פרטיות בעידן של שינוי

עורכת: תהילה שוורץ אלטשולר

המכון הישראלי
לדמוקרטיה

מבוא

תהילה שוורץ אלטשולר

דיון בזכות לפרטיות הוא במידה רבה כניסה אל תוך הערפל. ניתן לאתר מחלוקות כמעט בכל היבט הנוגע לאופייה של הזכות והיקף ההגנה שראוי להעניק לה, הן במישור הנורמטיבי הן במישור המושגי. יש הרואים בה תביעה ויש הרואים בה זכות, אינטרס, ערך, העדפה או מצב קיומי. הגנה על פרטיות נתפסת, לכן, בכמה וכמה דרכים: כתפיסה תיאורית, כתפיסה נורמטיבית, כתפיסה משפטית או כל השלוש יחדיו. עקרון הפרטיות כשלעצמו נובע מהשקפות עולם בדבר ממשל, זכויות אדם, יחסי פרט ומדינה ויחסי מרחב ציבורי ומרחב פרטי. אפשר להניח כי לפחות חלקית המחלוקות נובעות מכך שהדיון בזכות לפרטיות, כמו גם עיגונה החוקתי ועיגון ההסדרים המוסדיים הקשורים אליה, התפתחו מאוחר יחסית לזכויות אחרות.

גם בישראל – שבה מעוגנת הזכות לפרטיות בחוק יסוד: כבוד האדם וחירותו ובחוק הגנת הפרטיות – הזכות לפרטיות לא הוגדרה במדויק בחוק או בפסיקה. חוק הגנת הפרטיות אינו מגדיר את היקפה ובמקום זה מונה 11 מעשים שייחשבו פגיעה בפרטיות, ובכללם מעקב מטריד, האזנה אסורה על פי חוק, צילום אדם ברשות היחיד והפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם. אף שהמשפט הישראלי אימץ הגדרה רחבה של מושג הפרטיות כ"אינטרס היחיד שלא להיות מוטרד בצנעת חייו על ידי אחרים",[1] הדגיש בית המשפט כי היקפה של הזכות עמום ומשתנה בהתאם למציאות.[2]

היבט אחד של הזכות לפרטיות הוא זכותו של כל אדם לשמור ולהגן על זהותו ועל מתחם של הגנה מסביב לגופו, מחשבותיו, רגשותיו, סודותיו הכמוסים, אורח חייו ומעשיו האינטימיים. ההיבט הזה נובע מכך שפרטיות נתפסת כבעלת

1 ע"א 1211/96 **כהן נ' נשיונל קונסלטנטס**, פ"ד נב(1) 481.

2 בג"ץ 2481/93 **דיין נ' וילק** פ"ד מ"ח (2) 456.

משקל חיוני ביכולת לשמור על זהות ולגבש יחסים של אהבה, קרבה ואמון עם הסובבים וכן זהות פוליטית וציבורית. לא בכדי נתפס אובדן הפרטיות בעבר כְּאסון של חברה טוטליטרית ולא אנושית. היבט אחר קשור לכך שהזכות לפרטיות מאפשרת לאדם לבחור לאילו חלקים ומקומות במתחם הפרטי הוא נותן גישה לאחרים, וכן לשלוט באופן החשיפה, בהיקפה ובעיתויה.

וכך, בשונה ובאופן קיצוני יותר מזכויות אדם אחרות, הזכות לפרטיות היא זכות שגבולותיה, הקשריה והנורמות הנובעות מן ההגנה עליה אינם מוגדרים. ולא זו אף זו: בשנים האחרונות מגיעים המתח ואי־ההלימה בין הערכים המוכרים מן העבר לפרקטיקות של ההווה לשיאים חדשים.

במאמר פורץ דרך בנושא ההכרה בזכות לפרטיות, שהתפרסם בביטאון בית הספר למשפטים של אוניברסיטת הרוורד בשנת 1890, כתבו שני עורכי דין צעירים – לימים שופטי בית המשפט העליון האמריקני, סמואל וורן ולואיס ברנדייס – כי יזמות מודרנית והמצאות חושפות את הפרט לסבל נפשי ומצוקה.[3] הטכנולוגיה המתקדמת שאליה התכוונו כותבי המאמר הייתה מצלמות ניידות אשר אפשרו לראשונה לעיתונאים ולצלמי עיתונות לצלם אנשים ללא הסכמתם. כמאה ועשרים שנה מאוחר יותר טכנולוגיות מידע נתפסות כאיום מרכזי על פרטיות משום שהן מאפשרות העברה במהירות האור של מידע ברחבי העולם. נגישות האינטרנט, הופעתן של הרשתות החברתיות, תפוצתם של מכשירים סלולריים וריבוי מצלמות המותקנות במרחב הציבורי מביאים לשינויים של ממש במשמעות ובהיקף של הציפייה לפרטיות, ומכאן גם בהיקפה של הזכות לפרטיות. לא בכדי אמרו בהזדמנויות שונות מנכ"ל חברת גוגל ואחריו מייסד חברת פייסבוק כי הפרטיות מתה בעידן האינטרנט והרשתות החברתיות.[4] למעשה, פרטיות היא אחד מן הנושאים החברתיים הבוערים ביותר המקושרים עם טכנולוגיות תקשורת דיגיטליות.

לעקרון ההגנה על הפרטיות, כמצבור של זכויות, היבטים שונים המתקשרים עם טכנולוגיות שונות. ואכן, לא הרי מאגרי מידע בידי השלטון כהרי רשת

3 S. D. Warren & L. D. Brandeis, "The Right to Privacy", *Harvard Law Review* 4 (1890), pp. 193–220

4 www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

האינטרנט, מכשירים סלולריים ומכשירים נישאים אחרים, מאגרים ביומטריים, רשתות חברתיות, כריית מידע ועוד. אתר ויקיליקס פרסם בסוף נובמבר 2011 אוסף חדש של מסמכים שהוא מכנה "קובצי המרגלים",[5] הכולל מסמכים, מצגות, חוזים וקטלוגים של חברות המעניקות שירותי מעקב, צנזורה, ביון ואבטחה, כגון "סימנס", HP ו"נייס" הישראלית. ברוב המקרים מדובר בשירותים ובמוצרים הנמכרים ישירות לממשלות ולגופי ביון ואינם מוכרים לציבור. "נייס" הישראלית, למשל, משווקת מגוון "פתרונות מודיעין", בכללם פלטפורמה ליירוט ולניתוח כמויות גדולות מאוד של מידע תקשורתי, כגון שיחות טלפון או גלישה ברשת. לפי המסמך, מערכת זו יכולה, בין השאר, לזהות מטרות חשודות על ידי סריקת מיליארדי שיחות קול, טקסטים ומידע נוסף. בעידן של מלחמה בטרור שאחרי המתקפה על מגדלי התאומים נרכשות מערכות כאלה כעניין שבשגרה.

הציפייה הסבירה להגנה על פרטיות נוגעת בראש ובראשונה ליחסי הפרט והשלטון ולאפשרות שהשלטון יעשה שימוש לרעה בטכנולוגיות שיש להן פוטנציאל פגיעה בפרטיות. העובדה שחברות הטלפון מקיימות תרשומת של כל השיחות ושכך עושים גם המפעילים הסלולריים איננה תופעה חדשה. למעשה, רשויות המדינה משתמשות בתרשומת הזאת כאשר הן מבקשות מבתי משפט צווי חיפוש או האזנות סתר. ואולם אין מדובר עוד על מצלמות אבטחה בקניונים או על לוויינים חוצי גבולות. בעשור האחרון גופי ענק מסחריים הופכים להיות כורי מידע. בעוד מדינות מבקשות לעקוב אחר פרטים, חברות מבוססות מידע ונתונים כמו גוגל או פייסבוק קוצרות מידע על אותם פרטים ומאחסנות אותו על שרתיהן, הממוקמים לרוב בארצות הברית. אחת מן הפרקטיקות המעצימות את המתח בין הטכנולוגיה ובין הזכות לפרטיות היא איגום מידע (data ubiquity). טכניקות חדשות וזולות של איסוף, אחסון וניתוח נתונים התרחבו דרמטית בעשור האחרון. אפשר לומר – במונח השאול מן הדירקטיבה להגנת נתונים של האיחוד האירופי – שכולנו למעשה "מושאים של נתונים" (data subjects).

הסוגיה של אפליקציות מבוססות מקום, "בת הדוד" של פרסום מבוסס מידע, יכולה לשמש דוגמה מייצגת. כדי להפעיל אפליקציה מבוססת מקום (מציאת מסעדה, בית קולנוע, תחנת דלק ותחזית מזג אוויר וגם בירור של הזמן

5 http://wikileaks.org/the-spyfiles.html

המקומי) על המכשיר לדעת את מקומו של המשתמש. דבר זה נעשה בדרכים שונות, כמו טריאנגולציה ממגדלי סלולר או שימוש בשבב ג׳י־פי־אס הנמצא בתוך המכשיר. אלא שלמידע בדבר מקומו המדויק של משתמש בזמן נתון אין ערך גבוה כשלעצמו. שילוב של מידע היפר־פרטי עם מקום מאפשר להפוך אפליקציה מבוססת מקום לבעלת ערך למשתמשים ולשפר את חוויית השימוש. סוגים כאלה של מידע הם למשל התנהגות ומיקום בעבר (מהם החיפושים האחרונים ב־foursquare מן האזור? היכן חנה הרכב לאחרונה? כמה ״ציוצים״ הגיעו מן האזור?), העדפות בקניות, מצב כרטיס האשראי והתנועות האחרונות בו.

ככל שהפעילות ברשת אישית יותר וככל ששימושי הרשת נעים לכיוון שימושי אינטרנט אישיים (״Me Centered Web״),[6] כן נוספים צדדים שלישיים המבקשים להרוויח כסף באמצעות שימוש בכלים החינמיים שסופקו לנו כדי לתקשר ולחלוק מידע. חברות כמו Klout ו־PeerIndex מבקשות להוציא מן המערך המסובך של כלל הרשת החברתית מספרים פשוטים שיוצמדו לכל אחד מאתנו, אם נרצה בכך ואם לאו. המצב שבו לכל אדם יש ״מספר״ – מעין גורם השפעה (impact factor) המבטא את מידת ההשפעה שיש לו – איננו מצב בדיוני. הקושי במצב זה הוא שהמספר יקבע אם נקבל עבודה, שדרוג בחדר המלון, דוגמית של מבצע בסופרמרקט, הלוואה או כל דבר אחר.

גם אם ערכים של ״פרטיות החלטתית״ – במובן של החירות להחליט בעניינים שבצנעת הפרט, כגון נטייה מינית או הזכות לבצע הפלה, ובמובן של פרטיות מקומית (כלומר, הפעלת השליטה במרחב פרטי פיזי כמו בית או חצר) – נראים מוגנים ומוסכמים יחסית, כאשר מדובר בפרטיות המידע – העניינים נעשים מסובכים יותר.

זאת ועוד: טכנולוגיות של כריית מידע מציבות סימן שאלה על עצם ההבחנה בין פרטי לציבורי. מצד אחד – מיזמים ואפליקציות פרטיים ניזונים ממידע ציבורי ומתוצרים של איסוף מידע על ידי השלטון, ומצד אחר – רשויות ציבוריות משתמשות במידע שנכרה על ידי חברות פרטיות (למשל במעקב אחר

6 http://scholarlykitchen.sspnet.org/2010/10/26/rethinking-our-architecture-the-power-of-me-vs-the-arrogance-of-we

תכתובת דואר אלקטרוני של פרטים). יתרה מזו, באופן פרדוקסלי הציבור הרחב נשען על ההנחה שהמדינה היא שתגן עליו מפני ניצול לרעה של המידע הפרטי, כאשר טכנולוגיות נעשות זולות או שנעשה בהן שימוש תכוף על ידי חברות מסחריות. בו בזמן הוא נשען על חברות פרטיות וארגוני "כלבי שמירה" חוץ־שלטוניים כדי שיגנו עליו מפגיעתה של המדינה.

שאלה מטרידה היא עד כמה הגנת הפרטיות מפגרת לעומת מערכות איסוף המידע והטכנולוגיות המשמשות למעקב אחר גולשים לצורך ניתוחן והפקת רווח משני מהן. בניסיון להתמודד עם סופת פגיעה בפרטיות מתוזמרת היטב – לא מצד המדינה אלא מצד חברות מסחריות – נציבי הגנת פרטיות באירופה ובישראל מנסים לאכוף חוקי הגנת מידע שנחקקו ועוצבו בעידן אחר, קודם שגוגל ופייסבוק נולדו. אבל אימוץ טכנולוגיות חדשות מחייב את הרגולטורים והמחוקקים לשחק עמן משחקי חתול ועכבר. החקיקה ברוב מדינות המערב איננה מצוידת בכלים הנדרשים להתמודדות עם ההקשר הבינלאומי של אחסון וקצירה של מידע, והדבר משפיע לרעה על יעילות ההתמודדות האירופית או הישראלית עם חברות שמקום מושבן בארצות הברית.

ככלל, לא מפליא שההיסטוריה של החקיקה הנוגעת לפרטיות נושאת אופי תגובתי. דוגמאות מן העולם יש למכביר: כללים הנוגעים למסירת היסטוריה של אשראי בשנות השבעים, שאילת סרטים במחשבי ספריות וידאו בשנות השמונים, רישומים רפואיים בשנות התשעים ותנאי שימוש המאפשרים לחברות אינטרנט למסור פרטים לחברות לא מקוונות בתחילת שנות האלפיים. נדמה שניתן לאפיין דפוס התנהלות: חוקר, מומחה או האקר מגלה שלשירות או למוצר שיש לו תפוצה רחבה מאוד יש פרצה באבטחה או רכיב המאפשר פגיעה בפרטיות של משתמשים. הקביעה מאושררת בידי מומחי רשת נוספים. נציגי החברה משתמשים באסטרטגיה שיווקית מדורגת שראשיתה בהכחשה גורפת, המשכה בהסבר וסופה בהתנצלות ובהצהרה שהתקלה תתוקן והפגיעה תוסר. לבסוף מגיעה תגובה פוליטית־רגולטורית־משפטית: פנייה שלטונית אל החברות לקבלת הבהרות, שימועים בבתי נבחרים וברשויות רגולטוריות אחרות, חוות דעת והחלטות מדיניות שבחלקן צופות פני עבר, הצעות לתיקוני חקיקה והגשת תביעות ייצוגיות.

כך היה כאשר התברר בתחילת 2011 כי חברת אפל מסוגלת לעקוב אחר התנועות בַּמקום של משתמשי מכשירים סלולריים שהיא משווקת, ואף מבצעת מעקב כזה הלכה למעשה בשיטה לא מוצפנת;[7] כך היה גם בעניין חברת טום טום (TomTom) לאחר שהתברר כי היא מוכרת למשטרת גרמניה מידע שאספה באמצעות מכשירי הג׳י־פי־אס שהיא מייצרת[8] לצורך מעקב אחר עברייני תנועה.

התגובה הרגולטורית של רשות המסחר האמריקנית (Federal Trade Commission) לשימוש בטכניקות של איסוף וכריית מידע ברשת פורסמה באמצע 2011 בחוות דעת שקבעה אם מדובר בהפרה בוטה של פרטיות המשתמשים. חוות הדעת כללה המלצות לשליטה טובה יותר של המשתמשים במידע הנוגע להתנהגות הדיגיטלית שלהם וחייבה לשלב ״עוגיית פרטיות״ שתאפשר לגולש להפעיל מכניזם של ״אל תעקוב אחריי״. המכניזם הזה אמור למסור לחברות שעושות כריית מידע את העדפות הפרטיות של המשתמש.

ואולם הפָּרָשות מתרבות, ודומה שהן נעשות חמורות יותר ויותר. בתחילת דצמבר 2011 גילה חוקר אבטחה אמריקני תוכנת מעקב בשם Carrier IQ המותקנת ב־140 מיליון טלפונים חכמים בעולם. התוכנה עוקבת כמעט אחר כל פעולה, צליל והקלדה, מעתיקה אותם ומעבירה אותם בחזרה אל חברות התקשורת. לא מדובר רק במקומו הפיזי של המכשיר אלא גם בתכנים המועברים באמצעותו. בפעילות הזאת מעורבות כמעט כל היצרניות הגדולות של מכשירים מן הסוג הזה בעולם, כגון סמסונג, נוקיה, מוטורולה ואפל.[9] לאחר ההכחשות מצד המעורבים בדבר התגלתה טקטיקה הסברתית חדשה: האפליקציה משמשת כבקרה על ביצועי המכשיר ולא לצורכי מעקב. קשה להכחיש שתוכנה כזאת מהווה שער גישה ל״תיבת אוצר״ של מידע אישי על הרגלי הגולשים ותנועותיהם. מצד שני, כאשר הטכנולוגיה מתקדמת לכיוון שבו המכשיר עצמו הוא ״שביל

7 www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears

8 www.guardian.co.uk/technology/2011/apr/28/tomtom-satnav-data-police-speed-traps

9 ע׳ כביר וה׳ עילם, ״כל המידע מוקלט ונשמר: שערוריות המעקב של עולם הטכנולוגיה״, **ynet, כלכליסט**, 4.12.11:
www.calcalist.co.il/internet/articles/0,7340,L-3554064,00.html

פירורי הלחם" עבור מבצעי המעקב, ולא תוכנה כזאת או אחרת, אזי מתברר שלא מדובר בבעיה שניתנת לפתרון בשיטה המוצעת של opting out[10] שהציעה רשות המסחר האמריקנית. אפשר להניח כי ביום שבו יפורסם דוח נוסף, יהיה צורך להתמודד עם היבטים חדשים של העניין.

הלן ניסנבאום טוענת בספרה **פרטיות בהקשר** (*Privacy in Context*)[11] שאנשים אינם חפצים בהגבלה על שצף המידע אלא רק בהבטחה שהמידע זורם כראוי, בדרך שהיא מכנה "יושרה הֶקשרית" (contextual integrity). לטענתה, הזכות לפרטיות איננה הזכות לשלוט במידע אישי וגם לא הזכות להגביל גישה למידע הזה. הזכות לפרטיות, לדעתה, היא הזכות לחיות בעולם שבו מכבדים את הציפיות שלנו ביחס למידע האישי שלנו ונענים להן. ציפיות אלה מתעצבות לא רק מכוח ההרגל, אלא גם מכוח האמון בתמיכה ובהכרה שעקרונות חברתיים ופוליטיים מעניקים להן. השקפתה של ניסנבאום "מתכתבת" ללא ספק עם מה שבתי משפט, בארצות הברית בעיקר, רואים כ"ציפייה סבירה לפרטיות". ממש כפי שציפייה סבירה כדוקטרינה משפטית בהקשרים אחרים נקבעת, לפחות בחלקה, בהתאם למציאות, כך קשה לטעון כי מעשה כלשהו היה הפרה של ציפייה סבירה אם הפרקטיקה היא פרקטיקה חברתית מקובלת. וכך גם כאשר בנושאי טכנולוגיה ופרטיות עסקינן. השאלה הפתוחה היא, לכן, כפולה: ראשית, באיזו נקודה אפשר לומר שהחברה אימצה טכנולוגיה חדשה ברמה שאיננה מאפשרת עוד לטעון לציפייה סבירה כנגד שימוש באותה טכנולוגיה? שנית, האם נכון ומוצדק – כעניין נורמטיבי – לוותר במקרים מסוימים על הציפייה הסבירה לפרטיות המידע האישי?

פיטר פליישר, לשעבר הממונה בחברת גוגל על פרטיות בינלאומית, כתב כי הדרישה לפרטיות היא "השחור החדש באופנת הצנזורה" וכי הדרישה הזאת מנוגדת לעקרון חופש הביטוי. לטענתו, יש להפנים את העובדה שאין בנמצא פרטיות ושמי שמחפש פרטיות, כנראה יש לו מה להסתיר.[12] קשה להתעלם מכך

10 כלומר, המערכת תקפה אבל מאפשרים להוציא ממנה חריגים.

11 H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010)

12 http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html

שהתמיכה של חברות כמו גוגל בחופש הביטוי בהקשר זה נובעת מן המודל הכלכלי שלהן. מטפורית אפשר לטעון כי הזכות לחופש ביטוי היא השחור החדש באופנת כריית המידע. לפיכך דומה שהשאלה המרכזית היא שאלה של רווח והפסד בנוגע לאיסוף מידע: האם אנו מוכנים לקבל את היתרונות של שירותים מבוססי מקום על חשבון פרטיותנו שלנו? האם אנו מעוניינים להשאיר מרחב שבו פעולותינו אינן נמדדות או שאנו מעדיפים את היתרונות שיש במדידה ובמעקב אחר כל פעולה ובשילוב של סוגי מידע? (למשל, האם ההתעמלות שעשיתי שוות ערך לקלוריות שצרכתי; האם בתי חלתה פעמים רבות מדי החורף; האם אני מוציאה יותר כסף על נעליים לעומת אחרים בעלי משכורת דומה?)

שאלה מטרידה לא פחות היא אם אפשר בכלל לדבר על רווח והפסד במישור הנורמטיבי שעה שבפועל התהליך נראה ככזה שאיננו ניתן לעצירה ואשר במסגרתו אנו מסייעים לקדם בכיוון אחד בלבד את הטכנולוגיה, את הכלים העומדים לרשותנו ואת הציפיות החברתיות. אפשר שההיסטוריה תשפוט – בייחוד אם אלה שנמצאים מתחת לפער החברתי־טכנולוגי (כלומר אלה שגילם פחות מ־40) יפגינו אדישות כלפי סוגיות של פרטיות. בה בעת אפשר שלחץ ציבורי מספיק יצליח להביא לכך שסוגיות של פרטיות במדיה המקוונת ומחוצה לה יהיו נושא לקמפיינים ציבוריים ענקיים. איש אינו אוהב את הרעיון של "אח גדול", ויש להניח כי חברות ענק כמו גוגל, אפל ומייקרוסופט יהפכו למטרה קלה בשל עוצמתן.

ספר זה הוא תוצר של תהליך עבודה שנמשך שנים אחדות. שניים מן המאמרים בו הם פרי מחקר שנערך בתוך המכון הישראלי לדמוקרטיה, ושלושה נוספים התקבלו לאחר שפרסמנו "קול קורא" לספר בנושא פרטיות ועיתונאות. יותר מכול האסופה מבטאת את הפנים הרבות של הזכות לפרטיות ואת תקופת המעבר שזכות זו שרויה בה – מתקשורת מסורתית לתקשורת חדשה; מפרקטיקות אתיות ומשפטיות שתכליתן לפגוע בפרטיות בתוך מסרים של "אחד להמון" (one to many) בטלוויזיה לפרקטיקות של התמודדות עם הפגיעה בפרטיות של האחד בתוך ההמון.

בשל תחושה חזקה שסדנא דארעא חד הוא ואין חדש תחת השמש, חוזרים מחוקקים נבוכים בתחילת המאה העשרים ואחת למושכלות ראשונים של הגנת הפרטיות מתחילת המאה העשרים. מאמרו של **ראם שגב** עוסק במושכלות אלה

בהקשר של מושג הפרטיות. מתוך תפיסה מורכבת ורב־משמעית של המושג בוחן שגב אם ראוי להגדיר פרטיות כמצב של בידוד, למשל מצב שבו מידע על אדם אינו ידוע לאנשים אחרים, או כרמת השליטה של אדם על המידה שבה הוא מבודד מאנשים אחרים, למשל המידה שבה מידע על אודותיו ידוע לאחרים. שגב מתמודד גם עם השאלה אם יש לדבוק בתפיסה אחידה של פרטיות או בתפיסות שונות התלויות במאפיינים אישיים של אנשים או במסגרת התרבותית שבה אנשים חיים. הוא גם בוחן בחינה ביקורתית את מה שנתפס כהנחת יסוד של בתי המשפט בישראל ובמדינות אחרות שלפיה הפרטיות מסתיימת היכן שמתחיל ה"ויתור" עליה – החל ביציאה למקום ציבורי וכלה במילוי תפקיד ציבורי.

במישור ההגנה המשפטית על הזכות שגב מנסה להתוות מרחב של שיקולים בעד ונגד הגנה משפטית על פרטיות על מנת לאפשר הכרעה בינם ובין אינטרסים או ערכים אחרים (כאשר יש כאלה), ובייחוד הזכות לחופש ביטוי. הוא בוחן שיקולים כגון רווחה ואוטונומיה אישית, חשיבה עצמאית, רצונם של אנשים בקיומו של תחום פרטי ומידע שאינם חשופים לאחרים, נהגים ומוסכמות חברתיים המקובלים בחברה, בריאות נפשית והגנה על רגשות. מנגד הוא רואה שיקולים כגון הסתרת מידע כצביעות ופרטיות כמשקפת ניכור חברתי והיעדר אלטרואיזם; מאבחן את ההבחנה בין תחום "פרטי" לתחום "פומבי" או "ציבורי" כבסיס להסתרה ולדיכוי של נשים; ומסב את תשומת הלב להחצנות החברתיות השליליות של חסרונו של מידע פרטי בתהליכי קבלת החלטות. חיסרון זה עלול לפגוע באיכותן של ההחלטות המתקבלות.

נקודת המוצא של מאמרם של **עמית לביא־דינור ויובל קרניאל**, העוסק בזכות לפרטיות בתכניות מציאות, היא ששידורי הטלוויזיה ממלאים תפקיד כפול – של שחקן ושל סוכן חברות. תכניות המציאות חודרות לפרטיות של אדם זה או אחר אבל גם מעבירות מסר חברתי ותרבותי חשוב בנוגע ליחס המקובל והראוי בין המרחב הפרטי למרחב הציבורי. בכך הן משקפות ומעצבות את מושגי הפרטיות המשתנים. לביא־דינור וקרניאל מזהים מגמה של שינוי במושג הפרטיות בשידורי הטלוויזיה המתבטאת לא רק בפגיעה בפרט זה או אחר הנחשף בשידורים, אלא גם בפיחות עמוק במשמעות ערך הפרטיות ובמשקלו. אובדן הפרטיות בתכניות המציאות הוא לדידם החפצה של האדם המופיע בתכנית, הפשטתו מכל ערך וייחוד ופגיעה בכבודו. יתרה מזו, הם טוענים כי הצפייה

בתכניות מציאות כצפייה ב"אנשים רגילים", ולא כשחקנים, מגבירה את רמת ההזדהות של הצופים, בבחינת "אנשים פרטיים ורגילים הם אנחנו". לכן כאשר מתחוללת חדירה לפרטיותם של המשתתפים, מתרחשת גם פלישה לפרטיותם של הצופים מעבר להסכמה הנורמטיבית המקובלת.

