אוניברסיטת חיפה
University Of Haifa

הפקולטה למשפטים
FACULTY of LAW

המרכז למשפט וטכנולוגיה
The Law and Technology Center

The Caesarea Edmond Benjamin de Rothschild Foundation
Institute for Interdisciplinary Applications
of Computer Science

לוחמה בטרור בזירת המידע

מאת

תלמידי הסדנה הרב-תחומית במשפט וטכנולוגיה

המרכז למשפט וטכנולוגיה
הפקולטה למשפטים
אוניברסיטת חיפה

תשס"ב – 2002

סדנה רב-תחומית במשפט וטכנולוגיה

המרכז למשפט וטכנולוגיה
הפקולטה למשפטים
אוניברסיטת חיפה

צוות הכותבים

אודי איינהורן | **בן זהר**

ערן אלוני | **אפי מיכאלי**

קרן אלישע | **ניר סגל**

רחל ארידור | **גל עשת**

ערן בר-אור | **אלון פיול**

יעל ברגמן | **אסף צברי**

שחר גרינברג | **טל רון**

אייל גרינר | **מירי שי**

חביבה גרמן

מנחים ועורכים

ד"ר ניבה אלקין-קורן | **ד"ר מיכאל בירנהק**

בשיתוף המכון ליישומים בין-תחומיים של מדעי המחשב
ע"ש קרן קיסריה אדמונד בנימין דה-רוטשילד

הקדמה ודברי תודה

האירועים שהתחוללו בעולם בחודשי הסתיו של שנת 2001 הובילו מחוקקים וממשלות ברחבי העולם לבחון מחדש את מדיניותן באשר לשאלות של ביטחון. הטרור הגלובלי משתמש גם באמצעים טכנולוגיים מתקדמים, ומציב אתגרים קשים למעצבי המדיניות. לפיכך החלטנו להקדיש את סדנת המחקר למשפט וטכנולוגיה בשנת הלימודים תשס״ב לשאלת עיצוב המדיניות הראויה בממשק שבין ביטחון לטכנולוגיה, זכויות אדם, ומדיניות כלכלית. בסדנה השתתפו שבעה עשר סטודנטים מצטיינים מן הפקולטה למשפטים באוניברסיטת חיפה אשר נבחרו בתהליך מיון קפדני.

הסדנה למשפט וטכנולוגיה מהווה מסגרת מחקר ייחודית העוסקת בשאלות מעשיות מתחום מדיניות המידע. עיצוב המדיניות בתחום המשפט וטכנולוגיה מתרחש לא רק בבתי המשפט, אלא גם – ובמידה רבה – בכנסת וברשויות המדינה השונות. מעצבי המדיניות אשר זקוקים למידע, נתונים, הערכות, ניתוח המשמעות וההשלכות של המדיניות על מנת שיוכלו לקבוע את דרכי פעולתם, ניזונים בעיקר מקבוצות אינטרסים המספקות נתונים אשר כמובן מקדמים את ענייניהם. הקול הציבורי כמעט שאינו נשמע בדיונים האלה. גם חברות רבות, ובעיקר חברות סטארט-אפ חדשות, זקוקות להדרכה משפטית בנושאים בעלי נגיעה ציבורית. הסדנה למשפט וטכנולוגיה נועדה למלא את החלל הזה.

עבודת המחקר והכתיבה בסדנה התנהלה במספר שלבים. לאחר סיעור מוחות ראשוני וגיבוש נושאי המחקר, צוותו המשתתפים לצוותי עבודה, על-פי סוג המחקר: צוות אחד התמקד בפן הטכנולוגי, צוות אחר בפן המשפטי, והצוות השלישי נשלח לשדות מחקר אחרים – לימודים אסטרטגיים, כלכלה, תקשורת ועוד. בתום המחקר הראשוני נערכה סדרת מפגשים של משתתפי הסדנא, בהנחייתנו, בה לובנו השאלות והנושאים שעל הפרק. עם השלמת המחקר והשלמת הטיוטא הראשונית של נייר העמדה, סברנו כי יש מקום ללמוד מה עמדתם של מומחים ובעלי מקצוע בתחומים שבהם עסקנו. כך בא לעולם כנס שפיים (26-27 לדצמבר, 2001). במשך יומיים מרוכזים דנו בסוגיות שעל הפרק עם עשרות מומחים מתחומי מחקר ועיסוק שונים: מדעי המחשב, משפטים, לימודי תקשורת, לימודי ביטחון, ועוד. המשפטנים באו מהאקדמיה, מהשוק הפרטי, ומהמגזר הציבורי: משרד המשפטים ומשרד הביטחון. שמענו גם את עמדותיהם של העוסקים במלאכה במישרין: חוקרים בתחום ההצפנה, אנשי ביטחון, עורכי דין ואנשי עסקים. הדינמיקה שנוצרה במהלך שני ימי הדיונים, ההרצאות המאלפות והדיונים הפוריים הבהירו יותר מכל את הצורך בדיון בלתי תלוי ובעבודת מחקר עצמאית ורב תחומית בנושאים הקשורים למשפט וטכנולוגיה.

לקחי המחקר וכנס שפיים מסוכמים בנייר העמדה שלפניכם. נייר עמדה זה הוא פרי עמלם של תלמידי הסדנה ב"מידע ומסחר אלקטרוני" שהועברה על-ידינו בסמסטר א' של שנת הלימודים תשס"ב. בסוגיות רבות הוא משקף ניסיון ראשון מסוגו להתמודד עם סוגיות אשר טרם זכו לדיון ציבורי בישראל. הננו תיקווה כי נייר עמדה זה יהווה בסיס לדיון רציני בסוגיות הטעונות הכרעה ויסייע בעיצובה של מדיניות מושכלת בנוגע למלחמה בטרור ברשת האינטרנט.

פעילות הסדנה התאפשרה הודות לתמיכתו הנדיבה של המכון ליישומים בין-תחומיים של מדעי המחשב ע"ש קרן קיסריה, אדמונד בנימין דה-רוטשילד באוניברסיטת-חיפה. אנו מבקשים להודות לראש המכון, פרופסור מרטין גולומביק והמתאמת המדעית ד"ר אירית הרטמן, שסיפקו לא רק את האמצעים, אלא הפגינו התלהבות לאורך הפרוייקט כולו, ותרמו באופן פעיל למפגש עצמו. אנו מבקשים להודות גם לגב' שריל זורלא, מזכירת המכון, שסייעה לנו רבות בהפקת המפגש בשפיים.

שורת מומחים נכבדה הקדישה זמן ומאמץ לסדנה, ותרומתם של המשתתפים כולם הייתה רבה. המשתתפים מיקדו את השאלות העומדות לדיון, הציגו זוויות רבות ומגוונות לסוגיות שעל סדר היום, חידדו נקודות עמומות, ואנו מבקשים להודות לכולם (לפי סדר א"ב):

ד"ר גדי אהרוני; עו"ד עמית אשכנזי; עו"ד מייק בלס; עו"ד נאוה בן אור; פרופסור אריאל בנדור; קרין ברזילי-נהון; עו"ד מתי ברזם; עו"ד בועז גוטמן; שמעון גרופר; פרופסור עמנואל גרוס; אריק וולף; עו"ד דודי זלמנוביץ'; ד"ר לימור יגיל; ד"ר אסף יעקב; יורם כהן; ד"ר משה כהן-אליה; ד"ר רפי כהן-אלמגור; ד"ר הלל נוסק; ד"ר אריאל סובלמן; עו"ד דורית ענבר; אריאל פיסצקי; ד"ר יריב צפתי; פרופסור איל קושילביץ; עו"ד תמר קלהורה; פרופסור הוגו קרבצ'יק; יעל שחר; אפרת שמעוני; עו"ד טנה שפניץ; עו"ד שרון קרן; ד"ר יובל קרניאל; עו"ד רם רביב; עו"ד חיים רביה; פרופסור שיזף רפאלי; יוסי שני.

במהלך המחקר, הכתיבה והפקת הסדנה התייעצנו עם אנשים נוספים, ואנו מבקשים להודות גם להם: פרופסור ניב אחיטוב; פרופסור גבי וימן; עודד כהן; ד"ר דפנה למיש; ד"ר פניה עוז-זלצברגר; ד"ר עמוס פיאט.

אנו מבקשים להודות גם לאנשי הפקולטה למשפטים באוניברסיטת חיפה שסייעו לנו: הדיקן פרופסור יוסף אדרעי; ראש מינהל הפקולטה, משה סייג; רכזת הפקולטה, דורית ארבל; ומזכירת הדיקן, דסי פישר. הפקת האירוע התאפשרה בזכות עבודתו המסורה של טל רון, מתאם המרכז למשפט וטכנולוגיה.

ניבה אלקין-קורן, מיכאל בירנהק
חיפה, מאי 2002

תוכן

- תוכן עניינים מפורט

- ריכוז ממצאים והמלצות

I. מבוא

II. סביבת המידע כזירה מאובטחת: ביטחון, שוק חופשי והצפנה

III. סביבת המידע כזירת מעקב: ביטחון, פרטיות וחופש הביטוי

IV. סביבת המידע כזירת תעמולה: ביטחון, חופש הביטוי ואחריות ספקים

תוכן עניינים

הקדמה ודברי תודה ..... ג
ריכוז ממצאים והמלצות ..... ח
I. מבוא: שיקולי ביטחון – מיפוי האיומים 1
II. סביבת המידע כזירה מאובטחת:ביטחון, שוק חופשי והצפנה 7
א. הצגת הבעיה 7
ב. מהי הצפנה: הבסיס הטכנולוגי 8
1. מבוא 8
2. עקרון ההצפנה הבסיסי: המרת אותיות באותיות 9
3. ההצפנה הסימטרית 9
4. ההצפנה א-סימטרית: מפתח פומבי ומפתח פרטי 10
ג. הצרכים הביטחוניים 14
1. אבטחה 14
2. מעקב – מודיעין 15
3. הטעם שברגולציה 16
ד. המסגרת המשפטית 17
1. ישראל: מאיסור גורף לרישוי מוקדם ופיקוח מאוחר 17
2. ארצות הברית 23
3. המישור הבינלאומי 26
ה. השלכות ושיקולי מדיניות 36
1. התערבות בשוק ושיקולי מחקר ופיתוח 36
א. השפעת התערבות ממשלתית על תחומי מחקר ופיתוח 36
ב. הגבלות על ייצוא אמצעי הצפנה ועל השימוש בהם 37
2. השפעתה של רגולציה בתחום ההצפנה על המסחר האלקטרוני 38
3. הזכות לפרטיות 38
4. חופש הביטוי 41
5. חופש העיסוק 46
6. הזכות לקניין 49
ו. ריכוז המלצות 50
III. סביבת המידע כזירת מעקב: ביטחון, פרטיות וחופש ביטוי 53
א. הקדמה 53
ב. מודיעין בעידן המידע 54
1. רקע כללי 54
2. אמצעים לאיסוף מידע ומעקב ברשת 56
2.1 ניטור מידע 56
2.2 איסוף מידע על גבי השרת או המחשב האישי 59
ג. סיכול ואכיפה בעידן המידע: איום על זכויות הפרט? 61
1. מבוא 61
2. מהי פרטיות ומהי הזכות לפרטיות? 61
3. האם מוצדק להגן על הפרטיות בסביבת המידע? 63
4. מהם גבולות ההגנה על הפרטיות בעידן המידע? 65
ד. הגבלות משפטיות על פעולות סיכול ואכיפה בעידן המידע 67
1. המסגרת המשפטית 67
2. ההקשר הבינלאומי 68
2.1 הגנה על הזכות לפרטיות 68
2.2 הסדרים בינלאומיים להגנה על מידע אישי 69
3. האיחוד האירופאי 71
3.1 הדירקטיבה האירופאית להגנה על מידע אישי 71
3.2 יישום הדירקטיבה על-ידי המדינות החברות 72
3.3 התפתחויות משפטיות לאחר ה- 11 בספטמבר 73

3.4 החוק הבריטי החדש למלחמה בטרור 74
3.5 איסוף מידע על-ידי ספקי שירות ברשת 75
4. ארצות הברית 77
4.1 רקע כללי 77
4.2 פיקוח משפטי על פגיעה בפרטיות על-ידי רשויות האכיפה 78
5. מדינות נוספות 81
5.1 קנדה 81
5.1 אוסטרליה 82
ה. המסגרת המשפטית: ישראל 82
2. אכיפה 83
3. חיפוש ותפיסה 85
4. האזנת סתר בדין הישראלי 86
4. אחריות ספקי שירות באינטרנט 92
ו. עידן המידע: האם יש צורך בהסדר חדש? 94
1. האם מערכת האיזונים הקיימת מתאימה לרשת? 94
2. מהי המשמעות של יישום ההסדר המשפטי הקיים על הרשת? 95
3. ריכוז המלצות 95
IV. סביבת המידע כזירת תעמולה: ביטחון, חופש הביטוי ואחריות ספקים 97
א. מהו "טרור תעמולתי"? 97
1. טרור תעמולתי ותעמולה בשירות הטרור 97
2. תוכן התעמולה 98
3. דרכי תעמולה 99
4. האם המדיום משנה את המהות? לוחמה פסיכולוגית בעידן הטכנולוגי 99
ב. חופש הביטוי באינטרנט 101
ג. אחריות ספקים 103
1. שיקולים בהטלת אחריות על גורמי ביניים (ספקי שירות) 103
2. מודלים לאחריות גורמי ביניים 105
א. מודל אחריות 106
ב. חסינות מלאה 106
ג. חסינות מותנית ומוגבלת 107
3. המצב המשפטי בישראל 108
ד. ריכוז המלצות 109

ריכוז ממצאים והמלצות

סביבת המידע כזירה מאובטחת: ביטחון, שוק חופשי והצפנה

1. הסדרתה של ההצפנה בחקיקת משנה במסגרת של חקיקה כלכלית איננה ראויה. מדובר בהסדר ראשוני באופיו ובמהותו, שיש לו השלכה על זכויות יסוד. בפועל, המדיניות הננקטת קובעת איסורים והיתרים ללא הסמכה פרטנית בחוק, באופן שקביעת המדיניות נעשית על-ידי הרשות המבצעת ללא הכוונת המחוקק. מצב זה איננו רצוי מבחינת עקרונות המשפט המינהלי והחוקתי, ויש לו השלכות שליליות על גמישותה של המדיניות הננקטת בפועל, כמו האפקט המצנן שיש לה על התעשייה. **לפיכך, אנו סבורים שיש להסדיר את ההתייחסות המשפטית להצפנה בחקיקה ראשית.**

2. מטרת החקיקה היא לענות על צורכי ביטחון אמיתיים של אבטחת מידע ביטחוני ומידע רגיש אחר ושל שימור אמצעי מעקב והשגת מודיעין למערכת הביטחון. צרכים אלה אינם מתייתרים, למרות נגישותם וזמינותם הגבוהה של מוצרי הצפנה. **לפיכך, המטרה של החקיקה היא לתכלית ראויה והולמת את ערכיה של מדינת ישראל, כנדרש בחוקי היסוד.**

3. ההסדרה הקיימת והחקיקה המוצעת פוגעות בחופש העיסוק, בזכות לקניין, ועלולות לפגוע בזכות לפרטיות ולאיים על הזכות לחופש ביטוי ומחקר אקדמי. **לפיכך, את ההסדרה הקיימת יש לפרש ברוח חוק היסוד, והחקיקה המוצעת חייבת לעמוד בתנאי המידתיות שבחוק יסוד: חופש העיסוק וחוק יסוד: כבוד האדם וחירותו.**

4. כדי לעמוד בדרישת המידתיות, החוק צריך להגדיר בבהירות ובמפורש את תחום ההסדרה, את מבחניה ואת היקף שיקול הדעת של הרשות.

5. קיימים מספר מודלים להסדרה. אנו סבורים כי אין לחזור לאחור, ואין לקבל מודל של איסור שבצידו חריגים. המודל המשפטי הקיים הוא מודל של רישוי מוקדם, ובו נעסוק תחילה.

6. **<u>מודל הרישוי:</u> יש להגדיר את היקף שיקול הדעת של הרשות**, ולצמצמו לצרכים ביטחוניים של ממש. מבין אלה, צורכי סיכול פעילות טרור, להבדיל מצרכים של השגת ראיות בדיעבד, צריכים לזכות במירב האהדה.

7. **יש מקום להגדיר את תחומי העיסוק הדורשים רישוי מוקדם**. לשם כך, יש להבחין בין שימושים פרטיים-אזרחיים לשימושים ביטחוניים. יש לפטור שימושים מהסוג הראשון מהסדרה כלשהי. ככל שיש קושי לסווג מוצר כמיועד לשימוש פרטי-אזרחי, וזאת מחמת מאפייני מוצרי ההצפנה כ dual use, יש מקום להסדרה, בכפוף לאמור להלן:

8. **יש מקום לזהות את מטרות היצרן**, ולהגביל את דרישת הרישוי לחלקן בלבד: בעיקר, יש להבחין בין שיווק מקומי לייצוא. נוכח הגדרת הצרכים הביטחוניים כהערמת קשיים על הגעתם של מוצרי הצפנה לידי ארגוני טרור - יש מקום לפיקוח על ייצוא, אך פחות מכך על שיווק מקומי, ובמיוחד כאשר ייעוד המוצר קרוב יותר לקצה האזרחי מאשר לשימוש הביטחוני.

9. **יש להגדיר במפורש את קריטריוני הפיקוח**: האם נבדק היעד הסופי של המוצר או עוצמת ההצפנה. במדינות שונות ננקטים מבחנים שונים. אין אנו מכריעים בעניין זה, ומסתפקים בכך שיש מקום לקבוע את הקריטריון, ובכך לאפשר לתעשייה לכלכל את תוכניותיה בהתאם ולפעול בוודאות גבוהה יותר.

10. **יש להגדיר את תהליכי האישור במפורש:**
    - יש לתחום את היקף המידע שהרשות רשאית לבקש מיצרן המבקש רישיון;
    - יש לקבוע את שלבי הבדיקה בחוק. פרטי השלבים יכולים להיקבע בתקנות;
    - יש לקבוע הליך ערעור למבקש שבקשתו נפסלה. יתכן שהמקום לכך הוא ביקורת שיפוטית של בתי המשפט לעניינים מינהליים, במסגרת עתירה מינהלית. במקרה כזה, יהיה מקום לקבוע סדרי דין מיוחדים כדי להבטיח את סודיות תוכן הדיונים.

11. **פיצוח הצפנה**: במקרה שבו הרשות מבקשת גישה למוצר הצפנה קיים, קרי ל"דלת אחורית", יש ליצור מנגנון של ביקורת שיפוטית מוקדמת, בדומה לזה המקובל בחוק האזנות סתר, תשמ"א – 1981.

12. **מודל רישום**: יש מקום לשקול מודלים אחרים להסדרה. מודל אפשרי אחד הוא של רישום הצפנות, ללא פיקוח מוקדם עליהן. מודל כזה, בדומה לרישום מאגרי מידע על-פי חוק הגנת הפרטיות, תשמ"א-1981, יטיל חובה אחת ויחידה על יצרן מוצרי הצפנה: רישום עצם קיומה ופרטים כלליים עליה. באופן כזה, תוכל הרשות הביטחונית לדעת איזה מוצרים מצויים בידי מי. במידת הצורך, תוכל הרשות לפנות לבית משפט בבקשה מוקדמת, ולבקש היתר לחדור למוצר ההצפנה.

סביבת המידע כזירת מעקב: ביטחון, פרטיות וחופש ביטוי

1. השאלה המרכזית עמה התמודדנו במסגרת פרק זה היא האם מערכת האיזונים בין צרכי הביטחון לבין זכויות הפרט אשר התפתחה ביחס לציתות ומעקב בתקשורת אנלוגית מתאימה לרשת?

2. אנו סבורים שהטכנולוגיה החדשה איננה מצדיקה זניחה של הערכים הקודמים לה – הן בדבר האיזון בין פרטיות לבין האינטרסים הציבוריים של מניעת פעילות טרור וסיכולה.

3. עם זאת, את ההסדר המשפטי – בין בחקיקה ובין בפרשנות שיפוטית – יש לעצב תוך תשומת לב למאפיינים הטכנולוגיים. במיוחד, אנו מבקשים להדגיש מספר מאפיינים ייחודיים לרשת האינטרנט, לשימוש ברשת ולמשתמשיה אשר עשויים להיות רלוונטיים בישומן של נוסחאות האיזון השונות:

    1. **עקבות דיגיטליים** – רשת האינטרנט היא כאמור סביבת מידע, שבה כל תקשורת והחלפת מסרים מהווה למעשה סוג של עיבוד נתונים היוצר רישום. אפשרויות המעקב הן אינהרנטיות להפעלת המערכת. במקרים רבים "האזנה" או רישום יהוו ברירת מחדל, והשמירה על הפרטיות תחייב פעולה אקטיבית של מחיקה, או ביטול הרישום, או מניעתו. מבחינה משפטית אבחנה זו עשויה להיות בעלת נפקויות. כך, למשל, הכלל המשפטי בהקשר של שיחות טלפון צריך לקבוע את הנסיבות בהן מותר לבצע האזנה כאמור כפי שנעשה בחוק האזנות סתר. יישומה של נוסחת האיזון באינטרנט עשויה לחייב הגדרת הנסיבות אשר תחייבנה פעולה של הימנעות, או מחיקה של קבצים קיימים, או הטלת מגבלות על השימושים, על התפוצה ועל השמירה של נתונים אלו.

    2. בסביבה הדיגיטלית ישנם אמצעים חודרניים רבי עוצמה אשר בפועל מעמידים את הפרט במצב של שקיפות לא-מודעת ועלולים ליצור פגיעה חסרת תקדים בפרטיות. אמצעים אלה מאפשרים חדירה למרחב הפרטי. המחשב המחובר לרשת גלובלית יוצר למעשה מעין דלת כניסה אחורית אל צנעת מסמכיו של אדם על גבי המחשב. לאחרונה דווח, כי ניתן גם באמצעות תוכנה המושתלת במחשב האישי דרך הרשת להפיק צילומים של המתרחש באופן פיזי בביתו של אדם. בנוסף, תוכנות מעקב ומאגרי מידע מאפשרים איסוף מידע (על-ידי מעקב והצלבה) על משתמשים במרחב הציבורי.

    3. בסביבה הדיגיטלית קיים פער משמעותי בין הציפייה לפרטיות לבין המציאות הפולשנית בה הפרט חשוף יותר מבעבר לחדירה לפרטיותו. עובדה זו ניתן לייחס למספר גורמים:

        - מודעות לאמצעים חודרניים. האמצעים החודרניים אינם שקופים למשתמש – המדובר בשילוב מערכות תוכנה וחומרה אשר אינן

בולטות לעין למשתמש הקצה, והפנמת האיום לפרטיות הטמון בהן עשוי לחייב ידע טכנולוגי ותחכום מעל הממוצע.

- חוויית הגלישה יוצרת אשליה של פרטיות: היא נעשית בפרטיות - במקרים רבים הגולש ימצא בביתו או במשרדו, הגולש נמצא לבד ולא בציבור; הגלישה היא פעולה עצמאית ובלתי תלויה, לכאורה, בשיתוף פעולה עם אנשים אחרים; שירותים אינטראקטיביים נחווים במקרים רבים כפעילות במסגרת קבוצה סגורה ואינטימית. כל אלו עשויים להגביר כמובן את הציפייה לפרטיות.

- השינויים התכופים בסביבה הדיגיטלית מחייבים עדכון שוטף באמצעים וביכולות הקיימות לחדירה לפרטיות: הן על-מנת להיות מודעים לאיום והן על-מנת שניתן יהיה להתגונן מפניו.

4. ניתן כמובן להפחית את הציפייה לפרטיות ולהזהיר את המשתמשים בדבר חשיפתם לאמצעי מעקב בסביבה הדיגיטלית באמצעות חינוך והסברה. מצד שני, העובדה שהטכנולוגיה מצויה עדיין בהתהוות ומשתנה בקצב מסחרר עשויה לצמצם את האפקטיביות של פתרונות אלו.

5. משמעות יישום ההסדר המשפטי הקיים: ההסדר המשפטי הקיים מבחין בין האזנת סתר לבין צו חיפוש מבחינת החומרה, ולכן גם מתייחס להאזנת סתר ביתר קפדנות מבחינת הדרישות המשפטיות. האזנת סתר המוסדרת בחוק האזנות סתר המגן על סוד השיח - מחייבת צו של נשיא בית משפט מחוזי או סגנו, שיינתן בתנאים המוגדרים בחוק. צו חיפוש, לעומת זאת, הוא בסמכותו של בית משפט שלום. חיפוש והאזנת סתר נבדלים זה מזה מבחינת מודעות אובייקט המעקב, משך הזמן של הפגיעה, וההשלכה על צדדים שלישיים. בכל מה שנוגע לחיפוש המדובר בפגיעה חד-פעמית, הנחקר מודע לה, והפגיעה ממוקדת בו ובחפציו. האזנת סתר, מנגד, היא פגיעה מתמשכת, ללא ידיעת הנחקר, אשר עלולה לפגוע בפרטיות החשוד (כאשר במסגרת מכלול שיחות החשוד להן מאזינות רשויות החקירה, נכללת גם לתקשורת אישית של החשוד אשר אינה רלוונטית לחקירה) וכן לפגיעה בצדדים שלישיים (משתמשים אחרים בקו הטלפון, וכן צדדים המשוחחים עם הנחקר).

6. על רקע הדברים הללו נראה כי מעקב ברשת דומה יותר להאזנת סתר. המדובר בפעולה המתבצעת ללא ידיעת הנחקר – לעיתים תוך שיתוף פעולה עם ספק השירותים בלבד. המדובר בפעילות מתמשכת, העלולה גם לפגוע בפרטיותם של גולשים אחרים.

7. המלצות:

1. יש לשמור על פרטיות הגולשים, וכי השינויים הטכנולוגיים המפליגים הטמונים בסביבה הדיגיטלית אינם צריכים לצמצם את הזכות לפרטיות או את ההגנה עליה.

2. את הכללים המשפטיים הפרטניים, יש לעצב בשים לב למאפיינים הטכנולוגיים המיוחדים שנדונו לעיל. כמו כן, אין לשלול את הכיוון ההפוך: הבניית ערכים של פרטיות לתוך הטכנולוגיה.

3. יש להביא בחשבון את היעדר הגבולות ברשת, וכן יש להביא בחשבון את הפער הדיגיטלי: יכולתם (הכלכלית וטכנולוגית) של גולשים להתמודד עם האיום על זכותם לפרטיות שונה. לפיכך, יש לידע ולחנך את הציבור בדבר זכותו לפרטיות, האיומים עליה, והדרך להתמודד עם איומים אלה.

4. לצד האיום הציבורי (מהמדינה) על הזכות לפרטיות, יש בסביבה הדיגיטלית איום משמעותי לא פחות על הפרטיות – איום שמקורו בגורמים מסחריים-פרטיים. על רקע זה, עולה השאלה, באיזו מידה יש להגביל את המדינה בשימוש באמצעים הנגישים לכל גורם פרטי? שאלת היחס שבין הסדרה פרטית להסדרה ציבורית מחייבת דיון נפרד, וכאן אנחנו מבקשים להצביע על הקושי.

סביבת המידע כזירת תעמולה: ביטחון, חופש ביטוי ואחריות ספקים

1. השאלה הראשונה שצריכה לעלות על סדר יומו של המחוקק היא הערכת הצורך בחקיקה פרטיקולרית לעניין אחריות ספקי שירות לתוכן מזיק שמקורו בצדדים שלישיים. השאלה כרוכה בבדיקת התנהגותם בפועל של ספקי השירות בהיעדר הסדרה: האם אי-הוודאות גורמת לתוצאות לא-רצויות. יש מקום לבחון האם הספקים נמנעים ממתן שירותים מסויימים (צ׳אטים, פורומים, שירותי איחסון אתרים וכדומה), או מגבילים ביטוי ביישומים השונים המופעלים על-ידם. כך למשל, יש מקום לבחון כיצד מגיבה ספקית שירות אחסון אתרים לתלונה של גולשים כנגד אתר אחר, או כנגד דבריו של גולש אחר בפורום המופעל על-ידי הספקית.

2. אם יתברר כי אי-הוודאות המשפטית הקיימת גורמת לכך שבפועל מתרחשת ״צנזורה פרטית״ **הרי יש מקום, לדעתנו, להבהיר את המצב המשפטי באמצעות חקיקה**.

3. חקיקה כזאת צריכה למזער את ההשלכות הלא-רצויות שבהן דנו לעיל. במיוחד, יש לוודא כי שיקול הדעת שמפעיל הספק מוגדר בדיוק רב ככל האפשר, ומותיר לספק מרחב החלטה בהיר ומצומצם. בדרך זאת נמזער את ״האפקט המצנן״, את ״האצבע הקלה״ של הספק על סגירת אתרים ויישומים אחרים, ואת הפקרת שיקול הדעת הציבורי בידיים פרטיות.

4. לטעמנו, כל אחד מן המודלים הקיימים שנסקרו לעיל (מודל של אחריות מלאה, חסינות מלאה או חסינות מותנית ומוגבלת) סובל מחסרונות ניכרים.

5. נראה לנו שיש מקום לאמץ גישה של הסדר אחיד באשר לסוגים שונים של תכנים מזיקים: בין אם מדובר בלשון הרע, פגיעה בפרטיות, בהפרת זכויות קניין רוחני או בתעמולת טרור.

6. יש מקום לאמץ את העקרון הכללי שנקבע בחקיקה האמריקנית בדבר חסינות לגורמי הביניים, אך לסייגה: יש לאפשר לנפגעים אפיק אכיפה אפקטיבי, על-ידי פנייה לבית המשפט. בכך שונה הצעתנו מהדין האמריקני. בית המשפט יידרש לשקול את האינטרס הציבורי או זכות הפרט המוגנת, אל מול שיקולי המדיניות והאינטרסים הציבוריים האחרים. בדרך זאת יובטח כי האיזונים החוקתיים, הערכיים שפותחו בפסיקה, יישמרו, ולא יופרטו אל סַפַּק השירות המסחרי. סמכותו של בית המשפט תוגבל להוצאת צווי מניעה בלבד.

7. כל עוד לא הורה בית משפט לספק לפעול, ייהנה ספק השירות מחסינות מפני תביעות של ניזוקים.

I. מבוא: שיקולי ביטחון – מיפוי האיומים[1]

הסביבה הדיגיטלית תופסת מקום מרכזי בחיינו בראשית האלף השלישי. היא איננה רק כיכר שוק ציבורית ומאגר מידע אינסופי. נתח הולך וגדל של הפעילות האנושית מתרחש כיום בסביבה זו: תקשורת בין-אישית, מסחר, ניהול ושליטה במערכות תשתית חיוניות, מחקר ועוד. אלא, שסביבה זו הפכה גם לזירה ביטחונית, ואירועי האחד עשר בספטמבר ממחישים זאת היטב.

בשנים האחרונות התמודדה מערכת המשפט בארץ ובעולם, ועדיין מתמודדת, עם הצורך להתאים את הכללים שפותחו בהקשר לעולם "המוחשי" לסביבה "הווירטואלית". השאלות בהן עסקו מחוקקים, בתי משפט וחוקרים נגעו בעיקר להקשרים מסחריים, כמו התאמת דיני הקניין הרוחני ודיני הפרטיות למדיום החדש, או להקשרים פליליים, דוגמת הימורים ומאבק בפדופיליה. כיום, נתונה תשומת הלב העולמית לאיומים ביטחוניים חדשים, בדמות טרור גלובלי. מערכת המשפט נדרשת לתת מענה לאיומים אלה, בכל תחומי החיים, לרבות בסביבה הדיגיטלית. השאלה היסודית – המתח שבין צורכי הביטחון לזכויות אדם - איננה חדשה. במדינות שונות נצבר ניסיון רב בסוגיות אלה. השאלה המתעוררת כעת, היא האם מערכת הכללים הקיימת, שפותחה על סמך הניסיון שנצבר בעולם "המוחשי" ישימה בסביבה הדיגיטלית?

נייר עמדה זה מצביע על הסביבה הדיגיטלית כעל זירה רלוונטית למאבק בטרור, תוך זיהוי האיומים, הצרכים הביטחוניים, והשאלות הייחודיות לסביבה זו. נבחן האם המאפיינים הייחודיים של סביבה זו מחייבים פתרונות משפטיים חדשים, או שמא די בהחלת הפתרונות הקיימים. נרחיב בשלושה היבטים של זירת המידע, המחייבים בחינה מחדש: זירת אבטחה, זירת מעקב, וזירת תעמולה. באשר לכל אחד מאלה, נציג את הבעייתיות המתעוררת, נבחן את ההסדרים המשפטיים הקיימים בארץ ובעולם, ונגדיר קווים מנחים לגיבוש המדיניות המשפטית.

בעמודי המבוא האלה, נציג את הצורך להתייחס לסביבת המידע כאל זירה ביטחונית, נמפה את האיומים הביטחוניים החדשים, ועל-ידי כך, נמקד את הדיון.

מיפוי האיומים

עיצוב מדיניות משפטית ראויה בממשק שבין ביטחון וטכנולוגיה, זכויות אדם ומדיניות כלכלית, אינו אפשרי ללא הכרת האיומים הביטחוניים הנשקפים למדינות וליחידים וצורכי הביטחון הנגזרים כמו גם אמצעי הנגד הקיימים. השיח הביטחוני-אסטרטגי עוסק בדרך כלל בשאלות של בניין הכוח, סדר הכוחות, עוצמה צבאית, כלכלית ומורלית, באיתור נקודות תורפה ויתרונות יחסיים ואבסולוטיים ובניתוח האיומים. ניתן לחלק את האיומים הביטחוניים באופן סכמטי לשניים:

1. **איום קיומי** - איום העלול למוטט מדינה, או לפחות לגרום לפגיעה מהותית באובדן חיי אדם ו/או בנכסים אסטרטגיים ובתשתיות לאומיות בהיקף נרחב. בדרך כלל מדובר באיומים מצידן של מדינות בעלות מערך צבאי מסודר. בארצות הברית מקובל

[1] בכתיבתו של פרק זה נעזרנו רבות בהרצאותיהם של שמעון גרופר, אריק וולף, ד"ר אריאל סובלמן, אריאל פיסצקי, יעל שחר, יוסי שני, ותודתנו נתונה להם. האחריות לתוכן, כמובן, כולה שלנו.

לראות במלחמה גרעינית איום קיומי. בישראל מקובל לראות איום קיומי במלחמה כוללת רחבת היקף, עם מדינות ערב, דוגמת מלחמת יום הכיפורים.

2. **איום המהווה מטרד** – איום העלול לגרום לפגיעה בנפש ובחומר, אך לא במידה המסכנת את עצם קיומה של המדינה. בדרך כלל מדובר בפעולות טרור המבוצעות על-ידי ארגונים שאינם מדינתיים (אם כי חלקם נתמכים על-ידי מדינות) במטרה להשיג מטרות מדיניות.

מובן, כי אין מדובר בדיכוטומיה: בין שני הקצוות ניתן לאתר איומים בדרגות ביניים שונות. פיגועי הטרור ב- 11 בספטמבר 2001 העלו את ההתייחסות לאיומי הטרור במישור הבינלאומי מדרגה של מטרד לדרגה של איום הקרוב לאיום קיומי. הריגת אלפי בני אדם בתוך דקות ספורות, ופגיעה אנושה, כלכלית וסמלית, במרכזי העצבים של הכלכלה הבינלאומית ושל מערכת הביטחון האמריקנית קרובה יותר, לפחות מבחינת האפקט, לפגיעה של פצצה גרעינית, מאשר לפגיעת טרור נקודתית כלשהי. סכנת הטרור הביולוגי והחשש שארגוני טרור ירכשו שליטה בנשק גרעיני, ממחישים את העליה בחשיבותו של האיום הטרוריסטי. מכאן נובעת המסקנה, כי פחתה החשיבות של האבחנות בין איומים מדינתיים לבין איומי טרור שאינו מדינתי, ובין איום קיומי לאיום שהוא בבחינת מטרד. כפי שיוסבר בהמשך, עובדה זו מקבלת משנה תוקף ככל שמדובר בשימוש בכלים טכנולוגיים מתחום מערכות התיקשוב.

לוחמת מידע - Information Warfare

נייר זה מתמקד בשיקולי הביטחון הרלוונטיים למערכות תיקשוב בלבד. מערכות התיקשוב יכולות לשמש זירת מאבק ישירה, או במינוח המקובל – לוחמת מידע - Information Warfare.[2] זהו המושג הרחב ביותר, והוא מכיל גם את הטרור הקיברנטי. דו"ח מבקר המדינה לשנת 2001 מגדיר זאת "כביצוע פעולות, שמטרתן לפגוע במערכות המחשב של היריב (לוחמת מידע התקפית) תוך הגנה על מערכות המחשב שלך (לוחמת מידע הגנתית). סוגי הפגיעה הנפוצים הם: גניבת נתונים ומידע (פגיעה בסודיות), שיבוש והשמדתם (פגיעה באמינות ובזמינות), ופגיעה בהתקנים אלקטרוניים, שיבוש, השבתתם והשמדתם (פגיעה באמינות ובזמינות). אחד התרחישים הבסיסיים בתחום לוחמת מידע התקפית הוא תקיפה של מספר מערכות מחשב חיוניות בעת ובעונה אחת."[3]

---

[2] לדיון ראו טל רפפורט, דודו רשתי, אופיר בן אבי, "סקירה מקוצרת – מלחמת המידע", **אתר טכנולוגיות המידע הממשלתי – סקירה ממשלתית** (2001). http://www.itpolicy.gov.il/topics/netwar.htm#5.

[3] מבקר המדינה, "היערכות המדינה לאבטחת שירותים ממוחשבים", **דו"ח שנתי 52א לשנת 2001**, 275, 276. נמצא ב: http://mevaker.gsites.co.il/serve/showHtml.asp?bookid=145&id=57&frompage=276&contentid=1152&parentcid=1142&direction=1&bctype=1&frombutton=0&startpage=0&sw=800&hw=530.

אמצעי התקיפה כוללים קשת שלמה של תוכנות מזיקות ופוגעניות:[4] וירוסים,[5] תולעים,[6] סוסים טרויאנים,[7] פצצות לוגיות,[8] דלתות ממולכדות,[9] וכן רכיבי חומרה.[10] אמצעים אלה מכוונים כנגד מגוון יעדים. אחת מנקודות התורפה המרכזיות של החברה המערבית בעידן המידע היא מערכות המידע של תשתיות לאומיות: לוגיסטיקה, פיננסים, בריאות, מים, חשמל, תקשורת ועוד. זאת הן בשל התלות הרבה של החברה במערכות המידע, והן בשל היותן מקושרות ביניהן ברשת הפתוחה לציבור הרחב.[11] מערכות התיקשוב הן מטבען מערכות המספקות שירותים. ככל שהשירות חיוני

---

[4] לעיון נוסף בנושא, ראו: Dorothy Denning & Frank Drake, "A Dialog on Hacking and Security" in **Computers, Ethics and Social Values** 120-125 (Deborah G. Johnson & Helen Nissenbaum eds., NJ, 1995).

[5] "וירוס מחשב הוא תוכנית כמו כל תוכנית מחשב אחרת, אבל בניגוד לתוכנית רגילה, וירוס מחשב תוכנן להעתיק את עצמו לתוכניות אחרות. כמו כן, בניגוד לתוכנית רגילה, מטרת הוירוס היא לפגוע בתוכניות שנמצאות על המחשב. כשהמשתמש מפעיל את התוכנית שהודבקה בוירוס, מופעל גם קטע הקוד של תוכנית הוירוס, אשר יכול להכיל פקודות שעלולות לגרום נזק לקבצים במחשב על-ידי שינויים ואפילו מחיקתם." ראו יוחאי שרון, "האתר העברי הראשון בנושא וירוסים" http://www.cs.biu.ac.il/~yohais1/faq.html#1.

[6] תולעת היא תוכנה עצמאית שמשכפלת עצמה ממחשב למחשב ברחבי הרשת ולעיתים גורמת לעומס רב על המחשבים בהן היא עוברת, אולם לרוב אינה מסוגלת להזיק באופן חמור כמו הווירוסים. בניגוד לווירוסים, אין מדובר על קטע קוד שנצמד ומשנה קבצים קיימים אלא על תוכניות בעלת גוון עצמאי. המודל הראשון של תולעת הוצג כניסוי בתחילת שנת 1988 וגרם לסערה בעולם המיחשוב. גם אם התולעת, כאמור, אינה מיועדת לגרום לנזק בפני עצמה, העובדה שהיא מנצלת את משאבי המחשב, בסופו של דבר גורמת להאטת פעילותו, דבר שבמקרים רבים עשויים לפגוע במשתמש. לעיון נוסף, ראו: Peter J. Denning, "The Internet Worm", **American Scientist** 126-128 (March-April 1989). המאמר מופיע גם בספרו של דנינג, **Computers Under Attack** 193-200 (New York, 1990).

[7] *סוס טרויאני* אינו וירוס, למרות שיש לו תכונות הדומות לווירוס. סוס טרויאני הינו תוכנית שתפקידה להתיישב במחשב שלנו תוך הסתרת קיומה ולהפעיל או לאפשר הפעלה מרחוק של פעולות מסוימות במחשב. הסוסים הטרויאניים בהם מדובר מוחדרים למחשב באופן סמוי דרך קובץ חוקי לכאורה המגיע אלינו דרך האינטרנט, דואר אלקטרוני, דיסקט וכדומה, ומשתילים למעשה סוכן הנקרא "סרבר". הסוכן מתקין את עצמו בהתקנה סמויה ואינו מגלה את נוכחותו ובעצם אינו עושה דבר בפני עצמו. כשאנו מתחברים לאינטרנט, המחשב שלנו "מותקף" בפניות מכוונות או אקראיות של תוכנות פלישה וחדירה המופעלות על-ידי טיפוסים מפוקפקים. נסיונות החדירה נעשים דרך כניסות התקשורת לרשת האינטרנט. כשתוכנה כזו מגלה את הסוכן שלה (הסרבר) מותקן במחשב המטרה, מתאפשר לחודר החצוף להעביר אלינו הודעות מפתיעות במקרה התמים ולפרמט לנו את הדיסק הקשיח במקרה הרע. ראו: אמיר ענבי, אתר "פינת העזרים של אמיר" http://www.anavy.net/util36.html.

[8] הרעיון העומד מאחורי רוב הפצצות הלוגיות הינו שימוש לרעה בפקודה "Fork". פקודה זו מאפשרת ליישום לפתוח עותק נוסף של עצמו ולהריץ אותו במקביל. על-ידי הרצה משורשרת של אלפי פקודות כאלה, נוצר פקק בטבלת היישומים של המחשב, ובסופו של דבר המחשב ייתקע. על טבלת היישומים והשימושים המקוריים שיועדו לפקודה Fork ראו: Maurice J. Bach, **The Design of the Unix Operating System**, 192-200 (New-Jersey, 1990).

[9] דלתות ממולכדות (Back Doors/Trap Doors) הן פירצה במערכת מחשבים שמפתחיה, הטכנאים שלה או מנהל המערכת השאירו במודע לעצמם. לעיתים אפשר שמדובר על-פירצה בשיטת ההצפנה. דרך הדלת הממולכדת ניתן להיכנס למערכת, גם ללא שם וסיסמא.

[10] כמו למשל Chipping, מושג המתייחס להחדרת קוד הרסני על גבי שבבים במעבד, על-ידי היצרנים. הקוד יופעל בהתקיים תנאים מסוימים, למשל אם יתקבל סיגנל מסויים על תדר מסויים.

[11] על פגיעותה של תשתית התקשורת, ראו: G. Smith, "An Electronic Pearl Harbor? Not Likely", http//205/130/85/236/issues/15.1/smith.htm. על יעדים פוטנציאליים להתקפות, שיתוק אתרים, תולעים, פגיעה בנתבים (Routers), פגיעה בתשתיות ופגיעות משולבות, ראו: Institute for Security Technology Studies, Darthmouth College, September 22, 2001; M. A. Vatis, "Cyber Attacks During the War on Terrorism: A Predictive Analyis". על הסיכונים לתשתיות קריטיות – ראו דו"ח ועדת הסנאט: Critical Infrastructure Protection, General Accounting Office, Special Committee on the Year 2000 Technology Problem (U.S. Senate, October 1999). על פגיעות שרתים באינטרנט, ראו: Elinor Mills Abrey, "Key Internet SERVERS Vulnerable to Attack - Experts" (14.11.01), נמצא ב: http://www.info-sec.com/internet/01/internet_111401d_j.shtml.

יותר למשק המדינה ולניהולה התקין, הוא נחשב ל"תשתית קריטית" בעלת משמעות אסטרטגית. מן הערך האסטרטגי של תשתיות קריטיות נגזר הערך האסטרטגי שבתקיפתן ובפגיעה בהן.

ההתמודדות עם איומים על מערכות חיוניות עשויה להיות במספר מישורים: האחד, הוא מישור הפעולה המעשית: בארצות הברית קיימות מספר רשויות העוסקות בהגנת תשתיות חיוניות בכלל, ובתחום התיקשוב בפרט. ביניהן ניתן למצוא את ה- NIPC - המרכז להגנת תשתיות לאומיות,[12] ו- CIAO המשרד לאבטחת תשתיות קריטיות.[13] השיח בנושא זה בארצות הברית הוא פתוח, ומתקיים דיאלוג בין המערכות הממשלתיות למערכות האזרחיות. כך ניתן למצוא אתרים וארגונים המבקרים בחריפות את פעולות הממשל בנושא, הן מנקודת המבט של הפגיעה בזכויות והן מנקודת המבט של יעילות הפעולות הללו.[14] השיח בישראל דל ביותר, ולמעשה לא קיים. דו"ח מבקר המדינה הוא היוצא מן הכלל המעיד על הכלל, ואף הוא מגלה טפח ומסתיר טפחיים. מבקר המדינה הצביע על מורכבות לוחמת המידע ההגנתית, ועל הצורך בגוף שירכז את נושא אבטחת המידע בשירותים הממוחשבים השונים במדינה, על בסיס ראייה כלל-מערכתית.[15] מכל מקום ניתן ללמוד ממנו, שמדינת ישראל אינה ערוכה כיאות לאיומי לוחמת המידע.

אחד מאמצעי ההגנה היעילים והנפוצים הוא שימוש בתוכנות הצפנה. במישור המשפטי, מחייב האיום של לוחמת המידע, חשיבה מחדש, באשר לרגולציה של מוצרי הצפנה. אלה משמשים את המדינה לאבטחת המידע שברשותה, אך עלולים לשמש גם גורמים עויינים בהשגת מטרותיהם שלהם. סוגיה זאת מחדדת את השאלות שברקע הדיון כולו: האיזון שבין צורכי הביטחון לזכויות אדם, ההתערבות בשוק – והמחיר שהיא עלולה לגבות, ובעיקר, תחולתם של מושגים משפטיים מסורתיים בסביבה הדיגיטלית. בנושא זה נדון בפרק 2.

זירת מעקב

לצד האפשרות של גורמים עויינים להשתמש בסביבה הדיגיטלית כנשק (שימוש ישיר) משמשת הרשת אמצעי תקשורת של הגורמים העויינים, בינם לבין עצמם, וכן שדה לאיסוף מידע (שימוש עקיף).[16] הקושי המרכזי הוא שהרשת משמשת לא רק את הטרוריסט: דואר אלקטוני שנשלח על-ידי טרוריסט לחברו אינו נושא כותרת "זהירות! דואר טרור". משום כך, ביצוע פעולות מעקב

---

12 http://www.nipc.gov .

13 http://www.ciao.gov.

14 Richard Forno, “A Failure To Communicate” (NIPC, 2000), http://www.infowarrior.org/articles/2000-06.html.

15 לשיטת מבקר המדינה, לוחמת מידע הגנתית בנויה ממספר רבדים שונים: הרתעה, התרעה, אבטחה, איתור תקיפה עתידית ומניעתה, תגובה במישור המותקף ותגובה במישור הלאומי (הכנת המדינה להתמודדות ללא שירותים ממוחשבים זמינים במתכונת המקובלת, ותגובת המדינה על לוחמת המידע ההתקפית כלפי חוץ). מהגדרה זו לומד המבקר על מספר שאלות יסוד שיש לתת עליהן מענה: על מי להגן ועל מה, מפני מי ומפני מה להגן, מי יגן, איך להגן ו"כמה", איך להגיב. נוכח התלות ההדדית בין מערכות השירותים, אין די בהיערכותו של כל גוף באופן עצמאי, כפי שנעשה עד עתה, אלא יש צורך בבחינה כלל מערכתית של ההיערכות. ראו: http://www.mevaker.gov.il/docs/52a/rtf/1e.rtf (נבדק לאחרונה בפברואר 2002).

16 ראו: Michael Wilson, “Considering the Net as an Intelligence Tool”, נמצא ב: http://www.7pillars.com/papers/IntelNet.html.

אחרי פעילות הטרוריסטים על מנת לסכלה באיבה - עלול לגרום לפגיעה בפרטיותם של אחרים, ובעקיפין, בחופש הביטוי.

קושי נוסף הוא עירפול מושגי וטישטוש האבחנה שבין CyberCrime לבין CyberTerrorism.[17] האבחנה בין המושגים מבוססת על מטרותיו של הפושע/טרוריסט:[18] המונח הראשון מתייחס בעיקר לפשיעה ״רגילה״, ואילו השני לפעולות שנועדו לפגוע במרקם החיים הדמוקרטיים. מובן שאין מדובר בדיכוטומיה. ניתן לתאר קשת של מצבים: בקצה האחד נסווג ילד ״המשתעשע״ להנאתו ברשת, ותוך כדי כך גורם לנזקים רבים (וירטואליים, פינאנסיים, או אפילו פיזיים), ובקצה השני הטרוריסט הנעזר ברשת כדי להשיג פגיעות בנפש וברכוש, לקידום מטרותיו הפוליטיות. ובין הקצוות – אינספור מצבים אחרים.[19]

יש לציין, כי העדר מינוח אחיד אינו בעיה סמנטית בלבד: ההתייחסות לטרור, בעיקר מצד גורמים ״ביטחוניים״ מעניקה לרשויות חופש פעולה גדול יותר במונחים של נכונות הציבור ובתי המשפט לקבל פגיעה בזכויות הפרט, מאשר התייחסות לפשיעה ״רגילה״, גם אם הן השיטות והן אמצעי הנגד זהים בשני המקרים.[20] ובניסוח המשפטי, לאבחנה עשויה להיות השלכה על טיב האיזון החוקתי המופעל.

התמונה הופכת למורכבת עוד יותר, כאשר מוסיפים לה את זווית מבטן של הרשויות: בהקשר זה יש להבחין בין **אמצעים הגנתיים** ל**אמצעים התקפיים**. גם כאן מדובר ברצף ולא בדיכוטומיה. האמצעים ההגנתיים מחולקים סכמטית לסיכול ומניעה מוקדמת של פגיעות, בעיקר על-ידי מניעת חשיפת מידע (״ביטחון שדה״) והשגת מודיעין, ולהתגוננות מהפגיעות באמצעות אבטחת מידע. האמצעים ההתקפיים הם איתור הפוגעים ותפיסתם (אכיפה) או פגיעה ישירה בהם, וכן שימוש במערכות התיקשוב כנשק התקפי.

הפרק השלישי עוסק בשאלת המגבלות החלות על השימוש באמצעי מעקב בסביבה הדיגיטלית לצורכי ביטחון.

זירת תעמולה

האיומים הביטחוניים הקשורים בסביבה הדיגיטלית ניתנים למיון גם על-פי סוג הפגיעה: פיזית או שאיננה פיזית. במסגרת הסוג האחרון, ניתן לכלול גם את המונח ״SoftWar״, המייחס בעיקר להפצת מידע כוזב למטרות תעמולה, דמורליזציה וכיוצא בזה. הקשיים המשפטיים שמתעוררים סביב סוגיות אלה של הסתה, המרדה, הפצת מידע שיקרי (disinformation), תעמולה עויינת, ביטוי שנאה (hate speech) זכו לדיון מפורט מעמיק בסביבה הטרום-דיגיטלית. במסגרת זאת

---

[17] ראו: Ariel T. Sobelman, “No Friends - Everyone Is an Enemy in Cyberspace”, נמצא ב: http://www.oas.org/juridico/english/sobelman.htm.

[18] ראו הדיון בכנס שפיים (דיון בהשתתפות ד״ר יריב צפתי, ד״ר יובל קרניאל, ד״ר מיכאל בירנהק).

[19] על רקע זה מעניין לבחון את האמנה הבינלאומית שיזם האיחוד האירופי, למלחמה בפשיעה - Cyber-Crime On Convention. ראו: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[20] Richard Forno, “You Say Hacker, The Feds Say Terrorist”, **Security Focus Online** (Nov. 2001), נמצא ב: http://online.securityfocus.com/columnists/38.

נקבעה, לפחות במשפט הישראלי, שורת איזונים חוקתיים המנחים את הרשות המבצעת, כמו גם את בתי המשפט. כך למשל המתח שבין צורכי הביטחון לבין חופש העיתונות, האינטרס הציבורי לשמור על הסדר הציבורי מול חופש ההפגנה, וגבולותיו של ביטוי פוליטי הצורם לאוזני הרוב.

ברמה העקרונית, השאלות המתעוררות בסביבה הדיגיטלית דומות. אלא, שיישומם של האיזונים הקיימים בסביבה הדיגיטלית, ועיצוב כללים משפטיים פרטניים, מחייב דיון במאפיינים הטכנולוגיים הייחודיים של המדיום. בכך יעסוק הפרק הרביעי. בעיקר נתמקד שם בשאלת אחריותם של ספקי שירות.

II. סביבת המידע כזירה מאובטחת: ביטחון, שוק חופשי והצפנה[21]

א. הצגת הבעיה

פרק זה דן בשאלת ההסדרה (רגולציה) של מוצרי הצפנה. תוכנות הצפנה מאפשרות הגנה חזקה למדי על מידע המאוחסן ברשתות דיגיטליות, ומשום כך רלבנטיות לצורכי ביטחון בשני היבטים, אשר במידה רבה הם הפוכים זה לזה: צורך אחד הוא הרצון להגן על המידע הנמצא בידי מערכת הביטחון, כמו גם מערכות אזרחיות חיוניות דוגמת בתי חולים, שירותי תחבורה, אספקת מזון ורשתות תקשורת (להלן: *צורכי אבטחה*).[22] צורך שני הוא לשמור על היכולת הטכנולוגית להשיג מידע בעל ערך ביטחוני הנמצא בידי האויב (להלן: *צורכי מעקב*). צורכי האבטחה מושכים לכיוון עידוד שוק התוכנה ללא התערבות מדינתית, ואילו צורכי המעקב מושכים לכיוון של הטלת הגבלות על שוק התוכנה. בנוסף, עצם ההתערבות בשוק יוצרת קשיים שונים – שינוי מערך התמריצים בשוק התוכנה בקשר למחקר ופיתוח, פגיעה בחופש העיסוק ובזכות הקניין, כמו גם נגיסה ביכולתם של אזרחים לתקשר בביטחון ובפרטיות. משום כך קיימת גם פגיעה (עקיפה) בחופש הביטוי.

הנסיון במספר מדינות, כמו גם בישראל, מעלה שבעבר ננקטה הסדרה נוקשה למדי, אולם במהלך השנים הומרה מדיניות ההגבלה במדיניות פיקוח מתונה יותר. פרק זה בוחן את סוגיית ההצפנה, לאור השיקולים הכלליים שנמנו זה עתה ולאור המגמה של ליברליזציה: זהו מקום שבו הטכנולוגיה מעוררת קשיים ביטחוניים ויוצרת אפשרויות טכנולוגיות מעניינות, בו זמנית.

הדיון מתחיל בסקירת הטכנולוגיה, תוך הדגשת מגבלותיה "הטבעיות". בהמשך יבחנו הצרכים הביטחוניים והמסגרת המשפטית הקיימת. נסקור את סוגי ההסדרים שננקטו בעבר בארצות הברית ובישראל כמו גם הסדרים בינלאומיים מרכזיים, ונעמוד על ההתפתחות שחלה במדיניות ההסדרה. לאחר מכן, נעמוד על ההשלכות של מדיניות ההצפנה, והגורמים שאותם יש להביא בחשבון בעת עיצוב המדיניות ובעת הפעלתה. אלה הם שיקולים מסוגים שונים: חלקם נוגעים למשמעות הכלכלית של ההסדרה: שאלת עצם ההתערבות בשוק, ההשפעה על מערכת התמריצים של יצרני התוכנה וההשפעה על המסחר האלקטרוני. סוג שיקולים אחר נוגע לזכויות אדם: חופש העיסוק, זכות הקניין, שאלת הפרטיות וחופש הביטוי.

לטעמנו, מדיניות נבונה צריכה לשאוף למלא את צורכי הביטחון משני הסוגים (אבטחה ומעקב), תוך נסיון להתערבות מינימלית בשוק החופשי ונסיון למזער את הפגיעה בזכויות אדם. בהתאם, נצביע על מספר מודלים משפטיים אפשריים להתמודדות עם הסוגייה, אשר עשויים להוות בסיס לגיבושה של מדיניות נבונה יותר בתחום זה.

---

[21] בכתיבת פרק זה נעזרנו רבות בהרצאותיהם ובהערותיהם של ד"ר גדי אהרוני, עו"ד מתי ברזם, פרופ' מרטין גולומביק, יורם כהן, ד"ר אריאל סובלמן, פרופ' איל קושילביץ, פרופ' הוגו קרבצ'יק, עו"ד רם רביב, עו"ד חיים רביה, יוסי שני, ותודתנו נתונה להם. האחריות לתוכן היא, כמובן, שלנו בלבד.

