל אחד מן המשתתפים בשיחה. די בהיתר להאזין לאחד מהם כדי להכשיר את ההאזנה.

3.2.5. מעקבים אלקטרוניים:

אחד הכלים העומדים לרשות גורמי הביטחון הוא המעקב האלקטרוני. על מעקב מסוג זה, המתנהל לרוב באמצעות משדרים אלקטרוניים המוטמנים בחפציו של חשוד או איכון גיאוגרפי באמצעות שימוש בטכנולוגיה של תקשורת סלולארית, חל חוק הגנת הפרטיות. הדיון במעקבים אלו חורג מגדרי עבודה זו, אך למעלה מהדברים, ניתן אולי לשאול האם הוראות סעיף 2(1) לחוק הגנת הפרטיות אוסרות גם התחקות מקוונת אחר פעולותיהם של משתמשי האינטרנט באמצעות שימוש ברוגלות, cookies, וסוסים טרויאניים על ידי רשויות ביטחון וחדירה למחשבו של אדם מרחוק. לעניין זה ראה הדיון שקיימנו בתת הפרק 3.2.2 לעיל בשאלה האם הפעלת אמצעים אלו בישראל תיעשה מכוח הפסד״פ ולפי ההסדרים שנקבעו שם[187].

3.2.6. אחריות ספקי שירות באינטרנט:

סעיף 13 לחוק התקשורת (בזק ושידורים)[188] מחייב בעלי רישיון מכוח החוק (חברות טלפון, סלולר, כבלים וחברות תקשורת אחרות כמו גם ספקי שירותי אינטרנט) לציית להוראה של שר התקשורת להעניק שירותי בזק לכוחות הביטחון בישראל, להתקין מיתקן, לבצע פעולת בזק, או התאמה טכנולוגית למתקן בזק, לרבות מתן גישה למיתקן, ככל שהדבר דרוש לצורך ביצוע תפקידיהם של כוחות הביטחון או להפעלת סמכויותיהם לפי כל דין. ההוראות אינן מוגבלות בנושאים וכך ייתכן שהשר יורה לתת שירותים המנוצלים, הלכה למעשה, לנושאים שאינם קשורים רק להיבטים של סיכול טרור. הוראת השר עשויה לכלול גם הוראות לעניין שמירת סוד, אבטחת מידע והסיווג הביטחוני הנדרש לעובדים הנחשפים למידע המסווג. החוק איננו מגביל את סוג השירותים או הפעולות שיידרשו מחברת התקשורת ומטיל איפול מלא על תוכנה של הוראת השר. בנוסף, קיימים סעיפים מיוחדים ברישיון לביצוע שירותי בזק, הקובעים הוראות ספציפיות ביחס למחויבות בעל הרישיון כלפי מערכת הביטחון[189].

סמכותו של השב״כ לקבל נתוני תקשורת וההליך הסטטוטורי לקבלתם, נקבע במסגרת **סעיף 11 לחוק שירות הביטחון הכללי, תשס״ב-2002**. הוראות סעיף זה מקנות לראש הממשלה סמכות, כמעט בלתי מוגבלת, לקבוע בכללים מהם סוגי המידע שעל בעל רישיון בזק (ובניהם כאמור ספקי שירות באינטרנט) להעביר לידי השב״כ. התנאי היחיד שעל ראש הממשלה לעמוד בו, הוא כי המידע דרוש לשב״כ לצורך מילוי תפקידיו לפי חוק השב״כ. ראש הממשלה אכן קבע כללים לפי סמכותו בחוק השב״כ, אך אלו חסויים מכוח הוראות חוק השב״כ[190]. חוק השב״כ מקנה גם לראש השב״כ סמכויות נרחבות שלפיהן יכול הוא להתיר שימוש, לפי שיקול דעתו באותו מידע המצוי במאגרים אשר ביחס אליהם התיר ראש הממשלה את העברת המידע לשירות. גם כאן, התנאי היחיד לסמכות זו הוא כך שראש השב״כ משוכנע שהמידע דרוש לשירות לצרכי מילוי תפקידו. המידע אליו מתייחס סעיף 11 לחוק השב״כ, הוא למעשה כל מידע המצוי בידי בעל רישיון הבזק, לרבות נתוני תקשורת, ולמעט תוכן השיחה עצמה, שהסמכות לגביה מצויה בחוק האזנת סתר. מידע זה כולל גם נתוני תקשורת, כאשר חוק השב״כ אינו מגדיר את מונח זה[191].

---

187 נזכיר רק כי ס׳ 19 לחוק הגנת הפרטיות מכיר בצורכי רשויות הביטחון לפעול לשמירת אינטרסים חברתיים ציבוריים. אולם, חוק זה אינו כולל הסמכה פוזיטיבית לביצוע מעקב אלקטרוני אחר תנועותיו של אדם, אלא מתיר פגיעה בפרטיות בדרך של מתן פטור לרשויות הביטחון והחקירה, או מי מאנשיהן, אשר פעלו ״באופן סביר במסגרת תפקידם ולשם מילויו״.

188 סעיף 13 לחוק התקשורת (בזק ושידורים), תשמ״ב-1982, ס״ח 218.

189 איינהורן ואח׳, לעיל ה״ש 50, עמ׳ 93.

190 ראה סעיף 19(א)(1) לחוק השב״כ. דן חי, **נתוני תקשורת בישראל**, ויטל – הוצאה לאור, תשע״א-2011, עמ׳ 33-34.

191 ראה הגדרת ״נתוני תקשורת״ בחוק נתוני תקשורת – ״נתוני מיקום, נתוני מנוי או נתוני תעבורה, והכל למעט תוכנו של מסר בזק״. ראה גם הגדרות המונחים ״נתוני מיקום״, ״נתוני מנוי״, ו״נתוני תעבורה״. ראה גם דן חי, לעיל ה״ש 190, עמ׳ 49-67.

כנגד הסמכויות הנרחבות שהוקנו לשב״כ, סעיף 11 גם קובע אמצעי פיקוח על פעולותיו ובאופן זה היתר של ראש השב״כ להשתמש במידע המצוי במאגרים, יפרט, ככל הניתן, פרטים לעניין המידע הנדרש, והמטרה שלשמה הוא נדרש ופרטים לעניין מאגר המידע שבו הוא מצוי; ההיתר יהיה לתקופה שתיקבע בו ושלא תעלה על שישה חודשים, ואולם רשאי ראש השב״כ לשוב ולחדשו. ראש השב״כ מחויב בדיווח על היתרים שנתן לשימוש במידע שנאסף, לראש הממשלה, ליועץ המשפטי לממשלה ולועדת הכנסת לענייני השירות. גם פרטי הדיווח נקבעו בכללים, שראש הממשלה הוסמך להוציאם. כמו כן, סעיף 11 גם מקנה לראש הממשלה את הסמכות לקבוע בכללים הוראות במסגרתן תקבע הדרך שבה על בעל רישיון הבזק לשמור את המידע, תקופת השמירה ודרך העברתם לשב״כ. כאמור, כללים אלו הם חסויים לפי חוקי השב״כ[192]. אנו רואים כי הלכה למעשה הציבור לא מודע למידע אשר מעבירות ספקיות התקשורת לשב״כ, לאופן שמירת המידע על ידי הספקיות, על תקופת שמירה זו ופרטים נוספים. אחד החששות הגדולים לעניין הפרטיות ברשת בהקשר הוא שהפרקטיקה תוביל למצב של מדרון חלקלק וצייתנות יתר מטעם ספקי שירות אינטרנט וזאת במצב שבו הכללים אינם ידועים לציבור.

כמובן שהדיון שערכנו לעיל בתת הפרק 3.2.3 מלמד אותנו רבות על השימוש שעושות רשויות החקירה והביטחון בצווים מכוח הפסד״פ על מנת להיעזר בספקי שירות באינטרנט ולהשיג מידע מודיעיני בתצורה של תכתובות מבוססות אינטרנט של אזרחים בישראל והדיון שם יפה גם לענייננו.

ראוי לציין כי ביוני 2008 נכנס לתוקפו **חוק נתוני תקשורת**, המתיר גם לרשויות חוקרות אחרות (שאינם השב״כ ואמ״ן), לקבל נתוני תקשורת באמצעות פניה לביהמ״ש בבקשה לצו משופט שלום או ישירות מספקי התקשורת במצבים מסוימים. דיון מעמיק בהסדר חקיקתי זה חורג מגדרי עבודה זו[193].

3.2.7. <u>ראיות חסויות:</u>

מטבעם של דברים, המלחמה בטרור הבינלאומי מחייבת הפעלת אמצעי איסוף מודיעיניים מתוחכמים כפי שראינו לעיל, בין אם בחיפוש סמוי או גלוי במחשבו של אדם, ובין אם בהאזנת סתר וניטור תקשורתו הדיגיטאלית. על רקע ההנחה שארגוני המודיעין לא ישמחו לחשוף את יכולות האיסוף שלהם לטובת משפט זה או אחר, השאלה שעולה בהקשר זה היא כיצד ניתן להשתמש בראיות שהושגו באמצעי איסוף אלו ולרוב יהיו ראיות חסויות. בארצות הברית ובריטניה, ניתן להשתמש בראיות חסויות כדי להרשיע טרוריסטים, אך בישראל אסור להשתמש בראיות חסויות ואין להשמיע ראיה כזו שלא במעמד הנאשם. הפיתרון שנקבע בדין הישראלי הוא שימוש במעצר מינהלי[194].