בנימין שמואלי מציף במאמרו היבט אחר של הזכות לפרטיות, המחדד את משמעות ההפרדה בין הפרטי ובין הציבורי, בין האדם ובין המקום. שמואלי עושה זאת באמצעות דיון בשני מקרים שהגיעו לערכאות שעניינם פרסום תצלומו של אדם שצולם ברשות הרבים באמצעי התקשורת. מקרה אחד הוא פרסום תצלומים מכלאו השמור של יגאל עמיר, רוצחו של ראש הממשלה יצחק רבין, בעקבות בקשה לצו מניעה נגד שידור טלוויזיוני של צילומים מתא הכלא שלו מכוח הטענה שתא כלא הוא רשות היחיד, ולחלופין משום שמדובר ברשות הרבים אך התמונות משפילות ופרסומן אינו מתאים לאדם דתי. המקרה האחר הוא אדם חרדי אשר חילק תשמישי קדושה בדוכן ברחוב, צולם כשמאחוריו כרזה פרובוקטיבית של אישה חשופה, ולאחר שהתמונה פורסמה בעיתון תבע פיצויים בגין הפרת פרטיותו.

שמואלי מתעכב על סעיף 2(6) לחוק הגנת הפרטיות, הרואה בפרסום לשם כוונת רווח הפרת הפרטיות ומייצג מתח אינהרנטי בין הגנת הפרטיות לבין פעילותם של אמצעי התקשורת ההמונית המסחרית. שמואלי מציע להחליף את הסעיף, אשר רוקן מתוכן על ידי בתי המשפט בשני פסקי דין, במבחן של דומיננטיות. בהתאם למבחן זה עצם הצגת תמונה או מיצג אודיו־ויזואלי באמצעי תקשורת מסחרי יוצר חזקה שמדובר בשידור למטרת רווח, שהוא עוולה לפי סעיף 2(6) לחוק. עול הוכחת העניין הציבורי והפרכת החזקה צריכים ליפול, לדידו של שמואלי, על אמצעי התקשורת. כן הוא מציע לאמץ גישה דה־קונסטרוקטיבית כלפי תכנים ולבחון הן את הפגיעה בפרטיות הן את העניין הציבורי בה לא רק לפי מבחן "הכתבה בכללותה" אלא גם לפי חלקים מתוכה. לפיכך סבור שמואלי כי במקרים של דיון בבקשות לצווי מניעה יש לאפשר פרסום תכנים חלקי, כגון השחרת פנים או טשטוש התמונה, שיגנו על הזכות לפרסם ובד בבד ימנעו פגיעת יתר בזכות לפרטיות.

הקובץ נחתם במבט אל התקשורת החדשה. **יאיר עמיחי־המבורגר ואורן פרז** טוענים כי התפיסה המשפטית הקיימת של הזכות לפרטיות אינה תואמת את המציאות הדיגיטלית וכי האינטרנט יצר קונפליקט ביחס לרעיון הפרטיות. מחד

גיסא, ראשיתה של הפעילות המקוונת נכרכה במושג האנונימיות. האנונימיות מזוהה עם רעיון הפרטיות הואיל ואי־היכולת לזהות את פרטיו של הגולש מונעת מעקב וחדירה למתחם האישי שלו. מאידך גיסא, יכולתו של הפרט לממש את האוטונומיה שלו במרחב האינטרנטי תלויה, בהקשרים רבים, בוויתור על פרטיות. במובן זה העיקרון של כיבוד האוטונומיה של הפרט מחייב דווקא גמישות בתחימת גבולותיה של הזכות לפרטיות. הגנה דווקנית מדי על הזכות לפרטיות יכולה לפגוע ביכולת של הפרט לממש את האוטונומיה שלו.

עמיחי־המבורגר ופרז מצביעים על פער בין הניסיון להגדיר את הזכות לפרטיות והזכות לאנונימיות במושגים אבסולוטיים ובין עולם הצרכים וההעדפות של משתמשי האינטרנט. לדעתם, דפוסי ההתנהגות באינטרנט מצביעים על האפשרות שאנשים אינם תובעים או מצפים שהאינטרנט יעניק להם אנונימיות ופרטיות מוחלטת, ולכן פתרון אבסולוטי שיעדיף פן מסוים של הקונפליקט מתוך תפיסה היירכית של זכויות וערכים (למשל, האוטונומיה של הפרט או הסדר הציבורי) יפגע בערכים ובאינטרסים אחרים. נוסף על כך הם מצביעים על מוגבלות המשפט במתן מענה לסוגיית הפרטיות בשל טיעונים טכניים כמו האופי הגלובלי של הרשת וחוסר יכולתה של מערכת המשפט להסתגל לשינויים ובגלל טיעונים מהותיים שבמרכזם הנטייה המשפטית להשתמש במתווים דיכוטומיים על מנת להגן על זכויות. נטייה זו, בהקשר הנידון, מתעלמת מהעובדה שהמרחב האינטרנטי יוצר קונפליקט פנימי במונחים של ערך האוטונומיה: בהיבטים מסוימים ויתור כלשהו על הפרטיות (והאנונימיות) בשימוש באינטרנט יכול לאפשר הגשמה מלאה יותר של האוטונומיה של הפרט, ואילו בהיבטים אחרים מימוש האוטונומיה מחייב דווקא שמירה על הפרטיות באמצעות הבטחת האנונימיות של המשתמש. כמו כן, התפיסה החוקתית של הזכות לפרטיות – שמעמידה את המדינה כשחקן מפתח במשחק ההגנה על פרטיות הן כמי שאמון על ביצור רעיון הפרטיות והן כאויב הגדול שלה – מתעלמת מהמשקל הגדול של שחקנים פרטיים ברשת.

עמיחי־המבורגר ופרז אינם מתעלמים מפתרונות טכנולוגיים אפשריים אלא עומדים על הקשיים שיש בהם, כמו הפער בין האינטרס העסקי לאינטרס של הגולשים ושל החברה בכלל וחוסר המודעות של הגולשים, המכונה "כשל קוגניטיבי", לפתרונות אלה.

עמיר פוקס דן בשלושה שימושים שעושים גורמי הטרור באינטרנט: הראשון, שימוש ברשת כאמצעי תקשורת המונים לשם תעמולה והפצת מידע; השני, שימוש אינסטרומנטלי לצורכי תקשורת בין פעילים ובין גופים בארגון, איסוף מודיעין וגיוס פעילים וכספים; והשלישי, שימוש ישיר, כלומר טרור באמצעות הרשת (cyber terrorism). שימושים אלה חופפים במידה רבה לנגיעה שיש היום לרשת בכל תחומי החיים בעולם האזרחי, המסחרי, הממשלי והצבאי, ומקורם בכך שהמבנה של ארגון הטרור המודרני מתאפיין באופי בין־מדינתי ורב־מדינתי, נזיל ולא היררכי (כלומר, מכיל תאים רבים המפוזרים בכמה מדינות), כדי למזער את סיכוני החשיפה. שימושים אלה מציבים אתגר של ממש לשירותי המודיעין, הנדרשים להתמודד חזיתית עם אתרי האינטרנט של ארגוני הטרור, ובעיקר לאסוף מודיעין באמצעות יירוט המסרים הנשלחים באינטרנט ופענוחם.

פוקס מבקש לקרוא לחשיבה מחודשת על נקודת האיזון בין הזכות לפרטיות לבין צורכי הביטחון, ככל שמדובר במניעת מעשי טרור. קונקרטית הוא קורא לעצב מחדש את כללי האזנת הסתר הקיימים, ובייחוד את הדרישה שכל צו האזנה יהיה ספציפי, לגבי אדם מסוים או לגבי נקודת קצה, כלומר מספר טלפון או דוא"ל מסוימים. לטענתו, האיזון הקיים מבוסס על כך שכדי להאזין יש צורך באדם שיקשיב לשיחות או יקרא התכתבויות ויברור את החומר החשוד. הרציונל העומד מאחורי הכללים הקיימים, המאפשרים האזנה לקווים ספציפיים, הוא לפיכך הגבלת הרשויות מפני האזנות רחבות מדי שעלולות לגרום פגיעה בפרטיות.

מערכות יעילות לסינון תוכן המסוגלות לאתר תוכן חשוד בהתאם למשוואות המגדירות תוכן כזה מציבות אתגר לפני החקיקה הקיימת – גם משום שהחקיקה אוסרת למעשה את הפעלתן וגם משום שהן מחייבות שינוי לעומת הפרדיגמה המסורתית המוכרת מעידן הטלפוניה. באינטרנט, טוען פוקס, ניתן לעצב כלל איזון חדש שאינו מגביל את רשויות האכיפה לפי יחידת הקצה דווקא (כתובת הדואר האלקטרוני), אלא מאפשר לה "עוגנים" אחרים – לפי תוכן או לפי זיהוי המשתמש בדרך אחרת.

למעשה, על מנת למזער ככל האפשר את הפגיעה בזכות לפרטיות על ידי שימוש בסינון על פי תוכן באמצעות "תוכנות רחרחניות" פוקס מציע להתנות את השימוש בחשיפה למספר קטן של אנשים, בהידוק הפיקוח על מניעת זליגה של מידע ובהגבלת השימוש לצורכי ביטחון ולא למטרות מלחמה בפשיעה

"רגילה". הוא מדגיש גם את נחיצותו של דיון ציבורי על תיקון חוק האזנת סתר או חקיקה ייעודית לשימוש בתוכנות רחרחניות.

היבט נוסף שפוקס מתייחס אליו הוא הצורך ליידע את האוכלוסייה בדבר קיומה של מערכת קוראת תעבורה באינטרנט. אפשר שהמלצה זו היא נקודת משען ראויה לחשיבה צופה פני עתיד. כעניין של הסתכלות אמפירית, לפרט יש פחות ופחות שליטה על המידע האישי שלו. אלא שבאופן פרדוקסלי אנו היצרנים המרכזיים של מידע על עצמנו ואנו מוסרים עוד ועוד מידע כל הזמן, בעצם מרצון. מסירת המידע נעשית, יש להניח, בניסיון לייצר הֶקשרים שיסייעו לנו להתגבר על כמויות המידע המציפות אותנו מכל עבר. יש להודות כי גופים ציבוריים ופרטיים כאחד נסמכים על כך שאיננו מפעילים שליטה על המידע שלנו או איננו מודעים לכמות המידע המוחזק עלינו בידי אחרים.

אלא שלא את כל המידע עלינו ברשת אנחנו נותנים במודע, ולכן גם מרצון. אנשים רבים אינם מודעים לכך שכל פעולה שלהם במרחב המקוון מותירה אחריה טביעות אצבע דיגיטליות, "שביל פירורי לחם" או "שובל דיגיטלי". הם סבורים שמדובר ביחסים אינטימיים שלהם עם ה"מכונה", כלומר עם רשת פרטית וסגורה. לכן גדלה הנכונות לחלוק ללא התנגדות מידע. אפשר לומר שהא־סימטרייה במודעות היא בעיית המפתח. בעוד חברות ענק וממשלות צוברות כמויות עצומות של מידע, הציבור הרחב, זה שממנו נכרה מידע זה, נמצא במצב שאין מיידעים אותו והוא אינו מבין היכן נמצא המידע הזה ומדוע הוא שם. הא־סימטרייה הזאת היא מקור לחוסר צדק, ולא פחות מזה – לחרדה מוצדקת אצל פרטים.

מדיניות ברורה לקידום רמת השליטה של פרטים במידע אישי שקשור אליהם היא הכרחית, ויש להבטיח כי "מחזיקי המידע" יְיַדעו את "מושאי המידע" לגבי מידע שיש להם עליהם. במצב אידאלי על מדיניות כזאת להתבצע על בסיס בינלאומי מתוך שמירה על ארבעה כללים: (1) הבטחה שהאזרח יוכל לגשת בחופשיות למידע שהוא מושאו; (2) הקטנת מספר ה"חריגים" על בסיס ביטחון לאומי; (3) הרחבת המחויבויות והכללים החלים על גופים המחזיקים במידע פרטי גם כלפי גופים וחברות פרטיות; (4) הפעלת מנגנונים בינלאומיים לביקורת ויישוב סכסוכים.

אפשר שככל שהדברים אמורים בכריית מידע על ידי חברות פרטיות, אמצעי משלים הוא רגולציה עצמית המקדמת שקיפות ומעורבות של גולשים בעיצוב פרופיל הפרטיות שלהם. סנוניות ראשונות בהקשר זה הן יוזמת קואליציית

הפרסום הדיגיטלי המציעה "אייקון פרסום" – סמליל שַיראה שהאתר אוסף נתונים ויאפשר באמצעות הקלקה לסרב לכריית מידע.[13]

אמצעי חיוני משלים לכל מעורבות רגולטורית הוא קידום אוריינות דיגיטלית בקרב משתמשי הרשת, ולמעשה בקרב כלל אוכלוסיית המאה העשרים ואחת. מדובר בפיתוח מיומנויות נרכשות – טכניות וקוגניטיביות – שיקדמו קשרי גומלין של הפרט עם המרחב הדיגיטלי. אוריינות השתתפות בעידן המידע היא אגד המיומנויות של עצם המודעות ליכולת לדרוש מידע; ההבנה כיצד מידע נאסף, מובנה, מאוחסן ומיוצג על ידי השלטון והתאגידים המסחריים; והיכולת לתבוע שליטה ומעורבות בכל אלה. קונקרטית מדובר ברעיון שגם אם אדם הוא בן בית במרחב הדיגיטלי, אין פירוש הדבר שהכרח הוא שכל היבט בחייו יהיה כספר מקוון (e-book) פתוח לפני הציבור ושלכולם תהיה גישה למה שהוא אומר, עושה, מקליד, מסמס, מצלם, מציין, מעדכן, קונה, מוכר, שואל, גונב, אוכל, שותה, לובש, היכן הוא ובחברת מי. מדובר בהבנה שכל פעילות במרחב המקוון מותירה שובל דיגיטלי, שניתן לנצל אותו לצרכים חיוביים ושליליים כאחד; במודעות לאפשרות שלא להסכים לכל חלונית השואלת אם הגולש רוצה שהמידע יהיה זמין לטובת האפליקציה שהוא מבקש להוריד; בצורך בסיסמאות חזקות להגנת המחשב והטלפון הסלולרי החכמים; בהטמעת הרעיון ששימוש חינם בפלטפורמות שונות אינו הופך את המשתמש ללקוח. במקום זה המשתמש האורייני מבין שהוא המוצר עצמו. אפשר שהצורך הדוחק ביותר הוא לוודא שנבחרי הציבור אינם בורים דיגיטליים (digital ignorants) הדיגיטלית שלהם מספיקה ברמה המאפשרת להם לעמוד בראש החץ של ההתמודדות עם אתגרי הפרטיות שהחברה המערבית נקראת להתמודד עמם.

תודה לפרופ׳ מרדכי קרמניצר שליווה את הקובץ מראשיתו, לכותבי המאמרים שתרמו מזמנם ומכישרונם, לעורכי הטקסט המסורים ולאנשי מחלקת ההוצאה לאור של המכון הישראלי לדמוקרטיה.

ירושלים, יולי 2012

13 www.evidon.com/privacy_center.html#forward_i

טרור ופרטיות
הצעה לחשיבה מחודשת על הכלים להתמודדות עם פעילות טרור באינטרנט

עמיר פוקס

1. מבוא

היום, בעיצומה של מהפכת המידע, כמעט כל פעולה שאנו עושים מותירה אחריה עקבות דיגיטליים המאפשרים לתעד את חיינו. כרטיסי אשראי, גלישה באינטרנט, שימוש בטלפון נייד וכרטיסי מועדון לקוחות – שקשה אם לא בלתי אפשרי להתנהל בלעדיהם בעולם המודרני – מאפשרים ללמוד על העדפותינו, לשמור זאת במאגרי מידע עצומים ולהצליב את המידע עם מידע קיים או חדש. כך ניתן ליצור עלינו פרופיל מפורט, ללא ידיעתנו ובלי שנדרשנו לתת לכך את הסכמתנו.[1]

מקור מרכזי להשגת מידע עלינו הוא רשת האינטרנט, שהשימוש בה הפך בשנים האחרונות לחלק משגרת חייהם של יותר ממיליארד בני אדם ברחבי העולם. האפשרויות האינסופיות שמציעה הרשת, נוחות השימוש בה, עלותה הנמוכה, היותה אינטראקטיבית, שוויונית, בינלאומית ואנונימית – כל אלה סייעו להפיכתה לסוג תקשורת ייחודי ואטרקטיבי. בצד יתרונותיה של הרשת, יש לה גם חסרונות: היא מאפשרת לאנשים להסתיר את זהותם ומספקת במה נוחה למבקשים לבצע עבֵרות פליליות ולתכנן פעולות טרור או לעשות כל מעשה בלתי חוקי אחר. מעטים הופתעו כאשר לאחר הפיגוע במגדלי התאומים, בספטמבר 2001, התברר שארגון אל־קאעדה השתמש ברשת לצורך תכנון הפיגוע.

1 D. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy", *Stanford Law Review* 53 (2001), p. 1394

שירותי הביטחון ברחבי העולם הבינו את הצורך להשתמש ברשת האינטרנט כדי להתחקות אחר גורמים כאלה ולמנוע מהם לבצע את מעשיהם. במהרה התברר להם היתרונות העצומים הגלומים בטכנולוגיות המידע החדשות, דבר שהוביל לשינוי שיטות העבודה. למשל, חלק ניכר מהמידע שנאסף בעבר באמצעות מודיעין אנושי – כולל מרגלים, משתפי פעולה וחקירת חשודים – אפשר לאסוף היום באמצעים אלקטרוניים. החוקרים יכולים להישאר במשרדם ובאמצעות מערכות מחשב מתוחכמות ותוכנות חדישות לאסוף חומר מודיעיני רב מרחבי העולם, בהשקעה נמוכה של משאבים וכוח אדם.

איסוף המידע המודיעיני ברשת עשוי להיות בעייתי מנקודת הראות של זכויות האדם. להבדיל מחקירה פלילית ומאיסוף המידע הנחוץ לה, המידע המודיעיני נוגע לא פעם לאנשים שאינם חשודים בדבר ושמעולם לא הורשעו בעֲבֵרה על החוק. המידע נאסף בהנחה שהוא עשוי לשמש בעתיד למניעת עבֵרות, אף על פי שאין כל ודאות בכך. איסופו כרוך בדרך כלל בפלישה לחיי הפרט לאורך תקופה ממושכת. הטכנולוגיות החדישות העומדות היום לרשות שירותי הביטחון מחמירות את סכנת הפגיעה בזכויות האדם, ובעיקר את סכנת הפגיעה בזכות לפרטיות. זאת, בין השאר, בשל הגישה הקלה שהן מספקות לכמויות אדירות של מידע ובשל היכולת לשמור מידע זה לתקופות ממושכות. נוסף על כך, איסוף מידע דרך רשת האינטרנט נעשה באמצעות סריקה של כל ההודעות והמסרים העוברים בה, ולכן על מנת לאתר הודעת דואר אלקטרוני בעלת מידע מודיעיני חיוני, יש צורך בסריקה של אלפי הודעות אחרות של אנשים תמימים שהמידע בנוגע אליהם אינו נחוץ לשירותי הביטחון.[2] מציאות זו, המאפשרת פלישה לחייהם של מיליוני אזרחים תוך פגיעה בפרטיותם, מעלה את הצורך לדון בסמכויות המוענקות לשירותי הביטחון לשימוש בטכנולוגיות אלה. האם בשל הסכנות הביטחוניות שאתן הם נאלצים להתמודד, יש לתת להם יד חופשית בניצול הטכנולוגיות, או שיש להטיל עליהם הגבלות חמורות כדי להבטיח את השמירה על זכויות האדם?

השאלה הנידונה במאמר זה היא שאלת האיזון הראוי בין צורכי הביטחון של המדינה לבין החובה להגן על הזכות לפרטיות של אזרחיה ותושביה. למרות טשטוש הגבולות הפיזיים בעולם האינטרנט, מאמר זה אינו עוסק בשאלות

2 L. Tien, "Privacy, Technology and Data Mining", *Ohio Northern University Law Review* 30 (2004), pp. 391–392

נוספות הקשורות לפעולות של שירותי הביטחון, כמו איסוף מידע מחוץ לגבולות המדינה או מידע הנוגע לאזרחים זרים בשטחה.

יש לציין ששאלת פרטיותם של גולשי רשת האינטרנט נחשבת לתחום חדש יחסית, שטרם הוסדר בצורה כוללת על ידי החקיקה והפסיקה, ועל כן קיימת סכנה שרשויות הביטחון ינצלו את המצב לרעה וייפגע אינטרס הפרטיות של האזרחים. השאלה שאבקש להתמקד בה היא: האם התמודדות מול הטרור באמצעות רשת האינטרנט (להלן "הרשת") מעלה נימוק חדש ובעל משקל שביכולתו להסיט את נוסחאות האיזון שהיו מקובלות עד לעשור הנוכחי (טרם הופעת הרשת כאמצעי תקשורת נפוץ וזמין) בין הזכות לפרטיות לבין ההגנה על ביטחון אזרחי המדינה?

הביקורת על חדירת רשויות הביטחון לפרטיות הגולשים ברשת מתבססת, במידה רבה, על ניתוח התפיסות ארוכות הימים של איזון בין הזכות לפרטיות לבין ההגנה על ביטחון המדינה, כפי שבאו לידי ביטוי בכללי האזנת הסתר לשיחות טלפון, וכן במידה פחותה, בכללי החיפוש בבתים ובחצרות. לפי כללים אלה אין לסרוק מידע (שיחות טלפון, תכתובות דואר אלקטרוני), לבחון אותו ולפקח עליו ללא חשד ספציפי מוקדם, והדרך היחידה להאזין לשיחות טלפון או לעקוב אחרי תכתובות דואר אלקטרוני היא בעקבות חשד ספציפי כלפי אדם, מכשיר טלפון או כתובת דואר אלקטרוני. השאלה העיקרית היא אם איזון זה, שמקורו בכללים המסורתיים, רלוונטי גם בעידן הטרור באינטרנט, או שמא נכנסו למשוואה משתנים שמחייבים שקילה מחודשת. בבחינת השאלה יש להביא בחשבון כמה נתונים:

- **ראשית**, התפשטות הטרור הבינלאומי בעולם בעשור האחרון הגיעה לממדים חדשים ומבהילים, ובעיקר התעצמה השפעתו של הטרור על תהליכים בינלאומיים. בעבר נתפס הטרור כאיום בלתי אסטרטגי, פסיכולוגי, אך בעקבות פיגועי 11 בספטמבר וגל הג'האד העולמי במדינות רבות נוספות – וכן באזורנו בעקבות התחזקות החיזבאללה ושליטת החמאס ברצועת עזה – ברור שהטרור הפך לאיום ממשי ומוחשי על הדמוקרטיות המערביות.
- **שנית**, רשת האינטרנט מתפשטת ותופסת נפח גדל והולך בחייהם של רוב אזרחי העולם המערבי (וחלק גדול מאזרחי שאר העולם). יישומים שונים מאפשרים לבצע פעולות רבות (איסוף מידע, קיום תקשורת) שלא ניתן היה לבצען בעבר ללא השקעה רבה של זמן וכסף. בהתאם, גם ארגוני הטרור עושים שימוש אדיר מימדים ברשת.

- **שלישית**, ההתקדמות הטכנולוגית המהירה של רשת האינטרנט מאפשרת מעקב פולשני והדוק על חיי האזרחים, באופנים ובהיקף שלא היו אפשריים בעבר.

לאחר הצגה כללית של הזכות לפרטיות, יתמקד המאמר ב"מאזן האימה" הזה שבין ההתקדמות הטכנולוגית של הרשת והיתרונות שהיא מספקת לארגוני הטרור, ובין היכולות החדשות שהרשת מאפשרת לרשויות המדינה במלחמתן בטרור. בסעיף 5 להלן נבחנים נימוקים חדשים בעד שינוי האיזון הקיים. הם מצדיקים, לטעמי, חשיבה מחודשת על נוסחאות האיזון המסורתיות, ואולי אפילו יצדיקו בעתיד פגיעה קשה יותר בפרטיות האזרחים ביחס למה שהיינו מורגלים אליו בעבר, בעידן שקדם לכניסת רשת האינטרנט לחיינו.

2. הזכות לפרטיות

א. הגדרתה וחשיבותה של הזכות לפרטיות

בסרט "מלאכים בשמי ברלין" הולך לו המלאך בספרייה הציבורית ושומע את מחשבותיהם של הקוראים. כל הדאגות, השמחות והחרדות של האנשים נודעות לו ואין להם כל אפשרות להסתירן ממנו. כל שעליו לעשות כדי לגלות את המידע הכמוס ביותר של האנשים שסביבו הוא לעבור לידם. מנגד עומד רובינזון קרוזו, סמל הבדידות האולטימטיבי. הוא חי על אי בודד, אין אדם בעולם שמתעניין בו ולשום אדם אין מושג על מעשיו, על מקום הימצאו או על מחשבותיו. שתי דוגמאות אלה ממחישות את מורכבותה של הזכות לפרטיות. שלא כמו זכויות אדם אחרות, הזכות לפרטיות אינה בהכרח במיטבה ככל שיש לנו יותר ממנה. היעדר מוחלט של פרטיות ייחשב על ידי רוב הציבור כלא רצוי וכפוגע בדיוק כמו פרטיות מוחלטת.[3] הזכות מתקיימת בתוך מתחם אפשרויות שעל גבולותיו לא שוררת הסכמה. היקפה של הזכות לפרטיות נתון במחלוקת בספרות וכמעט

3 R. Gavison, "Privacy and the Limits of Law", *Yale Law Journal* 89 (1980), p. 440; E. Gross, "The Struggle of a Democracy against Terrorism—Protection of Human Rights: The Right to Privacy versus the National Interest—the Proper Balance", *Cornell International Law Journal* 37 (2004), p. 34

כל מאמר העוסק בה מתייחס לקושי להגדירה. בדוח הוועדה להגנה מפני פגיעה בצנעת הפרט, בראשות השופט יצחק כהן, נקבע כי "זהו אחד המונחים המשפטיים שאינו ניתן להגדרה מדויקת".[4] לדעת פרופ' סולוב, "נראה שפרטיות מתייחסת להכול, ולכן נראה שהיא מתייחסת לכלום".[5]

היעדרה של הגדרה מדויקת לזכות לפרטיות יכול להיחשב למפתיע בהתחשב בשימוש הרב הנעשה בזכות זו בעולם המשפט, ובהסתמכות עליה כדי להצדיק שורה של איסורים וזכויות בתחומים שונים: הדין הפלילי מגן מפני פגיעה בגופו של אדם, דיני הנזיקין מגִנים מפני הסגת גבול, דיני לשון הרע מגִנים מפני פגיעה בשם הטוב וחוק האזנת סתר אוסר על ציתותים ללא צו מיוחד. חוק הגנת הפרטיות מרחיב את ההגנה על הזכות וקובע שורה של איסורים בנוגע לחשיפת מידע על אדם, מעקב אחריו ועוד.[6] גם במשפט האמריקני מופיעה הזכות לפרטיות בהקשרים שונים, ובית המשפט העליון הסתמך עליה כדי לקבוע את הזכות החוקתית לסרב לחיפושים לא סבירים, את הזכות לבצע הפלות ולקבל החלטות בנושאים כמו נישואין, גידול ילדים וחינוך, ואת זכותם של אזרחים לא למסור מידע לרשויות ממשלתיות.[7]

אחת הסיבות לקושי שבהגדרת הזכות לפרטיות היא שהמונח "פרטיות" סובייקטיבי במהותו. אנשים שונים מגדירים אחרת מהי פרטיות, מה מאיים על תחושת הפרטיות שלהם ומהו היקף ההגנה על הפרטיות שראוי לדרוש מהמדינה. יש מי שרואים במסירת מידע על משכורתם השנתית פגיעה בפרטיות, אחרים ינדבו מידע זה בשמחה ויוסיפו את עלות השיפוץ שערכו לאחרונה בביתם; יש

4 **דין וחשבון הוועדה להגנה מפני פגיעה בצנעת הפרט** (יו"ר: שופט בית המשפט העליון, יצחק כהן), 1976, עמ' 1.