[22] ראו למשל את **חוק הבזק**, התשמ"ב - 1982, הקובע בסעיף 13(ב)(3), כי השר רשאי לתת הוראה לבעל רשיון, בין השאר, בעניין קיום הוראות שירות הביטחון הכללי או משטרת ישראל, בעניין סיווג ביטחוני של נושאי משרה מסוימים החשופים למידע מסווג, או של בעלי תפקידים מסוימים, או בעניין שמירת סוד, אבטחת מידע או אבטחת ציוד ומיתקנים אצל בעל הרשיון.

ב. מהי הצפנה: הבסיס הטכנולוגי

1. מבוא

להצפנה ישנה היסטוריה ארוכה ומעניינת. תורת ההצפנה ידועה במונח היווני קריפטוגרפיה ("כתיבה סמויה"). השימוש בהצפנה מאפשר תקשורת חסויה בין שני צדדים באמצעות שינוי - מניפולציה כלשהי - של המידע המועבר. הצדדים צריכים לתאם ביניהם את סוג השינוי ופרטיו, על-מנת שהעברת המסרים תצלח.[23]

במערכות ביטחון מועברות הודעות מילוליות למיניהן - הוראות קרב, מידע מודיעיני שמושג מהיריב, ומסרים אחרים אשר ניתן לבטאם בצורת טקסט. באופן מסורתי הועברו הטקסטים הללו לפקידי הצפנה שעמלו על הצפנתם והעברתם. הטקסט המקורי הומר באופן ידני על-ידי פונקציה כלשהי – מפתח. התוצאה המוצפנת היתה מועברת, בדרך כלל באמצעות גלי אלחוט או באמצעות שליח. הנחת העבודה היתה שהיריב יכול להניח את ידו על הגרסה המדויקת של הטקסט המוצפן, אך כל עוד לא היה המפתח בידו, היה הטקסט המוצפן חסין, במידה רבה, מפיענות.

פיענוח המסרים יכול להיעשות תוך מידה משתנה של אקטיביות מצד היריב - המאזין. כאשר כל שהיריב יכול לעשות הוא להאזין "בחיי" לערוץ התקשורת, מדובר על **האזנה פסיבית**. כאשר הוא יכול גם להקליט מסרים ולשחזרם מאוחר יותר, מדובר על **האזנה אקטיבית**. המידה האקטיבית ביותר היא כאשר ליריב ישנה האפשרות להחדיר מסרים משלו בתקשורת המואזנת, או לשנות מסרים עוד לפני שהגיעו לצד השני. היתרון הביטחוני מאפשרות כזאת ברור.

האלמנט הסודי ביותר הוא כמובן המפתח – והאורך שלו הוא הגורם הקריטי כאן. אם נקביל את המפתח המשמש בהצפנה למנעול קומבינציה פשוט, אזי כדי לפותחו יש לבחור מספרים בסדר מסוים. אם המפתח הוא באורך של שתי ספרות – יש מאה אפשרויות. שלוש ספרות – אלף אפשרויות. שש ספרות – מיליון אפשרויות. דרך הפיצוח תהיה לנסות ולנחש את הצירוף שנבחר, בין באופן רנדומלי ובין באופן שיטתי ומסודר, דרך הנקראת Brute-Force Attack.[24] ככל שהמפתח ארוך יותר, כך יגדל עומס העבודה המוטל על המפצח – ולכן איכות האבטחה תהיה טובה יותר. נשים לב שהעומס גדל בטור אקספוננציאלי (מעריכי) לאורך המפתח, ולכן מפתח של 64-256 סיביות תיחשבנה לסטנדרט מספק של אבטחה, למרבית הצרכים. יש להעיר כי, אות אחת של טקסט לרוב מגולמת בשמונה סיביות, לפי הקוד הותיק והנפוץ, קוד אסקי (ASCII), או 16

---

[23] הסקירה מתבססת על המקורות הבאים: Andrew Tanenbaum, **Computer Networks** 577-621 (3rd ed., 1996); Scott Oaks, **Java Security** 1-16, 289-328 (CA, 1998); Jonathan Knudsen, **Java Cryptography** 1-27 (1998). לאורך השנים היה לשימוש בהצפנה תפקיד מכריע בשדה הקרב. לדיון, ראו: David Kahn, **The Codebreakers**. השוואה בין שלוש מהדורותיו של הספר ממחישה את התפתחות תורת ההצפנה לאורך השנים מנקודות מבט טכניות ותיאורטיות. ראו: Kahn, **The Codebreakers: The Story of Secret Writing** (Macmillan: New York, 1967); (New American Library, 1973); (New-York: Scribner, 1996).

[24] ראו: Bruce Schneier, **Applied Cryptography: Protocols, Algorithms, and Source Code** 8, 151-154 (2nd ed., New-York 1996).

ביט עבור קוד Unicode.[25] הצפנת הטקסטים מאפשרת טיפול אחיד לאותיות ולסימנים, ולכן כשאנו נציין "אות" הכוונה תהיה לאות או לסימן.

2. עקרון ההצפנה הבסיסי: המרת אותיות באותיות

אחד מיסודות ההצפנה הוא עקרון ההחלפה: כל אות מוחלפת באות אחרת. השיטה פותחה על-ידי יוליוס קיסר במלחמתו בבני העיר כרטא. המפתח כאן היה המחרוזת בת 26 האותיות המיוחסת לאלפבית השלם. יש 26 עצרת אפשרויות למפתח (מספר השווה בקירוב ל-1 עם 26 אפסים). אם מחשב שוקד על תוצאה אחת בכל מיקרו-שניה, ומנסה לראות אם היא הצירוף שיפתח את המנעול (כלומר מבצע Brute-force Attack), יימשך פיצוח הקוד, בממוצע, 10 בחזקת 13 שנים.

למרות זאת, שיטה זו נחשבת פשוטה יחסית לשבירה, זאת בזכות תכונות סטטיסטיות של אותיות: שכיחותן של אותיות מסוימות, כמו – e, t, o, a, n, i, שכיחותם של צמדי אותיות, כמו למשל th, in, er, re, an, וכדומה. לכן אפשר לייחס את האות הפופולרית ביותר בטקסט המוצפן ל- e, ואת השניה בתפוצתה ל- t, וכן הלאה, ואז לנסות לפצח את המפתח לפי צמדים ושלישיות.

3. ההצפנה הסימטרית

למרות מגרעותיה, שיטת ההחלפה היוותה בסיס לשיטת ההצפנה הדיגיטלית החשובה הראשונה, ה- DES (Data Encryption Standard) שפותחה במקור תחת השם "Lucifer" על-ידי חברת IBM בתחילת שנות השבעים,[26] ואומצה על-ידי הממשל האמריקני בשנת 1977. הרעיון היה להפוך מקטעים של 64 ביט של טקסט מקור למקטעים של 64 ביט של טקסט מוצפן, באמצעות מספר שלבים מתמטיים עוקבים שבנויים על החלפת האותיות לפי מפתח באורך של 56 ביט.

כאשר מקטע טקסט מסוים חוזר על עצמו פעמיים במהלך ההודעה, יתקבל פעמיים בדיוק אותו מקטע מוצפן. למשל, אם המילה בת ה- 64 ביט "Example1" תופיע פעמיים בטקסט, הקוד המוצפן שלה יהיה זהה בשני המקרים. עקביות זו היא בדיוק התכונה שניתן לנצלה כדי לפצח את ה- DES, בדומה לפיצוח סטטיסטיקת האותיות.

שיטת ה-DES מוצאה כאמור במערכת "Lucifer". "Lucifer" פעלה על מפתחות באורך של 128 ביט, והסוכנות האמריקנית לביטחון לאומי (National Security Agency - NSA-ה) הורידה את המפתח לאורך של 56 ביט[27] ודרשה לשמור את האלגוריתם המדויק בסוד, כדי שהיא עצמה (הסוכנות) תוכל לפענח מסרים שהוצפנו בשיטה הזו, אך שום מוסד אחר (עם משאבי המחשוב המוגבלים של אז) לא יוכל לעשות זאת.[28] שיאה של מדיניות זו היה ביטול של כנסי קריפטוגרפיה

---

[25] בסביבות מחשוב מתקדמות, מופעלת שיטת unicode, בה כל אות מקודדת ב- 16 סיביות (כך שישנן 65536 אותיות אפשריות). בשיטה כזו ניתן לקדד סימנים משפות שונות בשפה אוניברסלית אחת. ראו: Ken Arnold, James Gosling, David Holmes, **The Java Programming Language** 8, 138, 277 (3rd ed. 2000).

[26] לפרטים הטכניים של מערכת לוציפר, ראו: J.L. Smith, "The Design of Lucifer, A Cryptographic Device for Data Communications", **IBM Research Report** RC3326 (1971).

[27] לסוכנות ה-NSA היו יחסי גומלין עם עולם ההצפנה. במקרים רבים, במקום שירשם פטנט על המצאה היא הופקעה לטובת סוכנות זו. על מקרים כאלה ואחרים, ראו בספרו של Kahn, לעיל, הערה 24 , עמ' 672-736.

[28] השיטה נרשמה כפטנט: U.S. Patent #3,962,539 (8 June 1976).

שערך IEEE (אגוד המהנדסים האמריקני) באמצעות צווים של ה-NSA, איומים ומעקבים, כאשר היה חשש שסודות כלשהם יתגלו.[29]

בשנת 1977, פיתחו שני חוקרים מאוניברסיטת סטנפורד, דיפי והלמן, מודל למכונה שתוכל לשבור את DES, והעריכו שניתן לבנות אותה ב- 20 מיליון דולר.[30] היום מכונה כזו תעלה לכל היותר מיליון דולר. מכונה כזו תשווה קטע של טקסט רגיל לקטע של טקסט מוצפן ו"תריץ" 2 בחזקת 56 אפשרויות עד שתמצא את המפתח.

בתחילת שנות התשעים פיתחו שני חוקרים שוויצרים, לאי ומייסי, שיטת הצפנה הדומה ל-DES אולם פועלת על מפתח באורך של 128 ביט, ושמה IDEA – International Data Encryption Algorithm.[31] ה-IDEA הינו כיום פטנט רשום של חברת Ascom System AG. עד כה, נחשבת שיטת ה-IDEA חסינה לפיצוח. שיטה דומה נוספת נקראת RC2/RC4. השיטות הללו פועלות כולן על עקרונות דומים, ומשמשות כסטנדרטים נפוצים בעולם. כולן מכונות "הצפנות סימטריות", מאחר ששני הצדדים משתמשים בדיוק באותו המפתח; הן מכונות גם "הצפנות קונבנציונליות".

<u>חולשת ההצפנה הסימטרית</u>

החוליה החלשה בכל השיטות אותן הזכרנו עד כה, היא זו: לא חשוב עד כמה השיטה טובה – אם היריב יוכל לגנוב את המפתח – היא תהיה חסרת תועלת. מאחר שמפתח ההצפנה ומפתח הפיענוח הם אותו מפתח, מתעוררת בעיה – מצד אחד אנחנו מבקשים להגן על המפתח מפני גניבה, אולם מצד שני צריך להעבירו לכל הצדדים ולכן אי אפשר להחביאו לגמרי. מאחר שרוב ההצפנות באינטרנט היום פועלות עדיין בשיטות הללו, שני הצדדים צריכים לתאם לפני ההתקשרות מהי שיטת ההצפנה ומהו המפתח הסימטרי שבחרו. ברור כי החוליה הראשונית, של העברת המפתח, אינה יכולה להיות מאובטחת – שכן עדיין לא סוכם המפתח.

<u>4. ההצפנה א-סימטרית: מפתח פומבי ומפתח פרטי</u>

כאן נכנסת לתמונה שיטת ה-RSA, הנקראת על שם מפתחיה Rivest, Shamir, Adleman. השיטה אינה פועלת על עקרון של הצפנה סימטרית, אלא על עקרון המפתח הפומבי, עקרון עדכני למדי במושגים של תורת ההצפנה (מדובר על כשלושים השנים האחרונות). בשיטה זו, לכל משתמש יש שני מפתחות, **מפתח פומבי** – המשמש את "שאר העולם" לשלוח למשתמש הודעות, **ומפתח פרטי** – שבו הוא משתמש כדי לפענח את ההודעות שנשלחו אליו. תוכנת ההצפנה הביתית

[29] ראו: S. Landau, "Zero-Knowledge and the Department of Defense", 35 **Notices of the American Mathematical Society** 5-12 (1988).

[30] התיאור המדויק של המכונה נמצא ב- W. Diffie & M.E. Hellman, "Exhaustive Cryptanalysis of the National Bureau of Standards Data Encryption Standard", 10 **IEEE Computer Magazine** 74-84 (June 1977).

[31] השיטה הוצגה לראשונה ב: Xuejia Lai & James Massey, "A Proposal for a New Block Encryption Standard", **Advances in Cryptology – Eurocrypt '90 Proceedings** 389-404 (1991).

הפופולארית PGP (Pretty Good Privacy)[32] מיישמת שיטה זו בצורה קלה לשימוש. ה-RSA משמש להעברת המפתחות הראשונית לאותו ה-Session, ואחר-כך משתמשים ב-DES או ב-IDEA, שהן שיטות הצפנה מהירות בהרבה.

ניתוח שיטת ה- RSA

כעת ננסה להמחיש את היסוד המתימטי שבבסיס השיטה.[33] לשם כך חשוב לעמוד על מושגי יסוד פשוטים:

בעיה חישובית – בעיה המקבלת קלט מסוים ומחשבת פלט מסוים (תשובה לבעיה).

ישנם שני סוגים של בעיות כאלה:

בעיה **פתירה** *(Tractable)* אם ידועה דרך לפתור אותה, כלומר קיימת בשבילה שיטה קבועה, *אלגוריתם (Algorithm)* המסוגל להתמודד עם כל הצירופים שהבעיה יכולה להכיל, ולפתור אותה בזמן שניתן לצפות מראש (קצר יחסית).

בעיה **אינה פתירה** *(Intractable)* אם לא ידועה כל דרך לפתור אותה באופן כללי, *בזמן הניתן לשליטה*. בעיות שאינן פתירות, כך נראה, ניתנות לניצול ליצירת מפתחות בטוחים, להעברת מידע בערוצים ציבוריים של תקשורת, כפי שקורה ב-RSA.

הרעיון הכללי הוא, שאלה השולחים את המסרים אחד לשני יחזיקו במידע נוסף שיעזור להם לפתור את *הבעיה הבלתי פתירה* (הספציפית) בצורה מיידית, ואילו זה שינסה לפרוץ את המידע המוצפן (ללא המידע הנוסף) ייתקל בבעיה שהדרך היחידה לפתור אותה היא להפעיל מחשבים רבי עוצמה במשך מאות מיליוני שנים (דבר שכמובן אינו אפשרי מבחינה מעשית). כלומר, עבור הצדדים לתקשורת, הבעיה פתירה, ועבור מי שאיננו שותף לה, היא אינה פתירה.

בשיטת RSA, שהוצגה לראשונה בכתב עת מדעי בארצות הברית בשנת 1977,[34] ישנם שלושה מרכזי מידע: **שולח** ההודעה, **מקבל** ההודעה **ונחלת הכלל** (למשל: מדור המודעות בעיתון או אזור לא מוצפן באינטרנט). נמחיש כאן את השיטה כפי שהיא פועלת במציאות, ואשר הייתה מוגנת בפטנט, שפג בספטמבר 2000.[35]

---

[32] התוכנה פותחה על-ידי Phillip Zimmerman. ספר הדרכה פרקטי המתאר כיצד להפיק את המיטב ממנה, הינו: Simson L. Garfinkel, **PGP: Pretty Good Privacy** (1995). הספר מתאר גם את ההיסטוריה של התוכנה ואת תלאותיו של מפתחה (pp. 85-116).

[33] לעיון נוסף, ראו: Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, **Introduction to Algorithms** 831-852 (1990).

[34] Ronald L. Rivest, Adi Shamir & Leonard M. Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystems", 21(2) **Comm. of the ACM** 120-126 (1978).

[35] U.S. Patent #4,405,829.

להלן פריטי המידע המעורבים בתהליך:

p, q = שני מספרים ראשוניים, שנבחרו על-ידי **המקבל** ולא נמסרו לאף אחד אחר (גם לא לשולח). המקבל יכול לבחור אותם באמצעות מחולל מספרים ראשוניים אקראי (מאחר שהבדיקה אם מספר הוא ראשוני, היא בעיה פתירה,[36] לעומת מציאת הגורמים של מספר, שאינה פתירה).[37]

n = p*q – מושם על-ידי המקבל **בנחלת הכלל.**

t = (p-1)*(q-1), מחושב על-ידי **המקבל** ולא נמסר לאף אחד (גם לא לשולח). הוא ירכיב אחר-כך את המפתח הפרטי.

E – מספר כלשהו שהמחלק המשותף הגדול ביותר שלו ושל t הוא 1 (במילים אחרות: הוא זר לחלוטין ל-t). מספר זה מחושב בקלות על-ידי **המקבל** (כי t ידוע לו) וגם הוא מושם בנחלת הכלל. כלומר, n ו-E הם זוג המפתחות הפומביים.

M – ההודעה ש**השולח** מעוניין לשלוח. שוב, נוח לחשוב על הודעה כמחרוזת של ביטים בינאריים (0, 1). אם נתייחס אליה כמספר בינארי אחד, ערכו העשרוני יהיה M. (השולח צריך לוודא מראש ש-M קטן מ-n).

D - בנוסף לכל אלה, ישנו פריט נוסף של מידע המחושב על-ידי **המקבל**, והוא ההופכי הכפלי של E, מודולו t, דהיינו: D*E=1 (mod t). מאחר ש-t ידוע למקבל הוא יכול לחשב את D בקלות. פעולת ה-mod (מודולו) היא השארית המתקבלת לאחר חלוקה ב-t. המקבל שומר את D בסוד ולא מוסרו לאף אחד.

סיכום ביניים: המקבל יודע את p, q, t, D, השולח יודע את M, וכולם יודעים את n ו-E.

בפרט - D הוא המפתח הפרטי של המקבל (אשר ישמש אותו לפיענוח ההודעה), E ו-n הם זוג המפתחות הפומביים שלו (שישמשו את השולח כדי להצפין את ההודעה עבורו).

לשליחת הודעה: **השולח** לוקח את ההודעה M, מתבונן במפתחות הפומביים n ו-E, מחשב ושולח את המסר המוצפן C בתקשורת הגלויה. את C נחשב מתמטית כך: C=M^E (mod n), (^ = חזקה).

קל לראות, שלשולח אין צפנים משלו, ואין לו למעשה שום דבר סודי חוץ מההודעה עצמה M; פעולת ההצפנה מתבצעת מיידית.

---

[36] ישנן שיטות קלות ומהירות לחולל מספרים ראשוניים גדולים. כדי לענות לשאלה האם מספר הוא ראשוני, צריך לענות ב"כן" או "לא". סדרת בדיקות שפותחה על-ידי Michael Rabin ו-Gary Miller (שיטת Rabin-Miller), עושה זאת בזמן קצר מאוד. ראו: M.O. Rabin, "Probabilistic Algorithm for Testing Primality", 12(1) **Journal of Number Theory**, February 128-138 (1980). מחולל המספרים הראשוניים, ממציא מספר ארוך, ומוודא שהוא ראשוני, תוך שימוש בשיטה זו. אם הוא אינו כזה, הוא ממציא מספר נוסף, וכך הלאה.

[37] איתור הגורמים של n מורכב בהרבה מבדיקת הראשוניות של מספר. זו הבעיה עליה יש לענות כדי לפצח את שיטת ה-RSA, וכדי לענות עליה, צריך להריץ מספרים עד השורש של n ולנסות לחלק את n בכל אחד מהמספרים הללו. שיטות מתקדמות יותר שפותחו, למשל על-ידי Pollard, לא שיפרו משמעותית את זמן הביצוע מהשיטה שתוארה כאן. ראו: J.M. Pollard, "A Monte Carlo Method for Factorization", 15 **BIT** 97-105 (1975). אם n הוא מספר באורך של אלף ספרות, הרצה שכזו, על המחשב החזק ביותר בעולם, תיקח הרבה יותר משנות היקום כולו (לשם השוואה, שנות היקום, בשניות, נאמדות ב- 2 בחזקת 61).

כעת לפיענוח הודעה: המקבל קיבל לידיו את C ויכול לחלץ את ההודעה המקורית M על-ידי פעולה מיידית, כל עוד שיש לו את המפתח הפרטי שלו D: M=C^D (mod n).

המחשה

המקבל בוחר שני מספרים ראשוניים p , q: 2,5, מחשב את n: 10, ומפרסם אותם בנחלת הכלל. כמובן, לשימושים מעשיים המקבל צריך לבחור p,q גדולים יותר (כדי שהיריב לא יוכל לפרק את n בקלות לגורמיו, התכונה עליה מתבססת כזכור ה-RSA).[38]

המקבל מחשב את t: t=(q-1)*(p-1)=(5-1)*(2-1)=4*1=4.

המקבל מחשב גם את E: הוא מחפש מספר כלשהו שיהיה זר ל-t כלומר זר ל- 4. אם יבחר את המספר 3, נראה כי הוא מתאים, כי 3 ו- 4 זרים הדדית (כלומר המחלק המשותף הגדול ביותר שלהם הוא 1 – מתאים להגדרה). אם הוא היה בוחר E=2 זה לא היה פועל, כי המחלק המשותף הגדול ביותר של 2 ו-4 הוא 2 (לא מתאים להגדרה, כי צריך שהמחלק המשותף הגדול ביותר יהיה 1).

כאמור, המקבל שם בנחלת הכלל את שני אלה (המפתחות הפומביים): n=10,E=3.

המקבל מחשב כעת את D: זהו ההופכי הכפלי של E, מודולו t, דהיינו: D*E=1 (mod t). מאחר ש-t ידוע למקבל הוא יכול לחשב את D בקלות:
D*E=1 (mod t) → D*3=1 (mod 4) → 9=1 (mod 4) → D=3.
D הוא המפתח הסודי של המקבל, והוא ישמור את ערכו (3) בסוד.

עכשיו, נניח שההודעה המקורית, אחרי העברה לביט – היא M=7. זו ההודעה שהשולח רוצה לשלוח לצד המקבל (ברור שבשימושים מעשיים מדובר על מספרים גדולים הרבה יותר).

השולח מחשב את ההודעה המוצפנת C כך מציבים בנוסחא:
C=M^E (mod n):
C=M^E (mod n)=7^3 (mod 10) =343 (mod 10) = 3.
נשים לב שהשולח השתמש בשני המפתחות הפומביים n ,E כדי ליצור מההודעה המקורית M את ההודעה המוצפנת C=3.

כעת המקבל קיבל את ההודעה המוצפנת 3 – נראה כיצד הוא משחזר את ההודעה המקורית באמצעות המפתח הפרטי שברשותו D=3:
M=C^D (mod n)=3^3 (mod 10)=27 (mod 10)=7.

ליריב אין דרך לדעת שההודעה המוצפנת C=3 היא למעשה ההצפנה של M=7, כי הוא אינו יודע את המפתח הפרטי D (שמקורו במספרים p,q שהם הגורמים של n). הפיענוח הושלם.

שיטת RSA מתבססת על התכונה המתמטית, שבעיית פירוק מספר גדול לגורמיו הינה בלתי פתירה. למה הכוונה? בכינוס מתמטי שנערך בשנת 1903, הכריז אחד הדוברים שהמספר הגדול

[38] עוד ראו: S.C. Coutinho, **The Mathematics of Ciphers** 33 (1999). ספר זה מתאר את היסודות המתמטיים הנחוצים למחקר בתורת ההצפנה ואלגוריתמים שונים לפירוק מספרים.

2^67-1 אינו ראשוני, וכדי לשכנע את הנוכחים, כל שעשה היה לכתוב: * 2^67-1=193707721 761838257287. ברור כי הדובר היה צריך לעבוד קשה בכדי למצוא את הגורמים הללו, אך ברגע שמצא אותם, קל היה לו להוכיח את הטענה שלו שמכפלתם אינה ראשונית. הבעיה היא כאמור, לפרק מספרים גדולים כגון 2^67-1, כאשר אין יודעים דבר על גורמיהם.

נכון לעכשיו, מספרים שלמים המכילים עד 200 ספרות יכולים להתפרק לגורמים תוך מספר שעות עבודה על מחשב חזק מאוד. אולם, אם נחשוב על הודעת טקסט באורך של עמוד מודפס, אזי הודעה כזו תכיל כ-8000 ביט[39] המיתרגמים למספר עשרוני בן 2400 ספרות,[40] הרבה מעל 200 הספרות שניתן להתמודד עימן. לכן, הודעה מוצפנת באורך של עמוד נמצאת הרחק ב"שדה הבעיות הבלתי פתירות", ולכן אי אפשר, בניגוד ל-DES, לשבור את RSA.

הביטחון שמעניקה שיטת RSA תלוי במידה רבה בקושי לפרק מספרים שלמים גדולים לגורמיהם. אם היריב יוכל לפרק את המספר n לזוג גורמיו p,q, ברור כי יוכל לפענח את ההודעה. על-ידי בחירה אקראית של שני מספרים ראשוניים בני 150 ספרות כל אחד והכפלתם זה בזה, ניתן ליצור מפתח פומבי, n, באורך של 300 ספרות, שאינו ניתן לפיצוח בזמן סביר באמצעות הטכנולוגיה הקיימת כיום. ללא פריצת דרך משמעותית בתכנון אלגוריתמים בתורת המספרים, מערכת ההצפנה RSA עדיין תספק את דרגת הבטיחות הגבוהה ביותר בעולם ההצפנה.

ג. הצרכים הביטחוניים

צורכי הביטחון בנושא זה נחלקים לשני יעדים עיקריים: צורכי אבטחה וצורכי מעקב. מעבר לשני צרכים אלה, נוכח המציאות שבה מוצרי הצפנה חזקים נגישים לכל דורש בשוק החופשי, עולה הצורך להסביר את המניע העיקרי להסדרה כולה: זהו הרצון להקשות על האויב, ובכלל זה על ארגוני הטרור.

1. אבטחה

מערכות ממשל חיוניות, וכן מערכות אזרחיות חיוניות, חייבות אבטחה מירבית. חדירה למערכות כאלה עלולה לגרום לנזקים מסוגים שונים: החל בשיבוש מערכות המחשב עצמן, ובכך גרימת נזק כלכלי בעיקרו, עובר בגניבת מידע מתוכן, ושימוש לרעה בו, וכלה בשיבוש פעולת המערכות בדרך שתגרום לנזקים פיזיים בעולם המוחשי. פעולות כאלה הן היבטים שונים של cyberterroism.[41] כך, לדוגמה, יהיה ניתן "להשמיד" מערכות פיננסיות מרכזיות במשק, או לשתק את אספקת החשמל במדינה. סייבר טרוריזם מסוג זה דורש כח חישוב גדול, וזאת על-מנת שיוכל לפצח קודים

[39] בעמוד טקסט יש כאלף אותיות בממוצע, כלומר 8000 ביט (השיטה הנפוצה היא שיטת הצפנה ASCII, המקודדת אות ב-8 ביט).

[40] 2 בחזקת 8000 הם 10 בחזקת 2400.

[41] עפר שלח, "שלא תדעו", **מעריב** (מוסף פסח, 6.4.99). נמצא ב: http://www.amalnet.k12.il/sites/minhal/maagar/mazkirut/min00144.htm (ביקור אחרון 20.12.01).

מסובכים המשמשים כהגנה על מערכות מידע. תפוצתם של מחשבי-על המסוגלים לבצע פעולות חישוב מסוג זה מוגבלת.[42] **המטרה היא למנוע נגישות של הטרוריסט אל המידע הרגיש.**

נציין כבר בשלב כזה, כי **ככל שמערכות הביטחון מפתחות מוצרי הצפנה משלהן, הרי בהיותן בעלות המוצרים והידע, אין כל קושי בכך שתוגבל תפוצת מוצרי ההצפנה האלה**. אולם בעובדה זאת לבדה אין כדי להצדיק רגולציה על מוצרי הצפנה שפותחו בשוק החופשי, מחוץ למערכת הביטחון.

נשמע הטיעון כי, לפחות בישראל, רבים מאנשי התעשייה המובילים הם יוצאי מערכת הביטחון, וכי קיים חשש לזליגת מידע. נציין כבר בשלב זה, כי גם אם הדבר נכון, הרי אין הוא מצדיק לבדו את קיומה של רגולציה על ההצפנה. **הדרך להתמודד עם החשש המובן של זליגת מידע היא באמצעות איסורים חוזיים, קנייניים (סוד מסחרי) ופליליים (איסורים על ריגול וכדומה)**, **אך לא בהתערבות בשוק ההצפנה.**[43]

ראוי עוד להזכיר כי גם בשוק האזרחי יש ביקוש לאבטחת מידע, ולעיתים הגנה על מידע אף נדרשת בחוק. כך למשל **חוק זכויות החולה**, התשנ"ו-1996 מטיל על מטפל או עובד מוסד רפואי, לשמור בסוד מידע הנוגע למטופל, וכן מטיל החוק חובה על מנהלי מוסדות רפואיים לנקוט אמצעי הגנה לעניין זה.[44] **חוק הגנת הפרטיות**, התשמ"א-1981 מטיל על בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, וכן על גופים ציבוריים מסויימים, בנקים, חברות ביטוח ומוסדת פיננסיים אחרים, חובה של אבטחת המידע שבידיהם.[45]

2. מעקב – מודיעין

אמצעי ההגנה המעשי הראשון נגד הטרור הינו המודיעין.[46] כדי לסכל פעילות טרור חייבים גורמי הביטחון להשיג מודיעין טוב, הכולל איסוף מידע על מגמות הטרור וכן מידע על הדינמיקה היום יומית.[47] לפיכך, רשויות הביטחון נזקקות לאפשרות פענוח שדרים מוצפנים. הטיעון הבסיסי (שהיה בעל תקפות מסוימת בעת מתן הצו בשנת 1974), קובע כי הגבלות ורגולציה על טכנולוגיית הצפנה בכלל, ואי מתן אישור לשימוש בהצפנה "חזקה" מדי בפרט, ירחיקו טכנולוגיה כזו מידם של יעדי המודיעין; מערכת רישוי ורישום מסודרת, במקביל, יכולה לתת מידע ושליטה מסוימים על השימוש בהצפנה.

בעבר, כבר נתקלו כוחות הביטחון ברחבי העולם בנסיונם של ארגוני טרור וגורמים עויינים אחרים להסוות את פעולתם באמצעות הצפנה. כך למשל בהצהרה שנתן ראש ה- FBI לוועדת הסנאט לענייני מודיעין,[48] מוזכר המקרה בו נעשה שימוש בהצפנה על-ידי המרגל אלדריך איימס, אשר נדרש על-ידי מפעיליו הסובייטים להצפין את המידע שהעביר. כן מאוזכר התכנון לפוצץ אחד-עשר

---

[42] שלח, **שם**.
[43] ראו סימנים ד, ה לפרק ז לחוק העונשין, התשל"ז -1977.
[44] ראו סעיף 19 לחוק זכויות החולה, התשנ"ו-1996, ס"ח 330.
[45] ראו סעיף 17 לחוק הגנת הפרטיות, התשמ"א-1981, ס"ח 128. לביקורת על היקפה של חובה זאת, ראו אבי זילברפלד, "חוק הגנת הפרטיות השלכות מעשיות", **מחשבים** PC 1987, 8-10.
[46] רוברט קופרמן, דרל טרנט, **טרור – הסכנה, המציאות, התגובה** (משרד הביטחון, התשמ"ב) 33.
[47] קופרמן וטרנט, **שם**, בע' 147.
[48] ראו דבריו של ראש ה FBI : Louis J. Freeh, "Threats to U.S. National Security" (1998), נמצא ב: http://www.infowar.com/civil_de/civil_022798b.html-ssi (ביקור אחרון 8.3.02).

מטוסים אמריקנים במזרח הרחוק על-ידי רמזי יוסוף וטרוריסטים נוספים. מחשבו הנישא של יוסוף, אשר נתפס במנילה החיל קבצים מוצפנים הנוגעים לתכנון הטרוריסטי.

המודיעין הינו אמנות מורכבת, ונפח התקשורת המועבר באמצעים המודרניים גורם למאבק מתמיד נגד המשאבים המוגבלים. לכן יש צורך במיפוי דרכי המידע והתמקדות ביירוט הערוצים החשובים ביותר כך שתשומת הלב תרוכז ככל האפשר רק בהודעות החשובות מבין זרם ההודעות העובר בערוצים השונים. רק לאחר שלב זה מתחיל השלב המוכר של התהליך המודיעיני. לשם כך יש ראשית להסיר מההודעה כל אמצעי הגנה (המתבטא בעיקר בהצפנה) לפני שניתן יהיה להחיל בהערכה המודיעינית של טיבה. אלו החושבים על פגיעות התקשורת מזווית הראיה הביטחונית מתייחסים להצפנה כמחסום העיקרי של המודיעין. בנוסף, יריב אשר ער לדרך שבה ערוצי התקשורת שלו מנוצלים יבקש לשנות ערוצים אלו כך שניצולם יהיה קשה יותר.[49] הצפנה הינה מהאמצעים היעילים ביותר למטרה זו.

לכן, ככל שיוגבל השימוש בהצפנה ותוגבל האפשרות לשווק מערכות הצפנה מתוחכמות, ייקל על ארגוני הביטחון ליירט שדרים המכילים מידע שיכול להביא לסיכול מעשי טרור. ומנגד, ככל שיהיו בידי הטרוריסטים קודים שאינם ניתנים לפיצוח, וטכנולוגיה ליצירת קודים שכאלה, יהיו יותר נפגעים בפשעים שלא ניתן למונעם.

3. הטעם שברגולציה

למרות צורכי הביטחון האלה, נראה במבט ראשון כי הטכנולוגיה כבר ניצחה: טכנולוגית הצפנה קיימת בשוק החופשי וזמינה כמעט לכל דורש: בחנויות ובאינטרנט, ומחירה שווה לכל נפש, ולעיתים קרובות – חינם. נוכח העובדה כי גבולות לאומיים אינם מהווים כיום מחסום של ממש, ובמיוחד נוכח העובדה שהסביבה הדיגיטלית מדלגת על פני מכשולים מעין אלה, עולה השאלה: האם יש כלל טעם ברגולציה?

נראה שהתשובה חיובית, משני טעמים מצטברים. האחד הוא טעם מוסרי, ומצטרף אליו טעם פרקטי. הטעם המוסרי הוא כי **גם אם מוצרי ההצפנה זמינים לטרוריסטים, אין בכך הצדקה כדי להקל עליהם, להפך**. במילים אחרות, העובדה כי יש קושי – עד כדי כשל – באכיפה, במובן זה שאין שליטה מלאה על הימצאותם של מוצרי הצפנה והגעתם לידי טרוריסטים – אינה מצדיקה "הרמת ידיים".[50]

הטעם הפרקטי כפול. תחילה, בהתמודדות מול הטרור, חשוב שמערכת הביטחון תדע מהי הטכנולוגיה המצויה בידי הטרוריסטים, אם בכלל. מידע כזה יקל על המדינה להיערך לסיכול הטרור. בנוסף, ככל שלמדינה יש "דלת אחורית", קרי מפתח-על המאפשר לה לחדור מבעד להצפנה, הרי נגישותה למידע הטרוריסטי גבוהה בהרבה. הטעם השני הוא, שכדי לנצל מוצר הצפנה בצורה האפקטיבית ביותר, יש בדרך כלל צורך בתמיכה טכנית הניתנת על-ידי היצרן. ככל שנגביל את היצרן, הרי נקשה על הטרוריסט להשתמש במוצר ההצפנה הזה.

לפיכך, אנו סבורים, ששיקולי הביטחון קיימים ומוצדקים, למרות הזמינות הגבוהה של מוצרי הצפנה חזקים בשוק החופשי. עם זאת, שיקולי הביטחון אינם לבדם, ויש לאזנם מול שיקולים

---

[49] ראו: **Codes, Keys and Conflicts: Issues in U.S. Crypto Policy** (ACM, US Public Policy Committee (1994) http://www.acm.org/reports/acm_crypto_study/chap4.html.

אחרים. באלה נעסוק בתת פרק ה, אך לפני-כן אנו מבקשים לסקור את המסגרת המשפטית הקיימת ואת השינויים שחלו בה בשנים האחרונות.

ד. המסגרת המשפטית

בפרק זה נציג את המסגרת המשפטית הנוכחית של ההסדרה באשר למוצרי הצפנה מסחריים: תחילה בישראל ואחר כך במישור הבינלאומי, בארצות הברית ובבריטניה. מובן שעל מוצרי הצפנה שפותחו על-ידי מערכת הביטחון חלים הסדרים משפטיים נוספים, שאינם מעוררים קשיים של ממש, וברור כי למערכת הביטחון הזכות (הקניינית) והסמכות (השלטונית) להגביל את זליגתם לשוק הפרטי.

1. ישראל: מאיסור גורף לרישוי מוקדם ופיקוח מאוחר

עיקרה של ההסדרה המשפטית הישראלית באשר להצפנה הוא בחקיקת משנה, מכוח חוק הפיקוח על מצרכים ושירותים, התשי״ח-1957 (להלן: החוק המסמיך).[51] מכוחו של חוק זה הוציא שר הביטחון, בשנת 1974, את צו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), תשל״ד-1974,[52] ואת אכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), תשל״ד-1974.[53] ההסדר הקבוע בחקיקת משנה זו, חייב קבלת רשיון מוקדם לשם עיסוק כלשהו באמצעי הצפנה. בשנת 1998 בוצע תיקון משמעותי בהסדר הקיים. השינוי מהווה מעבר ממשטר של איסור גורף על כל עיסוק באמצעי הצפנה ללא רשיון, למשטר ליברלי יותר, הקובע מדיניות של פיקוח מבוקר. השינוי בא לידי ביטוי בקביעה כי עיסוקים שונים באמצעי הצפנה, הם עיסוקים מותרים, שאינם חייבים ברשיון, ובקביעת שלוש דרגות של רשיון לעיסוק באמצעי הצפנה.[54] קיים פער משמעותי בין הסמכות החוקית לעניין רישוי אמצעי הצפנה, לבין המדיניות הננקטת בפועל, שהיא מתונה בהרבה.[55]

בתת-פרק זה נציג תחילה את חוק הפיקוח על מצרכים ושירותים, התשי״ח-1957, שמכוחו הותקנה חקיקת המשנה. נעבור לדיון בהסדר שקובעת אותה חקיקת משנה, אחר כך נדון בשינוי המשמעותי בהסדר המשפטי באשר להצפנה משנת 1998, במדיניות הננקטת בפועל ובפערים שבין כל אלה.

---

[50] לטיעון ברוח דומה, ראו: Codes, Keys and Conflicts, *ibid*.

[51] חוק הפיקוח על מצרכים ושירותים, התשי״ח-1957, ס״ח 240, בע' 24. חקיקת המשנה הינה מכוח סעיפים 4, 5, 15, 43 לחוק, אשר מופיעים בנספחים לחוברת זו. (להלן: החוק המסמיך).

[52] צו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), תשל״ד-1974, ק״ת תשל״ה, 45 (להלן: צו הצופן).

[53] אכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), תשל״ד-1974, ק״ת תשל״ה, 46 (להלן: האכרזה).

[54] סעיפים 1(3) ו – 3 לצו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) (תיקון), התשנ״ח-1998, ק״ת תשנ״ח, 1107 (להלן: צו הצופן המתוקן).

[55] ראו **מדיניות פיקוח ורישוי אמצעי הצפנה מסחריים** (מנכ״ל משרד הביטחון, 24.9.00)(להלן: מדיניות משרד הביטחון). נמצא בhttp://www.itpolicy.gov.il/topics/docs/mediniyut_hatspana_mod.pdf.

מסגרת ההסדר המשפטי עובר לשנת 1998

תחולת החוק המסמיך, מכוחו הותקנה חקיקת המשנה המסדירה את נושא ההצפנה, מותנית בקיומו של מצב חירום במדינה.[56] החוק הינו חוק-מסגרת, המעניק לשר או לכל חבר בממשלה,[57] סמכות רחבה להסדיר בצו ייצור, מכירה, צריכה, שימוש וכדומה, של מצרך או שירות,[58] ובלבד שיש לו יסוד סביר להניח שהדבר דרוש לקיום פעולה חיונית, למניעת ספסרות או למניעת הונאת הציבור.[59] מטרת החוק, כפי שעולה מההיסטוריה החקיקתית, היא לסייע לממשלה בהסדרת המצב הכלכלי במשק המדינה בשעת חירום, תוך הגנה על האזרח מפני חוסר הוגנות, הבאה לידי ביטוי בשעת חירום בתופעות כגון שוק שחור, ספסרות, אגירת מוצרים, האמרת מחירים, ותוך הבטחת פיתוח המשק וגידולו.[60] לאור מטרה זו, מתעוררת השאלה האם אכן הסדרת נושא ההצפנה, שהינה נושא ביטחוני, צריכה להיעשות מכוח חוק זה?[61] אומנם "פעולה חיונית", המצדיקה את התערבות השר, כוללת גם פעולה לשמירה על ביטחון המדינה והציבור,[62] אולם כוונת המחוקק הייתה הענקת כלים להתמודדות עם מצבו הכלכלי של המשק בשעת חירום.[63] ניתן לפיכך לטעון, לאור עקרונות המשפט המינהלי, כי ישנה כאן חריגה מסמכות.

לדעתנו, חריגת הצווים מגדר הסמכות שבחוק היא טעם ראשון לכך שהסוגיה ראויה להסדרה נפרדת, ישירה ומפורשת בחקיקה ראשית, ואינה צריכה לחסות בצל חקיקה כלכלית.

בכך אנו מצטרפים להמלצת ועדת המשנה של הכנסת לתקשוב ומידע בנושא היערכות מדינת ישראל לקראת עידן המידע, לחוקק חוק המסדיר את הסמכות והאחריות הכוללת לפיקוח על אמצעי הצפנה ורישוי העיסוק בהם.[64]

סמכותו הרחבה של השר להוציא צווים מכוח החוק המסמיך, כפופה לביקורת שיפוטית.[65] בדיון בכנסת בעת קבלת החוק, הועלתה ההצעה להקים מנגנון פיקוח פרלמנטרי נוסף על הביקורת

---

[56] סעיף 2 לחוק המסמיך. מצב חירום הוכרז בעבר לפי סעיף 9(א) לפקודת סדרי השלטון והמשפט, תש"ח-1948, וכיום לפי סעיף 49 לחוק יסוד: הממשלה. מצב החירום שהוכרז לא בוטל מעולם.

[57] בהתאם להגדרת "שר" בסעיף 1 לחוק המסמיך.

[58] סעיף 5 לחוק המסמיך.

[59] סעיף 3 לחוק המסמיך.

[60] ד"כ 21 (תשי"ז) 103-105.

[61] ראו למשל ברוך ברכה, **משפט מינהלי** (כרך ראשון, תשמ"ז) 88-87. המחבר מותח ביקורת על סמכויות ההתקנה הרחבות הניתנות לשרים מכוח חוק הפיקוח על מצרכים ושירותים, בהיעדר בקרה פרלמנטרית ממשית. לשיטתו מצב החירום משמש לא פעם מסווה להפעלת סמכויות ההתקנה מכוח חוק הפיקוח על מצרכים ושירותים, ללא קשר לקיומו האמיתי של מצב חירום.

[62] "פעולה חיונית" מוגדרת בצורה רחבה, בסעיף 1 לחוק המסמיך, כ"פעולה הנראית לשר כחיונית להגנת המדינה, לביטחון הציבור, לקיום אספקה סדירה או שירותים סדירים, לקיום יציבות של מחירי מצרכים או שכר שירותים, להגדלת היצוא או להגברת הייצור, לקליטת עולים או לשיקום חיילים משוחררים או נכי מלחמה".

[63] כפי שנלמד מדברי יו"ר ועדת הכלכלה בכנסת, ח"כ בנימין אבניאל, בעת שהציג את החוק בפני מליאת הכנסת בקריאה השניה. ד"כ 23 (תשי"ח) 421.

[64] ועדת משנה לתקשוב ומידע בנושא היערכות מדינת ישראל לקראת עידן המידע, הוקמה בשנת 1997, במסגרת ועדת הכנסת לתקשוב ומידע. יש להדגיש כי דו"ח הוועדה פורסם טרם שינוי צו הצופן בשנת 1998. (להלן: ועדת המשנה לתקשוב ומידע).

[65] אמנון רובינשטיין, ברק מדינה, **המשפט הקונסטיטוציוני של מדינת ישראל** (כרך ב, מהדורה חמישית, תשנ"ז), 812-833, 1165-1170. הביקורת השיפוטית בוחנת את שיקול דעתו של השר בהוצאת הצווים בכלל, האם הפעיל את סמכותו בתוך מתחם המטרות אשר הוגדרו בסעיף 3 לחוק המסמיך, והאם מטרת הצו קשורה לקיומה של שעת חירום. לדעת המחברים מגמת החלת ביקורת שיפוטית על השימוש בסמכויות החירום לפי החוק המסמיך, תגבר לאחר חקיקת חוק יסוד: חופש העיסוק. על הפגיעה בחופש העיסוק, ראו להלן, חלק ה.5 בפרק זה.

השיפוטית. לפי ההצעה, צווים בני-פועל תחיקתי יובאו לאישור ועדת הכלכלה של הכנסת, וזו תהיה רשאית, במידה שתראה לנכון, לבקש ממליאת הכנסת את ביטולם.[66] הצעה זו לא התקבלה, ועל-כן מנגנון הפיקוח היחיד הקיים ביחס לסמכות השר להוציא צווים, הוא מנגנון הביקורת השיפוטית.[67]

הסדרת הסוגיה בחקיקה ראשית ראויה, אם כן, גם מטעמים של הפרדת רשויות וקיום ביקורת של ממש על פעולת הרשות המבצעת.

מכוח סעיפים 4, 5, 15, ו- 43, לחוק המסמיך, התקין שר הביטחון בשנת 1974, חקיקת משנה העוסקת בנושא ההצפנה: צו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), תשל״ד-1974, ואכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה), תשל״ד-1974. החוק המסמיך קובע את עקרונות המדיניות ואמות המידה הבסיסיים. הצו והאכרזה הם חקיקת משנה שהרשות המבצעת מוסמכת לחוקק מתוקף הסמכה מפורשת בחוק.[68] ככלל, בידי הרשות המבצעת נתונה הסמכות להתקין הסדרים משניים, אך בפועל מוסרת לה הרשות המחוקקת גם סמכויות התקנה של הסדרים ראשוניים. תקנות מסוג זה מכונות תקנות ״מחוץ לחוק״ (prater legem), שכן בהן נקבעות לא רק הוראות לביצוע ההסדר שנקבע בחוק, אלא אף הוראות נוספות, הקובעות הסדרים ועקרונות מעבר לאלה שנקבעו בחוק. המחוקק הראשי מסתפק במקרים אלה בהצבת המטרה, לשמה יש להשתמש בחקיקת משנה. מרבית החקיקה הכלכלית היא מסוג זה והיא מפקידה בידי מחוקק המשנה מידה רבה יותר של חופש פעולה. חוק הפיקוח על מצרכים ושירותים מסמיך שר לקבוע בצווים אמצעי פיקוח כלכליים נרחבים. החוק מפרט את אמצעי הפיקוח ואת המטרות שלשמן יש להשתמש בסמכות, אך אין הוא קובע כל הסדר לגבי תוכנו של הפיקוח.[69] כך גם בענייננו: **צו** הצופן מחיל הוראות ביצוע בעניין רשיון עיסוק באמצעי הצפנה, ואילו **האכרזה** מכריזה מהם אותם מצרכים בני-פיקוח: מידע, אמצעי הצפנה, שיטת הצפנה, מפתח הצפנה, רשומה המתייחסת להצפנה ועיסוק באמצעי הצפנה.

לדעתנו, אין זה ראוי להפקיד בידי מחוקק המשנה את שאלת קביעת המדיניות. זהו עניין למחוקק לענות בו, ולכוון את הרשות המבצעת. ההסדרה הקיימת של ההצפנה היא הסדר ראשוני באופיו, וראוי לה להיקבע על-ידי המחוקק. זהו טעם נוסף להסדרת הסוגיה בחקיקה ראשית.

מהות ההסדר

נראה כי צו הצופן נועד להשיג איזון בין הצורך לשמור על ביטחונה הלאומי של מדינת ישראל מחד גיסא, לבין הרצון לאפשר תחרות סבירה בשוק תעשיית ההצפנה הישראלית, מבלי להטיל מגבלות מכבידות מדי על היצרנים ועל המשתמשים, מאידך גיסא.[70] העיקרון המרכזי שנקבע בצו הצופן

---

[66] ד״כ 23 (תשי״ח), 421-422, דברי ח״כ בנימין אבניאל.

[67] ד״כ 23 (תשי״ח) 429-430.

[68] סעיף 1 לפקודת הפרשנות [נוסח חדש], שהינו סעיף ההגדרות, כולל בין היתר בתיבה ״תקנה״ הן צו והן אכרזה. צו ואכרזה הם סוגים שונים של תקנות, שהרשות המבצעת מוציאה כחקיקת משנה. ההבדל בין צו לאכרזה הינו, שצו מחיל הוראות ביצוע פרטניות להוראות הכלליות המצויות בחוק, ואילו אכרזה הינה בעלת אופי דקלרטיבי, היא מודיעה, מכריזה, ואינה כוללת הוראות ביצוע.

[69] ראו רובינשטיין ומדינה, לעיל הערה 65, בע׳ 803.

[70] כאמור בסעיף 1 למדיניות משרד הביטחון, לעיל הערה 55.

הוא התניית העיסוק באמצעי הצפנה בקבלת רשיון מוקדם.[71] סמכות הרישוי נתונה ל"מנהל", הממונה על-ידי שר הביטחון. בפועל מונה מנכ"ל משרד הביטחון לתפקיד, וזה האציל את סמכותו לממונה על-פיקוח היצוא הביטחוני (מפ"י).[72]

למנהל סמכות להיכנס למקום בו עומד להתבצע עיסוק באמצעי הצפנה, לבדוק את אמצעי ההצפנה, ולדרוש מהמבקש רשיון פרטים נוספים, בטרם יחליט באשר לבקשת הרשיון, וגם לאחר מתן הרשיון.[73] למנהל סמכות רחבה באשר למתן הרשיון, ומכאן שיש בידו שיקול דעת רחב בנושא.[74] מובן שאופן הפעלת סמכותו של המנהל והחלטותיו כפופים לביקורת שיפוטית מכוח עילות המשפט המינהלי.[75] מבין אלה נדגיש במיוחד את עילות הסבירות והמידתיות, ואת הכפיפות לחוקי היסוד.

השינוי בהסדר המשפטי

לאור ההתפתחות הטכנולוגית והביקורת הגוברת על ההגבלה הגורפת שהטילו צו הצופן והאכרזה,[76] בוצע בשנת 1998 שינוי משמעותי בחקיקת המשנה העוסקת בנושא ההצפנה. הותקנו צו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה)(תיקון), התשנ"ח-1998,[77] ואכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה)(תיקון), התשנ"ח-1998.[78]

קדם לשינוי הזה דו"ח של ועדת המשנה לתקשוב ומידע של הכנסת בנושא אבטחת מידע. הוועדה הצביעה על מספר קשיים בהסדר המשפטי דאז, המצדיקים התערבות חקיקתית ושלטונית. הוועדה ציינה כי צו הצופן נותר בתוקפו בעיקר מנימוק ביטחוני, לאמור, הרצון לשמור את טכנולוגיות ההצפנה המתוחכמות בידי רשויות הביטחון. אולם, לאור זמינות טכנולוגיות ההצפנה כיום לכל דורש, נחלש כוחו של נימוק זה, ואין עוד מקום לפיקוח גורף על עיסוקים שונים באמצעי

---

[71] ראו סעיף 2(א) לצו הצופן. עיסוק באמצעי הצפנה מוגדר בסעיף 1 לאכרזה באופן רחב ביותר, ככולל פיתוח, ייצור, החזקה, שימוש, יבוא, ייצוא, הובלה, העברה, הפצה, מכירה או רכישה של אמצעי הצפנה, שיטת הצפנה או מפתח הצפנה.

[72] סעיף 1 לצו הצופן. עד לתיקון של שנת תשנ"ח, המנהל היה קצין הקשר, האלקטרוניקה והמחשבים הראשי בצה"ל (קשר"ר). ראו באתר משרד הביטחון: http://www.defence.gov.il/modh1/encryption/index.html.

[73] סעיף 6 לצו הצופן.

[74] סעיף 5 לצו הצופן: "המנהל רשאי לתת את הרשיון, לסרב לתיתו, לקבוע תנאים לנתינתו, להתלותו או לבטלו, הכל כפי שימצא לנכון".

[75] להיקף הביקורת השיפוטית על הפעלת סמכותה של רשות מינהלית, ראו רובינשטיין ומדינה, **לעיל** הערה 65, בע' 347-359.

[76] להרחבה ראו ויקטור בוגנים, "תשתית משפטית למסחר אלקטרוני", **שערי משפט** א (תשנ"ח), 169. המאמר נכתב טרם שינוי חקיקת המשנה בשנת 1998. המחבר מסביר כי צו הצופן והאכרזה גורפים לאור המציאות הטכנולוגית דאז, בשני היבטים: הגדרת אמצעי ההצפנה עליהם מוטל הפיקוח (כאמור, הפיקוח הוחל בשעתו על כל שיטות ההצפנה, גם הפשוטות ביותר), והיקף העיסוקים הנתונים תחת פיקוח (ההגדרה כוללנית עד כי ניתן לטעון כי היא מטילה פיקוח גם על לימוד שיטות הצפנה תנ"כיות). המחבר ממליץ לעדכן את החקיקה העוסקת בנושא ההצפנה בישראל ולהתאימה לרוח השעה. וכן בריאן ניגאן, איציק ירחי "סקירה מקוצרת – קוד הצופן", (1997) נמצא ב: http://www.itpolicy.gov.il/vadat_inter_gov/articles/zofen.htm. מאמר זה נכתב אף הוא טרם תיקון צו הצופן והאכרזה בשנת 1998. המחברים מתחו ביקורת על המצב המשפטי הקיים ביחס להצפנה בישראל, והמליצו לקבוע מדרג היתרים ביחס לעיסוק באמצעי הצפנה: התרה גורפת של שימוש באמצעי הצפנה לצורכי זיהוי, תוך הבטחה כי לא יהיה ניתן להסב את אמצעי הצפנה אלו לאמצעים להצפנת מידע. וקביעת דרגת ההיתר לעיסוק באמצעים להצפנת מידע, בהתאם לאיזון בין שיקולי ביטחון, מול שיקולי קיום מסחר ושימוש אמין ברשת, למול חירותו של הפרט להגן על צנעת חייו.

[77] צו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) (תיקון), התשנ"ח-1998, ק"ת תשנ"ח, בע' 1107(להלן: צו הצופן המתוקן).

הצפנה.[79] על-כן המליצה הוועדה לצמצם את ההגבלות על ייצוא אמצעי צופן, ולהותירן על כנן רק ביחס למדינות המוגדרות כאיום ביטחוני כלפי ישראל. הוועדה הציעה לקבוע בצו הקלות משמעותיות בדמות התרה גורפת של עיסוקים שונים באמצעי הצפנה, למעט פעילות ביטחונית.[80] לא כל המלצות הוועדה בדבר עדכון הצו יושמו. להלן נעמוד על עיקר השינויים שנתקבלו.

השינויים המרכזיים שהתקבלו ב 1998 הם :

1. העברת הסמכות הבלעדית לפיקוח על אמצעי הצפנה ולהענקת רשיון לעיסוק באמצעי הצפנה, למנהל הכללי של משרד הביטחון.[81]

2. הסמכת המנהל להודיע על אמצעי הצפנה כעל אמצעי חופשי. "אמצעי חופשי" הוא אמצעי הצפנה שהוצא מכלל פיקוח, והעיסוק בו אינו דורש רשיון, או שניתן לגביו רשיון כללי.[82]

3. הענקת פטור מרשיון לכל עיסוק באמצעי הצפנה חופשי, למעט פיתוח, ייצור, שינוי ושילוב של אמצעי הצפנה חופשי.[83] וכן הענקת פטור לכל רכישה, שימוש או החזקה של אמצעי הצפנה, אם המכירה או ההעברה של אמצעי הצפנה, לאותו אדם, נעשו לפי רשיון.

4. יצירת מדרג רשיונות לעיסוק באמצעי הצפנה, בשונה מצו הצופן והאכרזה המקוריים, שלא היה בהם סיווג מעין זה.[84] הצו המתקן איננו מגדיר את הקריטריונים לרישוי השימוש באמצעי הצפנה.

---

[78] אכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) (תיקון), התשנ"ח-1998, ק"ת תשנ"ח, בע' 1109 (להלן : האכרזה המתוקנת).

[79] הוועדה מצאה כי הצו במתכונתו משנת 1974 אוסר על שימושים שונים באמצעי הצפנה, אשר הלכה למעשה ניתנים להשגה בחופשיות בשוק הקיים. צו הצופן המקורי יצר מצב לפיו, אזרחים וארגונים, המשתמשים באותם אמצעים, מפרים את החוק, בעוד אחרים נמנעים מלכתחילה משימושים קיימים, ובכך נחסמת יכולתם להתפתח ולהתחרות בשוק העולמי. בנוגע לאבטחת מידע קובע הדו"ח, כי הצו מגביל את יכולת השימוש באמצעי אבטחת מידע, והפיתוח של מערכות מידע ברשויות ממשלתיות. באשר לפיתוח מסחר אלקטרוני, מציינת הוועדה, כי יישום דווקני של הוראות צו הצופן אינו מאפשר עיסוק בטכנולוגיות הצפנה, יישומן וייצואן.