3.2.8. <u>שיתוף במידע מודיעיני:</u>

תיקון מספר 1 לחוק הגנת הפרטיות הוסיף את פרק ד׳ לחוק: *״מסירת מידע או ידיעות מאת גופים ציבוריים״* המגביל את יכולתן של רשויות ציבוריות למסור מידע ולשתף רשויות אחרות במידע שברשותן. תיקון זה פסח על רשויות הביטחון, אשר זכו לפטור גורף מהאיסור על קבלה או מסירת מידע, כל עוד הדבר נעשה לשם מילוי תפקידה של הרשות ולא נאסר בחוק[195]. חוק הגנת הפרטיות לא קבע גורם מפקח סטטוטורי לעניין זה והתוצאה היא שסמכות הפיקוח מסורה לידי בית המשפט. התוצאה היא כוח רב לרשויות הביטחון להחליף ביניהן מידע, ובכלל זאת גם מידע שנאסף באמצעות מעקב מקוון ולאור סמכויות פיקוח חודרניות שניתנו לרשויות הביטחון בישראל.

---

192 דן חי, לעיל ה״ש 190, עמ׳ 36.

193 רשויות אלו הינן: משטרה צבאית חוקרת; המחלקה לחקירת שוטרים במשרד המשפטים; רשות ניירות ערך; רשות ההגבלים העסקיים ורשות המסים בישראל. במאי 2012 התפרסם כי משרד המשפטים מקדם תיקון נוסף לחוק הסדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס״ח-2007, אשר יקנה גישה לנתוני תקשורת לרשויות נוספות וביניהן: רשות העתיקות, רשות הטבע והגנים, משרד החקלאות, המשרד להגנת הסביבה, הממונה על הביטחון במשרד הביטחון ורשם מאגרי המידע. ראה ״רשות הציטוט״, **ידיעות אחרונות** 17.05.2012.

194 עמנואל גרוס, להלן ה״ש 2, עמ׳ 692.

195 ראה סעיף 23ב לחוק הגנת הפרטיות.

4. האם מערכת האיזונים הקיימת בדין הישראלי בין צורכי המודיעין לבין זכויות הפרט מתאימה להתפתחות הטכנולוגית בעידן המידע?

משסקרנו בפרקים הקודמים את תופעת הטרור והמאפיינים הייחודיים של המודיעין המסכל, בחנו את העקרונות המנחים של המשפט המשווה בסוגיית הניטור והמעקב המקוון וכן את הדין הישראלי הקיים בסוגיות אלו, ניתן כעת לערוך השוואה מושכלת שתעמיד זה מול זה את המצב המשפטי המצוי בישראל אל מול המצב המשפטי הרצוי בה, תוך תשומת לב להיבטים של פגיעה בפרטיות. אבקש לטעון כי את ההסדר והאיזון בין פרטיות לבין אינטרסים ציבוריים של סיכול פעילות טרור, בחקיקה ובפרשנות שיפוטית, יש לעצב תוך תשומת לב למהפכה הטכנולוגית של האינטרנט. הפעלת אמצעי מעקב מקוון יכולה להוביל לפגיעה עמוקה במיוחד בפרטיות, גם נוכח האפשרות שתתקיים הפנמה ציבורית לעובדה שתעבורת האינטרנט והתקשורת בין מחשבים נתונים למעקב מתמיד, ולהביא למדרון חלקלק ולתופעות של שיטור עצמי[196] והרתעה מהתקשרויות חוקיות ולגיטימיות.

4.1. חקיקה פרטנית ביחס לאמצעי מעקב מקוון או שימוש בכלים המשפטיים הקיימים?

העובדה שישראל היא מעצמה בתחום הלחימה בטרור, הניסיון הרב שנצבר בנושא והעובדה שרשויות המודיעין בישראל נמצאות בשורה הראשונה בעולם מבחינת ההתקדמות הטכנולוגית, מעלות את השאלה מדוע לא נחקק חוק דומה ל- Patriot Act בארץ? למרות הביקורת הקשה כנגדו, לית מאן דפליג כי ה- Patriot Act היווה דבר חקיקה כולל שביצע שינויים נרחבים במערך הדינים הקיים בארצות הברית והקנה סמכויות ברורות לרשויות הביטחון האמריקניות לעניין הפעלת אמצעי מעקב מקוון לצרכי לחימה בטרור. גם ה- RIPA הבריטי וה- CSIS הקנדי מהווים דברי חקיקה קוהרנטיים ומקיפים המרכזים את הסמכויות הניתנות לרשויות החקירה והביטחון ביחס להפעלת אמצעי חקירה וביניהם אמצעי המעקב המקוונים. מעיון בפרק הקודם ביחס לדין הקיים בישראל ניתן אולי להסיק שהתשובה הפשוטה אך הבעייתית היא שפשוט אין צורך בחקיקה שכזו, שכן בדין הקיים מקבלות רשויות הביטחון סמכויות רחבות ממילא אשר מאפשרות להן למלא את תפקידם הסטטוטורי.

בעוד שבארצות הברית ראינו כי אירועי ה- 11 בספטמבר הובילו לשינוי מהותי במערך האיזונים ביחס לזכויות האדם אל מול הפעלת אמצעי המעקב המודיעיניים ברשת והדברים התבטאו בחקיקה מפורשת וברורה "שחור על גבי לבן", הרי שבישראל ככל הנראה מעדיפים להתמודד עם הקניית סמכויות מעקב מקוון לגורמי ביון דווקא בתחום "האפור" ולא לקבוע דברים בחקיקה מפורשת. כך ראינו שלרשויות הביטחון בישראל מוענקות סמכויות אדירות לחדור לצנעת חיו של אדם במרחב הקיברנטי וזאת על סמך דברי חקיקה פזורים, שלא נמצאים במסגרת נורמטיבית כוללת אחת, בעלי תשתית מושגית שאינה אחידה, המצביעים בחלק מהמקרים על מידה רבה של חוסר קוהרנטיות. ראינו כי חלק מדברי חקיקה אלו הם כלליים ולא פרטניים ביחס לסוגי הטכנולוגיה שהתקדמה מאז שנחקקו וביחס לאמצעי המעקב שהשתכללו ולסביבה הדיגיטאלית לאחר מהפכת האינטרנט. בחלק מהמקרים הסמכות להפעלת אמצעי איסוף מקוונים על ידי רשויות ביטחון אינה מוסדרת בדבר חקיקה אלא נגזרת מפרשנות תכליתית של הסדרים דומים אחרים או מהרשאות חקיקתיות בעלות אופי כללי. במובן זה, מערך הדינים הקיים הוא מערך הדינים של אתמול במציאות טכנולוגית שמשתנה תדיר ובמצב זה גם פרשנות תכליתית של הסדרים לביצוע מעקב מקוון עלולים להביא לפגיעה בזכויות הפרט. באין הסדר פרטני בחקיקה, ובהתבססות גורמי הביון החשאיים על פרשנות משפטית של דברי חקיקה קיימים אשר לא מותאמים להתקדמות הטכנולוגית,

[196] להרחבה ראה, מיכאל בירנהק **חוק נתוני תקשורת והפגיעה בזכות לפרטיות**, הסניגור 130 (2008) 4, עמ' 6.

החשש גובר שמא ינצלו גורמי הביון את הלאקונה שנוצרה בהסמכתם להפעיל אמצעי מעקב חודרניים ברשת והאיזון בין אינטרס ביטחון הציבור לבין הפגיעה בפרטיות יופר.

טענות אלו רואות טעם ב"מודל החקיקתי של המאבק המשפטי בטרור" לפי החלוקה שהציעה בנושא זה **דפנה ברק-ארז**. לפי גישה זו, עקרונות שלטון החוק וחוקיות המינהל מחייבים שכל פעולה מנהלית תהיה מבוססת על הסמכה חקיקתית ספציפית, ברורה ומפורשת, במיוחד אם הפעולה פוגעת בזכויות יסוד[197]. כיום, עיגונה של ההסמכה לפעילות שלטונית הפוגעת בזכויות האדם, מתחייבת אף מנוסחו של חוק יסוד: כבוד האדם הקובע כי פגיעה בזכויות המוגנות מכוחו צריכה להתבסס על הסמכה מפורשת.

מפתיע כיצד מדינת ישראל, שנמצאת בחזית הלוחמה בטרור, לא מצאה לנכון להסדיר את הפעלת אמצעי המעקב והלחימה בטרור במרחב הקיברנטי בדבר חקיקה מקיף ושלם אחד אשר ינסה לתת מענה לכלל ההיבטים והשימושים שעושים ארגוני הטרור ברשת והוצגו בפרק 1 לעיל. "מטרייה" חוקית כאמור, יכולה לספק יתרונות ברורים כגון תשתית מושגים אחידה, וקוהרנטיות בין הוראות החוק, הרואה את התמונה המשולבת כולה. זאת בניגוד למצב כיום בו לעיתים ההסדר הכללי המתיר את פעילות המעקב של ארגוני הביטחון מתקשה להתמודד עם המאפיינים המיוחדים של המרחב המקוון, או לחילופין כשאנו עדים לנושאים בהם לא הושגה הכרעה ברורה ביחס לדין החל או כשההגנה והאיזונים בין האינטרסים של ביטחון המדינה וזכויות הפרט לא אוזנו כראוי.