5 D. Solove, "A Taxonomy of Privacy", *University of Pennsylvania Law Review* 154 (2006), p. 479. להתייחסות לקשיים בהגדרת הזכות ראו **שם**, עמ' 478–480, וההפניות המובאות שם.

6 לדוגמאות נוספות ראו י' און ואח', **פרטיות בסביבה הדיגיטלית** (בעריכת נ' אלקין־קורן ומ' בירנהק, חיפה: המרכז למשפט וטכנולוגיה, אוניברסיטת חיפה, 2005), עמ' 1–2.

7 U. S. Department of Defense, *Safeguarding Privacy in the Fight against Terrorism: Report of the Technology and Privacy Advisory Committee*, March 2004, p. 21 (להלן: דוח *TAPAC*).

אנשים שמנהלים בקולי קולות שיחות פרטיות בטלפון הנייד באמצע בית קפה, אחרים רואים בכך חשיפה לא ראויה.

הגדרת המונח "פרטיות" תלויה גם בחברה ובמקום. למשל, אזרחי ישראל מקבלים בטבעיות את בדיקת חפציהם האישיים בכניסה למקומות ציבוריים, אולם הניסיון להנהיג מדיניות דומה בלונדון, בעקבות סדרה של פצצות שהוטמנו במוקדי בילוי במרכז העיר, נתקל בהתנגדות חריפה. גם הנהגת תעודות זהות אלקטרוניות עברה בישראל כמעט בלי דיון ציבורי, בעוד שבארצות הברית ובבריטניה נתקל הרעיון במחאה ציבורית גורפת. ההבדלים התרבותיים בהתייחסות לזכות לפרטיות בולטים עוד יותר מאז ספטמבר 2001. בארצות הברית מתקיימים דיונים סוערים בתקשורת ובאקדמיה בנוגע לסמכויות שראוי לתת לשירותי הביטחון, שחלקן פוגעות בזכות לפרטיות. במסגרת דיון זה מועלות הצעות חוק בקונגרס, מוגשות עתירות לבתי המשפט והתקשורת עוסקת בכך באופן אינטנסיבי. דיון כזה כמעט שאינו מתנהל בישראל והוא קיים במידה פחותה במדינות אירופה. הגדרת המונח "פרטיות" תלויה גם באפשרויות הפגיעה בפרטיות, בייחוד על ידי השלטון. הטכנולוגיות הקיימות היום מאפשרות פגיעה בדרכים שבעבר לא היה אפשר לחזות אותן, ולכן גם לא הייתה התייחסות להגבלתן.

בספרות אפשר למצוא הגדרות רבות לזכות לפרטיות. בין ההגדרות הוותיקות ישנה זו שניסחו שופטי בית המשפט העליון האמריקני וורן וברנדייס, ולפיה זוהי זכותו של אדם "להיעזב לנפשו" (the right to be left alone).[8] מאז ניתנה הגדרה זו לפני כ־120 שנה, הועלו הצעות רבות להגדרות מרחיבות יותר.

פרופ׳ גביזון, למשל, מגדירה את הזכות במונחים של גישה, המתבטאת בשלושה עניינים: האחד הוא הגישה הפיזית לגוף האדם או למקום פרטי; השני קשור למידע על האדם, לשימוש בו או לפרסומו; השלישי קשור לשמירה על האנונימיות של האדם. לטענת פרופ׳ גביזון, שלושה גורמים נבדלים אלה – בדידות, סודיות ואנונימיות – יוצרים יחד הגדרה מורכבת של מושג הפרטיות.[9]

8 S. D. Warren & L. D. Brandeis, "The Right to Privacy", *Harvard Law Review* 4 (1890), p. 193

9 Gavison, **לעיל** הערה 3, עמ׳ 428–429.

אחרים מעדיפים להגדיר את הזכות לפרטיות במונחים של שליטה, כולל יכולתו של אדם לשלוט על המידע הקשור אליו ועל איכותו, וכן על האפשרות של אחרים להגיע אליו ועל הדרכים שבהן מידע אישי עליו הופך לפומבי.[10]

פרופ׳ סולוב טוען, לעומת זאת, שהמונח ״פרטיות״ מורכב מכדי שהגדרה בודדת תוכל להכיל אותו. הניסיונות לעשות זאת הסתיימו תמיד בהגדרות מעורפלות ורחבות, אשר ביטלו את מורכבות המונח ופגעו באינטרסים שעליהם אמורה הזכות לפרטיות להגן. הוא מעדיף, במקום זאת, לדון בסוגי הפעולות הפוגעות בפרטיות, בלי לנסות להגדיר במדויק את היקפה של הזכות.[11] אני מסכים עם כיוון זה. היעדרה של הגדרה מדויקת אינו מפחית מחשיבותה של הזכות. הכרה בה כזכות עצמאית ונפרדת חיונית כדי להבטיח שהיא תיכלל בכל איזון שייעשה בין אינטרסים שונים וכדי להבהיר שזוהי זכות הראויה להגנה. הכרה כזו חשובה במיוחד בהתחשב בעובדה שברוב המכריע של המקרים עומדים מול הזכות המעורפלת לפרטיות אינטרסים ברורים ונוקשים – כמו שיקולי ביטחון והזכות לחופש ביטוי – אשר גוברים עליה בנקל.[12]

על אילו אינטרסים נועדה הזכות לפרטיות להגן ומדוע חשוב שהמדינה תגן על הפרטיות? החסרונות של ההגנה על זכות זו ברורים. אם הכול יהיה גלוי וידוע, יהיו חיינו במידה רבה קלים יותר. הפשע והטרור יופחתו באופן משמעותי, שכן יהיה קל יותר לתפוס עבריינים ולסכל פיגועים. העולם יהיה מקום בטוח יותר וניתן יהיה להפנות את המשאבים המושקעים היום במניעת סכנות (שאתן נאלצים שירותי הביטחון להתמודד) למקומות מועילים יותר לחברה, כמו חינוך, תרבות ואתרי נופש. כמו כן, ביטול ההגנה על הפרטיות יאפשר להסיר את ההגבלות הקיימות היום על זכויות אחרות – למשל על חופש הביטוי ועל חופש העיתונות – בשל הצורך לשמור על צנעת הפרט. ניתן יהיה להסיר את ההגבלות מעל מאגרי מידע ולאפשר נגישות חופשית לכמויות אדירות של נתונים לקהל הרחב, דבר שעשוי לסייע לגורמים מסחריים ולהביא לצמיחה כלכלית.[13]

10 להסבר על גישה זו ראו Gross, **לעיל** הערה 3, עמ׳ 31. לסקירת הגישות השונות ראו ז׳ סגל, ״הזכות לפרטיות למול הזכות לדעת״, **עיוני משפט** ט (1983), עמ׳ 175.

11 ראו Solove, **לעיל** הערה 5, עמ׳ 485–486.

12 ראו Gavison, **לעיל** הערה 3, עמ׳ 459–467.

13 **שם**, עמ׳ 443–444. ראו גם Gross, **לעיל** הערה 3, עמ׳ 33.

אין להבין מזה שהצורך בפרטיות נובע דווקא מהרצון לאפשר את ביצועם של מעשים לא חוקיים או אפילו לא מוסריים, אף שאין ספק שהפרטיות מקלה על הסתרתם. הזכות גם אינה נובעת מהרצון להסתיר מאחרים מידע חיוני. גם כאשר אנו מתנהלים בחיי היומיום שלנו, בפעולות שגרתיות, אנו זקוקים למרחב שבו פעולותינו אינן גלויות לאחרים. אם אדם יציץ לביתנו כאשר אנו סועדים ארוחת ערב או צופים בטלוויזיה, נחוש תחושת חוסר נוחות גם אם אותו אדם אינו מאיים עלינו ואין לנו דבר להסתיר. הזכות לפרטיות נגזרת מתפיסת הפרט כיצור אוטונומי והיא נדרשת כדי לאפשר לכל אדם את החירות לפעול כראות עיניו.[14] בהקשר זה כתבה חנה ארנדט:

> לחיים המתנהלים אך ורק בפומבי, בנוכחות אחרים, היינו קוראים רדודים. אף שניתן לראותם, חיים אלה מאבדים את התכונה של התרוממות מקרקע אפלה יותר, החייבת להיוותר מוסתרת שמא תאבד מעומקה האמתי והלא־סובייקטיבי.[15]

הפרטיות חיונית גם כדי לאפשר לנו לבטא חלקים מחיינו שאנו מסוגלים לממש רק כאשר אנו לבד, כמו יצירת קשרים עם אנשים קרובים, כולל קשרים אינטימיים. יצירת מרחב החסום בפני העולם החיצוני והקמת חיץ בין האדם לבין אחרים מאפשרות לבני האדם לפעול בלי חשש מביקורת, שיפוט או בושה. השחרור מתגובותיהם של אחרים מאפשר מגוון פעולות רחב שהחברה מבקשת לעודד. הפרטיות מאפשרת לאנשים להתפתח, לחקור, להתנסות בחוויות חדשות, כולל כאלה שעלולות להביא לכישלונות. היא מאפשרת לאדם להתרכז, ללמוד, ליצור, לכתוב ולהירגע.

הזכות לפרטיות חשובה לא רק לפרט, חברה פתוחה ודמוקרטית תתקשה להתקיים ולהתפתח בלעדיה. חברה המכירה בזכותם של חבריה להתקיים גם בנפרד, מכירה בזכות להיות שונה ובחובתה להגן על כך. חברה כזו היא פתוחה יותר, סובלנית יותר ומעניינת יותר. היא מכילה מגוון דעות – עיקרון חיוני לכל

14 ראו Gavison, **לעיל** הערה 3, עמ׳ 442–450; און ואח׳, **לעיל** הערה 6, עמ׳ 11–12.

15 מתוך Hannah Arendt, *The Human Condition*, מצוטט אצל Solove, **לעיל** הערה 5, עמ׳ 555.

משטר דמוקרטי – ומאפשרת לאנשים לגבש דעות עצמאיות. נוסף על כך, היא שומרת על שורה של זכויות אדם אחרות, למשל חופש הביטוי, שכן אנשים לא יחששו לומר את שעל ליבם גם אם דעותיהם אינן מקובלות. חברה כזו מקיימת חופש אקדמי ובכך מרחיבה את הידע ומעודדת יצירת התארגנויות חדשות, גם כאלה התומכות בעקרונות שאינם בקונצנזוס.[16]

ב. הסכנות לפרטיות כתוצאה מאיסוף המידע והשימוש בו

הזכות לפרטיות אינה מוחלטת ולעתים היא נסוגה מפני אינטרסים אחרים או זכויות אחרות. לפני שנבחן את ההצדקות לשימוש בשיטות איסוף המידע החדשות, יש לבחון את הפגיעה הנובעת מהן, ואת ההשלכות של השימוש בהן על החברה כולה ועל כל אחד מהפרטים בה. היחס לפגיעה ולהשלכותיה עשוי להשתנות בהתאם לאפשרויות הטכנולוגיות העומדות לרשותנו. האפשרויות הקיימות היום להצלבת מידע המאוחסן במאגרים שונים, הופכת מידע סתמי כמו שם, כתובת או מספר תעודת זהות לבעל משמעות, שכן ניתן לקשור אותו למידע נוסף שנאגר על אותו אדם במאגרים אחרים וכך ללמוד עליו הרבה מעבר לפריט המידע הסתמי.

אופי הדיון בסכנות הנובעות מאיסוף המידע קשור כמובן לאופן שבו מוגדר המונח "פרטיות". יש מי שמציינים כסכנה את עצם העובדה שמידע עצום על אודותיהם נאגר אצל גורמים ממשלתיים, שכן הם רואים בכך פגיעה בפרטיות. אחרים מתקשים להבין את הבעיה הכרוכה בכך. הדיון שלהלן יתמקד בסכנות העיקריות שהוזכרו בספרות, ושלגביהן שוררת הסכמה.

הדיון בספרות מתמקד בשני דימויים עיקריים – האחד עוסק בשאלת איסוף המידע והשני בשימוש שנעשה בנתונים שנאספו. הדימוי הנפוץ ביותר, המתמקד באיסוף המידע, הוא של "האח הגדול" בספרו של ג'ורג' אורוול "1984". הספר מתאר חברה שהפרטים בה נתונים למעקב מתמיד ולשליטה מוחלטת. האנשים נדרשים לפעול ואף לחשוב בדרך אחת שקבע השלטון, וכל סטייה מדרך זו גוררת ענישה חמורה. הממשלה שולטת על כל ההיבטים של חיי היומיום באמצעות ביטול מוחלט של הפרטיות. אמנם המעקב אינו מתקיים כל הזמן,

16 Gavison, **לעיל** הערה 3, עמ' 455–456; Gross, **לעיל** הערה 3, עמ' 33; דוח *TAPAC*, **לעיל** הערה 7, עמ' 2.

אולם האפשרות להיות נתון למעקב לא פוסקת, ולעולם אין אדם יכול לדעת מתי צופים בו. חיילים מסתובבים ברחובות, מסוקים טסים בשמים – ובכל בית קיים מתקן המכונה Telescreen, שדרכו יכולה הממשלה להביט אל המתרחש בדל"ת אמותיו של כל אדם בכל רגע.

הטלסקרין דומה למתקן פיקוח שתיאר ג'רמי בנת'ם בשנת 1791, ה־Panopticon. מתקן זה יכול להכיל אסירים, חולי נפש או כל קבוצה אחרת שמבקשים לשלוט בה. המתקן הוא בצורת טבעת ובמרכזו מגדל עם חלונות. בתוך הטבעת ישנם תאים ובכל תא אדם אחד. המתקן מאפשר לעומדים במגדל לצפות בכל רגע באנשים שבתאים, בלי שאלה יוכלו לדעת מתי מתבוננים בהם ומתי לא. עצם הידיעה שמעקב כזה אפשרי מספיקה כדי להבטיח ציות מוחלט לכללים. כך מתאפשרת שליטה מלאה בלי צורך להפעיל כוח.[17]

אפשר לטעון שאיסוף מידע בלתי מבוקר דרך רשת האינטרנט יכול להביא – בשל הדרך שבה הוא מתבצע – להשגת שליטה דומה. מידע על הגולשים יכול להיאסף בכל רגע בלי שנמסר להם על כך ובלי שהם יודעים אילו פרטים על אודותיהם נשמרים ולאיזה צורך הם משמשים. כתוצאה מכך עלולים הגולשים לצנזר את דבריהם, להימנע מהתנסויות חדשות ולנהוג ככלל כפי שהם סבורים שמצופה מהם, גם אם אין להם כל כוונה לעבור על החוק. תוצאה זו מכונה בספרות "אפקט מצנן", והיא מתייחסת לפעולות חוקיות שאנשים יימנעו מלעשותן בשל החשש שאחרים צופים בהם, מתעדים אותם ומפרשים באופן מוטעה את כוונותיהם. האפשרות שהמידע ייאסף והידיעה שהמדינה עוסקת בכך עלולות לפגוע באינטרסים שעליהם נועדה להגן הזכות לפרטיות. הסכנה אינה רק לכל אחד מהפרטים אלא גם לחברה בכללותה; היא תתקשה ליצור סביבה פתוחה וסובלנית ועלולה להפוך לקונפורמיסטית ומפוחדת. בשל השלכות אלה נחשבו תמיד המעקבים לכלי של שליטה חברתית והשלטת נורמות הרצויות בעיני השלטון.[18]

17 Solove, **לעיל** הערה 1, עמ' 1414–1415. להתייחסות למתקן זה, ראו M. Foucault, *Discipline and Punish: The Birth of the Prison*, trans. A. Sheridan (New York: Vintage Books, 1977), pp. 195–228

18 התייחסות ל"אפקט המצנן" ראו אצל Solove, **לעיל** הערה 5, עמ' 532; G. Horn, "Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines", *New York University Annual Survey of American*

הדימוי השני מתייחס לסכנות המובנות בטכנולוגיות החדשות ומתמקד בשימוש שנעשה במידע שנאסף. לטענת פרופ׳ סולוב, שהציג דימוי זה, המטפורה של האח הגדול מתמקדת בתפיסה אחת של הפרטיות שבמרכזה ניצב אלמנט הסודיות. לפי תפיסה זו, הפרטיות נחוצה כדי לאפשר לאדם להסתיר מפני אחרים מידע הקשור בו וכדי למנוע מבוכה, פגיעה במוניטין וכדומה. אולם התמקדות בתפיסה זו של הפרטיות בלבד, מונעת הגנה על הפרט מפני פגיעות אחרות שעלולות להיגרם כתוצאה מהשימוש שנעשה במידע שנאסף עליו. להבהרת סכנות אלה מציע פרופ׳ סולוב דימוי חלופי – העולם המתואר בספרו של קפקא "המשפט". ק׳ עומד למשפט בלי שיידע מדוע ובלי שגורם רשמי כלשהו יטרח להסביר לו משהו. המנגנון הביורוקרטי אדיש לחלוטין לשימוש שנעשה במידע ולשגיאות שעלולות להיות בו, ולאזרחי המדינה אין כל אפשרות לברר את הסיבות שעמדו בבסיס החלטות הנוגעות בהם.[19] המדינה המתוארת בספר "המשפט", טוען פרופ׳ סולוב, משקפת את הבעיות הנובעות מאגירה של כמויות אדירות של נתונים ואחסונם במאגרי מידע לתקופות בלתי מוגבלות. אנשים מאבדים את השליטה על המידע הקיים עליהם, הם אינם יודעים למי יש גישה אליו, ובשל כך אין להם כל אפשרות להבין את ההחלטות המתקבלות בעניינים. מצב זה עלול לעורר תחושות של חוסר אונים ולגרום לאנשים לוותר מראש על כל ניסיון להשפיע על חייהם. החברה נהפכת לביורוקרטית, שרירותית ואטומה. על פי הדימוי של "האח הגדול", האנשים יודעים לפחות שאם ינהגו לפי הכללים יעזבו אותם הרשויות לנפשם. על פי הדימוי של "המשפט", לעומת זאת, הפרט נותר בלי כל יכולת להשפיע על מצבו.[20]

שני דימויים אלה – של האח הגדול ושל העולם הקפקאי – מבהירים את ההשלכות של מתן סמכויות בלתי מוגבלות לשירותי הביטחון בכל הקשור לאיסוף מידע ולשימוש בו. היום אפשר מבחינה טכנית להצליב מידע ולשמור כמויות אדירות של נתונים, וכך לאסוף מידע אפקטיבי רב על הגולשים באינטרנט

Law 60 (2005), pp. 765–766; K. Taipale, "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd", *Yale Journal of Law and Technology* 7 (2004–2005), pp. 146–148

19 Solove, **לעיל** הערה 1, עמ׳ 1398–1399.

20 **שם**, עמ׳ 1421–1423.

וליצור פרופיל מפורט שלהם. ההנחה היא שפרופיל כזה משקף את האמת על אודותיהם.[21]

ככל שקיימים יותר נתונים וככל שקל יותר לגשת אליהם, גובר הפיתוי להסתמך עליהם באופן עיוור לצורך קבלת החלטות על חייהם של הפרטים. אולם עליית חשיבותם של הנתונים הנאספים ושל הפרופילים המבוססים עליהם יוצרת שתי בעיות: ראשית, המידע שנאגר יכול להיות מוטעה, לא מעודכן או מיוחס לאדם בטעות, אולם לאותו אדם אין כל דרך לדעת זאת, וגם כאשר נודע לו על כך אין לו דרך לתקן זאת. שנית, גם אם הנתונים מדויקים אין באפשרותם לתפוס את כל מורכבות החיים האנושיים ולהכיל את האדם שמאחוריהם. הם מסוגלים לתפוס רק את פני השטח אך לא להסביר שינויים והתפתחויות.[22] המידע העצום שנאסף והיעדר הגישה (של האזרחים) אל הנתונים שנאספו יוצרים שילוב שמבהיר כיצד יכולה להתרחש פגיעה בפרטיותו של אדם גם אם הוא פועל בהתאם לחוק ואין לו דבר להסתיר.

3. רשת האינטרנט ושירותי הביטחון

א. מקורות חדשים וטכנולוגיות חדשות

רשת האינטרנט מעמידה לפני שירותי הביטחון אפשרויות עצומות לאיסוף מידע על אנשים. פעולות שבעבר דרשו השקעות עצומות של זמן וכסף נעשות היום בלחיצת מקש. מה הופך את איסוף המידע ברשת להליך כה פשוט?

רשת האינטרנט בנויה כך שבכל פעם שאנו גולשים בה או שולחים דואר אלקטרוני, אנו מותירים אחרינו שובל של רסיסי מידע, מעין עקבות דיגיטליים החושפים פרטים רבים עלינו. כמעט כל פעולה שלנו מגלה מידע נוסף שיכול להיות בעל ערך רב לשירותי הביטחון. שליחת דואר אלקטרוני, גלישה באינטרנט והורדת קבצים – כל הפעולות האלו נרשמות במחשב ובשרתים האחראים על התקשורת. להבדיל משיחות טלפון רגילות, שם נותר תוכן השיחה רק בזיכרונם של הדוברים, שיחות המתנהלות ברשת האינטרנט מתועדות במלואן – ולא רק

21 **שם**, עמ' 1424–1429; דוח *TAPAC*, **לעיל** הערה 7, עמ' 42.

22 **שם**, עמ' 36–38.

תוכנן מתועד, מתועדים גם פרטים כמו מועד ביצוע השיחה, השרתים שהעבירו אותה, המחשבים שדרכם היא נעשתה וכדומה. שירותי הביטחון יכולים לאסוף את המידע הקיים כבר ממילא, בניגוד למצב בעבר שבו היה צורך להגיע פיזית לבתיהם של אנשים, למקומות עבודתם, לסניפי הבנק שלהם ולחבריהם כדי לאסוף עליהם מידע.[23]

רשת האינטרנט היא אמצעי תקשורת זול ונגיש למגוון רחב של אנשים. משתנים כמו גבולות גאוגרפיים, שכבה כלכלית, גיל או השכלה משחקים בה תפקיד שולי. נוסף על כך, בשל האשליה שניתן להסתתר ברשת מאחורי זהויות בדויות, גולשים עשויים לגלות פרטים על עצמם במחשבה שהם לא יקושרו אליהם. מאפיינים אלה מאפשרים לשירותי הביטחון גישה לכמויות מידע עצומות.[24] את המידע שנאסף אפשר לשמור במאגרי מידע לתקופות ממושכות ולהצליב אותו עם מידע קיים או עם מידע חדש הממשיך להגיע. הטכנולוגיות הקיימות מאפשרות לאתר תבניות התנהגות ולמצוא בתוך הנתונים הקשרים שבני אדם לא יוכלו לגלות לבדם.[25]

רשת האינטרנט מבוססת על תקשורת בין מחשבים הנעשית באמצעות שליחה וקבלה של "חבילות". כל חבילה מכילה "כותרת חבילה", המכוונת את החבילה ליעדה וכוללת מידע בנוגע לכתובת האינטרנט של הנמען, כתובת האינטרנט של השולח (IP address) ומידע בנוגע לסוג החבילה (חלק מעמוד אינטרנט, חלק מתמונה וכולי). כאשר "החבילה" מגיעה ליעדה, המחשב שקיבל אותה "משליך" את הכותרת ו"פותח" את ההודעה המקורית, הכוללת את תוכן ההודעה.

מבנה זה עומד בבסיסה של אחת ההבחנות המרכזיות שעליהן בנויים החוקים הנוגעים להגנת הפרטיות באינטרנט – ההבחנה בין מידע המהווה תוכן לבין מידע שאינו תוכן. למשל, בנוגע לדואר האלקטרוני, ההודעה עצמה ושורת הנושא ייחשבו למידע שהוא תוכן, ואילו שאר הפרטים שב"כותרת החבילה" –

23 Solove, **לעיל** הערה 1, עמ' 1394; א' איינהורן ואח', **לוחמה בטרור בזירת המידע** (בעריכת נ' אלקין־קורן ומ' בירנהק, חיפה: המרכז למשפט וטכנולוגיה, אוניברסיטת חיפה, 2002), עמ' 53–54.

24 לסקירה מפורטת של מאפייני הרשת ראו און ואח', **לעיל** הערה 6, עמ' 19–24.

25 Tien, **לעיל** הערה 2, עמ' 394–395; דוח *TAPAC*, **לעיל** הערה 7, עמ' 4–5.

בהם פרטים על הנמען, השולח, מועד שליחת ההודעה וגודלה – ייחשבו למידע שאינו תוכן.[26] ההבחנה בין שני סוגי המידע מיטשטשת כאשר מדובר בגלישה רגילה באינטרנט, והשאלה מהו מידע של תוכן טרם הוכרעה באופן חד־משמעי בשיטות המשפט השונות.[27]

התפיסה המקובלת ברוב שיטות המשפט היא שמידע שהוא תוכן ראוי להגנה רבה יותר, שכן קריאתו נחשבת לפגיעה חמורה יותר בזכות לפרטיות. לכן ייתכן שגישתם של שירותי הביטחון למידע זה תוגבל, והם יאלצו להסתפק במידע הנמצא ב"כותרת החבילה". אולם גם מידע זה מאפשר ללמוד רבות על הגולשים. כך ניתן ללמוד על רשימת אנשי הקשר שלהם, על תדירות הקשר אתם ועל זמני הגלישה. כמו כן, רשימה של כתובות IP שהתבקשו ממחשב מסוים תאפשר ללמוד על הדרך שבה אדם גולש באינטרנט. רשימה של כתובות ה־URL (Uniform Resource Locators), המציינות את המיקומים המדויקים ברשת שאליהם הגיע הגולש, תגלה את החיפושים שהוא ביצע ואת העמודים שאותם קרא.

הגישה למידע זה יכולה להיעשות בשתי דרכים: שירותי הביטחון יכולים לפנות לספקי השירות ולדרוש מהם ישירות מידע על המנויים שלהם. ספקי השירות מחזיקים במידע רב הכולל גם פרטים אישיים של המנויים – כתובת, מספר טלפון, זמני גלישה, דרכי תשלום ואף מספר כרטיס האשראי או מספר חשבון הבנק. נוסף על כך, ספקי השירות שומרים בשרתים שלהם, אם כי לתקופות מוגבלות, העתק מכל הפעולות שעשו המנויים ברשת, כולל תוכנן של הודעות הדואר האלקטרוני.