[80] הוועדה המליצה על שינוי מהותי של החקיקה בנושא עיסוק ושימוש באמצעי הצפנה. השינוי נמצא חיוני לשם התאמת המצב המשפטי בישראל להתפתחות הכלכלית והמסחרית, כפי שהיא משתקפת ממגמת מדינות המערב, להסיר את מגבלות הפיקוח על שימוש ועיסוק באמצעי הצפנה. ראשית, במסגרת מדיניות היישום הומלץ לאמץ את המדדים הנהוגים בעולם בנוגע לאמצעי הצפנה חופשיים מפיקוח וממגבלות שימוש וייצוא. שנית, הומלץ לעדכן את צו הצופן, אשר החיל בשנת 1974 הגדרות גורפות, מגבלות על שימושים פנימיים וחיצוניים, ותהליך בירוקרטי של קבלת אישורים. שלישית, הומלץ לחוקק חוק, המסדיר את הסמכות והאחריות הכוללת לפיקוח על עיסוק בהצפנה. עוד המליצה הוועדה על הקמת רשות לאבטחת מידע, אשר תפעל על בסיס העיקרון שיש לשחרר כמה שיותר מידע ממשלתי לציבור, תוך שמירה על ביטחון מערכות המידע הממשלתיות. בנוסף, הומלץ על הקמת גוף על ממשלתי לתגובה לאיומים על מערכות מידע ברשת הלאומית. מדו"ח מבקר המדינה 52א עולה כי בשב"כ פועל כיום גוף הנקרא "הרשות ממלכתית לאבטחת המידע". במשרד האוצר פועל פרוייקט תהיל"ה, שהוא מהגופים המבצעים בתחום אבטחת מידע. תהיל"ה הוקמה בהמלצת הרשות הממלכתית לאבטחת מידע ופועלת בהנחייתה.

[81] סעיף 1(2) לצו הצופן המתוקן.

[82] סעיף 3 לצו המתקן המוסיף את סעיף 3ב לצו הצופן. כך למשל הגדיר המנהל את דפדפני הגלישה Interenet Explorer, Netscape Navigator, ואת תוכנות Microsoft Office, Winzip, כאמצעים חופשיים. ראו : http://www.mod.gov.il/modh1/encryption/tzofend.htm.

[83] סעיף 3 לצו המתקן המוסיף את סעיף 3א לצו הצופן.

[84] סעיף 1 לצו המתוקן.

מדרג הרשיונות

רשיון כללי - ניתן לכל סוגי העיסוק באמצעי הצפנה, למעט שינוי ושילוב.

רשיון מוגבל - ניתן לסוגים מסוימים של אמצעי הצפנה, לאמצעי הצפנה מסוים או למדינת יעד, וזאת לפי אמות מידה, כגון סוג המשתמש באמצעי ההצפנה.

רשיון מיוחד - ניתן לעיסוק מסוים באמצעי הצפנה מסוים.

5. הגדרת "סוג משתמש" באמצעי הצפנה כ"מוסד פיננסי, מוסד ממשלתי, או תאגיד, מוסד או ארגון מסוג אחר שאישר המנהל". נראה כי הגדרה ספציפית לסוג משתמש, משמעה צמצום הפיקוח הנעשה מכוח צו הצופן. בניגוד לתחולה הכוללת לפי צו הצופן, על "אדם העוסק באמצעי הצפנה" חל הפיקוח, מכוח הצו המתוקן, על קבוצת משתמשים מוגדרת.

6. הצו מורה על הקמת ועדה מייעצת, שבין חבריה נציג ציבור, והעומד בראשה הוא הממונה על-פיקוח היצוא הביטחוני.[85] תפקיד הוועדה לדון בבקשות לקבלת רשיון עיסוק באמצעי הצפנה. במידה שהוועדה תמליץ לדחות בקשת רשיון, יאמץ המנהל את המלצתה, ויודיע על כך למבקש בצירוף נימוקי החלטתו. המנהל אף רשאי לאצול לוועדה המייעצת או למי מוועדות המשנה, שרשאית היא למנות, מסמכויותיו, למעט הסמכות לתת, לסרב לתת, לבטל, או להתלות רשיונות.[86] מעבר לכך, הצו אינו מפרט את תהליך הרישוי.

7. באשר לייצוא מוצרי הצפנה נקבע כי למספר מדינות מצומצם, לא יינתן רשיון יצוא. במסגרת מדיניות הפיקוח על עיסוק באמצעי הצפנה מסחריים בתחומי מדינת ישראל נקבע, כי בעל רשיון למכירת אמצעי הצפנה חייב באישור בטרם ימכור אמצעי לרשות הפלשתינית.

הצו המתוקן הוא שלב חשוב בליברליזציה של הפיקוח על הצפנה, ומגמה זאת תואמת למגמה הנהוגה בעולם המערבי. עם זאת, ישנו פער בין המדיניות בפועל, שהיא עוד יותר ליברלית מההסמכה החוקית. מגמה זאת רצויה בעיננו, אולם לפער שבין המדיניות הננקטת בפועל לסמכות הרחבה יותר יש השלכות שליליות על שיקולי המחקר והפיתוח של התעשייה.

לפיכך, אנו סבורים שיש להמשיך את מגמת הליברליזציה, ולעצב את המסגרת החוקית ברוח זו.

[85] ראו אתר משרד הביטחון: http://www.defence.gov.il/modh1/encryption/index.html.
[86] סעיף 4 לצו המתקן המוסיף את סעיף 10א לצו הצופן.

2. ארצות הברית

בכל הקשור להצפנות, המשטר המשפטי בארצות הברית עבר שינוי מהותי בשנים האחרונות כאשר המגמה היא להפחית את ההגבלות והבקרה המוקדמת. ניתן לחלק את הרגולציה על הצפנה בארצות הברית לשתי תקופות.

עד לשנת 1996 נחשב ייצוא אמצעי הצפנה מעבר ל 40 ביט[87] לייצוא תחמושת, והפיקוח על הסחר באמצעי הצפנה בוצע באמצעות תקנות International Traffic in Arms Regulations -ITAR. מכיוון שאלו הגבלות מחמירות, ועל-מנת להיענות לדרישות שוק התוכנה, העלה הממשל בשנת 1993 את רעיון ה- Clipper Chip אשר היה אמצעי הצפנה בהיתר של הממשל, כאשר הממשל מחזיק את אמצעי הפיענוח של ה Clipper Chip ובכך ביקש לשמור לעצמו את אפשרות הגישה לכל תוכן המוצפן באמצעותו. הרעיון לא צלח בשל התנגדות מצד חברות התוכנה אשר היו מוגבלות בייצוא תוכנות והופלו לרעה בעולם מבחינת יכולת התחרות, מתנגדים נוספים היו ארגוני זכויות אדם ופרטיות.

בנובמבר 1996 שינה הממשל את עמדתו, והמשטר הרגולטיבי של איסור גורף וחריגים מועטים, הוחלף במשטר של הגבלות יצוא, שגם מחלקן ניתן היה לקבל פטור.[88] אמצעי הצפנה הוגדרו כתחמושת רק אם הם לצורכי צבא. מטרת הממשל הייתה לתמוך במסחר אלקטרוני, להגן על תשתיות המידע הגלובליות, להגן על פרטיות כמו גם על זכויות יוצרים ומידע בעל חשיבות, וכן מתן אפשרות לחברות אמריקניות להתחרות באופן שווה. הסמכות לפיקוח על הצפנות עברה לידי *מינהלת הסדרת הייצוא* (Bureau of Export Administration, להלן BXA) הכפופה למשרד הסחר (Department of Commerce). אמצעי ההצפנה סווגו מחדש: הם הועברו מה- Munitions Control ל- Commerce Control list. התקנות יצרו הליך לפיו בעל אמצעי הצפנה ברמה של עד 40 ביט יכול להסיר את המוצר שלו מרשימת ה- Commerce Control לאחר בדיקה אחת של ה-BXA ואז יהיה פטור למעשה מכל הגבלות הייצוא.[89] כמו כן ניתן היה לקבל רשיון ייצוא לאמצעי הצפנה, שלא ניתן להסיר מפיקוח, ברמת 56 ביט בטכנולוגיית DES[90] (או מקבילה) בשני תנאים: התנאי הראשון היה בדיקה חד-פעמית של המוצר לפני הייצוא, והתנאי השני היה קיומו של אמצעי עוקף הצפנה Key Escrow or Key Recovery.[91]

יש לציין שהממשל רשאי לקבוע את ההגבלות על הייצוא, שלא באמצעות חקיקה, מתוקפה של חקיקת חירום.[92] כפי שיפורט בהמשך, כיום קיימת ליברליזציה בתחום ייצוא הצפנות מארצות הברית, ואולם עיון בתקנות מראה כי שיקולים פוליטיים, כלכליים וביטחוניים משפיעים על

---

[87] להסבר טכני, ראו לעיל חלק ב בפרק זה.

[88] Executive Order 13026 (November 15, 1996).

[89] 61 FR 68572 (1996), http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg96.html#encryption1.

[90] להסבר טכני אודות שיטת DES ראו לעיל, חלק ב, בפרק זה.

[91] הכוונה במונחים אלו שלצד שלישי, שאיננו בעל המידע המוצפן, תהיה אפשרות לפענח את המידע. התקנות מגדירות מי יכול להיות צד שלישי ואת האופן שניתן לפנות אליו על-מנת לפענח מידע.

[92] International Emergency Economic Power Act (IEEPA), codified as 50 U.S.C. §1701; National Emergencies Act , codified as 50 U.S.C. §1601; The Export Administration Act, codified as 50 U.S.C. § 2401.

אפשרויות הייצוא למדינות השונות. מדיניות הליברליזציה נמשכה, בסדרת היתרים משנת 1998 ומשנת 2000.

המצב המשפטי כיום

בתוך ארצות-הברית: אין הגבלה על מסחר וייצור אמצעי הצפנה בכל רמה בתוך המדינה. **מחוץ לארצות-הברית:** רגולציה באמצעות תקנות הייצוא המיושמות על ידי מינהלת הסדרת היצוא (BXA). ה- Bureau of Export Administration אחראי להסדרת ייצוא אמצעי הצפנה.[93] האיסור הגורף היחיד שנותר תקף הוא ייצוא הצפנות למדינות תומכות טרור או אזרחיהם.[94] **היתרים משנת 1998**[95]: הצעד המשמעותי ביותר בשנה זו היה הוויתור של הממשל על הדרישה הגורפת לשלב אמצעים אשר יאפשרו פיענוח של ההצפנות (דלת אחורית). צעד נוסף היה חיזוק ההגנה הטכנולוגית על מוסדות פיננסיים. להלן מספר שינויים שבוצעו באותה שנה:

- ניתן לייצא, ברשיון ולאחר בדיקה, טכנולוגיות המשלבות אמצעי הצפנה לבנקים ומוסדות פיננסיים (לרבות חברות ביטוח), ל- 45 מדינות,[96] בלי אמצעי פיענוח,[97] וללא הגבלה על רמת ההצפנה. היתר זה איננו מיועד למוצרים לשיווק המוני אלא לשוק מוגבל ולמטרות ביצוע עיסקאות בטוחות בין המוסד הפיננסי והלקוח.
- היתר ייצוא לכל הצפנות עד 56 ביט לאחר בדיקה טכנית.
- ניתן לייצא הצפנות לחברות-בת אמריקניות או לסניפים של חברות אמריקניות מחוץ לארצות הברית.
- הותר לייצא טכנולוגיות הצפנה למסחר אלקטרוני תחת רשיון ל 45 מדינות בתנאי שהמסחר מאובטח והוא לא מבוצע ישירות בין משתמשי קצה.
- היתר ייצוא לסחורות או תוכנות בנושאי בריאות ורפואה, ל 45 המדינות, ללא הגבלה על רמת ההצפנה, ובלבד שנועדו למשתמשי קצה בלבד.
- מי שקיבל פטור מההגבלות על ייצוא לפני 40 ביט רשאי לשדרג את המוצר עד ל 56 ביט.

היתרים משנת 2000.[98] השינויים האחרונים הביאו למצב של ליברליזציה רבה בייצוא הצפנות במיוחד מול מדינות האיחוד האירופאי ומספר מדינות נוספות. תחת ההגבלות החדשות ניתן

---

[93] ראו: 740.13, 740.17, 742.15 Export Administration Regulations, נמצא ב- http://w3.access.gpo.gov/bxa/ear/ear_data.html .

[94] המדינות התומכות בטרור לפי הממשל האמריקני הן: סוריה, איראן, עיראק, לוב, סודן, צפון קוריאה וקובה. מידע נוסף על מדיניות הגדרת מדינות תומכות טרור ניתן למצוא במסמך של ה Congressional Research Service מחודש מארס 2001 על מדיניות החוץ של ארצות-הברית בהתמודדות עם טרור. http://www.fas.org/irp/crs/IB95112.pdf. הסבר נוסף באתר משרד החוץ שם http://www.state.gov/www/global/terrorism/1999report/sponsor.html

[95] ראו: 63 FR 50516 (09.22.98), 63 FR 72156 (31.12.98), נמצא ב http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg98.html#encrypti

[96] ראו: Supplement No. 3 to (EAR), 15 C.F.R. Sections part 740. כיום הסעיף איננו מופיע עוד, מכיוון שההגבלות אינן ייחודיות עוד למדינות אלו).

[97] Key escrow or Key Recovery.

[98] ראו 65 FR 2492 (14.1.00), 65 FR 62600 (19.10.00), נמצא ב- http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg00.html#65fr2492 . ראו גם הצהרה של הבית הלבן

לייצא מוצרים ותוכנות המכילים כל רמה של הצפנה לחברות, יחידים וארגונים לא ממשלתיים ללא רשיון ולאחר בדיקה טכנית בלבד. ההסדר של בדיקות לפני קבלת היתר ייצוא, חובת שילוב אמצעי פיענוח ורשיונות הוחלף במנגנונים של בדיקות בשלב מוקדם, והודעות על ייצוא לאחר ביצוע, על-מנת לתת לממשל מידע להיכן מיוצאת טכנולוגיית הצפנה ובאיזו רמה. התקנות מקלות על חברות תקשורת וספקיות גישה ומאפשרות להן שימוש רחב באמצעי הצפנה כמו גם ליצרנים של טכנולוגיות אלחוט בטווח קצר. להלן מספר שינויים מרכזיים:

- התקנות החדשות מתירות ייצוא, לאחר בדיקת הרשות, של מוצרים או תוכנות בכל רמה של הצפנה המיועדים ליחידים, לחברות ולשאר משתמשי קצה שאינם ממשלתיים. כמו כן ניתן להפיץ הצפנות לכל היעדים, מכיוון שהעלאה לאינטרנט של הצפנה איננה מקיימת "ידיעה" על העברת הצפנה למדינה תומכת טרור. השינויים מאפשרים להסתפק בהודעה לרשות, שאמצעי הצפנה יוצאו.[99]
- התקנות מפשטות את הייצוא למדינות האיחוד האירופאי, למדינות נוספות באירופה, וכמו כן ליפן, אוסטרליה וניו-זילנד.
- התקנות מקלות על ייצוא אמצעי הצפנה שנועדו לטכנולוגיות אלחוט בטווח קצר.
- ניתן לייצא הצפנה לחברות אמריקניות מחוץ לארצות הברית ללא בדיקה טכנית מוקדמת. חברות הצפנה הפועלות בארצות הברית שמעסיקות זרים אינן זקוקות עוד לרשיון ייצוא.
- ניתן לייצא Open Source Code ברשיון, ויש ליידע את הרשות לגבי מיקומו של הקוד.[100]
- התקנות מאפשרות לחברות תקשורת וספקי גישה לאינטרנט לשלב אמצעי הצפנה בשירות שהן מעניקות.
- יש חובה לאפשר ל BXA בדיקה (חד פעמית) ברוב המקרים.

ביקורת כלפי הממשל

השינוי האחרון (משנת 2000) של הממשל הפחית את הביקורת מצד ארגוני זכויות אדם ופרטיות. ה Center for Democracy and Technology,[101] פירסם את שני העקרונות שלפיהם יש לבחון, לטעמו, את המדיניות: הראשון הוא המידה שתקנות הייצוא מגבילות אנשים ברחבי העולם להשתמש בטכנולוגיות הצפנה על-מנת לשמור על פרטיותם, והשני, מידת החופש שניתן לאנשים

בהקשר של שינוי מדיניות ייצוא הצפנות: http://www.cdt.org/crypto/CESA/whousepress091699.shtml .

[99] מינהלת הסדרת היצוא (BXA) קנסה לאחרונה את חברת התוכנה NeoPoint על ששיווקה ביודעין, וללא רשות, תוכנות הצפנה בעוצמה של 128 ביט לדרום קוריאה. ראו: http://www.bxa.doc.gov/press/2002/PenaltyImposedExpEncSoft.html.

[100] קוד מקור חופשי (Open Source Code) הוא קוד בשפה קריאת מחשב (ראו חוק המחשבים, התשנ"ה–1995 סעיף 1, הגדרות) וניתן לשנות אותו ולדלות ממנו מידע על האלגוריתמים של ההצפנה. כאשר הוא חופשי (open) הכוונה שהוא נגיש לרבים ואינו למטרה מסחרית, למשל תוכנת מערכת ההפעלה של לינוקס.

[101] http://www.cdt.org.

להשתלב בכלכלת המידע מבלי לעבור על החוק. על בסיס עקרונות אלו מביע המרכז ביקורת על התקנות החדשות בארבעה מישורים:[102]

- היתר הייצוא ניתן רק למוצרים שנמכרו בתשלום. מכאן שאין היתר מפורש להפצת-חינם של מוצרים המכילים אמצעי הצפנה, לרבות תוכנות דוגמת דפדפנים מאובטחים אשר מופצות בחינם.
- ההגדרה הרחבה של מוסד שלטוני, שכולל כל ארגון וחברה ציבורית, מציבה רף דרישות גבוה במיוחד לחברות קטנות ויחידים המעוניינים לייצא מוצרים בעלי הצפנה חזקה לאותם גופים המוגדרים, שלא בצדק, שלטוניים.
- החובה למנוע מטכנולוגיות הצפנה חזקות להגיע למדינות תומכות טרור מציבה מכשול בפני ארגונים בינוניים וקטנים ובפני יחידים להפיץ טכנולוגיות. יש להבהיר שחובת הדיווח לגבי יעד הטכנולוגיה צריכה להתחשב בהקשר של הפצת טכנולוגיות באינטרנט שהוא אנונימי ביסודו.
- ההגבלות על ייצוא קוד מקור הקשור להצפנות[103] פוגעות בהפצת קוד שאינו למטרות מסחריות, ואשר נועד לשימוש ופיתוח על-ידי משתמשים רבים. חברות וארגונים יוכלו להתמודד עם ההגבלות אולם הפצת קוד לא מסחרי שאין עליו בעלות קניינית יוצרת בעיה של אכיפה, והטלת ההגבלות על כל מי שמפתח את הקוד אינה מעשית.

3. המישור הבינלאומי

לאחר התבוננות בנעשה בארץ ובארצות הברית אנו מבקשים לסקור את המסגרת המשפטית במישור הבינלאומי. בזירה זאת נוכל למצוא כיום גישה ברורה של צמצום (עד כדי ביטול) ההסדרה על מוצרי הצפנה ושירותי הצפנה.[104] מגמה זו מצאה ביטוי ממשי במדינות השונות, וברוב מדינות העולם המערבי ניתן כיום לייצר, להשתמש ולמכור מוצרי הצפנה ושירותי הצפנה באופן חופשי. תת-פרק זה סוקר בקצרה את פעילות הגופים קובעי המדיניות במישור העולמי וכן הוראות מדינתיות מיוחדות.

גורמים מרכזיים בעיצוב המדיניות הבינלאומית

בהתאם לדו"ח בינלאומי שנתי בנושא הצפנה,[105] ניתן לציין שני גופים כגורמים מרכזיים לדחיית מגבלות על הצפנה ופיתוח שוק חופשי ותחרותי למוצרי הצפנה: **האיחוד האירופאי (EU) והארגון לשיתוף פעולה ולפיתוח כלכלי (OECD).**

א. האיחוד האירופאי (EU)

נציבות האיחוד האירופאי הקימה בשנת 1992 ועדה בנושא אבטחת מידע והצפנה בתוכנית הכוללת מסגרת-עבודה אסטרטגית לאבטחת מידע; ניתוח של דרישות אבטחה; פתרון צרכים;

---

102 ראו פירוט העמדה במכתב לרשות הייצוא http://www.cdt.org/crypto/admin/991206comments.shtml.

103 הכוונה היא בעיקר לאלגוריתמים של הצפנות אשר נמצאים בשפה קריאת מחשב (source code).

104 **Cryptography & Liberty 1999/2000**: www.gilc.org/crypto/crypto-survey-99.html; http://www2.epic.org/reports/crypto2000/ (12.12.01).

פירוט, סטנדרטיזציה ווידוא של אבטחת מידע; אינטגרציה של התפתחויות טכנולוגיות לאבטחה; ושילוב של פונקציות ביטחוניות במערכות מידע.[106] הנציבות פרסמה מספר דוחות וניירות עמדה,[107] לפיהם יש בכוונתה לפתח אסטרטגיה להבטחת שוק פנימי למוצרי הצפנה ושירותים נלווים, וכן ליצירת מסגרת שתגן על אלו הבוחרים להשתמש במוצרי ההצפנה במסגרות המתאימות. ניירות עמדה אלה אכן היתרגמו למספר דירקטיביות שחלקן ייסקר להלן.

ביטוי למגמה לפיה יש להנהיג שוק חופשי למוצרי הצפנה ושירותי הצפנה, ניתן למצוא בדירקטיבה על חתימה אלקטרונית (**Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures**).[108] לנושא החתימה האלקטרונית והגופים המסחריים הפועלים במסגרת תהליך ההכרה בחתימה ישנו קשר הדוק לתחום ההצפנה, שכן כל תהליכי האשרור מתבססים על מפתחות הצפנה. סעיף ההגדרות בדירקטיבה נותן ביטוי מפורש ומעוגן לתהליך ההצפנה, באישור החתימה האלקטרונית, הכולל מידע לאימות חתימה ("signature-verification-data") לרבות קודים או מפתחות הצפנה ציבוריים שמשתמשים בהם לצורך אימות חתימה אלקטרונית, מכשיר לאימות חתימה ("signature-verification device") דהיינו תוכנה או חומרה שמשתמשים בה לישום מידע לאימות חתימה, ותעודה דיגיטלית ("digital certificate") המקשרת את מידע אימות החתימה לאדם ומאשרת את הזהות של אותו אדם.
סעיפים 3-4 קובעים כי המדינות אינן רשאיות להנהיג מגבלות על כניסה לשוק נותני שירותי האישור (certification) וכי אין להקים דרישות-קדם לקבלת אישורים שלטוניים. יחד עם זאת, ניתן להפעיל תוכניות וולנטריות, שמטרתן תהיה הגברת איכויות השירותים. על תוכניות אלה חלה חובה להיות אוביקטיביות, שקופות לציבור ולא-מפלות. כמו כן, יש לקיים מערכת פיקוח על נותני השירותים. בין היתר, נציבות האיחוד דורשת ממדינות חברות לדווח לנציבות על כל הצעה מדינתית להטיל כללים ומגבלות על מוצרי הצפנה.

ב. הארגון לשיתוף פעולה ולפיתוח כלכלי (OECD)[109]

ב- 1997 פרסם ה- OECD (Organization for Economic Co-operation and Development) קווים מנחים למדיניות הצפנה.[110] ההנחיות מכוונות בעיקר לרשויות שלטוניות, אך נכתבו מתוך ציפייה כי יעוררו התייחסות הן מכיוון הסקטור הפרטי והן מן הציבורי. עקרונות אלה מפורטים להלן:

1. שיטות הצפנה צריכות להיות אמינות על-מנת לייצר ביטחון בעת שימוש במערכות תקשורת.

---

[105] שם.
[106] Council Decision 92/242/EEC of 31 March 1992 in the field of information security.
[107] http://europa.eu.int/scadplus/leg/en/lvb/l24121.htm.
[108] OJL 013 (19.01.2000) pp. 0012 - 0020.
[109] Organization for Economic Co-operation and Development. מדובר בפורום שהוקם בשנת 1961 ובסיסו בפריס. הפורום כולל את 29 המדינות המפותחות (ישראל אינה חברה). פורום בינלאומי זה מוציא הנחיות בנושאים שונים הנוגעים לתחומי כלכלה ומסחר, והמלצות אלה, על אף שבאופן רשמי אינן מחייבות, זוכות להתייחסות רבה ולהשפעה על המדינות החברות וכן על מדינות שאינן חברות בפורום. ראו: http://www.oecd.org.

2. למשתמש צריכה להישמר הזכות לבחור שיטת הצפנה בכפוף לדין החל.
3. שיטות הצפנה צריכות להיות מפותחות ביחס לצרכים ודרישות של קהל היעד.
4. סטנדרטים טכניים ברמה הלאומית והבינלאומית.
5. הזכות הבסיסית לפרטיות לרבות ביטחון התקשרויות והגנה על מידע אישי במדיניות הצפנה לאומית ובשימוש בשיטות השונות.
6. מדיניות לאומית צריכה לאפשר גישה חוקית לטקסט הלא-מוצפן ולמפתח ההצפנה.
7. אחריות מאשרי שירותי ההצפנה או בעלי המפתח צריכה להיקבע בבהירות.
8. יש להימנע מיצירת מכשולי מסחר ביחס להצפנה ועל-ידי כך להגיע לשיתוף פעולה בינלאומי בקביעת מדיניות.

יש לשים לב לעיקרון השלישי, המתייחס לצורך בפיתוח שיטות הצפנה, על-פי דרישות השוק החופשי (Market driven development of cryptographic methods). העיקרון קובע כי מחקר ופיתוח בתחום ההצפנה צריך שיוכתבו על-פי הצרכים, הדרישות והמחויבויות של פרטים, עסקים וממשלות. באופן זה ניתן יהיה להבטיח כי הפיתוחים יותאמו לטכנולוגיות המשתנות, לדרישות הצרכנים, ולהתפתחויות בשוק באופן כללי.

ג. דחיית מדיניות ה- Key Escrow/Key Recovery ומעבר לגילוי כפוי של מפתחות וגישה מורשית

בד-בבד עם דחיית הגישה של קיום אמצעים מקומיים-לאומיים, דחו רוב המדינות את מדיניות "Key Escrow/ Key Recovery" (התפישה לפיה משתמשים יוכלו להשתמש בהצפנה במערכות שלהם, אולם גוף שלישי - שלטוני - יקבל את המפתח לצופן מנותני שירותי ההצפנה, ואותו גוף שלטוני יהיה אחראי על העמדת המפתח לרשויות המתאימות במקרים שיתבקש לעשות זאת). מדיניות זו אומצה בחוק הצרפתי בשנת 1996, אך החוק בוטל בשנת 1999. המדיניות אף קודמה במשך שנים מעטות על-ידי ממשלת בריטניה (ולכך נשוב בהמשך). ארצות הברית ניסתה לקדם מדיניות זו ונתקלה בסירוב מצד ה- OECD, וכן בביקורת מצד מומחי ביטחון שהדגישו את הבעייתיות במצב שבו גוף מרכזי מחזיק את המפתח להצפנה כאשר נקודות הביקורת העיקריות נגעו בוולונטריות, פרטיות, עלויות ויעילות. דחייתה הסופית של המדיניות היתה בהסכמי Wassenaar בדצמבר 1998 (שידונו להלן). כיום, מדינות ספורות פועלות לפי שיטה זו, ובארצות הברית – כפי שנדון לעיל - מגבלות על יצוא שעודדו את השיטה בוטלו בינואר 2000.

בעקבות דחיית מדיניות ה- Key Escrow, אומצה גישה חדשה על-ידי מדינות רבות: דרישה ל"גישה חוקית" "lawful access" למפתחות הצפנה או לטקסט רגיל. לפי גישה זו פרטים ידרשו לחשוף מפתחות הצפנה לרשויות האכיפה ואם יסרבו יהיו חשופים לתביעות פליליות. עד לשנת 2000 רק מדינות ספורות חוקקו חוקים מהסוג המתואר, אולם כעת צפוי המצב להשתנות. הנחיות ארגון ה- OECD שתוארו לעיל ציינו את עיקרון הגישה אך לא תמכו בו. ההנחיות ציינו כי מדיניות לאומית רשאית לאפשר גישה חוקית לטקסט או למפתחות הצפנה, אולם מדיניות זו

[110] http://www1.oecd.org/dsti/sti/it/secur/index.htm.

חייבת לכבד עקרונות אחרים שהופיעו בהנחיות הארגון. נושא זה עורר ויכוח נוקב במסגרת ה-OECD, עד שלבסוף החליט הארגון שלא לתמוך בגישה גלובלית ל"גישה החוקית".

בהקשר של גישת ה- "lawful access", יש לתת את הדעת לזכות להימנע מהפללה-עצמית שקיימת ושרירה במדינות רבות בעולם. בבסיס הזכות עומד איסור על גופים שלטוניים לכפות על אדם לתת עדות שעלולה להפליל אותו. בהקשר זה קיימת טענה כי לאור הזכות לא ניתן לכפות על אינדיבידואלים לחשוף מפתחות הצפנה או סיסמאות שאינן רשומות במקום אחר. בארצות הברית הועלתה הטענה בהקשר של התיקון החמישי לחוקה,[111] ואילו באירופה מתבססת הטענה על האמנה האירופאית לזכויות אדם, שמאפשרת לאדם לשמור על זכות השתיקה.[112]

ד. הסכמי Wassenaar[113]

הסכמי Wassenaar הם שורת הסכמים בין 33 מדינות להגבלת יצוא של נשק קונבנציונלי וטכנולוגיה בעלת "שימוש כפול" (שימוש הן למטרות מסחריות והן למטרות צבאיות). בטכנולוגיה נכללים מספר מוצרי הצפנה שנחשבים בעלי "שימוש כפול". יודגש כי אין המדובר באמנה או בסוג חקיקה, אלא החלפת דעות ברמה הבינלאומית, ומכאן שהתאמת המדינות החברות היא עניין שבשיקול דעתן ונעשית באמצעות חקיקה במישור הלאומי. הוראותיו העיקריות של ההסכם מתייחסות לייצוא חופשי של מוצרי הצפנה לפי חלוקה לביטים, הקלה על יצוא מוצרים מוצפנים לשם הגנה על קניין רוחני וכן הוראה לפיה יצוא מוצרי הצפנה שאינם מוזכרים בהסכמים דורש רישיון. החשיבות היא לעובדה כי כיום קיימת פירצה משמעותית ומכוונת המאפשרת מסחר חופשי ביחס להפצת נכסים לא מוחשים של הצפנה לרבות "הורדות" מהאינטרנט.[114]

ה. סיווג בינלאומי

מדינות העולם זוכות במסגרת הדו"ח הבינלאומי שנזכר לעיל, לסיווג ולמיון ביחס לאמצעי ההגבלה המוטלים באותה מדינה על מסחר במוצרי הצפנה ושירותי הצפנה.[115] הדו"ח מחלק את המדינות שנבחנו לשלוש קטגוריות על בסיס אמצעי שליטה על הצפנה. הסיווג נועד לאפשר מפה עולמית של מדיניות הצפנה לשם השוואה, ואין בסיווג סנקציות נלוות.

הקטגוריה "הירוקה" כוללת מדינות שמקדמות מדיניות שמאפשרת מסחר ללא הפרעות משפטיות במוצרי הצפנה, כמו במצב שהמדינה אימצה את הנחיות ארגון ה- OECD. הקטגוריה "הצהובה" כוללת מדינות בהן הוצעו אמצעי שליטה מדינתיים על הצפנה, לרבות הגבלות על שימוש, יבוא, או במצב שהמדינה פועלת בהקפדה לפי הסכמי Wassenaar. הקטגוריה האחרונה - וזאת הנחשבת

---

111 ראו למשל: **Doe v United States**, 487 US 201, 219 (1988) (Stevens J, dissenting)("[a defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe--by word or deed.")

112 http://www.fipr.org/ecomm99/ecommaud.html.

113 www.wassenaar.org.

114 **Cryptography & Liberty 1999/2000:** ; www.gilc.org/crypto/crypto-survey-99.html **E-commerce: A Guide to the Law of Electronic Business** 63 (Daniel Tunkel & Stephen York, eds., 2d ed., 2000). http://www2.epic.org/reports/crypto2000 (12.12.01);

הלא-רצויה ביותר – היא הקטיגוריה "האדומה", וכוללת מדינות בהן יש אמצעי שליטה גורפים על הצפנה. מדינות רבות אינן מתאימות לקטגוריה אחת בדיוק, ולכן הדו"ח במקרים המתאימים ממקם מדינות בין קטגוריות.

בהתאם לשיטת סיווג זו הוגדרה ישראל בשנת 1998 בצבע האדום, כלומר הקטגוריה בעלת המגבלות הרבות ביותר על הצפנה. בשנת 1999 חל שיפור ורמת ההגבלות שונתה, לצבע אדום-צהוב. ואילו בשנת 2000 הדירוג הישראלי הוא צהוב, קרי קטגוריית הביניים.

ו. המצב המשפטי בבריטניה

באנגליה נכנס לתוקפו בחודש מאי 2000 חוק ליישום הדירקטיבה האירופאית בנושא חתימה אלקטרונית (99/93/EC) הוא ה **Cryptography Service Provider and the Electronic Communication Act 2000**. החוק הבריטי קובע את סדרת הפעולות שיש לבצע לקראת רישום נותני שירותי הצפנה וכן קובע הכרה משפטית בחתימה אלקטרונית. בהתאם להנחיות החוק על מזכיר המדינה מוטלת חובה לייסד ולתפעל **מרשם של נותני שירותי הצפנה.**[116] חברות שתהיינה זכאיות לרישום הן חברות המעניקות שירותים מסוג של וידוא המפתח הציבורי של פרט, ניהול מפתחות הצפנה, שירותי חותמות-זמן על חתימות אלקטרוניות, איחסון מפתחות הצפנה וכדומה. אומנם החוק אינו מספק קריטריון ספציפי לקבלת אישור לרישום, אך הוא מונה פרטים נדרשים וביניהם הטכנולוגיה המוצעת, זהות המבקש רישום והאופן שבו הוא מספק את הטכנולוגיה לציבור. חוק זה, למעשה, דוחה מפורשות את גישת ה- Key Escorw ונוקט גישה של קיום מרשם נותני השירותים שיהיה פתוח לציבור, להבדיל ממרשם ממשלתי חסוי שירכז את המפתחות עצמם.
ההיבט המרכזי בחוק הוא היות המרשם וולונטרי. כתוצאה מכך, כל ספק שירותי הצפנה יכול לסחור בשוק החופשי בלא קשר להיעדרו מהמרשם הציבורי, או אפילו אם בקשתו להירשם נדחתה. יחד עם זאת, יש לזכור כי משמעות היותו של המרשם ציבורי היא כי הוא פתוח לעיון הציבור, ככלי לבחירה וביקורת בתחום.[117]

4. המישור הבינלאומי - פיענוח

לאחר שסקרנו את ההסדרה הישירה הנוגעת להצפנה, נבחן את צידו השני של המטבע: השאלות המתעוררות כאשר חומר מוצפן מפוענח על-ידי צד שלישי. אדם החפץ להגן על מידע מסוים ובוחר להצפינו יכול לעשות זאת במספר דרכים, כך בין היתר, אמצעי ההגנה בעידן הדיגיטלי יכולים להימצא בכניסה לחנות וירטואלית או לשרת בדמות סיסמה, בבית הצרכן בדמות הממיר והטלויזיה בתשלום (Pay TV) או הגנה שמשולבת בתוך המוצר עצמו ומגבילה את יכולת השימוש הפונקציונלית. כל אחת מהדרכים המתוארות מצריכה פיענוח של ההצפנה על-מנת לגשת ולהשתמש במידע.

---

[115] ראו: **Cryptography & Liberty 1999/2000**, נמצא ב: www.gilc.org/crypto/crypto-survey-99.html; http://www2.epic.org/reports/crypto2000/. (12.12.01).

[116] נתוני שירותי הצפנה מוגדרים בסעיף 6 לחוק כך: "any service which is provided to the senders or recipients of electronic communication, or to those storing electronic data, and is designed to facilitate the use of cryptographic techniques".

[117] ראו: **E-commerce: A Guide to the Law of Electronic Business**, supra note 115, at 59.

החקיקה הבינלאומית ביחס לפיענוח הצפנה נעשית בעיקר בשלוש מסגרות: הגנה באמצעות מסגרת נלווית לזכות יוצרים, חקיקה ביחס לגישה מותנית לשירותים מקודדים וחקיקה הנוגעת למאגרי מידע.

א. מסגרת נלווית לזכות היוצרים

זכות היוצרים במהותה מספקת לבעל הזכות שליטה על שימושים מוגדרים ביצירה. בשנים האחרונות התפתחו כלים שונים להגן באופן טכנולוגי על יצירות, ואילו המשפט בחר להכיר בזכותו של בעל זכות היוצרים להשתמש במיכשור כאמור ולהגן על עצמו ועל יצירתו במצב שבו אנשים חפצים להערים על המיכשור. להלן נציג את ההסדרים המישפטיים המרכזיים המקנים מעמד מועדף לאמצעים טכנולוגיים המשמשים להגנה על זכות היוצרים. את ההגנה על ההצפנה מפני הפיענוח במסגרת זכות היוצרים נבחן לאור אמנת WIPO, החוק האמריקני ה- DMCA, פעולות האיחוד האירופאי ביחס לאישור האמנות הבינלאומיות, הדירקטיבה האירופאית החדשה לזכויות יוצרים, ולבסוף נציג גם את עמדת החוק הבריטי בעניין.

WIPO Copyright Treaty, WIPO Performances and Phonograms Treaty[118]

אמנות אלה הן מבית היוצר של הארגון העולמי לקניין רוחני. בבסיס האמנות של הארגון אמנת פריז וברן, ואילו האמנות העוקבות לרבות אמנה זו (משנת 1996) הרחיבו את ההגנה הניתנת תוך התחשבות בהתפתחויות טכנולוגיות דיגיטליות. האמנות WIPO Copyright Treaty (WCT), ו- WIPO Performances and Phonograms Treaty (WPPT) נועדו לעדכן את ההגנה הבינלאומית של זכויות יוצרים וזכויות שכנות בעידן האינטרנט. הראשונה כבר תקפה, השניה צפויה להיכנס לתוקף בקרוב.

בהתאם ל WCT, היוצר-המחבר יהנה מהגנה משפטית על הפצה, השכרה מסחרית ושידור לציבור של היצירה על הרשת (network). הגנה ספציפית ניתנת למערכות זיהוי וניהול היצירות (identifying and managing). סעיף 11 לאמנה דורש ממדינות החתומות להגן על אמצעים טכנולוגים אפקטיבים שמשמשים להגנה ומימוש של זכות יוצרים, וכן להגביל פעולות שאינן מאושרות על-ידי בעל הזכות או אינן מותרות לפי דין קיים.

ה- Digital Millennium Copyright Act (DMCA)[119]

במסגרת התאמת הדין האמריקני לאמנה זכויות היוצרים של ה- World Intellectual Property Organization (WIPO)[120] משנת 1996, נחקק בשנת 1998 ה DMCA. החוק נועד למנוע עקיפת אמצעים טכנולוגיים המגנים על יצירות. ליבו של האיסור נמצא בסעיף 1201 האוסר עקיפת אמצעי גישה טכנולוגיים:[121]

---

[118] ראו: http://www.wipo.int/treaties/ip/copyright/copyright.html

[119] Pub. L. No. 105-304, 112 stat. 2860 (Oct. 28, 1998). נוסח החוק נמצא ב: http://www4.law.cornell.edu/uscode/17/1201.html.

[120] WIPO Copyright Treaty http://www.gseis.ucla.edu/iclp/wipo1.htm (1996).

[121] 17 U.S.C. § 1201(a) (1)(A).

"No person shall circumvent a technological measure that effectively controls access to a work protected under this title".

בנוסף, החוק אוסר ייצור, מכירה, מתן שירות והפצה אשר נועד כולו או ברובו לפיענוח הגנות טכנולוגיות המוגנות בזכויות יוצרים:[122]

"No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that - (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;"

שאלה פרשנית שטרם עמדה למבחן בתי המשפט היא מה היקף האיסור: האם הוא חל על-פיענוח הגנות טכנולוגיות בכלל או רק על הגנות טכנולוגיות המגנות על יצירות אשר הן בתורן מוגנות על-ידי דיני זכויות יוצרים. האיסור על-פיענוח הגנות טכנולוגיות איננו מוגבל לטכנולוגיות מקומיות (אמריקניות), ולפיכך גם פיענוח של טכנולוגיה מוגנת שמקורה מחוץ לארצות-הברית היא הפרה של האיסור שבחוק. החוק קובע עוולה אזרחית, אולם במקרה שההפרה בוצעה לצורך מסחרי או רווח כספי הרי היא גם עבירה פלילית.[123] החוק קבע מספר הגנות כלליות, ומביניהם נציין את ההגנה על פעולות לצורכי מחקר, בדיקה והערכה של אמצעי הגנה:

- החוק אינו מפקיע את סמכות הממשל, מערך המודיעין וגופי האכיפה לפעול לצורכי חקירה, הגנה, אבטחת מידע ומודיעין.[124]
- ישנו חריג המאפשר לפצח הגנות על אמצעי גישה טכנולוגיים, לצורכי מחקר ולשם מציאת פגמים בטכנולוגיות הצפנה.[125] החריג הוכנס בשל חשש של המחוקק, שהאיסור על-פיענוח אמצעי גישה יבלום את התפתחות המחקר ומציאת הפגמים בטכנולוגיות קיימות.[126]
- הגנת שימוש הוגן אינה מכשירה פיענוח בניגוד להוראות הסעיף.[127]

ההליך הפלילי הראשון בגין חוק זה התנהל נגד אזרח רוסי, דמיטרי סקליירוב,[128] אשר פיתח תוכנה שעוקפת את ההגנה הטכנולוגית של eBook, השייך לחברת Adobe.[129] התוכנה פותחה עבור

[122] 17 U.S.C. §1201(b)(1).
[123] 17 U.S.C. §1204 (a).
[124] 17 U.S.C. §1201(e).
[125] 17 U.S.C. §1201(g).
[126] ראו את דוחות הוועדות השונות בקונגרס: H.R. Rep. No. 105-551, pt. 2, at 27 (1998); S. Rep. No. 105-190, at 15 (1998). המחוקק דרש לקבל דיווח, שנה לאחר כניסת החוק, האם החוק אכן השפיע לרעה על מחקר הצפנות. לפי הדיווח מוקדם להסיק מסקנות. ראו: http://www.loc.gov/copyright/reports/studies/dmca_report.html#N_12_.
[127] 17 U.S.C. §1201(c).
[128] לפרטים על מקרה זה, ראו: http://www.eff.org/IP/DMCA/US_v_Sklyarov/ .
[129] http://www.adobe.com/products/ebookreader/overview1.html.

חברת ElcomSoft[130] הרוסית, אשר גם היא נתבעת. בדצמבר 2001 נחתמה עיסקת טיעון, והתביעה ויתרה למעשה על העמדתו לדין של סקליירוב מבלי שיורשע.[131]

החוק זכה עד כה לפרשנות במסגרת מספר הליכים אזרחיים:

- חברות סרטים תבעו למנוע מאתרים את הפצתו של קוד אשר פיצח את ההגנה הטכנולוגית של סרטי DVD. טענות בדבר שימוש הוגן ואי חוקתיות ה DCMA בשל היותו מגביל, במידה רבה, את חופש הביטוי – נדחו בערכאה הראשונה ובערכאת הערעור.[132]
- בתביעה נוספת, שגם היא עסקה בשאלת ההצפנה של ה DVD, דן בית משפט מדינתי בקליפורניה בשאלת הפיענוח תחת המסגרת המשפטית של דיני סודות מסחריים.[133] בהליך ביניים, הוסר צו המניעה שאסר להפיץ את הקוד המפענח באתרי אינטרנט. עוד נאמר שם:

"DVDCCA's [The Plaintiff] statutory right to protect its economically valuable trade secret is not an interest that is "more fundamental" than the First Amendment right to freedom of speech or even on equal footing with the national security interests and other vital governmental interests that have previously been found insufficient to justify a prior restraint."[134]

- פרשה נוספת נגעה לחוקר שביקש לפרסם את מחקרו, ונתקל באיום על-פי ה-DMCA. פרופ' פלטן פיצח את ההגנה הטכנולוגית של "סימני מים" (watermarks) דיגיטליים במסגרת תחרות ציבורית של מפתחי ההגנה. פלטן ויתר על הפרס וביקש לפרסם את תוצאות המחקר. אולם לטענתו, תעשיית המוסיקה (ה- RIAA) איימה לתבוע אותו לפי ה DMCA. פלטן פנה לבית המשפט, בבקשה לפסק דין הצהרתי שיכיר בזכותו לפרסם את המחקר כחלק מחופש הביטוי שלו. בית המשפט המחוזי בניו ג'רזי דחה את התביעה,[135] ותעשיית המוסיקה הצהירה כי אינה מתנגדת לפרסום.[136]

---

[130] ראו את אתר החברה: www.elcomsoft.com.

[131] סקליירוב התחייב להעיד נגד אלקומסופט. את אישור בית המשפט להסדר הטיעון ניתן למצוא באתר משרד המשפטים האמריקני: http://www.usdoj.gov/usao/can/press/assets/applets/2001_12_13_sklyarov.pdf .

[132] ראו: *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), aff'd *Universal City Studios, Inc. v. Corley* 2001 WL 1505495 (2nd Cir. 2001). עוד בסוגיית חופש הביטוי, ראו להלן, חלק ה.4 בפרק זה.

[133] Trade Secret Act, Cal. Civ. Code, § 3426.1 et. seq.

[134] *DVD CCA v. Bunner* 93 Cal. App. 4th 648 (2001).

[135] *Felten v. RIAA* (D.N.J.).

[136] http://www.wired.com/news/politics/0,1283,48726,00.html.

המגמה המסתמנת במשפט האמריקני היא של הטלת איסור על-פיענוח הצפנות המגנות על יצירות המוגנות בזכויות יוצרים. טרם ניתן להגיע למסקנה באשר לאיסור על-פיענוח במסגרת ההגנה על סוד מסחרי. על רקע דברי בית המשפט, המובאים לעיל, לפיהם ההגנה על סוד מסחרי בעל ערך כלכלי אינה בסיסית יותר מאשר הגנה על חופש הביטוי, יש לתהות האם ההגנה על זכויות יוצרים היא בסיסית יותר מחופש הביטוי והאם הגישה לפיה האיזון בין חופש הביטוי לדיני זכויות היוצרים מתמצה בהסדרים שבחוק זכויות יוצרים היא סבירה?

<u>האיחוד האירופאי</u>

בהחלטת האיחוד האירופאי- **Council Decision of 16 March 2000, on the approval on behalf of the European Community of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty**, אישרה מועצת השרים בשם האיחוד האירופאי את שתי האמנות מבית היוצר של הארגון הבינלאומי לקניין רוחני (WCT, WPPT שנדונו לעיל), וכן הסמיכה את הנציבות לפעול בנושא ברמות שונות כמייצגת האיחוד האירופאי. בהתאם להחלטה זו, האיחוד האירופאי ככזה, יוכל לראשונה להפוך לצד לאמנות ארגון WIPO בתחום זכויות יוצרים וזכויות שכנות.

European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.[137]

מטרת הדירקטיבה היא אימוץ חקיקה ביחס לזכות היוצרים וזכויות שכנות באופן שישקפו את ההתפתחויות הטכנולוגיות ובמיוחד את עידן המידע, וכן להכניס לתוך משפט הקהילה את האמנות מבית WIPO כפי שנדונה לעיל. הדירקטיבה עוסקת בשלושה תחומים עיקריים: זכות ההעתקה, זכות השידור והעברה בפומבי וזכות ההפצה.

לענייננו חשובה ההגנה המשפטית אותה מחויבות המדינות החברות להעניק כנגד עקיפת אמצעים טכנולוגים אפקטיבים החוסים על היצירה. בנוסף ההגנה המשפטית מתייחסת לפעולות מכינות כגון יצור, יבוא, הפצה, מכירה או הספקה של שירותים ליצירות עם שימושים מוגבלים. הגנה נוספת היא על זכויות בניהול המידע (management information) דהיינו מידע אודות היצירה, בעלי הזכויות ורשיונות השימוש. הדירקטיבה מקנה הגנה משפטית לאמצעי ההגנה הטכנולוגיים שננקטו, מפני שינוי או עקיפה בלתי מורשים.[138]

<u>בריטניה</u>

החוק הבריטי **Copyright, Designs and Patents Act 1988**, קובע בסעיפים 296-297 איסור על-פיתות, יבוא, מכירה, השכרה ופרסום כל מכשיר או אמצעי המיועדים לעקוף הגנה על עותק של יצירה מוגנת. האיסור הרחב כולל פרסום מידע המסייע לפרסום פעולות עקיפה מעין אלה. בנוסף, החוק אוסר פיענוח בלתי-מורשה.[139]

---

[137] **OJL** 167, (22.06.2001).

[138] http://europa.eu.int/scadplus/leg/en/lvb/l26053.htm

[139] ראו: **E-commerce: A Guide to the Law of Electronic Business**, supra note 115, at 70.

עוד יש להזכיר פסק-דין בריטי מהעת האחרונה **Mars UK v. Teknowledge Ltd**.[140] פסק-הדין עסק בתביעה על הפרת סודיות באמצעות הנדסה חוזרת, למכשיר שהכיל מידע מוצפן. בהתאם לדרישות שפותחו בפסיקה קודמת,[141] מצא בית המשפט שהמידע המוצפן לא היה סודי היות שהמכשיר (cashflow) היה זמין לציבור, וכן לא היו נסיבות מיוחדות שכפו מחויבות של סודיות. החשיבות היא לעובדה שדובר במכשיר זמין, ומכאן ניתן לומר כי כאשר מדובר בתשדורת של מידע מוצפן, שאינו זמין, קיימת אפשרות לקבוע כי מדובר במידע סודי. פסק-הדין מבהיר כי הצפנה לכשעצמה אינה הופכת חומר מוצפן לסודי כאשר אין יחסים אחרים שמחייבים זאת בין המקור למפענח.[142]

ב. גישה מותנית

אמצעי שני בו נעשה שימוש על-מנת להגן על המידע שנחשב מוגן, וכתוצאה מכך מגן על שיטות הצפנה ומגביל פיענוח, הוא הגנה משפטית על שירותים טכנולוגיים המבוססים על הגבלת הגישה לתוכן. דירקטיבה אירופית משנת 1998 קובעת חקיקה אחידה ביחס להליכים כנגד מיכשור או שירותים המעניקים גישה לא-מורשית לשירותים מוגנים כגון טלויזיה, רדיו, כבלים, לווין, פרסום אלקטרוני וכיוצא באלה שירותים הנתנים לציבור על בסיס של מנויים או תשלום בעבור צפיה.[143] מכשור לא-חוקי מוגדר ככל ציוד או תוכנה שמיועדת להעניק גישה לשירות מוגן (סעיף 2(e)). פעולה מפֵרָה תחשב יצור, יבוא, הפצה, מכירה, השכרה ובעלות לצרכים מסחריים של מכשור לא-חוקי. כמו כן יש לאסור התקנה, תחזוקה או החלפה למטרות מסחריות של מכשור לא-חוקי. על המדינות באיחוד חל איסור להגביל את ההגנה הניתנת לשירותים מותנים שמקורם במדינה אחרת באיחוד, וכן חל איסור להגביל את התנועה החופשית של מכשירי גישה מותנית, מלבד אלה שהוגדרו כלא-חוקיים. על המדינות היה להתקין חקיקה פנימית בהתאם להנחיות הדירקטיבה עד לתאריך 28.05.00.[144] אנגליה, למשל, יישמה את הדירקטיבה במסגרת ה- Copyriht, Design and Patents Act 1988 (CDPA).[145]

ראוי לציין כי למרות הגדרותיה הרחבות של הדירקטיבה לא ברור האם סיסמאות שהושגו שלא-כדין ייחשבו כ- "illicit devices", היות שסיסמה אינה בהכרח ציוד וגם לא תוכנה המיועדת להעניק גישה לשירות המוגן.[146]

ג. מאגרי מידע

---

140 **Mars UK v. Teknowledge Ltd** [2000] FSR 138.

141 **Coco v. AN Clark** [1969] RPC 41.

142 **E-commerce: A Guide to the Law of Electronic Business**, supra note 115, at pp. 63-64.

143 ראו: **Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJ L 320, 28/11/1998 P. 0054-0057**, נמצא ב: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31998L0084&model=guichett

144 http://europa.eu.int/scadplus/leg/en/lvb/l26050.htm

145 ראו סעיפים 297-298A, והסבר: ב: ALAI 2001 Congress Questionnaire, http://www.law.columbia.edu/conferences/2001/Reports/uk_ic_en.doc (ביקור אחרון: אפריל 2002).

146 **E-commerce: A Guide to the Law of Electronic Business**, supra note 115, at 71.

אמצעי שלישי באמצעותו מוגנת ההצפנה - באופן שקיים איסור משפטי על הפיענוח - הוא באמצעות ההגנה הניתנת למאגרי-מידע. באיחוד האירופאי קיימת דירקטיבה להגנה על מאגרי מידע המספקת הגנה כאמור – **Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases**.[147]

הדירקטיבה יוצרת זכות קניין רוחני חדשה, במסגרת נפרדת מדיני זכויות היוצרים המסורתיות, ביחס למאגרי מידע שהושקעו בהם השקעה ניכרת מבחינת כמות או איכות (להבדיל מיצירתיות ומקוריות הנדרשים כתנאי להגנה בזכויות יוצרים), ואוסרת על הוצאת מידע או שימוש אחר בחלק שאיכותית או כמותית יחשב משמעותי (סעיף 7(1)). בדירקטיבה זו נקבע איסור על הוצאת מידע ממאגר-המידע בכל דרך ובכל פורום למשך תקופה של 15 שנים, כך שיש בה מעין איסור על-פיצוח המידע. הגנות השימוש ההוגן ביחס לזכות זו צומצמו והם מהוות רשות ולא הגנות חובה. ההגנות מתירות שימוש פרטי שלא למטרות יצירת מאגר אלקטרוני, למטרות לימוד ושימוש לשם ביטחון הציבור או הליך משפטי (סעיף 9). ההגנה האחרונה - חריג ספציפי המיועד <u>לצורכי ביטחון הציבור</u> – מתירה הוצאת מידע ממאגר-מידע לשם צורכי הביטחון, ופעולה לא תחשב הפרה של זכות הקניין הרוחני ככל שהיא קיימת במאגר (זאת בנוסף לזכות היוצרים במאגר ביחס לסידור ולארגון כל עוד הם עונים על דרישת המקוריות).[148]

ה. השלכות ושיקולי מדיניות

לאחר שהכרנו את מהות ההצפנה מבחינה טכנולוגית, יכולתה ומגבלותיה, את הצרכים הבטחוניים הכרוכים הן במוטיבציה להצפין והן במוטיבציה למנוע (מאחרים) להצפין, וסקרנו את ההסדרה המשפטית הקיימת בארץ ובעולם ביחס לנושא ההצפנה והפיענות, היקפה ומגמותיה, נותר לתת את הדעת לאותם שיקולים אשר יהוו קווים מנחים לגיבוש מדיניות ראויה בתחום זה. שיקולים אלו כוללים מלבד שיקולי ביטחון אשר מניעים את ההסדר כולו, גם שיקולים כלכליים, הן במובן הצר (שוק אמצעי ההצפנה או הסחר האלקטרוני) והן במובן הרחב (עצם ההתערבות בשוק החופשי), וכן שיקולים מתחום זכויות האדם, החל מהזכות לפרטיות וחופש הביטוי, וכלה בזכות לקניין ולחופש העיסוק. בחינת מגוון השיקולים באופן ממוקד ולעומקם, תספק דווקא בסיכום הדיון נקודת מבט רחבה, ותסייע בגיבוש קווי מדיניות להסדר המשפטי הרצוי.

<u>1. התערבות בשוק ושיקולי מחקר ופיתוח</u>

<u>א. השפעת התערבות ממשלתית על תחומי מחקר ופיתוח</u>

בתחום ההצפנה (והמחשבים בכלל) יש לפיתוח תמידי משמעות כלכלית מרחיקת לכת. חברות בתעשיית ההיי-טק חייבות לחדש ולעדכן את מוצריהן כל הזמן על-מנת לעמוד בתחרות (מדובר על

[147] ראו: OJL 77 (27.03.96).

[148] http://europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=1996&nu_doc=9&type_doc=Directive

ממוצע של 18 חודשים בלבד בין מוצר למוצר), והדבר נכון במיוחד כאשר מדובר בשיטות הצפנה והגנה על מערכות, מאחר שבמקביל לפיתוחן מתפתחים כל הזמן האמצעים לפריצתן.

לעוסקים בתחום במגזר הפרטי, יש אינטרס מובן וברור לפתח את מוצריהם ללא הגבלה ובהתאם לדרישות השוק. עם זאת, בשל קיומם של אינטרסים אחרים (שעל חלקם עמדנו לעיל, כמו ביטחון, ועל חלקם נעמוד בהמשך, כמו פרטיות וחופש מידע) מתעוררת הדילמה של היקף הרגולציה הדרושה בתחום זה. השאלה אותה יש לבחון בהקשר של מחקר ופיתוח הינה, מה תהיה ההשפעה הכלכלית של הרגולציה על תמריצי החברות הפרטיות, והאם הדבר רצוי להן ולמשק בכללותו.