מנגד ניתן לטעון כי הסדר קודיפיקטיבי שכזה יכול ליצר חשש לחוסר התאמה או לכפילות בין ההסדר המיוחד להפעלת אמצעי מעקב מקוונים על ידי רשויות ביטחון לבין ההסדרים הכלליים שנקבעו וכי הסמכויות הכלליות של הרשות הביטחונית כגוף של הרשות המבצעת, נקבעו בחקיקה מסמיכה כללית. יתרה מכך, תחימת גבולות הסמכות של המודיעין המסכל בישראל בחקיקה ספציפית יכולה אף לפגוע בביטחון, שכן הלחימה בטרור, במיוחד בזירה המתפתחת טכנולוגית, מחייבת גמישות, דינאמיות והתאמת האמצעים לצרכים. במובן זה, חוק מפורט יכול לפגוע בגמישות המבצעית הנדרשת ואף להוביל לחשיפה מבצעית מיותרת. טענות מסוג זה מתאימות למצדדים ב"מודל הביצועי" או ה"ביצועי החלש" שהציעה ברק-ארז, אשר מתיר פעילות לסיכול טרור של הרשות המבצעת לאור הסמכות חקיקתיות רחבות וכלליות ללא הדרכה נורמטיבית באשר לאופן הפעלתן[198] והשארת ההסדר המשפטי שיחול על הפעלת אמצעי מעקב מקוונים להסדרה מנהלית-ביצועית במידה רבה, על מנת לקדם את האינטרסים של ביטחון הציבור.

כמו כן, ניתן לטעון כי ההסדרים המשפטיים שנוסחו בחקיקה כמו חוק האזנת סתר, חוק המחשבים וחוק נתוני תקשורת משקפים עקרונות ואיזונים קיימים אשר לא מגבילים את עצמם לטכנולוגיה מסוימת או להתפתחותה[199]. ישנה גם טענה כי הסדר סטטוטורי לכל פעולה ממגוון פעולותיו של שירות ביטחון הוא אמנם ראוי ונכון מבחינה דמוקרטית, אך הופך את ארגון המודיעין המסכל למשטרה ומאיין למעשה את היתרון שיש לארגון שכזה על פני גורמי האכיפה הרגילים.

לאור זאת, בהחלט יש מקום לשאלה האם צריך לקבוע הסדרים כוללים ביחס לאמצעי האיסוף המקוונים כשלמעשה מדובר בחקיקה המסדירה תחום טכנולוגי שמתאפיין בקצב התפתחות מהיר במיוחד, ועל כן יש סבירות שהסדרים שנקבעו יאבדו את הרלוונטיות שלהם בזמן קצר. דומני ששאלה זו ראוי שתיבחן לעומק, אך הדיון בכך חורג מהמצע הנדון כאן.

כאמור, התקדמותו של העידן הדיגיטאלי והתפתחות הרשת, מעלות שאלות קשות שהדין הקיים מתקשה כיום להתמודד עימן או, לכל הפחות, יתקשה להתמודד עימן ככל שהטכנולוגיה תתקדם. הנה מספר

197 דפנה ברק-ארז, **המאבק המשפטי בטרור: ההיבט המוסדי**, עיוני משפט לב, תש"ע 2010, 46 עמ' 51.

198 דפנה ברק-ארז, לעיל ה"ש 197, עמ' 55.

199 להרחבה על הגישות השונות ביחס לנושא: גישה מונחית טכנולוגיה וגישה נייטרלית לטכנולוגיה, ראה גם ויקטור ח. בוגנים "חוק המחשבים והתמודדות המשפט עם האתגר הטכנולוגי" **שערי משפט** ד(2) התשס"ו 2006, 283.

דוגמאות אשר עולות מעיון בפרקים הקודמים:

<u>מהו דינו של חיפוש המבצעת רשות ביטחון בישראל באמצעות הפעלה סמויה של רוגלה או סוס טרויאני?</u> ראינו בתת פרק 3.23.2.2 כי פרשנות מרחיבה של הוראות ההסדר החוקי לחיפוש בחומר מחשב בפסד״פ יכולות להוות גם הסמכה לחיפוש מרחוק באמצעות רוגלות וסוסים טרויאנים. דומני שגם כאן מדובר בדוגמא טובה לשיקולים שהעלנו בדיון לעיל ביחס לחקיקה פרטנית או קונקרטית לגבי סמכויות המודיעין המסכל בחקיקה ספציפית, ודברים שנאמרו שם, יפים גם כאן. בקצרה אוסיף כי לטעמי, גם אם נקבע כי אין להסדיר נושא זה בחקיקה ספציפית, יש לקבוע כללים ונהלים ברורים ביחס לחדירה לחומר מחשב בדרך זו על ידי רשויות ביטחוניות בישראל. נהלים אלו יפרטו באילו מצבים תתאפשר חדירה שכזו, מהם השיקולים שנותן ההיתר ישקול, מהו פרק הזמן בו תתבצע החדירה, מהם הדרכים לוודא שהמידע החשוד יופרד ממידע אישי שאינו קשור ומהם נהלים לפיקוח ודיווח על הפעלת אמצעים אלו על ידי רשויות הביטחון.

<u>האם פעולת חיפוש במחשבי חשודים או ספקי אינטרנט, החושפת את רשויות החקירה לתרשומות שיחה, תחשב חיפוש לפי הוראות הפסד״פ או האזנת סתר</u>. בפרק השלישי ראינו כי ההסדר המשפטי הקיים בישראל ביחס לאמצעי המעקב המקוון מבחין מבחינת החומרה בין האזנת סתר לבין צו חיפוש, ולכן גם מתייחס להאזנות סתר ביתר קפדנות מבחינת הדרישות המשפטיות. אך יחד עם זאת ראינו כי קו הגבול בין תוצרי החיפוש במערכות מחשב לעומת האזנת סתר לתקשורת בין מחשבים אינו ברור וכי החקיקה אינה מבחינה בין חיפוש במחשב בודד (Stand Alon), מחשב המצוי ברשת מחשבים או ברשת של ספק אינטרנט. זאת בניגוד לחקיקה האמריקאית שאף היא מתירה השגת מידע מקוון באמצעות צווי חיפוש בשרתי ספקי אינטרנט, אך עושה זאת בחקיקה ספציפית. ראינו גם שהאזנת סתר מחייבת צו של נשיא בית משפט מחוזי או סגנו, או לחלופין היתר מראש הממשלה או שר הביטחון. צו חיפוש, לעומת זאת, הוא בסמכותו של בית משפט שלום. ההשלכות של חיפוש על יעד המודיעין לעומת האזנת סתר שונות מאוד בכל הקשור לפגיעה בפרטיות. בחיפוש במחשבו של אדם, מדובר בפגיעה חד-פעמית, שלרוב הנחקר מודע לה כשמדובר בחיפוש גלוי, והפגיעה ממוקדת בו ובמחשב שבחזקתו. האזנת סתר, מנגד, היא פגיעה מתמשכת, ללא ידיעת הנחקר, אשר עלולה לפגוע בפרטיות החשוד (כאשר לרוב במסגרת מכלול שיחות החשוד להן מאזינות רשויות החקירה, נכללת גם תקשורת אישית של החשוד אשר אינה רלוונטית לחקירה) וכן לפגיעה בצדדים שלישיים (משתמשים אחרים בשרת או במחשב, וכן צדדים המשוחחים עם הנחקר). על רקע דברים אלו, נראה כי חיפוש ומעקב מקוון סמוי באמצעות ספקי האינטרנט דומה יותר להאזנת סתר.

תהליך חקיקתו הארוך של חוק המחשבים, מאמצע שנות ה-80 ועד שנחקק לבסוף בשנת 1995, הביא לכך שההתפתחות הטכנולוגית הגדולה של רשת האינטרנט באמצע שנות ה-90 של המאה ה-20 לא באה לידי ביטוי בחוק זה. כך יוצא שההסדרה הנורמטיבית של היבטי חיפוש ותפיסת חומר במערכות מחשב לא מתייחסת באופן ברור לעובדה שבמחשבו של אדם נמצאות גם תרשומות המכילות את סוד שיחתו ויכולות לעלות עד כדי הפרקטיקה של האזנת סתר. עם זאת, ראינו כי למרות פסיקתו של ביהמ״ש המחוזי בעניין פילוסוף, הוראות הפסד״פ עדין מבהירות שבחיפוש שלטוני במחשב, המביא לקליטת סוד שיחו של אדם, אין מדובר בהאזנת סתר, והנחיות פרקליטות המדינה לא השתנו. גם כאן נראה לטעמי שישנו יתרון לחקיקה ספציפית בתחום זה, שתבצע הפרדה באיזונים הנדרשים לפעולות שונות של איסוף מידע ברשת. כזכור, בארצות הברית הדברים מוסדרים בחקיקה ברורה, אך מבחינת התוצאה הסופית אין הבדלים של ממש שכן חקיקה זו גם היא מאפשרת תפישת מידע תוכני כגון דוא״ל באמצעות צווי חיפוש.