כדי להגיע למידע בזמן אמת, על שירותי הביטחון "לצותת" לכל התנועה העוברת דרך השרת של ספק השירות ולאתר את התקשורת המתבקשת. ציתות לקו מאפשר לסרוק את תנועת החבילות העוברות דרך נקודה זו ברשת, והוא נעשה באמצעות תוכנות המכונות "רחרחניות". אחת ההשלכות העיקריות של טכנולוגיה זו על הזכות לפרטיות היא שמעקב באינטרנט יהיה תמיד כרוך

26 O. Kerr, "Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't", *Northwestern University Law Review* 97 (2003), pp. 611–615

27 **שם, עמ' 644–647. ראו גם** D. Solove, "Reconstructing Electronic Surveillance Law", *George Washington Law Review* 72 (2004), pp. 1287–1288

בבחינה של כל התנועה הזורמת דרך נקודה מסוימת ברשת, כולל זו של אנשים תמימים שאינם חשודים בדבר.[28]

שירותי ביטחון ברחבי העולם מיהרו להבין את היתרונות הגלומים ברשת האינטרנט. חלק מהשיטות והתוכנות הנמצאות בשימושם אינן ידועות לציבור, כך שלא ניתן לדעת את היקף השימוש בטכנולוגיות החדשות. עם זאת מפרסומים שונים ניתן ללמוד על כמה מהתוכנות הנמצאות היום בשימוש ברחבי העולם.

הדוגמה הידועה ביותר היא התוכנה שנמצאת בשימוש ה־FBI בארצות הברית, המכונה The Carnivore. זו תוכנה רחרחנית המסוגלת לעקוב אחר התקשורת העוברת דרך ספק שירות מסוים. התוכנה מאפשרת לאסוף שני סוגים של מידע: מידע שאינו תוכן – כתובות דואר אלקטרוני של הנמען ושל אנשי הקשר שלו וכתובות IP; ומידע תוכן – הודעות הדואר עצמן, תוכנם של עמודי אינטרנט שנקראו וכדומה. השימוש בתוכנה זו אפשרי רק לאחר שה־FBI פנה לבית המשפט וקיבל צו שבו הגדיר השופט את סוג המידע שמפעילי התוכנה מוסמכים לאסוף. התוכנה מכוילת לפי קביעת השופט, והמידע המבוקש נשמר לצורך ניתוח מאוחר יותר.[29] יש הטוענים שהתוכנה דווקא מחזקת את ההגנה על הפרטיות, שכן היא מחייבת הגדרה מדויקת של המידע המבוקש.[30] מנגד, ארגוני זכויות אזרח טוענים שהתוכנה פוגעת בפרטיות הרבה מעבר לנדרש. כך למשל נטען על ידי American Civil Liberties Union (ACLU) שהתוכנה מאפשרת פגיעה רחבה בזכויות, שכן שהדבר היחיד המונע מהממשלה לקרוא את כל הדואר האלקטרוני העובר דרך השרת הן ההוראות שהיא עצמה כתבה.[31]

28 Kerr, **לעיל** הערה 26, עמ' 649–651.

29 **ראו** T. McCarthy, "Don't Fear Carnivore: It Won't Devour Individual Privacy", *Missouri Law Review* 66 (2001), pp. 834–837. **ראו גם** איינהורן ואח', **לעיל** הערה 23, עמ' 57–58; Gross, **לעיל** הערה 3, עמ' 38.

30 Kerr, **לעיל** הערה 26, עמ' 648.

31 **ראו למשל** J. Stanley & B. Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society* (New York: ACLU Publication, January 2003), p. 8 (להלן: דוח *ACLU*).

דוגמה נוספת היא תוכנה בשם "אשלון" (Echelon) המופעלת בשיתוף פעולה של כמה מדינות (ארצות הברית, אנגליה, קנדה, אוסטרליה וניו זילנד). התוכנה אוספת דואר אלקטרוני, שיחות טלפון ותקשורת אלקטרונית אחרת באמצעות עמדות המפוזרות בעולם. היא מסוגלת לקלוט כמויות אדירות של מידע – כשלושה מיליארד תשדורות אלקטרוניות ביום. היא פועלת באמצעות תוכנות רחרחניות המפקחות על התשדורות העוברות ברשת, מאתרות תשדורות בעלות ערך מודיעיני ושומרות אותן.[32]

רעיון אחר – השאפתני ביותר שהועלה עד היום – מגולם בתוכנה The Total Information Awareness System (TIA) שהדיון עליה התעורר בארצות הברית לאחר הפיגוע במגדלי התאומים בספטמבר 2001. תוכנה זו נועדה לשלב את כל מאגרי המידע המוחזקים בידי הסוכנויות הממשלתיות עם מאגרי מידע של חברות פרטיות. הצלבת המידע אמורה להיעשות באמצעות מערכת שסורקת, מרכיבה ומעבדת נתונים אישיים של כל הפרטים בתוך ארצות הברית וגם מחוץ לה, כדי לגלות תבניות, להעלות השערות, לדווח ולהזהיר מפני התנהגות חשודה. כתוצאה מביקורת ציבורית על השימוש בנתונים של אזרחים אמריקנים, החליט הקונגרס ביולי 2003 להפסיק את העברת הכספים לפיתוחה. עם זאת הותר מימון תוכנות דומות שלא עלו לדיון ציבורי, אף שהן מעלות שאלות דומות בנוגע לזכות לפרטיות של אזרחים ותושבים אמריקנים.[33]

ב. אתגרים חדשים ו"אוקיינוס המידע"

הרשת נותנת בידי שירותי הביטחון כלים רבים להתחקות וללמוד על הפעולות וההרגלים של המשתמשים בה; התוכנות המתקדמות מעניקות יכולת לחדור אל צנעת הפרט ואל פרטיות האזרחים, שרובם תמימים לחלוטין. עם זאת, כפי שאציג

32 **שם**, עמ' 8–9. ראו גם איינהורן ואח', **לעיל** הערה 23, עמ' 55.

33 התייחסות לזה ראו בדוח *TAPAC*, **לעיל** הערה 7, עמ' 1–5; J. Rosen, "The Naked Crowd: Balancing Privacy and Security in an Age of Terror", *Arizona Law Review* 46 (2004), p. 610n; G. Hosein, *Threatening the Open Society: Comparing Anti-Terror Policies and Strategies in the U.S. and Europe* (Privacy International Report, 2005), pp. 10–13

בהמשך, הופעת רשת האינטרנט בחיינו לא הפכה את עבודת רשויות הביטחון לקלה יותר. אף על פי שכל הפעולות ברשת אינטרנט משאירות "טביעת אצבע" והכול מתועד, הניסיון לברור מתוך ים המידע הזה את המידע שעשוי לסכל טרור משול למציאת מחט בערֵמת שחת. לעומת זאת גורמי הטרור יכולים לעשות שימוש קל ויעיל באינטרנט לשם השגת מטרות רבות,[34] שבעבר היו כרוכות בסיכון של חשיפה, בהוצאות כספיות, או שהיו בלתי אפשריות כלל. לכן, אף שמקובל להציג את השימוש באינטרנט על ידי רשויות הביטחון כאמצעי "נוח" להשגת מידע על פעילי הטרור, המציאות מורכבת הרבה יותר. גם גורמי הטרור עברו לשימוש באינטרנט, שתפס את מקומם של אמצעי התקשורת האחרים (כגון שיחות טלפון), אך עובדה זו מקשה ולא מקלה על הרשויות לעקוב ולאתר את פעילי הטרור בזמן אמת. כמו כן, ארגוני הטרור שינו את המבנה שלהם בצורה שמקשה עוד יותר על ניצול הרשת לשם מעקב אחריהם. על כך אפרט להלן בסעיף 8ב.

4. השימוש באינטרנט על ידי גורמי הטרור

השימוש שעושים גורמי הטרור באינטרנט הוא בעל אופי מגוון ונוגע לתחומים שונים; במידה רבה הוא חופף להשתלטות הרשת על כל תחומי החיים בעולם האזרחי, המסחרי, הממשלי והצבאי. ניתן לחלק את השימוש שעושים ארגוני הטרור ברשת לשלושה תחומים עיקריים:[35]

- שימוש ברשת כאמצעי תקשורת המונים: לשם תעמולה והפצת מידע.
- שימוש אינסטרומנטלי: תקשורת בין פעילים ובין גופים בארגון, איסוף מודיעין, גיוס פעילים וכספים ועוד.
- שימוש ישיר: טרור באמצעות הרשת (cyber terrorism).

34 G. Weiman, *Terror on the Internet* (Washington, DC: United States Institute of Peace Press, 2006), p. 30

35 **שם**, עמ' 25.

א. שימוש ברשת כאמצעי תקשורת המונים

בעשור האחרון כמעט כל ארגוני הטרור משתמשים באינטרנט באינטנסיביות, כתחליף לאמצעי תקשורת ההמונים. לרשת יש יתרונות רבים עבור ארגוני הטרור ביחס לאמצעי התקשורת הקונבנציונליים:[36]

- הרשת אינה מצונזרת או מפוקחת, וניתן להעביר בה כל מסר שהארגון מעוניין בו.
- המידע ברשת נגיש בחינם לכל אדם בכל מקום בעולם ובכל עת, בלי תלות בשעות שידור.
- ניתן להעלות ברשת מדיה מגוונת: טקסטים, תמונות, סרטים ומוזיקה, שיכולים להעצים את המסר וליצור אפקט תעמולתי חזק, למשל: שידור הוצאות להורג.[37]
- הרשת מאפשרת הפצת מידע בצורה אינטראקטיבית: כל אדם יכול לחפש ולמצוא את המידע שמעניין אותו, ליצור קשר עם אנשי יחסי הציבור של הארגון ולקבל תשובות ספציפיות לשאלות המטרידות אותו.

היום כמעט כל ארגון טרור מפעיל אתר אינטרנט. חלק מאתרים אלה קמים ונופלים ומחליפים כתובות בקצב מהיר ביותר, כך שה"מרדף" אחריהם והמלחמה בהם הופכים לחסרי סיכוי כמעט. האתרים של ארגוני הטרור מכילים את ה"אני מאמין" של הארגון וכן תמונות וסרטי תעמולה. אתרים של ארגונים רבים מעבירים גם מסרים שונים ומגוונים – ואף סותרים – המיועדים לקהלים שונים. המסרים האופייניים הם מסוגים אלה:[38]

- הצגת הארגון כנרדף וכקרבן והצנעת פעילות הטרור שלו במטרה לשכנע צדדים שלישיים בצדקת המאבק ובהפיכת הארגון ללגיטימי.
- התגאות והתפארות בפעילות הטרור של הארגון באמצעות קבלת אחריות לביצוע פיגועים על ידי הארגון, וכן שימוש בסרטים ובתמונות המכוונים לציבור התומכים של הארגון.

36 **שם**, עמ' 26–30.
37 **שם**, עמ' 26.
38 **שם**, עמ' 55–57.

- הפחדה ואיומים בפעולות ובפיגועים נוספים בעתיד, המכוונים כלפי הציבור או המדינה שבהם נלחם הארגון.

הרשת מהווה אפוא כר נוח ביותר להפצת מסריו של הארגון, הן כלפי הציבור התומך בו וכלפי קהלים אובייקטיביים והן כלוחמה פסיכולוגית בציבור שהוא יעד להפחדה. ארגון טרור, כפי שמשתמע גם מהמילה הלועזית terror, מבקש לזרוע פחד ואימה ולהשיג באמצעות זאת מטרות מגוונות. לצד השימוש בפיגועי טרור משמשים אמצעי התקשורת כלי להעצמת מסר ההפחדה שמעביר הארגון.[39] אולם בעוד שבכלי התקשורת הלגיטימיים עלולה הפצת מסרי הארגון לעבור ביקורת ואימות נתונים, ולעתים גם צנזורה כלשהי, באתר האינטרנט של הארגון אפשר לעוות את המציאות ולהציג נתונים בצורה הנוחה לארגון, לכלול מסרי שנאה ולהסית לפעולות טרור נוספות.

ב. שימוש אינסטרומנטלי

בדומה לארגונים אזרחיים לגיטימיים, ארגוני הטרור משתמשים באינטרנט גם ככלי עבודה יומיומי. לאינטרנט יש שני יתרונות ייחודיים עברו ארגוני הטרור:

- **אנונימיות.** ניתן להשיג מידע ולתקשר באמצעות האינטרנט באופן אנונימי יחסית, תוך החלפת כינויים וכתובות, שימוש ב"אינטרנט קפה" וכדומה. עם זה יש לזכור שקשה לשמור על אנונימיות מוחלטת לאורך זמן תוך שמירה על עלויות נמוכות ושימוש נוח ברשת.
- **נגישות זולה.** האינטרנט הוא אמצעי נגיש בכל שעה, מכל מקום ובמחיר זול. בעבר השמירה על קשר בין תאי פעילות מרוחקים של ארגוני טרור, הממוקמים במדינות העוינות את הארגון, הייתה קשה ויקרה (עלות שיחות בינלאומיות, שליחת שליחים ואיגרות). לעומת זאת השימוש ברשת הוא זול, נגיש ומהיר.

להלן יפורטו שימושים אינסטרומנטליים שונים שעושים ארגוני טרור ברשת.

39 **שם**, עמ' 34.

תקשורת בין פעילים[40]

דואר אלקטרוני. תחליף זול, נוח ובטוח לטלפון. הדואר האלקטרוני נגיש בכל מקום בעולם (אין צורך להחליף מספרים תוך כדי תנועה או להחזיק במכשיר סלולרי, המסגיר את מיקום הדובר), אפשר להשתמש בו מ"אינטרנט קפה" וקל להחליף כתובות במהירות (לעומת מספרי טלפון). כמו כן, הוא מאפשר הפצת מסרים לכמות גדולה של מכותבים בפעולה אחת (באמצעות רשימות תפוצה מוכנות מראש), במהירות ובלחיצת מקש, בלי צורך לערוך התקשרויות רבות.

תוכנות מסרים מידיים. תוכנות המקלות על קיום דו־שיח ורב־שיח, וכן על תכנון, תיאום ופתרון בעיות על ידי יצירת קשר מהירה והתכתבות בין פעילים. ניתן להשתמש בתוכנות אלה ברקע של עבודה אחרת במחשב, לדעת בכל עת מי מאנשי הקשר מחובר לרשת וליצור קשר מידי.

חדרי צ'ט ופורומים.[41] באתרים רבים של ארגוני הטרור קיימת אפשרות של שימוש בפורום (שיחות פומביות בין משתמשי האתר), בצורה זו או אחרת. כדי להשתתף בפורום אין צורך בכתובת דואר אלקטרוני, וכדי לקרוא אותו אין צורך בכינוי, סיסמה או שם משתמש. באמצעות יישומים אלה ניתן להעביר מסרים למספרים עצומים של קוראים ומשתמשים, בצורה מהירה ויעילה. נוסף על כך, פורומים שונים של פעילי ארגון אל־קאעדה ושל ארגונים אחרים צצים ומשנים כתובות במהירות בתוך אתרים מסחריים קיימים, המאפשרים פתיחת פורומים באופן חופשי (למשל יאהו). פורומים אלה מעלים תמונות, מסיתים נגד אויבי הארגון ועונים על שאלות בתחום ההלכה הדתית.

הפצת מסרים פומביים, לרבות הוראות הפעלה, באמצעות העלאת כרוזים לאינטרנט.[42] אחת הדרכים של ארגון הטרור להפיץ מסרים לפעילים שעמם הוא לא מקיים קשר רציף היא באמצעות כרוזים שמועלים לאתר האינטרנט. לעתים המסר שבכרוזים מרומז או סמוי, אך לעתים הוא גלוי, למשל הקריאה הברורה באתרי אל־קאעדה להוציא לפועל פיגועים נגד ארצות הברית. במבט ראשון זו

40 **שם**, עמ' 114.
41 **שם**, עמ' 130.
42 **שם**, עמ' 115.

נראית כאמירה כללית, אך עבור תאים רדומים הנמצאים במקומות נידחים היא עלולה להיות טריגר מוסכם לתחילת הוצאתו לפועל של פיגוע.

הפצת מידע בקרב הארגון, וכן בין ארגונים ובקרב "קהיליית הטרור", באמצעות העלאת מידע וקבצים לרשת.[43] המידע מועלה לאתרי האינטרנט הגלויים של הארגון, ולעתים הוא מופץ באמצעות תוכנות שיתוף קבצים לכל דורש. דוגמאות לשימושים כאלה: "המדריך לטרוריסט" שניתן להורדה באתר החמאס, מדריכים לגבי גיוס סוכנים, זיוף מסמכים, התקנת חגורות נפץ וכולי. במידה מסוימת, האפשרות להעביר קבצים ארוכים ומפורטים ברשת – הכוללים תמונות, תרשימים וסרטים – יכולה לשמש תחליף לתכנית אימונים במחנה מסודר שדורשת מדריכים, מקום, הסעה (או הטסה) ושהייה של פעילים. מחנה אימונים וירטואלי שכזה אכן הוקם לאחר הריסת המחנות האמיתיים באפגניסטן על ידי ארצות הברית.[44] מובן שאין בכך תחליף מלא לקורס מעשי, אך מדובר בדרך קלה ויעילה של שיתוף והפצת ידע שנצבר.

איסוף מודיעין

הרשת היא כר נוח לאיסוף מידע מודיעיני ולהעברת מידע מגוון בין פעילים ובין גופים שונים.

איסוף מידע ממקורות גלויים ברשת.[45] ברשת האינטרנט אפשר למצוא מפות של ערים ותצלומי אוויר שמספקות תוכנות חינמיות רבות. כמו כן ניתן ללמוד על לוחות זמנים של רכבות, טיסות או אוטובוסים, שעות פתיחה וסגירה של מקומות ציבוריים וכדומה. נוסף על כך, ניתן לאתר תצלומים של מקומות שונים, חלקם אפילו באמצעות מצלמות רשת שנמצאות באופן מקוון באתרים ציבוריים, וכך להשיג מודיעין לקראת פעולה עתידית. באופן דומה אפשר ללמוד ממקורות גלויים על דרכי הרכבת פצצות ומטענים, הכנת חומרי נפץ והפעלת כלי נשק שונים. הרשת אף יכולה לאפשר השגת מידע על אנשים ספציפיים, כולל תמונות ופרטים נוספים.

43 **שם**, עמ' 127.

44 **שם**, עמ' 126–127.

45 **שם**, עמ' 112.

עוד מקור מידע גלוי גדול ברשת הוא היישום Google Earth המספק תמונות לוויין מפורטות של כל מקום בכדור הארץ. בתמונות אלה ניתן גם לקבל מידע על גובה כל נקודה מעל פני הים, וכן נקודת הציון הגיאוגרפית המדויקת שלה. לפי דיווחים מחקירתו של אחד המחבלים שהשתתפו בפיגוע במומבאי בנובמבר 2008, החוליה עשתה שימוש בתצלומי לוויין ובמכשירי GPS כדי לנווט ברחובות העיר. בעקבות זאת הוגשה תביעה לבית המשפט בהודו, להורות למפעילי האתר לטשטש תמונות של נקודות רגישות במומבאי. בהקשר זה יש לציין שחוליית הטרור במומבאי היא דוגמה ל"חוליית הטרור של המאה העשרים ואחת":[46] החוליה הייתה מצוידת במכשירי טלפון סלולרי ולוויני, ב־GPS ובמכשירי בלקברי המאפשרים גלישה קלה באינטרנט. בזמן הפיגוע היו חברי החוליה בקשר עם מפעיליהם בפקיסטן שהעבירו להם עדכונים מהתקשורת ועודדו אותם להמשיך בפעולה.[47]

ניתן לומר אפוא, באופן כללי, שכשם שאפשר היום לערוך מחקר על כל נושא שעולה על הדעת ולאסוף מידע במהירות באמצעות הרשת, כך גם פעילי הטרור יכולים לאסוף מודיעין ולחקור כל נושא העולה על דעתם בצורה דומה.

איסוף מידע ממקורות שאינם גלויים. פעילי טרור יכולים להשיג מידע חסוי באמצעות פריצה לאתרים ממשלתיים או למחשבים פרטיים, וכן למאגרי מידע שאינם נגישים לציבור.

שימוש ברשת לקראת פיגועים

אפשר לעשות ברשת גם שימוש אקטיבי ממשי, בפעולות המכינות את הפיגוע. לעתים הרשת היא שמאפשרת את הפיגוע עצמו, כמו בפעולה שביצעה המחבלת אמנה מונא שפיתתה באמצעות צ'ט ברשת את הנער אופיר רחום שייפגש עמה בירושלים, וכך נחטף רחום לרמאללה ונרצח.[48] דוגמה אחרת לשימוש ברשת לקראת פיגוע היא רכישה מקוונת של כרטיסי טיסה על ידי מחמד עטא, מפקד

46 ראו http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5311241.ece

47 ראו סיכום האירוע על ידי מכון ראנד: www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf, עמ' 7.

48 Weiman, **לעיל** הערה 34, עמ' 133.

פיגועי ספטמבר 2001 בניו יורק. בשנת 2009 פרסם השב"כ אזהרה לאזרחי ישראל מפני ניסיונות גיוס שמבצעים ארגוני הטרור באמצעות רשתות חברתיות כגון facebook. החשש היה שהארגונים ינסו ליצור קשר ולפתות ישראלים לצאת לפגישה עסקית בחוץ לארץ, ושם יחטפו אותם או ינסו לגייסם.[49]

גיוס פעילים וכספים

גיוס פעילים. השלב הראשוני, החדרת מוטיבציה ושכנוע פעילים פוטנציאליים להתגייס לארגון, נעשה באמצעות תעמולה שמתנהלת על גבי האתר של הארגון. כמו כן, גולשים שיוצרים קשר ומתעניינים באתר מקבלים פנייה אישית ממנהלי האתר, וכך נוצר הקשר הראשון בין הארגון לגולש.[50]

גיוס כספים. גיוס כספים לארגוני הטרור נעשה בחלקו הגדול על ידי תרומות. פרסום חשבונות הבנק, השכנוע ושווק הארגון נעשים באמצעות אתרי האינטרנט. מפעילי האתרים מזהים גולשים שחשים אהדה כלפי הארגון ומציעים להם לתרום באמצעות תכתובות דואר אלקטרוני, בדרך כלל על ידי ארגון מתווך שפועל באופן חוקי ומציג את עצמו כבעל מטרות הומניטריות (לדוגמה, קרן שמימנה פעולות של החמאס והייתה ממוקמת בטקסס).[51] בחלק מהאתרים מופיעים מסרים שבהם הארגון מתפאר בהישגיו ולעתים אף מנסה לפרט את "מחיר" הפיגועים. באתר החמאס מופיע צלאח שחאדה (ראש הזרוע הצבאית של החמאס בעזה שחוסל על ידי ישראל ביולי 2002) ומפרט את מחיר כלי הנשק והפיגועים, מתוך מטרה לעודד את תומכי הארגון להשתתף בהוצאות ולתרום.[52]

ג. שימוש ישיר

את השימוש הישיר ברשת ניתן לחלק לשני אופנים: טרור וירטואלי ממשי, ותקיפת מחשבים.

49 ראו לדוגמה הדיווח על אזהרת השב"כ באתר **הארץ**: www.haaretz.co.il/hasite/spages/1086342.html

50 Weiman, **לעיל** הערה 34, עמ' 118–120.

51 **שם**, עמ' 135.

52 **שם**, עמ' 117.

טרור וירטואלי

המונח טרור וירטואלי מתייחס לתחום שהוא לפי שעה איום שטרם יצא לפועל.[53] מדובר בפעולות שיבוצעו באינטרנט באופן ישיר (פיגוע באמצעות המקלדת). פיגועים כאלה עלולים לגרום נזקים לתשתיות חיוניות (אנרגיה, תחבורה) וכתוצאה מכך עלולה להיגרם אף פגיעה קשה בחיי אדם (למשל עקב שיתוק צמתים מרומזרים, שיתוק השליטה במטוסים וברכבות וכדומה). תוצאה נלווית חשובה של האיום בטרור כזה היא הפחד הפסיכולוגי הקשה של אזרחים ושל רשויות, והתחושה ששום דבר אינו מוגן ובטוח.

עד היום טרם נרשם ולו פיגוע אחד כזה, אך הנושא תופס תשומת לב תקשורתית רבה בגלל הפחד הפסיכולוגי מפני הלא נודע ובשל סיבות כלכליות – לחברות רבות שמוכרות טכנולוגיות של אבטחת מידע יש אינטרס להעצים את החשש מפני סכנה זו.[54] אולם יש להכיר בכך שלעתיד לבוא מדובר בסכנה אמיתית. בביצוע פעולת טרור וירטואלית הסיכון ל"תוקף" הוא מינימלי, משום שניתן לתקוף ממרחק עצום, ולעומת זאת פוטנציאל הסכנה הוא אדיר. עם זאת נראה שנכון להיום טרם התפתחו בקרב ארגוני הטרור היכולות הדרושות לבצע טרור וירטואלי רחב היקף.

תקיפת מחשבי רשויות

אפשר להצביע על אופן פעולה נוסף שבו משתמשים פעילי הטרור באינטרנט – "הצפה" של מחשבי הממשלה והרשויות בהודעות ופניות, באופן שמקשה על פעולתם או אף מפיל את אתרי האינטרנט שלהם. סוג זה של שימוש באינטרנט, שבניגוד לסוג הקודם לא נשאר תאורטי בלבד, אינו גורם לתוצאות הרות אסון אלא מהווה מטרד בלבד ועלול לגרום גם לנזק כספי. כמו כן קשה להפריד, במקרה זה, בין טרוריסטים לבין האקרים "חובבים" ואנרכיסטים שונים, המשתמשים במתקפות על אתרי הממשלה כדי להביע מחאה או כדי להטריד.

53 **שם**, עמ' 148.

54 **שם**, עמ' 150.

5. לחימה בטרור באמצעות האינטרנט

הלחימה בטרור באמצעות האינטרנט מתמקדת בשני ראשים: התמודדות ישירה מול אתרי האינטרנט של ארגוני הטרור; ואיסוף מודיעין, בעיקר באמצעות יירוט המסרים הנשלחים באינטרנט ופענוחם.

א. התמודדות ישירה מול אתרי האינטרנט של הארגונים השונים

אחת הדרכים המרכזיות להתמודד עם הלוחמה הפסיכולוגית ופרסומי ארגוני הטרור היא סגירת אתרי האינטרנט שלהם.[55] לא אתמקד בדרך פעולה זו, שכן היא איננה קשורה בסוגיית הפגיעה בפרטיות אלא בסוגיות של חופש הביטוי. עם זאת הדיון בהמשך יושפע מהעובדה שדרך פעולה זו הוכחה כחסרת יעילות. אתרי האינטרנט שנסגרים חוזרים וקמים במהירות בכתובות אחרות. נוסף על כך, ישנן מדינות שתומכות בטרור במישרין או בעקיפין (ולענייננו, הן אינן מוכנות לפעול לסגירתם של אתרים המאוחסנים בשרתים בשטחן). כך גם לגבי פורומים שונים שנפתחים ונסגרים בקצב מהיר ביותר, אפילו על גבי אתרים של ספקים לגיטימיים (כמו יאהו).[56] לכן דרך הפעולה של סגירת אתרים או נטרולם היא לא יעילה גם בלי להיכנס לשאלת ההצדקה של פעולות כאלה בשל סוגיות של חופש הביטוי.