ב. הגבלות על ייצוא אמצעי הצפנה ועל השימוש בהם

גישה זו של אי-התערבות ממשלתית, היא הגישה הרצויה בעיניה של התעשייה, ולא רק בתחום של מחקר ופיתוח. התייחסות לנושא זה ניתן למצוא בהקשר של רגולציה הנוגעת להצפנה באופן כללי, ובפרט לגבי האפשרות של הגבלת ייצוא אמצעי הצפנה. בארצות הברית, בתקופה בה ההגבלות היו מחמירות יותר, יצאו כנגדן חברות המחשבים וקראו לרפורמה בתחום, וזאת בטענה כי ההגבלות גורמות לפגיעה כלכלית חמורה בחברות האמריקניות. כך למשל, ה- CSPP (Computer Systems Policy Project)[149] קרא לשינוי המדיניות ולפתיחת הגבולות, באשר הגבלת הייצוא פגעה ביכולתן של החברות האמריקניות להתמודד כראוי בשוק העולמי ולעמוד בתחרות.

רגולציה בתחום ההצפנה יכולה להתבטא (בנוסף להגבלות בייצוא) באיסורים שונים לגבי שימוש בהצפנה שלא על-ידי הרשויות, או בהגבלות על מידת הפיתוח המותרת בתחום. מאחר שתחום פיצוח ההצפנה מתפתח כל העת (ויוסיף להתפתח גם במידה שהדבר ייאסר, על-ידי גורמים שאינם שומרי חוק) המשמעות של שני מצבים אלה דומה: גופים פרטיים ואנשים פרטיים לא ייהנו עוד מאבטחת מידע.

Koops[150] דן באפשרות הטלת האיסור על הצפנה. לדבריו, כאשר מתעוררת בעייתיות כלשהי בחברה כתוצאה מגורם מסוים, הנטייה הטבעית של המדינה היא להוציא אל מחוץ לחוק את אותו גורם. הדבר הגיוני כאשר מדובר בגורם או בפעילות שכל תוצאותיה והשפעותיה הן שליליות (כמו רצח), אולם להצפנה יש גם צדדים חיוביים רבים. לכן, לדעת Koops הוצאת ההצפנה מחוץ לחוק כלל איננה מהווה אפשרות של ממש. עם זאת, האופציה של איסור הצפנה עלתה לדיון במספר ממשלות בעולם, ולכן הוא בוחר להתייחס לכך בכל זאת.

איסור יכול שיהיה מוחלט, או חלקי (התרת הצפנה ברמה לא גבוהה, או לגורמים מסוימים בלבד). אולם בכל מקרה מדובר באיסור שאיננו בר-אכיפה, וייווצר מצב שבו דווקא גורמים פליליים וטרוריסטיים הם אלה שימשיכו לעשות שימוש בהצפנה. אלו שיושפעו מן האיסור הם אזרחים שומרי חוק, כאשר מעבר לפגיעה האינדיבידואלית (מבחינת פרטיות, ויחסי הכוחות בין האזרח לשלטון), תהיה תוצאה נוספת של פגיעה קולקטיבית, אשר תתבטא בנזק כלכלי: סחר בינלאומי ייפגע מאחר שחברות לא יוכלו לתקשר אלה עם אלה בביטחון. בנוסף, אם האיסור הוא רק מדינתי ולא ייאכף ברמה גלובלית, חברות ממדינות שבהן קיים איסור לא יוכלו לעמוד בתחרות עם חברות ממדינות אחרות – וכלכלתן של אותן מדינות המגבילות הצפנה, תיפגע בצורה אנושה.

---

[149] http://www.cspp.org/Reports.asp?FormMode=Call&LinkType=Text&ID=9565291994

מסיכום ההשפעות השונות עולה, כי רגולציה מכל סוג שהוא בנושא ההצפנה, לא תועיל מבחינה כלכלית. התיאוריות הכלכליות השונות מבהירות כי השוק פועל בצורה הטובה ביותר כשוק חופשי, ללא התערבות. התמונה משתנה כמובן כאשר קיימים כשלי שוק, אז דרושה לעיתים התערבות ממשלתית. השאלה היא אם אקטים טרוריסטים המוסתרים על-ידי הצפנה, ופיצוח הצפנה על-ידי גורמים עוינים, מהווים כשלי שוק מעין אלה, המצריכים (מן הבחינה הכלכלית הטהורה) התערבות. נראה כי לדעת תעשיית המחשבים - ואף לדעת גורמים בינלאומיים - התמודדות עם הבעיה תיעשה בצורה הטובה ביותר על-ידי המשך פיתוח הגנות בתנאי שוק תחרותיים.

2. השפעתה של רגולציה בתחום ההצפנה על המסחר האלקטרוני

השפעה כלכלית נוספת שעשויה להיות להגבלות על ההצפנה, היא בתחום המסחר האלקטרוני. על-פי התיאוריה של Schilling,[151] המתבססת על ניתוח כלכלי לפי תורת המשחקים, במצב שבו מידת הרגולציה תעלה, תרד רמת השימוש באינטרנט של המשתמש הפרטי. זאת, למרות שיש לציבור אינטרס במניעת פשע ומעשי טרור. שכן ברמת רגולציה גבוהה המגבילה את אפשרויות ההצפנה הקיימות בשוק, וללא הצפנה חזקה המגינה על פרטיותו, אין המשתמשים מרגישים בטוחים מספיק, ולפיכך יעדיפו להימנע מהפעילות המסחרית. טענה דומה הועלתה גם במסמך שהוגש לממשל האמריקני על-ידי EPIC (Electronic Privacy Information Center), במסגרת תגובות מן הציבור לגבי המדיניות הרצויה בנושא מסחר אלקטרוני.[152] על-פי המלצות מסמך זה, ראוי שהממשל יימנע מהתערבות רגולטורית בתחום ההצפנה, ויאפשר לשוק לפתח אמצעי הצפנה חזקים, שכן רק מגמה כזו תביא לעידוד השימוש באינטרנט באופן כללי, ובנטילת חלק במסחר אלקטרוני בפרט. המשמעות היא כי התחום המתפתח של מסחר אלקטרוני, שהינו מכשיר כלכלי יעיל ורצוי, ייפגע באופן ישיר וייאבד את יעילותו, במידה שהמדינה תטיל הגבלות רחבות בנושא ההצפנה.

3. הזכות לפרטיות

הצפנה הינה אמצעי אשר במישור המושגי מגן על פרטיות המשתמש. הצפנה ומערכות הצפנה מהוות מעין דלתות ומנעולים בסביבה הדיגיטלית, המגנים על יותר ויותר מידע אישי, תכתובות

---

150 Bert-Jaap Koops, **The Crypto Controversy: A Key Conflict in the Information Society** 125-131 (1999).

151 Thorsten Schilling, "Raiding the Net: Is There a Need for an Information Highway Patrol?" 1 **Netnomics** 37, 51 (1999).

152 ראו: Public Comment on Barriers to Electronic Commerce- Comment on Behalf of Electronic Privacy Information Center (EPIC) by Sarah Andrews, Policy Analist, Andrew Shen, Policy Analist (17.3.00), available at http://osecnt13osec.doc.gov/ecommerce/barriers.nsf/review/46112999BDD282C9852568A6000093AF.

דואר אלקטרוני, מסחר אלקטרוני ואלמנטים נוספים אשר ניתן להסיק מהם מידע הנחשב בגדר רשות הפרט.[153]

הצפנה אינה מבחינה בין סוגי משתמשים ואופני שימוש, ורמת ההצפנה הינה אחידה, לטוב ולרע, אצל המשתמש התמים ואצל הפושע או הטרוריסט. אם נמתח את מטאפורת הדלתות והמנעולים מעט, הרי שלמרות שעיקרון הפרטיות (כמו גם הזכות הקניינית שתדון בהמשך) יתמוך בוודאי בעובדה שלכל פרט זכות להגן כמה שיותר על המידע הפרטי הנוגע לו, הרי שלא כל אדם יכול לבנות כל גדר, להתקין כל מנעול או קו טלפון אשר יחפוץ. ישנם תמיד מנגנוני פיקוח - החל מייצור מנגנוני ההגנה, התקנתם, תקינותם - וכלה בשיווקם. הסיבות לכך הן רבות ומשתנות מתחום לתחום. באופן מופשט, על הרגולציה לקחת בחשבון את מקרי הקיצון בחברה ולא את האזרח התמים. לענייננו - את הטרוריסט אשר בעידן הטכנולוגיה ישתמש בתכתובות אלקטרוניות וכן באמצעים אחרים המוגנים בהצפנות בדיוק כפי ש"הטרוריסט הישן" השתמש באמצעים פיזים המוגנים באופן פיזי כזה או אחר. גם באשר לאמצעים מהעידן הישן (אם ניתן לקרוא להם כך) וגם באשר לאמצעים המודרניים, צריכות להיות (וישנן) דרכים לפרוץ, מעין "דלת אחורית", המוחזקת בידי רשויות השלטון – המדינה.

למרות הקבלה זו, המייחד את אמצעי ההצפנה הוא, שהם מיועדים מלכתחילה להסתיר ולכן לא די במתן אישור פרטני לשם פיענוח הצפנה מסוימת (כפי שנעשה במקרה של ציתות לקו הטלפון למשל), אלא יש לדאוג מבעוד מועד לכך שתהיה בכלל אפשרות טכנולוגית לפענח את ההצפנה. בכך, הרגולציה נוגעת לא רק למשתמש או למשתמש פוטנציאלי (אפקט מצנן), אלא נוגעת באופן ישיר לכלל האוכלוסיה. ההסדרה של אמצעי ההצפנה עוד הרבה לפני שלב השימוש בהם – בשלב הייצור, היבוא, והמסחר בהם למשל - משפיעה על כלל האזרחים כפרטים וכן על סקטורים שלמים במשק העוסקים בייצור ושיווק אמצעי הצפנה.[154] דיון ממושך התקיים בנושא זה בארצות הברית, ובו השאלה העיקרית היתה האם ועד כמה לאפשר למוסדות הממשל, תחת מגבלות שונות (אישור בית המשפט, חלוקה לשני מוסדות שונים אשר יחזיקו במפתח משותף ועוד), להחזיק באפשרות השימוש ב"דלת אחורית", קרי להחזיק במעין "מפתח מאסטר" או באלגוריתם המאפשר את שיחזור המפתח הפרטי. ברור שככל שרמת הפיקוח והשליטה על הייצור המקומי ויבוא אמצעי ההצפנה תגדל, כך למדינה תהיה אפשרות כניסה דרך "דלתות אחוריות" בדרכים שונות ופגיעה אפשרית בפרטיות האזרח.

ניתן להציג את הפגיעה בפרטיות האזרח הנובעת ממתן שליטה למדינה על מנגנוני ההצפנה ("דלת אחורית") בשני מישורים: פגיעה ישירה ופגיעה עקיפה.

פגיעה ישירה - מתן אפשרות טכנית וחוקית, ולו גם במקרים חריגים, להתערב ולפענח הצפנות ובכך לחדור מבעד לאותן דלתות ומנעולים - יש בה כדי לפגוע במקרים מסוימים באזרח שומר החוק אשר איננו אפילו בגדר חשוד. למשל, כאשר מכורח הנסיבות מתעורר צורך לעבור דרכו או

[153] סעיף 2 לחוק הגנת הפרטיות, התשמ"א-1981 מפרט מהי פגיעה בפרטיות, וניתן ליישם את ההוראה גם לסביבה הדיגיטלית. כך למשל סעיף 2(5) מגדיר העתקה או שימוש בתוכן של מכתב או כתב אחר שלא נועד לפרסום כפגיעה בפרטיות. ניתן לכלול בהגדרה זו גם דואר אלקטרוני. בנוסף ישנו איסור חדירה לחומר מחשב שלא כדין בסעיף 4 לחוק המחשבים, התשנ"ה-1995.

דרך תכתובותיו (למשל דרך שרת האינטרנט המשרת אותו ואלפי אזרחים תמימים, אך גם טרוריסטים). פגיעה כזו נוספת לפגיעה האינהרנטית הטמונה בחקירה המשטרתית המכוונת מטבעה כנגד חפים מפשע אשר טרם הוכחה אשמתם והפגיעה במקרה של טעות.

<u>**פגיעה עקיפה**</u> - **עצם השליטה** על אמצעי ההצפנה (האפשרות לפענח) וקיומה של דלת אחורית כזו, עוד בטרם ישנה התערבות כלשהי, וגם אם אין כלל התערבות כזו, יוצרת הרתעה בקרב הציבור: היא עלולה להוות גורם מצנן אשר ירתיע אנשים משימוש במאגרי מידע דיגיטליים, שירותים מכוונים, מסחר אלקטרוני ועוד, דבר אשר יש לו השפעה פרטית, ציבורית וכלכלית.

יש אם כן ליישב בין הזכות לפרטיות הנתונה לכל פרט ופרט לבין האינטרס הציבורי, ולפעול בשני מישורים המקבילים לשני האיומים על הפרטיות.

לפיכך אנו סבורים שיש לנהוג כאמור להלן:

לגבי הפגיעה הישירה: יש לנקוט אמצעים אשר יאפשרו לרשויות הביטחון לממש את צורכי המודיעין, במידה שאינה עולה על הנדרש.

- **יש להגדיר את המטרה שלשמה מותרת הפגיעה בפרטיות בצורה ברורה ומפורשת, ולצמצם אותה לצורכי סיכול טרור בלבד, ולא להתיר אותה לשם השגת ראיות לאחר שהאירוע התרחש (אלא אם יש חשש להישנות מעשי הטרור, שאז מדובר על סיכול).**
- **יש לקבוע מנגנון של ביקורת חיצונית בלתי-תלויה, ורצוי כי זאת תהיה ביקורת שיפוטית מוקדמת, בדומה להסדר הקיים באשר להאזנות סתר. מוצע לקבוע כי רשות המבקשת לחדור מבעד ל"דלת אחורית" או לפצח הצפנה תפנה לבית המשפט לפני הביצוע, ובית המשפט יוכל לשקול את מידת הצורך בחדירה או בפיצוח מול הפגיעה הישירה הצפויה מהם.**

לגבי הפגיעה העקיפה, יש להגדיר את מידת ההתערבות של המדינה בייצור ויבוא של אמצעים טכנולוגיים, ובכך לקבוע עד כמה ניתנת לה האפשרות להשיג גישות ל"דלתות אחוריות". ככל שההסדר הכללי בנוגע להצפנה יהיה מצומצם יותר, בהיר ומפורש יותר, תצטמצם ממילא הפגיעה העקיפה בפרטיות.

עוד יש להעיר שדווקא אי-מתן אפשרות פיענוח ("דלת אחורית") מספקת או קביעת קריטריונים והליכים נוקשים מדי לשם פיענוח ספציפי בפועל, עלולים דווקא להביא לתוצאה הפוכה, ולפגוע יותר בזכות לפרטיות של החשודים ואף לא רק בהם. כך למשל, במקום לפצח את תכתובות

[154] כפי שמוסדר למשל בצו הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) (תיקון), התשנ"ח-1998.

הדואר האלקטרוני, ישתמשו רשויות האכיפה במצלמות או במעקב אנושי, שפגיעתם מקיפה יותר וממוקדת פחות בפרטיות החשוד.[155]

4. חופש הביטוי

את הקשר בין הצפנה לחופש ביטוי ניתן להבין בשני אופנים. האופן הראשון – ישיר, מבקש לומר כי הצפנה בעצמה היא ביטוי ולכן ראויה היא להגנה במסגרת חופש הביטוי.[156] לפי גישה זאת, כל הגבלה על הצפנה מגבילה בהכרח גם את חופש הביטוי. האופן השני – עקיף – בהיעדר יכולת הצפנה חזקה, עשויים גולשים (וגם חברות וגופים ממשלתיים) להימנע מביטוי, מחשש שפרטיותם תיפגע. לפיכך, להיעדרה של הצפנה חזקה ולרגולציה של הצפנה שמעוררת את החשד כי למדינה יש יכולת נגישות למידע מוצפן, יש אפקט מצנן על הביטוי. האופן העקיף ידון על-ידינו בתת הפרק הדן בפרטיות. כאן נתמקד בשאלת תחולתם של עקרונות חופש הביטוי על הצפנה.
השאלה הראשונה המתעוררת היא האם תוכנה היא ביטוי? אם כן, מהו היקף ההגנה לה זוכה תוכנה במסגרת ההגנה על חופש הביטוי? הקושי היסודי הוא שבתוכנה יש שני מרכיבים: אחד הוא מרכיב ביטויי, והשני הוא מרכיב פונקציונאלי - כאשר אדם יוצר תוכנה שבאמצעותה הוא מנסה לפרוץ למחשב ממשלתי, למשל, או לגרום לקריסת מערכת מחשבים ממשלתית, ובמעשהו זה אותו אדם מנסה להביע מחאה כלשהי, לא קל להכריע האם התנהגות זו חוסה תחת כנפי עקרון חופש הביטוי.

השאלות התעוררו עד כה בארצות הברית בשני הקשרים הנוגעים להסדרת הצפנה: באשר לתוכנת ההצפנה עצמה, ובאשר לתוכנות פיצוח של הצפנה. המשפט האמריקני החיל בסוגיה זאת את הדוקטרינות שפותחו בו באשר ל"התנהגות סימלית", עוד בימים כשההתמודדות עם הסוגיה היתה בסיטואציות פחות "טכנולוגיות". הכוונה היא לסיטואציות בעלות אותם יסודות, כמו מקרה בו אדם שורף את דגל המדינה ברשות הרבים, כדי למחות נגד מדיניות הממשלה, או כמו המקרה שנזדמן בשנות השישים של המאה העשרים לבית המשפט העליון האמריקני, בפרשת **O'Brien**.[157] O'Brien ואחרים שרפו בפומבי את צווי הגיוס שקיבלו. לדבריהם, עשו זאת כמחאה נגד מלחמת וייטנאם. אובריאן נעצר והועמד לדין באשמת שריפת צו הגיוס, לפי חוק משנת 1965. בית המשפט העליון פסק, שלא ניתן לקבל את הטיעון שכל התנהגות או פעולה יכולות להיחשב לביטוי, כאשר בוצעו במטרה להביע רעיון או עמדה כלשהי. יתרה מכך, בית המשפט ניתח מצב בו פעולה (התנהגות) וביטוי שלובים זה בזו, והגיע למסקנה, שאפילו אם המרכיב של הביטוי בתוך ההתנהגות הינו "speech" כמובנו בתיקון הראשון לחוקה, הרי שאינטרס מדינתי חשוב בהסדרת

---

[155] נקודת מבט שונה מעלה פרופסור מייקל פרומקין, אשר בודק את ההצפנה עצמה, עוד בטרם ישנה התערבות שלטונית כלשהי. פרומקין טוען שגם אם משתמשים בשיטת ההצפנה, הרי שהיא עצמה מגלמת בתוכה פגיעה בפרטיות בשני אופנים: 1. אין מדובר בשני צדדים בלבד. ישנו כעת גורם המנפיק מפתח ציבורי ופרטי. 2. כאשר רוצים לשחזר מפתח ציבורי, יש למסור פרטים אישיים מסוימים כדי לעשות זאת (כוונתו היא לשיחזור על-ידי השלטונות ולא על-ידי בעלי המפתח). נקודת מבט זו אינה קשורה לשני האיומים על זכות הפרטיות שבהם דנו (הקשורים באופן הדוק לפעולת השלטונות) אלא קשורים לפגיעה האפשרית בזכות זו על-ידי מנגנון ההצפנה עצמו או יצרני אמצעי ההצפנה. ראו: Michael Froomkin, "It Came form Planet Clipper : The Battle Over Cryptographic Key 'Escrow'" 1996 **U. Chi. L. Forum** 15. נמצא ב: http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm.

[156] Amitai Etzioni, **The Limits of Privacy** 80, 90 (New York, 1999).

ה- "non-speech element" בתוך ההתנהגות, עשוי להצדיק את הגבלת חופש הביטוי. משמע, אין להיזקק לסטנדרט המוחלט של הגנה על חופש ביטוי, כפי שנעשה כאשר יש מניעה של ביטוי טהור על בסיס תוכנו, אלא די בסטנדרט מעט נמוך יותר, המכונה "intermediate scrutiny".[158] נשיא בית המשפט, Warren, קבע לשם כך מספר תנאים, שבהתקיימם, הסדרה ציבורית, שתגביל את התיקון הראשון לחוקה תהיה מוצדקת:

(1) ההסדרה היא בסמכותה החוקית של הממשלה;

(2) ההסדרה מקדמת אינטרס ממשלתי/ממלכתי חשוב;

(3) ההסדרה אינה קשורה לדיכוי של חופש הביטוי;

(4) הפגיעה האגבית בחופש הביטוי אינה עולה על הנדרש לקידום האינטרס הממלכתי.

באותו עניין נפסק, שהחוק בו דובר לא נועד לצמצם את הביטוי או לפגוע בו, אלא לשמר את האפקטיביות של שיטת הגיוס (זהו האינטרס הממלכתי), וכן, ש- O'Brien לא הועמד לדין בשל דעותיו, אלא בגלל התנהגותו, שפגעה באינטרס הממלכתי.

באשר לתוכנות הצפנה: התעוררה השאלה, האם ניתן לאמץ את הלכת O'Brien גם בהקשר זה. בתי המשפט האמריקנים התקשו לשמור על אחידות בענין זה.

המקרה הראשון ידוע כפרשת **Karn**: פיליפ קארן, מתכנת שעסק בטכנולוגיה סלולרית, ביקש היתר לייצא קוד מקור של אלגוריתמים של הצפנה על גבי דיסקט, אשר פורסם זה מכבר עלי ספר.[159] בעוד שהספר הוכרז על-ידי ה- Department of State וה- Department of Commerce כמוצר הניתן לייצוא חופשי (freely exportable), הוחלט על-ידי אותם הגורמים, שהייצוא של הקוד בפורמט דיגיטלי אסור בהתאם לתקנות המסדירות את ייצוא תוכנות ההצפנה. קארן ערער על החלטת הממשל בפני בית המשפט המחוזי ב District of Columbia.[160] טענתו היתה שהדיסקט נשוא התביעה מהווה ביטוי, במיוחד עקב כך שבקוד התוכנה משובצות הערות של המתכנת, שלא נועדו למחשב המפעיל את התוכנה, אלא לאדם הקורא את הקוד ומנסה להבינו; והואיל ומדובר בביטוי, אזי הדיסקט חוסה תחת ההגנה שניתנת לביטוי בתיקון הראשון לחוקה. מכאן טען, שהאיסור על ייצוא הדיסקט אינו חוקתי ובטל. בית המשפט דחה את תביעתו. אמנם, בית המשפט הסכים להניח, שההגנה שמעניק התיקון הראשון לחוקה אכן חלה גם על קוד של תוכנה; אולם פסק, שכאשר ההגבלה של הביטוי איננה מבוססת על תוכנו (content-based), אלא היא נייטרלית ביחס לתוכן (content-neutral), משמע – נועדה להגביל פונקציה אחרת שהביטוי

---

[157] **United States v. O'Brien**, 391 U.S. 367 (1968).

[158] בפסיקה האמריקנית מקובלים שלושה סטנדרטים לבחינת היקף ההגנה על חופש הביטוי. הסטנדרט הגבוה ביותר "strict scrutiny" מופעל כשהמדינה מונעת מראש ביטוי מסוים או כשהמדינה מפלה בין סוגים שונים של ביטויים על בסיס תוכנם. סטנדרט נמוך יותר הוא, כאמור, ה- "intermediate scrutiny", שבו משתמשים בתי המשפט כשהמגבלה על הביטוי אינה על בסיס תוכנו; לפי סטנדרט זה בית המשפט שם על כפות המאזניים את זכותו של הדובר לחופש הביטוי מול האינטרס המדינתי בדבר הגבלת הביטוי, כאשר מי שמשקלו רב יותר גובר. הסטנדרט השלישי והנמוך ביותר מכונה "rational basis", לפיו הדובר צריך להראות שלהסדרה המדינתית אין בסיס הגיוני.

[159] ראו: Schneier, לעיל, הערה 25.

משרת, ההגבלה תהיה מוצדקת אם היא עומדת בתנאים שנקבעו בפרשת O'Brien.[161] בהמשך לכך, קבע בית המשפט שבפרשה זו מבחן O'Brien מתקיים – הסדרת ייצוא התוכנה היא בתחום סמכותה של הממשלה; ההסדרה לא נועדה לפגוע בחופש הביטוי אלא לקדם אינטרס מדינתי חשוב (להקשות על מדינות יריבות לסרבל את הגישה של ממשלת ארצות הברית למידע חיוני לבטחון המדינה); וכן, הפגיעה בחופש הביטוי היא במידה ראויה.[162] חשוב לשים לב, שקארן ניסה לטעון שמבחן O'Brien חל רק על <u>התנהגות</u> שמגלמת בתוכה ביטוי, אך בית המשפט דחה טענה זו, וקבע שהמבחן חל על כל צורה של ביטוי.[163]

עניין **Bernstein** הביא לפסיקה הפוכה. הפעם, ידו של חופש הביטוי הייתה על העליונה. דניאל ברנשטיין הוא מתמטיקאי, העוסק בקריפטוגרפיה באוניברסיטאות אילינוי בשיקגו ובברקלי בקליפורניה. במסגרת עבודתו האקדמית פיתח אלגוריתם הצפנה חדשני – אותו כינה "Snuffle". ברנשטיין ביקש להפיץ ולייצא את התוכנה שפיתח בצירוף מאמר המנתח את הקוד ומסביר אותו; כמו כן, שאף להעלות לדיון את ממצאיו בכנסים אקדמיים, גם מחוץ לגבולות ארצות הברית. מטרתו הייתה להפיץ את רעיונותיו בקרב הקהילה המדעית בעולם, כחלק מתהליך אקדמי רגיל של החלפת רעיונות ומידע. תקנות הייצוא מנעו מברנשטיין לפרסם את עבודתו ולדון בה, כך שלדבריו נפגעו המוניטין והקריירה שלו, ובמיוחד נפגע חופש הביטוי שלו. בשנת 1996 עתר ברנשטיין לבית המשפט המחוזי הפדרלי בקליפורניה. השופטת Patel, פסקה תחילה שתוכנת הצפנה הינה ביטוי המוגן על-ידי התיקון הראשון לחוקה, מאחר שכל דבר הכתוב בשפה כלשהי הוא מעצם הגדרתו ביטוי הנהנה מההגנה החוקתית;[164] בהמשך לכך החליטה, ששיטת רישוי תוכנות ההצפנה מהווה מניעה מוקדמת של חופש הביטוי (prior restraint);[165] ולפיכך קבעה לבסוף, שתקנות הייצוא הן בלתי חוקתיות.[166]

בית המשפט לערעורים במחוז התשיעי אישר את הפסיקה של השופטת Patel,[167] אולם בצורה מעט מצמצמת יותר: תקנות הייצוא נמצאו בלתי חוקתיות, אך לא באופן גורף - רק כאשר הממשל מטיל איסור שמונע זרימה של רעיונות מדעיים (אם באמצעות קוד מקור ואם בדרך אחרת) מבלי להבחין ביניהם לבין מוצרי הצפנה כמוצרים, אז האיסור אינו חוקתי. כלומר, בית המשפט קבע שלא כל תוכנה תיחשב כביטוי - רק כאשר הקריפטוגרף משתמש בקוד כאמצעי ביטוי, באותו אופן כמו שכלכלן משתמש בגרפים ומתמטיקאי בנוסחאות כדרך להביע את המחקר

[160] **Karn, Jr. v. U.S. Department of State, et al.**, 925 F.Supp. 1 (D.D.C. 1996).

[161] **Karn**, **שם**, 10.

[162] **Karn**, **שם**, 11.

[163] בית המשפט דחה את עתירתו של קארן מסיבה נוספת והיא שה- Arms Export Control Act קובע, שהחלטות שנקבעות על-ידי המוסמכים לכך תחת החוק הזה, אינן נתונות לביקורת שיפוטית. קארן ערער על פסק הדין, אך ערכאת הערעור החזירה את התיק לבית המשפט קמא (107 F.3d 923). זאת, היות וטרם החל הדיון בערעור, הועברה הסמכות להתקין תקנות בעניין הגבלת הייצוא של תוכנות הצפנה מה-Department of State ל- Department of Commerce, והאחרונה עמדה להתקין תקנות חדשות בנושא.

[164] **Bernstein v. United States Department of State**, 922 F.Supp. 1426, 1435 (N.D. Cal. 1996).

[165] **Bernstein v. United States Department of State**, 945 F.Supp. 1279 (N.D. Cal. 1996).

[166] **Bernstein v. United States Department of State**, 974 F.Supp. 1288 (N.D. Cal. 1997).

[167] **Bernstein v. United States Department of Justice**, 176 F.3d 1132 (9th Cir. 1999).

שלהם, אז תינתן הגנה של התיקון הראשון לחוקה.[168] חשוב לשים לב לכך, שעל אף שמדובר בביטוי הכולל גם "non-speech element", בית המשפט ציין, שלא בכל מקרה כזה יש צורך להחיל את הלכת O'Brien, ועקב המניעה המוקדמת על חופש הביטוי החיל את הסטנדרט הגבוה ביותר לבחינת היקף ההגנה.

לאחר ההחלטה הזו, ביקש משרד המשפטים האמריקני דיון נוסף בפורום רחב יותר בעניין Bernstein, ובקשתו נענתה בחיוב, תוך השעיית תוקפו של פסק הדין האחרון.[169] אלא שהשינוי במדיניות ההצפנה ייתר את הדיון.

המקרה השלישי אשר עסק בסוגיית תוכנות הצפנה וחופש הביטוי היה עניין **Junger**. פרופסור פיטר יונגר הוא מרצה למשפטים ב- Case Western Reserve University בקליבלנד, המלמד קורס בשם "משפט ומחשבים". יונגר כתב מספר תוכנות הצפנה בסיסיות מאד, ורצה להציב אותה באתר האינטרנט של הקורס, כדי להדגים לתלמידיו "כיצד עובד מחשב". היות שעל-פי תקנות הייצוא, פרסום באינטרנט נחשב לייצוא,[170] הוא נדרש לקבל רשיון ייצוא ממשרד המסחר. משפנה לקבל רשיון, נתקל בסירוב, ולכן עתר לבית המשפט המחוזי באוהיו, בטענה לפגיעה בחופש הביטוי שלו.[171] בית המשפט קיבל את עמדת המדינה, ופסק שייצוא תוכנת הצפנה אינו מוגן על-ידי התיקון הראשון לחוקה, גם אם לעיתים תוכנת הצפנה עשויה לכלול מרכיב של ביטוי. ההסבר היה שתוכנת הצפנה היא פונקציונלית בעיקרה ופחות מכך ביטוי. יונגר ערער לבית המשפט לערעורים במחוז השישי,[172] שדחה פה אחד את החלטת הערכאה קמא. בערעור נפסק, שהמרכיבים הפונקציונליים בתוכנה אינם מאפילים על המרכיבים הביטויים, ושיש להחיל במקרים כאלו את הלכת O'Brien.

בשתי פרשות אחרות, הידועות כפסקי הדין בעניין ה- DVD, בחנו בתי המשפט בניו-יורק ובקליפורניה את חוקתיותן של הגבלות על פרסום והפצה של תוכנות לפיצוח אמצעי הגנה דיגיטליים. גם כאן בתי המשפט לא היו תמימי דעים בפסיקתם.

הרקע העובדתי של שתי הפרשיות כמעט זהה. תעשיית הסרטים האמריקנית ניסתה להגן על השקעותיה בסרטים בפורמט דיגיטלי על גבי DVD באמצעות טכנולוגיה שנקראה Contents Scramble System (CSS), שנועדה למנוע צפיה בלתי-מורשית בסרט שבתקליטור או את העתקתו. נער נורווגי כתב תוכנה - DeCSS - המפצחת את טכנולוגית ההגנה הזו (לדבריו, במטרה לאפשר צפיה בסרטי DVD בכוננים הפועלים בסביבת Linux). קוד תוכנת הפיצוח הופץ באינטנסיביות באינטרנט, והתובעים, שחיפשו את הדרך היעילה ביותר לקטוע את הפצתו, תבעו בעיקר מפעילי אתרים אשר הפיצו את הקוד.

---

[168] Ibid, at 1141,1145; השופט Nelson, בדעת מיעוט, סבר שתוכנת מחשב איננה יכולה להיחשב ביטוי.

[169] **Bernstein v. United States Department of Justice**, 192 F.3d 1308 (9th Cir. 1999).

[170] 15 C.F.R. § 734.2(b)(9).

[171] **Junger v. Daley, United States Secretary of Commerce,** 8 F.Supp.2d 708 (N.D. Ohio 1998).

בפרשה הראשונה, שהתנהלה בניו-יורק, היה הנתבע העיקרי אריק קורלי, האקר ידוע, שהציב עותק של תוכנת הפיצוח באתר האינטרנט שלו. חברות הסרטים תבעו אותו על סמך הוראותיו המפורשות של ה- Digital Millennium Copyright Act (DMCA), האוסרת פרסום והפצה של תוכנות לפיצוח אמצעי הגנה דיגיטליים.[173] השופט Kaplan, שישב בערכאה הראשונה,[174] פסק לטובת חברות הסרטים; קורלי עירער, אך ערעורו נדחה.[175] אחת מטענותיו העיקריות של קורלי היתה שהחלת ה- DMCA על הפצת תוכנות פיצוח סותרת את זכותו החוקתית לחופש הביטוי, היות שכבר נפסק לפני כן שקוד מחשב הינו ביטוי המוגן על-ידי התיקון הראשון לחוקה. שתי הערכאות הסכימו לכך, שקוד מחשב הוא ביטוי מוגן,[176] והשופט Newman אף ציין, בערכאת הערעור, שקביעה זו נכונה אף על-פי שהקוד מובן רק למתכנתים, בדיוק כמו שתווים המובנים רק למוזיקאי נחשבים לביטוי מוגן.[177] היקף ההגנה, כך נפסק, מושפע מהיות התוכנה צירוף של יסוד ביטויי ("speech") ויסוד פונקציונלי ("non-speech"),[178] ועל כן הסטנדרט המתאים הינו ה-"intermediate scrutiny", ולא סטנדרט מוחלט, כלומר המבחן שיש לפעול על-פיו הוא מבחן O'Brien.[179] בהמשך לכך נקבע, שה- DMCA לא נועד לדכא את חופש הביטוי, או את הרעיונות הגלומים בתוכנת פיצוח, אלא נועד לשרת את האינטרס החשוב, והחוקתי גם כן, בדבר הגנה על יצירות המוגנות בזכויות יוצרים ומניעת "פיראטיות"; כמו כן, פגיעת החוק בחופש הביטוי הינה מידתית היות ואין דרך אחרת להשיג את המטרה, ומכאן שהאיסור של ה- DMCA על הפצת ה-DeCSS הוא חוקתי ותקף.[180]

בחוף המערבי של ארצות הברית התנהלו הליכים בעניין דומה, בתביעה שהגישה ה- DVD Copy Control Association, המחזיקה בזכויות במערכת ה- CSS, ומעניקה רשיונות ליצרנים של נגני DVD להתקינה, נגד אנדרו באנר, שפירסם באתרו את קוד תוכנת הפיצוח, DeCSS. אולם, החלטתו של בית המשפט בקליפורניה שונה באופן מהותי מזו של בתי המשפט בניו-יורק. הפעם, חופש הביטוי גבר. בערכאה נמוכה ניתן, מכוח ה- Uniform Trade Secret Act, צו מניעה שאסר על באנר ואחרים לפרסם ולהפיץ את ה- DeCSS, בטענה שתוכנת הפיצוח כוללת סודות מסחריים של ה- CSS. באנר ערער לבית המשפט לערעורים של קליפורניה, והערעור התקבל. שוב, בית המשפט קבע שקוד מחשב הוא ביטוי מוגן תחת התיקון הראשון לחוקה, אך הפעם בית המשפט לא פנה למבחן O'Brien, והתיר את פרסומו של הקוד; זאת מכיוון שבאיזון בין חופש הביטוי לבין ההגנה על סוד מסחרי, שאינה הגנה חוקתית, בית המשפט מחיל את הסטנדרט הגבוה ביותר, ולא

---

172 **Junger v. Daley, United States Secretary of Commerce,** 209 F.3d 481 (6th Cir. 2000).

173 17 U.S.C. § 1201(a)(2), (b)(1).

174 **Universal City Studios, Inc. v. Reimerdes**, 111 F.Supp.2d 294 (S.D.N.Y. 2000).

175 **Universal City Studios, Inc. v. Corley**, 273 F.3d 429 (2nd Cir. 2001). (להלן: Universal II).

176 **Universal City**, 111 F.Supp.2d, at 327.

177 **Universal II**, 273 F.3d, at 445.

178 **Universal City**, 111 F.Supp.2d, at 328-329.

179 **Universal City**, 111 F.Supp.2d, at 329-330; **Universal II**, 273 F.3d, at 450.

180 **Universal City**, 111 F.Supp.2d, at 330-333.

את הסטנדרט הבינוני שמתאים למבחן O'Brien.[181] ייתכן שהאסטרטגיה של התובעת, שהעמידה מול הפגיעה הנטענת בחופש הביטוי רק את טענת הסוד המסחרי, מבלי לטעון להגנה על זכויות יוצרים והפרה של הוראות ה- DMCA, היא שהכשילה את תביעתה.[182]

בתי המשפט בישראל טרם נדרשו לשאלה זאת. חופש הביטוי בישראל מוכר כעקרון יסוד, הגם שאיננו מנוי במפורש בחוקי היסוד. במספר פסקי דין פסקו שופטי בית המשפט העליון כי יש לקרוא את הזכות לתוך חוק יסוד: כבוד האדם. לפיכך, יש להניח כי ההגבלה על הביטוי תיבחן לאור מבחן הוודאות הקרובה, וזה עשוי להיקרא לתוך פסקת ההגבלה.

5. חופש העיסוק

הפגיעה בחופש העיסוק

ההסדר המשפטי של ההצפנה מגביל את העיסוק בהצפנה, ומכאן שבעת הערכת ההסדר או עיצוב הסדר חדש, וכן בעת הפעלת ההסדר הקיים, יש לבחון אותו גם לאור זכות היסוד לחופש העיסוק, כפי שהיא מעוגנת כיום בחוק יסוד: חופש העיסוק.[183]

באכרזת הפיקוח על מצרכים ושירותים (עיסוק באמצעי הצפנה) המתוקנת, ישנה הגדרה מקיפה למונח עיסוק, הכוללת בין השאר "פיתוח, ייצור, שילוב, קנייה, מכירה, שימוש וייצוא של אמצעי הצפנה". כאמור בצו הצופן, המיישם הגדרה זו, לא יעסוק אדם באמצעי הצפנה אלא על-פי רשיון מאת המנהל ובהתאם לתנאי הרשיון. בפועל, עם התחלת העבודה על אמצעי הצפנה חדש, על המבקש להגיש בקשה לקבלת רשיון לכל סוגי העיסוק, ליחידת הממונה על-פיקוח היצוא הבטחוני (מפ"י) במשרד הביטחון לשם קבלת רשיון עיסוק לפיתוח אמצעי ההצפנה. בהמשך, כאשר למבקש יהיה אמצעי הצפנה מושלם, הוא יגיש בקשה נוספת לרשיון עיסוק לייצור, לייצוא, למכירה או לכל עיסוק נדרש אחר.

במקרה של השלמת פיתוח, שינוי במוצר או עדכון גירסה מהותי, עליו לצרף לבקשת רשיון העיסוק גרסה "עובדת" של המוצר, קבצי מקור, תיעוד נלווה וחומר נוסף על-פי בקשת משרד הביטחון, כל זאת על-מנת לאפשר בדיקה מקיפה של המוצר. בתום בדיקה זו יקבל המבקש רישיון עיסוק מתאים או, על-פי החלטת המנהל הכללי ובהמלצת הועדה המייעצת, הודעה על דחיית הבקשה.

כאשר פוקע תוקף רשיון, נדרשת חברה העוסקת באמצעי הצפנה, להגיש בקשה לחידוש הרשיון. לבקשה זו עליה לצרף הצהרה על אי הכנסת שינויים באמצעי ההצפנה. במקרים של חידוש רשיון עיסוק למכירה, עליה לצרף גם את דו"ח יעדי המכירות.

פרוצדורות אלו, מגבילות את חופש העיסוק, המעוגן בחוק יסוד. חוק היסוד קובע מפורשות כי <u>כל רשות מרשויות השלטון</u> חייבת לכבד את חופש העיסוק של כל אזרח או תושב.[184] הדרישה כי כל

---

[181] **DVD Copy Control Association v. Bunner**, 113 Cal. Rptr. 2d 338, 350-351.

[182] חיים רביה, "פיצוח ה- DVD" (18.11.01); ניתן לצפיה ב: http://www.law.co.il/hebarticles/bunner.htm .

[183] חוק יסוד: חופש העיסוק, תשנ"ד-1994, ס"ח תשנ"ד, 90.

[184] שם, בסעיף 5.

המעוניין לעסוק באמצעי הצפנה יבקש את אישור המנהל הכללי של משרד הביטחון, מטילה צל כבד על מחוייבות משרד הביטחון, כרשות שלטונית, לכבד את זכות האדם לחופש עיסוק. כפי שציינו לעיל, המדיניות הננקטת על-ידי מפ"י בפועל פוגעת פחות בחופש העיסוק, אלא שהמלצתנו היא לצמצם את הפער שבין המדיניות הננקטת בפועל לבין ההסמכות החוקית. משום כך ראוי לבחון את חוקתיות התקנות הקיימות, ואין להסתפק בכך שהמדיניות בפועל פוגענית פחות.

כפיפות ההסדרה הקיימת לחוק היסוד

הצו בדבר הסדר העיסוק באמצעי הצפנה (צו הצופן), משנת 1974 הותקן על-ידי שר הביטחון מכוח חוק הפיקוח על מצרכים ושירותים, תשי"ח-1957. כבר בנוסח המקורי, משנת 1974, הוטלה ההגבלה היסודית על העיסוק באמצעי הצפנה: "לא יעסוק אדם באמצעי הצפנה אלא על-פי רשיון מאת המנהל ובהתאם לתנאי הרשיון." אין ספק, כי המדובר בהוראת חיקוק שהיתה תקֵפה ערב חיקוקו של חוק היסוד, ולכן, על-פי לשון המחוקק, היא עמדה בתוקף עד ל- 14 למרס 2002.[185] חוק היסוד נחקק בשנת 1992, מספר שנים לא מבוטל לאחר החתימה על צו הצופן. מכאן, שיש קושי משפטי להתייחס לצו הצופן כבטל, אך על-פי לשון הוראת השעה, פירושו של צו הצופן, ייעשה ברוח הוראת חוק יסוד: חופש העיסוק.[186]

עם זאת, אכרזת הפיקוח על מצרכים ושירותים (עיסוק בענייני הצפנה) (תיקון) שהתפרסמה ב 13 לאוגוסט 1998 איננה נהנית מפסקת שימור הדינים שבחוק היסוד.[187] היא כללה הגדרה חדשה של המונח "עיסוק באמצעי הצפנה" שלא צמצמה את הפגיעה בחופש העיסוק, ובמידה מסוימת אף הרחיבה אותה. צו הצופן המתוקן, שפורסם אף הוא באותו יום וכאמור עושה שימוש בהגדרות האכרזה, לא מקל בהגבלות שמטיל, אלא הופך את פרוצדורת קבלת הרישיון למורכבת יותר ולפחות וודאית, על-ידי כך שהוא מחלק את סוגי הרשיונות לשלושה סוגים וממנה ועדה מייעצת לצד ה"המנהל" לה הוא יכול להאציל את סמכויותיו כדי שתדון ותחליט בשמו על בקשות רישיון המוגשות לו. יתכן שתיקונים אלו ראויים לביקורת שיפוטית, מתוקף היותם הוראות שפוגעות בחופש העיסוק. ביקורת שיפוטית בוצעה על-ידי בית המשפט העליון במספר מקרים, לגבי הוראות חוק שעמדו בסתירה לזכויות שעוגנו במסגרת המהפכה החוקתית.[188]

---

[185] שם, בסעיף 10.

[186] בדנ"פ 2316/95 **גנימאת נ' מ"י**, פ"ד מט (4), 589, 654, כותב הנשיא ברק כך: "מהי האנטומיה של השפעת חוקי היסוד על-פירוש הדין הישן? ודאי שחוקי היסוד אינם משנים את לשונו של החוק הישן... השינוי האפשרי הוא אך בהבנתנו אותו... המקום הגיאומטרי לשינוי בהבנת הדין הישן הוא בתכלית האובייקטיבית של דבר החקיקה... בגדרה של תכלית אובייקטיבית זו נדרש לא פעם לאזן בין ערכי יסוד המתנגשים... וכאן פועל חוק היסוד את פעולתו הפרשנית. מכוחו עשוי להינתן משקל שונה ממה שניתן בעבר לערכים ולאינטרסים הקבועים בו. כתוצאה מכך עשויה להשתנות נקודת האיזון בין אינטרסים וערכים הקובעים את תכליתו האובייקטיבית של החוק...".

[187] ק"ת 5917.

[188] ראו לדוגמא בג"צ 1715/97 **לשכת מנהלי ההשקעות בישראל נ' שר האוצר**, פ"ד נא (4) 367; בג"צ 6055/95 **שגיא צמח נ' שר הביטחון**, תק-על 97 (4), 140; ע"א 6821/93 **בנק המזרחי נ' מגדל**, פ"ד מט (4) 221 (להלן: עניין **בנק המזרחי**); בג"צ 1031/99, 1030, 1053, 1119, 1201 **כבל ואח' נ' יו"ר הכנסת ואח'** (טרם פורסם).

נקבע, כי "התרופה לאי-חוקתיות חוק היא בטלותו, וכי הסמכות לקבוע את דבר האי חוקתיות נתונה לבתי המשפט".[189] הביקורת השיפוטית בפסיקה בהקשר לבדיקה האם חיקוק תקף או בטל, יסודה בפסקת ההגבלה שבסעיף 4 לחוק יסוד: חופש העיסוק.

ראשית יש להתייחס לשאלה, האם העובדה כי הפגיעה בענייננו נעשית ב"צו" שהוא סוג נמוך מאוד בהיראַרכיה של חקיקת המשנה ובכל מקרה לא חוק, מתעלמת מהדרישה שפגיעה בזכות יסוד תיעשה בחוק? כנראה שעניין זה איננו מהותי, היות שהוספה הסיפא "או לפי חוק כאמור, מכח הסמכה מפורשת בו". הצו הותקן על-ידי שר הביטחון מכוח ההסמכה של חוק הפיקוח על מצרכים ושירותים, התשי"ח-1957.[190]

עוד נראה, כי שאלת הלימת ערכי מדינת ישראל והתכלית הראויה, אינן בעייתיות לעניין צו הצופן, כי סביר שביטחון המדינה ואזרחיה הוא ערך הולם שמהווה תכלית ראויה של רגולצית העיסוק באמצעי הצפנה. הבעיה מתעוררת לגבי שאלת המידתיות. הנשיא לשעבר שמגר קבע בפרשת **בנק המזרחי** שלושה מבחנים מצטברים לבחינת מידתיות הפגיעה: התאמה להשגת התכלית, מינימליות הפגיעה וסבירותה.[191]

למותר לציין, כי חקיקה ראשית או תיקון לחקיקת המשנה הקיימת כיום צריכה לעמוד בתנאי פיסקת ההגבלה של חוק יסוד: חופש העיסוק.

השאלה המרכזית לעניין זה היא שאלת המידתיות, וזאת בתורה נובעת מאחד המאפיינים המרכזיים של מוצרי ההצפנה. אלה הם מוצרים בעלי שימוש כפול (dual use): הם עשויים לשמש מטרות אזרחיות חיוביות, כמו הגנה על מידע פרטי, מידע מסחרי וכדומה, אך עלולים לשמש גם נשק בידי הטרוריסט.

לפיכך, אנו סבורים כי כדי לעמוד בדרישת המידתיות, על ההסדרה להיגזר ממאפייני המוצר הנדון, ומהפונקציה שהוא נועד למלא.

- **יש מקום להבחין ככל שניתן בין השימושים השונים של המוצר. יש להכיר בקיומה של קשת מצבים, כאשר בקצה האחד מוצרים המשמשים רק לשימושים מסחריים ואין להם שימוש ביטחוני, ובקצה האחר מוצרים שיש להם שימושים ביטחוניים בלבד, ואין להם שימושים אזרחיים. מובן שרוב המוצרים יימצאו על פני הקשת, ומיקומם לענין זה ייקבע על-ידי בתי המשפט.**
- **מוצרים המצויים בקצה האזרחי או הנוטים אליו, צריכים להיות פטורים מהסדרה בכלל. כך למשל מוצרי אימות חתימות דיגיטליות.[192]**
- **לעומת זאת, אין קושי ברגולציה של מוצרים המצויים בקצה השני, הביטחוני.**

---

[189] ראו עניין **בנק המזרחי**, שם, בע' 418 (השופט חשין).

[190] ס"ח התשי"ח, ע' 24.

[191] עניין **בנק המזרחי**, לעיל הערה 189, בע' 347 (הנשיא שמגר).

[192] במידה מסויימת מאפיין זה כבר קיים כיום, בדמות הגדרת אמצעי כ"אמצעי חופשי". אלא, שמספר מוצרי ההצפנה המוגדרים כאמצעים חופשיים הינו מצומצם, ובכך הקושי של היעדר המידתיות.

- **באשר למגוון המוצרים אשר מצויים על פני הציר, ולא בקצותיו, הרי המידתיות תושג בהגדרות בהירות יותר של המותר והאסור, בתיחום בהיר יותר של שיקול הדעת של הרשות, ובקיומה של ביקורת שיפוטית.**

בנוסף, על ההסדרה להבחין במפורש ובאופן בהיר בין מטרותיו של יצרן מוצרי ההצפנה.

- **מוצרים אשר לפי טיבם וטבעם משמשים לשימושים פרטיים בלבד אינם צריכים להיות כפופים להסדרה כלשהי. לפיכך, שיוק מוצרים כאלה לשוק המקומי צריך להיות פטור מהסדרה.**
- **כדי להשיג את היעדים הביטחוניים, ניתן להגביל את אפשרות הייצוא של מוצרים שהשימוש בהם קרוב יותר לקצה הביטחוני.**

6. הזכות לקניין

פגיעה נוספת של ההסדרה על הצפנה היא בזכות לקניין הנהנית ממעמד חוקתי מפורש.[193] עיקר הפגיעה נמצא בתהליך אותו נדרש מבקש הרישיון לעבור.[194] שוב, גם כאן, המדיניות הננקטת בפועל על-ידי מפ"י פוגענית פחות מאשר ההסמכה הרחבה יותר המצויה בחקיקת המשנה. אלא, שלטעמנו לא רק המדיניות בפועל צריכה להיות חוקתית, אלא גם המסגרת המשפטית שלה, וכאמור, אנו סבורים שיש להתאים בין המסגרת החוקית לבין המדיניות בפועל. הצו דורש המצאה של התוכנה גופא והנלווה לה, לעיון לשם אישור של הרשות – משרד הביטחון. מעשית, מדובר למעשה בהצגת קבצי המקור של התוכנה וחשיפת האלגוריתם לפיו פועל אותו אמצעי הצפנה. במשרד הביטחון אומרים כי בפועל, רק אחוז קטן מהחברות נדרש לחשוף את קוד המקור.[195] אלא שהחברות אינן יודעות זאת מראש, ולפיכך קיים "אפקט מצנן", מה גם שהפגיעה באלה הנדרשות לחשוף את קוד המקור ברורה. במונחי השיח הקנייני, הרי יש כאן חשיפה של הסוד המסחרי. סוד מסחרי מוגן בדין, הן בחוק והן בפסיקה.[196]

בדומה לדיון בזכות לחופש העיסוק, הרי גם כאן ההסדרה הקיימת ובוודאי שהסדרה עתידית כפופות לביקורת החוקתית, ובדומה לשם, גם הזכות לקניין איננה מוחלטת, וניתן לפגוע בה בתנאי פיסקת ההגבלה.

לפיכך, אנו סבורים כי הגדרה מפורשת של הליכי בקשת הרישיון, המבהירים כי חל איסור על המדינה לפגוע בסוד המסחרי של מבקש הרישיון, תענה על דרישת המידתיות. ניתן להוסיף חובת פיצוי של המדינה במקרה שבכל זאת תתרחש פגיעה שכזאת.

---

193 חוק יסוד: כבוד האדם וחירותו, סעיף 3.

194 צו הפיקוח על מוצרים ושירותים (עיסוק באמצעי הצפנה), התשל"ה – 1974 (להלן: "הצו"), סעיף 2.

195 ראו דברי יורם כהן בכנס שפיים.

196 ראו חוק עוולות מסחריות, התשנ"ט-1999; בג"צ 1683/93 **יבין פלסט בע"מ נ' ביה"ד הארצי לעבודה**, פ"ד מח (2) 244.

ו. ריכוז המלצות

1. הסדרתה של ההצפנה בחקיקת משנה במסגרת של חקיקה כלכלית איננה ראויה. מדובר בהסדר ראשוני באופיו ובמהותו, שיש לו השלכה על זכויות יסוד. בפועל, המדיניות הננקטת קובעת איסורים והיתרים ללא הסמכה פרטנית בחוק, באופן שקביעת המדיניות נעשית על-ידי הרשות המבצעת ללא הכוונת המחוקק. מצב זה איננו רצוי מבחינת עקרונות המשפט המינהלי והחוקתי, ויש לו השלכות שליליות על גמישותה של המדיניות הננקטת בפועל, כמו האפקט המצנן שיש לה על התעשייה. **לפיכך, אנו סבורים שיש להסדיר את ההתייחסות המשפטית להצפנה בחקיקה ראשית.**
2. מטרת החקיקה היא לענות על צורכי ביטחון אמיתיים של אבטחת מידע ביטחוני ומידע רגיש אחר ושל שימור אמצעי מעקב והשגת מודיעין למערכת הביטחון. צרכים אלה אינם מתייתרים, למרות נגישותם וזמינותם הגבוהה של מוצרי הצפנה. **לפיכך, המטרה של החקיקה היא לתכלית ראויה והולמת את ערכיה של מדינת ישראל, כנדרש בחוקי היסוד.**
3. ההסדרה הקיימת והחקיקה המוצעת פוגעות בחופש העיסוק, בזכות לקניין, ועלולות לפגוע בזכות לפרטיות ולאיים על הזכות לחופש ביטוי ומחקר אקדמי. **לפיכך, את ההסדרה הקיימת יש לפרש ברוח חוק היסוד, והחקיקה המוצעת חייבת לעמוד בתנאי המידתיות שבחוק יסוד: חופש העיסוק וחוק יסוד: כבוד האדם וחירותו.**
4. כדי לעמוד בדרישת המידתיות, החוק צריך להגדיר בבהירות ובמפורש את תחום ההסדרה, את מבחניה ואת היקף שיקול הדעת של הרשות.
5. קיימים מספר מודלים להסדרה. אנו סבורים כי אין לחזור לאחור, ואין לקבל מודל של איסור שבצידו חריגים. המודל המשפטי הקיים הוא מודל של רישוי מוקדם, ובו נעסוק תחילה.

מודל הרישוי:

6. **יש להגדיר את היקף שיקול הדעת של הרשות**, ולצמצמו לצרכים ביטחוניים של ממש. מבין אלה, צורכי סיכול פעילות טרור, להבדיל מצרכים של השגת ראיות בדיעבד, צריכים לזכות לעדיפות.

7. **יש מקום להגדיר את תחומי העיסוק הדורשים רישוי מוקדם**. לשם כך, יש להבחין בין שימושים פרטיים-אזרחיים לשימושים ביטחוניים. יש לפטור שימושים מהסוג הראשון מהסדרה כלשהי. ככל שיש קושי לסווג מוצר כמיועד לשימוש פרטי-אזרחי, וזאת מחמת מאפייני מוצרי ההצפנה כ dual use, יש מקום להסדרה, בכפוף לאמור להלן:

8. **יש מקום לזהות את מטרות היצרן**, ולהגביל את דרישת הרישוי לחלקן בלבד: בעיקר, יש להבחין בין שיווק מקומי לייצוא. נוכח הגדרת הצרכים הביטחוניים כהערמת קשיים על הגעתם של מוצרי הצפנה לידי ארגוני טרור - יש מקום לפיקוח על ייצוא, אך פחות מכך על שיווק מקומי, ובמיוחד כאשר ייעוד המוצר קרוב יותר לקצה האזרחי מאשר לשימוש הביטחוני.

9. **יש להגדיר במפורש את קריטריוני הפיקוח**: האם נבדק היעד הסופי של המוצר או עוצמת ההצפנה. במדינות שונות ננקטים מבחנים שונים. אין אנו מכריעים בעניין זה, ומסתפקים בכך שיש מקום לקבוע את הקריטריון, ובכך לאפשר לתעשייה לכלכל את תוכניותיה בהתאם ולפעול בוודאות גבוהה יותר.

10. **יש להגדיר את תהליכי האישור במפורש:**

- יש לתחום את היקף המידע שהרשות רשאית לבקש מיצרן המבקש רישיון;
- יש לקבוע את שלבי הבדיקה בחוק. פרטי השלבים יכולים להיקבע בתקנות;
- יש לקבוע הליך ערעור למבקש שבקשתו נפסלה. יתכן שהמקום לכך הוא ביקורת שיפוטית של בתי המשפט לעניינים מינהליים, במסגרת עתירה מינהלית. במקרה כזה, יהיה מקום לקבוע סדרי דין מיוחדים כדי להבטיח את סודיות תוכן הדיונים.