<u>נתוני תקשורת – האומנם מידע מוגבל לעומת האזנת סתר?</u> בפרק 3.2 ראינו כי הדין הישראלי מתייחס בחומרה רבה יותר לפגיעה בפרטיות כאשר מדובר בהאזנה לתוכן ההתקשרות, ואילו לגבי עיון של רשויות

המדינה בנתוני תקשורת הדין מניח הסדרים סטטוטוריים קשיחים פחות[200]. אני מסכים עם הטענה המושמעת בספרות לפיה גישה זו, שיוצרת מדרג של תוכן השיחה ונתוני התקשורת שלה, אינה ראויה ואינה מותאמת לעידן הדיגיטאלי[201]. גם קבלת נתוני התקשורת של אדם, המאפשרת לרשויות לדעת עם מי שוחח, באיזה אמצעי (דוא״ל, צ׳אט, פורום, מסרים מידיים), סוג הקובץ שצורף לשיחה, שורת הנושא של ההודעה, תאריך ועיתוי ההתקשרות, באמצעות אלו ספקי תקשורת בוצעה ההתקשרות, באלו אתרים גלש (ולאור זאת לבסס ראיות ביחס למידע המיוחס לאדם זה) – כל אלו מיצרים תמונה מאוד מדויקת על חיו של אדם ודפוסי התנהגותו וגורמים לחשיפה חסרת תקדים[202]. כאן יש להזכיר כי איתור טכנולוגיית האינטרנט המבוססת על תמסורת של חבילות, מחייבת שלצד יירוט נתוני התקשורת ייורט תוכן ההתקשרות. בידוד נתוני התקשורת מן המסר המצורף, תלוי אפוא בהתחייבות הרשות להפריד ביניהן לבין תוכן ההתקשרות[203]. בהיעדר מידע גלוי וכללים פומביים ביחס להפעלת הרשויות אמצעים אלו בישראל, יש מקום לחשש לפגיעה בזכויות הפרט.

<u>האומנם שיחה ברשת היא ״ברשות הרבים״?</u> **קוזלובסקי** ומלומדים אחרים מצביעים על כך שישנם מקרים בהם הפרט נוקט צעדים ממשיים להגנה על פרטיותו ועל סוד שיחו גם כאשר הוא משוחח בשיחת רשת או באמצעות רשת האינטרנט, ועל מערכת המשפט לכבד זאת[204]. לפי טענה זו, על אף ששיחות בפורומים ואתרי אינטרנט לרוב נגישות לכלל משתמשי הרשת, בנסיבות בהן הפרט נוקט אמצעים לשמירה על פרטיותו קיימת צפייה סבירה לפרטיות ועל כן אין להתיר האזנה לשיחות אלו אלא אם ניתן לכך היתר על ידי בית משפט שיפעיל לצורך כך שיקול דעת שיפוטי ולא באמצעות היתר לרשות המבצעת. דומני כי הדיון שקיימנו בפרק 1.2.1 לעיל אודות השימוש שעושים ארגוני טרור בפורומים ובחדרי צ׳אט ״סגורים״ לא עולה בקנה אחד עם גישה זו, ולעניות דעתי, גם אם לפרטים ישנה ציפייה סבירה לשמור על סוד שיחתם, הרי שהאינטרס של ביטחון המדינה ראוי שיגבר כאן. אך כיצד ניתן לקבוע את הגבול? האם כל שיחה ברשת חברתית תיחשב שיחה הנעשית ״ברשות הרבים״? הפיתרון לדעתי, מצוי בנקודת הביניים, ובהחלת כללים ברורים ומידתיים על רשויות המודיעין המסכל.

<u>שימוש בספקי אינטרנט וחברות תקשורת כ״זרוע ארוכה״</u>: יש מי שיטען כי החקיקה האמריקאית, שמאפשרת באופן ברור קבלת מידע מקיף ביותר מספקי אינטרנט כמעט ללא ביקורת שיפוטית, נותנת כלים לתגמול או הפעלת סנקציות כלפי גורמים אלו, מכפיפה פיתוחים טכנולוגיים לאפשרויות ההאזנה הקיימות ומאפשרת שיתוף מידע בין חברות טכנולוגיה פרטיות וגורמים ממשלתיים, היא חקיקה בעייתית אשר לא שומרת על איזון נכון מול זכויות האדם. נראה כי גם החקיקה הקנדית שראינו מבקשת לעשות שימוש בחברות תקשורת כ״זרוע ארוכה״ כשהצעת חוק שהוגשה השנה תחייב חברות אלו להשיג יכולת טכנית לפקח ולנטר על כל פעילות מקוונת דרכן, על מנת שעם מתן צו תוכל להעביר את המידע לרשויות הביטחון. הדין הישראלי אינו כה מפורש ביחס לשיתוף פעולה שכזה ומלבד לקביעות הכללית של חוק השב״כ, חוק נתוני תקשורת וחוק התקשורת (בזק ושידורים), הכללים ביחס למידע שיקבל לידיו השב״כ נשארו חסויים או כלליים ורחבים במידה שלא מאפשרת ביקורת ופיקוח אפקטיביים עליהם, כאשר הביקורת השיפוטית ממילא כמעט ולא קיימת. בשאלה איזו גישה ראויה יותר – גישה המבקשת להסמיך מפורשות בחקיקה פעילות זו כאשר המשקל הניתן לזכויות הפרט הוא מועט, או גישה אשר לא מגדירה את

---

200 ראה הדיון בפרק 3.1 ו- 3.2 לעיל ביחס לפרוצדורה המורכבת לקבלת צו להאזנת סתר לעומת יכולת גורמי חקירה לעיין בנתוני תקשורת בארצות הברית (לאחר חקיקת ה- USA Patriot Act) ובישראל.

201 להרחבה ראה, מיכאל בירנהק, **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה**, נבו הוצאה לאור בע״מ, תשע״א, עמ׳ 76.

202 מיכאל בירנהק לעיל ה״ש 196, עמ׳ 4, עמ׳ 4-6.

203 אלעד אורג, לעיל ה״ש 103, עמ׳ 124.

204 נמרוד קוזלובסקי ״**הגנה על הפרטיות במרחבי האינטרנט**״ אתר פסק דין, www.psakdin.co.il/fileprint.asp?FileName=/Ip/Public/art_bddh.htm; נמרוד קוזלובסקי ״**משטרת האינטרנט**״ אתר פסק דין, www.psakdin.co.il/fileprint.asp?filename=/ip/public/art_bbxx.htm.

הדברים במפורש ומשאירה את הנושא להסדרה מנהלית על ידי הגוף המבצע – דעתי היא שגם כאן הפיתרון הראוי נמצא אי שם באמצע הדרך אך ללא ספק קיימת חשיבות בעיני לשאלת ההסדרה הסטטוטורית המפורשת.

4.2. ***"ביטחון המדינה" - סיכול טרור או מניעת פשיעה וקידום אינטרסים ממלכתיים חיוניים?***

בפרק 3.2 ראינו שכשהחקיקה הישראלית מסמיכה את רשויות הביטחון להפעיל אמצעי מעקב מקוונים בחקיקה, הסמכות ניתנת במצבים בהם מדובר במידע החיוני לשם תפקידי הרשות, או כשהדבר נעשה למטרת "ביטחון המדינה", כאשר מונח זה אינו מוגדר דיו וכשתפקידם של רשויות המודיעין המסכל מוגדר גם הוא בצורה רחבה ביותר. היעדרן של הגדרות ברורות למונחים אלו אינו מקרי ונראה כי כוונת המינוח הרחב היא למנוע עכבות משפטיות לשיקול הדעת המבצעי של אותם גופים[205].

לטעמי, השארת המונח "ביטחון המדינה" כמונח עמום המאפשר פרשנות רחבה, כבסיס להפעלת שיקול דעת מבצעי, מינהלי ושיפוטי לאמצעי מעקב חודרניים ברשת, מעלה את החשש שאמצעים אלו לא יופנו רק לטיפול באיומי טרור אלא גם באינטרסים אחרים שלא מצדיקים את רמת האיזונים שנקבעה להפעלת אמצעים אלו בדין. העדר כללים מנחים לשיקול דעת בנושאים הכלולים תחת הכותרת של "ביטחון המדינה" פותח פתח לשימוש לרעה במונח זה.

באופן זה עלינו לתת את הדעת להבדלים בין המטרות והמאפיינים של סיכול טרור לבין מניעת פשיעה או איתור עבריינים, אשר שניהם אינטרסים שיכולים להוות הצדקה להפרת זכויות האדם. מלחמה בפשיעה נעשית ברובה לאחר ביצוע הפשע ומבוססת על ההנחה כי החברה מסוגלת לספוג פשעים אלו וכן על ההנחה שענישת עבריינים תרתיע את הציבור. בשונה מכך, הלחימה בטרור מבקשת לסכל את פעולות הטרור לפני שאלו קורות ולכן הצורך בפעילות מיידית ורחבה ככל שניתן. לאור זאת נראה כי אין לקבוע דין אחד לסיכול טרור ולמאבק בפשיעה – יש מקום לצמצם את הסמכויות להפעלת אמצעי מעקב מקוון ללא היתר שיפוטי רק לגבי המלחמה בטרור ולא לגבי הפרות חוק אחרות[206]. בפרק השלישי ראינו שבדין האמריקני הפרדה מסוג זה מטושטשת. למשל, ה-Patriot Act מתיר ביצוע פעולות מעקב ואיסוף אלקטרוני גם במצבים שבינם ובין סיכול טרור או איסוף מודיעין זר אין קשר. באופן זה יכול להיווצר מדרון חלקלק שבו הסמכויות החודרניות שמוענקות לרשויות הביטחון יפגעו בזכויותיהם החוקתיות של חשודים אף שמעשיהם לא עולים בגדר פעילות טרור[207].