ב. התמודדות מודיעינית עם הטרור באינטרנט

כפי שפורט לעיל, פותחו בשנים האחרונות יכולות אדירות למעקב וליירוט תקשורות של פעילי טרור. עם זאת יש להפריד בין שתי קבוצות עיקריות של אמצעים ויכולות ולבחון כל קבוצה בנפרד מבחינת המצב המשפטי הקיים או הרצוי.

מעקב אחר כתובות דואר אלקטרוני חשודות

דרך חשובה לאיסוף מודיעין באמצעות האינטרנט היא המעקב אחר כתובות דואר אלקטרוני חשודות.[57] ההיקף ומידת ההרמטיות (המידה שבה אפשר ליירט את תכתובות הדואר האלקטרוני מהכתובת החשודה) שניתן להשיג במעקב אחר

55 **שם**, עמ' 193.

56 **שם**, עמ' 29.

57 **שם**, עמ' 182.

כתובות דואר אלקטרוני אינם גלויים לציבור. עם זאת מדובר ביכולת פשוטה לניתוח מנקודת המבט של הגנת הפרטיות, משום שמבחינה רעיונית כמעט שאין הבדל בין מעקב אחר כתובת דואר אלקטרוני חשודה, המתבצע בעקבות חשד קונקרטי כלפי המשתמש בה, ובין מעקב אחר מספר טלפון חשוד (למעט הסוגיה של דואר שנקרא שכמפורט להלן באשר לדין המצוי, נתפס לפחות בתחילת התפתחות הדין כחיפוש ולא כהאזנת סתר). מכיוון שכך, ראוי שתהיה שקילות בין הכללים שמופעלים באשר להאזנות סתר לטלפונים, ובין הכללים שייושמו לגבי מעקב אחר כתובות דואר אלקטרוני. מובן שאפשר שלא להסכים עם הכללים הקיימים היום באשר להאזנות סתר בישראל. אולם סוגיה זו מעניינת פחות בעיניי, שכן אין חידוש גדול בטכנולוגיה של הדואר האלקטרוני לעומת הטלפון, ככל שאנו עוסקים במעקב אחר כתובת אינטרנט ספציפית, החשודה בקשר לפעילות טרור. כל דיון בהצדקת האיזונים בקשר להאזנות סתר לטלפונים יהיה רלוונטי גם לגבי האינטרנט, ובמידה שווה כמעט לחלוטין.

תוכנות "רחרחניות"

בשונה ממעקב ספציפי אחר כתובות דואר אלקטרוני חשודות, תוכנות "רחרחניות" (כדוגמת Carnivore) מתחברות לספקית אינטרנט ועוברות על כל התעבורה שלה. כלומר, הבדיקה כאן היא מקפת ואינה מתבססת על חשד קונקרטי במשתמש מסוים. לתוכנות מסוג זה יש יכולות מגוונות, אך המכנה המשותף לכולן הוא שניתן לשלוף באמצעותן חומר שמעניין את רשויות האכיפה לא רק לפי כתובות מסוימות של דואר אלקטרוני, אלא לפי תוכן התכתובות או נתונים נוספים.[58] בחלק מהתוכנות מדובר גם על הצלבה של חומרים ממקורות שונים – נתוני גלישה של המשתמש (לפי כתובת ה־IP שלו), אתרים שהוא גולש אליהם, חיפושים שהוא מבצע, רכישות שעשה באמצעות הרשת, קשריו, פורומים שבהם הוא משתתף וכולי. מדובר בכלי שמאפשר לרשויות להגדיר תנאים לוגיים שלפיהם יתקבל חומר מסוים המעורר חשד – לפי תוכנו, קשריו, מאפייני הגלישה או נתונים רבים אחרים.[59] לדוגמה, ניתן לבחון תכתובות שבהן מאוזכרים כמה רכיבים המשמשים

58 **שם**, עמ' 184–185.

59 Tien, **לעיל** הערה 2, עמ' 393–396.

לייצור חומרי נפץ, בשילוב עם נתוני גלישה חשודים כגון גלישה לאתרי ארגוני טרור, השתתפות בפורומים אסלאמיים קיצוניים וכדומה.

לדעתי, התוכנות הרחרחניות הן שמעלות את השאלה המרכזית שעל הפרק – כלומר את ההתלבטות שמולה עומדות היום החברות הדמוקרטיות. בדרכן להשיג מטרות ביטחוניות של מניעת טרור, מציבות התוכנות האלה איום על הזכות לפרטיות. איום זה בא לידי ביטוי בכמה אופנים:

אגירת מידע. כדי שייווצר בסיס הנתונים שבו יכולה התוכנה לחפש ולהצליב מידע על פי תנאים לוגיים שונים, יש הכרח להקליט ולשמור את כל התעבורה בספקית האינטרנט (ולשם הגברת היעילות, יש לשמור את הנתונים מכמה ספקים לאורך זמן מסוים, ולהצליב את המידע). המשמעות המידית היא שגם כל התעבורה (תכתובות דואר אלקטרוני) של המשתמשים התמימים, שאינם חשודים בדבר, מוקלטת ונשמרת. עצם קיומו של בסיס נתונים כזה, שממנו אפשר לדלות מידע על כל גולשי האינטרנט באשר הם, הוא כשלעצמו פגיעה בפרטיות, ולטענת ארגוני זכויות האדם מדובר בפגיעה חמורה ביותר.[60] היקף המידע המצטבר על כלל האוכלוסייה הוא עצום, וחלקו הוא מידע המתייחס לגרעין הקשה של הפרטיות – מידע אינטימי ממש. כמו כן יש כאן בעיה עם התפיסה הפרוצדורלית הנוכחית שלפיה לא ניתן לבצע חיפוש או האזנות סתר בלי שקיים סוג כלשהו של חשד שבעקבותיו מבצעים את החיפוש או את האזנת הסתר.[61]

False Positive. מתוחכמות ככל שיהיו, התוכנות המדוברות עלולות להניב מפעם לפעם (וייתכן שאף בתדירות גבוהה) תוצאות שגויות. במילים אחרות, לעתים אנשים תמימים או תכתובות דואר אלקטרוני תמימות יזוהו בטעות כחשודים, בשל שימוש אקראי במילים מחשידות או בשל גלישה תמימה לאתרים מחשידים (למשל לשם צרכים אקדמיים), בצורה שתפעיל את התנאים הלוגיים המוגדרים בתוכנה (מובן שהתוכנות אמורות להיות מתוחכמות מספיק כדי למנוע תוצאות שגויות כאלה). גם אם נניח ששירותי הביטחון לא ימשיכו לעקוב אחרי המשתמשים שהתוכנה עלתה על עקבותיהם בטעות – כבר היו מפעילים אנושיים שקראו את המידע עליהם כדי לקבל את ההחלטה שמדובר

60 Weiman, **לעיל** הערה 34, עמ' 227.

61 Tien, **לעיל** הערה 2, עמ' 398.

במשתמש תמים. הפגיעה החמורה בפרטיותו של הגולש התמים כבר נגרמה. הבעיה מתחדדת כמובן בשל נטייתם של שירותי הביטחון שלא לקחת סיכונים. אין זה מובן מאליו שהם יקיימו את תנאי "המצב הרצוי" ויחדלו לעקוב אחרי המשתמש התמים שנתפס ברשת.

קשיי פיקוח. בעיה קשה בשימוש בתוכנות הרחרחניות היא הקושי האינהרנטי לפיקוח של גורם חיצוני על השימוש בתוכנה בידי הדרג המבצע.[62] בניגוד למצב בהאזנות סתר, בין בטלפון ובין בדואר אלקטרוני, שם מוגדר בבירור מה החשד ומה הנזק שצפוי להיגרם לאינטרס הפרטיות, כאשר מתבקש שימוש בתוכנות רחרחניות המצב שונה בתכלית. התנאים הלוגיים שאמורים לזהות את ה"גולש החשוד" הם מורכבים ביותר. יתרה מזו, יש להגמישם ולשנותם כל העת כדי להתאימם לתמונת המצב המודיעינית. כדי להשיג פיקוח אפקטיבי (למשל על ידי בית משפט) יהיה על הדרג המבצעי להסביר ולפרט את אופן הפעולה של התוכנה לפני בית המשפט, שיכולתו להבין את פעולת התוכנה היא מוגבלת. נוסף על כך, לשם יעילות העבודה עם התוכנה חייב הגורם המפקח לאפשר שיקול דעת מסוים לגורם המבצעי לשנות ולאלתר בהפעלת התוכנה, שכן אחרת לא יתאפשר מתן מענה למציאות המודיעינית המשתנה.

החשש הוא שבסופו של דבר לא יושג פיקוח אפקטיבי של גורם מפקח (בית משפט, שר הביטחון וכדומה). בגלל מורכבות המערכת, הקושי לצפות את כמות המידע הרלוונטי ואיכותו, והצורך בגמישות, יזכו מפעילי התוכנה לשיקול דעת נרחב בהפעלתה, ויש סכנה שהשימוש יהיה מוגזם ואולי אף ינוצל לרעה.

Profiling. בהפעלת סינון מידע על פי "מאפיינים חשודים" קיים סיכון אינהרנטי שהתוכנות ישמשו לביצוע מעקב אחרי אוכלוסיות מיעוט "חשודות" על בסיס אתני/ דתי/ תרבותי, פרקטיקה המכונה profiling. פרקטיקה זו פוגעת בשוויון ומהווה למעשה אפליה פסולה כלפי מגזרים חשודים. יש לציין שגם אם השימוש בתוכנות נעשה בתום לב, מעצם העובדה שהיום עיקר הטרור הגלובלי הוא אסלאמי, עלולה להיות נטייה לראות כחשוד כל משתמש אינטרנט אסלאמי הגולש לאתרים אסלאמיים, ומכאן קצרה הדרך ל-profiling.

62 D. J. Solove, "Electronic Surveillance Law", *George Washington Law Review* 72 (2004), pp. 1269–1270

6. מגבלות משפטיות על איסוף מודיעין – המשפט הישראלי

א. הזכות לפרטיות

הזכות לפרטיות מוזכרת במשפט הישראלי בהקשרים רבים, אף שעד היום לא הוגדרה בחוק או בפסיקה באופן מדויק. המשנה לנשיא (כתוארו אז) אהרן ברק התייחס לשאלת היקפה של הזכות בבג"ץ דיין:

> הזכות החוקתית לפרטיות משתרעת בין השאר – ובלא כל ניסיון להקיף את הזכות על כל היבטיה – על זכותו של אדם לנהל את אורח החיים בו הוא חפץ בד' אמות ביתו, בלא הפרעה מבחוץ. ביתו של אדם הוא מבצרו, ובגדריו הוא זכאי לכך כי יניחו אותו לעצמו, לפיתוח האוטונומיה של הרצון הפרטי שלו [...] הזכות לפרטיות נועדה על כן, להבטיח כי אדם לא יהא שבוי בביתו, ולא יהא אנוס לחשוף עצמו בביתו להפרעות שאין הוא רוצה בהן [...] זכות הפרטיות מותחת את הקו בין הפרט לבין הכלל, בין "האני" לבין החברה. היא משרטטת מתחם אשר בו מניחים את הפרט לנפשו, לפיתוח "האני" שלו, בלא מעורבות של הזולת.[63]

הזכות לפרטיות עוגנה בחוק יסוד: כבוד האדם וחירותו. ההכרה בה כזכות חוקתית מחייבת שכל פגיעה בה תיעשה אך ורק לפי התנאים שנקבעו בפסקת ההגבלה שבסעיף 8 לחוק היסוד, כלומר "בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שאינה עולה על הנדרש או לפי חוק כאמור מכוח הסמכה מפורשת בו". חוק היסוד אינו מאפשר ביטול חוקים שהיו קיימים במועד כניסתו לתוקף ואשר התירו במפורש פגיעה בזכות לפרטיות, גם אם הם אינם עומדים בתנאים של פסקת ההגבלה.[64]

63 בג"ץ 2481/93, **יוסף דיין נ' ניצב יהודה וילק ו־5 אח'**, פ"ד מח (2), 456, עמ' 469–470.

64 ראו סעיף 10 לחוק יסוד: כבוד האדם וחירותו. עם זאת קבע בית המשפט כי יש לפרש חוקים קיימים ברוח חוקי היסוד.

בשנת 1981, עוד בטרם הפכה הזכות לפרטיות לזכות חוקתית, חוקקה הכנסת את חוק הגנת הפרטיות שקבע שפגיעה בזכות היא עברה פלילית ועוולה אזרחית. החוק אינו מגדיר את היקף הזכות ובמקום זאת מונה 11 מעשים שייחשבו לפגיעה בפרטיות, כולל מעקב אחרי אדם העלול להטרידו, האזנה אסורה על פי חוק, צילום אדם ברשות היחיד, הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם ועוד. החוק אינו חל על רשויות הביטחון – המשטרה, אגף המודיעין בצה"ל, המשטרה הצבאית, השב"כ והמוסד – בכל הנוגע ל"פגיעה שנעשתה באופן סביר במסגרת תפקידם ולשם מילויו".[65]

חוק הגנת הפרטיות אינו מגביל איסוף של מידע, אולם פרק ב בו עוסק במאגרי מידע וקובע חובת רישום שלהם. גם בנושא זה ההגנות על הזכות לפרטיות אינן חלות על פעולות של שירותי הביטחון. למשל, החוק קובע כי רשם מאגרי המידע ינהל פנקס שיהיה פתוח לציבור, ובו יירשמו כל מאגרי המידע. כאשר המאגר שייך לרשות ביטחון, רק זהות בעל המאגר ומטרות הקמתו יהיו גלויים, ואילו סוגי המידע, דרכי קבלתו ומהותו ייוותרו חסויים. נוסף על כך, החוק מעגן את זכותו של כל אדם לעיין במידע הקיים עליו במאגרי המידע, אולם זכות זו אינה חלה על מאגרי מידע של רשויות הביטחון, וממילא מתבטלת גם הזכות לתקן את המידע אם הוא מוטעה.[66] שירותי הביטחון גם פטורים מההגבלות המוטלות על גופים ציבוריים אחרים בנוגע לקבלת מידע הנדרש להם ולהעברת המידע שהם אוספים. סעיף 23 ב לחוק קובע שהם רשאים לקבל ולהעביר מידע באופן חופשי, כל עוד הדבר נחוץ לצורך מילוי תפקידם ולא נאסר במפורש בחוק.

סמכות כזו עוגנה למשל בחוק השב"כ, המעגן את סמכות השב"כ לקבל נתונים מספקי האינטרנט "למעט תוכן שיחה כמשמעותו בחוק האזנת סתר", אולם כולל כתובות דואר אלקטרוני, מספרי טלפון וכדומה – אם ראש הממשלה קבע שהנתונים נחוצים לשב"כ לצורך מילוי תפקידיו. השימוש במידע ייעשה בהיתר מיוחד מראש השב"כ, לאחר שמצא שהדבר נחוץ לצורך מילוי תפקידי השב"כ. בהיתר יפורטו "ככל הניתן" פרטי המידע הנדרש, המטרה לה הוא נחוץ

65 חוק הגנת הפרטיות, תשמ"א-1981, סעיף 19.

66 **שם**, סעיפים 12 ו־13.

ופרטי מאגר המידע שבו הוא מופיע. כל הֵיתר יכול להינתן לתקופה של שישה חודשים, הניתנת להארכה. דיווח על היתרים כאלה יינתנו אחת לשלושה חודשים לראש הממשלה וליועץ המשפטי לממשלה, ואחת לשנה לוועדת הכנסת לענייני השב"כ.[67]

ב. הגבלות על איסוף מידע

האם חוקים העוסקים בביצוע חיפושים והאזנות על ידי שירותי הביטחון מעניקים הגנות רחבות יותר לזכות לפרטיות? שני חוקים עוסקים באיסוף מידע הנחשב לתוכן. הראשון הוא פקודת סדר הדין הפלילי (מעצר וחיפוש) המסדירה תפיסת מסמכים, והשני הוא חוק האזנת סתר המסדיר עריכת האזנות בזמן אמת.

פקודת סדר הדין הפלילי

חיפוש במחשב חייב להיעשות מכוחו של צו חיפוש שניתן על ידי שופט בית משפט השלום. צו כזה יינתן, בין השאר, כאשר החיפוש נחוץ לצורכי חקירה, משפט או הליך אחר, או כאשר לשופט יש יסוד להניח שהחפץ משמש לביצוע פעולות לא חוקיות. צו המתיר חיפוש במחשב חייב לציין במפורש את ההיתר לחדור למחשב, את תנאי החיפוש ואת מטרותיו. החוק מציין שקבלת מידע מתקשורת בין מחשבים במהלך החיפוש לא תיחשב להאזנת סתר.[68]

רף ההוכחה הנדרש מרשויות אכיפת החוק המבקשות צו החיפוש הוא נמוך. הן אינן נדרשות לפרט את טיב החומר שאותו הן מחפשות, ודי שיציינו בבקשה שעל צו החיפוש לכלול היתר לחדירה למחשב. החוק אינו דורש שהחיפוש יהיה האמצעי האחרון, לאחר שאמצעים אחרים לא השיגו את המטרה. החוק גם אינו מנחה את השופט לגבי השיקולים שעליו להתחשב בהם טרם אישור הבקשה או לגבי האיזונים שהוא נדרש לעשות.[69]

67 סעיף 11 לחוק שירות הביטחון הכללי, תשס"ב-2002.

68 סעיפים 23 ו־23א לפקודת סדר הדין הפלילי (מעצר וחיפוש) (נוסח חדש) תשכ"ט-1969. ראו גם איינהורן ואח', **לעיל** הערה 23, עמ' 85.

69 נ' קוזלובסקי, **המחשב וההליך המשפטי: ראיות אלקטרוניות וסדרי דין** (תל אביב: לשכת עורכי הדין בישראל, 2000), עמ' 64-65.

דרך פוגענית פחות להשגת חומר הנמצא במחשב מופיעה בסעיף 43 לפקודה. כאשר המידע נמצא אצל צדדים שלישיים, כמו למשל אצל ספקי שירות אינטרנט, אפשר לדרוש מהם ישירות את המידע וכך להימנע מהצורך לחפש בכל המסמכים במחשב ולהיחשף לפריטי מידע רבים שאינם נחוצים לחקירה.[70]

חוק האזנת סתר

חוק האזנת סתר מסדיר האזנות לשיחות הכוללות שיחות בטלפונים רגילים וניידים, במכשירי קשר ובפקסים, וכן תקשורת בין מחשבים.[71] החוק קובע איסור כללי שלפיו האזנה לשיחה ללא הסכמת מי מבעלי השיחה היא עברה פלילית שדינה חמש שנות מאסר. לאיסור זה נקבעו כמה חריגים.

החריג הראשון מתייחס להאזנה לשיחות שנעשו ברשות הרבים. האזנה כזו אינה דורשת היתר מיוחד כל עוד היא נעשית על ידי מי שהוסמך לכך "מטעמים של ביטחון המדינה" או "לשם מניעת עברות או גילוי עבריינים". "רשות הרבים" מוגדרת בחוק "מקום שאדם סביר יכול היה לצפות ששיחותיו יישמעו ללא הסכמתו" – מבחן אובייקטיבי.[72] בתקנות נקבע שהסמכה כזו יכולה להינתן גם בדיעבד, אם לא הייתה אפשרות אחרת.[73]

החריג השני מתייחס להאזנות לשיחות שנעשות ברשות הפרט. על פי החוק, בשני מקרים בלבד תותר האזנת סתר: למטרת מניעת עברות וגילוי עבריינים ולמטרת ביטחון המדינה. כאשר ההאזנה נעשית לצורכי אכיפת חוק רגילה, היא חייבת להיות מאושרת על ידי נשיא בית משפט מחוזי או סגנו. צו כזה יינתן רק אם השופט שוכנע, "לאחר ששקל את מידת הפגיעה בפרטיות", שהדבר דרוש לצורכי חקירה או למניעת עברות מסוג פשע. הצו חייב לציין, אם הפרטים ידועים, את שם האדם לו מותר להאזין או את זהות הקו לו מאזינים ואת מקום השיחות. כן יפורטו בצו דרכי ההאזנה. כל צו יינתן לתקופה של עד שלושה חודשים, הניתנת להארכה. בכל חודש על מפכ"ל המשטרה לדווח ליועץ

70 **שם**, עמ' 62.
71 סעיף 1 לחוק האזנת סתר, תשל"ט-1979.
72 **שם**, סעיף 8. ראו בעניין זה גם Gross, **לעיל** הערה 3, עמ' 60.
73 תקנה 2 לתקנות האזנת סתר, תשמ"ו-1986.

המשפטי לממשלה על מספר ההיתרים שניתנו ופעם בשנה על השר לביטחון פנים לדווח לוועדת החוקה, חוק ומשפט של הכנסת על מספר הבקשות שהוגשו ומספר ההיתרים שניתנו, כולל מספר האנשים ומספר הקווים שלהם התירו האזנה.[74] במקרים דחופים, כאשר מפכ"ל המשטרה משוכנע שלא ניתן לדחות את ההאזנה עד לקבלת צו משופט, הוא רשאי להתיר האזנת סתר לתקופה שלא תעלה על 48 שעות. היועץ המשפטי לממשלה רשאי לבטל היתר זה ושופט בית משפט מחוזי יכול לאשר אותו בדיעבד.[75]

האזנה מטעמים של ביטחון המדינה נעשית על סמך אישור של ראש הממשלה או שר הביטחון, לבקשת ראש השב"כ או ראש המודיעין הצבאי, ללא צורך בהליך שיפוטי. גם בהיתר זה צריך לציין את זהות האדם לו הותרה ההאזנה, או את זהות הקו ואת מקום השיחות. כן יש לפרט את דרכי ההאזנה.[76] אישור כזה ניתן אף הוא לתקופה של עד שלושה חודשים, הניתנת להארכה. אחת לשלושה חודשים על שר הביטחון לדווח ליועץ המשפטי לממשלה על היתרים שניתנו לפי החוק, ופעם בשנה יימסר דיווח על מספר ההיתרים שניתנו לוועדה משותפת של ועדת חוקה, חוק ומשפט וועדת חוץ וביטחון, היושבת בדלתיים סגורות.[77] במקרים דחופים יכולים ראש השב"כ או ראש אגף המודיעין של צה"ל להתיר האזנה כזו לתקופה של עד 48 שעות והיועץ המשפטי לממשלה, שר הביטחון או ראש הממשלה רשאים לבטל היתר זה.[78]

אף שאין כלל ביקורת שיפוטית על האזנות סתר מטעמי ביטחון המדינה, בהיבט אחד לפחות – כפי שראינו – החוק מקשה על רשויות האכיפה: לא ניתן (אלא על פי פרשנות יצירתית של חוק האזנת סתר) להפעיל תוכנה המסננת דואר אלקטרוני לפי תוכן. עם זה מובן שהחוק מקל מאוד על השגת היתרי האזנות סתר ספציפיות, שכן אין כל צורך בפיקוח ובאישור של בית המשפט אלא בהוראה של הרשות המבצעת עצמה (שר הביטחון וראש הממשלה).

74 סעיף 6 לחוק האזנת סתר, תשל"ט-1979.
75 **שם**, סעיף 7.
76 **שם**, בסעיף 4 (ב).
77 **שם**, סעיף 4.
78 **שם**, סעיף 5.

יש לציין שחלק גדול מהמידע – שאינו תוכן של דואר אלקטרוני – שבו משתמשות התוכנות הרחרחניות לשם איתור ומעקב אחרי גולשים חשודים, הוא כזה שהרשויות יכולות לקבלו מחברות האינטרנט ומבזק בלי להיות כפופות לחוק האזנת סתר, כמפורט להלן.

ג. חוק נתוני תקשורת

בסוף שנת 2007 נחקק חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007. חוק זה זכה לכינוי המפוקפק "חוק האח הגדול" (להלן: חוק נתוני תקשורת). החוק רלוונטי לשאלת הפגיעה בפרטיותם של משתמשי האינטרנט, אך כפי שיוסבר להלן, הוא אינו מתיר סינון והאזנת סתר על פי תוכן של תכתובות דואר אלקטרוני, ולכן לא שינה את המצב המשפטי הבסיסי בשאלה שבה מתמקד מאמר זה.

החוק מאפשר לרשויות האכיפה לקבל, לפי עילות כלשהן, נתונים ממאגרי מידע (של חברות התקשורת) לשם גילוי עברות ועבריינים ולהצלת חיי אדם. הנתונים כוללים איכון של טלפונים סלולריים, פירוט שיחות (כולל איתור מספרי היעד והמקור) ונתונים של מנויי/ משתמשי אינטרנט (מספרי תעודות זהות, כתובות). דרך המלך לקבלת המידע היא על ידי צו של שופט בית משפט שלום, אם כי במקרים דחופים של מניעת עברות מסוג פשע או הצלת חיי אדם, ניתן לקבל נתונים גם לפי בקשת שוטר בלבד, באישור קצין מוסמך (בדרגת סגן ניצב ומעלה שהוסמך לכך על ידי המפכ"ל). כמו כן, המשטרה רשאית לקבל מחברות התקשורת את "ספר הטלפונים" המלא שלהן ועוד נתונים כלליים על הרשת.

חשוב להבין שהחוק מאפשר היום לרשויות החוקרות נגישות רחבה מאוד לנתוני תקשורת. יש לצרף לכך את העובדה שבימינו נתוני תקשורת – אף שאינם תוכן – מגלים פרטים רבים שנחשבים לפרטיים מאוד: עם מי אנו מדברים, איפה היינו, מהם הרגלי הגלישה שלנו, מי הם אנשי הקשר שלנו וכולי. עם זאת יש לציין שחוק זה **אינו מאפשר** למשטרה לסנן תכתובות דואר אלקטרוני **לפי תוכנן**. בדומה לצווי האזנות הסתר, גם החומר שמועבר לפי חוק נתוני תקשורת הוא לגבי אדם ספציפי, מנוי אינטרנט או מספר טלפון.

ככלל, ראיות שהושגו על ידי האזנת סתר בניגוד לתנאים שנקבעו בחוק לא יהיו קבילות כראיה בבית המשפט. החוק מאפשר חריגים לכלל זה לפי חוק האזנת סתר או – כאשר מדובר בפשע חמור – לאחר שבית המשפט דן וקבע שהן יהיו קבילות, לאחר ששוכנע כי "הצורך להגיע לחוק האמת עדיף על הצורך להגן על הפרטיות".[79]

ד. איזה חוק חל על איזה סוג של מידע?