11. **פיצוח הצפנה**: במקרה שבו הרשות מבקשת גישה למוצר הצפנה קיים, קרי ל"דלת אחורית", יש ליצור מנגנון של ביקורת שיפוטית מוקדמת, בדומה לזה המקובל בחוק האזנות סתר, תשמ"א – 1981.

מודל רישום

12. יש מקום לשקול מודלים אחרים להסדרה. מודל אפשרי אחד הוא של רישום הצפנות, ללא פיקוח מוקדם עליהן. מודל כזה, בדומה לרישום מאגרי מידע על-פי חוק הגנת הפרטיות, תשמ"א-1981, יטיל חובה אחת ויחידה על יצרן מוצרי הצפנה: רישום עצם קיומה ופרטים כלליים עליה. באופן כזה, תוכל הרשות הביטחונית לדעת איזה מוצרים מצויים בידי מי. במידת הצורך, תוכל הרשות לפנות לבית משפט בבקשה מוקדמת, ולבקש היתר לחדור למוצר ההצפנה.

III. סביבת המידע כזירת מעקב: ביטחון, פרטיות וחופש ביטוי[197]

א. הקדמה

בשנים האחרונות הפכה רשת האינטרנט לאמצעי מרכזי להעברת מסרים ולניהול מידע. הרשת מאפשרת שימוש באמצעים חדשים לשיגור ולקבלת מסרים בין גורמים שונים ולניהול מידע באופן יעיל, נגיש ואינטראקטיבי. ההתפתחויות הטכנולוגיות ועידן המידע השפיעו רבות על חשיבתם ועל דרכי עבודתם של ארגוני המודיעין בעולם. בעוד שהמודיעין הקלאסי הסתמך בעיקר על מודיעין אנושי - **Human Intelligence**,[198] הרי שבשנים האחרונות מבססים ארגוני המודיעין את עבודתם על השגת חומר מודיעיני באמצעים טכנולוגיים, ובעיקר בסיגינט –**Signal Intelligence**. סיגינט משמעותו מודיעין המופק מהאזנה לאותות (סיגנאלים) ופענוחם, בין אם המדובר בגלים אלקטרומגנטיים או תעבורה סיב-אופטית וכל סטנדרט תקשורתי אחר, לרבות תקשורת נתונים ותעבורת אינטרנט כגון: דואר אלקטרוני, מסרים מידיים ותשתיות אתרים.[199] שינוי התפיסה והעברת הדגש אל מודיעין טכנולוגי נובע, בין היתר, מהעובדה שיעדי המודיעין עושים שימוש באמצעי תקשורת שונים ומגוונים ולכן חשופים הרבה יותר מבעבר למעקב באמצעים אלו. לצד הפעילות החוקית ברשת (כגון מסחר אלקטרוני, חינוך והוראה, מחקר אקדמי), משמשת הרשת אמצעי תקשורת גם ליעדים מודיעיניים מסוגים שונים: החל מגורמים פליליים וכלה בארגוני טרור. מרכזיותה של הרשת כאמצעי תקשורת הופך אותה כמובן ליעד חשוב, המהווה מקור לחומר מודיעיני הנאסף על-ידי ארגוני המודיעין.

סביבת המידע כזירת מעקב מקנה לארגוני המודיעין מספר יתרונות בולטים באיסוף המידע. ראשית, אמצעי ההאזנה האלקטרוניים הפועלים על רשת גלובלית, בשילוב עם יכולות מחשוב רבות עוצמה מאפשרים איסוף יעיל של חומר מודיעיני, אשר בעבר היה כרוך בהשקעת משאבים וכוח אדם עצום, או שלא היה אפשרי כלל. שנית, כל פעולה ברשת דיגיטלית מותירה "עקבות דיגיטליים". הפעולות השוטפות של משלוח דואר אלקטרוני, גלישה, שיגור והורדת קבצים, מהוות למעשה עיבוד נתונים ונרשמות בקבצים שונים של המחשב האישי והשרתים המעורבים בתקשורת. כך למשל, בניגוד לשיחת טלפון הנותרת בחלל האוויר ובזיכרונם של הדוברים בלבד, דיון בצ'אט יוצר תרשומת של תוכן השיחה, כמו גם של המועד בו התבצעה החלפת המסרים, המחשבים והשרתים באמצעותם בוצעה וכדומה. בנוסף, הרשת מאפשרת העברת מסרים

[197] בכתיבתו של פרק זה נעזרנו רבות בהרצאותיהם של עו"ד עמית אשכנזי, עו"ד מייק בלס, עו"ד נאוה בן אור, גב' קארין ברזילי-נהון, עו"ד מתי ברזם, עו"ד בועז גוטמן, עו"ד שרון גולדנברג, פרופ' עמנואל גרוס, עו"ד דודי זלמנוביץ, ד"ר אסף יעקב, ד"ר משה כהן-אליה, מר אריאל פיסצקי, עו"ד תמר קלהורה, עו"ד שרון קרן, עו"ד חיים רביה, פרופ' שיזף רפאלי, ועו"ד טנה שפניץ ותודתנו נתונה להם. האחריות לתוכן, כמובן כולה שלנו.

[198] המונח **Human Intelligence** (יומינט) מתיחס למודיעין אנושי. הכוונה למודיעין המופק ממקורות איסופיים אנושיים כגון: מרגלים, סוכנים, משתפי-פעולה, חקירת שבויים. בעבר, מקור המודיעין הבלעדי והאיכותי ביותר. בשימוש גם כיום, אם כי לצד מקורות נוספים המופקים בצורות אחרות לא-אנושיות.

[199] המונח **Signal Intelligence** (סיגינט) מתיחס למודיעין תקשורתי; מודיעין אלקטרוני; מודיעין טכנולוגי. מדובר בעיקר בהאזנה לתקשורת טלפון, סלולאר, פקס ובשנים האחרונות גם אינטרנט, דואר-אלקטרוני. לעיתים, כשלב מקדים להפקת המוצר המוגמר, נדרש פיצוח אמצעי הצפנה המגנים על המקור. סיגינט מהווה כיום מקור המודיעין הנפוץ והאיכותי ביותר, בעיקר בקרב ארגוני המודיעין המובילים בעולם, בעלי התשתיות הטכנולוגיות המתקדמות ביותר.

מורכבים בפורמטים שונים: לא רק החלפת טקסטים בדואר אלקטרוני, אלא גם צ׳אט בזמן אמיתי, דיבור, תמונות וידאו, וכמובן גם תוכנות ויישומי מחשב. בנסיבות אלה עושר המידע שניתן לאסוף, ורמת הפירוט, הינם חסרי תקדים.

אולם, יתרונותיה של סביבת המידע בתחום של מעקב ואיסוף מידע, עלולים ליצור איום מסוג חדש על חירויות הפרט. איום זה נובע מן העובדה, שאמצעי איסוף המידע והמעקב בסביבת המידע חודרניים ומשוכללים יותר. הדבר נובע גם מאופן ההאזנה המתחייב לאור מאפייניה המיוחדים של התקשורת ברשת האינטרנט. כך למשל, התקשורת באינטרנט מבוססת על חלוקת נתונים ל״חבילות קטנות״ (Packets), המשוגרות על-ידי המחשב השולח ומנותבות ברשת בנפרד, עד שלבסוף יאספו ויסודרו על-ידי המחשב המקבל. בנסיבות אלו, תמסורות של יעדים מודיעינים עלולות להיבלע בתמסורות תמימות. לפיכך מעקב ברשת כרוך, במקרים רבים, בהאזנה ואיסוף חומר רב גם על מי שאינם חשודים כלל.

מאפייניה הייחודיים של הרשת עשויים לחייב בחינה מחדש של הכללים הקיימים המבטאים את נוסחאות האיזון בין צרכי הביטחון לזכויות הפרט. החקיקה במשטרים דמוקרטיים מאזנת בין צורכי המודיעין של רשויות הביטחון השונות, לבין השמירה על זכויות הפרט. יישומו של מערך האיזונים הקיים בסביבה הדיגיטלית עשוי לחייב התאמה לצרכים, לאמצעים ולאיום החדש על זכויות הפרט. בנוסף, במסגרת הניתוח המשפטי יש לקחת בחשבון את העובדה שפעולות מודיעיניות רבות עלולות להתבצע על גבי ציוד ושרתים של גורמים מסחריים, ולעיתים אף באמצעותם.[200]

פרק זה עוסק בשאלה מהי המסגרת המשפטית הראויה לפעולות מודיעיניות ברשת האינטרנט. הדיון ייפתח בסקירה קצרה של המאפיינים המייחדים את אמצעי המעקב ופעולות האיסוף המודיעיני בעידן המידע. בהמשך, נדון באיומים שאמצעים אלו עלולים להטיל על זכויות הפרט, כמו הזכות לפרטיות וחופש הביטוי. לבסוף, נסקור את מערכת האיזונים הקיימת בין צורכי המודיעין לבין זכויות הפרט במסגרת הכללים המשפטיים הקיימים. נבחן באיזו מידה נותנת המסגרת המשפטית הקיימת מענה לצורכי הביטחון בסביבה הדיגיטלית, ובו בזמן מקנה הגנה מספקת לזכויות הפרט.

ב. מודיעין בעידן המידע

1. רקע כללי

עבודת המודיעין בעידן המידע מורכבת משלושה שלבים. **בשלב ראשון** נדרש ארגון המודיעין לזהות את התשתית הטכנולוגית אליה מעוניין הוא לחדור. לעיתים הדבר פשוט ביותר וניתן לביצוע למעשה על-ידי כל אדם מן הישוב כגון: יירוט רשת קשר אנלוגית שניתנת לקליטה על-ידי מכשיר קשר פשוט. לעיתים מדובר במשימה מורכבת וקשה ביותר העשויה לדרוש פיתוח מערכת שתהיה מסוגלת לקלוט וליירט את התשדורת האמורה לעיתים אף תוך פיצוח אבטחה מתוחכמת.

---

[200] סעיף 13 לחוק הבזק, התשמ״ב-1982, מורה על הקצאת משאבים, בהתאם להחלטת שר הביטחון או השר לביטחון פנים, מצד בעל רשיון לביצוע פעולות בזק, למתן שירותי בזק או לשידורי לווין, לטובת כוחות הביטחון. בנוסף, קיימים סעיפים מיוחדים ברשיון לביצוע שירותי בזק, הקובעים הוראות ספציפיות ביחס למחויבות בעל הרשיון כלפי מערכת הביטחון. למשל, לפי הרצאתו של עו״ד קרן שרון מחברת סלקום, סעיף 48 לרשיון חברת סלקום מורה על הקצאת משאבים מוחלטת לטובת מערכת הביטחון. סעיף 66א לרשיון סלקום מחייב את החברה להקצות שירותים מיוחדים למערכת הביטחון.

לדוגמה: תקשורת קווית מוצפנת או חדירה למחשבים המוגנים ב- Firewall. **בשלב הבא**, נדרש ארגון המודיעין ליירט את אותה תשדורת ולמעשה לצותת לה. הדבר מצריך כוח אדם שאמור להיות מסוגל להתמודד עם תעבורות בשפות שונות, קריאת טקסטים וכדומה. לעיתים, ולאור כמויות המידע העצומות, משמשת בתפקיד זה פלטפורמה ממוחשבת המפעילה אלגוריתמים שמסוגלים, למשל, לזהות מילים חשודות העולות מתוך טקסט או מלל. לפיכך, הסינון הינו אלמנט קריטי בעבודת מודיעין, וכפי שייראה בהמשך הוא מאפיין גם ארגוני מודיעין מודרניים במלחמתם העכשווית כנגד הטרור. **השלב השלישי** והאחרון הוא ניתוח, מחקר והפצת תוצר מודיעיני מוגמר לצרכני המודיעין החל מדרגים נמוכים רלוונטיים ועד לקברניטי מדינות. שלב זה רלוונטי פחות לדיון הנוכחי. ניתן להדגים שלבים אילו בדרך פעולתה של NSA שתתואר להלן.

באופן לא מפתיע פעולתם של ארגוני המודיעין חסויה וניתן ללמוד עליה באופן עקיף וחלקי בלבד מתוך מה שפורסם אודות פעילותם והאמצעים בהם הם משתמשים בכלי התקשורת. מקורות עתונאיים,[201] כמו גם ארגוני זכויות אדם למיניהם אשר עוקבים אחר פעולותיהם של ארגוני המודיעין,[202] מדווחים כי ארגון המודיעין הגדול בעולם בתחום הסיגינט הוא ה – **NSA** האמריקני: **National Security Agency**. ארגון זה פועל לצד ה – **CIA** וה- **FBI** ושווה מעמד להם כסוכנות פדראלית. עוד נטען, כי ארצות הברית מפעילה, בשיתוף עם מדינות מערביות נוספות, מערכת טכנולוגית, המאפשרת ליירט בזמן אמת מסרים שמועברים באמצעי תקשורת רבים ברחבי העולם. מדובר ברשת ריגול והאזנות בינלאומית שמכונה "אשלון" **(Echelon)**, אותה מפעילה ה-**NSA**, בשיתוף עם שירותי הביון של קנדה, בריטניה, אוסטרליה וניו זילנד. הפרויקט המקורי נוסד בשנת 1971, אך תחומי פעילותו התרחבו בהדרגה מאז.[203] על-פי דיווח של האיגוד האמריקני לזכויות האזרח, "אשלון" מותקנת כיום במאה ועשרים תחנות האזנה הפרושות בסיאטל, מערב וירג'יניה, פורטו ריקו, דנמרק, ניו זילנד, קנדה, אוסטרליה, הולנד וקפריסין, ומסתייעת בלוויינים.[204] ארצות הברית מעולם לא הודתה רשמית בקיום המערכת אך ועדת חקירה של האיחוד האירופי בעניין "אשלון" קבעה לאחרונה, שרשת הריגול האלקטרונית קיימת ואף הביאה הוכחות לקיומה.[205]

---

[201] ראו למשל "כשל המודיעין האלקטרוני" (Ynet): http://www.ynet.co.il/articles/1,7340,L-1116808,FF.html; Echelon: The Skies Have Ears (CNN): http://www.cnn.com/1999/TECH/computing/12/30/echelon.idg/.

[202] ראו למשל פרוייקט ה- Echelon Watch של הארגון האמריקני לזכויות האזרח (ACLU: American Civil Liberties Union), הנמצא ב - http://www.aclu.org/echelonwatch.

[203] הפרויקט נוסד בהתאם לאמנה לשתוף פעולה בתחום הסיגינט - **UKUSA Signals Intelligence 1948 Treaty**. אף שהמדובר באמנה חסויה, ניתן למצוא התייחסויות לאמנה זו במקורות אינטרנט שונים, ביניהם גם מקורות בעלי רמת אמינות גבוה. ראו למשל התייחסות לאמנה באתר פדרציית המדענים האמריקניים (The Federation of American Scientists), נמצא ב: http://www.fas.org/irp/eprint/sp/sp_f2.htm.

[204] ראו רשימת תחנות האזנה "חשודות", המבוססת על מקורות עיתונאיים, מומחים בתחום וספרים בנושא באתר פדרציית המדענים האמריקניים, נמצא ב: http://www.fas.org/irp/news/1999/02/radome.htm

[205] Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) - Temporary Committee on the ECHELON Interception System. ראו: http://www2.europarl.eu.int/omk/OM-

בפרויקט אשלון מערכת האזנה חשאית המותקנת במחשבי-על ומסוגלת לקלוט שלושה מיליארד תמסורות אלקטרוניות מדי יום (על-פי הערכות, קרוב לעשרה מיליארדי מסרים עוברים ברשת מדי יום). דו"ח ועדת הבדיקה מטעם האיחוד האירופאי בנושא אשלון, אשר אושר על-ידי הפרלמנט האירופי, אישש חשדות לפיהם "אשלון" יכולה לקלוט וליירט תקשורת של גולשים בכל רחבי העולם. זאת בין אם מדובר בשיחות טלפון, פקס, תקשורת לוויינית, דואר אלקטרוני, הורדות של תוכנות מהאינטרנט, קשרי מיקרוגל ותעבורה סיבית-אופטית. לרוב, "אשלון" לא מקליטה את השיחות אלא נמצאת במצב "האזנה" למערכת. לשם כך, המערכת עושה שימוש בתוכנות "רחרחניות" (Sniffers)[206] שמפקחות על תעבורת המידע בשישה צמתים מרכזיים באינטרנט, ואוספות מידע רב ככל שניתן, שלאחר מכן מועבר ל-"מילון", אוסף של תוכנות בינה מלאכותית שמתמחות באיתור חומר בעל ערך מודיעיני. תוכנות "אשלון" מאתרות מסרים הכוללים מלים "חשודות" (כגון: "חומרי נפץ", "בן לאדן", "אל קעידה", וכן מילות קוד תמימות לכאורה, המוכרות בקרב גורמי הביטחון כמאפיינות יעדי מודיעין) מיירטת אותם, ממיינת אותם ושולחת לזרועות המודיעין במדינות השונות.

2. אמצעים לאיסוף מידע ומעקב ברשת

לצורך הדיון המשפטי ניתן לסווג את אמצעי המעקב השונים ברשת בהתאם לאופן בו נאסף המידע: על-ידי *ניטור*, דהיינו רישום פעולות המתבצעות ברשת התקשורת על-ידי משתמשים שונים, או על-ידי *חדירה* לשרת המחשב ורישום הפעולות המתבצעות על גבי השרת. לאבחנה בין פעולות מעקב במרחב הציבורי לפעולות מעקב במרחב הפרטי (תוך חדירה למערכות שהינן קניינו הפרטי של המשתמש) עשויות להיות השלכות משפטיות. היבט נוסף שעשוי להשליך על הניתוח המשפטי הינו סוג המידע הנאסף: למשל, תוכן התקשורת, יומן התקשורת בלבד (Log), או נתונים דמוגרפיים כלליים/סטטיסטיים על קבוצות משתמשים במערכת.

2.1 ניטור מידע

ניטור מידע מהווה למעשה ציתות משוכלל באמצעות ב"רחרחן" (Sniffer): תוכנה, הסורקת את השרת ובודקת את כל הפעילות שלו לפי פרמטרים שונים. הרחרחן הידוע והמתוקשר ביותר לאחרונה הוא **הקרניבור – Carnivore**.[207] באופן רשמי יועד הקרניבור למלחמה בפשע – בפדופיליה למשל, אולם הוא הופך כמובן לכלי רלוונטי ושימושי, גם במסגרת המאבק בארגוני הטרור הפועלים לעיתים קרובות תוך שימוש ברשת.

Europarl?PROG=REPORT&L=EN&PUBREF=-//EP//TEXT+REPORT+A5-2001-0264+0+NOT+SGML+V0//EN&LEVEL=2

[206] במונח **Sniffer** ("רחרחן") הכוונה לתוכנה, ש"עוברת" על שרת מרכזי באינטרנט או במרכזיית טלפון ובודקת את כל הפעילות שלו לפי פרמטרים שונים. פעילות תקשורתית רלוונטית "נשלפת" ומועברת להמשך טיפול מודיעיני.

[207] כינוי זה ניתן לתוכנה על-ידי ה- FBI הואיל והיא "לועסת" את כלל המידע אך, "בולעת" ו"מעכלת" רק את המידע הספציפי הרצוי. לאחרונה שינה ה-FBI את שמה של התוכנה ל- DCS1000, במהלך מיוחצ'ן היטב, הואיל והשם עצמו עורר ביקורת והתנגדות ציבורית חריפה. ראו דיווח על כך באתר של ארגון ה-ACLU, הנמצא ב: http://www.aclu.org/news/2001/w021401b.html.

ההאזנה לתעבורת האינטרנט מתבצעת בדרך-כלל בצורה פאסיבית, תוך שהמערכת עוקבת אחר כלל התקשורת ודולה, תוך הקלטה, את המידע הספציפי בו היא מעוניינת (זיהוי ה **packets** – הרלוונטיים). בעבר, הועלו טענות כי המערכת הינה אקטיבית ושותלת בעצמה מידע בתעבורה, על-מנת לייעל את פעולתה, אולם עד כמה שידוע, אין הדבר נכון. המעקב מתבצע למעשה, על גבי המערכות של ספקי האינטרנט. החומר המודיעיני הנאסף על-ידי הקרניבור זהה במקרים רבים למידע הנרשם ממילא על גבי השרתים של ספקי האינטרנט כחלק בלתי נפרד מהפעלת הרשת. על-פי המצב המשפטי ששרר לפני ה- 11 בספטמבר 2001 היה צורך בצו חיפוש על-מנת להעביר מידע זה לרשויות החקירה. מצב זה השתנה בעקבות חקיקתו של ה USA PATRIOT Act[208]. כאשר ה-FBI אוסף את המידע באופן עצמאי, מושתל הרחרחן במעין תיבת-סעף על-ידי ה- **FBI** על גבי צמתי המידע של ספק השירות. ספקי אינטרנט אמריקניים דיווחו כי ה-FBI ניסה לשדל אותם להתקין על-גבי המערכות שהם מפעילים את תוכנת הרחרחן עוד לפני ה-11 בספטמבר. מספר ספקי אינטרנט[209] וכמובן ארגוני זכויות האדם[210] יצאו במאבק נגד התופעה. הדי המאבק שככו אמנם לאחר אירועי ה-11 בספטמבר, אולם עדיין נשמע קולם של ספקי השירות בעניין, בייחוד בעקבות החקיקה החדשה.[211]

לקרניבור שני שימושים: ציתות תוכני וזיהוי המשתמשים.[212] ציתות תוכני (**content wiretap**) – כולל האזנה לסיגנאלים אלקטרו-מגנטיים או סיב-אופטיים ה"משודרים" מטעם היעד המודיעיני, וסינון התקשורת האינטרנטית מתוכם, בדומה להאזנה לטלפון. בדרך כלל ייורטו הודעות דואר אלקטרוני שנשלחו מאת היעד המודיעיני ואליו: תעבורה טכנית, פעילות חשבון הדואר האלקטרוני, או כלל התעבורה הנכנסת ויוצאת של משתמש מסוים, או של כתובת IP מסוימת. שימוש כזה מחייב אישור בית משפט פדראלי.[213]

שימוש נוסף בקרניבור הוא לצורך זיהוי המתקשרים (**trap and trace / pen register**), והוא כולל איתור וזיהוי של כל יוצרי הקשר אל יעד המודיעיני או ממנו. איתור וזיהוי כאמור כוללים: זיהוי כתובות דואר אלקטרוני, זיהוי שרתים (Web, FTP) אליהם ליעד המודיעיני יש גישה, מעקב אחר המשתמשים בדף אינטרנט או FTP ספציפי, כלל דפי האינטרנט או תיקיות ה- FTP שליעד

---

208 ראו תת-פרק ד.4 להלן.

209 ראו דיווח על מאבקם של ספקי שירות כגון: AOL, EartLink, Mci ב-FBI, בשיתוף עם ארגון ה-ACLU, ב-Wall Street Journal Online מה- 14.7.2000. דיווח על הכתבה ב-WSJ ניתן למצוא ב אתר ZDNET: http://www.zdnet.com/zdnn/stories/news/0,4586,2656409,00.html

210 ראו למשל מכתב מטעם ה-ACLU בנושא הקרניבור לחברי הקונגרס מיום 11.7.2000, נמצא באתר ה-ACLU: http://www.aclu.org/congress/l071100a.html.

211 ראו: "IT Workers Chew Over 'Carnivore' Bill" באתר ה-CNN: http://www.cnn.com/2001/TECH/industry/10/11/carnivore.resistance.idg, ואת המשך המאבק הציבורי שמנהל ה-ACLU, תחת השם: "Safe and Free in Times of Crisis" באתר ה-ACLU, נמצא ב: http://www.aclu.org/safeandfree/index.html.

212 המידע הטכני שלהלן מבוסס על מקורות אינטרנט ברמות אמינות שונות, לאור חסיון מערכת הקרניבור, כגון: http://stopcarnivore.org/ ו- http://www.robertgraham.com/pubs/carnivore-faq.html

213 ראו להלן תת-פרק ד.4.

גישה אליהם. השימוש בתוכנה לצורך זיהוי המתקשרים ללא חשיפת תוכן ההתקשרות הינו שימוש נפוץ, וההגבלות המשפטיות על שימוש זה מצומצמות.[214]

בהקשר לדואר-אלקטרוני, הקרניבור למעשה מאזין לתחלופת המידע בין שני משתמשי דוא"ל כשאחד מהם הוא היעד. את הרחרחן מעניין בעיקר פרוטוקול ה – **SMTP** הנוצר בתקשורת זו ומפרט את כתובת השולח, הנמען וההודעה עצמה המורכבת מ – **Header** ו- **Body**. במידה שהותר ל – **FBI** מעקב מסוג של **trap and trace** בלבד, הרי שהוא רשאי "להאזין" אך ורק לחלקו הראשון של הפרוטוקול הכולל פרטים על השולח והנמען בלבד.

חלקו הראשון של הפרוטוקול מורכב מנתונים החושפים את זהותם של הצדדים להודעת הדואר האלקטרוני הספציפית:

```
<--220 mx.altivore.com SMTP server.
>>>HELO mx.example.com
<--250 mx.altivore.com Hello [192.0.2.183], pleased to meet you
>>MAIL FROM: <alice@example.com>
<--250 <alice@example.com> … Sender ok
>>>RCPT TO: <bob@altivore.com>
<--250 <bob@altivore.com>
>>>DATA
<--354 Start mail input; end with <CRLF>.<CRLF>
>>>(e-mail message)
>>>\r\n.\r\n
<--250 Queued mail for delivery
>>>QUIT
<--221 mx.altivore.com closing connection
```

חלקו השני של הפרוטוקול מורכב מכותרת ותוכן הודעת הדואר האלקטרוני הספציפית:

```
From: "Alice Cooper"
To: "Bob D Graham"
Subject: Shipment
Date: Thu, 7 Sep 2000 15:51:24 -0700
Message-ID:
MIME-Version: 1.0
Content-Type: text/plain;
            charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600

How is the plutonium shipment coming? I need it by Friday.
```

[214] ראו להלן תת-פרק ד.4

--Alice

ראוי לציין כי בהשוואה לפרוייקט "אשלון", הקרניבור הינו רחרחן "כירורגי" בלבד שאינו מסוגל ואינו מתיימר, ככל הנראה, לעקוב אחר תעבורה בהיקף רב ממספר משתמשים גדול. נראה גם כי זו אחת הסיבות ל"פתיחות" המפתיעה שמפגין ה- **FBI** ביחס למידע על הרחרחן, יכולותיו ואופן השימוש בו. ברם, גם אם כוונת ארגון המודיעין היא לעקוב אחר תעבורת האינטרנט והדואר האלקטרוני של אדם אחד בלבד, הרי שלטענת גורמי תקשורת ומחשבים ומומחי בינה מלאכותית, הסבירות כי "פיזית" יצליח ה- **FBI** למשל להתמקד באדם אחד, או ליתר דיוק בסיגנאל או בביט בודד, כמעט אפסית, ולכן לא מן הנמנע כי נפגעת פרטיותם של משתמשים רבים אחרים בסביבתו של היעד.

2.2 איסוף מידע על גבי השרת או המחשב האישי

קיימים מספר אמצעים חודרניים הנשתלים במחשב האישי לשם איסוף מידע. הנפוץ שבהם בתחום המסחרי הוא השימוש בטכנולוגיה המכונה Cookies (עוגיות). המדובר בקובץ טקסט שהאתר שומר בדיסק הקשיח של הגולש, המאפשר לערוך רישום ומעקב אחר הרגלי הגלישה של המשתמש, כגון: האתרים בהם ביקר הגולש, הפרסומות שהוצגו בפניו ואילו שנענה להן, וכדומה. במקורן נועדו העוגיות כדי למנוע את הטורח שבהרשמות חוזרת ונשנית לאתרים, שהתנו את השימוש בהם במסירת פרטים אישיים. ברמה הטכנית, השתלת הקובץ איננה מחייבת מודעות, הסכמה או שיתוף פעולה מצד המשתמש. יחד עם זאת, הגרסאות החדשות של הדפדפנים מאפשרות לבטל את קבלת העוגיות, לשנות את הגדרות הדפדפן כך שיתריע בכל פעם שאתר מנסה לשלוח אליו עוגיה, או למחוק את העוגיות במחשב האישי לאחר כל חיבור לאינטרנט.[215]

יצוין כי טכנולוגיה זו איננה מאפשרת לכשעצמה איסוף מידע על גולש, זיהויו בשם או כתובתו הפיזית, אולם לעיתים קרובות הגולש עצמו מוסר מידע זה או מגדיר אותו בדפדפן, ולעיתים ניתן להסיק פרטים אלו מתוך הצלבתם של מאגרי מידע אחדים. השימוש המסחרי בעוגיות מעורר סוגיות כבדות משקל הנוגעות להגנת הפרטיות, ועניינן עלה לא מכבר על סדר היום באיחוד האירופי.[216]

---

[215] תוכנות שמוחקות עוגיות מספקות פתרון יעיל יותר נגד עוגיות. תוכנות כמו Guidescop ו- Burnt Cookies עוקבות אחר השינויים בתיקייה שבה נשמרות העוגיות. בעזרתן ניתן למחוק עוגיות, לעיין בעוגיות שבדיסק הקשיח ולהחליט אם לשמור או למחוק אותן. הסקירה מתבססת על גל מור, "רואים לנו את הכל" נמצא ב- www.ynet.co.il/Ext/Comp/ArticleLayout/CdaArticlePrintPreview/1,2506,l-234131,00.html. ראו גם האתר: www.cookiecentral.com וכן חיים רביה, "על גלישה ופרטיות - או על עוגיות ברשת" נמצא ב: http://www.law.co.il/hebarticles/cookies1.htm.

[216] ראו: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. נוסח הדירקטיבה נמצא ב: www.cdt.org/privacy/eudirective/EU_Directive_.html (24.12.01).

מערכת פנס הקסם – Magic Lantern

אמצעי נוסף, שזכה לכותרות ודיון ציבורי, לאחר ה-11 בספטמבר הוא "פנס הקסם" – Magic Lantern. המדובר במערכת בה משתמשת סוכנות ה- FBI, במטרה להתמודד עם מידע מוצפן המצוי במחשביהם של פושעים וטרוריסטים.[217] בעוד שלניטור מידע באמצעות רחרחנים כגון הקרניבור, יתרונות משלו בעבור סוכנות האיסוף, הרי שעדיין נותר קושי בפיצוח חומר מוצפן שנאסף. פנס הקסם פותר קושי זה בעבור ארגון המודיעין, תוך שהוא חוצה גבול נוסף ומעורר דאגה במתחם הפרטיות של פרטים וארגונים.

פנס הקסם הוא למעשה תוכנת פיצוח (keylogging software) המושתלת במחשבו של היעד. התוכנה מסוגלת "לראות" את הסיסמאות אותן מקליד החשוד ובכך למעשה לגלות את מפתח ההצפנה בו הוא משתמש. מכאן, הדרך פשוטה וקצרה לחשיפת כל חומר מוצפן, החל מהודעות דואר אלקטרוני ועד מספרי כרטיסי אשראי. על-מנת לשתול את התוכנה, ה- FBI, מעלה את רף החדירה שלו אל פרטיותו של אותו חשוד, באופן חסר תקדים. התוכנה היא למעשה וירוס שיכול להישלח אל היעד בדואר אלקטרוני, או דרך גורם שלישי, אמין בעיני היעד. הווירוס יכול להיות מוחדר וירטואלית אל המחשב המיועד גם באמצעי פריצת מחשבים אחרים וכמובן שלא נשללת האפשרות לשתילה פיזית לחלוטין, הכרוכה כמובן בפריצה לחצרים.[218]

משמצויה התוכנה במחשבו של היעד, נתון למעשה המשתמש במחשב במעקב פאסיבי. המעקב הופך לאקטיבי, משמופעל יישום ההצפנה הפופולארי PGP (Pretty Good Privacy), בו נדרש המשתמש למסור סיסמת הפעלה (passphrase) ובכך למעשה מוסר לסוכן העוקב את מפתח הצופן. חשוב להזכיר, כי בעוד שהתוכן המבוקש מוגן על-ידי אותם מפתחות, הרי שהמפתחות עצמם מוגנים אך ורק על-ידי אותה סיסמה. המפתחות הגנובים מאפשרים כמובן למחזיק את יכולת הפיצוח, שהמשתמש סבור היה כי היא ברשותו בלבד.

הדיון הציבורי נסב כמובן סביב שאלת הפרטיות, אך העלה גם את הטענה המעניינת בדבר לגיטימיות פעילות ממשלתית הטומנת בחובה אלמנטים הנחשבים לפליליים, בנסיבות אחרות,

---

[217] חשיפתו העיתונאית הראשונה של פנס הקסם ארעה ביום 20.11.01 באתר של רשת התקשורת MSNBC, נמצא ב: http://www.msnbc.com/news/660096.asp. סוכנות המודיעין הודתה פומבית בשימוש בפנס הקסם לאחר לחץ תקשורתי רק ביום 12.12.01, ראו הדיווח באתרה של רשת MSNBC, נמצא ב: http://www.msnbc.com/news/671981.asp?0si=-. השימוש הראשון של ה- FBI בתוכנה נעשה בפרשת מאפיה, הידועה כפרשת Scarfo. ראו דיווח עיתונאי על הפרשה באתר ABCnews.com: http://abcnews.go.com/sections/scitech/CuttingEdge/cuttingedge011221.html. במסגרת מעקב אחר אחד מראשי המאפיה במדינת ניו-ג'רזי, Nicodemo Scarfo, הודה סגן עוזר מנהל ה- FBI, Randall Myrch, בפני בית המשפט כי סוכני הארגון פרו פיזית למשרדו של Scarfo ושתלו במחשביו את התוכנה במטרה לגנוב מפתחות הצפנה. מפתחות אלו איפשרו לארגון לפצח מסרים מוצפנים ששימשו ראיות מפלילות כנגד איש המאפיה.

[218] כפי שארע בפרשת Scarfo.

על-ידי האקרים למשל.[219] בנוסף, עורר השימוש בתוכנה את שאלת התמודדותן של חברות האנטי-וירוס השונות עם הווירוס ה"לגיטימי". סוכנות ה- FBI מנסה כמובן לשדל את החברות לשתף עימה פעולה ולא "לזהות" את התוכנה כווירוס ואף נפוצו שמועות על הסכמים לשיתוף פעולה בין חברות מסויימות לממשל האמריקני.[220]

ג. סיכול ואכיפה בעידן המידע: איום על זכויות הפרט?

1. מבוא

מערכות סיכול ואכיפה הן הביטוי המעשי לשמירה על האינטרס הציבורי בכלל, ועל הסדר הציבורי בפרט. כפי שהדברים מובנים היום, רשויות המדינה הן אלו האמונות על שמירת אינטרס הציבור על-ידי מערכות שונות לאיתור, יירוט ומעקב אחר מידע במטרה למנוע פעולות הנוגדות את אינטרס הציבור, וכולל, כמובן, פעולות בטרור. הסכנה העיקרית שבהפעלת מערכות מעקב ואיסוף מידע היא הפגיעה בזכויות הפרט, בעיקר הזכות לפרטיות ולחופש ביטוי.

האמצעים הטכנולוגיים בעידן חופש המידע הביאו את הדיון בזכות לפרטיות למישורים חדשים. חדירה לפרטיותו של אדם אינה מצריכה עוד להגיע לביתו ולפשפש בחפציו. כיום, חדירה לפרטיות נמצאת במרחק לחיצת כפתור. קיימים מקרים בהם המדינה בעצמה מבקשת להציב אמצעי האזנה קבועים או ארעיים בשם האינטרס הציבורי. בהנחה שאמצעים אלו אכן משרתים את האינטרס הציבורי, האם יש לסבול פגיעה בפרטיותם של אותם חפים מפשע שנקלעו לדרכה של המדינה למידע הרלוונטי?

2. מהי פרטיות ומהי הזכות לפרטיות?

שורשים לזכות לפרטיות ניתן למצוא עמוק בהיסטוריה האנושית, ועיגונים ברורים קיימים בתנ"ך, במיתולוגיה היוונית ובסין העתיקה. בתרבות המערבית נוכל למצוא עיגונים כבר משנת 1361 באנגליה, ובשנת 1890 במאמר המפורסם של וורן וברנדייס אשר טבעו את המושג "The Right To Be Left Alone".[221] הזכות לפרטיות במידע היא זכות חדשה יחסית שמשמעותה

---

[219] ראו דבריהם של David Sobel, יועצו המשפטי של ה- Electronic Privacy Information Center (http://www.epic.org/) והסנטור הרפובליקני Dick Armey באתר MSNBC, נמצא ב - http://www.msnbc.com/news/660096.asp.

[220] חברת Network Associates (www.nai.com) יצרנית PGP ותוכנת האנטי-וירוס הפופולרית McAfee הואשמה במין הסכם מסוג זה. ראו דיווח על הפרשה והכחשתה של החברה באתר Wired.com, נמצא ב - http://www.wired.com/news/conflict/0,2100,48648,00.html . איש אבטחת המחשבים המוכר למדי בחוגי האינטרנט, Robbert Graham, כותב באתרו הפרטי www.robbertgraham.com את הדברים הבאים: "The official company position of any mainstream company is that they have no position. It would be bad business to help law enforcement invade customer's privacy, and it would be bad business to specifically work against the efforts of legitimate law enforcement. They are going to do their best to do neither." נמצא ב: http://www.robertgraham.com/journal/020110-magic-lantern-position.html.

[221] ראו: Louis D. Brandeis & Samuel D. Warren, "The Right to Privacy", 4 **Harv. L. Rev.** 193 (1890).

שנויה במחלוקת. הקושי סביב הגדרת הזכות לפרטיות משתקף היטב בהגדרתה כ"זכות אישית אשר מובנת מאליה עד שמישהו לוקח אותה".[222] הגדרה שלילית זו אינה מספקת, והשאלה הבסיסית היא מה משמעותה של "פרטיות". המונח *פרטיות* מתאר מצב עניינים, נסיבות בהן מצוי הפרט ביחס לאחרים. לפיכך, *הזכות לפרטיות* נוגעות לאותם מצבים בהם החוק מקנה הגנה לזכותו של הפרט להגן על פרטיותו. במשפט האמריקני התפתחה הזכות לפרטיות במידע בעקבות מאמרם המפורסם של וורן וברנדייס, שטענו כי הזכות לפרטיות היא זכות נפרדת ובלתי תלויה בזכויות אחרות. אחרים, כגון, William Prosser, טענו שזכות זו מורכבת מארבע עילות נזיקין: חדירה למרחב הפרטי של אחר; ניצול שמו או תדמיתו של אחר; פרסום מידע פרטי ופרסום המעמיד את האדם באור מטעה.[223] במהלך השנים נעשו ניסיונות רבים להגדיר מהי פרטיות, ומהי הזכות לפרטיות.[224]

יש המגדירים פרטיות במונחים של גישה. דהיינו, פרטיות מתייחסת ליכולתו של הפרט להגביל את הגישה אליו. רות גביזון למשל, טוענת כי "[P]rivacy is a limitation of others access to an individual".[225] במובן זה, אובדן פרטיות מתחולל כאשר לאחרים יש מידע על הפרט, כאשר הם מפנים אליו תשומת לב, או מקבלים נגישות אליו.[226]

אחרים, מגדירים פרטיות במונחים של שליטה. אם בעבר נגעה פרטיות לשליטה במרחב הפרטי-אינטימי, במובן "ביתו של אדם מבצרו", הרי שבעידן המודרני הורחב מושג זה וחל אף על שליטה במידע אודות הפרט, או במידע פרטי. לפיכך, פרטיות בעידן המודרני משמעה לא רק שליטה של אדם במרחב הפרטי הפיזי, אלא גם שליטה על ההחלטות האינטימיות,[227] שליטה על ההיכרות עם ענייניו האישיים, או שליטה במידע אודותיו.[228] במובן זה פרטיותו של אדם נמדדת ביכולתו לקבוע מתי, כיצד ובאיזו מידה יעשה שימוש במידע אודותיו.[229] על-פי גישה זו, הזכות לפרטיות

---

222 David H. Flaherty, "On the Utility of Constitutional Rights to Privacy and Data Protection", 41 **Case Western Reserve L. Rev.** 831-55, 831(1991).

223 ראו: William Prosser, "Privacy", 48 **Cal. L.J**. 383-423 (1960). ראו גם: Richard Posner, **The Economics of Justice** 272 (1981). עמדה זו זכתה לביטוי ב: **Restatement (Second) of Torts** § 652A (1976):

(2) The right of privacy is invaded by:
(a) unreasonable intrusion upon the seclusion of another, ...; or
(b) appropriation of the other's name or likeness, ...; or
(c) unreasonable publicity given to the other's private life, ...; or
(d) publicity that unreasonably places the other in a false light before the public, ...

224 ראו: **Philosophical Dimensions of Privacy: An Anthology** (Ferdinand D. Schoeman ed., Cambridge 1984).

225 Ruth Gavison, "Privacy and the Limits of Law", 89 **Yale L.J.** 421, 428 (1980). הנגישות, לדעת גביזון, מבוססת על שלושה אלמנטים: סודיות, אנונימיות, וניבדלות (solitude).

226 Irwin Altman, "Privacy Regulations: Culturally Universal or Culturally Specific?" 33 **J. of Soc.** 67 (1977); Anita L. Allen, **Uneasy Access** 3 (1988).

227 Julie C. Inness, **Privacy, Intimacy, and Isolation** 7 (1992).

228 כך למשל סבור צ'ארלס פריד כי פרטיות הינה לא רק היעדר מידע אודותינו אצל האחר, אלא גם יכולתנו לשלוט במידע אודותינו. ראו: Charles Fried, "Privacy [A Moral Analysis]" in **Philosophical Dimensions of Privacy**, supra note 226, at 210 (1984); Charles Fried, "Privacy", 77 **Yale L.J.** 475, 482 (1968).

229 Alan F. Westin, **Privacy and Freedom** (1971).

היא זכותו של אדם לשלוט על מידע שנוגע לו, ועל השימוש במידע שנאסף אודותיו. אדם זכאי לקבוע באילו נסיבות מידע אודותיו יהפוך לפומבי במובן זה שיפורסם, או יהיה נגיש לציבור הרחב בדרך אחרת. הגדרה זו מחייבת, כמובן, הכרעה בשאלה מהו אותו מידע פרטי אשר זכאי להגנה, ואילו זכויות שליטה נתונות לפרט ביחס למידע זה. הואיל והזכות לפרטיות מגדירה את קו הגבול בין ה"פרטי" (אשר אמור להיות תחת שליטה פרטית) וה"ציבורי" (המצוי מחוץ לתחום השליטה של הפרט), תשקף זכות זו במקרים רבים את התפיסות החברתיות והתרבותיות בנוגע לאבחנה פרטי/ציבורי. הזכות לפרטיות במובן זכותו של אדם לשלוט במידע אודותיו, עשויה ליצור קושי מושגי, שכן ההגנה על פרטיות במידע מחייבת במקרים רבים הגנה על "פרטיות" במה שמוגדר כ"מרחב הציבורי".[230]

3. האם מוצדק להגן על הפרטיות בסביבת המידע?

העדר בסיס תיאורטי בהיר להגנת הפרטיות במידע המצוי במרחב הציבורי היא אולי הגורם להגדרות המשפטיות העמומות בכל מה שנוגע לזכות לפרטיות.[231] על-מנת שניתן יהיה להגדיר את מהותה והיקף תחולתה של הזכות לפרטיות במידע יש לבחון מהן ההצדקות לקיומה. יש הסבורים כי פרטיות מהווה ערך עצמאי הראוי להגנה, בעוד שאחרים סבורים שפרטיות איננה ערך כלל,[232] או מחזיקים בעמדה הריאליסטית לפיה פרטיות הינה נחלת העבר ואינה בת קיום בעולם האורבני האלקטרוני המודרני.[233] מנגד, יש הרואים בפרטיות אמצעי שנועד להבטיח קיומם וקידומם של ערכים אחרים. בהגבלת כוחה של המדינה בהקשר זה ניתן להצביע על מספר טענות:

3.1 אוטונומיה. יש המדגישים את חשיבותה של הזכות לפרטיות כחלק ממערכת ההגבלות שחלה על המדינה ביחס לפרט ונועדה לשמור על חירותו. בהקשר הרחב יותר, נימוק זה עשוי להצדיק הגנה על הזכות לפרטיות לא רק ביחסי האזרח והמדינה, אלא גם בהקשרים מסחריים. כך למשל, יש הטוענים כי הזכות לפרטיות הינה חיונית על-מנת להבטיח את האוטונומיה של הפרט, ויכולתו לבחור עבור עצמו באורח חופשי ועצמאי כיצד ינהל את חייו. במובן זה טוען פריד, פרטיות הנה ערובה לחופש אישי: אם נדע כי כל פעולותינו נרשמות, וכי כל מה שנאמר או נעשה ייוודע לכולם – הדבר עלול להשפיע על פעולות שננקוט.[234] שקיפות בדרך כלל איננה דו-סיטרית, ומעניקה לצד המשקיף אפשרות לשלוט בפרט הנצפה ולכוון את התנהגותו.[235] הזכות לפרטיות נועדה אם כן

---

[230] Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public", 17 **L. & Phil.** 559 (1998).

[231] לעמימות ההגדרות ראו: Gregory J. Walters, **Human Rights in the Information Age A Philosophical Analysis** (Toronto, 2001) at 158.

[232] ראו למשל עמיר גולדברג, "לוחמי החופש ברשת, נא להירגע", **הארץ - קפטן אינטרנט**, 05.02.200; ניב אחיטוב, **עולם ללא סודות, על חברת במידע הפתוח** (2001).

[233] ראו את עמדתו של נשיא חברת סאן Scott McNealy, ודיון: Polly Sprenger, "Sun on Privacy: 'Get Over It'", **WIRED** (26.1.99), נמצא ב: http://www.wired.com/news/politics/0,1283,17538,00.html.

[234] ראו: Fried, Privacy, לעיל, 229, עמ' 210.

[235] ג'רמי בנתהם טבע את המונח "פנופטיקון" בהקשר של בית הסוהר "היעיל". מתקן כליאה יעיל על-פי עמדתו ייעל את השליטה על-ידי ריכוז האסירים בלב המתקן, במבנה שקוף חשופים לעיני כל הסוהרים, בכל רגע נתון. דימוי זה הורחב בהמשך על-ידי Foucault אשר טען כי חיי הפרט בחברה הפוסט-מודרנית הם חיים של שקיפות. הפרט חשוף לעיני כל ללא יכולת למצוא פינת מסתור. לשימוש במונחים אילו לניתוח

לאפשר חופש אישי, פעולה אוטונומית וגיבושה של זהות עצמית.[236] במובן זה הזכות לפרטיות מהווה מרכיב חיוני בשימור קשרים חברתיים ובסיס לסולידריות חברתית.[237] ההנחה בהקשר זה היא כי האוטונומיה של הפרט מהווה בסיס חשוב ליכולתו ליצור קשרים אותנטיים עם העולם.[238]

3.2 הבניית הזהות והגדרה עצמית. איסוף מידע ברשת מאפשר יצירת פרופיל משתמש המנותק מן האדם אשר המידע נוגע לו, ומבחינה טכנית ניתן לעשות בו שימוש בהקשרים שונים מבלי שיש צורך בשיתוף פעולה מצידו. היכולת לשלוט במידע מבססת את כוחו של הפרט להגדיר את זהותו כלפי עצמו, וכלפי אחרים, וכן למנוע מאחרים להגדיר בעבורו את תדמיתו, אישיותו ומעשיו. בכל מה שנוגע ליכולת להגביל את השימוש במידע פרטי בידי גופים מסחריים הזכות לפרטיות מאפשרת לפרט להימנע מלהפוך למצרך, להרחיק מסביבתו גורמים מסחריים שאין הוא מעוניין בהם, ולבחור להיות במגע עסקי או חברתי עם גורמים אחרים. הזכות לפרטיות בהקשר זה מאפשרת לאדם ליטול חלק בקביעת מקומו בסולם החברתי, ולא לקבל על עצמו את השיבוץ המסחרי ואת אפשרויות הבחירה המסחריות השלובות עימו. במובן זה, הזכות לפרטיות נגזרת מתפישה של אוטונומיית הפרט וזכותו להגדרה עצמית.[239]

3.3 מימוש זכויות אדם אחרות – כגון חופש ביטוי. הזכות לפרטיות עשויה להיות חיונית למימוש זכויות אזרח אחרות, ובראשן חופש הביטוי. כאשר הפרט יודע, כי רשויות המדינה מאזינות או מפעילות מערכות המסוגלות ליירט כל מידע ובכללו גם את ביטויו שלו, יחשוש הפרט מהתבטאות חופשית לחלוטין. כאשר אדם יודע שהוא במעקב, או כי דבריו וצעדיו נרשמים ונשמרים הוא עלול להימנע מלהתבטא בחופשיות. לעיתים די בעצם הידיעה בדבר השימוש באמצעי מעקב, גם אם לא נעשה בהם שימוש תמידי בפועל, על-מנת לגרום לצנזורה עצמית. תופעה זו ידועה בשם תופעת ה"אפקט המצנן".[240]

קיים קשר בין פרטיות לאנונימיות. האפשרות להעביר מסרים בצורה אנונימית ברשת היא אחד הכלים החשובים בשמירה על הפרטיות ובהעצמת חופש הביטוי. אפשרות זו הכוללת בחובה את היכולת להעביר מסרים, לאסוף מידע או ידע ללא חשיפת זהות הגולש, מקנה לגולש מרחב פעולה רב שאינו מחייב חשיפת זהותו האמיתית. זהו היבט מסוים של הזכות לפרטיות המגולמת בביטוי "The Right to be Left Alone". כלומר, הפרט אינו רוצה שייחסו לו פעולות מסוימות ולכן בוחר אמצעי הגנה כגון שימוש בהעברת מסרים אנונימית. פיצוח מנגנונים להעברת מסרים אנונימיים על-מנת לשרת את אינטרס הציבור עלולה לגרום לפגיעה חמורה בחופש הביטוי ברשת וכן לפגיעה

הסכנות שבאובדן הפרטיות בעידן המידע ראו: Oscar H. Gandy, Jr. The Panoptic Sort: A Political Economy of Personal Information (Boulder, 1993).

[236] לתפישה זו המכוונת לקשר שבין פרטיות לאוטונומיה של הפרט, ראו: Nissenbaum, supra note 232; Julie E. Cohen, "Examined Lives" Informational Privacy and the Subject As Object", 52 **Stan. L. Rev.** 1373-1438 (2000).

[237] להרחבה, ראו הרצאתו של ד"ר משה כהן-אליה בכנס שפיים, 26.12.01, מושב ערב.

[238] ראו הרצאתו של ד"ר משה כהן-אליה, שם.

[239] ראו כהן-אליה, **שם**.

בפרטיותו של מעביר המסר. כמובן השאלה היא באיזו מידה יש לאפשר או אפילו לעודד ביטוי אנונימי. מחד גיסא, ברור שהאפשרות לביטוי אנונימי עשויה להפיק שיח ציבורי עשיר יותר, הכולל עמדות ומידע אשר לא היו מגיעים לידיעת הציבור אם הדוברים היו נדרשים לחשוף את זהותם. מאידך גיסא, ביטוי אנונימי, המאפשר לדובר למסור מידע או להביע דעה ללא מחויבות לתוצאות דבריו, עלול לגרום נזק. כך למשל, עלולים להיחשף בדרך זו סודות מדינה, או להתפרסם דברים חסרי שחר שעלולים להוות לשון הרע. בדומה, האפשרות לאנונימיות עלולה לסייע לשימוש ברשת לפעולות טרור.

האפקט המצנן של העדר פרטיות על חופש הביטוי עלול לבוא לידי ביטוי גם בהיבט אחר של הזכות לחופש ביטוי – הוא הזכות לחפש, לקרוא ולקבל מידע. אדם היודע כי כל פעולותיו נרשמות, עלול להימנע מאיתור מידע וביצוע חיפושי מידע בנושאים בהם הוא מעוניין, מחשש שמא הדבר עלול לפגוע בו (כך למשל, חיפוש מידע בנושא תרופות למחלה מסוימת, זהות מינית, או מאמרים הקשורים לתנועה פוליטית או זרם חברתי חדש).

4. מהם גבולות ההגנה על הפרטיות בעידן המידע?

זכותה של החברה (על-ידי המדינה – באת כוחה) לשמירה על הסדר הציבורי מקימה את הצידוק המוסרי לקיומן של מערכות סיכול ואכיפה כגון מערכות האזנה (ציתות), חיפוש ותפישה. כנגד זכות זו עומדות זכויות היסוד של הפרטים וביניהן הזכות לפרטיות והזכות לחופש ביטוי. הניסיון לאזן בין צורכי הביטחון לבין זכויות הפרט בכל מה שנוגע לאיסוף מידע ברשת יוצר דילמות מעשיות לא פשוטות. האם יש לתת למדינה את האפשרות לצותת לכל שיחה או מידע העובר ברשת ללא כל בקרה? או שמא יש להגבילה למקרים מיוחדים בלבד? ניתן להצביע על שתי דרכים מעשיות המבטאות נוסחאות איזון שונות בין האינטרס של ביטחון המדינה לבין זכויות הפרט.

הדרך הראשונה היא לאפשר למדינה ליירט את כל המידע ללא כל סינון, ולנתח רק את המידע החשוד. אפשרות זו מאפשרת גישה בדיעבד גם למידע שבתחילה נראה לא מסוכן. טלו למשל את אירועי ה- 11 בספטמבר 2001; המסרים שעברו בין מתכנני הפיגוע לבין מבצעיו לא עוררו חשד בזמן אמת. אך בדיעבד, מידע זה היה רלוונטי ביותר לאיתור האחראיים לפיגוע.

עם זאת, ליירוט כל המידע שעובר ברשת השפעות עקיפות רבות על זכויותיהם של הגולשים המתבטאים באמצעותה. הפרטים המבקשים להעביר מידע אישי שאינו קשור לטרור או לפעולות פוגעניות כאלו או אחרות יחששו לעשות כן מכיוון שמידע זה מיורט ומתועד על-ידי המדינה ובבוא היום קיים החשש כי יעשה בו שימוש נגדם. טלו למשל זוג נאהבים בעלי משפחות נפרדות המבקשים להביע רגשותיהם באמצעות מסרים ברשת. הידיעה כי דבריהם מיורטים ונשמרים על-ידי המדינה תגרום לצינון ביטוי רגשותיהם ולפגיעה חמורה בפרטיותם.

הדרך השנייה לאיזון בין האינטרסים של המדינה והאינטרסים של פרטים בתוכה בהקשר לחופש הביטוי ברשת, היא לאפשר למדינה לצותת לכל מידע וליירט רק את זה שבו היא חושדת שעלול להביא לפגיעה בסדר הציבורי. אפשרות זו מבטיחה כי לא ניתן יהיה לשחזר בעתיד מידע שלא יורט. אולם, החשש שמא מידע מסוים יהיה רלוונטי בשלב מאוחר יותר, יגרום לכך שהגדרת מידת

---

[240] Fried, Privacy, לעיל, הערה 229.

החשד המאפשרת יירוט תהיה רחבה ותכלול גם ביטויים שאינם מהווים איום על אינטרס הציבור באופן מידי וברור. כך, למשל, יתכן מצב בו החברה תאפשר יירוט ביטויים של קרובי משפחתו של טרוריסט רק בגלל החשד שמא נעשה שימוש בצינור זה להעברת מידע שעלול להזיק. ציתות לצינור מידע זה יפגע בחופש הביטוי ובפרטיותם של משפחת הטרוריסט גם במצבים בהם אין שום אינדיקציה להתבטאות פוגענית מצידם.

ההכרה בזכותו של אדם לפרטיות במידע, מטילה על המשתמשים במידע הגבלות בכל מה שנוגע לאיסוף המידע, לשימוש במידע, ולעיבודו. הגבלות אלו על ״חופש זרימת המידע״ עלולות לגבות מחיר יקר. לטכנולוגיות המידע תרומה עצומה ליעילות ולקידמה. כך, למשל, בתחום המסחרי, בצמצום עלויות ובהורדת מחירים, באספקת שירותים חדשים, בהצלת חיי אדם במקרה של פגיעה בריאותית, וכמובן במלחמה בפשע ובארגוני טרור. הגנה על הפרטיות המטילה הגבלות על השימוש במידע, עלולה במקרים רבים לפגוע בזכויות ובאינטרסים אחרים. כך למשל, הזכות לקבל מידע,[241] זכותו של הציבור (וחובתה המתבקשת של המדינה) להגנה עצמית המחייבת אף היא לעתים פגיעה בפרטיות של פרט זה או אחר.

היקף ההגנה המשפטית לזכות לפרטיות תלוי באיזון שבין הזכות לפרטיות לזכויות ואינטרסים אחרים הראויים להגנה. בהקשר זה, ראוי להבחין בין ההגנה על הפרטיות המאוימת על-ידי המדינה, לבין ההגנה על הפרטיות כנגד איומים שמקורם בפרטים אחרים, כגון בחברות הפועלות בשוק המסחרי.