ראינו גם שבישראל, ההגדרה של ביטחון המדינה מתירה מרחב נכבד לשב"כ ולאמ"ן לאסוף מודיעין שלא תמיד עונה להגדרה של "מאבק בטרור", אלא יכול להגיע גם למצבים של שמירה על אינטרסים חיוניים למדינת ישראל. הגם שאינטרסים אלו הינם ראויים וזקוקים להגנה, הרי שלדעתי אין להחיל עליהם את מערך האיזונים החוקי שהתיר החוק בישראל על מנת לסכל פעילות טרור. הדברים מתחדדים שבעתיים שעה שאנו עדים לכך שרשויות נוספות בישראל, כגון רשות שמורות הטבע והגנים, רשות העתיקות ורשויות המיסים השונות, דורשות גם הן לקבל לידן תוצרי מודיעין הנובעים מסמכויות האיסוף המקוון המתקדמות שיש ברשות השב"כ ורשויות הביטחון והאכיפה האחרות בישראל.

4.3. ***ביקורת ודיווח על הפעלת סמכויות מעקב מקוון:***

הדיון לעיל בתת הפרק 4.1 יפה גם כאן. בעוד שחקיקה היא מטבע הדברים חלק מהספרה הציבורית, הרי שיטען הטוען שכשאין חוק, קשה להפר את הוראותיו, וקשה עוד יותר לפקח על השימוש בסמכויות

205 מנחם הופנונג, **ישראל – ביטחון המדינה מול שלטון החוק**, נבו (1991), עמ' 23.

206 אלעד אורג, לעיל ה"ש 103, עמ' 125-126.

207 USA Patriot Act § 802: "Definition of domestic terrorism". כאמור, ה- Patriot Act יצר הגדרה חדשה ל "Domestic Terrorism" אשר מטילה ספק בקיומה של דיכוטומיה כל שהיא בין עבירה פלילית רגילה לעבירת טרור. עמנואל גרוס, לעיל ה"ש 2, עמ' 637.

המינהל. חשש זה גובר שבעתיים כשאנו עוסקים בלב ליבו של "התחום האפור", בפעילות המודיעינית של ארגון מודיעין מסכל, אשר זכות הציבור לדעת אודותיו מוגבלות מאוד. הפגיעה הקשה ביותר בזכויות האדם יכולה להיות זו שאיננו מודעים אליה. לפחות לא עד ועדת החקירה הבאה כתוצאה מאי סדרים והפרות שיתגלו חלילה. הדיון בפרקים הקודמים מצביע לטעמי על כך שאין ספק שישנו צורך להקנות לרשויות הביטחון סמכויות להפעיל אמצעי מעקב מקוונים על מנת לסייע להם בלחימה העיקשת בטרור. אולם יש גם מקום לטענה שבד בבד עם הקניית סמכויות אלו, נדרשת שקיפות רבה יותר וביקורת אפקטיבית יותר על השימוש בהן.

כך למשל, חוק האזנת סתר אינו מחייב את רשויות הביטחון עצמן לדווח על מהלך ההאזנה או על תוצאותיה. הדיווחים נעשים על ידי ראש הממשלה או שר הביטחון, שמדווחים אחת לשלושה חודשים ליועץ המשפטי לממשלה, רטרואקטיבית, על ההיתרים שניתנו. פעם בשנה נדרש גם דיווח לוועדה מיוחדת של הכנסת הדנה בעניין בדלתיים סגורות, אך על פי החוק דיווח זה הוא על מספר ההיתרים שניתן בלבד [208]. לאור זאת, לא קיים מידע פומבי אודות בקשות להיתרים להאזנת סתר של השב"כ או אמ"ן, ועל כן קשה לבחון את הליך מתן היתרים אלו[209]. לדעתי יש מקום לטענה כי אינטרס הציבור מחייב שבמקביל למתן היתרים לרשויות הביטחון על מנת לסכל טרור ופעילות חבלנית עוינת, יקודם גם שלטון החוק כאשר יפורסם יותר מידע אודות ההיתרים שניתנו ושנדחו. ביקורת ציבורית על האזנת סתר ומעקב מקוון של רשויות ביטחון יכול לקדם את האכיפה על המידתיות והסבירות בהפעלת אמצעים חודרניים אלו ולצמצם את הפגיעה בפרטיות שלא לצורך. על מנת שלא לפגוע בחקירות, בפעילויות לסיכול טרור או לחשוף כלים ויכולות מודיעיניות, פיתרון אפשרי יכול להיות העברת יותר מידע לוועדה המיוחדת של הכנסת לפי חוק האזנת סתר ובמסגרת זאת לחשוף בפניה מידע כמו מהות ההיתרים, נתונים על ההאזנה ותוצאותיה (בחתך של מקרים שהאזנת סתר שהותרה הובילה למעצר, סיכול טרור, כתב אישום או הרשעה ובכמה פעמים היה ניתן להגיע לתוצאות של סיכול הטרור גם בלי האזנת סתר, מהם המקרים בהם ניתן אישור להאזנה והדברים התבררו ככאלו שלא מהווים איום ממשי ועוד).

לטעמי, הדיווח והביקורת המתקיימת על הפעלת אמצעי האזנת סתר, ובכלל זאת האזנת סתר לתעבורה מקוונת על ידי רשויות הביטחון בישראל, לא מאזנת כראוי בין הפגיעה בזכויות הפרט לבין האינטרס הביטחוני והאיזונים שנקבעו בנושא בחקיקה הבריטית יכולים להוות בסיס לשינוי של הדין הקיים בישראל בנושא זה. פיקוח ראוי יותר על פעילות זו יכול להביא עימו גם שיפור וייעול של תהליכי הסיכול.

כאמור, אין ברשותנו נתונים או מידע על ההיתרים, הנהלים וההנחיות של השב"כ ביחס להפעלת אמצעי מעקב מקוונים, שכן אלו חסויים מתוקף חוק השב"כ. אך ככל שניתן להסיק מעיון במידע הפומבי ביחס להאזנת סתר שמבצעת המשטרה[210], יש בהחלט מקום לדאגה, שכן לא תמיד מתנהלת שם פעילות זו תוך הקפדה על האיזונים שנקבעו בחוק. לא תמיד ישנה הקפדה יתרה על הסבירות והמידתיות בהן נעשה השימוש בסמכויות חודרניות אלה, ולא אחת מתרחשת פגיעה חמורה בפרטיות על אף כל אמצעי הפיקוח השיפוטיים והמנהליים שנקבעו בחוק. יש בכך כדי ללמדנו כי ייתכן בהחלט שגורמי מודיעין מסכל גם הם אינם חפים משגיאות וגם בקרבם יכולות להתרחש תקלות שהמשמעות שלהן היא לא אחת פגיעה בזכותו החוקתית המוגנת של אדם לפרטיות. ערך "ריסון הכוח" שטבע השב"כ ביחס להפעלת פעילותו הוא נכון וראוי, אך במיוחד בהקשרו של המעקב המקוון, יש לוודא כי אנו מאפשרים לדמוקרטיה הישראלית אמצעי ביקורת ופיקוח על מנת לממשו.

---

208 ראה סעיף 4(ה) לחוק האזנת סתר.

209 ראה בנושא זה את בג"ץ 414/89 **בן נ' שר המשפטים**, פ"ד מג (4) 327 והביקורת עליו במאמרו של זאב סגל "על הזכות המוגנת בבג"ץ, הזכות לדעת והאזנת סתר" **משפטים** כ"א, תשנ"ב, 559.

210 כנסת ישראל, לעיל ה"ש 146, שם, משרד המשפטים, **דין וחשבון של צוות הבדיקה בנושא האזנת סתר** – בעקבות בחינתו של היועץ המשפטי לממשלה, מר אליקים רובינשטיין, את תיק המחלקה לחקירות שוטרים בפרשת האזנת הסתר ביחידה הארצית לחקירות הונאה שנפתח נגד ניצב משה מזרחי, אפריל 2005, **הדין והחשבון השנתי של מבקר המדינה** מס' 54ב, יוני 2003.

4.4. שיקול דעת שיפוטי, מיניסטריאלי או מינהלי באישור הפעלת אמצעי מעקב מקוון?

ראינו שחוק האזנת סתר, המסדיר בישראל את הפעלת אמצעי המעקב המרכזי ברשת האינטרנט, מקנה סמכות לגורם מיניסטריאלי להתיר האזנת סתר. ניתן בהחלט למצוא טיעונים טובים מדוע יש להטיל את הסמכות להיתרים על האזנת סתר למען ביטחון המדינה על ראש הממשלה ושר בכיר כשר הביטחון, לאור האחריות הכבדה המתלווה לסמכות זו[211], אך עם זאת עלינו תמיד לזכור כי עקרון הפיקוח המדורג, לפיו ככל שעולה רמת הפולשניות שבמעקב, כך יש להבטיח ביקורת ופיקוח קפדניים יותר, מחייב שלא להפקיד סמכות כה פוגענית כגון היתר להאזנת סתר בידי שר ללא ביקורת שיפוטית. ראש הממשלה או שר הביטחון אינם מהווים גורם עצמאי המסוגל לפקח מנקודת מבט ניטראלית על הצורך בהאזנת הסתר, וללא היכרות מעמיקה עם העולם המודיעיני ותחום השירותים החשאיים, אין בידם יכולת לקיים בדיקה מעמיקה על נחיצות ההיתר. מחויבותם המוסדית הינה לשיקולי בטחון, בעוד ששופט הוא גורם אשר מעצם תפקידו ומהותו רואה את התמונה במלואה, ומסוגל לשקול את האינטרסים הנוגדים ולהגיע לידי החלטה מאוזנת. החשש בהקשר זה הוא ברור, שמא היתר מאת ראש הממשלה או שר הביטחון יהפוך לחותמת גומי חסרת משמעות, שהרי אין בידו לפקח באופן מעשי ומקצועי על הנושא[212]. ראינו שגם בבריטניה ובארצות הברית, לשר ממונה או לרשות מנהלית יש סמכות להתיר האזנת סתר ללא צו שיפוטי, וכי ההסדר של בתי משפט ייעודיים לנושא מכוח ה-FISA האמריקני נוטים לאשר לרוב הוצאת צווים עם שיקול דעת שיפוטי מינימאלי. לאור זאת נראה שהפיתרון הראוי לדין הישראלי הוא הליך היתר מסודר בו נשקלים כל השיקולים הרלוונטיים על ידי הגורם המבצע, השר המקבל את ההחלטה נועץ בגורם מקצועי בלתי תלוי, וכל זאת תוך קיום מעקב שוטף אחר דרך יישום ההיתר ונחיצותו בדיעבד על ידי מערך ביקורת.