ההבחנה בין חיפוש לבין האזנת סתר אינה תמיד ברורה. הבעיה העיקרית נוגעת למעמדו של דואר אלקטרוני שטרם נקרא על ידי הנמען: האם קריאתו תיחשב להאזנת סתר או שיש צורך בהליכים לפי פקודת סדר הדין הפלילי? אין מחלוקת על הקביעה שבדרכה לשרת של הנמען ההודעה מוגנת על ידי חוק האזנת סתר. כן אין מחלוקת על הקביעה שלאחר שההודעה נקראה על ידי הנמען, רשויות אכיפת החוק יוכלו להסתפק בצו חיפוש רגיל לצורך קריאתה. השאלה מתעוררת רק בנוגע לזמן שבו ההודעה ממתינה על ספק השירות של הנמען.[80] יש לציין שבכל מקרה שאלה זו איננה רלוונטית לגבי השימוש בתוכנות רחרחניות, שאמורות לסנן על פי תוכן ולא על פי צו ספציפי, בין של חיפוש ובין של האזנת סתר.

בישראל עמדה שאלה זו במרכזם של שני פסקי דין. בעניין **בדיר** הורשעו שלושה אחים בהאזנת סתר אסורה לאחר שנקבע שהם האזינו להודעות בתאי טלפון קוליים.[81] בעניין **נטוויז'ן**[82] פנתה המדינה לבית משפט השלום, והוא אישר את בקשתה לצו חיפוש. הצו הורה לחברת נטוויז'ן להעביר לצה"ל, לצורך חקירה סמויה שהוא ניהל, את כל הודעות הדואר האלקטרוני הנמצאות בתיבות של ארבעה מנויים של החברה וכן את כל ההודעות שיגיעו למנויים אלה בשישים הימים שמיום מתן הצו. נטוויז'ן ערערה על ההחלטה וטענה, בין השאר, שאין הבדל בין תא קולי לתא דואר אלקטרוני ולכן המדינה מציגה שתי עמדות סותרות. למעשה, המדינה "ביקשה להרשיע את הנאשם [בעניין **בדיר**] בפעולה

79 **שם**, סעיף 13 .

80 למחלוקת זו ראו קוזלובסקי, **לעיל** הערה 69, עמ' 95–96.

81 ת"פ 40250/99 (מחוזי ת"א), **מדינת ישראל נ' מונדיר בן קאסם בדיר ואח'** (2001).

82 בש"פ 98606/00 (מחוזי ת"א) **נטוויז'ן נ' צה"ל** (2000).

שלדעת פרקליטת המדינה אינה מהווה לכאורה האזנת סתר אסורה".[83] כן טענה נטוויז'ן שהעברת הודעות שטרם התקבלו אצלה דורשת אף היא צו לפי חוק האזנת סתר. הערעור נדחה ונטוויז'ן ערערה למחוזי בטענה, בין השאר, שפסיקת בית משפט השלום מייתרת את חוק האזנת סתר.[84]

עוד בטרם נידון הערעור שינתה פרקליטת המדינה דאז עדנה ארבל את המדיניות הרשמית. לפי המדיניות החדשה, תפיסת דואר אלקטרוני שטרם הגיעה לשרת של ספק האינטרנט מחייבת צו לפי חוק האזנת סתר. לעומת זאת, כדי לקרוא דואר אלקטרוני הנמצא אצל ספק השירות די בצו חיפוש של בית משפט שלום.[85]

באפריל 2003, במסגרת ערעור לבית המשפט העליון, חזרה בה המדינה מאישומם של האחים בדיר בהאזנת סתר אסורה והסכימה לזכותם.[86] בית המשפט העליון נמנע מלנקוט עמדה בנוגע לחוק שיש להחיל על מקרים כאלה, כך שבדומה למצב בארצות הברית – שאלה זו טרם הוכרעה על ידי בתי המשפט.

שאלה נוספת מתעוררת בנוגע לציתות לשיחות המתנהלות ברשת האינטרנט (צ'טים). בעניין זה נקבע כי כאשר השיחה נגישה לציבור הרחב, "קליטת המידע על ידי רשויות החקירה אינה משום האזנת סתר ואינה זקוקה להיתר. שכן בנסיבות אלה אין לומר כי קמה לאדם צפייה סבירה ששיחותיו לא תישמענה, וניתן אף לומר כי הפך את כל שומעיו הפוטנציאליים לשותפים לשיחה".[87] אולם כלל זה מתעלם מכך שהציפייה לפרטיות אינה נוגעת לתוכנם של הדברים, שלגביהם

83 ראו עו"ד חיים רביה, "תיק בדיר: פסיקה עקרונית, מחייבת שיקול מחודש של מדיניות הפרקליטות בנושא האזנה לדואר אלקטרוני", 11.9.2001:
www.law.co.il/articles/criminal-law/2001/09/11/172

84 לדיון בטענות הערעור ראו במאמרו של מי שייצג את נטוויז'ן בהליכים אלה, עו"ד חיים רביה, "ההגנה על הפרטיות בדואר אלקטרוני בישראל", 23.4.2000:
www.law.co.il/articles/privacy/2000/04/23/42

85 עו"ד חיים רביה, "לא ידו הארוכה של החוק", 27.6.2000:
www.law.co.il/articles/privacy/2000/06/27/40

86 ע"פ 10343/01, **מונדיר בדיר נ' מדינת ישראל**, תק־על 2003 (2), 649.

87 קוזלובסקי, **לעיל** הערה 69, עמ' 90–91.

ברור לגולשים שהם נקראים על ידי אנשים רבים אחרים. הציפייה לפרטיות קשורה דווקא לכך שלא ניתן לזהותם ולקשר את הדברים אליהם. אנונימיות זו היא המאפשרת להם להתבטא בחופשיות ולומר דברים שהיו נמנעים מהם לו זהותם הייתה גלויה.

ה. פיקוח על שירותי הביטחון

במסגרת איסוף המידע פטורים היום שירותי הביטחון כמעט מכל ביקורת חיצונית. כתוצאה מכך, הציבור אינו יכול לדעת כיצד מנצלים שירותי הביטחון את הסמכויות הנרחבות שהוענקו להם בחוק. אי־אפשר לדעת איזה סוג של מידע נמסר להם מספקי השירות, באיזו תדירות, לאילו מטרות הוא משמש ולאיזה תקופות נשמר מידע זה. לא ידוע כמה האזנות סתר מבצעים שירותי הביטחון בכל שנה, ובעיקר אי־אפשר לדעת אם שירותי הביטחון עומדים בדרישות המינימליות שהחוק מציב לפניהם.

חובות הדיווח בחוק הן מינימליות ומתמצות במסירת דיווחים תקופתיים כלליים וסודיים ליועץ המשפטי לממשלה ולוועדות בכנסת. לגורמים אלה לא הוענקו כל סמכויות ביקורת או אכיפה, ולא ברור מהן דרכי הפעולה העומדות לפניהם כאשר הם סבורים ששירותי הביטחון חרגו מסמכותם.

7. משפט משווה

א. המשפט האמריקני

ההגנה החוקתית על הזכות לפרטיות

הזכות לפרטיות אינה מעוגנת במפורש בחוקה האמריקנית, אולם בית המשפט העליון האמריקני קבע שהסעיפים הקיימים, ובעיקר התיקון הרביעי לחוקה, מגִנים עליה. תיקון זה אוסר על חיפוש לא סביר ועל הוצאת צו חיפוש כללי, בדומה לזה שהתיר לפני הכרזת העצמאות האמריקנית למלך הבריטי ולנציגיו להיכנס לכל בית שיחפצו, בכל עת שימצאו לנכון, בלי שיהיה להם חשד ספציפי על פשע שהתבצע או עומד להתבצע. בתי המשפט האמריקניים פסקו שחיפוש כזה פוגע בזכות לפרטיות. על מנת שהחיפוש יהיה חוקי, עליו להיעשות בכפוף

לצו בית משפט אשר יגדיר את היקפו. הצו יינתן רק לאחר שהממשלה הראתה עילה מסתברת שבוצע פשע ושהמידע המבוקש חיוני לצורך החקירה, או שסביר שעומד להתבצע פשע והמידע חיוני לצורך מניעתו.[88]

בתחילה שימש התיקון הרביעי לצורך הגנה על הפרטיות רק בתוך ביתו של אדם, ובית המשפט העליון פירש את המונח "חיפוש" כמצריך כניסה פיזית לשטח פרטי או כאשר מדובר בחיפוש על גופו של אדם. אולם ככל שהתפתחו טכנולוגיות המעקב התברר כי תפיסה זו צרה מדי והיא מאפשרת פגיעה יחסית נרחבת בזכות לפרטיות. לכן ב־1967 הרחיב בית המשפט העליון את ההגדרה של "חיפוש" וקבע מבחן כפול: מבחן סובייקטיבי – האם הייתה ציפייה של האדם לפרטיות? ומבחן אובייקטיבי – האם ציפייה זו היא סבירה? רק בהתקיים שני תנאים אלה תידרש הממשלה לקבל צו חיפוש מבית המשפט. על בסיס מבחן זה נקבע שיש צורך בצו לצורך ציתות לשיחות טלפון, אף שהדבר אינו כרוך בכניסה פיזית לשטחו של אדם.[89]

עם זאת בית המשפט העליון פירש את המבחן פירוש מצומצם וקבע שכאשר אדם מסר מידע כלשהו לצד שלישי, לא יכולה להיות לו עוד ציפייה סבירה לפרטיות, ולכן אין צורך בצו חיפוש לצורך השגת המידע. על בסיס עיקרון זה קבע בית המשפט, למשל, כי התיקון הרביעי אינו מונע מהרשויות לפנות לחברות הטלפון ולקבל מהן נתונים על כל מספרי הטלפון שחויגו ממכשיר מסוים, שכן הלקוח כבר מסר להן מידע זה לצורך קבלת השירות. בדומה, בית המשפט קבע כי רשומות פיננסיות אינן מוגנות תחת התיקון הרביעי שכן אדם מסר את המידע לבנק.[90]

הלכה זו מצמצמת באופן ניכר את ההגנה של החוקה על הזכות לפרטיות באינטרנט. כל המידע שמסרו המנויים לספקי השירות, כולל מידע הנדרש לצורך קבלת השירות, יכול להיות מועבר לרשויות בלי צורך בצו חיפוש. הממשלה יכולה לקבל מידע זה בלי קשר לשאלות כגון: עד כמה נרחבת החדירה

88 לדיון בדרישות התיקון הרביעי ראו Rosen, **לעיל** הערה 33, עמ' 611; Tien, **לעיל** הערה 2, עמ' 400–402.

89 (*Katz v. United States*, 389 U.S. 347 (1967

90 לסקירה של פסקי הדין השונים לפי הלכה זו ראו דוח *TAPAC*, **לעיל** הערה 7, עמ' 23; Solove, **לעיל** הערה 1, עמ' 1435–1437.

לפרטיות? האם מסירת המידע הייתה רצונית? מהו המידע החדש המתגלה על האדם כתוצאה מהצלבת המידע הקיים אודותיו? הלכה זו גם שוללת את ההגנה על המידע, כאשר הצד השלישי נדרש למסור אותו בניגוד לרצונו ובניגוד להבטחתו שלא לעשות בו שימוש אחר (מלבד השירות המסופק).[91]

ההגנה בחוק על הזכות לפרטיות

ההגנה החוקתית המוגבלת שהעניק בית המשפט העליון האמריקני לזכות לפרטיות הביאה את הקונגרס לחוקק חוקים בניסיון לספק בכל זאת הגנה כלשהי. שני חוקים עוסקים בתקשורת אלקטרונית: החוק הראשון – The Electronic Communications Privacy Act (ECPA), משנת 1986 – נועד להסדיר את גישתן של רשויות אכיפת החוק למידע במסגרת חקירות פליליות. השני – The Foreign Intelligence Surveillance Act (FISA), משנת 1978 – מסדיר איסוף של מודיעין חוץ. באוקטובר 2001, לאחר הפיגוע במגדלי התאומים, חוקק הקונגרס את ה־Patriot Act שבמסגרתו נעשו בחוקים אלה שינויים שהרחיבו את סמכויות שירותי הביטחון. חלק ניכר משינויים אלה לא היו קשורים כלל לפיגוע, וחלקם אף נדחו בעבר על ידי הקונגרס בשל הפגיעה הנרחבת שלהם בזכויות האדם.[92]

חוקים אלה, שייסקרו להלן, נתונים לביקורת קשה בשל פגיעתם הנרחבת בזכות לפרטיות ובשל הסמכויות הנרחבות שהם מעניקים לשירותי הביטחון.[93] אולם גם התומכים בעקרונות הכלליים שנקבעו בהם מבקרים אותם בטענה שהם מיושנים ואינם מתאימים להתפתחויות הטכנולוגיות של השנים האחרונות.

Electronic Communication Privacy Act (ECPA)

החוק מורכב משלושה חלקים. חלק אחד – The Stored Communication Act – מגן על הזכות לפרטיות בתקשורת מאוחסנת. שני החלקים האחרים –

91 O. Kerr, "A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It", *George Washington Law Review* 72 (2004), pp. 1209–1212; וכן Rosen, **לעיל** הערה 33, עמ' 615.

92 Solove, **לעיל** הערה 27, עמ' 1277; P. Swire, "The System of Foreign Intelligence Surveillance Law", *George Washington Law Review* 72 (2004), p. 1311

93 ראו, למשל, דוח *ACLU*, **לעיל** הערה 31.

The Wiretap Act ו־The Pen Register Statute – מגִנים על הזכות לפרטיות בתקשורת בזמן אמת. כתוצאה מחלוקה זו, תקשורת העוברת ברשת כפופה לחוקים שונים. הסיבה העיקרית לחלוקה זו היא האמצעים השונים הנדרשים כדי להשיג את המידע. כדי להגיע לתקשורת נייחת יש לפנות לספק השירות על מנת שיאתר את המידע הנדרש במחשבים שלו. לעומת זאת השגת תקשורת בתנועה היא תהליך מתמשך הדורש התקנה של תוכנה מרחרחת המותקנת על המחשב של ספק השירות.[94]

חוק האזנת סתר (The Wiretap Act)

החוק אוסר על צד שלישי, כולל רשויות אכיפת החוק, ליירט תקשורת פרטית בין שני צדדים אלא בהתקיים אחד החריגים המנויים בחוק. החוק חל על כל סוגי התקשורת והוא אוסר על האזנה בכל מקום – בביתו של אדם, בעבודה, במשרדי ממשלה, בבית הכלא או באינטרנט. על פי החוק, בקשה לצו האזנה תוגש רק לאחר שניתן לה אישור בדרג גבוה בתוך משרד המשפטים. בית המשפט יאשר את הצו רק אם השתכנע שיש probable cause (יסוד סביר/ עילה מסתברת) שפשע בוצע, מבוצע או עתיד להתבצע, וששיטות חקירה אחרות שפוגעות פחות בזכויות האדם לא יביאו להשגת אותה מטרה. החוק כולל רשימה של פשעים שבגינם ניתן לבקש צו כזה, וב־Patriot Act הוספו לרשימה עברות נוספות. במהלך ביצוע הצו, על רשויות אכיפת החוק לוודא שהאזנה לתקשורת שאינה רלוונטית היא מינימלית, ויש להפסיק את ביצוע ההאזנה מיד לאחר שהושגה המטרה. כל צו מוגבל לתקופה של שלושים יום. במקרים שבהם מפרה הממשלה את החוק, היא תיקנס והראיות שהושגו בניגוד לחוק ייפסלו.[95]

על אף תנאים מחמירים אלה, בתי המשפט כמעט שאינם מסרבים לבקשות לצווי האזנה שהוגשו על פי חוק זה. בין 1968 ל־2002 אישרו בתי המשפט

94 Kerr, **לעיל** הערה 91, עמ' 1231–1232.

95 U.S. Department of Justice, Computer Crime and Intellectual Property Section (Criminal Division), *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, July 2002, § IV.D.3 (להלן: *DOJ Manual*). ראו גם Solove, **לעיל** הערה 27, עמ' 1282; McCarthy, **לעיל** הערה 29, עמ' 844.

29,250 ציתותים (9,238 במסגרת חקירות פדרליות ו־19,322 במדינות) וסירבו רק ל־32 בקשות. מאז 1980 גדל מספר הבקשות בהתמדה.[96]

The Pen Register Statute

חוק זה נועד לספק הגנה מסוימת לנתוני תקשורת, כמו רשימת מספרי טלפון שחויגו, אך ספק אם מטרה זו מושגת. על פי החוק, על הממשלה להשיג צו משופט פדרלי כדי לקבל את המידע. הצו יינתן אם הרשויות הוכיחו שהמידע שהן מבקשות רלוונטי לחקירה פלילית שהן מקיימות. בית המשפט אינו אמור לבצע בחינה עצמאית של העובדות, ולכן קשה לראות כיצד יכולה הממשלה להיכשל בבקשה מסוג זה. צו לפי החוק יינתן לתקופות מתחדשות של שישים ימים. הפרה של החוק על ידי הממשלה לא תביא לפסילת הראיות, והתרופה היחידה היא תביעה פלילית.[97]

במסגרת השינויים שנעשו ב־Patriot Act הורחב החוק גם לרשת האינטרנט, אם כי היו שופטים שפירשו כך את החוק עוד לפני כן. היום מאפשר החוק לרשויות לקבל מידע בזמן אמת על כל הכתובות שאליהן שלח אדם דואר אלקטרוני, הכתובות שמהן קיבל דואר, כתובות ה־IP שביקש – כל זאת בלי שקיים נגדו חשד כלשהו וכמעט ללא ביקורת שיפוטית.[98]

The Stored Communications Act (SCA)

פסיקת בית המשפט העליון שלפיה התיקון הרביעי אינו מגן על מידע המאוחסן במחשבים של ספקי השירות אפשרה לממשלה להשיג מידע זה כמעט בלי הגבלות. נוסף על כך רשאים ספקי השירות, בהיותם גוף פרטי, למסור לממשלה כל מידע שהם חפצים בלי הגבלות. כדי לסתום לקונות אלה ולספק לגולשים הגנה מסוימת על פרטיותם נחקק חוק זה. הוא קובע שורה של כללים סבוכים

96 דוח *TAPAC*, **לעיל** הערה 7, עמ׳ 27.

97 *DOJ Manual*, **לעיל** הערה 95, סעיף IV.C. ראו גם Solove, **לעיל** הערה 27, עמ׳ 1288–1289; Kerr, **לעיל** הערה 26, עמ׳ 632.

98 סעיף 216 ל־Patriot Act. לדיון בהשלכות של הרחבת החוק, ראו דוח *ACLU*, **לעיל** הערה 31, עמ׳ 9; Kerr, **לעיל** הערה 26, עמ׳ 633–634.

המגבילים את סמכות הממשלה לדרוש מספקי השירות למסור להם מידע ואת סמכותם של ספקי השירות למסור לממשלה מידע על מנוייהם.[99]

תחולתו של החוק מוגבלת. ההגנה שלו משתרעת רק על מידע המאוחסן באופן זמני על ידי ספק השירות במהלך העברת המידע. למשל, הודעות דואר אלקטרוני שכבר נקראו על ידי הנמענים אינן מוגנות על ידי החוק. מאחר שרוב האנשים נוהגים לשמור עותק מהודעות הדואר שלהם אצל ספק השירות גם לאחר קריאתן, החוק מאפשר למעשה לממשלה לגשת לתקשורת רבה עם מעט מאוד הגבלות.[100]

ההגנה שמעניק החוק לזכות לפרטיות פחותה באופן משמעותי מזו שמעניק לה חוק האזנת הסתר. על פי החוק, הממשלה יכולה לבקש מבתי המשפט סוגים שונים של צווים שיאפשרו לה גישה למידע הנמצא אצל ספק השירות. העיקרון המנחה הוא שככל שאינטרס הפרטיות גדול יותר, השגת הצו דורשת רף הוכחה גבוה יותר. הגנה משמעותית, הדורשת הוכחה של עילה מסתברת, ניתנת רק לדואר אלקטרוני שטרם נקרא על ידי הנמען ואשר מאוחסן על המחשב של השרת במשך פחות מ־180 ימים. עבור כל מידע אחר יכולות הרשויות לבקש צווים מנהליים שהשגתם קלה וכרוכה בדרך כלל רק בהצהרתן לפני בית המשפט שקיים בסיס סביר להאמין שהמידע יהיה רלוונטי לחקירה פלילית. מידע כזה כולל נתונים אישיים על המנוי, כגון: שם, כתובת, מספר טלפון, היסטוריית תשלומים, סוגי השירות שבהם השתמש וכתובות דואר אלקטרוני שאליהן שלח הודעות. ה־Patriot Act הרחיב את הרשימה והוסיף גם רשומות בנוגע למועדי הגלישה ומשכם, כתובות אינטרנט זמניות, מספרי חשבונות בנק ומספרי כרטיסי אשראי.[101]

החוק גם מגביל את יכולתם של ספקי שירות ציבוריים למסור מידע לממשלה. ספקים פרטיים, כמו מקומות עבודה או אוניברסיטה, חופשיים לכאורה למסור כל מידע שהם חפצים. אולם החוק מונה את המקרים שרק בהם יוכלו ספקים ציבוריים לגלות מרצונם מידע לממשלה, למשל כאשר מדובר במקרה חירום ויש

99 *DOJ Manual*, **לעיל** הערה 95, סעיף III.A.

100 **שם**, סעיף III.B. ראו גם Solove, **לעיל** הערה 27, עמ׳ 1283.

101 *DOJ Manual*, **לעיל** הערה 95, סעיפים III.C ו־III.D. ראו גם Solove, **לעיל** הערה 27, עמ׳ 1283–1284; Kerr, **לעיל** הערה 91, עמ׳ 1218–1220.

בידיהם ראיות לפשע, או כאשר הם נתקלים בתמונות פורנוגרפיות של ילדים. נוסף על כך, הם חופשיים למסור מידע שאינו תוכן לגורמים לא־ממשלתיים.[102]

לממשלה אין כמעט תמריצים לפעול לפי החוק. ראיות שהושגו בניגוד לחוק יהיו קבילות בבתי המשפט בהליך פלילי, והקנסות נמוכים.

סיכום ECPA

אף שלכאורה מדובר בשלושה חוקים נפרדים המסדירים מצבים שונים, במציאות ההבחנה ביניהם אינה תמיד קלה, בין השאר בשל העובדה שהחוק נחקק לפני התפתחות האינטרנט והדואר האלקטרוני, וההבחנות הקבועות בו אינן הולמות סוג תקשורת זה.

למשל, ההגדרה של "יירוט" בחוק האזנת סתר אינה חד־משמעית, ולכן היקף תחולתו של החוק אינו ברור. הודעת דואר אלקטרוני אינה נשלחת ישירות לנמען. היא מפורקת ליחידות קטנות המועברות ברשת דרך מחשבים שחלקם מאחסנים אותן למשך אלפיות של שנייה. השאלה היא אם תקשורת המאוחסנת בדרכה לנמען נחשבת עדיין "בתנועה" לצורך חוק האזנת סתר. שאלה זו לא נענתה באופן ברור בפסיקה האמריקנית. ביוני 2004 קבע בית משפט פדרלי לערעורים שקריאת דואר אלקטרוני שממתין לנמען על השרת של ספק השירות לא נחשבת להאזנת סתר, שכן הדואר נמצא במצב נייח ולכן לא מדובר ביירוט. החלטה זו גררה גל מחאות, בטענה שהיא מייתרת את חוק האזנת סתר ומאפשרת לרשויות לצותת לדואר אלקטרוני תוך התעלמות מחוק זה. באוגוסט 2005, בדיון נוסף שהתקיים בעניין, ניתן פסק דין שדחה את הטענה שלא מדובר בהאזנת סתר, אולם הפסיקה נמנעה מלקבוע הלכה חד־משמעית בשאלה זו.[103]

בעיה נוספת היא ההפרדה בין מידע שהוא תוכן, הזוכה להגנה משמעותית יותר בחוק, לבין נתוני תקשורת הזוכים להגנה סמלית בלבד. הפרדה זו אינה תמיד ברורה, בעיקר כשהיא מתייחסת לרשימת אתרי האינטרנט שאליהם גלשו

102 *DOJ Manual*, **לעיל** הערה 95, סעיף III.E; Kerr, **לעיל** הערה 91, עמ' 1220–1222.

103 נושא זה נידון בפסק הדין *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004). להתייחסות לפסק הדין ולדיון נוסף, ראו Kerr, **לעיל** הערה 91, עמ' 1232; Solove, **לעיל** הערה 27, עמ' 1279–1280.

ממחשב מסוים ומונחי חיפוש שהקיש המשתמש במנועי חיפוש מאותו מחשב.[104] השאלה אם מידע כזה נחשב לתוכן טרם הוכרעה, והסכנה היא שהממשלה תעדיף במקרים כאלה לבחור בהליך המקל אתה, וכך תגבר הפגיעה בזכות לפרטיות.[105]

פסק דין משמעותי נוסף – עניין **וורשאק**[106] – נוגע לפרשנותו של ה־SCA. החוק מאפשר למדינה לקבל בצו, בהקשר לחקירה פלילית, פירוט נתונים מחברות המחזיקות במידע דיגיטלי. יש לציין שהמבחנים לקבלת צו מקלים הרבה יותר מאשר צווי חיפוש בביתו של אדם או צווי האזנת סתר, והם מקבילים למבחנים של השגת ראיות המצויים בידי צד שלישי, שלגביהם ישנה חזקה של ויתור על פרטיות. לאחר שהתברר לוורשאק שהמדינה קיבלה מספקי האינטרנט שלו חומר אודותיו, שכלל אף את **תוכנן** של התכתבויות הדואר האלקטרוני, הוא דרש סעד הצהרתי שיאסור על המדינה לעשות זאת בעתיד. בית המשפט הכריע שלמרות שתוכן הדואר האלקטרוני אכן מוחזק בידי צד שלישי, הזכות והציפייה לפרטיות גוברת, בדומה לשיחות טלפון או מכתבים, ולכן צו לפי ה־SCA לא יכול לכלול תוכן של דואר אלקטרוני.

נקודה רלוונטית היא כי במענה לטענת המדינה שספקי האינטרנט עורכים "ממילא" סריקות ממוחשבות על תכתובות הדואר האלקטרוני – למציאת וירוסים, דואר זבל (ספאם) וכן למציאת פורנוגרפיית ילדים – הבחין בית המשפט בין פרקטיקה זו ובין העברת התוכן עצמו למדינה. בית המשפט ציין שסריקות אלה דומות לסינון הלגיטימי על ידי פקידי הדואר שנועד לאתר חבילות החשודות כמכילות חומרי נפץ או סמים ואינו מתייחס לתכנים של דברי הדואר.