בכל מה שנוגע לאיזון בין הזכות לפרטיות לבין צרכים שלטוניים ניתן להצביע מבחינה היסטורית ותרבותית על שתי מסורות עיקריות: האחת מעונינת להגביל את כוח המעקב של המדינה – החל בעיר המדינה (הפוליס) היוונית, דרך התנועה הפרוטסטנטית האנגלית ומסורת המשפט המקובל וכלה בעקרונות החוקה האמריקנית וזכויות הקניין שם. השנייה, מעניקה כוח רב לשלטון לעקוב אחר הפרט, החל בספרטה הרומית, עובר בכנסיית ימי הביניים, ועד למדינת-הלאום הקונטיננטאלית. בהערת אגב, יצוין כי ישראל, מן הסתם, מצויה בתווך.[242]

גם בכל מה שנוגע להגנה על הפרטיות בהקשרים מסחריים קיים הבדל בין המסורת אשר מוצאת את ביטויה במשפט האמריקני לבין המסורת הקונטיננטלית. ההגנה על הזכות לפרטיות במשפט האמריקני מתמקדת בזכויות כנגד חדירה לפרטיות מצד המדינה, ונזהרת מלהגביל את פעולתם החופשית של גופים כלכליים הפועלים בשוק החופשי, ועושים שימוש במידע פרטי כמשאב כלכלי לכל דבר. הגישה האירופאית, לעומת זאת, מדגישה את האיסוף והשימוש במידע פרטי על-ידי גופים מסחריים.

איזון מתחייב גם בהקשר של חופש הביטוי. היקף חופש הביטוי מושפע ישירות ממידת ההגנה הניתנת לו. חופש הביטוי במובנו המוחלט הוא החופש להביע דעות בכל דרך שהיא ללא חשש

[241] הזכות לקבל מידע טומנת בחובה אינטרס ציבורי ואינטרס פרטי. אינטרס הציבור הוא זכות הציבור לדעת (משום שמידע אודות מעשיהם של פרטים עשוי להיות חיוני לחברה כולה). אינטרס הפרט הוא לעצב את דעתו ולשם כך נזקק הוא למידע גם אודות ענייניו הפרטיים של פלוני. ראו זאב סגל, ״הזכות לפרטיות מול הזכות לדעת״ **עיוני משפט** ט (התשמ״ג) 175, 178.

[242] נוסחת האיזון בין אינטרס ביטחון המדינה לבין הזכות לפרטיות בישראל תידון בהרחבה להלן, בתת-פרק ה. ההסדר המשפטי הנוהג בישראל בנוגע לחיפוש, תפיסה והאזנות סתר מכרסם בהגנה על זכות

לפגיעה באינטרס כלשהו של המתבטא. ככל שחופש הביטוי רחב יותר כך יטו הפרטים להתבטא בחופשיות רבה יותר. עידן המידע בכלל ורשת האינטרנט בפרט מביאים את הדיון בחופש הביטוי למדרגה חדשה.

רשת האינטרנט והמידע הזורם בה מהווים "שוק רעיונות חופשי",[243] המקנה במה לכל דורש ומאפשר לגולשים לחלוק דעתם ללא מגבלה גיאוגרפית כלשהי. היכולת להעביר מסרים למיליוני בני אדם בלחיצת כפתור ובעלות נמוכה מכתיר את רשת האינטרנט כאמצעי התקשורת הדמוקרטי ביותר שנוצר עד כה. יתרונות אלו, המאפשרים ביטוי וזרימת מידע חופשיים מול רצונה של החברה לשליטה על המידע העובר ברשת, מקימים מכשול חוקתי של ממש העומד בפני פעולותיה של המדינה. חופש הביטוי מהווה את סוד קסמה של רשת האינטרנט. ייחוד זה נפגע כאשר המדינה מפעילה אמצעי מעקב אודות התכנים והמסרים העוברים ברשת במטרה להגן על אינטרס הציבור בכלל ועל הסדר הציבורי בפרט. כל ניסיון מצידה של המדינה לשלוט בנעשה ברשת, ולאסוף או ליירט ביטוים ברשת על-ידי מערכות ציתות, האזנה ומעקב, עלול לפגוע בזכות הפרט לחופש ביטוי ולפרטיות.[244]

בדיון שלהלן נבחן כיצד באות לידי ביטוי גישות אילו במסגרת ההסדרים המשפטיים הקיימים בנוגע לפעולות מעקב וחיפוש. בהמשך נבחן האם ההסדרים מתאימים לפעולות הסיכול והאכיפה ברשת האינטרנט.

ד. הגבלות משפטיות על פעולות סיכול ואכיפה בעידן המידע

1. המסגרת המשפטית

אמצעי סיכול ואכיפה המופעלים על-ידי רשויות השלטון תחומים, לפחות לכאורה, על-ידי כללים ועקרונות מהמשפט הציבורי. ראשית, רשויות המדינה כפופות למשפט החוקתי ולזכויות היסוד שהוכרו כמסגרת על מהבחינה הנורמטיבית. במסגרת זאת כל פעילות תהיה כפופה לאיזונים מול זכויות אדם בסיסיות. שנית, הרשויות כפופות לעקרונות המשפט המנהלי, ואלו מתווים מסגרת כללית של פעולה לפי עקרון החוקיות, שהרי אין לרשות אלא מה שהוקנה לה לפי חוק. הרשות אינה יכולה להפעיל אמצעי סיכול ואכיפה ללא הסמכה חוקית לפעולה זו. מעבר לכך, אין די בקיום סמכות, שכן על הרשות לפעול בסבירות ובהגינות, ובתוך כך גם לשקול שיקולים של זכויות אדם שהוזכרו לעיל. שלישית, פעולת הרשות כפופה לאפשרות התמידית לביקורת שיפוטית. זאת ועוד, ביקורת שיפוטית אפשרית על כל השלבים, הן קודם להפעלת אמצעי סיכול ואכיפה (בעת בקשת צווים נדרשים), והן לאחריהם, אם בתקיפה ישירה ואם בתקיפה עקיפה.

האדם לפרטיות. הדין הישראלי נועד להבטיח, כי פגיעה בפרטיותו של אדם, לשם הגנה על צרכים ביטחוניים, לא תותר אלא במידה שאינטרס ציבורי גובר על הזכות לפרטיות.

243 ראו: Alan Gewirth, **Human Rights: Essay on Justification and Application** 56 (Chicago, 1982).

244 ראו: David H. Flaherty, "On the Utility of Constitutional Rights to Privacy and Data Protection", 41 **Case Western Reserve L. Rev.** 831, 843 (1991).

בפרק זה נסקור את הדינים הרלוונטיים במישור הבינלאומי, בארצות הברית, באיחוד האירופאי ובמדינות נוספות. בסקירת הדינים נדגיש במיוחד חקיקה חדשה שנכנסה לתוקפה, אם כי לא בהכרח נולדה, לאחר אירועי ה- 11 בספטמבר. דגש מיוחד יושם על החוק האמריקני החדש ה- USA PATRIOT Act, וכן חוק בריטי חדש מסוף חודש דצמבר Anti-Terrorism, Crime and Security Act 2001. בתום סקירת הדינים נקדיש התייחסות נפרדת לגופים מסחריים וחובות שהוטלו עליהם בכל הנוגע לאיסוף מידע, שמירתו ומסירתו לרשויות אכיפה. בהקשר זה ניתן למצוא מסגרת דיון רחבה באמנת פשעי-מחשב מחודש נובמבר 2001, אשר מרחיבה באופן משמעותי את קטגוריית "ספקי-השירות".

2. ההקשר הבינלאומי

2.1 הגנה על הזכות לפרטיות

התייחסות מודרנית ברמה הבינלאומית לזכות לפרטיות נמצאת בהכרזה האוניברסלית על זכויות האדם משנת 1948.[245] מספר רב של אמנות בינלאומיות כלליות מכירות מפורשות בזכות לפרטיות, ביניהן האמנה האזרחית (ICCPR)[246] ואמנות האומות המאוחדות. ברמה האזורית, מצויות אמנות שהפכו את הזכות לפרטיות לזכות הניתנת לאכיפה במובן המשפטי: כך בשנת 1950 האמנה האירופאית להגנה על זכויות אדם,[247] שמכוחה הוקמו הנציבות האירופאית לזכויות אדם ובית הדין האירופאי לזכויות אדם, וצ'רטר הזכויות של הקהילייה האירופאית אשר מגן על הפרטיות ועל מידע אישי.[248]

ההכרה בזכות לפרטיות בדין הבינלאומי מאפשרת ביסוס של הזכות לפרטיות כזכות אדם בסיסית בכל סיטואציה שתתעורר. יתר על כן, רוב מדינות המערב מכירות בזכות במישור הדין הפנימי כזכות חוקתית, דהיינו זכות הנמצאת במישור נורמטיבי רם מדברי חקיקה רגילים. זאת ועוד, כאשר מדובר בחוקות חדשות יותר, ניתן למצוא התייחסות ספציפית לזכות לפרטיות

---

[245] **Universal Declaration of Human Rights** (1948), סעיף 12: "לא יהא אדם נתון להתערבות שרירותית בחייו הפרטיים, במשפחתו, במעונו, בחליפת מכתבים שלו ולא לפגיעה בכבודו או בשמו הטוב. כל אדם זכאי להגנת החוק בפני התערבות או פגיעה באלה." http://www.hrweb.org/legal/udhr.html (ביקור אחרון: 23.12.01).

[246] **International Convenant on Civil and Political Rights (1966)**, סעיף 17:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy family, home or correspondence, nor to unlawful attacks no his honour and reputation.
> 2. Everybody has the right to the protection of the law against such interference or attacks."

http://www.hrweb.org/legal/cpr.html (ביקור אחרון: 23.12.01).

[247] ראו: European Convention of Human Rights & Fundamental Freedoms (1950), Art. 8:

> "1. Everybody has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the rights and freedoms of others."

ולזכות לשלוט במידע אישי. בדו"ח משנת 2000 של ארגון להגנת הפרטיות, נמצא כי בארבעים מתוך חמישים מדינות שנסקרו שם (ובהן ישראל) קיימת מודעות וזכויות ברורות בדבר גישה לתיעוד ציבורי.[249] ההגנה במישור הבינלאומי וההכרה בזכות לפרטיות בדין הפנימי של מדינות רבות ברחבי העולם מצביעות על חשיבותה הרבה של הזכות לפרטיות, ועשויות להיות בעלת השלכה ישירה על האיזונים הנדרשים בכל סיטואציה בה חשופה הזכות לפגיעה, במיוחד באווירה הפוליטית אשר נוצרה לאחר אירועי ה- 11 בספטמבר ולאור הטכנולוגיות החדשות המאפשרות חדירה חסרת תקדים לפרטיות.

2.2 הסדרים בינלאומיים להגנה על מידע אישי

הזכות לפרטיות חלה גם במקרים ספציפיים הנוגעים לזכות הפרט למנוע איסוף נתונים אישיים אודותיו ועיבודם. הגנה בינלאומית על נתונים אלקטרוניים הנוגעים לפרט קיימת באמנה משנת 1990: **Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data**.[250] אמנה זו דנה בקבצי מידע אישי ועיבוד נתונים במגזר הציבורי ובמגזר הפרטי. האמנה קובעת כי השגת נתונים, עיבודם ואחסונם יעשה בהתאם למטרות שלשמן נאספו. על הנתונים להיות נאותים, נוגעים לעניין ולא לחרוג מעבר למטרות שבשמן נאספו ואוחסנו. קיימת חובה על מחזיק המידע להבטיח את דיוק הנתונים, לרבות אפשרות תיקון ועדכון מעת לעת, אולם בה בעת להפעיל אמצעי אבטחה מתאימים כדי להגן על הנתונים מפני גישה או שינוי בלתי-מורשים. על-פי האמנה, יש לוודא את קיומם של אמצעי הגנה על פרטיות האדם, ולשם כך האנשים, שפרטיהם כלולים בנתונים, חייבים לקבל גישה למידע באופן שיבטיח את האפשרות לקבוע את קיום קובץ הנתונים, מטרתו ואת זהות הגורם השולט במידע; אפשרות לקבל אישור שהנתונים האישים אכן מאוחסנים; אפשרות להשיג תיקון או מחיקה הנוגדים דין מקומי. יחד עם זאת, האמנה מכירה בחריגים שיעוגנו בחקיקה פנימית במדינות, למען מטרות של הגנה על ביטחון המדינה, ביטחון הציבור והעניינים הכספיים של המדינה, וכן מטרות אכיפה של דין פלילי או כאשר הצעד הכרחי כדי להגן על זכויות של אחרים.[251]

הסדר אחר, אף כי הוא ברמת הנחיות בלבד ואינו מהווה דין נורמטיבי, נמצא בהנחיות האו"ם: United Nations Guidelines Concerning Computerized Personal Data Files.[252] מסמך זה קובע אוריינטציה בלבד, כאשר יישום הרגולציה ביחס למידע אישי ממוחשב הושאר לשיקול דעתה של כל מדינה. ההנחיות מגדירות שורה של עקרונות ביחס לסטנדרט מינימום של הגנה על הפרטיות ברמה המדינתית:

---

[248] ראו: **Charter of fundamental rights of the European Union,** OJC 364 http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000Y1218(01)&model=guichett (ביקור אחרון: 24.12.01).

[249] מדובר בסקר שנערך על-יד המרכז לפרטיות אלקטרונית בוושינגטון והמרכז הבינלאומי לפרטיות בלונדון. הדו"ח סוקר את מצב הזכות לפרטיות בכחמישים מדינות, ובוחן בהם נושאים של פרטיות, לרבות הגנה על מידע, ציתות טלפוני, מאגרי מידע, מערכות זיהוי וחופש המידע. נמצא ב: www.privacyinternational.org/survey/phr2000/html (ביקור אחרון: 23.12.01).

[250] **Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data** (ETS No. 108, Strasbourg, 1981). נמצא ב: http://www.coe.fr/eng/legaltxt/108e.htm ((ביקור אחרון: 23.12.01).

[251] יהונתן בר-שדה, **האינטרנט והמשפט המסחרי המקוון** (1996) 184-186.

- **חוקיות והוגנות**- יש לאסור איסוף מידע באופן שאינו חוקי או שאינו הוגן.
- **דיוק**- מחויבות המחזיק במידע לבצע בדיקות קבועות של דיוק ורלוונטיות המידע המאוחסן.
- **פירוט המטרות**- המטרה שלשמה נאסף המידע צריכה להיות ספציפית, לגיטימית וידועה, כך שניתן יהיה להגביל את האחסון בתחום, בזמן וביכולת השימוש.
- **גישה**- מי שמציג הוכחה לזיהוי יהיה זכאי לדעת האם מידע אודותיו נאסף.
- **איסור הפליה**- למעט חריגים, אין לאפשר איסוף מידע שבאמצעותו ניתן יהיה להפלות; מידע זה כולל מידע על גזע, צבע עור, נטייה מינית, דעה פוליטית, דת ואמונות אחרות לרבות חברות בארגונים או איגודים.
- **סיוג תחולה**- חריגים אפשריים רק אם הם הכרחיים להגן על ביטחון לאומי, סדר ציבורי, בריאות ומוסר הציבור וזכויותיהם של אחרים, וזאת בתנאי שהחריגים יפורטו בחוק ויקבעו מגבלות לכך. ביחס לאיסור הפליה ומידע הקשור לכך, יש צורך במגבלות נוספות על החריגים בהתאם להגנה הבינלאומית על זכויות אדם.
- **ביטחון**- יש לנקוט אמצעים מתאימים על-מנת להגן על קבצי מידע הן מפני תקלות והן מפני התערבויות מכוונות.
- **פיקוח וסנקציות**- החוק בכל מדינה יגדיר איזו רשות תהיה אחראית לפקח על העקרונות שצוינו לעיל. במקרה של הפרה יש להטיל סנקציות פליליות וסעדים מתאימים לנפגעים.
- **זרימת מידע מעבר לגבולות המדינה**- במקרים שקיימת הגנה חוקית מתאימה על המידע יש לאפשר זרימה של המידע באותן טריטוריות.
- **תחולה**- ניתן ורצוי להרחיב את העקרונות גם למידע שמאוחסן באופן שאינו ממוחשב. כמו כן ההנחיות מציעות ליישם את העקרונות ביחס לקובצי מידע שנמצאים בידי גופים שלטוניים, זאת בכפוף לתיקונים נדרשים.[253]

הסדר בינלאומי נוסף, אם כי חשיבותו הנורמטיבית פחותה בהרבה, קיים בדמות הנחיות ארגון ה-OECD לגבי נתונים אלקטרוניים: **OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, Recommendation of the Council**.[254] הנחיות אלו קובעות את העקרונות הבסיסיים לגבי איסוף, שימוש, וגילוי של נתונים ומידע אישי. בהתאם להנחיות, יש להטיל מגבלה על איסוף נתונים אישיים בדין מקומי, נדרשת שקיפות באשר למטרת איסוף המידע ובהתאם השימוש, גילוי אפשרי רק בהסכמה, פיתוח הגנות המעוגנות בחוק, אימוץ מדיניות של פתיחות ביחס לנתונים אישיים, ושימור זכות היחיד לקבל אישור שנתונים אודותיו נאספו וכן

---

[252] ראו: United Nations Guidelines Concerning Computerized Personal Data Files, adopted by the General Assembly on 14 December 1990.

[253] ראו: http://europa.eu.int/comm/internal_market/en/dataprot/inter/un.htm.

[254] OECD, "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

לאפשר לו לעיין בנתונים, לבדוק את נכונותם ולערער על הנתונים במידה שהם שגויים.[255] הוראות בינלאומיות נוספות ניתן למצוא באיחוד האירופאי.

3. האיחוד האירופאי

האיחוד האירופאי "חי ונושם" לאור האמנות שהקימו אותו (אמנת רומא, אמנת "החוק האירופאי היחיד" ואמנת מסטריכט), ולפיהן תחומים מסוימים נמסרו מלכתחילה לסמכותה הבלעדית של הקהילייה, תחומים אחדים הוכפפו למעין "סמכות מקבילה" ותחומים אחרים נותרו בסמכותן הבלעדית של המדינות.[256] לפיכך, ניתן לראות בדברי החקיקה השונים של האיחוד האירופאי[257] הסתייגויות הנוגעות לתחומים שהושארו מחוץ לסמכות האיחוד, כמו נושאים של ביטחון ואינטרסים מדינתיים כלליים (להבדיל מכלכליים), ואפשרות לחקיקה מקומית שתאפשר חריגה מההוראות במקרים אלה. היבט נוסף של חלוקת הסמכויות המוזכרת לעיל, ניתן למצוא בדברי החקיקה השונים המתייחסים ברובם למגזר הפרטי ולא לרשויות האכיפה במדינות השונות. התייחסות כזאת, ניתן למצוא בעיקר בהקשר של הטלת חובות על גוף פרטי (כמו על ספקי שירות) לפעול בהתאם לבקשות רשויות האכיפה.

בתת-פרק זה נסקור את קביעת מסגרת-הפעולה באיחוד האירופאי בכל הנוגע להגנה על מידע אישי והנחיות נוספות שהרחיבו קו פעולה זה. בהמשך נדון במסגרת המשפטית שנוצרה לאחר אירועי ה- 11 בספטמבר, כאשר עיקר הדיון יוקדש לאמנת פשעי-המחשב שנפתחה לחתימות המדינות, ולחוק הבריטי החדש, המיועד להתמודד עם הצורך במתן סמכויות מתאימות לרשויות האכיפה למיגור הטרור מול הצורך לשמור על זכויות האדם במדינה.

3.1 הדירקטיבה האירופאית להגנה על מידע אישי

הדירקטיבה האירופאית להגנה על מידע אישי משנת 1995 (EU Directive on Data Protection),[258] מחייבת את המדינות החברות לחוקק חוקים שיחולו על המגזר הפרטי להגנה על הזכות לפרטיות ביחס לאיסוף, עיבוד, אחסון והעברה של מידע אישי. דירקטיבה זו אפשרה למעשה תנועה חופשית של נתונים אלקטרוניים בין מדינות האיחוד, וזאת תוך הבטחה כי הפרטים ייהנו מרמה גבוהה של הגנה מפני ניצול-לרעה של נתונים אלה.[259] עיקרי הדירקטיבה:

---

[255] בר-שדה, לעיל הערה 251, בעי 186-187.

[256] ערן לב, **משפט הקהילייה האירופית** (1994) 32-34.

[257] החקיקה הקהילייתית מורכבת מארבעה סוגי חקיקה: **האמנה** הינה דבר החקיקה העליון, ולכן ניתן להשוותו לחוקה במדינה פדראלית, אולם אין לה תחולה ישירה בתוך המדינות; **תקנות (Regulation)** שנחשבות לדבר החקיקה הקרוב ביותר לחקיקה מקובלת במדינה ריבונית, והן מהוות דבר החקיקה היחיד באיחוד שיש לו תחולה ישירה; **הנחיות (Directives)** הינה יצירה קהילייתית "מקורית" בהיותה חקיקה הקובעת מטרות מחייבות, אך משאירה למדינות החברות את קביעת הדרכים ליישום אותה מטרה. השימוש בתקנות מקובל יותר באותם תחומים שבסמכותה הברורה של הקהילייה וככלי לקירוב והרמוניזציה של המשפט הפנימי במדינות החברות; **החלטות (Decision)** המצויות ברמה הנמוכה ביותר במדרג הנורמטיבי ודומות לצו אינדיווידואלי. ראו לב, **שם**, בעי 43-45.

[258] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data נוסח הדירקטיבה נמצא ב: www.cdt.org/privacy/eudirective/EU_Directive_.html (ביקור אחרון: 24.12.01).

[259] בר-שדה, לעיל הערה 251, בעי 187.

מידע אישי (personal data) מוגדר בדירקטיבה ככל מידע הנוגע לאדם מזוהה, או שניתן לזהותו, בעקיפין או במישרין, במיוחד ביחס למספר מזהה או לגורם אחד או יותר הספציפיים לזהותו הפיסית, הפסיכולוגית, המנטלית, הכלכלית, התרבותית או באמצעות מספר תעודת זהות.

הדירקטיבה מגדירה מספר סייגים על תחולת ההסדר. סעיף 3(2) קובע מצבים בהם התחולה על כל פעולת עיבוד מידע מסויגת:

- במהלך פעילות שנופלת מחוץ לדין האיחוד (בהתאם לאמנה המייסדת), ובכל מקרה של עיבוד מידע הנוגע לביטחון הציבור, הגנה, ביטחון המדינה (לרבות אינטרסים כלכליים) ופעילויות המדינה בתחומים של משפט פלילי, במסגרת האמנות המקימות את האיחוד האירופאי, הוסכם כי דינים אלה יושארו בסמכויות המדינות ולכן קיים החריג.
- עיבוד מידע על-ידי אדם פרטי במהלך פעילות פרטית וביתית.
- יש לזכור כי אף שהחקיקה הפנימית בכל מדינה חייבת להיעשות ברוח הדירקטיבה, סעיף 5 קובע מפורשות, כי המדינות רשאיות להגדיר מצבים נוספים בהם עיבוד מידע אישי יהיה מותר.

בהתאם לדירקטיבה, כל עסק נדרש לעמוד במספר תנאים. כך, בין היתר, יש להבטיח כי מידע פרטי שייאסף מלקוחות יעובד באופן חוקי והוגן, למטרות ספציפיות, מפורשות ולגיטימיות, המידע יהיה מעודכן ויישמר כראוי. בנוסף העסק מחויב להודיע ללקוחות מי אחראי על המידע, על הזכות לגשת למידע ועל הזכות לתיקונים. הדירקטיבה מדגישה כי לאחר איסוף החומר אין לעבדו אלא אם הלקוח נתן באופן ברור את הסכמתו. הפרת החובות מעניקה לאדם זכות פיצוי, כאשר הסעדים יינתנו לפי חוקי מדינת הלאום. כמו כן, המדינות נדרשות להקים גוף מפקח עצמאי שיהיה בעל סמכויות מגוונות, לרבות חקירה, מעקב וחסימה.

ביחס למדינות מחוץ לאיחוד, קיים איסור על העברת מידע פרטי למדינות שלא עומדות בסטנדרט האירופאי להגנת על מידע. ארצות הברית ומדינות האיחוד האירופאי הגיעו להסכמה המכונה "safe harbor framework", לפיה חברות אמריקניות יחשבו כעונות על הסטנדרט תוך מתן אפשרות לרגולציה עצמית - ולא ממשלתית - בהתאם לשבעה עקרונות בסיסיים: הודעה, בחירה, הגבלת העברות נוספות, ביטחון המידע, רלוונטיות, גישה ואכיפה.[260]

בקשר של מדינות זרות, ביום 4.12.01 אישרה ועדת המדינות החברות הצעה של הנציבות לפסקאות חוזיות סטנדרטיות שתאומצנה על-ידי גופים מעבדי-מידע במדינות שאינן מדינות איחוד. אמצעי זה נועד למנוע סירוב העברות מידע בשל חוסר התאמה לדרישות האמנה.[261]

3.2 יישום הדירקטיבה על-ידי המדינות החברות

אף על-פי שהדירקטיבה היא משנת 1995, החקיקה הרלוונטית במדינות רבות נכנסה לתוקפה רק בתחילת שנת 2000. יתר על כן, כנגד חמש מדינות הוגשו הליכים בפני בית הדין האירופאי בשל איחור באימוץ חקיקה מתאימה בהתאם ללוח הזמנים שנקבע בדירקטיבה (לוקסמבורג, אירלנד,

[260] לדו"ח הועדה של האיחוד האירופאי מיום 13.02.2002 אשר בדקה לאחרונה את יישום ההסכם בין ארצות הברית לאיחוד האירופאי בנוגע להגנת המידע הפרטי ראו: http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf (ביקור אחרון: 18.2.02).

[261] ראו: http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/art31.htm (ביקור אחרון: 23.1.02).

גרמניה, צרפת ודנמרק). מתוך אותן מדינות, רק בדנמרק נחקק בינתיים החוק הנדרש שנכנס לתוקפו ביולי 2000.[262]

הדירקטיבה משנת 1995 להגנה על מידע אישי, יצרה באיחוד האירופאי מסגרת עבודה מקיפה, שבה התקבלו הנחיות והחלטות נוספות המרחיבות את היקף התחולה של העקרונות. הוראות מקיפות נוספות התקבלו ביחס לשוק הטלקומוניקציה, כאשר אלה מתייחסות בעיקרן אל חובות שונות המוטלות על ספקי שירות באינטרנט, ולכן יידונו בנפרד במסגרת הפרק על איסוף מידע בידי גורמים מסחריים שהלן.

3.3. התפתחויות משפטיות לאחר ה- 11 בספטמבר

Convention on Cybercrime 2001

לאחר ה-11 בספטמבר נחתמה אמנה נוספת אשר עשויה להשפיע על סמכויות האכיפה, והיחסים שבין המדינה לספקי השירות. מדובר באמנה בינלאומית לפשעי-מחשב (Convention on Cybercrime) מבית היוצר של מועצת אירופה.[263] האמנה נפתחה לחתימותיהן של מדינות אירופה ושל מדינות נוספות שהשתתפו בניסוחה (ישראל אינה נכללת בהן). מחודש נובמבר ועד מועד כתיבת דברים אלה (דצמבר 2001) חתמו עליה 31 מדינות, לרבות ארצות הברית, קנדה ויפן. האמנה תכנס לתוקף, רק לאחר שחמש מדינות יאשררו אותה (יקלטו את האמנה בדין הפנימי) ומתוכן שלוש לפחות חייבות להיות חברות במועצת אירופה.[264]

דברי-ההסבר[265] מבהירים כי האמנה באה להגשים שלוש מטרות עיקריות: (1) הרמוניזציה בדין הפלילי הלאומי בתחומים של פשעי-מחשב; (2) מתן סמכויות פרוצדורליות לאומיות הנדרשות לחקירה והעמדה לדין בגין עבירות מחשב ועבירות אחרות שבוצעו באמצעות מערכות מחשב; (3) הקמת מערכת יעילה לשיתוף פעולה בינלאומי. בהתאם למטרות אלה האמנה בנויה מארבעה פרקים: מונחים, אמצעים שיש לאמץ ברמה הלאומית הן ביחס לדין מהותי והן ביחס לדין פרוצדורלי, שיתוף פעולה בינלאומי וסעיפי סיוג ותחולה. האמנה מגדירה תשע עבירות כדין מהותי: גישה לא-חוקית, יירוט לא-חוקי, התערבות במערכות, שימוש לרעה במכשור, זיוף הקשור לאמצעי מחישוב, הונאה הקשורה למחשוב, פורנוגרפית-ילדים, ועבירות הקשורות לזכויות יוצרים וזכויות שכנות. נושאים המכוסים במסגרת הדין הפרוצדורלי חלים לא רק על עבירות הבסיס שצוינו לעיל, אלא גם על כל עבירה המבוצעת באמצעות מערכות מחשב או שהראיות על העבירה הן באמצעים אלקטרוניים. האמנה מגדירה שורה של סמכויות הנתונות לרשויות האכיפה:

- הוראת שמירה על מידע מאוחסן (expedited preservation of stored data)- סעיף 16.

---

[262] ראו: Implementation of Directive 95/46 : http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm

[263] נוסח האמנה נמצא ב: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. מועצת אירופה הינה גוף בינלאומי שהוקם בשנת 1949. כיום חברות בגוף 41 מדינות לרבות מדינות ממזרח אירופה.

[264] מעקב אחר המדינות שחותמות על האמנה ומעמדן: http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=8&DF.

[265] http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

- שמירה וחשיפה חלקית של מידע "תקשורתי" (expedited preservation and partial disclosure of traffic data)- סעיף 17.
- צווי הפקת מידע (production order)- סעיף 18.
- חיפוש ותפיסה של מידע ממוחשב (search and seizure of computer data)- סעיף 19.
- איסוף בזמן-אמת של מידע "תקשורתי"(real-time collection of traffic data) -סעיף 20.
- יירוט בזמן-אמת של מידע תוכני(.interception of content data)- סעיף 21.

כל הסמכויות שניתנו לרשויות כפופות לסעיפים 14-15 לאמנה, לפיהם יש לתחום את הסמכויות בתנאים ספציפיים ומוגדרים בחוק.

הפרק השלישי באמנה מגדיר הוראות נוספות ביחס לעבירות מחשב מסורתיות והוראות סיוע הדדי כמו גם כללי הסגרה. ההוראות דנות בסיוע בינלאומי בשני סוגים של מקרים: במקרה שיש בסיס משפטי בדמות אמנות, חקיקה הדדית וכדומה, אזי ההסכם הקיים יורחב גם למצבים המוזכרים באמנה, ובמצב בו אין בסיס משפטי קודם יחולו ההוראות שנקבעו בפרק זה. בנוסף מכיל הפרק הוראה מיוחדת בדבר גישה טרנס-גבולית למידע מחשבי מאוחסן שאינו דורש סיוע הדדי (עם הסכמה או זמינות ציבורית) ומאפשר הקמת רשת שמטרתה להבטיח סיוע מהיר בין המדינות החתומות על האמנה.

סעיף 22 עוסק בסמכות שיפוט, וקובע סדרה של קריטריונים לפיהם צדדים מחויבים להקים סמכות שיפוט על עבירות פליליות הקבועות באמנה. הביסוס הוא על עקרונות מוכרים של טריטוריאליות ולאומיות. הסעיף מאפשר גם יצירת בסיסי סמכות שיפוט נוספים במסגרת הדין הפנימי. במקרים שבהם תקום סמכות שיפוט ליותר ממדינה אחת, למשל במתקפות וירוס חוצה-גבולות באינטרנט, על המדינות הנוגעות בדבר להיוועץ אחת ברעותה על-מנת לקבוע באיזו מדינה יתנהל הדיון המשפטי. סעיף חשוב נוסף הוא סעיף 42 העוסק בהסתייגויות (Reservations) ומאפשר מספר הסתייגויות (מדובר ברשימה סגורה), לאור אופיה של האמנה ומהותה.

3.4 החוק הבריטי החדש למלחמה בטרור

חוק בריטי חדש ומקיף אושר לאחרונה בפרלמנט: **Anti-terrorism, Crime and Security Act 2001.**[266] החוק נועד לתקן את חוק הטרור משנת 2000, ולקבוע הוראות נוספות ביחס לטרור וביטחון. בין היתר ולענייננו החוק מרחיב את סמכויות הסיכול האכיפה של רשויות השלטון, מאפשר שמירת מידע תקשורתי לתקופה ממושכת וקובע הוראות לגילוי מידע לרשויות. מעבר לכך, החוק עוסק בשורה של תחומים הכוללים טיפול בנכסים ובכספים של ארגוני טרור, הגירה, עבירות שנאת זרים, נשק להשמדה המונית, בטיחות של רעלים ותעשיה גרעינית, ביטחון בתחום התעופה, שוחד ושחיתות ועוד.

3.5 איסוף מידע על-ידי ספקי שירות ברשת

CyberCrime Treaty

האמנה בנושא פשעים ברשת (Cyber-crime Treaty), שנדונה לעיל, עוסקת באופן נרחב בהטלת חובות על ספקי שירות, וזאת במסגרת הכוללת של צעדים פרוצדורליים וסמכויות המוקנות לרשויות האכיפה. ראשית יש לציין כי אמנה זו מגדירה באופן רחב ביותר את המונח "**ספק שירות**". המונח מיועד לכלול קטגוריה רחבה של אנשים וגופים המשמשים בתפקיד מסוים בהתקשרויות או בעיבוד מידע במערכות מחשב. בהתאם להגדרה, ברור כי גם גופים פרטיים וגם גופים ציבוריים, שמספקים למשתמשים יכולת להתקשר עם אחר, כלולים בהגדרה. לכן, אין משמעות לשאלה, האם המשתמשים יוצרים קבוצה סגורה או שהשירות מוצע לציבור, או האם השירות ניתן בחינם או בתשלום. הקבוצה הסגורה לה מספקים את השירות יכולה להיות עובדים בחברה פרטית להם השירות מוצע דרך שרת של החברה. כמו כן, ההגדרה כוללת גופים המאחסנים או מעבדים בדרך אחרת מידע בעבור הגופים שהוזכרו לעיל או בעבור המשתמשים. לדוגמא, ההגדרה כוללת שירותים של "אירוח" ו"מטמון" (hosting and caching), כמו גם שירותים של חיבור לרשת. יחד עם זאת, ספק תוכן בלבד אינו מיועד להיכלל בהגדרה של "ספק שירות", ובלבד שאיננו מציע גם קישור או שירותי עיבוד מידע.[267]

במסגרת הסמכויות הדיוניות שקובעת האמנה, מוטלות חובות על ספקי השירות. כך, בסעיף 18 מחייבת האמנה חקיקה, לפיה תוכלנה הרשויות לכפות על ספק שירות להעביר מידע על לקוח, מידע שבאמצעותו ניתן יהיה לקבוע את סוג ההתקשרות, זהות המשתמש ומיקומו הגיאוגרפי. ספקי השירות גם יחויבו בהתאם לסעיפים 20-21 לספק מידע תוכני והתקשרותי בזמן-אמת על התקשורת שמתנהלת על גבי שרתיהם. ראוי עוד לציין כי למרות קיום הסעיפים המחייבים מגבלות ועיגונים ברורים בחקיקה, האמנה מאפשרת לדרוש מספק השירות לשמור על סודיות גם במסגרת שיתוף הפעולה עם הרשויות, ויש לתהות מה ההשפעה שתהיה לחובת סודיות זו מחד גיסא, וליכולת לכפות על הספקים לספק מידע מאידך גיסא, על הקשר המסחרי (והמשפטי) שבין ספק השירות לצרכנים.

חקיקה בריטית נוספת בעלת חשיבות משנת 2000 היא - **Regulation of Investigatory Powers Act 2000**. למעשה, החקיקה מחייבת נותני שירותים לחשוף מפתחות הצפנה או את מיקום המפתחות, אך מטרתה להבטיח איזון ראוי בין יכולת רשויות האכיפה להתערב בתשדורות אלקטרוניות לבין קביעת הגנה הכרחית על זכויות הפרט והאינטרסים העסקיים שיש להגן עליהם בשעת פעילות כזו מצד הרשויות. התקנות מתייחסות לארבע פעולות שונות: יירוט תשדורות, מעקב צמוד, מקורות מידע אנושיים וחשיפה של מידע מוצפן. את הפעולות ניתן יהיה לבצע רק לאחר קבלת צו מתאים, אשר חייב לעמוד על בסיס ראייתי לאחת העילות המנויות: הפעולה לטובת ביטחון המדינה, למניעת פשע חמור או להבטחת אינטרסים כלכליים של בריטניה.

בכפוף להוראות החוק, נותן שירותים יהיה כפוף כעת למחויבות משפטית להעניק גישה לתשדורות ולחשוף כל מידע מוגן, כלומר כל מידע מוצפן, בין אם מדובר בתשדורות שעדיין

---

[266] http://www.hmso.gov.uk/acts/acts2001/20010024.htm (ביקור אחרון: 23.12.01)

[267] ראו את דברי ההסבר לאמנה: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (ביקור אחרון: 24.01.02).

מתנהלת, ובי אם מדובר במידע המאוחסן אצל נותן השירות. ראוי להעיר כי קיימת עמדה לפיה חוקיות החוק מוטלת בספק לאור האמנה האירופאית לזכויות אדם אשר נקלטה בדין הבריטי בחוק (**Human Rights Act 1998**).[268]

סקטור הטלקומוניקציה

תחום הטלקומוניקציה זכה להתייחסות חקיקתית נרחבת באיחוד האירופאי, וזאת כחלק ממגמה להבטיח תחרות פתוחה בשוק זה. במסגרת ההסדרה התייחסו גם לתחום הפרטיות ב: **EU Directive on Personal Data and Privacy in the Telecommunication Sector**.[269] הדירקטיבה כופה טווח רחב של מחויבויות על ספקי שירות להבטיח את הפרטיות של המשתמשים באמצעי-התקשורת, לרבות פעולות הקשורות לאינטרנט. הכללים מתייחסים לתחומים, שעד להנחיות אלה נפלו למעשה "בין הכיסאות" במסגרת הכללית של דיני ההגנה על מידע. התחולה היא על עיבוד מידע אישי בהקשר של שירותי טלקומוניקציה הזמינים לציבור באיחוד, ובמיוחד שירותים דיגיטליים (Integrated Services Digital Network-ISDN) ותחום הטלפונים הניידים.

הדירקטיבה מטילה הגבלות על גישה למידע. טכנולוגיה של זיהוי המתקשר (Caller ID) חייבת לשלב אפשרות לחסימה של המספרים המועברים. מידע שנאסף במסירת ההתקשרות חייב להיות "מטוהר" עם סיום התקשרות. למנויים יש זכות לקבל חשבונות שלא יפרטו פריטים וסוגי שירותים. הספק צריך לאפשר למנוי לחסום שיחות אוטומטיות המגיעות מצדדים שלישיים. מרשם לקוחות חייב להיות מצומצם לפרטים ההכרחיים בלבד. שימוש לצורכי שיווק בהודעות מוקלטות ומשלוח פקסים חייב להיות מוגבל למנויים שהסכימו לכך.

כעבודת המשך לדירקטיבה זו הציעה הנציבות ביולי 2000 דירקטיבה על עיבוד מידע ופרטיות בסקטור התקשרות האלקטרונית.[270] ההצעה הוגשה כחלק מחבילה כוללת, שמטרתה לחזק את התחרות לתקשורת אלקטרונית בשוק האירופאי. ההצעה היא, כי הדירקטיבה תחליף את הדירקטיבה הקיימת משנת 1997, על-ידי הרחבת ההגנה הקיימת להתקשרות של יחיד לקטגוריה טכנולוגית ומשפטית רחבה יותר של "התקשרויות אלקטרוניות" (electronic communications). ההצעה מחליפה הגדרות קיימות של שירותי טלקומוניקציה ורשתות, בהגדרה חדשה של שירותי התקשרויות אלקטרוניות ורשתות. בנוסף, ההצעה מוסיפה הגדרות חדשות והגנות לשיחות, התקשרויות, מידע תקשורתי (traffic data) ומידע על מיקום (location data), וזאת במטרה להגביר את זכות הצרכן לפרטיות ולתת אפשרות שליטה בעיבוד של סוגי מידע שונים.

הוראות מוצעות אלה יבטיחו, לדוגמא, את ההגנה על כל המידע הקשור להעברות באינטרנט, יאסרו שיווק מסחרי לא-משדל באמצעות אי-מייל (Spam) ללא הסכמה מראש בשיטת ה"opt-in", ויקנו הגנה למשתמשי טלפונים ניידים מפני איתור מיקום מיידי ומהאזנה. הדירקטיבה המוצעת

---

[268] **שם**, 60.

[269] European Parliament and Council Directive 97/66/EC of 15 December 1997 concerning the processing of Personal Data and the Protection of Privacy in the Telecommunication Sector, OJL 24 (30.01.1998).

[270] A Proposal for a Directive of the European Parliament and of the Council concerning the processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector (2000) 385, OJC 365 (19.12.00).

מאפשרת עוד למנויי השרתים והספקים לבחור האם ברצונם להיות רשומים במרשמים ציבוריים. יחד עם זאת, יש לציין כי גם דירקטיבה מוצעת זו, מעניקה למדינות אפשרות להגביל את הוראותיה במגבלות של צורכי ביטחון ואכיפה.[271] הצעה זו נדונה בפרלמנט באירופאי, שכבר העביר שינויים אחדים, על-מנת לאפשר Spam, ולהגביל את שמירת המידע של ספקי השירות למטרות אכיפת החוק. לפי התיקון כל מעקב וציתות חייב להיות הכרחי, מתאים, פרופורציונלי ומוגבל בזמן. האמצעים חייבים להיות מעוגנים בחוק חרות ומאושרים על בסיס פרטני על-ידי רשות מתאימה בכפוף למחויבות לאמנה האירופאית על זכויות אדם ולפסיקת בית הדין לזכויות אדם, כך שמעקב אלקטרוני רחב-היקף או כללי אינו אפשרי.[272]

מידע אישי וחתימה אלקטרונית

EU Directive 1999/93/EC on Electronic Signatures[273]: דירקטיבה זו מרחיבה את הוראות הדירקטיבה על מידע אישי, ומטילה חובת פיקוח ושמירת מידע על גופים המעניקים שירותים ביחס לאישורי חתימה אלקטרונית (certification-service-providers). גופים אלה רשאים לאסוף מידע אישי רק ישירות מנשוא המידע או לאחר קבלת הסכמתו המפורשת, וכן רק ביחס לנדרש ומתחייב לשם הוצאת האישור. אין לאסוף את המידע למטרות אחרות (סעיף 8).

4. ארצות הברית

4.1 רקע כללי

הזכות לפרטיות מוגנת בארצות הברית בתיקון הרביעי לחוקה:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[274]

התיקון הרביעי לחוקה מגביל את סמכויות הממשל לפגוע בפרטיות אזרחי המדינה, ומחייב את הממשל לא לפגוע בזכויות אלה ללא עילה חוקית. התיקון הרביעי לחוקה מציב סטנדרט של "probable cause",[275] כאשר הממשל מבקש ליירט תקשורת או לקבל צו חיפוש, שהרי ביצוע פעולות מסוג זה עלול לפגוע בזכות לפרטיות של הנעקב ושל אחרים. את העילה יש לפרט בתצהיר. כמו כן, ישנה מערכת בלמים ואיזונים בחוקים השונים ובפסיקה.

---

[271] http://www.privacyinternational.org/survey/phr2000/overview.html#Heading12 (24.12.01)

[272] לשינויי הדירקטיבה במסגרת ועדות הפרלמנט האירופאי, ראו: http://www.privacyinternational.org/issues/cybercrime/index.html#coe (24.12.01).

[273] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJL 013 (19.01.00) p. 0012-0020 http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31999L0093&model=guichett.

[274] U.S. Const. Amend. IV.

[275] ראו: **United States v. Cavanagh**, 807 F.2d 787 (9th Cir. 1987).

באוקטובר 2001 אושר ה- USA PATRIOT Act. החוק מעצים ומרחיב את סמכויות המעקב של הרשויות הממונות על אכיפת החוק בארצות הברית (domestic law enforcement), ושל הסוכנויות לביטחון, העוסקות באיסוף מודיעין בינלאומי (international intelligence agencies). יש הטוענים שהחוק הזה משנה את מערכת הבלמים והאיזונים שעוצבה בשנות השבעים, בעקבות שימוש לא מבוקר שנעשה בסמכויות מעקב של הסוכנויות השונות (מעל 10,000 אזרחים היו נתונים תחת מעקב קבוע, כולל מרטין לותיר קינג). לדוגמא, לפי החוק החדש, על-מנת שבית משפט ייחייב ספק שירות למסור יומני דואר וכתובות של אדם מסוים, הסטנדרט שנדרש הוא רק שהממשל יציג עובדות לפיהן סביר להאמין שהרישומים רלוונטיים לחקירה שמתקיימת. שאלה היא אם סטנדרט זה עולה בקנה אחד עם תנאי ה- "probable cause" שבתיקון הרביעי לחוקה. מנגד, יש הטוענים שצריך להבחין בין איסוף "מידע תוכני" לגבי אדם מסוים לבין איסוף מידע מסוג "numerical information" (כגון: מספרים שאליהם חייג, או כתובות דוא"ל שאיתן ניהל תכתובות), שהסטנדרט עבור איסופו יכול להיות נמוך יותר.

החוק החדש מכניס שינויים בכחמישה עשר חוקים קיימים. שינויים רבים פוגעים בזכות לפרטיות בתקשורת האלקטרונית שמנהלים האזרחים. יתכן שהממשלה תהא רשאית כעת לעקוב אחרי גולשים תמימים, אם הקישו מושג "מעורר חשד" במנוע חיפוש באינטרנט - כל שנדרש מהממשלה הוא להצהיר בפני בית משפט שהמעשה עשוי להוביל למידע רלוונטי לחקירה שמתנהלת באותה העת. אותו אדם שמצותתים למחשבו, אינו צריך להיות מושא החקירה או חשוד בעבירה כלשהי.

4.2 פיקוח משפטי על פגיעה בפרטיות על-ידי רשויות האכיפה

החוק האמריקני מכיר בארבעה אמצעים לפיקוח: יירוט שידורים לרבות האזנות (interception orders), צווי חיפוש ותפישה של חפצים ממשיים (search warrants), צווי איתור שנועדו לבדוק למי או מהיכן בוצעה שיחה (pen/trap order) וצווי בית משפט וקבלת מידע על-ידי רשויות האכיפה (הזמנת מידע) subpoena and court orders. הצווים השונים דורשים רמה שונה של ודאות והתערבות שיפוטית ביחס ישר לפגיעה בזכויות כמו פרטיות וחופש ביטוי.

4.2.1 האזנה ויירוט

א. מחוץ לגבולות ארצות הברית

רשויות המודיעין אינן מוגבלות בהפעלת אמצעי פיקוח מחוץ לארצות הברית. אין כל חיקוק בנושא, למעט הנחיה של הנשיא רייגן, התקפה עד היום.[276] ההנחיה קובעת כי במקרה שאזרח או תושב קבע אמריקני הוא נשוא ההאזנה,[277] יש לקבל אישור התובע הכללי, שבידיו ההחלטה, אם קיימת עילה מסתברת שהיעד הוא סוכן זר.

---

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

[277] "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an associated which is a foreign power, as defined in 50 U.S.C. §1801(a)(1), (2), or (3). See 50 U.S.C. §1801(i).

ב. בתוך ארצות הברית

שני חוקים מסדירים את הפיקוח בתוך ארצות הברית. האחד הוא The Federal Wiretap Act (1968),[278] המאפשר הפעלת אמצעי פיקוח והאזנה, באמצעות צו בית משפט, לאחר שמצא, על סמך תצהיר המדינה, כי יש עילה מסתברת שפשע בוצע, מבוצע או עתיד להתבצע. החוק מכיל רשימה סגורה של פשעים בגינם ניתן לבקש צו במסגרת חוק זה.[279] בחוק החדש[280] הוספו לרשימה פעולות טרור ועבירות לפי חוק הונאה במחשבים.[281]

The Foreign Intelligence Surveillance Act of 1978[282] (FISA) מאפשר הוצאת צווי האזנה, על-ידי בית-דין מיוחד, לסוכנים זרים.[283] גם פה יש להראות עילה מסתברת ואולם על-מנת להוציא צו למי שהוא אזרח או תושב קבע אמריקני יש להראות שהמידע הכרחי לביטחון הלאומי ואילו לגבי מי שאינו אזרח, יש להראות שהמידע קשור לביטחון הלאומי. יש לשים לב להגדרת סוכן זר, לפיה חברות של אזרח אמריקני בארגון טרור אינה עולה לכדי הגדרת "סוכן זר" ויש צורך שאותו אזרח יפעל לקידום המטרות הטרוריסטיות. ההבדל נעוץ בהגנה שמעניק התיקון

---

[278] The Omnibus Crime Control and Safe Streets Act of 1968 commonly known as the "wiretap law".

[279] 18 U.S.C. §2516(1).

[280] USA PATRIOT Act §§ 201-202.

[281] Computer Fraud and Abuse Act (CFAA), 18 USC §1030.

[282] Pub. L. No. 95- 511, 92 Stat. 1783, codified as 50 U.S.C. §1801.

[283] ראו: United States Signals Intelligence Directive, 27 July 1993. המושג 'Agent of a foreign power' מוגדר כך:

a. Any person, other than a U.S. person, who:
(1) Acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor;
(2) Acts for, or on behalf of, a foreign power that engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
b. Any person, including a U.S. person, who:
(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a foreign power, which activities involve, or may involve a violation of the criminal statutes of the United States; or
(2) Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such foreign power, which activities involve or are about to involve, a violation of the criminal statutes of the United States; or
(3) Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for, or on behalf of, a foreign power; or
(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in such activities.

הראשון לחוקה לאזרחים אמריקנים לפיו חברות ופעילות באירגון טרור יכול שיהיו לקידום רעיון מסויים, ולא ניתן למנוע מאזרח באופן שיטתי להביע את דעתו. במקרי חירום (סכנת חיים או פגיעה גופנית חמורה), ניתן להפעיל אמצעי פיקוח לפי שני החוקים גם ללא צו שיפוטי .

4.2.2 צווי איתור pen/trap order[284]

הצווים נועדו לאתר את המיקום של שיחות יוצאות או נכנסות. בתי המשפט מאשרים את הצווים כל אימת שהם יכולים לספק מידע רלוונטי בגין עבירה פלילית, שיקול הדעת של בית המשפט הוא בעיקר טכני לגבי אופן הגשת הבקשה. סעיף 216 לחוק החדש מרחיב את ההיתר לביצוע איתורים מתקשורת קווית ומוסיף תקשורת אלקטרונית.[285] סעיף 214 לחוק החדש 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).[286] מערכת Carnivore של ה-FBI מבצעת פעולה דומה באינטרנט. המערכת ממוקמת בצמתי מידע גדולים ומאתרת את המקור ואת היעד של המסרים המועברים ברשת. הבעיה הנוצרת היא, שהמערכת סורקת בפועל כמות גדולה מאד של מידע, על-מנת למצוא את פיסת המידע הנקודתית שרק לגביה יש אישור לביצוע האיתור, ובנוסף, לא ניתן להפריד בין התוכן לבין מידע אודות היעד, משום שהם מועברים ביחד. לאור העובדה שה- FBI איננו מפרט את אופן פעולת המערכת קיים חשש שהמערכת אוספת מידע תוכני ולא רק את מקור המסר ויעדו.[287]

4.2.3 צווי חיפוש ותפישה

צווי חיפוש מוצאים באישור שופט כאשר קיימת עילה מסתברת שבוצעה עבירה. בעת ביצוע החיפוש או אחריו יש להודיע לבעל המקום שבוצע חיפוש, אולם, החוק החדש הרחיב את הסמכות לביצוע חיפושים חשאיים בהם בעל המקום לא יודע שבוצע חיפוש במקרקעין/מיטלטלין שלו. צווי חיפוש משמשים לתפישת מידע תוכני שהתקבל ומאוחסן באמצעים אלקטרוניים[288] לרבות דואר אלקטרוני שטרם נקרא. החוק החדש מתיר ליירט מידע מאוחסן של תקשורת קווית לרבות תא קולי באמצעות צו חיפוש.[289] תחת FISAניתן לבצע חיפושים, ללא פיקוח שיפוטי, באישור התובע הכללי.[290] חקירה, במסגרת חוק זה, כמו גם חיפוש נגד מי שהוא אזרח, לא תתבצע בגין אמירות המוגנות תחת התיקון הראשון לחוקה.

4.2.5 קבלת מידע שנאסף בידי ספקי גישה

---

[284] "pen register" are devices used to record telephone numbers that are dialed from a telephone "trace devices" are used to determine where a telephone call originated, ובתרגום חופשי: "עט רישום" הינו מכשיר המשמש לתיעוד מספרי הטלפון אשר חוייגו ממכשיר הטלפון. "מכשירי מעקב" משמשים לקביעה מהיכן בוצעה השיחה.

[285] USA PATRIOT Act, §216.

[286] USA PATRIOT Act, §214.

[287] http://www.eff.org/Privacy/Surveillance/Carnivore/20000728_eff_house_carnivore.html

[288] 18 USC §2703 (a) and (b).

[289] USA PATRIOT Act, §209.

[290] 50 USC §1822.

רשויות האכיפה רשאיות להזמין ולקבל מידע לצורך ביצוע חקירות. הזמנת המידע אינה כפופה לביקורת שיפוטית. החוק החדש מסמיך את רשויות האכיפה להזמין ולקבל מספקי גישה ותקשורת מידע רב יותר מבעבר, לרבות זמן ומשך השיחה/גלישה ברשת, כתובת IP, אופן התשלום ופרטי המשלם.[291] הרשויות יכולות להזמין רשומות עיסקיות דוגמת מידע בגין עסקאות שבוצעו בחברות התקשורת (e-commerce) וכל מידע לא תוכני הקשור למנויי ספקיות גישה.[292]

סעיף 217 לחוק החדש מאפשר עיון במידע שנתפס תוך כדי השגת גבול במחשבים.[293] הרציונל הוא שמי שפורץ למחשב איננו יכול לצפות לפרטיות על המידע שלו. החוק החדש מאפשר לספק השירות למסור מידע לא תוכני, ללא צו ומבלי שהתבקש, במקרה של סכנת חיים או פגיעה חמורה.[294]

Communications Assistance for Law Enforcement Act (CALEA[295]) דורש מחברות התקשורת שתתאמנה את המערכות שלהן להפעלת אמצעי פיקוח על-ידי רשויות האכיפה.

5. מדינות נוספות

5.1 קנדה

Personal Information Protection & Electronic Documents Act 2000

מטרת החוק הקנדי הייתה להסדיר פרטיות במידע אישי, פיננסי ורפואי, וליצור הסדרה אמינה ואחידה ביחס למסחר אלקטרוני ומסמכים אלקטרוניים. החוק נועד להעניק זכויות לפרט בהגנה על מידע אישי. החוק מגדיר את הדרכים באמצעותן יכולים ארגונים לאסוף ולהשתמש במידע אישי, ואת הזכויות שיש לפרט לגשת אל המידע ולשנותו. החוק דורש שהעסקים יגלו מהי מטרת איסוף המידע וכי יקבלו הסכמה לפני שיעשו כן. חשוב להעיר כי החוק אינו מוציא מתחולתו חברות שאינן קנדיות, כך שתחולת החוק יכולה לכלול גופים שאינם קנדיים אך האוספים מידע בקנדה או על אזרחים קנדיים. כמו כן, החוק מעיד על עצמו שהוא בא להתאים את המצב המשפטי בקנדה לדרישות שהוגדרו בדירקטיבה האירופאית שתוארה לעיל. ההכפפה לחוק נעשית בהדרגה כך שגופים מסחריים מסוימים כבר כפופים אליו, החל בשנת 2002 גם גופים רפואיים יאלצו לענות על דרישותיו, ומשנת 2004 כל הגופים יוכפפו לחוק.

המצב המשפטי לאחר ה- 11 בספטמבר

בקנדה מתנהל כיום תהליך, המושפע במידה רבה מאירועי האיד עשר בספטמבר, לתיקון לחוק הפלילי המקומי- **C-6 Anti-Terrorism Bill**.[296] תיקון זה מכניס לקוד הפלילי מספר סעיפים חדשים, המיועדים להתמודד עם טרור. העבירות החדשות שנוספו מרחיבות את הדין הקיים ביחס לקבוצה של מצבים הנחשבים מצבים של פעולה טרוריסטית, כך עבירה כנגד אישיות במישור

[291] USA PATRIOT Act, §§210, 211.
[292] 18 USC §2703 (c).
[293] USA PATRIOT Act §217.
[294] USA PATRIOT Act, §212.
[295] 18 U.S.C. §2522.
[296] הפרלמנט הקנדי אישר את התיקון ביום 28.11.01, והתיקון הועבר לאישור הסנאט, שאחריו חוזר החוק לפרלמנט לצורך ישומו. http://www.canadianliberty.bc.ca/ (24.12.01).

הבינלאומי, או כנגד אנשי או"ם, עבירות שמערבות שימוש בחומרי-נפץ או מכשירים קטלניים אחרים וכן עבירות שקשורות למימון פעולות טרור.[297]

5.1 אוסטרליה

Privacy Amendment (Private Sector) Act 2000

באוסטרליה תוקן לאחרונה החוק להגנת הפרטיות. החוק מתייחס, בין היתר, לניהול מערכות מידע של חברות ודורש לאבטח מידע אלקטרוני אישי ורגיש. החוק שנכנס לתוקף בדצמבר 2001 מציב ב- NPP4 שתי דרישות בסיסיות:

1. הגנה על מידע אישי מפני שימוש לרעה וגישה לא מורשית, שינויים וחשיפה.
2. השמדה או ביטול אפשרות זיהוי של מידע אישי כאשר זה הופך למיותר.

לפי עקרון ה- NPP4 יש לנקוט "צעדים סבירים" לשמירה על ביטחון פיזי של המידע, ביטחון מערכות המחשב והרשתות, קיום תקשורת בטוחה וכן נדרש אימון מתאים של צוות העובדים.