ביחס להפעלת שיקול הדעת המיניסטריאלי, ניתן גם לשאול האם בישראל מקבלים שר הביטחון וראש הממשלה מידע מספק ורלוונטי מרשויות הביטחון, בבואם להתיר הפעלת אמצעי מעקב מקוון. עיון בתקנות האזנת סתר מלמד אותנו כי במקרה של בקשה להיתר האזנת סתר לשיחה חסויה לפי פקודת הראיות, נדרש השב״כ בבית המשפט להציג את נימוקיו לכך שההאזנה דרושה מטעמי ביטחון המדינה. בבקשה שכזו יתאר השב״כ את התשתית העובדתית עליה מבוססת הבקשה להאזנת סתר, ואת הנימוקים שהובילו להחלטה על הגשת בקשה להאזנת סתר. לאחר שנשקל הצורך בביצוע ההאזנה מול הפגיעה הצפויה בפרטיות יעד ההאזנה וסביבתו עקב ביצוע ההאזנה יפורטו גם חומרת הסכנה לביטחון המדינה; הסיכוי לאיסוף מידע רלוונטי באמצעות ההאזנה; עוצמת החשד והתשתית הראייתית אשר יצדיקו האזנת סתר; מידת הקשר בין המואזן לבין העבירה; מידת הפגיעה הצפויה במי שאינו חשוד ומשך ההאזנה הדרוש[213]. לעניות דעתי, דברים שנקבעו בחריג זה לסמכותו של השב״כ ראויים להיקבע ככלל, ובקשה להיתר האזנת סתר של רשות ביטחונית חייבת לכלול פרטים אלו גם כשהבקשה מופנית לשר ולא רק לבית המשפט. כך יישמרו גם האינטרסים של ביטחון המדינה (שכן המידע נשאר חסוי ברשותו של השר) וגם כללי מינהל תקין ראויים יותר, כשההנחה היא שהצורך בהעלאת נימוקים מבוססים על הכתב תסייע לשיפור פעילות הרשות הביטחונית ותמנע האזנות סתר במקום בו ניתן להסתדר גם בלעדיהן.

---

211 בועז גנור ״׳הדילמה הדמוקרטית׳ בלוחמה בטרור״ **משפט וצבא** 17 (התשס״ד), עמ׳ 170.

212 להרחבה ראה האגודה לזכויות האזרח, לעיל ה״ש 137, שם.

213 ראה טופס 2 (תקנה 2(ב)(1) ל**תקנות האזנת סתר (בקשה להיתר האזנה)**, תשס״ז-2007, ק״ת תשס״ז מס׳ 6586.

סיכום, מסקנות ומבט לעתיד

ההתפתחות המהירה של אמצעי הניטור הטכנולוגיים ומרכזיותה של הפעילות המקוונת במוקד הליבה של ארגוני הטרור הופכים את תופעת המעקב והחיפוש האלקטרוניים לאחת הסוגיות המרכזיות בנושא הלחימה בטרור, ומשפיעים מאוד על מערך האיזונים שנקבע בעבר ביחס להפרת זכויות הפרט בהפעלת אמצעי איסוף ומעקב "קונבנציונאליים". בעבודה זו בחנו את היחס המצוי והראוי בין הצורך להפעיל אמצעי מעקב על פעילות מקוונת של הפרט במדינה דמוקרטית לבין האינטרסים המוגנים של זכויות האדם וסקרנו את תופעת המעקב והחיפוש המקוונים, הן ביחס לפן הטכנולוגי הכרוך בה והן ביחס לפן המשפטי, תוך איתור הבעיות העולות מתופעה זו ביחס לפגיעה בזכויות הפרט ותוך ניסיון ללמוד מהפתרונות השונים שהוצעו להסדרת הנושא במשפט המשווה. ראינו שישנו אינטרס חברתי ברור במציאת איזון ראוי ויעיל בין זכויות הפרט לבין היכולת של ארגוני הביטחון לנטר ולעקוב באופן מקוון אחר פעילותם של טרוריסטים ברשת.

<u>בפרק הראשון</u> סקרנו את משמעות המונח טרור ומאפייני התופעה. ראינו שלמרות שמדובר במונח שקשה להגיע לגביו להסכמה בינלאומית, הרי שהטרור הולך ולובש אופי בינלאומי שמחייב את המדינה הדמוקרטית להפעיל אמצעי פיקוח חודרניים כלפי מסגרת רחבה ביותר של בני אדם, לעיתים קרובות תוך שימוש ובשיתוף עם גורמים מסחריים ולפגוע בזכויות האדם. ראינו כי ארגוני הטרור עושים שימוש נרחב ברשת לצרכיהם בדגש על השימוש ברשת כאמצעי תקשורת בשירות הטרור. לאור זאת התעכבנו <u>בפרק השני</u> על המיקוד המודיעיני של גורמי הביון בישראל ובעולם בתווך הזה ודנו במאפיינים המיוחדים של אמצעי המעקב שמופעלים בזירת האינטרנט לניטור מידע תקשורתי ותוכני המועבר ברשת ולחדירה ואיסוף מידע מהשרת והמחשב האישי של חשודים בטרור וסקרנו את האיומים על זכויות הפרט ביחס ליכולות ניתור ומעקב אלו. <u>בפרק השלישי</u> בחנו את ההגבלות המשפטיות על פעולות הסיכול והמעקב המקוון ובחנו את מערכת האיזונים הקיימת בין צורכי המודיעין וזכויות הפרט במסגרת הדין הקיים בדמוקרטיות שונות בעלות מסורת של הגנה על זכויות הפרט. את הדיון סיימנו בסקירת האיזונים הקיימים בהקשר זה בדין הישראלי הקיים. <u>בפרק הרביעי</u> ניסינו לבחון האם מערכת האיזונים בין צרכי הביטחון לבין זכויות הפרט אשר התפתחה בישראל ביחס להפעלת אמצעי ציתות ומעקב בתקשורת אנלוגית מתאימה לרשת.

בעבודה זו ראינו כי כמו במשפט האמריקני, בישראל מוענקות לרשויות הביטחון סמכויות אדירות לחדור לצנעת חיו של אדם במרחב המקוון. בניגוד לארצות הברית, בריטניה וקנדה, הדין הישראלי מסמיך לכך את הרשויות על סמך דברי חקיקה פזורים, שלא נמצאים במסגרת נורמטיבית כוללת אחת, בעלי תשתית מושגית שאינה אחידה או קוהרנטית. דעתי היא כי לצד הטלת סמכות רחבה לרשויות הביטחון לפקח על פעילות מקוונת של הפרט, סמכויות אלו צריכות להיות מוסדרות באופן פרטני ותוך תשומת לב לטכנולוגיה המתפתחת, על מנת שלא לאפשר לגורמי מודיעין מסכל מרווח שיאפשר להם להפר את האיזון בין ביטחון הציבור והפגיעה בפרטיות.

השאלות שהעלנו בפרק הרביעי מצביעות לטעמי על כך שיש מקום לדון באופן מקיף בהסמכה החוקית לפעילות המעקב המקוונת של גורמי הביטחון בישראל, בצורך להפריד בין פעילות חודרנית במרחב המקוון לסיכול טרור לבין קידום אינטרסים אחרים, באופן בו ההסדרים הקיימים מתירים את הפגיעה בזכויות הפרט תוך שיקול דעת שיפוטי או מינהלי, ובאופן בו הדין הישראלי מקיים ביקורת ופיקוח על הפעלת סמכויות אלו על ידי רשויות הביטחון.

ייתכן בהחלט כי דיון שכזה יכול להצביע על כך שהאיזונים שנקבעו בדין הישראלי לפני מספר עשורים בהקשר של העולם האנלוגי שהכרנו אז, אינם מתאימים יותר לעידן הדיגיטאלי בו אנו נמצאים.

רשימת מקורות

** כל הקישורים המאוזכרים בעבודה הינם פעילים ונבדקו לאחרונה בתאריך ה-9 בספטמבר 2012.*

<u>חקיקה ישראלית</u>:

- חוק יסוד: כבוד האדם וחירותו, ס"ח תשנ"ב מס' 1391.
- חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007, ס"ח תשס"ח מס' 2122.
- חוק שירות הביטחון הכללי, התשס"ב-2002, ס"ח תשס"ב מס' 1832.
- חוק המחשבים, תשנ"ה-1995, ס"ח תשנ"ה מס' 1534.
- חוק התקשורת (בזק ושידורים), תשמ"ב-1982, ס"ח 218.
- חוק הגנת הפרטיות, התשמ"א-1981, ס"ח תשמ"א מס' 1011.
- חוק האזנת סתר, התשל"ט–1979, ס"ח תשל"ט מס' 938.
- פקודת הראיות [נוסח חדש], תשל"א-1971, פורסם דיני מדינת ישראל, נוסח חדש 18, עמ' 421.
- פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט-1969.
- פקודת מניעת טרור, תש"ח-1948, ע"ר מס' 245, 29.9.1948, עמ' 73.
- תקנות האזנת סתר (בקשה להיתר האזנה), תשס"ז-2007, ק"ת תשס"ז מס' 6586.
- תקנות האזנת סתר, התשמ"ו- 1986, ק"ת התשמ"ו 111.
- תקנות ההגנה (שעת-חירום), 1945, ע"פ סעיף 6 לדבר המלך על ארץ ישראל (הגנה), 1937.
- "תפישת הודעות קוליות האגורות בתא קולי ומסרים בדואר אלקטרוני האגורים במחשבי ספק השירות" הנחיות פרקליטת המדינה 14.15 (2004).
- "יעוד, ערכים וחזון השירות", קוד אתי לשירות ביטחון כללי (1998), פורסם באתר שירות הביטחון הכללי www.shabak.gov.il/about/pages/values.aspx.