בהכרה של בית המשפט בפרקטיקה זו יש לדעתי משום כרסום בהבחנה המוחלטת בין תוכן לנתוני תקשורת, בעיקר בכל האמור לגבי פורנוגרפיית ילדים. שכן מדובר בשימוש בתוכנה אוטומטית שעוברת על **כל** נפח התקשורת ומאתרת את אותן תמונות שללא ספק הן חלק מתוכן ההתקשרות. עם זאת קיים הבדל מסוים בין מעבר על תמונות לבין מעבר על מלל, בעיקר בהתייחס לכמות המידע שעוברת פיקוח.

104 ראו **לעיל**, סעיפים 6 ג־ד על אודות גישת המשפט הישראלי.

105 ראו Solove, **לעיל** הערה 27, עמ' 1287–1288; Gross, **לעיל** הערה 3, עמ' 74–75.

106 *Warshak v. United States*, no. 06-4092 (6th cir. 18.6.07)

The Foreign Intelligence Surveillance Act (FISA)

איסוף מודיעין זר שונה באופיו ובמטרותיו מזה הנעשה לצורך חקירה פלילית. במקרה הראשון, הרשויות לא יוכלו להוכיח את קיומה של עילה מסתברת, שכן לא התרחש פשע. איסוף המידע נעשה לצרכים מניעתיים ולתקופות ממושכות. מטעמים אלה הבהיר בית המשפט העליון האמריקני כי ההגבלות שקבע בנוגע לתיקון הרביעי אינן חלות כאשר איסוף המידע נעשה לצורכי מודיעין. קביעה זו אפשרה לשירותי הביטחון לפעול כמעט ללא הגבלה, מכוח סמכותו הכללית של הנשיא להורות על איסוף המידע.[107]

ב־1972 התייחס בית המשפט העליון לראשונה לנושא זה וקבע שלמרות ההבדלים, גם כאשר המידע נאסף לצורכי מודיעין יש צורך בצו של שופט, אם כי ייתכן שבנסיבות חריגות ניתן יהיה לוותר עליו. השופטים נמנעו מלקבוע את הסטנדרטים שבהן תידרש הממשלה לעמוד לצורך קבלת צו כזה, והעדיפו לקרוא לקונגרס לחוקק חוק שיעגן סמכות זו.[108] אך בטרם הספיק הקונגרס לחוקק את החוק, נחשפה פרשת ווטרגייט. ועדת צ׳רץ׳, שהוקמה על ידי הסנאט כדי לחקור את הפרשה, פרסמה את מסקנותיה ב־1976. הנתונים שהופיעו בדוח חשפו את ההיקף העצום של פעילות שירותי המודיעין. למשל, ל־FBI היו תיקים על למעלה מחצי מיליון אזרחים ובשנת 1972 לבדה נפתחו 65,000 תיקים חדשים. כ־300,000 אנשים קוטלגו במערכת המחשב של ה־CIA וכ־100,000 אזרחים אמריקנים היו נתונים למעקב של המודיעין הצבאי. בין האנשים שהיו נתונים למעקב של גופים אלה היו חברי אופוזיציה, שופטי בית המשפט העליון, מרצים באוניברסיטאות, סופרים, חברי המפלגה הקומוניסטית, חברי התנועה לזכויות האזרח ומתנגדי המלחמה בווייטנאם. ג׳ון סטיינבק, ארנסט המינגווי, צ׳רלי צ׳פלין, מרלון ברנדו, מוחמד עלי, אלברט איינשטיין, נשיאים וחברי קונגרס – הופיעו ברשימות. שירותי המודיעין השתמשו בנתונים שאספו, בין השאר, כדי להשפיע על מעסיקים לפטר עובדים, ליזום חקירות של מס הכנסה או להביך אנשים לפני משפחתם. הוועדה מצאה שכל הנשיאים השתמשו בסמכותם להורות

107 Swire, **לעיל** הערה 92, עמ׳ 1312–1313.

108 *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972). וראו התייחסות לפסק הדין אצל Swire, **לעיל** הערה 92, עמ׳ 1314–1315.

על איסוף מידע מסוג זה, גם כאשר לא הייתה כל ראיה לפעילות לא חוקית ואף על פי שלא נשקפה כל סכנה לביטחון הלאומי. הוועדה המליצה על הפרדה בין איסוף מודיעין זר לבין איסוף מודיעין הקשור לביטחון הפנימי של ארצות הברית וקבעה שיש להגביל את סמכותם של שירותי המודיעין בכל הנוגע להאזנות ולמעקבים אחרי אזרחי ארצות הברית.[109]

זה הרקע לחקיקתו של FISA אשר מסדיר איסוף של מודיעין זר בתוך גבולות ארצות הברית. החוק מתיר לצותת למי שהוגדר "כוח זר" או "סוכן זר". בזמנו כללה ההגדרה את כל המדיניות הקומוניסטיות, אולם היא הייתה רחבה דיה כדי לכלול גם כל ממשלה זרה אחרת וכן ארגונים העוסקים בטרור בינלאומי. ביצוע ההאזנה כרוך בהשגת צו מבית משפט מיוחד שהוקם מכוח החוק ובו יושבים 11 שופטים פדרליים. הצו יינתן אם הוכח לפני השופטים שאיסוף המודיעין הוא מטרת החקירה, וכי קיימת עילה מסתברת להאמין שהאדם לו מבקשת המדינה לצותת הוא "כוח זר" או "סוכן זר". גם אם הראיות שהושגו דרך צו כזה ישמשו בשלב מאוחר יותר בהליך פלילי, הנאשם לא יוכל לראותן או לנסות להפריך אותן (הוא רק יידע על קיומן, והשופט יראה אותן במעמד צד אחד).[110] כל צו ניתן לתקופה של תשעים יום, הניתנת להארכה. הדיון בבית המשפט המיוחד מתקיים בדלתיים סגורות ובמעמד נציגי הממשלה בלבד. אם נדחית הבקשה רשאית הממשלה לערער על ההחלטה לפני בית משפט מיוחד לערעורים, שהוקם אף הוא מכוח החוק.[111] בין 1979 ל־2002 אושרו 15,247 צווים.[112] בשנים אלה נדחו רק בקשות ספורות לצווים.

כדי להבטיח שהחוק לא ישמש מסלול עוקף ונוח לחוק האזנת הסתר, המחייב את הרשויות בחקירות פליליות ומציב לפניהן דרישות מהותיות שהן עלולות להתקשות לעמוד בהן, נקבעו נהלים מחמירים שאסרו על העברת מידע שהושג דרך FISA לגורמים העוסקים בחקירות פליליות, אלא במקרים ספציפיים, ורק אם הושגו כאשר המטרה הראשונית הייתה איסוף מודיעין ולא

109 ראו Solove, **לעיל** הערה 27, עמ׳ 1273–1277; Swire, **לעיל** הערה 92, עמ׳ 1315–1320.

110 **שם**, עמ׳ 1323.

111 ראו Rosen, **לעיל** הערה 33, עמ׳ 613; Swire, **לעיל** הערה 92, עמ׳ 1320–1323.

112 דוח *TAPAC*, **לעיל** הערה 7, עמ׳ 28.

חקירה פלילית. בהתבסס על כלל זה, ובידיעה שהחומר המושג דרך החוק משמש לצרכים מוגבלים, הורחבה תחולתו בהדרגה. כך, בית המשפט המיוחד קיבל את בקשות הממשלה גם כשהמטרה העיקרית הייתה אמנם איסוף מודיעין – אך לא הייתה זו המטרה היחידה. הקונגרס הרחיב את החוק גם לחיפושים בבתים, ליומני דואר וטלפון ולרשומות מסוגים רבים, כמו למשל רשומות של שכירת רכב.[113]

בעקבות הפיגוע במגדלי התאומים נעשו שני שינויים משמעותיים בנוגע לחוק. הראשון נעשה במסגרת ה־Patriot Act שקבע בסעיף 218 שבית המשפט יכול לאשר האזנות לפי החוק בכל מקרה שבו איסוף המידע המודיעיני הוא "מטרה משמעותית" של החקירה, במקום המטרה היחידה כפי שנדרש קודם. השינוי השני, שנעשה בידי היועץ המשפטי ג'ון אשקרופט במרס 2002, ביטל את האיסור על העברת מידע שהושג על פי חוק זה מגופי המודיעין לגופים העוסקים בחקירות פליליות. ההנחיות החדשות מתירות העברה חופשית של מידע בין שני הגופים.[114] במאי 2002 קבע בית המשפט המיוחד שהוקם מכוח החוק שההנחיות הללו אינן חוקיות ויש לבטלן. לראשונה מאז נחקק החוק השתמשה הממשלה בזכותה לערער על החלטת בית המשפט לבית משפט מיוחד לערעורים, וזה קבע בנובמבר 2002 שההנחיות תקפות. השופטים קבעו, בעקבות הערעור, שהמשמעות של הרחבת החוק ב־Patriot Act היא שניתן להשתמש במידע גם לצורכי אכיפת חוק רגילה. הם אף הרחיקו וקבעו שספק אם בעבר, לפני שינוי החוק, היה צורך בקיומה של הפרדה כזו, המבוססת על דיכוטומיה מוטעית בין חקירות פליליות רגילות לבין חקירות של גופי המודיעין וטענו שמעולם לא היה צורך לפרש כך את FISA.[115] לפי טענת בית המשפט לערעורים, לא ברור כיצד אמורה המדינה להשתמש במידע שאותו היא אוספת אם לא בהליכים פליליים.[116]

פסיקה זו והרחבת תחולתו של החוק היו נתונים לביקורת. בין השאר נטען שהשינוי שנעשה ב־Patriot Act מאפשר את הרחבת החוק גם לחקירות שהן

113 Swire, **לעיל** הערה 92, עמ' 1325–1329.

114 לסקירת ההנחיות ראו **שם**, עמ' 1335.

115 In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611 (2002). לניתוח פסק הדין ראו Swire, **לעיל** הערה 92, עמ' 1337; Solove, **לעיל** הערה 27, עמ' 1290.

116 Swire, **לעיל** הערה 92, עמ' 1337.

בעיקרן פליליות ושיכולות להסתיים בכתבי אישום. אולם תביעה פלילית אינה יכולה להתבסס על ראיות שהושגו בחשאי והנאשם אינו יודע עליהן. החלת הכללים המקלים של FISA על מקרים מעין אלה מאפשרת לממשלה לעקוף את הדרישות של החוקה ושל החוק. בסיס נוסף לביקורת היה היעדר הגדרה ברורה בחוק עבור "סוכן זר". אפשר לטעון שסוחרים העובדים עבור קרטל סמים מקולומביה גם הם "סוכנים זרים". אך מה לגבי "המאפיה הרוסית"? ככל שתורחב הפרשנות של "סוכן זר" גם למקרים פליליים, יתייתר הצורך בחוק האזנת הסתר וההגנות שבתיקון הרביעי ייעלמו. הרחבת הסמכויות עלולה להפוך את FISA לכלי העיקרי לאיסוף מידע, והעובדה שההליכים מכוחו מתנהלים במעמד צד אחד בלי פיקוח חיצוני משמעותי מחזקת את החשש שמספר ההאזנות לפי החוק יתרחב ושהמצב יחזור לזה שהיה לפני שנחשפה פרשת ווטרגייט. ואכן, בשנת 2003 עלה לראשונה מספר צווי החיפוש תחת FISA על אלה שהוצאו לצרכים של חקירה פלילית רגילה.[117]

האזנות לפי צו נשיאותי של הנשיא ג'ורג' וו' בוש

בעקבות חשיפה של הניו יורק טיימס בדצמבר 2005[118] התברר שהנשיא ג'ורג' וו' בוש הורה, בחשאי, לרשות הביטחון הלאומית (NSA) לבצע האזנות ללא צו לשיחות ולתכתובות דואר אלקטרוני היוצאות מארצות הברית ונכנסות אליה (שיחות ותכתובות של אזרחי ארצות הברית עם מדינות זרות). ההאזנות היו לאנשים "המקושרים לאל-קאעדה" או קשורים לארגוני טרור, כחלק מהמלחמה בטרור לאחר פיגועי 11 בספטמבר. נראה שהפרקטיקה הודלפה לעיתון עקב ספקות שהתעוררו בקרב אנשי NSA באשר לחוקיות המהלך. לאחר החשיפה

117 לטענות אלה בנוגע לפסק הדין, ראו דוח *ACLU*, **לעיל** הערה 31, עמ' 9; Swire, **לעיל** הערה 92, עמ' 1354–1355; Solove, **לעיל** הערה 27, עמ' 1290; D. Jonas, "The Foreign Intelligence Surveillance Act through the Lens of the 9/11 Commission Report: The Wisdom of the Patriot Act Amendments and the Decision of the Foreign Intelligence Surveillance Court of Review", *North Carolina Central Law Journal* 27 (2005), p. 95

118 J. Risen & E. Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *NY Times*, December 16, 2005, p. 1

בתקשורת ספג הממשל ביקורת חריפה מצד מלומדים רבים שטענו כי תכנית המעקב של הנשיא בוש איננה חוקית. משרד המשפטים פרסם מצדו חוות דעת משפטית מנומקת, שמגנה על חוקיות התכנית, ולאחר מכן התפרסמו כמה ניירות עמדה סותרים של שני הצדדים. אלה, בתמצית, טענות משרד המשפטים האמריקני בדבר חוקיות הוראת הנשיא:

- הנשיא הגדיר את פעולות ההאזנה שעליהן הורה כ"חיוניות לביטחון הלאומי". על הנשיא מוטלת חובה להגן על ארצות הברית מפני התקפה. החוקה, בסעיף ב פסקה 2, מעניקה לנשיא את הסמכות להיות מפקד הצבא (The President shall be Commander in Chief of the Army and Navy of the United States). מכאן – לפרשנותו של משרד המשפטים – נובעת סמכותו להפעיל את האמצעים הנחוצים להגנה על המדינה מפני איומים מן החוץ. לטענת משרד המשפטים, הסמכות הטבועה בחוקה מחוזקת על ידי החוק שהתקבל בקונגרס ב־18 בספטמבר 2001 המסמיך את הנשיא להשתמש בכוח כדי להגן על ארצות הברית מפני טרור בינלאומי: Authorization for the Use of Military Force (AUMF).[119]
- חוות הדעת של משרד המשפטים מתייחסת גם לחוק המסדיר האזנות לגורמי חוץ: Foreign Intelligence Surveillance Act (FISA). החוק אוסר על כל האזנה שנעשית שלא בהתאם אליו אלא אם היא מותרת בחוק ספציפי אחר. לטענת משרד המשפטים, AUMF מסמיך את הנשיא לבצע האזנות סתר שלא על פי הכללים שנקבעו ב־FISA. ביצוע האזנות ללא צו הוא, לטענת המשרד, חלק אינהרנטי מהפעלת כוח צבאי.[120]
- לטענת משרד המשפטים, כדי שלא יתעוררו סוגיות חוקתיות של פגיעה בסמכויות הנשיא לפי החוקה, יש לפרש את ה־AUMF כפי שמשרד המשפטים מבקש לפרשו.[121]

119 D. Cole & M. Lederman, "The National Security Agency's Domestic Spying Program: Framing the Debate", *Indiana Law Journal* 81 (2006), pp. 1381–1384

120 **שם**, עמ' 1395.

121 **שם**, עמ' 1400.

ואלה, בתמצית, טענותיהם של המלומדים שתקפו את החוקיות של הוראת הנשיא:

- FISA נחקק בעקבות הרצון המפורש שהביע הקונגרס להגביל את הסמכות הכללית של הנשיא או של כל רשות אחרת, והוא מקפל בחובו את האיזון העדין שבין פרטיות לבין הצורך בביטחון לאומי. FISA שולל כל אפשרות של האזנה ללא צו (שניתן על ידי בית משפט שמקים החוק, על סמך ראיות לחשד מבוסס), למעט חריג מוגדר של האזנה בזמן מלחמה, למשך חמישה עשר ימיה הראשונים של המלחמה. טענת משרד המשפטים, ש־AUMF כולל הרשאה משתמעת לחרוג מ־FISA, אינה משכנעת כלל וכלל, שכן AUMF לא מזכיר כלל האזנות, לא כל שכן האזנות ללא צו. רק הרשאה ברורה וספציפית בחוק הייתה יכולה להעניק לנשיא סמכות לחרוג מ־FISA. חריג ה"מלחמה" מדבר בעד עצמו – אפילו הכרזה רשמית של הקונגרס על מלחמה (המלחמה בטרור בעקבות פיגועי ספטמבר 2001 לא לוותה בהכרזה כזו) מעניקה סמכות לביצוע האזנות ללא צו רק למשך חמישה עשר ימים. האם סביר שחוק שאיננו עוסק במלחמה שהוכרזה רשמית, כדוגמת AUMF, יעניק לנשיא סמכות נרחבת יותר מאשר הכרזת מלחמה פורמלית?[122]
- באשר לטיעון הסמכות ה"טבועה" והכללית של הנשיא טוענים המלומדים שמעולם לא נאמר שסמכות זו היא בלתי מוגבלת לחלוטין. ברור שלקונגרס יש סמכות להגבילה, וכך עשה כאשר חוקק את FISA. אין בכך שום סוגיה חוקתית באשר לסמכות הנשיא בחוקה, שכן לא נאמר שזוהי סמכות שאינה ניתנת להגבלה, וגם אין לפרשה ככזו.[123]
- פרשנות יצירתית ל־AUMF, כפי שמבקש משרד המשפטים לעשות, מעלה סוגיות חוקתיות כבדות, שכן פגיעה כזו בפרטיות, ללא איזונים ובלמים כפי שנעשה ב־FISA, סותרת את התיקון הרביעי לחוקה.[124] על כן

122 **שם**, עמ' 1415–1416.

123 **שם**, עמ' 1420.

124 התיקון הרביעי מגן מפני חיפוש או כניסה שרירותיים למרחביו הפרטיים של אדם ללא חשד סביר וקונקרטי נגדו.

מתחייבת על אחת כמה וכמה פרשנות שאינה מרחיבה את משמעותו של AUMF.[125]

מבחינה פרקטית נפתר לבסוף הוויכוח הציבורי לאחר שלושה עשר חודשים. בינואר 2007 הכריז משרד המשפטים האמריקני כי מעתה ואילך תיפסק ההאזנה ללא צווים, וכי בית המשפט המיוחד שהוקם לפי FISA ידון בבקשות להאזנות שבוצעו מאז הוראת הנשיא ללא צו בנוהל מזורז.[126]

יש לשים לב שכל הדיון שלעיל אינו בשאלה מהו הדין הרצוי או האידאלי, אלא מהו הדין הקיים והאם הנשיא, בהוראתו, עבר על החוק. שני הצדדים לא טענו שהחוקה אינה מאפשרת חקיקת חוק אחר, פוגעני יותר מ־FISA. הדיון גם לא התמקד בשיקולי היעילות מחד גיסא ובפגיעה בפרטיות מאידך גיסא. עם זאת הוויכוח העקרוני, הנוגע לאיזון בין הזכות לפרטיות ובין הביטחון הלאומי, בצבץ מתחת לפני השטח.

יש לציין שאין מידע מוצק על האופן שבו פעלה התכנית של NSA. ויטס טוען בספרו כי ככל הנראה NSA עברה על כמויות גדולות של תקשורת (שיחות והתכתבויות) בצורה ממוכנת ואיתרה התקשרויות חשודות על פי דפוסי תקשורת וייתכן שגם על פי התכנים[127] – בתנאי שלפחות אחד מהצדדים להתקשרות היה מחוץ לארצות הברית. ויטס מציין שלפי תחושתו פעלה התוכנה באופן סביר יחסית. הוא מסתמך על כך שהיא הוצגה בפירוט לקונגרס, וזה אישר את פעולתה ותיקן למענה את FISA.[128]

ב. האיחוד האירופי

סעיף 8 לאמנה האירופית לזכויות האדם מעגן את הזכות לפרטיות וקובע כי לכל אדם יש זכות לכיבוד חייו הפרטיים וחיי משפחתו. סעיף 8(2) מאפשר למדינות להגביל זכות זו, אולם רק כאשר הדבר נעשה בהתאם לחוק וכאשר הפגיעה

125 Cole & Lederman, **לעיל** הערה 119, עמ׳ 1421.

126 E. Lichtblau & D. Johnston, "Court to Oversee U.S. Wiretapping in Terror Cases", *NY Times*, January 18, 2007

127 B. Wittes, *Law and the Long War* (London: Penguin Press, 2008), p. 236

128 **שם**, עמ׳ 245.

נדרשת לצורך הגנה על אינטרסים של ביטחון לאומי, שלום הציבור, כלכלה יציבה, בריאות ומוסר הציבור וזכויות של אחרים.

בית המשפט האירופי לזכויות אדם קבע, בשונה מהפסיקה בארצות הברית, כי סעיף זה מתייחס גם להגנה על מידע אישי של אזרחים, כולל הגנה על נתוני תקשורת. כן קבע בית המשפט שמעקב אחר אזרחים יכול להיעשות רק כל עוד הסמכויות לכך עוגנו בחוק מפורט, המאפשר לאזרחים לדעת מתי הם עלולים להיות נתונים למעקב. על החוק לקבוע ביקורת שיפוטית עצמאית ולא להסתפק באישור של הדרג המבצע, וכן להבטיח שהפגיעה לא תהיה מעבר לנדרש ושהיישום לא יהיה שרירותי.[129]

חיזוק להגנה על פרטיותם של אזרחים ועל מידע הנוגע להם ניתן בכמה דירקטיבות שחוקק האיחוד האירופי, אם כי עם השנים נשחקה הגנה זו כאשר נטען שהמידע נחוץ לצורכי ביטחון. בשנת 1995 אימץ האיחוד את הדירקטיבה Data Protection Directive, שמטרתה המוצהרת הייתה לשפר את זרימת המידע בין מדינות האיחוד על ידי יצירת כללים אחידים בנוגע לשמירה על פרטיות נתונים. הדירקטיבה חלה על המגזר הפרטי, והיא מחייבת מדינות להבטיח את הזכות לפרטיות בכל הקשור ל"עיבוד מידע", מונח הכולל איסוף, עיבוד, שינוי, שימוש, העברה ומחיקה של מידע אישי. סעיף 3 לדירקטיבה קובע שהיא לא תחול בכל מקרה שבו עיבוד המידע נעשה לצורכי ביטחון המדינה, כולל חוסנה הכלכלי וצרכים הקשורים למשפט הפלילי.[130] בין השאר, מדינות האיחוד נדרשות להבטיח את דיוק הנתונים, למנוע שימוש בהם למטרות אחרות מאלה שלשמן נאספו ולהודיע לאנשים על כל שימוש שנעשה במידע הנוגע אליהם. הדירקטיבה דורשת שתינתן לאנשים אפשרות להתנגד להכללתם במאגרי מידע ולשימוש במידע עליהם, אולם היא כוללת רשימת חריגים ארוכה ומעורפלת שמחלישה אפשרות זו באופן משמעותי.[131]

129 הלכות אלה נפסקו בכמה פסקי דין: *Klass v. Germany* (1978); *Malone v. UK* (1984), *Kruslin v. Fance* (1990); *Kopp v. Switzerland* (1998)

130 Data Privacy Directive, Council Directive 95/46/EC, 1995

131 S. Salbu, "The European Union Data Privacy Directive and International Relations", *Vanderbilt Journal of Transnational Law* 35 (2002), pp. 668–673. ראו גם Gross, **לעיל** הערה 3, עמ' 87.

על מנת להבטיח את ההגנה על הנתונים נאסר על מדינות להעביר מידע על אזרחיהן למדינות שאינן מעניקות הגנה זהה לנתונים. ארצות הברית, שאינה מעניקה הגנה למידע אישי כנדרש בדירקטיבה, הגיעה להסכם עם האיחוד האירופי שיאפשר העברת נתונים בתנאים מסוימים, אולם ההליך שנקבע הוא לא פורמלי ומתבסס על התחייבות של חברות אמריקניות שהן ישמרו על הזכות לפרטיות כנדרש.[132]

ב־1997 אימץ האיחוד האירופי דירקטיבה נוספת Data Protection-Telecommunication Directive. דירקטיבה זו מתייחסת לתחומים שנותרו לא מוגנים בדירקטיבה של 1995, והיא מטילה הגבלות נוספות על ספקי שירות של טלפונים נייחים וניידים, טלוויזיה דיגיטלית ומערכות טלקומוניקציה נוספות. הדירקטיבה מגבילה את הגישה לחשבונות, מחייבת שטכנולוגיה של זיהוי המתקשר תאפשר גם חסימה של המספר, דורשת מתן אפשרויות לחסימת שיחות ומגבילה את רשימת הפרטים שמותר לספקים לכלול במרשם הלקוחות.[133] גם דירקטיבה זו אינה חלה על עיבוד נתונים לצורכי ביטחון המדינה.

ביולי 2002 חוקק האיחוד את הדירקטיבה Electronic Communication Privacy Directive, שהחליפה את הדירקטיבה מ־1997.[134] דירקטיבה זו מרחיבה עוד את ההגנה על מידע אישי בתקשורת אלקטרונית בהקשר של גופים פרטיים ומסחריים. עם זאת עיקר חשיבותה נעוץ בקביעה בסעיף 6 בנוגע לחובתם של ספקי השירות למחוק את נתוני התקשורת לאחר שאין להם עוד צורך בהם.

זו ההתייחסות הראשונה לנושא שמירת הנתונים (data retention) על ידי ספקי השירות, נושא שהוא מהבוערים ביותר באירופה בשנים האחרונות. ספקי השירות נוהגים למחוק את נתוני התקשורת של לקוחותיהם לאחר שהם לא זקוקים להם יותר לצורך מתן השירות או לכל צורך פנימי אחר כמו חיוב הלקוחות.

132 Salbu, **לעיל** הערה 131, עמ׳ 675–684.

133 לדיון בדירקטיבה זו ראו A. B. Munir & S. H. M. Yasin, "Retention of Communications Data: A Bumpy Road Ahead", *John Marshall Journal of Computer and Information Law* 22 (2004), p. 732. ראו גם Gross, **לעיל** הערה 3, עמ׳ 88.