המצב המשפטי לאחר ה- 11 בספטמבר

לאחר אירועי ספטמבר נחקקו באוסטרליה מספר חוקי cyber-crime, לרבות עבירות-מחשב שהעונש עליהם יהיה עשר שנות מאסר. בפועל החוק עוסק בעבירות מחשב ועבירות באמצעות מחשב "סטנדרטיות" כמו שימוש לא מורשה, ומאפשר יכולות חקירה גם למקרים פלילים "טהורים" כמו רצח והונאות. החוק הכיל שבע עבירות "היי-טק" חדשות שכיסו האקרים, התקפות מניעת-שירות, ונדליזם באתרים, הפצת וירוסים ושימוש במחשבים בעבירות כמו הטרדה, הונאה וחבלה.[298]

ה. המסגרת המשפטית: ישראל

הזכות לפרטיות הינה זכות יסוד חוקתית, המעוגנת בחוק יסוד: כבוד האדם וחירותו.[299] מעמדה החוקתי מבטיח כי כל פגיעה בה חייבת להיעשות בהתאם לתנאי פסקת ההגבלה,[300] דהיינו, הפגיעה צריכה להיעשות בחוק, או מכוחו, עליה להלום את ערכיה של מדינת ישראל כמדינה יהודית ודמוקרטית, להיות לתכלית ראויה, ובמידה שאינה עולה על הנדרש. לאור חשיבותה של הזכות לפרטיות, ראתה הכנסת לנכון לעגן את ההגנה עליה בחוק עוד טרם עיגונה החוקתי. בשנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981.[301] לפי החוק, פגיעה בזדון בזכות לפרטיות, הינה עבירה פלילית.[302] הרציונל לקביעה מחמירה זו, המעמידה בפני החברה נורמת התנהגות גבוהה

---

[297] http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_1/90168bE.html (24.12.01).

[298] http://australianit.news.com.au/articles/0,7204,2944524%5E15306%5E%5Enbv%5E,00.html (ביקור אחרון: 24.12.01).

[299] סעיף 7 לחוק יסוד: כבוד האדם וחירותו.

[300] סעיף 8 לחוק יסוד: כבוד האדם וחירותו.

[301] חוק הגנת הפרטיות, התשמ"א-1981, ס"ח התשמ"א 128.

[302] סעיף 5 לחוק הגנת הפרטיות.

ביותר, הוא ההשקפה כי הפוגעים בצנעת הפרט, לא יורתעו מעונש כספי בלבד.[303] אם נעשתה הפגיעה בפרטיות בנסיבות בהן מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה, הוא יזכה להגנה בפני תביעה אזרחית או פלילית.[304] המונחים חובה מוסרית או חברתית, הם מונחי שסתום, ובכך טמונה סכנה להרחבת היקף הפגיעה המותרת בפרטיות.[305]

באמצעות חוק הגנת הפרטיות ביקשה הכנסת לתת מענה משפטי להחמרת הפגיעה בפרטיות, עקב התפשטות אמצעי התקשורת ההמוניים, התפתחות מכשירים טכנולוגיים המאפשרים האזנה, התחקות ובילוש ממרחק, וגידול תפוצתם, ועקב התרחבות האיסוף והריכוז של המידע בידי גורמים ציבוריים ופרטיים.[306] עם זאת, חוק הגנת הפרטיות, אינו דן בנושא איסוף מידע במרכזי מחשבים, מתוך הנחה שנושא זה יוסדר בחקיקה נפרדת.[307] איסוף מידע באמצעות מחשב גם אינו מנוי בסעיף 2 לחוק, כפגיעה אפשרית בפרטיות. אולם רשימה זו הינה רשימה פתוחה, הניתנת להשלמה על-ידי בית המשפט, מתוך הכרה בכך שההתפתחות הטכנולוגית עלולה ליצור בעתיד דרכי פגיעה, שלא ניתן היה לחזותן עם חקיקת החוק בשנת 1981.[308] רק בפרק ב׳ לחוק הגנת הפרטיות, העוסק בהגנה על פרטיות במאגרי מידע, נתנה הכנסת דעתה להיבט מצומצם של פגיעת ההתפתחות הטכנולוגית בזכות לפרטיות, ביודעה כי אי הגנה יעילה על המידע האישי העצום הנאגר במחשבים, עלולה להוביל לפגיעה קשה בפרט.[309] בתת-פרק זה נסקור את ההסדרים המשפטיים המאפשרים פגיעה בפרטיות בישראל בתחום האזנת סתר, חיפוש ותפישה.

2. אכיפה

עבריינות מחשבים נתפסת, בעיני רבים, כחמורה פחות מעבריינות רגילה, הן בשל העובדה שפריצה למחשב מחייבת תחכום רב וידע טכנולוגי, והן בשל העובדה שעבירות כאלה נעשות על-ידי אנשים שיושבים מאחורי מסך ומקלדת והנזק שהם גורמים לו הוא מוחשי פחות מאשר הנזק שנגרם בפריצה לכספת של בנק, למשל. האקרים, במקומות רבים, נחשבים לגיבורי תרבות ולא לפושעים. אלא, שלעבירות מחשב עלולות להיות השלכות חמורות, והן מצריכות טיפול מיוחד. בשל כך נחקק חוק המחשבים בשנת 1995.[310]

חוק זה הינו פרי עבודתו של צוות בין-משרדי ובין-תחומי שמינה שר המשפטים, והוא מאגד בתוכו היבטים אחדים הנוגעים למחשב.[311] הצורך בחקיקתו התעורר, בין השאר, בשל אופיו המיוחד של המחשב והמקום המרכזי שהוא תופס בחיינו, התגברותה של עבריינות המחשבים והקשיים בהתאמת הדינים הקיימים לשימוש ברעה במחשבים. פרק ב׳ של החוק מאפשר טיפול בעבירות מחשב, ובכך – הגנה על אינטרסים מופשטים, שהוראות חוק שהיו קיימות לפני חוק זה, לא נתנו

---

[303] ד"כ כ (תשמ"א) 1770 (ח"כ אמנון לין).
[304] סעיף 18(2)(ב) לחוק הגנת הפרטיות.
[305] חברי הכנסת עקיבא נוף ושולמית אלוני העלו סוגיה זו בדיון בקריאה שניה ושלישית, אך הסתייגותם נדחתה, כאמור בד"כ כ (התשמ"א) 1769.
[306] הצעת חוק הגנת הפרטיות, התש"ם-1980, ה"ח 206.
[307] **שם**.
[308] **שם**.
[309] ד"כ כ (תשמ"א) 1767 (דברי יו"ר ועדת החוקה, חוק ומשפט דאז, ח"כ דוד גלס).
[310] חוק המחשבים, התשנ"ה-1995.

להן פתרון ישיר. יצוין, כי השימוש במונח "שלא כדין", בחלק מסעיפי פרק זה, משמעותו – העברת נטל ההוכחה אל התביעה.[312]

בפסקי הדין שדנו בחוק זה, נעשה שימוש במיוחד בשני סעיפים – סעיף 2 (שיבוש או הפרעה למחשב או לחומר מחשב) וסעיף 4 (חדירה לחומר מחשב שלא כדין):

בעניין **רפאלי**,[313] נקבע כי רפאלי עבר על סעיפים 2 ו- 4 לחוק המחשבים. נפסק כי גם מחיקת חומר מחשב חסר תועלת היא עבירה על החוק, ואין צורך להוכיח שהמחיקה גרמה לנזק או לשיבוש למחשב.

בעניין **בדיר**,[314] ביצעו הנאשמים עבירות באמצעות מערכת הטלפוניה הממוחשבת, והורשעו בחדירה לחומר מחשב שלא כדין. נפסק שאין צורך בהוכחת נזק לצורך הרשעה בעבירה זו. כמו כן נקבע שאין צורך שהחדירה תהיה כרוכה במומחיות בהפעלה ותכנות מחשב: יכול שהעבירה תתבצע על-ידי סוכן תמים, אדם ששוטה לפעול על-ידי הנאשמים.

על אהוד טננבאום, "האנלייזר",[315] נגזרו שישה חודשי עבודות שרות ו- 75,000₪ קנס, בגין פריצה למחשבי הפנטגון בארצות הברית. נקבע שהוא עבר על סעיפים 2 ו-4 לחוק המחשבים. המדינה ערערה על קולת העונש. בהודעת ערעור (ע"פ 71227/01), מבקשת המדינה להחמיר בעונשו של טננבאום משיקולי הרתעה. לשיטתה קלות העונש פוגעת במסר ההרתעתי והענישתי, ובהגנה על שלום הציבור ועל בטחונו, בפרט בתקופה בה המחשב מצוי בכל תחום ותחום של החיים המודרניים. עוד טוענת המדינה כי עונש מרתיע נדרש כמעין סכר מפני הפיתוי הרב לבצע עבירות מחשבים, לאור קלות ביצוען והסבירות הנמוכה להיתפס.

קושי נוסף באכיפה הוא שלעיתים העבירה היא בינלאומית– אדם שמשתמש בשרתים הנמצאים בחו"ל, בעוד שהמדינה בה הוא מתגורר – אין לה דבר מלבד קשר אקראי עם השרתים בחו"ל.[316] סעיף 140 לתקנות ההגנה לשעת חירום קובע כי אדם המפריע לשוטר או לחבר בכוחות הממשלה בעת מילוי תפקידו, עובר עבירה.[317] ניתן להרשיע בעבירה זו האקרים הפורצים לאתרי אינטרנט של הממשלה או הצבא.

---

[311] הצעת חוק המחשבים, התשנ"ד-1994, ה"ח 2287 (מיום 13.6.94)

[312] בועז גוטמן, "חקיקת מחשבים ויישומה", **משפט וצבא: ביטאון המערכת המשפטית בצה"ל** 13 (1999), 175-185.

[313] ת"פ (ירושלים) 3813/99 **מ"י נ' עודד רפאלי**, תק-על 2000(2), 1091.

[314] ת"פ 40250/99 **מ"י נ' בדיר** (טרם פורסם)(להלן: עניין **בדיר**). עוד נקבע בפסק הדין כי מרכזיות טלפוניה מודרניות הן מחשב כהגדרתו בחוק, ושחדירה לתא קולי ושמיעת ההודעות שהושארו בו, מהווה האזנת סתר אסורה.

פסה"ד נמצא ב: http://www.law.co.il/computer-law/main.htm (14.2.02)

[315] ת"פ (כפר סבא) 3709/00 **מדינת ישראל נ' אהוד טננבאום**, תק-של 2001(2), 41.

[316] בועז גוטמן, "עבירות מחשב – אתגר חדש". אבחנה בין עבירת מחשב (פעולה שמטרתה פגיעה במחשב עצמו או ברשת המחשבים), לבין עבירה לפי הפקודה למניעת טרור (המחשב משמש ככלי עזר לביצוע העבירה, למשל פעיל חמאס המנהל את פעולות החברים ממחשב אישי המוצפן במשרדי אגודה המסווה לקרן לנזקקים). דיון בקשיי הגילוי, המניעה, האכיפה וההוכחה של עבירות מחשב, לאור אופייה של רשת האינטרנט. נמצא ב: http://www.psakdin.co.il/Ip/public/art_bduc.htm (14.2.02)

[317] תקנות ההגנה (שעת חרום), 1945.

3. חיפוש ותפיסה

פעולות החיפוש והתפיסה מותרות בדין על-מנת להגן על אינטרסים של ביטחון המדינה, ועל הזכות לחיים, וכן כדי לאפשר מניעת פשעים וענישה. מנגד, פעולות אלו עשויות לפגוע בזכות הפרטיות ובאינטרסים כלכליים שונים של גופים שונים.

בעניין **פלוני**,[318] נקבע שיש לשקול שימוש במעצר מנהלי לאור פסקת ההגבלה בחוק יסוד: כבוד האדם וחירותו. יש למצוא איזון בין הגנה על ביטחון המדינה לבין זכות היסוד של האדם לחירות.

בעניין **הוועד הציבורי נגד עינויים**,[319] שעסק בסמכות חוקרי שב"כ לבצע חקירות בחשודים בפעילות חבלנית עוינת ובאמצעים הפיזיים הננקטים נגדם, נקבע, כי הפגיעה בחירותו של הנחקר תתאפשר רק במידה שהיא לתכלית ראויה ולא מעבר לנדרש, כאשר נשקל מן הצד השני הרצון להגן על כבוד הנחקר ועל חירותו.[320] לעניין דרישת המידיות, היא תתקיים במידה שקיימת מידת סיכון קונקרטי וממשי להתרחשות האירוע. (באותו מקרה - כאשר מדובר ב"פצצה מתקתקת").

<u>חיפוש ותפיסת חומר במערכות מחשב</u>

חוק המחשבים הוסיף להגדרת "חפץ" בסעיף ההגדרות של פקודת סדר הדין הפלילי[321] (להלן: פסד"פ) גם את "חומר מחשב" ואף הוסיף את ההגדרות "מחשב", "חומר מחשב" ו"פלט" לפקודה זו – כהגדרתם בחוק המחשבים. בדברי ההסבר להצעת החוק הוסבר, שהיתרים לחדירה למחשב מסוים יינתנו לפי דיני החיפוש. מאחר שהוראות החיפוש בפסד"פ לא כללו חיפוש בחומר מחשב, הן תוקנו, כך, שמתאפשר גם חיפוש מידע או תוכנה המצויים במחשב או שייכים לו. בנוסף, התקבלה תוספת לסעיף 32 לפסד"פ (סעיף 32(ב)), לפיה נדרש צו של בית משפט לתפיסת חומר מחשב של מוסד. הנימוק – על-מנת למנוע שיבושים בפעולת העסק או הגוף הציבורי. צו חיפוש וחדירה לחומר מחשב יכול להינתן על-ידי שופט מכוח סעיפים 23 לפסד"פ (צווי חיפוש), 23א לפסד"פ (חדירה לחומר מחשב) ו-43 לפסד"פ (הזמנה להשיג חפץ). קבלת מידע מתקשורת בין מחשבים אגב חיפוש, לא תיחשב להאזנת סתר (סעיף 23א(ג) לפסד"פ).

בעניין **נטוויזן נ' צה"ל**,[322] חייב בית המשפט את ספקית השירות לספק לרשויות הביטחון חומר שנאסף במחשביה ושהועבר באמצעות דואר אלקטרוני של ארבעה מלקוחותיה. חברת נטוויז'ן נדרשה לספק את החומר הנ"ל מכוח סעיפים 23 ו-43 לפסד"פ. לאור הודעת פרקליטת המדינה כי צו לתפיסת דואר אלקטרוני המצוי במחשביו של ספק שירות יינתן רק מכוח חוק האזנת סתר, ציין בית המשפט, כי גם חפץ שנתפס אגב חיפוש ללא צו שלא כחוק – אינו פסול בשל כך לשמש כראיה. השופט אבן ארי ציין את ההלכה שנקבעה בעניין **נחמיאס**,[323] שם קבע הנשיא ברק כי "הסדר חדש זה בא לאזן בין זכות הפרטיות לבין הפגיעה בה: בין אי קבילות הראיה לבין ההגנה על אינטרס הציבור." כן החליט בית המשפט כי ניתן לתפוס את החומר שנאגר במחשבי נטוויז'ן, גם אם ההליך שהוביל לאגירתו התברר מאוחר יותר כלא תקין.

---

[318] בש"פ 3514/97, עמ"מ 6/97 **פלוני נ' מדינת ישראל**, תק-על 97(2) 177,176.

[319] בג"צ 5100/94, 4054/95 **הועד הציבורי נגד עינויים נ' ממשלת ישראל**, פ"ד נג (4) 817.

[320] עניין **הועד הציבורי נגד עינויים, שם**, בע' 834-835 (הנשיא ברק).

[321] פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט-1969.

[322] ב"ש 090868/00 **חב' נטוויז'ן בע"מ נ' צבא ההגנה לישראל ואח'** (טרם פורסם), (להלן: עניין **נטוויז'ן**).

[323] ע"פ 1302/92 **מ"י נ' נחמיאס**, פ"ד מט (3) 309 (להלן: עניין **נחמיאס**).

הסדרים חוקיים נוספים לחיפוש ותפיסה

ייתכן שניתן יהיה לסגור אתר אינטרנט מכוח סעיף 5 לפקודה למניעת טרור[324] שקובע כי כל רכוש של ארגון טרור, ובכלל זה רכוש הנמצא במקום פעולה של הארגון, בידי חבר בארגון או ששימש לפעולות הארגון, יוחרם. ומכוח סעיף 6 לפקודה, המתיר למפכ"ל המשטרה לסגור מקום פעולה של ארגון טרור.

סעיף 74 לתקנות ההגנה לשעת חירום,[325] מתיר החרמת חפצים שיש חשד שנעשתה לגביהם עבירה או שעשויים לשמש ראייה בעבירה, סעיף 99 מתיר תפיסה של כל פרסום בלתי מותר, סעיפים 100-101 מתירים חיפוש בכל מכשיר, המשמש להדפסה וסעיף 120 מאפשר להחרים את רכושו של כל אדם שעבר עבירה על תקנות אלו.

סעיף 1 לחוק עזרה משפטית בין מדינות[326] מגדיר פעולת חקירה גם כחיפוש במקום וכתפיסת ראיה או חפץ (כולל חומר מחשב) ובדיקתם. סעיף 2(א) מגדיר עזרה משפטית, בין היתר, גם כפעולות חיפוש ותפישה, הקשורות לעניין אזרחי או פלילי. בסעיפים 29-30 יש נוהל בקשה לתפישת חפץ.

4. האזנת סתר בדין הישראלי

התפתחות הטכנולוגיה המודרנית העלתה לדיון את הסוגיות המשפטיות הנובעות מפיתוח אמצעי ציתות ומעקב ומהשימוש הגובר והולך בהאזנה אלקטרונית. קלות השימוש במכשור האזנה, אי-מודעות הנפגע להאזנה לשיחותיו, הקושי לחשוף האזנה קיימת והמוגבלות להתגונן מפניה הובילו לצורך הדחוף לפתור כמה מהבעיות הנובעות מהאזנת סתר.

הצעת חוק ראשונה בנושא האזנת סתר הוגשה עוד בשנת 1962.[327] בדברי ההסבר נאמר: "יש מקום להבטיח, על-ידי הוראה פלילית, שצנעת השיחה לא תיפגע על-ידי האזנת סתר". ההצעה לא בשלה לחוק, והצעה נוספת גובשה שש-עשרה שנים לאחריה,[328] והיא היסוד לחוק שנתקבל בכנסת.[329] ביסוד הצעת החוק ניצבה המטרה למצוא את האיזון המתאים בין זכות האדם לפרטיות ולשמירת צנעתו לבין זכות הכלל להגן על עצמו בדרכים שונות, ובין השאר על-ידי שימוש באמצעי-הציתות של הטכנולוגיה המודרנית.[330] החוק נועד להבטיח, כי פגיעה בפרטיותו של אדם, על-ידי ביצוע האזנת סתר, תותר אך במקרים בהם אינטרסים ציבוריים-חברתיים גוברים על הזכות לפרטיות.

בחקיקת חוק האזנת סתר הסתמכו מנסחי החוק על המודל האמריקני, בו קיימת אבחנה מפורשת בין האזנת סתר שהיא אסורה, לבין האזנה לשיחה והקלטתה בהסכמת אחד מבעלי השיחה, שהיא מותרת. מאחורי אימוץ תפיסה זו עמדה הסברה, כי אם בארצות-הברית, "מעוז לשמירת זכויות

[324] הפקודת למניעת טרור, תש"ח-1948.
[325] תקנות ההגנה (שעת-חירום), 1945.
[326] חוק עזרה משפטית בין מדינות, התשנ"ח-1998.
[327] הצעת חוק למניעת האזנת-סתר, התשכ"ג-1962, ה"ח התשכ"ג 62.
[328] הצעת חוק דיני העונשין (האזנת סתר), תשל"ח-1978, ה"ח תשל"ח 301.
[329] חוק האזנת סתר, תשל"ט-1979, ס"ח תשל"ט 118 (להלן: חוק האזנת סתר).
[330] ע"פ 48/87 **איתן צ'חנובר נ' מ"י**, פ"ד מא (3) 581, 587-588 (להלן: עניין **צ'חנובר**).

הפרט", תפיסה זו אינה מהווה פגיעה פלילית בזכויות הפרט, הרי שהיא ראויה ליישום גם בישראל.[331]

לפי חוק האזנת סתר, האזנה לשיחת הזולת, קליטתה או העתקתה, באמצעות מכשיר וללא הסכמה של **אף אחד** מבעלי השיחה, היא האזנת סתר אסורה על-פי החוק.[332] מכאן, שאם אחד מבעלי השיחה הסכים לציתות, אין זו האזנת-סתר.[333] האזנה לשיחה והקלטתה למטרת ביצוע עבירה או מעשה נזק, מהוות האזנת סתר אסורה, אף אם ניתנה הסכמתו של אחד מבעלי השיחה.[334] בעניין **צוברי**[335] נקבע, כי אדם יכול להיחשב כ"בעל שיחה" אף אם הוא מאזין בלבד, בתנאי שהאחר מכוון את המסר ישירות אל המאזין.

נמצא, כי מישור אחד בו עוסק חוק האזנת סתר הוא עצם האיסור על האזנת סתר. במישור הנוסף מסייג החוק את תחולת האיסור בקובעו שני חריגים: החריג האחד מתייחס למקרים בהם ההאזנה מותרת מלכתחילה ללא צורך בהיתר. כאשר השיחה נערכת **ברשות הרבים**, האזנה לה על-ידי מי שהוסמך לכך, אינה האזנת סתר שלא כדין.[336] על אף שהאזנות אלו טעונות הסמכה, נמנע החוק מקביעת הסמכה קונקרטית.[337] עם זאת, נראה כי ההסמכה חייבת להיות שמית, להתייחס לעניין מסוים, וככל שניתן להיות מוגבלת בזמן ובמקום.[338] החריג השני חל על מקרים בהם יינתן היתר להאזנת סתר, שלא ברשות הרבים. החוק מציב מחסומים מהותיים ודיוניים חמורים יותר בפני האזנה לרשות היחיד.[339] האזנת סתר כאמור תותר אך ורק לשתי מטרות, לשם הגנה על ביטחון המדינה או לשם מניעת עבירות וגילוי עבריינים. ההיתר יכול שיינתן לרשות מרשויות המדינה בלבד: האזנות סתר למטרת ביטחון המדינה ניתנות לביצוע בהיתר בכתב מאת ראש הממשלה או שר הביטחון,[340] ובמקרים דחופים בהיתר מאת ראש שירות הביטחון הכללי או ראש אגף המודיעין במטה הכללי של צה"ל.[341] האזנות סתר לשם מניעת עבירות וגילוי עבריינים,

---

[331] ד"כ התשל"ה 3974.

[332] ראו הגדרת "האזנה" ו"האזנת סתר" בסעיף 1 לחוק האזנת סתר. לפרשנות הפסיקה להגדרות "שיחה", "בעל שיחה" ו"שיחת הזולת", ראו: עניין **צ'חנובר**, **לעיל** הערה 330, בע' 596-591. בפרשה זו פסק בית-המשפט העליון, כי "מי שמשמיע דברים באמצעי קשר אשר מגיעים או מסוגלים להגיע לאוזניהם של רבים - הופך את כל שומעיו לבעלי שיחתו... כאשר הפותח בשיחה אומר את דבריו באופן שאחרים יכולים להאזין, הוא נוטל על עצמו את הסיכון, שאחרים שהוא לא התכוון שיאזינו לשיחתו, ישמעוה. דומה הוא לאדם הצועק את דבריו לחברו ברשות-הרבים. אין הוא יכול לצפות שדבריו יישארו סמויים."

[333] בדברי ההסבר לסעיף 1 להצעת חוק דיני העונשין (האזנת סתר), תשל"ח-1978 נאמר: "מוצע שלא תיאסר האזנה לשיחה כשאחד מבעלי השיחה הסכים להאזנה זו. ההנחה היא שהסכמה כאמור מוציאה את השיחה מגדר שיחה שהתכוונו לעשותה אישית בלבד, וכשם שאדם עשוי להפעיל את זכרונו ולשחזר שיחה ששוחח עם אחר, כך יכול הוא להקליטה ואף יכול הוא לבקש מאחר לעשות זאת".

[334] סעיף 3 לחוק האזנת סתר.

[335] ע"פ 1497/92 **מ"י נ' צוברי**, פ"ד מז (4) 177, 193.

[336] סעיף 8 לחוק האזנת סתר. "רשות הרבים" מוגדרת כ"מקום שאדם סביר יכול היה לצפות ששיחותיו יישמעו ללא הסכמתו, וכן מקום שבו מוחזק אותה שעה עצור או אסיר". הסמכה לביצוע האזנת סתר כזו תינתן על-ידי ראש רשות ביטחון מטעמים של ביטחון המדינה, או על-ידי קצין משטרה לשם מניעת עבירות וגילוי עבריינים (סעיף 8(1)(א) ו-(ב) לחוק האזנת סתר, בהתאמה). לפרשנות המושג ראו: ע"א 546/78 **בנק קופת עם בע"מ נ' הנדלס**, פ"ד לד (3) 57; ד"נ 13/80 **הנדלס נ' בנק קופת עם**, פ"ד לה (2) 785.

[337] ראו לעניין זה: תקנה 2 לתקנות האזנת סתר, התשמ"ו-1986, ק"ת התשמ"ו 1118.

[338] אלכס שטיין "האזנת סתר ומעקבים אלקטרוניים נסתרים כאמצעים לקידומה של חקירה פלילית ובטחונית" **משפטים** יד (תשמ"ה) 527, 546-543.

[339] **שם**, בע' 533.

[340] הגדרת "שר" בסעיף 1, וסעיף 4 לחוק האזנת סתר.

[341] הגדרת "רשות ביטחון" בסעיף 1, וסעיף 5 לחוק האזנת סתר.

טעונות היתר מאת נשיא בית-משפט מחוזי או סגנו.[342] במקרים דחופים די בהיתר מאת מפכ"ל משטרת-ישראל.[343]

האזנת סתר ללא היתר כדין מהווה עבירה פלילית, שניתן להטיל בגינה סנקציה עונשית לפי הוראת סעיף 2(א) לחוק האזנת סתר.[344] הסעיף קובע שתי עבירות פליליות נוספות: עבירת השימוש במידע ועבירת הצבת מכשירים.[345] סעיף 2(2) לחוק הגנת הפרטיות קובע, כי "האזנה אסורה על-פי חוק" מהווה פגיעה בפרטיות.[346] ברם, בעוד שהאזנת סתר מהווה עוולה לפי חוק הגנת הפרטיות,[347] היא אינה מהווה עבירה פלילית לפי אותו חוק.[348]

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.[349] בטרם תיקונו של חוק האזנת סתר בשנת תשנ"ה,[350] היווה סעיף 13 הוראה מנדטורית שאינה מותירה מקום לשיקול-דעת בית-המשפט בנוגע לקבילות הראיות. כיום, רשאי בית-המשפט, בנסיבות מסוימות ולפי שיקול-דעתו, לקבל כראייה האזנת סתר גם אם הושגה שלא כחוק.[351]

היתר לביצוע האזנת סתר, הן למטרת ביטחון המדינה, והן לשם מניעת עבירות, ניתן לתקופה שלא תעלה על שלושה חודשים, וניתן להאריכו מחדש.[352] נראה, כי היתר כאמור טומן פגיעה קשה בפרטיות, אף קשה מזו הנובעת מצו חיפוש. בעוד החיפוש מבוצע באורח חד-פעמי ובמודעותו של החשוד, האזנת סתר נמשכת לאורך זמן, נעשית ללא ידיעתו של החשוד, ואף עלולה לפגוע בפרטיותם של צדדים שלישיים תמי-לב.

---

[342] סעיף 6(א) לחוק האזנת סתר.

[343] סעיף 7 לחוק האזנת סתר.

[344] על אופיו של חוק האזנת סתר כחוק פלילי ניתן ללמוד גם משמו המקורי בהצעת חוק דיני העונשין (האזנת סתר), תשל"ח-1978, (**לעיל** הערה 329). ראו גם: אורי רוזן "על האזנת סתר ועל פגיעה בפרטיות בהאזנת סתר" **משפטים** יז (תשמ"ז) 146, 148-149 (להלן: רוזן).

[345] סעיף 2(ב) ו- (ג), בהתאמה. על תחולתם המקבילה של חוק האזנת סתר וחוק הגנת הפרטיות על מעשים אלו, ראו: על אחריות פלילית ואזרחית בגין מעשה אחד, לפי חוק האזנת סתר וחוק הגנת הפרטיות, ראו: רוזן, **שם**, בע' 160-162.

[346] חוק הגנת הפרטיות. הדעה הרווחת כיום מקנה עדיפות להסדר הקבוע בחוק האזנת סתר על פני זה הקבוע בחוק הגנת הפרטיות.

[347] סעיף 4 לחוק הגנת הפרטיות קובע, כי "פגיעה בפרטיות היא עוולה אזרחית...". על אחריות פלילית ואזרחית בגין מעשה אחד, לפי חוק האזנת סתר וחוק הגנת הפרטיות, ראו: רוזן, **לעיל** הערה 344, בע' 160-169.

[348] סעיף 5 לחוק הגנת הפרטיות קובע את רשימת הפגיעות בפרטיות, המהוות עבירה פלילית, אולם אינו נוקב בחלופה לפי סעיף 2(2) לחוק הגנת הפרטיות. לפיכך, בעניינים המהווים האזנת סתר אין להעמיד לדין לפי חוק הגנת הפרטיות. ראו לעניין זה עניין **בדיר, לעיל**, הערה 315; רוזן, **לעיל**, הערה 345, בע' 156-160.

[349] סעיף 13(א) לחוק האזנת סתר.

[350] חוק האזנת סתר (תיקון), התשנ"ה-1995, ס"ח התשנ"ה 180. בעבר קבע סעיף 13(א) לחוק האזנת סתר כלל פסילה. ביסוד תיקון הוראת סעיף 13 ניצבה הכוונה ליצור נוסחת איזון בין צורכי גילוי האמת ועשיית הצדק לבין מניעת הפגיעה בזכויות הפרט, תוך מתן שיקול-דעת לבית-המשפט להורות על קבלת ראיה, אף שהושגה תוך ביצוע עבירות על חוק האזנת סתר. ראו: הצעת חוק האזנת סתר (תיקון), התשנ"ד-1994, ה"ח התשנ"ד-1994.

[351] לעניין המצב המשפטי בטרם תיקון חוק האזנת סתר, ראו: ע"פ 2286/91 **מ"י נ' אילוז**, פ"ד מה (4) 289, 304. לעניין המצב המשפטי לאחר התיקון, ראו: עניין **נחמיאס**, לעיל הערה 323, בע' 325-326, 357-358.

[352] סעיפים 4(ג) ו- 6(ה) לחוק האזנת סתר.

תפקידו של בית-המשפט

הואיל והמחוקק הוא שקבע את האיזון הראוי בין האינטרסים המתנגשים בחוק האזנת סתר, מתפקידו של בית-המשפט לעסוק במלאכת פרשנות החוק, וביישומו הקונקרטי של איזון האינטרסים. כאמור, האזנת סתר לשם מניעת פשע טעונה היתר מראש מאת בית-המשפט.[353]

יישום ההסדר שבחוק האזנת סתר תלוי, במידה רבה, בתוכן שיצקו בתי-המשפט לביטויים "ברשות הרבים" ו"ברשות היחיד". נראה, כי אין מקום לפרשנות מילולית לביטויים אלו, ועל שיקולי המדיניות המנחים להתאים עצמם להתקדמות הטכנולוגיה. ניתן להציע אבחנה אובייקטיבית-קניינית, הקובעת כי תחום פרטי, שכל אדם הינו בר-רשות להיכנס לתוכו ולשהות בו, הוא בבחינת רשות הרבים. ברם, מאחר שמטרתו של חוק האזנת סתר להגן על אדם ולא על קניין, אפשר שאבחנה זו אינה במקום.[354] על-כן, יתכן שיש להעדיף תפיסה רחבה יותר, המגנה על פרטיות של אדם ולא על פרטיותו של מקום. אפשר אף להציע מבחן סובייקטיבי, הנסמך על ציפיות הצדדים.[355]

נמצא, כי הקידמה הטכנולוגית בשוק התקשורת מעוררת ספקות משפטיים, ובית-המשפט מתקשה במלאכתו להכריע במקרי הגבול בהסתמכו על ההסדר המשפטי הקיים.[356] יחד עם זאת, נראה כי שינויים המתחוללים בטכנולוגיה מובילים, בבוא העת, לשינוי הכלים המשפטיים. כך, לדוגמא, תוקן חוק האזנת סתר לאור התפתחות התקשורת האלחוטית.[357]

חוק האזנת סתר הגדיר בראשיתו "שיחה" כ"בדיבור או בדרך תקשורת אחרת". במשך השנים התעוררה השאלה, אם האזנה לשיחה המשודרת על גלי האתר, נכנסת אף היא לתחום האסור. בעוד שבעבר הלא-רחוק האזנה למכשיר טלפון אלחוטי לא היוותה עבירה לפי חוק האזנת סתר, כיום אין עוד ספק, שהאזנה למכשיר טלפון סלולארי כפופה להסדר שבחוק האזנת סתר.

ולעניין עידן האינטרנט, כשנחקק חוק האזנת סתר לא חזה המחוקק לנגד עיניו אפשרות לציתות ומעקב אחר הפרט במדיה הדיגיטלית. אם כן, מהם הכלים המשפטיים העומדים לרשות בית-המשפט בהידרשו להכריע בסוגיות מעקב וציתות במדיה הדיגיטלית?

"שיחה" מוגדרת ככוללת "תקשורת בין מחשבים". לפיכך, קליטת מידע מתקשורת בין מחשבים היא האזנה, ובהיעדר הסכמה של המשוחחים זוהי האזנת סתר, המהווה עבירה פלילית.[358] יש

---

[353] סעיף 6(א) לחוק האזנת סתר.

[354] האבחנה מבוססת על מאמרו של שטיין, לעיל הערה 338, בע' 533-535, 556.

[355] **שם**, בעמ' 533, 535.

[356] ראו עניין **צ'חנובר, לעיל** הערה 330; רע"פ 5424/96 **מ"י נ' דב טל**, תק-על 96(3) 88; ע"פ (ת"א) 1770/97 **מדינת-ישראל נ' לאופר**, תק-מח 98 (2) 2377.

[357] ראו הצעת חוק האזנת סתר (תיקון מס' 3) (איסור האזנה לשיחה בטלפון אלחוטי), התשנ"ה-1994, ה"ח התשנ"ה 122; הצעת חוק האזנת סתר (תיקון מס' 4) (איסור האזנה לשיחה בטלפון אלחוטי והחמרת עונשים), התשנ"ה-1994, ה"ח התשנ"ה 123.

[358] סעיף 2 לחוק האזנת סתר קובע את האחריות הפלילית להאזנה אסורה.

לציין, כי האזנה לתקשורת בין מחשבים אינה מהווה "חדירה לחומר מחשב", כאמור בסעיף 4 לחוק המחשבים.[359]

מהפסיקה מסתמנת ההלכה, לפיה כל שימוש באמצעי תקשורת, המאפשר נגישות לציבור הרחב, חשוף להאזנה בלתי מורשית, שאינה אסורה בדין.[360] מכאן מתעוררת השאלה, האם שימוש בשירותי האינטרנט לצורכי שיחה חשוף להתחקות והאזנה בכלל, ומטעם גורמי חקירה וביטחון בפרט? מחד גיסא, משתמשי האינטרנט "מצפים לשמירה על פרטיותם, וכל שכן האינטרס הציבורי, המבקש לעודד שימוש חופשי בתקשורת מחשבים מודרנית, מחייב שהוראות חוק האזנת סתר יקויימו בקפדנות. כך תקויים גם תכליתו של החוק. מאידך גיסא, ריסון זה של הרשויות מפני פגיעה בפרטיות השיח בעידן של תקשורת מודרנית, אינו תמיד אפשרי, גם אם רצוי, כאשר מנגד עלול להיפגע אינטרס חיוני אחר של הציבור".[361]

זאת ועוד: בעניין **בדיר** נקבע,[362] כי תקשורת בין מחשבים כוללת, בין היתר, התקשרות לתא קולי, המנוהל באמצעות מחשב. מכאן, שהאזנה להודעה קולית במשיבון, ללא הסכמת משאיר ההודעה או מקבלה, הינה האזנת סתר. לפיכך, נראה כי הגנת חוק האזנת סתר נפרשת על דרכי ההתקשרות, אולם סוד השיח, לכשעצמו, אינו מוגן.

בעניין **נטוויז'ן**[363] התעוררה השאלה, באיזו מידה רשאיות רשויות החקירה והביטחון לחדור להודעות הדואר האלקטרוני של מנוי ישראלי באינטרנט, ואם רשאיות הן לחייב ספקי גישה לאינטרנט לבצע פעולות מעקב וציתות ממושכים לצורכי החקירה. על-פי המצב המשפטי כיום, כפי שהוא משתקף גם מעמדת פרקליטות המדינה, דואר אלקטרוני שכבר הועבר לספק הגישה לאינטרנט ניתן לתפיסה לפי צו בית-משפט שלום, מכוח הוראות פקודת סדר-הדין הפלילי (מעצר וחיפוש).[364] באשר לדואר אלקטרוני, אשר טרם הועבר ליעדו, תפיסתו תעשה לפי צו נשיא בית-משפט מחוזי או סגנו מכוח חוק האזנת סתר.[365]

---

[359] חוק המחשבים, התשנ"ה-1995, ס"ח 366. ראו בהקשר זה: מיגל דויטש "חקיקת מחשבים בישראל" **עיוני משפט** כב (תשנ"ט) 427, 440-442.

[360] ראו נמרוד קוזלובסקי "משטרת האינטרנט", נמצא ב: http://www.itpolicy.gov.il/topics/article_law2_karma_police.htm (ביקור אחרון: 11.01.02). לשיטתו, אימוץ הלכה גורפת זו אינו רצוי, שכן טמונה בה פגיעה קשה בזכות האדם לפרטיות, לצנעת חייו ולסוד שיחו. הצעתו היא לקובע אמת מידה לפיה כאשר הפרט נוקט אמצעים ממשיים להגנה על סוד שיחו ברשת האינטרנט, מוסקת מכך הציפייה הלגיטימית לפרטיות, ועל שיטת משפטנו לכבד שיחה מעין זו כ"רשות היחיד", וככזו להגן עליה מפני האזנה. פרופסור שטיין מבקר במאמרו מבחן אובייקטיבי-סובייקטיבי זה בדבר צפייתו הלגיטימית של הפרט, ומנמק מדוע אין זה ראוי לאמצו במסגרת חוק האזנת סתר. לשיטתו, יש לקבוע את גבולות רשות היחיד לפי הערכה אובייקטיבית של אמצעי ההצנעה אפקטיביים וחוקיים, שננקטו על-ידי הפרט, במטרה להקנות פרטיות לשיחותיו. קריטריונים אובייקטיביים מחדדים את האבחנה בין "רשות היחיד" לבין "רשות הרבים", ומסייעים בידם של חוקרי המשטרה לבצע תפקידם לפי חוק האזנת סתר. (שטיין, **לעיל** הערה 338, בע' 532-539).

[361] ראו עניין **נטוויז'ן**, לעיל הערה 322.

[362] עניין **בדיר**, **לעיל** הערה 314.

[363] עניין **נטוויז'ן**, **לעיל** הערה 322.

[364] פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969, דמ"י נ"ח 284.

[365] חיים רביה "לא ידו הארוכה של החוק" (יוני 2000). נמצא ב: http://www.law.co.il/hebarticles/2nv_v_idf.htm (ביקור אחרון: 12.01.02).

תחולתו הטריטוריאלית של חוק האזנת סתר

בעניין **אלמצרי** נקבע, כי האזנות סתר מחוץ לגבולותיה של מדינת ישראל אינן חייבות היתר מראש של בית-המשפט.[366] בעניין **עסאף**[367] דן בית-המשפט העליון בחוקיות האזנה לשיחות בין תושב דרום לבנון לתושב ישראל, כאשר ההאזנה בוצעה בו זמנית בישראל ובלבנון. סניגורו של המערער טען, כי חוק האזנת סתר אינו חל על דרום לבנון, וכי ממילא אין בית-משפט בישראל מוסמך להתיר האזנות סתר מעין אלה. נפסק, כי חוק האזנת סתר אינו דורש היתר האזנה לשיחותיו של כל אחד מן המשתתפים בשיחה. די בהיתר להאזין לאחד מהם כדי להכשיר את ההאזנה. לפיכך, אפילו נאמר שההאזנות לטלפון שבלבנון היו פסולות כראיה, נמצא כי ההאזנות לטלפון שבישראל, שבהן הוקלטו שיחותיהם של שני בעלי השיחה, קבילות כראיה.

עזרה הדדית בין מדינות בביצוע האזנות סתר

תכליתו של חוק עזרה משפטית בין מדינות הינה להסדיר את העקרונות, הדרכים והפעולות השונות בדבר הענקת העזרה המשפטית מצד מדינת ישראל למדינות זרות, וכן להסדיר את ההוראות לעניין בקשות שמפנה מדינת ישראל למדינה אחרת לקבלת עזרה משפטית.[368]

האזנת סתר נכללת בהגדרת "פעולת חקירה", אשר מנויה בין הפעולות שניתן לבצע במסגרת העזרה המשפטית.[369] על אף שהעזרה המשפטית המוסדרת בחוק ניתנת הן בעניינים אזרחיים והן בעניינים פליליים, בקשת מדינה אחרת להאזנת סתר בישראל, תבוצע בקשר לעניין פלילי בלבד. הרשות המוסמכת בישראל תבקש היתר לביצוע האזנת סתר מאת בית-משפט מחוזי בהתקיים אחד התנאים הקבועים בסעיף 31(2) לחוק עזרה משפטית בין מדינות.[370] ניתן לומר, כי בקשת עזרה משפטית ממדינה זרה אינו דבר שבשגרה, ויש להעמיד נימוקים וטעמים ראויים מדוע ייעתר בית-המשפט לבקשה המוגשת לו. על מבקש הבקשה לשכנע את בית-המשפט, בין היתר, מדוע נדרשות הראיות לצורך ההליך העומד בפני בית-המשפט, ומדוע לא יפנה המבקש עצמו וישיג את הראיות מהמדינה הזרה, בפרט כאשר המדובר במסמכים זמינים הנדרשים בהליך אזרחי.[371]

---

[366] ע"פ 4211/91 **מ"י נ' אל מצרי**, פ"ד מז (5) 624. לביקורת על פסק הדין בעניין **אל מצרי**, ראו: יהונתן גינת "התחולה החוץ-טריטוריאלית של זכויות האדם וגבולותיו של חוק האזנת סתר" **הפרקליט** מב (תשנ"ה) 518. המחבר סבור, כי לאור חוק-יסוד: כבוד האדם וחירותו פרשנותו הנכונה של חוק האזנת סתר היא החלתו על כל אדם באשר הוא אדם, בין אם הוא נמצא בגבולותיה של מדינת ישראל ובין אם מחוצה להם. לשיטתו, אם ההנחה הבסיסית היא הגנה על פרטיות האדם, הרי שחוק האזנת סתר אוסר האזנה לשיחה מקום שבעל השיחה מצפה, ורשאי לצפות, לפרטיות. צפייה לגיטימית זו אינה נעלמת עם השינוי במקום השיחה. מכאן, שאין להציב את מבחן מיקומו של אמצעי התקשורת אליו מצותתים מעל מבחן הפגיעה בפרטיות. על-כן, חוק האזנת סתר בעל תחולה חוץ-טריטוריאלית, והאזנת סתר בשטחים המוחזקים דורשת היתר מראש מאת בית-המשפט לביצוע ההאזנה.

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

[368] כאמור בדברי ההסבר להצעת חוק עזרה משפטית בין מדינות, התשנ"ז-1997, ה"ח התשנ"ז 131.

[369] ראו סעיפים 1 ו- 2 לחוק עזרה משפטית בין מדינות. יש לציין, כי סעיף 5 לחוק עזרה משפטית בין מדינות קובע הוראת מילוט, בהתרתו סירוב לבקשת מדינה אחרת, אם העזרה המשפטית עלולה לפגוע, בין היתר, בביטחון מדינת ישראל או שלום הציבור.

[370] היתר להאזנת סתר יינתן רק אם הוא נתבקש לגבי עבירה, שלפי דיני המדינה המבקשת דינה מאסר העולה על שלוש שנים; או לגבי עבירה שאילו נעברה בישראל ניתן היה להתיר האזנת סתר בגינה; או אם האזנת הסתר היא לצורך חילוט רכוש כאמור בסעיף 6 לחוק עזרה משפטית בין מדינות.

[371] בש"א (ירושלים) 2168/99 **פרופ' מלווינה נ' ד"ר וולף**, תק-מח 99(3), 29742, 29743.

מעקבים אלקטרוניים נסתרים אחרי תנועותיהם של אנשים וחפציהם

חוק האזנת סתר אינו מגן על הפרט מפני חדירה ומעקב אלקטרוניים בתחום הפרטיות בכללותה, אלא נועד להגן על הפרט רק מפני חדירה לתחום שיחותיו הפרטיות.[372] על מעקב אלקטרוני אחר תנועותיו של אדם חל חוק הגנת הפרטיות.[373]

חוק הגנת הפרטיות מכיר אף הוא בצורכי רשויות הביטחון לפעול לשמירת אינטרסים חברתיים-ציבוריים. אולם, בניגוד לחוק האזנת סתר, חוק הגנת הפרטיות אינו כולל **הסמכה פוזיטיבית** לביצוע מעקב אלקטרוני אחר תנועותיו של אדם,[374] אלא מתיר פגיעה בפרטיות בדרך של מתן **פטור** לרשויות הביטחון והחקירה, או מי מאנשיהן, אשר פעלו "באופן סביר במסגרת תפקידם ולשם מילויו".[375]

חוקיותה של פגיעה בפרטיותו של אדם, נבחנת על-פי סבירותו של המעקב האלקטרוני שבוצע לגביו, ובהתחשב במטרותיה הלגיטימיות של חקירה פלילית או ביטחונית.[376] חומר שהושג במסגרת מעקב שלא כדין פסול מלשמש ראיה בבית-המשפט, אלא בהסכמת הנפגע, זולת אם בית-המשפט התיר השימוש מטעמים שיירשמו.[377]

מתעוררת השאלה, האם הוראת סעיף 2(1) לחוק הגנת הפרטיות אוסרת התחקות מקוונת אחר פעולותיהם של משתמשי האינטרנט? הגלישה ברשת האינטרנט מותירה "עקבות" אחר המשתמש, המאפשרים יצירת פרופיל אישי אודותיו. מכאן, שגובר החשש לפגיעה בזכותו של המשתמש לפרטיות.[378]

4. אחריות ספקי שירות באינטרנט

במשפט הישראלי אין כיום הסדרה ספציפית, לא בחקיקה ולא בפסיקה, לשאלת אחריות ספקי שירות באינטרנט לתוכן או למהות המידע המתפרסם על גבי שרתיהם.[379] לעניין אחריות הספקים לפגיעה בפרטיות, הובעה הדעה, בהקשר לעוגיות (Cookies), כי כל אדם מודע לפגיעה בפרטיותו באמצעות עוגיות, אך לא נוקט כל פעולה במטרה למנוע את הפגיעה, הרי שלא ניתן להטיל אחריות בגין הפגיעה בפרטיות על ספק השירות. לא יתכן שהציבור ייהנה מיתרונות הפגיעה בפרטיות

---

372 שטיין, **לעיל** הערה 338, בע' 528-529.

373 חוק הגנת הפרטיות מגדיר פגיעה בפרטיות, בין היתר, כ"בילוש או התחקות אחרי אדם, העלולים להטרידו..." (סעיף 2(1)). סעיף 5 לחוק הגנת הפרטיות אף קובע, כי פגיעה בפרטיות כאמור יכולה שתהא עבירה פלילית, בנסיבות בהן נפגע אינטרס הציבור.

374 לביקורת ראו: שטיין, **לעיל** הערה 338, בע' 555-556.

375 סעיף 19(ב) לחוק הגנת הפרטיות. יש לציין, כי חוק הגנת הפרטיות נוקט "נוסחת איזון" שונה ומורכבת מזו שנקט חוק האזנת סתר, כיוון שגלומים בו אינטרסים רבים יותר, הזוכים להגנה משפטית. להרחבה בהקשר זה ראו: רוזן, **לעיל** הערה 344.

376 שטיין, **לעיל** הערה 338, בע' 555.

377 סעיף 32 לחוק הגנת הפרטיות.

378 חיים רביה "פרטיות ברשת" (ארבעה חלקים, ינואר-פברואר 1999). נמצא ב: http://www.law.co.il/hebarticles/privacy1.htm (ביקור אחרון: 12.01.02).

379 בריאן ניגאן, "אחריות לחומר בלתי חוקי באינטרנט", (מרץ 1998), נמצא ב: http://www.itpolicy.gov.il/vadat_inter_gov/articles/illegal.htm.

באמצעות העוגיות, ובמקביל ידרוש פיצוי כספי על השימוש בעוגיות. מנגד, במידה שמדובר בהפצת לשון הרע באתר אינטרנט, יש להטיל על ספק השירות חובה לחשוף את זהות המפיץ, אם יתבקש על-ידי בית המשפט, על אף הפגיעה בפרטיות. זאת משום שעל לקוחות ספק השירות להיות מודעים לחובת האחרון לקיים צווי בית משפט, וכן משום שלא יעלה על הדעת לאפשר למפיצי תוכן מזיק (כגון: לשון הרע) כסות הגנה חוקית, אשר תמנע את גילוי זהותם מטעמי פרטיות.[380]

יתכן שניתן ללמוד מהדין הקיים ביחס לספקי שירות סלולרי וזכייני שידורי הכבלים באשר לדין הראוי ביחס לאחריות ספקי שירות אינטרנט. סעיף 13 לחוק הבזק, התשמ"ב-1982,[381] מורה על הקצאת משאבים, בהתאם להחלטת שר הביטחון או השר לביטחון פנים, מצד בעל רשיון לביצוע פעולות בזק, למתן שירותי בזק או לשידורי לווין, לטובת כוחות הביטחון. בנוסף קיימים סעיפים מיוחדים ברשיון לביצוע שירותי בזק, הקובעים הוראות ספציפיות ביחס למחויבות בעל הרשיון כלפי מערכת הביטחון.[382] בסעיף 6כה לחוק הבזק קבועה רשימת שידורים שלבעל רשיון לשידורי כבלים או לווין אסור לשדר.

יש לציין כי מהפרקטיקה הנוהגת נלמד, כי ספקי שירות אינטרנט מוודאים, כי ראיות דיגיטליות לביצוע עבירה כלשהי, ישמרו על ידם, מרגע קבלת הפנייה מהלקוח בנוגע לביצוע העבירה. זאת על-מנת להציגן בפני המשטרה לכשיתבקשו.[383] קיומה של פרקטיקה נוהגת שכזו מחדד את הצורך בעיגון חקיקתי לאחריות ספקי שירות אינטרנט, הן בכדי להטיל על כל ספקי השירות אחריות זהה והן כדי למנוע תופעת המדרון החלקלק.[384]

---

[380] אביב אילון, יהונתן בר שדה, "מעקב קיברנטי". נמצא ב: http://www.psakadin.co.il/public/art_balx.htm

[381] חוק הבזק, התשמ"ב-1982, ס"ח 218.

[382] למשל, לפי הרצאתו של עו"ד קרן שרון מחברת סלקום, סעיף 48 לרשיון חברת סלקום מורה על הקצאת משאבים מוחלטת לטובת מערכת הביטחון. סעיף 66א לרשיון סלקום מחייב את החברה להקצות שירותים מיוחדים למערכת הביטחון.

[383] כפי שעולה מדברי מר אריאל פיסצקי, מנכ"ל אבטחת מידע בנטוויז'ן, בכנס שפיים.

[384] תופעת המדרון החלקלק עלולה להתרחש במידה שנטוויז'ן למשל, עקב נכונותה לפגוע בפרטיות הלקוח על-ידי שמירת ראיות דיגיטליות בידה, טרם התבקשה לכך על-ידי המשטרה, תדרש לבצע פגיעות נוספות בפרטיות, מבלי שיהיה להן כל עיגון חוקי.

ו. עידן המידע: האם יש צורך בהסדר חדש?

1. האם מערכת האיזונים הקיימת מתאימה לרשת?

האם מערכת האיזונים בין צרכי הביטחון לבין זכויות הפרט אשר התפתחה ביחס לציתות ומעקב בתקשורת אנלוגית מתאימה לרשת? אנו סבורים שהטכנולוגיה החדשה איננה מצדיקה זניחה של הערכים הקודמים לה – הן בדבר האיזון בין פרטיות לבין האינטרסים הציבוריים של מניעת פעילות טרור וסיכולה. עם זאת, את ההסדר המשפטי – בין בחקיקה ובין בפרשנות שיפוטית – יש לעצב תוך תשומת לב למאפיינים הטכנולוגיים. במיוחד, אנו מבקשים להדגיש מספר מאפיינים ייחודיים לרשת האינטרנט, לשימוש ברשת ולמשתמשיה אשר עשויים להיות רלוונטיים בישומן של נוסחאות האיזון השונות:

1. "עקבות דיגיטליים" – רשת האינטרנט היא כאמור סביבת מידע, שבה כל תקשורת והחלפת מסרים מהווה למעשה סוג של עיבוד נתונים היוצר רישום. אפשרויות המעקב הן אינהרנטיות ונעשות כדבר שבשגרה כחלק מהפעלת המערכת. בעוד שבכל מה שנוגע לשיחות טלפון יש להתקין מכשיר האזנה מיוחד על-מנת להאזין לסוד השיח, באינטרנט תוכן השיחה וזיהוי האמצעים של הדובר והנמען נרשמים אוטומטית. במקרים רבים "האזנה" או רישום יהוו ברירת מחדל, והשמירה על הפרטיות תחייב פעולה אקטיבית של מחיקה, או ביטול הרישום, או מניעתו. מבחינה משפטית אבחנה זו עשויה להיות בעלת נפקויות. כך, למשל, הכלל המשפטי בהקשר של שיחות טלפון צריך לקבוע את הנסיבות בהן מותר לבצע האזנה כאמור כפי שנעשה בחוק האזנות סתר. יישומה של נוסחת האיזון באינטרנט עשויה לחייב הגדרת הנסיבות אשר תחייבנה פעולה של הימנעות, או מחיקה של קבצים קיימים, או הטלת מגבלות על השימושים, על התפוצה ועל השמירה של נתונים אלו.

2. בסביבה הדיגיטלית ישנם אמצעים חודרניים רבי עוצמה אשר בפועל מעמידים את הפרט ומעשיו במצב של שקיפות (או שקיפות בפוטנציה) ועלולים ליצור פגיעה חסרה תקדים בפרטיות. אמצעים אילו מאפשרים חדירה למרחב הפרטי. המחשב המחובר לרשת גלובלית יוצר למעשה מעין דלת כניסה אחורית אל צנעת מסמכיו של אדם על גבי המחשב. לאחרונה דווח, כי ניתן גם באמצעות תוכנה המושתלת במחשב האישי דרך הרשת להפיק צילומים של המתרחש באופן פיזי בביתו של אדם. בנוסף, תוכנות מעקב ומאגרי מידע מאפשרים איסוף מידע (על-ידי מעקב והצלבה) על משתמשים במרחב הציבורי.

3. בסביבה הדיגיטלית קיים פער משמעותי בין הציפייה לפרטיות לבין המציאות הפולשנית בה הפרט חשוף יותר מבעבר לחדירה לפרטיותו. עובדה זו ניתן לייחס למספר גורמים:

- מודעות לאמצעים חודרניים. האמצעים החודרניים אינם שקופים למשתמש – המדובר בשילוב מערכות תוכנה וחומרה אשר אינן בולטות לעין למשתמש הקצה,

והפנמת האיום לפרטיות הטמון בהן עשוי לחייב ידע טכנולוגי ותחכום מעל הממוצע.

- חוויית הגלישה יוצרת אשליה של פרטיות: היא נעשית בפרטיות - במקרים רבים הגולש ימצא בביתו או במשרדו, הגולש נמצא לבד ולא בציבור; הגלישה היא פעולה עצמאית ובלתי תלויה, לכאורה, בשיתוף פעולה עם אנשים אחרים; שירותים אינטראקטיביים נחווים במקרים רבים כפעילות במסגרת קבוצה סגורה ואינטימית. כל אלו עשויים להגביר כמובן את הצפייה לפרטיות.
- השינויים התכופים בסביבה הדיגיטלית מחייבים עדכון שוטף באמצעים וביכולות הקיימות לחדירה לפרטיות: הן על-מנת להיות מודעים לאיום והן על-מנת שניתן יהיה להתגונן מפניו.

ניתן כמובן להפחית את הציפייה לפרטיות ולהזהיר את המשתמשים בדבר חשיפתם לאמצעי מעקב בסביבה הדיגיטלית באמצעות חינוך והסברה. מצד שני, העובדה שהטכנולוגיה מצויה עדיין בהתהוות ומשתנה בקצב מסחרר עשויה לצמצם את האפקטיביות של פתרונות אלו.

2. מהי המשמעות של יישום ההסדר המשפטי הקיים על הרשת?