<u>תזכירי והצעות חוק ישראליים</u>:

- הצעת חוק שירות הביטחון הכללי, התשנ"ח-1998, ה"ח תשנ"ח מס' 2689, 244.
- הצעת חוק דיני העונשין (האזנת סתר), תשל"ח-1978, ה"ח תשל"ח מס' 1361, 302.

<u>הנחיות של גופים שלטוניים</u>:

- "תפישת הודעות קוליות האגורות בתא קולי ומסרים בדואר אלקטרוני האגורים במחשבי ספק השירות" הנחיות פרקליטת המדינה 14.15 (2004).
- "יעוד, ערכים וחזון השירות", קוד אתי לשירות ביטחון כללי (1998), פורסם באתר שירות הביטחון הכללי www.shabak.gov.il/about/pages/values.aspx.

<u>פסיקה ישראלית</u>:

- בג"צ 951/06 **עזרא שטיין נ' רב ניצב משה קראדי**, דינים עליון 2006 (26) 755.
- בג"ץ 5100/94 **הוועד הציבורי נגד עינויים בישראל נ' ממשלת ישראל**, פ"ד נג(4) 817.
- בג"ץ 414/89 **בן נ' שר המשפטים**, פ"ד מג (4) 327.
- בג"צ 73/53 **חברת "קול העם " בע"מ נ' שר-הפנים**, פ"ד ז(2) 871.
- בג"צ 16/48 **ברון נ' ראש המשלה ושר הבטחון**, פ"ד א 109.
- בש"פ 7368/05 **זלוטובסקי ואח' נ' מדינת ישראל** (פורסם בנבו) (החלטה מיום 4.9.2005) פסקה 7 לפסק הדין.
- עמ"מ 94 / 10 **פלונים נ' שר הביטחון**, נג (1) 97.
- ע"פ 568/99 **עסאף נ' מ"י**, תק-על 2001(2) 242.
- ע"פ 1497/92 **מדינת ישראל נ' אלי בן משה צוברי**, פ"ד מז (4) 177.
- ע"פ 4211/91 **מ"י נ' אל מצרי**, פ"ד מז (5) 624.
- ת"פ (ת"א) 40206/05 **מדינת ישראל נ' אליעזר פילוסוף ואח'**, תק-מח 2007(1) 4872 (החלטה מיום 5.2.2007).
- ב"ש (ת"א) 090868/00 **חב' נטוויז'ן בע"מ נ' צבא ההגנה לישראל ואח'** (פורסם בנבו) (22.6.2000).
- ת"פ (ת"א) 40250/99 **מ"י נ' מונדיר בן קאסם בדיר** (פורסם בנבו) (4.9.2001).

<u>ספרים בעברית</u>:

- דן חי, **נתוני תקשורת בישראל**, ויטל – הוצאה לאור, 2011.
- מיכאל בירנהק, **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה**, נבו הוצאה לאור בע"מ, 2011.
- דן חי, **ההגנה על הפרטיות בישראל**, מילגה הוצאה לאור בע"מ, 2006.
- עמנואל גרוס, **מאבקה של דמוקרטיה בטרור – היבטים משפטיים ומוסריים**, נבו הוצאה לאור בע"מ, 2004.
- בועז גנור, **מבוך הלוחמה בטרור: כלים לקבלת החלטות**, הרצליה: הוצאת מפעלות המרכז הבינתחומי, 2003.
- נמרוד קוזלובסקי, **המחשב וההליך המשפטי**, הוצאת לשכת עו"ד, 2000.
- מנחם הפופנונג, **ישראל – ביטחון המדינה מול שלטון החוק**, נבו הוצאה לאור בע"מ, 1991.

<u>מאמרים בעברית</u>:

- "רשות הציטוט" **ידיעות אחרונות** 17.05.2012.
- שמואל אבן ודוד סימן-טוב "**לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**" המכון למחקרי ביטחון לאומי, מזכר 109, יוני 2011.
- מרטין ס' ליביקי "השימושים האסטרטגים בעמימות במרחב הקיברנטי" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 3.

- מרים דאן קוולטי "על המשכיות ושינוי בשיח על איומי הסייבר" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 11.
- אמיר לופוביץ "לוחמה קיברנטית והרתעה: מגמות ואתגרים במחקר" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 41.
- יורם שוייצר, גבי סיבוני ועינב יוגב "המרחב הקיברנטי וארגוני הטרור" **צבא ואסטרטגיה**, כרך 3, גיליון 3 (2011) 33.
- טבנסקי ליאור "לחימה במרחב הקיברנטי: מושגי יסוד" **צבא ואסטרטגיה**, כרך 3, גיליון 1 (2011), עמ' 80-65.
- אריה רוטר "**חוק שירות הביטחון הכללי – אנטומיה של חקיקה מהתהליכים הפנים ארגוניים ועד לחוק הכנסת, ביטוי לשינוי התפיסה ביחסים שבין חוק לביטחון בישראל**" מרכז המחקר המכללה לביטחון לאומי, מרץ 2010.
- דפנה ברק-ארז "המאבק המשפטי בטרור: ההיבט המוסדי" **עיוני משפט** לב, תש"ע, עמ' 46.
- שרון אהרוני-גולדנברג "חדירה למערכות מחשב – היקפה הרצוי והמצוי של העברה", **ספר דויד וינר** (2009) 429.
- מיכאל בירנהק "חוק נתוני תקשורת והפגיעה בזכות לפרטיות" **הסניגור** 130 (2008), 4.
- דנה בלאנדר "טרור – כואב, אבל עמום" המכון הישראלי לדמוקרטיה, **פרלמנט**, כתב עת מקוון (גליון 59) 2008.
- קרין תמר שפרמן "פני הטרור העתידיים – סייבר-טרור" המכון הישראלי לדמוקרטיה, **פרלמנט**, כתב עת מקוון (גליון 59) 2008.
- ויקטור ח. בוגנים "חוק המחשבים והתמודדות המשפט עם האתגר הטכנולוגי" ***שערי משפט*** ד(2) התשס"ו 283.
- יעל און ואח' "**פרטיות בסביבה הדיגיטלית**" המרכז למשפט וטכנולוגיה, עורכים: ניבה אלקין-קורן, מיכאל בירנהק, (2005).
- בועז גנור "'הדילמה הדמוקרטית' בלוחמה בטרור" **משפט וצבא** 17 (התשס"ד), עמ' 170.
- דפנה בן-פורת "**מסמך רקע בנושא: חקיקה בעניין האזנת סתר בבריטניה ובקנדה**" הכנסת, מרכז מחקר ומידע, מוגש לועדת החוקה, חוק ומשפט (2004).
- אודי איינהורן ואח', נייר עמדה "**לוחמה בטרור בזירת המידע**", המרכז למשפט וטכנולוגיה, עורכים: ניבה אלקין-קורן, מיכאל בירנהק, תשס"ב-2002.
- אלעד אורג **אנונימיות, משפט ואינטרנט, על חשיבה משפטית בנוגע לפעילות אנונימית באינטרנט ובכלל** (עבודה מסכמת לצורך קבלת תואר "מוסמך במשפטים") אוניברסיטת תל-אביב, הפקולטה למשפטים (2002).
- יריב צפתי, גבריאל וימן, "טרור באינטרנט" **פוליטיקה** 4 (1999).
- גבי ויימן "תיאטרון הטרור: אתגרה הקשה של הדמוקרטיה" בתוך: **סוגיות בדמוקרטיה הישראלית**, כהן אלמגור ר' (עורך) (1999).
- צימרמן אריאל "**הצעת חוק השב"כ : ניתוח משווה - הערות מרכזיות להצעת החוק לאור המשפט המשווה**" המכון הישראלי לדמוקרטיה , נייר עמדה מס' 3, ירושלים , התשנ"ז 1997.
- זאב סגל "על הזכות המוגנת בבג"ץ, הזכות לדעת והאזנת סתר" ***משפטים*** כ"א, תשנ"ב, 559.

מקורות בעברית באינטרנט:

- "מטרת וירוס להבה: השגת רישומים טכניים מאיראן" **YNET** 5 ליוני 2012, .www.ynet.co.il/articles/0,7340,L-4238369,00.html
- "ישראל וארה"ב ביחד: מלחמת סייבר נגד איראן" **YNET** 1 ביוני 2012 . www.ynet.co.il/articles/0,7340,L-4236972,00.html
- רם לוי "מרחב הלחימה החמישי" אתר **IsraelDefence**, 16 לדצמבר 2011, .www.israeldefense.co.il/?CategoryID=512&ArticleID=1470
- אתר חדשות ערוץ 2 "**יובל דיסקין: "יכולות טרור אינטרנטי מאיימות על מדינות שלמות**" גלובס 1.11.2010 .www.globes.co.il/news/article.aspx?did=1000597974
- שירות הביטחון הכללי "**סקירת מאפייני הפיגועים הבולטים בעימות הנוכחי – ניתוח מאפייני הפיגועים בעשור האחרון**" (2010) ניתן לצפייה באתר השב"כ www.shabak.gov.il/publications/decade/Pages/default.aspx
- שירות הביטחון הכללי "**פעילות חזבאללה מול ערביי ישראל**" מאי 2010, www.shabak.gov.il/publications/study/Pages/hizballahdecade.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93
- מרכז המידע למודיעין ולטרור, טרור ואינטרנט: **הכרזה על "אנתיפאדה אלקטרונית" נגד ישראל באמצעות רשת פייסבוק באינטרנט**, המרכז למורשת המודיעין (מל"מ) (2010) www.terrorism-info.org.il/he/article/18136.
- שירות הביטחון הכללי "**גיוס אזרחים ישראלים על ידי גורמי טרור ברשת האינטרנט**" מאי 2009, www.shabak.gov.il/publications/study/Pages/internetTerror.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93.
- מרכז המידע למודיעין ולטרור, מבזק טרור ואינטרנט טרור ואינטרנט: **לאחרונה הוגשו כתבי אישום נגד שני תושבי רהט, חברי התנועה האסלאמית, בחשד כי פעלו מטעם גורמי ג'יהאד עולמי ואלקאעדה**, המרכז למורשת המודיעין (מל"מ) (2008) www.terrorism-info.org.il/he/article/18439
- מרכז המידע למודיעין ולטרור, מבזק טרור ואינטרנט **כוחות הביטחון עצרו בחודש האחרון שישה צעירים ערבים אזרחי ישראל ותושבי מזרח ירושלים, חלקם סטודנטים באוניברסיטה העברית בירושלים**, המרכז למורשת המודיעין (מל"מ) (2008) www.terrorism-info.org.il/he/article/18438 .
- מרכז המידע למודיעין ולטרור, מבזק טרור ואינטרנט: **דו"ח של הסנאט האמריקאי מנתח את השימוש הנרחב שעושה ארגון אלקאעדה באינטרנט במסגרת המלחמה על התודעה שהוא מנהל**, המרכז למורשת המודיעין (מל"מ) (2008) www.terrorism-info.org.il/he/article/18444.

- מרכז המידע למודיעין ולטרור, מבזק טרור ואינטרנט **חמא"ס שידרגה לאחרונה את אתר האינטרנט של גדודי עז אלדין אלקסאם**, המרכז למורשת המודיעין (מל"מ) (2008) www.terrorism-info.org.il/he/article/18454.
- מרכז המידע למודיעין ולטרור, מימון הטרור: **חזבאללה מגייס תרומות עבורו ועבור מוסדות הקשורים עימו באמצעות אתרי האינטרנט שלו בלבנון ובארצות נוספות ברחבי העולם**, המרכז למורשת המודיעין (מל"מ) (2008) www.terrorism-info.org.il/he/article/18466 .
- מרכז המידע למודיעין ולטרור, האינטרנט בשימוש ארגוני הטרור: **תשתית אתרי האינטרנט של הג'האד האסלאמי בפלסטין וספקיות השירותים בהן מסתייע הארגון**, המרכז למורשת המודיעין (מל"מ) (2007) www.terrorism-info.org.il/he/article/18566.
- מרכז המידע למודיעין ולטרור, **האינטרנט כזירת מאבק עם ארגוני הטרור: השימוש שעושים חזבאללה וחמאס באינטרנט במלחמה על התודעה ודרכי ההתמודדות עם התופעה**, המרכז למורשת המודיעין (מל"מ) (2007) www.terrorism-info.org.il/he/article/18589.
- לקט מרכז המידע למודיעין ולטרור, **המלחמה על התודעה במסגרת העימות בין ארגוני הטרור לבין ישראל כמקרה מבחן**, המרכז למורשת המודיעין (מל"מ) (2007) www.terrorism-info.org.il/he/article/18625.
- האגודה לזכויות האזרח **"הצעת חוק השב"כ – הערות האגודה לזכויות האזרח"** (2002), פורסם באתר האגודה לזכויות האזרח www.acri.org.il/he/?p=5634 .
- שירות הביטחון הכללי, פורטל הטרור, **מילון מושגים**, תאריך פרסום לא זמין, ניתן לצפייה באתר השב"כ www.shabak.gov.il/publications/Pages/dictionary-terms.aspx.
- נמרוד קוזלובסקי "הגנה על הפרטיות במרחבי האינטרנט" **אתר פסק דין**, תאריך פרסום לא זמין www.psakdin.co.il/fileprint.asp?FileName=/Ip/Public/art_bddh.htm.
- נמרוד קוזלובסקי "משטרת האינטרנט" **אתר פסק דין**, תאריך פרסום לא זמין www.psakdin.co.il/fileprint.asp?filename=/ip/public/art_bbxx.htm.

ועדות ודוחות בעברית:

- כנסת ישראל, **סיכום דיוני ועדת החקירה הפרלמנטרית לחקר האזנות הסתר**, ינואר 2009.
- משרד המשפטים, **דין וחשבון של צוות הבדיקה בנושא האזנת סתר** – בעקבות בחינתו של היועץ המשפטי לממשלה, מר אליקים רובינשטיין, את תיק המחלקה לחקירות שוטרים בפרשת האזנת הסתר ביחידה הארצית לחקירות הונאה שנפתח נגד ניצב משה מזרחי, אפריל 2005.
- משרד המשפטים, **הוועדה לבדיקת בעיות משפטיות הנובעות ממסחר אלקטרוני**, דוח חלקי, מאי 2004.
- **הדין והחשבון השנתי של מבקר המדינה** מס' 54ב, יוני 2003.

אמנות בינלאומיות:

- Council of Europe, Convention on Cybercrime, Budapest 2001 23.XI.2001, *available at*: conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

דירקטיבות האיחוד האירופאי:

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *available at*: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT.

תחיקה - בריטניה:

- Anti Terrorism Crime and Security Act 2001, c. 24. (Eng.) *available at*: www.legislation.gov.uk/ukpga/2001/24/contents.
- Terrorism Act, 2000, c. 11 (Eng.) *available at*: www.legislation.gov.uk/ukpga/2000/11/contents .
- Regulation of Investigatory Powers Act 2000, c. 23 (Eng.), *available at*: www.legislation.gov.uk/ukpga/2000/23/contents.
- Regulation of Investigatory Powers (Interception of Communications: Code of Practice), Order, 2002, No. 1693 (Eng.).

תחיקה - קנדה:

- An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts (Bill C-30), *Available at*: www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5380965.
- National Defence Act (R.S.C., 1985, c. N-5).
- Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23).

תחיקה - ארצות הברית:

- Cyber Intelligence Sharing and Protection Act of 2011, H.R.3523.
- Protect America Act of 2007, Pub.L. 110-55, 121 Stat. 552.

- Intelligence Reform and Terrorism Prevention Act of 2004, Pub.L. 108-458, 118 Stat. 3638.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, P.L. 107-56, 115 Stat. 272.
- Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010.
- Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701-2710, 3121-3126.
- The Foreign Intelligence Surveillance Act of 1978, Pub.L. 95-511, 92 Stat. codified as amended at 50 U.S.C. §1801-1811.
- Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, codified as 18 U.S.C. §2510-2522.
- Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. §401 note.

פסקי דין - ארצות הברית:

- United States v. Truong Dinh Hung, 629 F. 2d 908 (4th Cir. 1980).

מאמרים באנגלית:

- Denning, D. E., *Terror's Web: How the Internet is Transforming Terrorism*, in Handbook on Internet Crime (Y. Jewkes and M. Yar, eds.), Willan Publishing (2010).
- Gabriel Weimann, *www.terror.net how modern Terrorism Uses the Internet*, United States Institute of Pace, Special Report 116 (2004).
- Tsfati, Yariv, and Weimann, Gabriel, *www.terrorism.com: Terror on the Internet*, Studies in Conflict and Terrorism (2002).
- Cicero, Pro Milone (N.H. Watts trans., Harvard Univ. Press, 5th ed. 16) (1972).

מקורות באנגלית באינטרנט:

- The National Counterterrorism Center, *2011 Report on Terrorism* (2012), *available at* www.nctc.gov/docs/2011_NCTC_Annual_Report_Final.pdf.
- Michael Jacobson, Terrorist Financing and the Internet, Studies in Conflict & Terrorism, 2010, *available at*: www.tandfonline.com/doi/pdf/10.1080/10576101003587184

- America Civil Liberties, *Surveillance Under the USA Patriot Act* (2010), *available at*: www.aclu.org/national-security/surveillance-under-usa-patriot-act.
- Brian Ross and Rhonda Schwartz, *Major Hasan's E-Mail: 'I Can't Wait to Join You' in Afterlife*, abc News, November 2009 *available at*: abcnews.go.com/Blotter/major-hasans-mail-wait-join-afterlife/story?id=9130339#.UEJZYsHN_kc .
- United States Senate Committee on Homeland Security and Governmental Affairs, *Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat* (2008) *available at*: hsgac.senate.gov/public/_files/IslamistReport.pdf.
- Denning, Dorothy E., *Cyberterrorism*, 2000 *available at*: www.cs.georgetown.edu/%7Edenning/infosec/cyberterror-GD.doc .