ההסדר המשפטי הקיים מבחין בין האזנת סתר לבין צו חיפוש מבחינת החומרה, ולכן גם מתייחס להאזנת סתר ביתר קפדנות מבחינת הדרישות המשפטיות. האזנת סתר המוסדרת בחוק האזנות סתר המגן על סוד השיח - מחייבת צו של נשיא בית משפט מחוזי או סגנו, שיינתן בתנאים המוגדרים בחוק. צו חיפוש, לעומת זאת, הוא בסמכותו של בית משפט שלום. חיפוש והאזנת סתר נבדלים זה מזה מבחינת מודעות אובייקט המעקב, משך הזמן של הפגיעה, וההשלכה על צדדים שלישיים. בכל מה שנוגע לחיפוש המדובר בפגיעה חד-פעמית, הנחקר מודע לה, והפגיעה ממוקדת בו ובחפציו. האזנת סתר, מנגד, היא פגיעה מתמשכת, ללא ידיעת הנחקר, אשר עלולה לפגוע בפרטיות החשוד (כאשר במסגרת מכלול שיחות החשוד להן מאזינות רשויות החקירה, נכללת גם לתקשורת אישית של החשוד אשר אינה רלוונטית לחקירה) וכן לפגיעה בצדדים שלישיים (משתמשים אחרים בקו הטלפון, וכן צדדים המשוחחים עם הנחקר).[385]

על רקע הדברים הללו, איזה הסדר משפטי ראוי ליישם ברשת? **נראה כי מעקב ברשת דומה יותר להאזנת סתר**. המדובר בפעולה המתבצעת ללא ידיעת הנחקר – לעיתים תוך שיתוף פעולה עם ספק השירותים בלבד. המדובר בפעילות מתמשכת, העלולה גם לפגוע בפרטיותם של גולשים אחרים.

3. ריכוז המלצות

המלצותינו יוצאות מתוך נקודת הנחה, לפיה יש לשמור על פרטיות הגולשים, וכי השינויים הטכנולוגיים המפליגים הטמונים בסביבה הדיגיטלית אינם צריכים לצמצם את הזכות לפרטיות או את ההגנה עליה. עם זאת, את הכללים המשפטיים הפרטניים, יש לעצב בשים לב למאפיינים

[385] ראו דברי עו"ד נאוה בן אור, בע' 22 לתמליל מושב אחר הצהריים, כנס שפיים (27.12.01).

הטכנולוגיים המיוחדים שנדונו לעיל. כמו כן, אין לשלול את הכיוון ההפוך: הבניית ערכים של פרטיות לתוך הטכנולוגיה.[386] בנוסף, יש להביא בחשבון את היעדר הגבולות ברשת,[387] וכן יש להביא בחשבון את הפער הדיגיטלי: יכולתם (הכלכלית וטכנולוגית) של גולשים להתמודד עם האיום על זכותם לפרטיות שונה. לפיכך, יש לידע ולחנך את הציבור בדבר זכותו לפרטיות, האיומים עליה, והדרך להתמודד עם איומים אלה.

קושי נוסף, הוא שלצד האיום הציבורי (מהמדינה) על הזכות לפרטיות, יש בסביבה הדיגיטלית איום משמעותי לא פחות על הפרטיות – איום שמקורו בגורמים מסחריים-פרטיים. על רקע זה, עולה השאלה, באיזו מידה יש להגביל את המדינה בשימוש באמצעים הנגישים לכל גורם פרטי? שאלת היחס שבין הסדרה פרטית להסדרה ציבורית מחייבת דיון נפרד, וכאן אנחנו מבקשים להסתפק בהצבעה על הקשיים.

[386] ראו למשל את הסטנדרט הטכנולוגי של P3P באתר http://www.w3c.com, וכן: Lessig Lawrence, **Code and other law of Cyberspace** (N.Y. 1999).

[387] ראו: David R. Johnson & David G. Post, "Law and Borders: The Rise of Law in Cyberspace" 48 **Stan. L. Rev.** 1367 (1996).

IV. סביבת המידע כזירת תעמולה: ביטחון, חופש הביטוי ואחריות ספקים[388]

א. מהו "טרור תעמולתי"?

1. טרור תעמולתי ותעמולה בשירות הטרור

יש הרואים בטרור סוג של תקשורת. דהיינו, העברת מסר באמצעות מעשים במקום באמצעות מילים. במובן זה הטרור עצמו מהווה תעמולה. קבוצות וארגונים הנוקטים פעולות אלימות על-מנת לקדם מטרות פוליטיות, יוצרים את אפקט החרדה והפחד באמצעות התקשורת. האפקט התקשורתי של הפעולות האלימות הוא היוצר את אפקט הטרור של אותן פעולות אלימות. ארגוני טרור תלויים בפרסום הניתן להם, בלעדיו אין הם יכולים להתקיים. במובן זה מתקיימים יחסים סימביוטיים בין טרור לאמצעי התקשורת.[389] יחסים אלה באים לידי ביטוי בכך שארגוני הטרור זקוקים לתקשורת כ"אוויר לנשימה"[390] משום שללא פומביות ופרסום לא יהיה למאבקם כל ערך, ואילו ערוצי התקשורת השונים המצויים בתחרות מתמדת על נתחי השוק נדרשים לספק מידע, וריגושים ועל כן עלולים ליפול בקלות לידיהם של ארגוני הטרור המספקים דרמה בשפע, וכך להפיץ, מבלי להיות מודעים לכך, את תעמולתם. לפיכך, ככל שתקשורת ההמונים מתפתחת ומתפשטת ובאמצעותה גדל הסיקור הניתן לארגוני טרור למיניהם, הפוטנציאל למעשי טרור גדל. היבט זה מעורר כמובן דילמות באשר להיקף ולאופי הסיקור התקשורתי של פיגועי טרור, דילמות שמצויות מחוץ לגדר הדיון הנוכחי.

אולם תעמולה ישירה מהווה גם חלק מרכזי בפעילותם של ארגוני טרור. "טרור תעמולתי" או לוחמה פסיכולוגית (Psychological Warfare או בקיצור PsyWar) הינו ניסיון ליצור מציאות נוחה באמצעות השפעה על עמדות מודעות ולא מודעות של היריב. מטרותיה של התעמולה עשויות להיות מגוונות. לעיתים מטרתה לזרוע חרדה, ולהרתיע אוכלוסיות. הרציונל - אם האויב חושש, קל יותר לנצחו. מלחמה פסיכולוגית "חכמה" תוקפת את ה"אני מאמין" של היריב, תפיסותיו, וערכיו.[391] על-מנת שלוחמה פסיכולוגית תצליח יש צורך להכיר ולהבין את דעותיו והערכים בהם דוגל ה"אויב".[392] פרק זה יעסוק בסוגיות הנוגעות לתעמולה בשירות הטרור. ככל שארגון הטרור הינו מתוחכם ומבוסס יותר, כך יגבר השימוש שנעשה על ידו בלוחמה פסיכולוגית.[393] טרור תעמולתי עושה שימוש בחופש הביטוי הניתן לאמצעי התקשורת ההמוניים, על-מנת להעביר את מסריו הפוגעניים. התקשורת החופשית בחברה מערבית פגיעה ביותר לניצול ומניפולציה על-ידי ארגוני טרור. ארגוני טרור רואים בתקשורת החופשית כלי יעיל ונוח ועל כן הם עושים בו שימוש ציני, גם כאשר הם חשים בוז לערכי הדמוקרטיה וחותרים נגדם. טרור תעמולתי עושה שימוש

---

[388] בכתיבת פרק זה נעזרנו רבות בהרצאותיהם של פרופסור אריאל בנדור, ד"ר הלל נוסק, ד"ר לימור יגיל, עו"ד דורית ענבר, ד"ר יריב צפתי, ד"ר יובל קרניאל, וגב' יעל שחר, ותודתנו נתונה להם. האחריות לתוכן היא כמובן שלנו בלבד.

[389] ראו: Paul Wilkinson, "The Media and Terror: A Reassessment", 9 **Terrorism and Political Violence** 51-65 (1997): www.st-and.ac.uk/academic/intrel/research/cstpv/publications1c.htm. (להלן: Wilkinson). לגישה הפוכה ראו: Michel Wieviorka, "The Making of Terrorism" (Chicago 1993) (דוחה את הטענה כי מתקיימים יחסים סימביוטים בין התקשורת לארגוני טרור).

[390] מרגרט תאצ'ר אמרה כי ארגוני טרור רעבים ל- "oxygen of publicity".

[391] שרי גולדשטיין-פרבר, "לוחמה פסיכולוגית בעידן ההרתעה השני", **מערכות** 378-379 (2001), 2, בע' 3.

[392] John Elliston, "Psywar Terror Tactics" (1996): www.parascope.com/ds/1096/psy.htm.

בערכי הדמוקרטיה ובראשם בחופש הביטוי על-מנת למלכד את רשויות השלטון, כך שיאלצו להסכין עם התעמולה המתפרסמת או לצנזר את התקשורת ובכך לעורר עליהם ביקורת ציבורית.[394]

ארגוני הטרור עושים שימוש באמצעי תעמולה לקידום ארבע מטרות עיקריות:[395]

1. הפצת תעמולה וזריעת פחד ואימה בקרב "קבוצת המטרה".
2. גיוס תמיכה נרחבת ככל האפשר במאבקם בקרב האוכלוסייה המקומית ודעת הקהל העולמית. הם עושים זאת, באמצעות הצגת צדקת מטרתם ותיאור ניצחונם הבלתי נמנע.
3. שיבוש תגובות הממשל, למשל באמצעות הצגת פעולות הממשל כנגד טרוריסטים כאמצעים רודניים וחסרי תועלת.
4. גיוס פעילים והפעלתו בפעולות הסברה, גיוס תומכים, וגיוס כספים.

2. תוכן התעמולה

ברמה ההסברתית ראוי להבחין בין תעמולה המופנית לקהלי יעד השונים. תעמולתם של ארגוני הטרור מופנית כלפי תומכים פוטנציאלים, כלפי הציבור המקומי שהוא חלק מן ה"אויב", וכן כלפי הקהילה הבינלאומית. תכני התעמולה יושפעו כמובן מקהל היעד. בהקשר זה מקובל להבחין בין שני היבטים של תעמולה:[396]

הראשון, **ההיבט "הקשה"**, מתייחס ליצירת דעות שליליות בקרב הציבור לגבי המדינה, הממשלה החברה וכדומה. המטרה היא ליצור ניכור בין הציבור למדינה. הדרך בה ארגוני הטרור עושים זאת היא באמצעות הצגת "מתנגדיהם" כהתגלמות הרֶשע. מאחר שהאויב כה מושחת, מוטלת עליהם חובה, כך יאמרו, להשמידו.[397]

השני, **ההיבט "הרך"**, מתייחס ליצירת דעה חיובית ותמיכה בקבוצה או בארגון אשר מובילים את המאבק. כאן המטרה היא לעודד אנשים לתמוך בארגון ואף להצטרף אליו. הדרך לעשות זאת היא באמצעות שכנוע אנשים, צעירים בעיקר, לקבל על עצמם את ערכיו של הארגון ודרכי פעולתו או להזדהות עמו. לרוב מדגישים ארגוני הטרור את צדקת מטרתם, המבוססת בדרך כלל על אידיאולוגיה חילונית כלשהי. הם אינם מציגים עצמם כ"טרוריסטים" הנוקטים פעולות טרור, כי אם כ"לוחמי חופש" בעלי מטרה ודרך מוצדקות. ארגוני הטרור יצניעו בדרך כלל את פעילותם האלימה משיקולים הסברתיים-תדמיתיים, אך יציגו את פעילות השלטונות תוך שימוש במונחים כגון: טבח, רצח, והשמדת עם. ארגוני הטרור מציגים עצמם כצדיקים נרדפים אשר חופש הביטוי שלהם מוגבל ואוהדיהם נעצרים על-ידי השלטונות, כל זאת כחלק ממלחמתם הפסיכולוגית.

---

393 Wilkinson, supra note 392.

394 יריב צפתי, גבי וימן, "טרור באינטרנט", **פוליטיקה** 4 (תש"ס) 45, 46-47 (להלן: צפתי ווימן, "טרור באינטרנט").

395 Wilkinson, supra note 392.

396 B. Raman, Psychologigal Warfare (Psywar) in the New Millennium (1999), available at: www.subcontinent.com/sapra/nationalsecurity/img_1999_02_002.html

397 האתרים של החזבאללה והחמאס, למשל, מתמקדים בהצגת הפעילות הישראלית כטרור. הצגת האויב בדרך זו נועדה להצדיק את השימוש באלימות ואת הפגיעה בחפים מפשע. בדומה צבא השחרור הלאומי הקולומביאני מציין באתרו כי האלימות אותה נוקט הארגון היא תוצאה של האלימות השוררת בעולם ולא הגורם למציאות זו. ראו צפתי ווימן, "טרור באינטרנט", לעיל הערה 394, בע' 48-49.

המטרה היא לערער את הטענות בדבר הלגיטימיות של הממשל הקיים, וכן להדוף את כל האשמה בדבר השימוש באלימות כלפי מתנגדיהם. רטוריקה נוספת אותה נוקטים ארגוני הטרור על-מנת ליצור לעצמם דעה חיובית כלפיהם היא רטוריקה של שלום ואי-אלימות, זאת למרות שמדובר, כאמור, בארגונים אלימים. רוב הארגונים יטענו בתעמולתם כי הם מעוניינים בפתרון של שלום.

3. דרכי תעמולה

דרכי התעמולה המקובלות הן באמצעות: עלונים, ספרים, רדיו טלוויזיה, פקס, ולאחרונה גם באמצעות האינטרנט. עד מלחמת העולם השנייה נעשה עיקר התעמולה באמצעות עלונים מודפסים. במהלך המלחמה גבר השימוש ברדיו כאמצעי תעמולה. השימוש בטלוויזיה כאמצעי תעמולה החל בשנות השישים של המאה העשרים, בעיקר בתקופת מלחמת וייטנאם. גם בזמן המלחמה הקרה נעשה שימוש בתעמולה אז נעזרו רבות בעיתונאים, מחברים והוצאות ספרים.

עלונים, ספרים, שידורי רדיו, טלפון, פקס, והאינטרנט משרתים בעיקר את ההיבט "הקשה" של התעמולה תוך יצירת ניכור בין האזרחים למדינה, אך אין להם כמעט השפעה על ההיבט "הרך" שמטרתו, כאמור, ליצור הזדהות עם הארגון הנדון. ערכה של הטלוויזיה לטרוריסט מתבטא בכך שהיא משרתת גם את הצדדים "הרכים" של התעמולה.[398] פרסום תמונות או סרטונים קצרים באמצעות האינטרנט יכול לשרת אף הוא, צד זה של התעמולה.

4. האם המדיום משנה את המהות? לוחמה פסיכולוגית בעידן הטכנולוגי

מטרות ארגוני הטרור נשארות כשהיו, גם בסביבה הדיגיטלית. אלא, שהמדיום מציע אפשרויות חדשות, ומאפייניו עשויים להשליך על מעמדם של הדוברים, המסרים, מידת האפקטיביות שלהם ועוד – ומתוך כך, על היחס המשפטי אליהם. השאלה, אם כן, היא באיזו מידה השימוש שעושים ארגוני הטרור באינטרנט לצורכי תעמולה שונה משימושים שנעשו באמצעי תקשורת אחרים, ולכן מחייב טיפול משפטי שונה?

ניתן להצביע על מספר מאפיינים של המדיום הדיגיטלי, המחייבים התייחסות. המאפיינים שלהלן אינם רשימה ממצה, אולם משקפים היבטים ייחודיים של המדיום הדיגיטלי. יש להעיר כי מאפיינים אלה עשויים להיות חופפים בחלקם, ומכל מקום, יש לראותם כמכלול.

- **אינטראקטיביות**: האינטרנט, בניגוד לאמצעי התקשורת הקונבנציונאליים, מאפשר יחסים אינטראקטיביים בין הארגון לבין ציבור הגולשים. היבט זה מאפשר להשתמש ברשת כאמצעי יעיל להפעלתם של פעילים, וניהול פעילויות. כך למשל, בנוסף לתעמולה המתפרסמת באתר האינטרנט עצמו, אתרי טרור רבים מציעים לציבור הגולשים לרכוש ספרים, קלטות וידאו ואודיו, מדבקות, חולצות וסמלים של הארגון,[399] כל אלה מהווים גם הם אמצעי תעמולה. מובן שפעילות מהסוג הזה איננה אפשרית בתקשורת ההמונים המסורתית.

[398] Raman, supra note 399.

[399] צפתי ווימן, "טרור באינטרנט", לעיל הערה 394, בע' 53, 56.

- **מיקוד המסר**: אינטראקטיביות עשויה לאפשר לארגון הטרור למקד את המסר. לוחמה פסיכולוגית שעשתה שימוש בכלי תקשורת המונים כוונה כלפי קהילה רחבה או כלפי קבוצת אנשים בלתי מסוימת. האינטרנט, לעומת זאת, מאפשרת לבחור קהל יעד מצומצם מתוך הקהילה ולכוון את התעמולה כלפיו בלבד. ניתן לתפור מסרים שונים לקהילות שונות (דעת הקהל העולמית, מצטרפים פוטנציאליים לאירגון, וכדומה). משום כך, השימוש ברשת עשוי להיות יעיל יותר מנקודת מבטו של הטרוריסט.
- **גלובליזציה**: העובדה שמדובר ברשת גלובלית, הנגישה לכל בכל רחבי העולם, מאפשרת לארגוני טרור להגיע לציבורים נוספים מחוץ לאזור בו הם פועלים. לעובדה זו עשוי להיות יתרון הסברתי עצום, לצד היתרון התפעולי המאפשר גיוס פעילים מחוץ לגבולות המדינה והפעלתם.
- **נגישות וזמינות**: תעמולה ברשת האינטרנט יכולה להתבצע בעלויות נמוכות יחסית: משלוח דואר אלקטרוני, הקמת אתר באינטרנט. ניתן גם בעלות נמוכה יחסית להקים אתר המפיץ את המסרים התעמולתיים.
- **עצמאות**: בניגוד לפרסום בכלי התקשורת ההמוניים המנוהלים באופן ריכוזי על-ידי המוציאים לאור המפעילים מנגנוני עריכה ופיקוח על התוכן, האפשרות להתבטא ברשת האינטרנט זמינה לכל. ניתן לעשות שימוש במערכות אינטראקטיביות קיימות: כגון צ'אטים, ופורומים המנוהלים על-ידי ספק האינטרנט או בעל אתר. ראוי לציין כי בעוד שארגון טרור המבקש להעביר מסר באמצעי תקשורת המוניים יעשה שימוש בפעולות טרור על-מנת לזכות בחשיפה התקשורתית, נגישותה של רשת האינטרנט מייתרת זאת.
- **הצטמקות הקהל?** למרות העובדה שרשת האינטרנט נגישה לכל דובר ללא כל מערכת צנזורה, סינון או עריכה, ובעלות נמוכה, יש בה חסרונות עבור הדובר הטרוריסט: המסרים התעמולתיים עלולים להיבלע ב"ערפיח המידע" הקיים ברשת,[400] ולא לעמוד במרכז תשומת הלב הציבורית, בניגוד למצב שבו כלי התקשורת ההמוניים קובעים את סדר היום הציבורי. בנוסף, בהשוואה לכלי תקשורת המוניים (כגון רדיו וטלוויזיה), אחוזי החדירה של האינטרנט נמוכים יחסית בקרב הציבור הרחב. יתרה מזאת. הגלישה ברשת מחייבת רמת אוריינות גבוהה יחסית לזאת הנדרשת מצופה טלוויזיה, כמו גם אמצעים כספיים. במילים אחרות, הפער הדיגיטלי מביא לכך שקהל היעד הפוטנציאלי של הטרוריסט המבקש להשתמש ברשת מצומצם יותר, ומתוחכם יותר.
- **לגיטימציה**: חלקם של המאפיינים שמנינו עד כה, ובעיקר האינטראקטיביות, הנגישות, והעצמאות מאפשרים לארגון הטרור לא רק להעביר את המסר, אלא גם לזכות בלגיטימציה גבוהה יותר מאשר יכול היה להשיג באמצעות כלי התקשורת המסורתיים. ברשת, ארגון הטרור הוא דובר, ומעמדו כדובר זהה, לפחות בנקודת המוצא, לזה של עיתון מקוון, אתר מסחרי, או כל ארגון פוליטי לגיטימי. הדבר עשוי

[400] ראו: David Shenk, **Data Smog** (New York, 1997).

לבוא לידי ביטוי למשל בכתובת האתר (URL), או בקישוריות (לינקים) לאתרים אחרים. לרוב ההפניה היא לאתרים בעלי אידיאולוגיה הקרובה לזו של הארגון או אתרים אחרים הקשורים לארגון עצמו. ניתן אף למצוא הפניות לאתרים של ארגוני זכויות אדם.[401] קישורים מסוג זה עשויים ליצור רושם של שיתוף פעולה, חסות או תמיכה אחרת. בכך, מנצל הטרוריסט-הדובר את יתרונות המדיום להשגת לגיטימציה.

ב. חופש הביטוי באינטרנט

במבט ראשון, תעמולה של ארגון טרור היא חלק בלתי נפרד מפעילות הטרור, ומתוך כך מתעורר הצורך הציבורי למנוע אותה ככל האפשר. הדרכים להיאבק בטרור מגוונות, וכל דרך בה נוכל להיאבק בו, משרתת את הציבור: כשם שהמשפט אוסר גיוס כספים לארגון טרור, חברות בו, וכמובן מניעת הפעילות החבלנית עצמה, כך, לכאורה, על המשפט להקשות גם על ההפצת התעמולה מטעם אותם ארגונים. אלא, שיש בתעמולה היבט אחר: היא מהווה ביטוי. לפיכך, יש לבחון את שאלת היחס המשפטי לתעמולת הטרור ברשת (גם) במשקפיים של חופש הביטוי.

במסגרת הדיון של חופש הביטוי, יש לברר תחילה מהו למעשה האינטרס המוגן. מובן שהדאגה איננה לגורל זכותו של הטרוריסט להתבטא בחופשיות, אלא לגורלו של האינטרס הציבורי לדעת, או כפי שאינטרס זה מכונה בדרך כלל, "זכות הציבור לדעת". אכן, לא תמיד ברור לנו מה התועלת הגדולה עבורנו שבחשיפה לביטוי של טרוריסט. יתכן שבמקרים רבים אכן אין בכך כל תועלת לציבור. אלא, שעקרון חופש הביטוי מניח כי לחשיפה לדעה אחרת, ואפילו שיקרית, יש יתרון: היא ממריצה את הביטוי הנגדי, מאתגרת את "האמת", חושפת את "פרצופו האמיתי" של היריב, ומאלצת אותנו לבחון שוב את עמדותינו.[402] בכל מקרה, ההצדקות המקובלות של חופש הביטוי מניחות כי אין זה תפקידה של המדינה להתערב ולהגביל את הגישה לביטוי.

שאלות הנוגעות לחופש הביטוי אינן חדשות למשפט הישראלי. הזכות לחופש הביטוי אמנם איננה מנויה במפורש בחוקי היסוד, אולם היא נחשבת לזכות יסוד,[403] ומספר שופטים העירו בהערות אגב בפסיקה כי יש לקרוא אותה לתוך חוק יסוד: כבוד האדם וחירותו.[404] בפסיקה הישראלית פותחה דוקטרינה ענפה בנושא זה, הבנויה סביב מערכת של איזונים בין חופש הביטוי לבין זכויות אחרות (למשל הזכות לשם טוב). במקרים אלה מופעל בדרך כלל "איזון אופקי".[405] או איזונים בין חופש הביטוי לבין אינטרסים ציבוריים אחרים, דוגמת שלום הציבור, הסדר הציבורי וכדומה

---

[401] צפתי ווימן, "טרור באינטרנט", לעיל הערה 394, בע' 57.

[402] הדברים שבטקסט מניחים את תיאוריית חקר-האמת של ג'ון סטיוארט מיל כהצדקה לחופש הביטוי, אולם ניתן להגיע למסקנות דומות גם לפי הצדקות אחרות. לדיון בבסיס העיוני של חופש הביטוי, ראו אילנה דיין אורבך, "המודל הדמוקרטי של חופש הביטוי", **עיוני משפט** כ (תשנ"ז) 377; גיא פסח, "הבסיס העיוני של חופש הביטוי ומעמדה המשפטי של העיתונות", **משפטים** לא (תשס"א) 895.

[403] ע"פ 255/68 **מ"י נ' בן משה**, פ"ד כב (2) 427, 435; ע"א 723/74 **הוצאת עיתון "הארץ" בע"מ נ' חברת החשמל לישראל בע"מ**, פ"ד לא (2) 281, 295; בג"צ 153/83 **לוי נ' מפקד המחוז הדרומי של משטרת ישראל**, פ"ד לח (2) 393, 398.

[404] בג"צ 2481/93 **דיין נ' מפקד מחוז ירושלים**, פ"ד מח (2) 456, 468; ע"א 4463/94 **גולן נ' שירות בתי הסוהר**, פ"ד נ (4) 136, 158.

(שאז מופעל "איזון אנכי").[406] איזונים אלה, שהנפוץ שבהם הוא "מבחן הוודאות הקרובה", מתייחסים לאפשרות להגביל את הביטוי של הדובר.[407] הם פותחו בשים לב למאפיינים הטכנולוגיים של כלי התקשורת. כך למשל, אחת ההצדקות המקובלות להתערבות בתכני השידור של תחנות רדיו וטלוויזיה המעבירות את שידוריהן באמצעות הספקטרום האלקטרו-מגנטי ("גלי האתר") היא שזהו משאב ציבורי ומוגבל.[408]

משום כך, מתעוררת שאלת היקף תחולתם של האיזונים שפותחו בפסיקה על המדיום החדש.[409] **עמדה אחת** גורסת כי האיזון הוא בעיקרו ערכי, איננו תלוי-טכנולוגיה, ועל כן הסביבה החדשה איננה צריכה לשנות את היחס העקרוני של המשפט לבעיה המתעוררת.[410] **עמדה אחרת** הפוכה. לפיה, לא רק שאין להחיל את הכללים הקיימים בסביבה הדיגיטלית כדבר מובן מאליו, אלא שהמדיום החדש מחייב בחינה מחודשת של העקרונות והאיזונים הקיימים. בהקשר של חופש הביטוי מתחייב, לפי עמדה זאת, צמצום ניכר (עד כדי ביטול) של התערבות המשפט בחופש הביטוי, גם באמצעי התקשורת המסורתיים.[411] **עמדת ביניים** גורסת כי הטכנולוגיה השונה מחייבת שינוי משפטי, אולם זה איננו חייב להיות דרמטי. את הכללים המשפטיים יש לעצב על-פי אותם עקרונות וערכים בהם החזקנו עד כה, אך יש להתאים אותם למדיום החדש, על-פי מאפייניו הייחודיים. בעיקר מדגישים מצדדי עמדה זאת כי ברשת האינטרנט אין בעייה של מחסור (בשונה מאשר גלי האתר). בנוסף, רגולציה של ביטוי ברשת כרוכה בעלויות חדשות, בשל האפשרויות "הדמוקרטיות" הגלומות ברשת: הנגישות גבוהה יותר, עלות הביטוי קטנה יותר, וישנה אפשרות לביטוי אינטראקטיבי: הגולש איננו רק צרכן פסיבי של הביטוי, אלא יש לו את היכולת להשתתף באופן פעיל בביטוי במדיום המוני.[412] רגולציה, גם אם מטרתה לגיטימית, עלולה לפגוע בכל אלה. **נראה שהמשפט הקיים נוטה לעמדה האחרונה, לפיה נקודת המוצא בעיצוב הכללים המשפטיים היא האיזונים הערכיים הקיימים, אבל יישומם ברשת מחייב תשומת לב למאפיינים הייחודיים שלה, ולהשלכות האפשריות של יישום כזה**: השופט מישאל חשין בתפקידו כיו"ר ועדת הבחירות המרכזית קבע כי אין להרחיב את ההגבלות שבחוק על דרכי תעמולה אל ביטוי של פוליטיקאי בצ'אט באינטרנט.[413] הנמקתו התבססה, בין היתר, על מאפייניה הייחודיים של הרשת ועל חשיבות חופש הביטוי.

---

405 ראו למשל ע"א 214/89 **אבנרי ואח' נ' שפירא**, פ"ד מג (3) 840.

406 ראו למשל בג"צ 399/85 **כהנא נ' הועד המנהל של רשות השידור**, פ"ד מא (3) 255; בג"צ 606/93 **"קידום" יזמות ומו"לות (1981) בע"מ נ' רשות השידור**, פ"ד מח (2) 1; בג"צ 6218/93 **כהן נ' לשכת עורכי הדין**, פ"ד מט (2) 529.

407 להרחבה בנושא המבחנים, שפיתוח בית-המשפט באשר לשאלה האם ביטוי נופל למסגרת העבירות, האוסרות ביטויים מסוגים שונים, ראו אלון הראל, "עבירות המגבילות את חופש הביטוי ומבחן "אפשרות ההתממשות של נזק: חשיבה מחודשת", **משפטים** ל (תשנ"ט), 69.

408 ראו למשל בג"צ 1/81 **שירן נ' רשות השידור**, פ"ד לה (3) 365.

409 לדיון יסודי ראו יובל קרניאל, "חופש הביטוי באינטרנט", **עלי משפט** א (תש"ס) 163.

410 לטיעון ברוח זאת, ראו אריאל בנדור, "הסדרה משפטית של האינטרנט לאחר אירועי ה-11 בספטמבר – בין מציאות למשפט" **משפט וממשל** ו (צפוי להתפרסם בתשס"ב).

411 לעמדה זאת, ראו אלון הראל, "אינטרנט וחופש הביטוי: הרהורים מחודשים על הרגולציה של ביטוי בעידן האינטרנט" **משפט וממשל** ו (צפוי להתפרסם בתשס"ב).

412 להשוואה בין מאפייני הטכנולוגיות הקיימות למאפייני הרשת, ראו: **Reno v. ACLU**, 521 US 844 (1997).

בהקשר לרשת מתעוררת שאלה נוספת עקב המאפיינים הטכנולוגיים: הביטוי של הדובר מתאפשר על-ידי פעולה של צדדים שלישיים שונים, כמו ספקי שירותי איחסון לאתרים, מנהלי אתרים ופורומים מקוונים וכדומה. מכאן הצורך לגבש עמדה באשר לאחריותם: האם אפשר להטיל עליהם אחריות לביטוי שהם מאפשרים את קיומו (אחריות עקיפה)? האם ראוי לעשות כך? מה ההשלכות הנלוות של קביעת מדיניות כזאת?

ג. אחריות ספקים

במקרים שבהם יש אינטרס ציבורי המצדיק את הגבלת הביטוי של ארגון הטרור ואת זכות הציבור לדעת, השאלה היא כיצד ניתן לממש אינטרס זה. מובן, שמתעורר קושי מעשי להגביל את הביטוי של ארגוני הטרור עצמם, שהרי הם אינם בתחומי המדינה, וממילא (וגם אם הם פועלים בתחומה), הם אינם מצייתים לחוק.

לפיכך, המקום הטבעי אליו הופנתה תשומת הלב, היא גורמים מתווכים שונים, המאפשרים לארגוני הטרור, בעצם פעילותם, להפיץ את מסריהם באתריהם (להלן: "אתרי טרור"). כך למשל ספק אינטרנט המאחסן על גבי השרתים שלו את האתרים של ארגוני הטרור; ספק המאפשר למנויים גישה לאתרים כאלה (בין אם הם מאוחסנים בשרתים שלו או לא), אתרי אינטרנט היוצרים קישור לאתרי-טרור, אתרים המפעילים שירותים אינטראקטיביים (פורומים, צ'אטים וכדומה), ועוד. מתווכים אלה מהווים בפועל מעין "צוואר הבקבוק" טכני: הם נקודה נוחה שבה ניתן לצמצם את היקף פעילות התעמולה של ארגוני הטרור. מכאן מתעוררת שאלת אחריותם של גורמי הביניים הללו.

שאלת האחריות של ספקי השירות השונים איננה ייחודית ל"ביטוי" טרוריסטי: היא התעוררה בהקשר של ביטויים מזיקים אחרים, דוגמת לשון הרע, הפרת זכויות יוצרים, הפצת פורנוגרפיה, ופגיעה בפרטיות. הניסיון שהצטבר עד כה מעלה שלצד הרצון לסכל ולהגביל את הביטויים המזיקים, ישנם שיקולים נוספים הקשורים למבנה השיח הציבורי ברשת, לתיפקוד השוק ועוד. תחילה נסקור את השיקולים השונים בשאלת הטלת האחריות על ספקי השירות: מהם היתרונות של כלל כזה ומהן השלכותיו? לאחר מכן נציג את המודלים המשפטיים שפותחו בהקשר זה. בהמשך, נסקור את המצב המשפטי הקיים בארץ – על אי-הוודאות שבו. נסיים בהמלצותינו.

<u>1. שיקולים בהטלת אחריות על גורמי ביניים (ספקי שירות)</u>

כאמור, הקושי לזהות, לאתר ולאכוף את החוק על ארגון הטרור הוא זה שמוביל לגורם הביניים. במילים אחרות, המניע המרכזי מאחורי הכלל של הטלת אחריות על גורמי הביניים הוא הרצון להגן על אינטרסים מוגנים, וכאן, האינטרס הציבורי שבמניעת פעילות תומכת-טרור. להטלת האחריות על הספקים יש מספר יתרונות בהקשר זה:

---

[413] ראו תב"מ 16/2001 **ש"ס – התאחדות הספרדים העולמית שומרי תורה נ' ח"כ אופיר פינס, סגן יו"ר ועדת הבחירות המרכזית** (החלטת יו"ר ועדת הבחירות המרכזית, 30.1.01).

- קל יותר לאתר ספק שירות, מאשר את משתמש-הקצה הבודד שהפיץ תעמולת טרור.[414] הספק מנהל את עסקו בגלוי, לאורך זמן, יש לו נוכחות עסקית-פיזית ופעילות פיננסית ומשפטית שקל לאתר.
- בעידן הטכנולוגי מתעצמת הבעייתיות שבאיתור הדובר המקורי, שכן לא ברור כלל כיצד ניתן להחיל ולאכוף חוקים מדינתיים על טרור תעמולתי המופץ באינטרנט, שהינה רשת גלובלית. דוגמא לבעיה זו ניתן לראות בפרשת *LICRA v. Yahoo!*. בפרשה זאת קבע בית משפט צרפתי כי חברת יאהו! חייבת לציית לחוק הצרפתי האוסר הפצת פריטים נאציים באינטרנט, ולכן צריכה לחסום את גישת הגולשים בצרפת לאתרים שבהם מוצעים פריטים כאלה למכירה.[415]
- ואכן, רוב הארגונים האנטי-משטריים פועלים בדרך כלל מחוץ למדינה כלפיה מכוונים מעשיהם. הפתרון לבעיה זו טמון ביצירת אמנות הסדרה בינלאומיות, אולם גם פתרון זה אינו פשוט, שכן כלל לא בטוח שמה שמדינה אחת תראה כ"טרור תעמולתי" יראה ככזה על-ידי מדינה אחרת.
- הטלת אחריות על גורמי הביניים מאפשרת לא רק אכיפה בדיעבד, אלא גם מניעה מראש: הטלת האחריות יוצרת תמריץ לספק השירות לסנן תוכן לפני פרסומו, ועל-ידי כך למנוע הפצת תוכן שעלול לסכן אותו באחריות משפטית.
- להשלמת התמונה, בהקשר הרחב של הטלת אחריות על גורמי ביניים בגין תוכן מזיק שמקורו במשתמשים ישנו שיקול נוסף: במקום שהנזק יפול כולו על כתפי נפגע בודד, הרי שהטלת האחריות על הספק מאפשרת פיצוי לניזוק. עקרון זה מעביר את הנזק, בשלב הראשון, אל הספק, שהוא בדרך כלל "כיס עמוק". כעניין מצוי, יש להניח שהספק יגלגל את העלות אל ציבור הצרכנים שלו: באופן כזה, הנזק יתפזר בין ציבור הגולשים, באמצעות דמי המנוי. היבט זה רלוונטי פחות למצבים של מניעת טרור, שכן המטרה המרכזית היא למנוע את הנזק מראש ולא לזכות בפיצוי בדיעבד.

אלא, שלצד יתרונות אלה, להטלת אחריות על ספק השירות, עלולות להיות השלכות לא-רצויות:

- הטלת האחריות על ספקי השירות תחייב אותם לנקוט שורת אמצעים כדי להימנע מחבות (למשל יצירת מנגנון בקרה ופיקוח), או כדי להתגונן מפניה (למשל על-ידי ייעוץ משפטי או, בהקשר האזרחי, רכישת ביטוח). לאמצעים אלה יש עלות כספית גבוהה.

---

[414] צפתי ווימן, "טרור באינטרנט", לעיל הערה 394, בע' 58.

[415] ראו: **League Against Racism and Antisemitism (LICRA) v. Yahoo! Inc., Yahoo! France** (County Court, Paris, 20.11.00. http://www.lapres.net/html/yahen11.html. בית משפט אמריקני קבע כי יאהו! איננה חייבת לציית לצו הצרפתי. **Yahoo!, inc., v. La Ligue Contre le Racisme et L'antisemitisme**, 169 F.Supp.2d 1181 (N.D. Cal., 2001)., נמצא ב http://www.cand.uscourts.gov/cand/tentrule.nsf/4f9d4c4a03b0cf70882567980073b2e4/daaf80f58b9fb3e188256b060081288f/$FILE/yahoo%20sj%20%5Bconst%5D.PDF .

- השתת העלויות על ספק השירות משמעותה בפועל היא כי מנויי הספקים, קרי, ציבור הגולשים, הם שיישאו בעלויות המאבק בטרור – ולא ציבור משלמי המיסים בכללותו.
- השלכה צפויה נוספת היא ייקור שירותי האינטרנט. התוצאה היא מעמסה נוספת על הפעילויות החיוניות המתרחשות בסביבה הדיגיטלית: מחקר, פיתוח, חינוך, מסחר, ועוד. נוכח הפער הדיגיטלי בתוך החברה, והתחרות במישור הבינלאומי, הרי שלמעמסה זאת יש השלכה חמורה.
- החשיפה המשפטית והכלכלית יוצרת תמריץ בקרב ספקי שירותים להימנע מאספקת שירותים אינטראקטיביים, שבהפעלתם כרוך סיכון. בשירותים אלה הספק איננו מקור התוכן, ולכן גם אינו שולט בתוכן המופץ על-ידי הגולשים. מצד שני, שירותים אלה מהווים את מקור כוחה של הרשת, וטומנים בחובם אפשרויות כלכליות ודמוקרטיות רבות.
- להטלת האחריות יש השלכה מידית על חופש הביטוי: הספק, חושש שתוטל עליו אחריות, ולכן, במקרה של סָפֵק, יעדיף למנוע פרסום או פעולה של גולש. ספק השירות ייטה, אם כן, להפעיל "צנזורה פרטית". בכך ייפגע "מרחב הנשימה" החיוני של חופש הביטוי.
- למעשה, מדובר בהפרטה של מערכת האכיפה. שיקוליו של ספק השירות בבקרה ובפיקוח שיפעיל יהיו שיקולי עלות-תועלת מסחריים. מובן שאלה הם שיקולים לגיטימיים מבחינת הספק. אלא, ששיקולים אלה יחליפו בפועל את מערכת האיזונים המורכבת שפותחה בפסיקה – איזונים שנועדו להגן על זכויות אדם מחד גיסא, ולהבטיח את האינטרס הציבורי מאידך גיסא. יתרה מזאת. שיקול הדעת של הספק איננו כפוף לכללי המשפט המינהלי והחוקתי, הספק איננו נבחר, ואיננו חייב דין וחשבון (accountability) לציבור באשר לאופן הפעלת שיקול דעתו ותוכנו.

2. מודלים לאחריות גורמי ביניים

ניתן לסווג את המודלים הקיימים בחקיקה לשלושה סוגי הסדרים מרכזיים: הסדר של אחריות בקצה האחד, הסדר של חסינות בקצה השני, ובתווך – הסדר של חסינות מותנית ומוגבלת, הקמה בהתקיים תנאים מסוימים. יצויין, כי באירופה אומץ הסדר אחיד החל על כל סוגי ההפרות והנזקים, בעוד שההסדר האמריקני קובע הסדרים משפטיים שונים לפי סוגי הנזקים וההפרות - אם מקורם בלשון הרע, בהפרת זכויות יוצרים או בתחום אחר.[416] חשוב להדגיש כי מודלים אלה התפתחו בסביבתו של המשפט האזרחי: במצבים בהם ניזוק יחיד ביקש למנוע את המשך הפגיעה בו, ולזכות בפיצוי כספי בגין הנזק שנגרם לו, עקב תוכן שפורסם ברשת על-ידי גורם אחר כלשהו. משום כך, ההיקש מתחום זה לתחום הציבורי-פלילי של מניעת טרור מחייב זהירות רבה. סטנדרט האחריות בהקשר הפלילי גבוה יותר: הוא מחייב הוכחת כוונה פלילית מעבר לספק סביר.

---

[416] לדיון השוואתי, ראו: Kamiel Koelman, Bernt Hugenholtz, "Online Service Provider Liability for Copyright Infringememnt", **WIPO Workshop on Service Provider Liability** (Geneva, 1999).

א. מודל אחריות

מודל אפשרי אחד קובע כי גורמי הביניים אחראים לפעילויות השונות המתבצעות באמצעותם ו/או דרכם. מודל זה מצוי, למשל, בחקיקה האזרחית המטילה אחריות לא רק על המזיק, או המפר, הישיר, אלא גם על גורמים נוספים, המסייעים, בעקיפין, למזיק/מפר. כך למשל, בחוק איסור לשון הרע, תשכ"ה-1965 מוטלת אחריות לא רק על המוציא לשון הרע, אלא גם על "עורך אמצעי תקשורת", "אחראי אמצעי תקשורת", "מדפיס ומפיץ".[417] בדומה, דיני זכויות יוצרים מטילים אחריות, במצבים מסוימים, על מנהלי אולמות שמחה בגין השמעת יצירות מוסיקליות ללא רשיון, בידי תקליטנים.[418] כך גם במשפט האמריקני, שם מוכרת לצד האחריות הישירה בגין הפרת זכויות יוצרים גם אחריות עקיפה, על-פי שתי דוקטרינות משפטיות: הפרה תורמת (contributory infringement), ואחריות שילוחית (vicarious liability).[419] יצויין, כי במשפט הישראלי קיימת מזה זמן הדוקטרינה של "מעוולים במשותף",[420] ולאחרונה הכיר בית המשפט גם בעוולה של הפרה תורמת, לפחות בהקשר של דיני פטנטים.[421]

ב. חסינות מלאה

מודל אחר, המצוי בקצה השני של הקשת, מעניק חסינות מלאה לגורם הביניים. גישה זאת באה לידי ביטוי בסעיף 230 לחוק התקשורת האמריקני משנת 1996, המעניק חסינות לספקי שירותים אינטראקטיביים מפני אחריות בגין תוכן שמקורו באחר:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.[422]

יצוין כי החוק האמריקני מבחין בין מוציא לאור, החב באחריות מוחלטת, לבין מפיץ, שאחריותו קמה אם ידע, או היה עליו לדעת, על הנזק/ההפרה שנגרמים על-ידי צדדים שלישיים. סעיף 230 מעניק, לפי לשונו, חסינות מפני האחריות המוחלטת בלבד. אולם, סעיף זה פורש בהרחבה על-ידי

---

[417] ראו סעיפים 11, 12 לחוק איסור לשון הרע, תשכ"ה – 1965, וכן ק"פ (ת"א) 145/00 **שאול ויסמן נ' חגי גולן** (בית משפט השלום, החלטה מיום 16.10.01). http://www.law.co.il/computer-law/globes.htm.
בדומה, לפני תיקון החוק האמריקני, חלה אחריות מוחלטת על מוציא לאור, וסטנדרט אחריות מופחת על מפיץ. ראו למשל: **Cubby v. CompuServe, Inc.**, 776 F. Supp. 135 (S.D.N.Y., 1991); **Stratton v. Prodigy** (1995 WL 323710 N.Y. Sup. 1995).

[418] ראו סעיפים 2(1)-2(3) לחוק זכות יוצרים, 1911, וכן ת"א (ת"א) 46/94 **אקו"ם - אגודת קומפוזיטורים, מחברים ומולי"ם למוסיקה בישראל בע"מ נ' י.ט. גזית ירושלים בע"מ**, תק-של 97(4) 1371; ת"א (ת"א) 25/98 **הפדרציה הישראלית לתקליטים וקלטות בע"מ נ' אטלנטיס נשר בע"מ**, תק-מח 98(1) 2668; ע"א (ת"א) 1987/97 **אקו"ם - אגודת קומפוזיטורים, מחברים ומולי"ם למוסיקה בישראל בע"מ נ' אולמי חאן הדקל בע"מ**, תק-מח 99(1) 2144.

[419] ראו למשל: **Religious Technology Center v. Netcom Online Communication Services Inc**, 907 F. Supp 1361 (N.D. Cal. 1995.

[420] ראו סעיף 12 לפקודת הנזיקין [נוסח חדש].

[421] ראו ע"א 1636/98 **רב בריח בע"מ נ' בית מסחר לאביזרי רכב חבשוש בע"מ**, פ"ד נה (5) 337.

[422] ראו: 47 U.S.C. §230(c)(1).

בתי המשפט בארצות הברית, ונקבע כי ספקי השירות חסינים בכל מקרה, אפילו אם נמסרה להם הודעה על הנזק/ההפרה.[423]

ג. חסינות מותנית ומוגבלת

בין שני המודלים שתוארו זה עתה, מצוי מודל ביניים. לפי מודל זה, יהיה הספק פטור מאחריות ביחס לפעולות מסוימות בלבד, אם עמד בדרישות מסויימות שנקבעו בחוק. לדוגמא, חוק זכויות יוצרים האמריקני קובע הסדר פטור מפורט, המותנה בשלושה סוגי תנאים.[424] התנאי הראשון מתייחס **למיהות הספק**: עליו לבוא בגדר המונח online service provider, כפי שהוא מוגדר שם.[425] התנאי השני מתייחס **לסוג הפעולות**: החסינות תחול רק על הפעולות המנויות שם: העברה וניתוב תוכן במערכת,[426] שמירה זמנית אגב העברה (שימוש בזיכרון מטמון – caching),[427] איחסון,[428] וקישוריות (לינקים).[429] התנאי השלישי מגדיר **דרישות** שעל הספק לעמוד בהן כדי לזכות בחסינות, ובעיקר, מינוי "נציב תלונות",[430] ונקיטת מדיניות של הודעה-והסרה, שמשמעותה הסרה מיידית של החומר המפר, עם קבלת תלונה,[431] אימוץ מדיניות אכיפה, וכן נדרש הספק שלא למנוע מבעלי הזכויות לנקוט אמצעי פיקוח טכנולוגיים.[432]

הכלל שאומץ בדירקטיבה האירופית באשר למסחר אלקטרוני קובע גם הוא פטור מאחריות לפעולות מסוימות, בהתקיים תנאים המנויים שם, באשר לכל אחת מן הפעולות המזכות בחסינות.[433]

---

[423] ראו: **Zeran v. America Online, Inc**., 129 F.3d 327 (4th Cir. 1997). באותו מקרה הופץ ב-AOL (אתר וספק) מידע על אדם, לפיו הוא תומך בפיצוץ הבניין הפדרלי באוקלהומה ואף מוכר חולצות עם כתובת המביעה את תמיכתו. אותו אדם הודיע ל- AOL שמדובר בשקר, אך זו לא טרחה להסיר את הפרסום מהרשת, מחדל שהוביל לתביעתו את AOL. בית המשפט קבע שמטרת הקונגרס היתה להעניק הגנה רחבה לספקי שירותי האינטרנט ועל-כן יש לפרש באופן מרחיב את המונח "publisher" ב- 47 U.S.C. §230(c), ולכלול בו לעניין זה גם את המשמעות של מפיץ. כלומר: על ספק שירותי אינטרנט לא תחול אחריות של publisher או של distributor. במילים אחרות, החוק העניק לספקי האינטרנט חסינות מפני תביעות נזיקיות על-ידי מי שנפגע מפרסום לשון הרע וכדומה נגדו. כמו כן, החסינות מוענקת לספק גם בפני מפרסם הדברים, בגין פעולות צנזורה עצמית שנקט ספק השירות. פסק הדין מבטא את ההלכה הנוהגת בארצות הברית בסוגיה זאת. לביקורת, ראו את דעת המיעוט ב: **Doe v. American Online, Inc.**, 783 So.2d 1010 (S.Ct. Fla. 2001).

[424] 17 U.S.C. §512.

[425] 17 U.S.C. §512(k).

[426] 17 U.S.C. §512(a).

[427] 17 U.S.C. §512(b).

[428] 17 U.S.C. §512(c).

[429] 17 U.S.C. §512(d).

[430] 17 U.S.C. §512(c)(2).

[431] 17 U.S.C. §512(g).

[432] 17 U.S.C. §512(i).

[433] ראו סעיפים 12-15 לדירקטיבה: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJL 178.

3. המצב המשפטי בישראל

בישראל החוק הקיים איננו מסדיר במפורש את אחריותם של ספקי שירות אינטרנט לתוכן מזיק או אסור שמקורו בצדדים שלישיים. בתחומים מסוימים, חלה אחריות על גורמי ביניים מסורתיים (שאינם ספקי אינטרנט) בין מכוח הוראות חוק מפורשות (למשל חוק זכות יוצרים), ובין מכוח הפסיקה (למשל בדיני פטנטים). **המצב המשפטי הקיים בסוגיה זאת הוא אם כן עמום ומעורפל, ויש מקום לתהות על חוקתיות חלק מן ההסדרים הקיימים.**[434]

בחוק הישראלי שורת איסורים על פעילויות טרור,[435] וגם על סיוע עקיף לפעולות טרור,[436] אך תחולתם של איסורים אלה בסביבה הדיגיטלית איננו מובן מאליו. כך למשל ישנה בתקנות הגנה (שעת חירום) 1945 חובת צנזורה, כלומר הגשה מוקדמת לאישור הצנזור הצבאי של ידיעות המיועדות לפרסום.[437] החוק מגדיר מהו "פירסום" בצורה רחבה למדי, וכולל בין היתר "להפיץ, לפזר, למסור, להודיע, או לעשות מצוי לכל בני האדם."[438] לא ברור האם אתר אינטרנט שמתנהל בו פורום יהיה אחראי, לפי הגדרה זאת, לעבירות המתבצעות על-ידי הגולשים המשתתפים בפורום. בדומה, ספק המאפשר גישה לאתרי טרור. איסור נוסף המצוי בתקנות הוא מתן שירותי הדפסה להתאחדות בלתי מותרת.[439] שוב – גם כאן לא ברור אם סעיף זה ישים לגבי אתרי אינטרנט.

הפקודה למניעת טרור, תש"ח-1948 משקפת את המדיניות לפיה המאבק בטרור מחייב גם מאבק בתשתיות נלוות. כך למשל סעיף 1 לפקודה מגדיר חברות בארגון טרור באופן רחב, הכולל גם את מי שמפרסם דברי תעמולה לטובת הארגון; סעיף 2 כולל בהגדרת "פעילות בארגון טרור", בין היתר, נאום תעמולה באסיפה פומבית או ברדיו מטעם ארגון טרור, וסעיף 4 מגדיר "תמיכה בארגון טרור", ככוללת, בין היתר, פרסומים,[440] בע"פ או בכתב, של אהדה או קריאה לתמיכה בארגון טרוריסטי; החזקת חומר תעמולה עבור ארגון שכזה; תמיכה בכסף או בשווה כסף; העמדת חפץ או מקום לרשות ארגון טרוריסטי. גם כאן, ישנה עמימות רבה: לא ברור אם האיסורים האלה חלים רק על מקור התוכן (הדובר עצמו), או גם על מי שמספק לו את בימת הפרסום. עם זאת, בתי המשפט פירשו את הפקודה בצמצום, וזאת נוכח פגיעתה הישירה בזכויות יסוד, דוגמת חופש הביטוי.[441]

---

434 ראו למשל את עמדתו של גד ברזילי, "מרכז נגד פריפריה: דיני "מניעת טרור" כפוליטיקה", **פלילים** ח (תש"ס) 229.

435 ראו במיוחד את הפקודה למניעת טרור, תש"ח-1948.

436 ראו למשל תקנות הגנה (שעת חירום), 1945, במיוחד סעיפים 58, 66.

437 ראו סעיפים 87, 96 לתקנות הגנה (שעת חירום), 1945.

438 ראו סעיף 86 לתקנות הגנה (שעת חירום), 1945.

439 לדיון, ראו ע"פ 538/89 ***ורשבסקי נ' מ"י***, פ"ד מד (2), 870 (בית דפוס הדפיס חוברות הדרכה של החזית העממית. המערער הורשע בעבירה לפי תקנה 85(1)(ז) לתקנות ההגנה (שעת חירום), 1945).

440 המונח פרסום לעניין הפקודה מוגדר בחוק העונשין, תשל"ז-1977, בסעיף 34כד: "פרסום – כתב, דבר דפוס, חומר מחשב או כל מוצג חזותי אחר, וכן כל אמצעי שמיעתי, העשויים להעלות מלים או רעיונות, בין לבדם ובין בעזרת אמצעי כלשהו".

441 ראו בג"צ 547/98 **נועם פדרמן נ' ממשלת ישראל**, תק-על 99(4), 314; ת"פ (י-ם) 557/96 **מ"י נ' אריה בר יוסף**, תק – של 98(2), 762.

מגבלה נוספת על חופש הביטוי מצויה בפקודת העיתונות, המחייבת רשיון משר הפנים לשם הוצאת עיתון, ומקנה לו סמכות לסגור עיתון.[442] נראה, כי נוכח הפגיעה בחופש הביטוי, יש מקום לפרש חוק זה בצמצום, כך שהפקודה איננה חלה על האינטרנט, וכי לא יידרש רשיון להקמת אתר באינטרנט. נראה כי אין חולקים על עמדה זאת.

ד. ריכוז המלצות

השאלה הראשונה שצריכה לעלות על סדר יומו של המחוקק היא הערכת הצורך בחקיקה פרטיקולרית לעניין אחריות ספקי שירות לתוכן מזיק שמקורו בצדדים שלישיים. השאלה כרוכה בבדיקת התנהגותם בפועל של ספקי השירות בהיעדר הסדרה: האם אי הוודאות גורמת לתוצאות לא-רצויות. יש מקום לבחון האם הספקים נמנעים ממתן שירותים מסויימים (צ׳אטים, פורומים, שירותי איחסון אתרים וכדומה), או מגבילים ביטוי ביישומים השונים המופעלים על ידם. כך למשל, יש מקום לבחון כיצד מגיבה ספקית שירות אחסון אתרים לתלונה של גולשים כנגד אתר אחר, או כנגד דבריו של גולש אחר בפורום המופעל על-ידי הספקית.

- אם יתברר כי אי-הוודאות המשפטית הקיימת גורמת לכך שבפועל מתרחשת ״צנזורה פרטית״ **הרי יש מקום, לדעתנו, להבהיר את המצב המשפטי באמצעות חקיקה**.
- חקיקה כזאת צריכה למזער את ההשלכות הלא-רצויות שבהן דנו לעיל. במיוחד, יש לוודא כי שיקול הדעת שמפעיל הספק מוגדר בדיוק רב ככל האפשר, ומותיר לספק מרחב החלטה בהיר ומצומצם. בדרך זאת נמזער את ״האפקט המצנן״, את ״האצבע הקלה״ של הספק על סגירת אתרים ויישומים אחרים, ואת הפקרת שיקול הדעת הציבורי בידיים פרטיות.
- לטעמנו, כל אחד מן המודלים הקיימים שנסקרו לעיל (מודל של אחריות מלאה, חסינות מלאה או חסינות מותנית ומוגבלת) סובל מחסרונות ניכרים.
- נראה לנו שיש מקום לאמץ את גישה של הסדר אחיד באשר לסוגים שונים של תכנים מזיקים: בין אם מדובר בלשון הרע, פגיעה בפרטיות, בהפרת זכויות קניין רוחני או בתעמולת טרור.[443]
- יש מקום לאמץ את העקרון הכללי שנקבע בחקיקה האמריקנית בדבר חסינות לגורמי הביניים, אבל לסייג אותה בחריג: כדי להגן על האינטרסים והזכויות יש לאפשר לנפגעים אפיק אכיפה אפקטיבי, על-ידי פנייה לבית המשפט. בכך שונה הצעתנו מהדין האמריקני. בית המשפט יידרש לשקול את האינטרס הציבורי או זכות הפרט המוגנת, אל מול שיקולי המדיניות והאינטרסים הציבוריים האחרים. בדרך זאת יובטח כי האיזונים החוקתיים, הערכיים שפותחו בפסיקה, יישמרו, ולא יופרטו

---

[442] סמכות זו הייתה הבסיס לדיון בפרשת **קול העם**. ראו בג״ץ 73/53 **חברת ״קול העם״ בע״מ נ׳ שר הפנים**, פ״ד ז, 871. עוד לעניין זה, ראו בג״ץ 644/81 **עומר אינטרנשיונל אינק נ׳ שר הפנים**, פ״ד לו (1), 227 (עתירה כנגד צו הפסקת פרסום עיתון המשיב. הצו הוצא מכוח פקודת העיתונות לאחר שהופיע בעיתון דברי שבח למעשי טרור).

[443] ראוי לציין בהקשר זה כי הטעם לגישה האמריקנית הדיפרנציאלית איננו ברור, ונראה כי הוא נובע מהפעלת לחצים כלכליים ופוליטיים של קבוצות אינטרסים מסחריות. לדיון כללי בהשפעת גורמים אינטרסנטיים על החקיקה האמריקנית בהקשר של זכויות יוצרים, ראו: Jessica Litman, **Digital Copyright** (2001).

אל סַפַק השירות המסחרי. סמכותו של בית המשפט תוגבל להוצאת צווי מניעה בלבד.

- כל עוד לא הורה בית משפט לספק לפעול, ייהנה ספק השירות מחסינות מפני תביעות של ניזוקים.