134 Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (2002)

בדרך כלל אין לנתונים אלה כל שימוש מסחרי, ולצרכים של שיווק ומחקר די בדוגמאות של מידע אנונימי.[135] עם זאת מאחר שנתוני תקשורת יכולים לגלות מידע ניכר על אדם, מעוניינים שירותי הביטחון וגורמי אכיפת חוק בשמירתם. היו אפוא מדינות שביקשו לכלול בדירקטיבה סעיף שיאפשר להן לכפות על ספקי השירות לשמור את נתוני התקשורת של כל לקוחותיהם לתקופות ממושכות. רוב מדינות האיחוד התנגדו בתקיפות להכללת סמכות כזו בשל הפגיעה בפרטיות. אולם זמן קצר לאחר הפיגוע במגדלי התאומים שינו חלק מהמדינות את עמדתן. למרות התנגדות הפרלמנט האירופי התקבל בסופו של דבר סעיף 15(1) המתיר למדינות לאמץ חקיקה שתדרוש מספקי שירות לשמור ולאחסן נתוני תקשורת של מנוייהם. הגבלות אלה של הפרטיות יתקבלו רק אם הן נחוצות, הולמות ופרופורציונליות בחברה דמוקרטית לצורך הבטחת ביטחון המדינה וביטחון הציבור; וכן בתחום הפלילי – למניעה, לחקירה, לגילוי ולתביעה.[136]

יש לציין שבשנת 2006 אימץ פרלמנט האיחוד האירופי דירקטיבה (EC/2006/24)[137] המחייבת את מדינות האיחוד האירופי לחוקק חוקים שיחייבו ספקי שירותי תקשורת לאחסן מידע הנוגע לשיחות טלפון ותכתובות דואר למשך שישה חודשים לפחות (ובמקרים מסוימים עד שנתיים). על הנתונים לכלול מידע שיאפשר לזהות את המשתמש, נתוני זמן השיחה ומשכה. מידע זה אמור להיות נגיש (במקרים המתאימים) לגורמי המשטרה במדינות. דירקטיבה זו הייתה נחוצה, משום שלפני שנחקקה היו ספקיות התקשורת במדינות רבות חייבות למחוק כל מידע ממאגריהן לאחר שלא היה בו עוד שימוש לצורכי ההתחשבנות עם הלקוחות.[138]

135 ראו Munir & Yasin, **לעיל** הערה 133, עמ׳ 731; Gross, **לעיל** הערה 3, עמ׳ 88.

136 לדיון בנושא זה ראו M. Birnhack & N. Elkin-Koren, "The Invisible Handshake: The Reemergence of the State in the Digital Environment", *Virginia Journal of Law and Technology* 8 (2003), p. 92. ראו גם Munir & Yasin, **לעיל** הערה 133, עמ׳ 731–734; Gross, **לעיל** הערה 3, עמ׳ 88.

137 הטקסט המלא מופיע באתר: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

138 F. Bignami, "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law* 8 (2007), pp. 233–255

דירקטיבה זו, כמו כל חקיקה באיחוד האירופי, כפופה לאמנה האירופית לזכויות אדם (EHCR), המגִנה על הזכות לפרטיות. על כן הפגיעה בפרטיות יכולה להיעשות רק באמצעות חוק, לשם תכלית ראויה ותוך שמירה על מידתיות.[139] לאחר דיונים ארוכים ותיקון ההצעה המקורית צומצמה מסגרת הזמנים של איסוף המידע, הועלתה חומרת העבֵרות שלגביהן מותר לאסוף מידע, והוכנסו אמצעים לשמירה על סודיות המידע ולהגבלת השימוש בו למטרות הדירקטיבה בלבד. נוסף על כך, על המדינות לדווח אחת לשנה לאיחוד האירופי על איסוף המידע ועל מספר הפעמים שנעשה במידע שימוש.[140]

יש לציין שוב שבדומה לחוק נתוני תקשורת הישראלי, גם הדירקטיבה האירופית איננה משנה את המצב הבסיסי שלפיו לא ניתן להקליט ולסנן חומר על פי תוכנו ללא חשד כלפי אדם, טלפון או דואר אלקטרוני ספציפי. לכן אינני מוצא לנכון להרחיב בנקודה זו. עם זאת חשובה ההבנה שבכל הקשור לנתוני תקשורת, המוסכמה מאז ומעולם היא שיש פחות אינטרס של פרטיות בנתונים אלה לעומת התוכן. הגישה הרווחת היא של נכונות גוברת והולכת לאפשר לגורמי הביטחון לשמור ולהשתמש בנתוני תקשורת במסגרת חקירות של פשיעה, ולאו דווקא פשיעה הקשורה לטרור.

גרמניה

בגרמניה אומץ בשנת 2007 חוק ברוח הדירקטיבה משנת 2006. החוק מחייב ספקי שירות לשמור נתוני תקשורת כאמור, כולל כתובות שבהן ביקרו המשתמשים. נגד החוק הוגשו עתירות רבות, ובית המשפט החוקתי בגרמניה טרם פסק סופית בנושא. עם זאת בהחלטה שהתקבלה ב־19 במרס 2008 הגביל בית המשפט את תחולת החוק באופן זמני עד ההחלטה הסופית על חוקתיות החוק. ההגבלה אומרת שהחוק יחול רק על חקירות של פשע חמור, כהגדרתו בחוק הפלילי הגרמני (ולא על חקירה של כל פשע).

139 **שם**, עמ׳ 242.

140 **שם**, עמ׳ 252.

שוודיה

ביוני 2008 קיבל הפרלמנט השוודי חוק שלפיו מותר לממשלה, ללא צו שיפוטי, לעקוב באופן גורף אחר דואר אלקטרוני ושיחות טלפון (אם כי רק בתווך פיזי של עורקי תקשורת בינלאומיים, ולא בתוך שוודיה), **תוך סינון המידע לפי מילות מפתח ותנאי חיפוש**. בהנמקה ל"שאלות נפוצות" באתר האינטרנט של ממשלת שוודיה מוסבר הצורך בחוק בהגנה על ביטחונה של שוודיה מפני מלחמות, טרור, התקפות ממוחשבות והפצת נשק לא קונבנציונלי. להלן טענות נוספות שמעלה הממשלה השוודית להגנה על היישום, שלטענתה פגיעתו בפרטיות היא מינימלית:[141]

- השימוש בחוק ייעשה רק למטרות "הגנה" ולא למטרות משטרתיות.
- כל חומר שייאסף ואינו קשור לאיומים על הביטחון יימחק.
- תנאי החיפוש ינוסחו כך שהפגיעה בפרטיות תהיה מינימלית.
- לגבי כל אישור תיעשה שקילה אם התועלת עולה על הנזק הצפוי לפרטיות ואם אין אמצעי פוגעני פחות.
- מסרים בין אדם לעורך דינו יימחקו מהמאגר.
- יקום גוף פיקוחי ("מועצה להגנת הפרטיות") שיוכל להורות על הפסקת האיסוף ומחיקת מידע. תפקיד המועצה הוא לבדוק שהחוק מנוצל רק למטרות שלמענן נועד.
- תיעשה הפרדה ברורה בין איסוף על פי החוק הרלוונטי, שמכוון רק לאיומים חיצוניים ולענייני ביטחון, לבין חקירה משטרתית אחרת. מודגש בבירור שהחוק לא נועד למלחמה בפשע.
- יוקם גוף מעין שיפוטי שיאשר שימוש בחוק.
- תמונה ועדה פרלמנטרית לפיקוח על איסוף המידע על פי החוק.

141 מתוך אתר הממשלה השוודי. יש לציין שאין בנמצא תרגום אנגלי מלא של החוק השוודי: Signal Surveillance Act. ראו www.sweden.gov.se/sb/d/10941/a/110692#110692

החוק גרר מחאה חריפה והפגנות נגד הפגיעה בפרטיותם של אזרחי שוודיה.[142] בעקבות זה עוכבה כניסת החוק לתוקף עד סוף שנת 2009, אך בסופו של דבר החוק נכנס לתוקף.

בריטניה

ברחבי בריטניה מוצבות יותר מארבע מיליון מצלמות. בריטי ממוצע מצולם כשלוש מאות פעם ביום. מאז 1994 הקצה משרד הפנים לצרכים אלה כ־78 אחוזים מהתקציב למניעת פשע. השימוש במצלמות החל בשנות התשעים בתגובה לשורה של פצצות שהטמין ה־IRA, אולם הן מעולם לא סייעו במאבק שניהלה הממשלה נגד הארגון ובמהרה הן שימשו לצרכים אחרים. היום הן משמשות בעיקר לגביית תשלום ממכוניות הנכנסות למרכז לונדון.[143] דוגמה זו מצביעה רק על אחת מהסמכויות הנרחבות הניתנות לרשויות אכיפת החוק ולרשויות אחרות בבריטניה. סמכויות הציתות, המעקב ואיסוף המידע בבריטניה הן מהמרחיקות לכת בעולם המערבי, ולא רק בהקשר של המאבק בטרור.

באוקטובר 2000 נכנס לתוקף בבריטניה חוק זכויות האדם שעיגן את האמנה האירופית לזכויות האדם בחוק המקומי. בכך ניתנה לזכות לפרטיות, המופיעה בסעיף 8 לאמנה האירופית, מעמד מחייב במשפט הבריטי, והתאפשרה קבלת תרופות להפרתה בתוך מערכת המשפט המקומית.[144] להלן יפורטו שני חוקים בריטיים העוסקים בסמכויותיהן של רשויות אכיפת החוק בכל הנוגע לאיסוף מידע על אזרחי המדינה ולשימוש במידע זה.

The Regulation of Investigatory Powers Act (RIPA)

באוקטובר 2000 נכנס לתוקף בבריטניה חוק חדש – The Regulation of Investigatory Powers Act (RIPA). מטרתו המוצהרת הייתה להתאים את

142 ראו דיון באתר www.usatoday.com/news/world/2008-06-18-3616058072_x.htm

143 Rosen, **לעיל** הערה 33, עמ' 609–610. ראו גם מסמך שפרסם ארגון Liberty, ארגון בריטי לזכויות האזרח, *Nothing to Hide, Nothing to Fear? Privacy v. Government*, סתיו 2003: www.liberty-human-rights.org.uk

144 אפשר גם לפנות לבית הדין האירופי לזכויות האדם, לאחר מיצוי הסעדים במערכת המקומית.

המעקבים והציתותים להגבלות החדשות שמטיל חוק זכויות האדם ולהרחיב את יכולתן של הרשויות לאסוף מידע בסביבה הדיגיטלית.[145] החוק קובע שני הסדרים – אחד לאיסוף מידע מסוג תוכן והשני לאיסוף מידע מסוג נתוני תקשורת שאינם תוכן. גישה למידע הנחשב תוכן, כמו שיחות טלפון ודואר אלקטרוני, מוסדרת בפרק הראשון של חלקו הראשון של החוק. האזנה למידע כזה תאושר בעקבות בקשה של שירותי הביטחון או המודיעין משר בממשלה – בדרך כלל שר הפנים או שר החוץ. הצו יינתן אם השר מאמין שההאזנה נחוצה לצורך אחת משלוש המטרות המוזכרות בחוק: ביטחון המדינה, מניעה וגילוי של פשע חמור או הבטחת חוסנה של הכלכלה הבריטית. על השר להיות משוכנע שהוצאת הצו היא פרופורציונלית להשגת המטרה ושלא ניתן להשיג את המטרה בדרכים אחרות.[146]

סעיף 12 של החוק מאפשר לשר לכפות על חברות טלפון וספקי שירותי אינטרנט יכולת טכנית שתאפשר ביצוע ציתותים בכל פעם שהרשויות ידרשו זאת מהן. ספקי השירות מחויבים לאפשר את ביצוע הציתות בתוך זמן סביר מרגע שהתבקשו ולהעביר לרשויות מידע בזמן אמת. איסוף נתוני התקשורת מוסדר בפרק השני של חלקו הראשון של החוק. נתונים אלה כוללים מידע מזהה בנוגע לאדם, יומנים של שיחות שנעשו ושהתקבלו, משך השיחות, שעת ההתקשרות, כתובות דואר אלקטרוני של נמענים, גודל הודעות הדואר, אתרי אינטרנט שבהם ביקרו הגולשים ועוד. החוק אף מונה את רשימת הגופים הרשאים לקבל נתונים אלה. כדי להשיג את הנתונים די שאדם העובד באחד מגופים אלה, ואשר הוסמך לכך, קבע שהם נחוצים לאחת המטרות המנויות בחוק ושקבלתם היא פרופורציונלית. רשימת המטרות היא ארוכה ומעורפלת: ביטחון המדינה, מניעת פשע, חוסנה הכלכלי של המדינה, הגנה על בריאות הציבור, גביית מיסים, בטיחות הציבור ועוד. באישור הפרלמנט ניתן אף להרחיב את רשימת המטרות.[147]

145 C. Hirsch, "Policing Undercover Agents in the United Kingdom: Whether the Regulation of Investigatory Powers Act Complies with Regional Human Rights Obligations", *Fordham International Law Journal* 25 (2002), p. 1315. ראו גם Birnhack & Elkin-Koren, **לעיל** הערה 136, עמ' 77.

146 סעיף 5 ל־RIPA.

147 סעיפים 21–25 ל־RIPA. ראו הסבר על החוק באתר האינטרנט של משרד הפנים הבריטי: www.homeoffice.gov.uk. להתייחסות לחוק ראו Gross, **לעיל** הערה 3, עמ' 82–83.

ביוני 2002 ביקש משרד הפנים הבריטי להרחיב את רשימת הגופים המוסמכים לקבל נתוני תקשורת לפי החוק, אך בשל ביקורת ציבורית נאלץ המשרד למשוך את ההצעה. שנה לאחר מכן הועלתה הצעה דומה לפני הפרלמנט, והפעם אושרה ההצעה. משרד הפנים הצדיק את הוספת חלק מהגופים לרשימה בטענה שממילא הם מקבלים נתונים אלה, וראוי לעגן זאת בצורה מסודרת בחוק.[148] היום כוללת הרשימה לא רק את גופי המודיעין והחקירות, אלא גם 61 סוכנויות ומחלקות ממשלתיות, בהן מועצות מקומיות, סוכנויות לאיכות סביבה ופקחי בריאות.[149]

החוק הסדיר הקמת טריבונל מיוחד לדיון בתלונותיהן של אזרחים הסבורים שזכויותיהם נפגעו מכוח החוק. אולם הסמכויות שניתנו לטריבונל מוגבלות. עם זה יש לו סמכות שיפוט בלעדית ואין אפשרות לערער על החלטותיו.[150] מספר התלונות שהוגשו לטריבונל הוא נמוך. בשנת 2009 התקבלו 157 פניות חדשות, החקירה לגבי 58 מתוכן הסתיימה, וכן הסתיימה חקירת 67 מתוך 75 מקרים שנותרו משנת 2008. 107 מקרים הועברו לדיון ב־2010. מקרה אחד הוכרע לטובת המתלונן, ובסך הכול היה זה המקרה הרביעי שבו נקבע שהייתה הפרה של RIPA.[151]

החוק היה נתון לביקורת בטענה שהוא מעניק סמכויות רבות מדי לרשות המבצעת, בלי ביקורת שיפוטית. האזנות לשיחות טלפון ולדואר אלקטרוני נעשות על בסיס אינטרסים רחבים ומעורפלים, הניתנים לפרשנות רחבה של השר. הסמכויות לקבלת נתוני תקשורת כמעט שאינן מוגבלות והן ניתנו לגופים שאינם אמונים על שמירת הפרטיות ואינם יודעים לבצע חקירות. נוסף על כך,

148 Explanatory Memorandum to the Regulation of Investigatory Powers (Communications Data). ראו גם התייחסות במסמך של ארגון Liberty, **לעיל** הערה 143.

149 Regulation of Investigatory Powers (Communications Data) Order 2003. ראו בנושא זה Hosein, **לעיל** הערה 33, עמ׳ 39.

150 סעיפים 65–70 ל־RIPA. ראו Hirsch, **לעיל** הערה 145, עמ׳ 1324–1327.

151 Report of the Interception of Communications Commissioner for 2010 (Commissioner: The Rt. Hon Sir Paul Kennedy), Presented to Parliament by the Prime Minister pursuant to section 58 (6) of the Regulation of Investigatory Powers Act 2000. ראו www.official-documents.gov.uk/document/hc1011/hc03/0341/0341.pdf

אין כל הגבלה על התקופה שבה מותר לגופים המנויים בחוק לשמור על נתוני התקשורת שקיבלו. עוד נטען שהחוק מיושם באופן חשאי, דבר המסביר את מספר התלונות הנמוך לפני הטריבונל.[152]

The Anti-Terrorism Crime and Security Act

זמן קצר לאחר הפיגוע במגדלי התאומים חוקק הפרלמנט הבריטי חוק חדש – The Anti-Terrorism Crime and Security Act. חלק 11 של החוק (סעיפים 102–107) עוסק בין השאר בחובתם של ספקי השירות לשמור את נתוני התקשורת גם לאחר שכבר אין להם צורך בנתונים. בריטניה היא המדינה האירופית הראשונה שעיגנה סמכויות כאלה בחקיקה מקומית.

החוק מסמיך את שר הפנים לנסח Code of Practice שיסדיר את חובתם של הספקים לשמור על נתוני התקשורת כאשר הדבר נחוץ לצורכי ביטחון המדינה או למטרת מניעה או חקירה של פשעים הקשורים ישירות או בעקיפין לביטחון. חובה זו אינה חלה על מידע הנחשב לתוכן התקשורת. כמו כן, החוק מסמיך את השר להגיע להסכמים עם ספקי התקשורת בנוגע לאופן שמירת הנתונים. החוק הוא וולונטרי ואי־ציות לו אינו יכול לשמש עילה להעמדה לדין פלילי או לנקיטת הליכים אזרחיים נגד ספקי השירות. אולם סעיף 104 מאפשר לשר לכפות על הספק לשמור נתונים לתקופה מוגבלת אם השר משוכנע שהדבר נחוץ לצורך אחת המטרות שצוינו לעיל. סעיף 106 של החוק מאפשר לשר לקבוע הסדרים להשתתפות בעלויות שמירת המידע.

במרס 2003 פרסמה הממשלה טיוטת חוק שלפיה שמירת הנתונים דרושה לצורך המלחמה בטרור. החוק – שהתקבל בפרלמנט – קובע תקופות קצובות לשמירה על נתונים לפי מהותם. למשל, נתונים מזהים של המנוי – כגון שם, תאריך לידה, חשבונות, שיטות תשלום, פרטי כרטיס אשראי וכתובת דואר אלקטרוני – יש לשמור למשך שנה. נתונים כגון כתובות דואר אלקטרוני שאליהן שלח המנוי הודעות וקיבל מהן הודעות, וכן מועדי שליחתן וקבלתן,

152 ביקורת כזו ראו למשל באתר האינטרנט של ארגון Justice, מארגוני זכויות האזרח המובילים בבריטניה: www.justice.org.uk. ראו גם Hirsch, **לעיל** הערה 145, עמ׳ 1329–1330.

יש לשמור לתקופה של שישה חודשים. מידע על כתובות אינטרנט שבהן ביקר המנוי יש לשמור למשך ארבעה ימים בלבד.[153]

ארגונים לזכויות האזרח בבריטניה התנגדו לחוק. ההתנגדות העקרונית כוונה לעצם יצירת מאגר מידע אישי של מיליוני אנשים שאינם חשודים בדבר. העובדה שמאגר כזה עשוי לסייע בעתיד לרשויות אכיפת החוק אינה יכולה, לטענת הארגונים שהתנגדו לחוק, להצדיק סמכויות כה גורפות לשמירת נתונים ולשימוש בלתי מוגבל בהם.[154]

נוסף על הבעיות בחוק עצמו, השילוב שלו עם ההוראות של RIPA עורר דאגה בנוגע לשימוש שיכול להיעשות בנתונים שיישמרו מכוחו. אמנם החוק מחייב שהנתונים יישמרו רק לצורכי ביטחון, אולם הגישה אליהם מוסדרת על ידי RIPA, וחוק זה מתיר גישה נרחבת לנתוני התקשורת על ידי שורה של רשויות ולמגוון מטרות שבינן לבין ביטחון אין כל קשר.[155]

8. טיעונים להתרת פגיעה מסוימת בזכות לפרטיות

בסעיף זה ייבחנו כמה טיעונים המבקשים להוכיח, כי נקודת האיזון בין הזכות לפרטיות לבין ההגנה על ביטחון המדינה, כפי שבאה לידי ביטוי בחוק האזנת הסתר בישראל וברוב מדינות העולם, ראויה לבחינה מחודשת בעקבות הופעת "הטרור החדש" – לפחות בכל הקשור למעקב אחרי השימוש שעושים ארגוני הטרור באינטרנט. כאמור, בהיעדר שינוי במצב הקיים, שלפיו נדרש חשד ספציפי כתנאי למעקב הפוגע בפרטיותו של אדם, אי־אפשר להשתמש בתוכנות "רחרחניות" (שבוחנות את כל התעבורה גם ללא חשד ספציפי) לחיפוש וסינון תכנים של תכתובות דואר אלקטרוני, תוכנות מסרים מידיים ותוכנות מסרים אחרות, או להצלבת מידע זה עם נתוני גלישה וכדומה.

153 זמנים אלה מפורטים בנספח א של הקוד. ראו www.opsi.gov.uk/si/si2003/draft/5b.pdf

154 לסקירה מרוכזת של ההתנגדויות מטעם הארגונים השונים ראו Munir & Yasin, **לעיל** הערה 133, עמ' 740–749.

155 **שם**, עמ' 737–738; Hosein, **לעיל** הערה 33, עמ' 39; Justice, *Access to Communications Data by Public Authorities*, Justice Briefing, 2002

א. הטרור התעצם ונעשה מסוכן יותר

טיעון מרכזי שמועלה לעתים על ידי אנשי רשויות הביטחון וגורמים נוספים הוא שעוצמתו של הטרור של ימינו היא גדולה והוא מאיים יותר בהשוואה לטרור בעבר. נטען כי הטרור של היום מהווה סיכון על עצם קיומן של המדינות הדמוקרטיות, ולכן יש לשנות את האיזון הקיים בין פגיעה בפרטיות לבין שמירה על הביטחון.

מחד גיסא יש להכיר בעובדה שארגונים כגון אל־קאעדה מציבים אתגרים חדשים לדמוקרטיות באשר הן. כמו כן, מלחמת לבנון השנייה (בקיץ 2006) הייתה דוגמה ליכולתו של ארגון טרור (חזבאללה) להזיק ולפגוע במדינה שלמה, באזרחיה ובביטחונה. ניצחון חמאס בבחירות ברשות הפלסטינית, ולאחר מכן כיבוש רצועת עזה בידי המנגנון הצבאי שלו, מדגימים את הכוח הרב שיכול להיות לארגוני טרור. מאידך גיסא יש לזכור שפיגועיו הראוותניים של ארגון אל־קאעדה ברחבי העולם לא פגעו או איימו בשום שלב על עצם קיומן של ארצות הברית, בריטניה או ספרד.

נקודה נוספת היא הסכנה שנשק לא קונבנציונלי יגיע לידיהם של ארגוני טרור. סכנה זו, שטרם ברורה הקונקרטיות שלה, היא גורם שיש להביאו בחשבון בגלל פוטנציאל ההרס העצום של הנשק הלא קונבנציונלי. יש לציין כי קיימת טענה שגם אם הסיכוי שארגוני טרור יוכלו לעשות שימוש בנשק גרעיני הוא נמוך, הסבירות לשימוש בנשק ביולוגי אינה מבוטלת. ועדה שמינה הקונגרס האמריקני העריכה שקיימת סבירות כי עד שנת 2013 ייעשה שימוש בנשק לא קונבנציונלי בהתקפת טרור במקום כלשהו בעולם.[156] לאור זה גדלה מאוד החיוניות של המניעה המוקדמת (לעומת התגובה העונשית המאוחרת).

דרך אחרת (שבה נוקט ויטס) היא להציג את הטענה כך: המשטר החוקי הישן בארצות הברית (שלפיו נחקק FISA) הושפע מהניצול לרעה של מנגנוני המודיעין בשנות השבעים של המאה הקודמת, ויצא מנקודת הנחה שמתן סמכויות מעקב נרחבות לממשלה מהווה סיכון גדול לציבור, יותר מכל איום שהממשלה תצטרך

156 ראו ד' פרידמן, "מניעת תפוצה וטרור של נשק השמדה המונית: דו"ח ועדה של הקונגרס האמריקני", **מבט על** 84, 10.12.2008, אתר המכון למחקרי ביטחון לאומי: www.inss.org.il/heb/research.php?cat=98&incat=&read=2407

להתמודד אתו באמצעות אותן סמכויות. אולם לדעתו של ויטס, הנחה זו אינה תקפה עוד לאחר אירועי 11 בספטמבר. כאשר מאזן האיומים השתנה, גם האיזון בין האינטרסים הנוגדים צריך להשתנות בהתאם.[157]

עם זאת ברור שאין להעניק לרשויות הביטחון כוח בלתי מוגבל, ובכך לתת משקל מוחלט להגנה על הביטחון ולהתיר פגיעה בפרטיות. אם מחיר ההגנה על הדמוקרטיה יהיה רמיסה מוחלטת ובלתי מפוקחת של הזכות לפרטיות (למשל על ידי מעקב אחרי גלישת כל האזרחים ברשת, תוך הכנת תיק מודיעיני ממוחשב על כל גולש), ייחצה הקו המבדיל בין מדינה דמוקרטית למדינה אוטוריטרית. אי לכך ברור שגם מול איומי הטרור החדשים חשוב להביא בחשבון את הזכות לפרטיות. הפגיעה בה אינה יכולה להיות מוחלטת. לכן, גם בהנחה שהטיעון בדבר התעצמות הטרור תקף ונדרש איזון שונה בין ביטחון להגנה על הפרטיות, לא נובעת מכך בהכרח הצדקה להפעלת תוכנות רחרחניות, שכן הפעלתן של אלה היא למעשה האזנת סתר לאזרחים תמימים שאין לגביהם חשד כלשהו.

ב. שינוי המבנה של ארגוני הטרור

מפרסומים שונים עולה שהמבנה של ארגון הטרור המודרני שונה מהמבנה של ארגוני הטרור הישנים. מאפייניו המבניים של ארגון הטרור החדש הם אלה:[158]

- אופיו אינו טריטוריאלי אלא בין־מדינתי ורב־מדינתי.
- אין מדינה ספציפית שמפעילה את הארגון, ולכן קשה לצפות את מעשיו, לשלוט בו או לדכאו באמצעות הפעלת לחץ על אותה מדינה.
- הארגון יכול להסתגל ולהתאים עצמו לשינויים מהירים בנסיבות.
- מבנה הארגון "נוזלי" וגמיש הרבה יותר מבעבר. ארגוני טרור ישנים היו בנויים בצורת פירמידה היררכית ברורה (בדומה לארגונים אזרחיים או צבאיים גדולים) של מפקדות, מועצות ותאים אזוריים, הכפופים למפקדות כלליות וגופים מנהלתיים. לעומתם ארגוני טרור מודרניים, כדוגמת אל־קאעדה, מאופיינים במבנה "שטוח" – תאים רבים הפזורים ברחבי העולם,

157 Wittes, **לעיל** הערה 127, 227–228.

158 Weiman, **לעיל** הערה 34, עמ' 21.

ללא מפקדות וללא פיקוד היררכי ברור.[159] התאים מקיימים קשרים ארעיים עם תאים אחרים וארגונים אחרים, אך לא בצורה מסודרת ולא על בסיס קבוע. המנהיגים אינם נותנים פקודות מפורשות אלא מפרסמים ברשת מידע נגיש בצורה אנונימית. המוטיבציה הראשונית למבנה זה היא הצורך במידור מודיעיני של כל חוליה ממפקדיה ומהסובבים אותה. בצורה זו, חשיפה של תא אחד אינה גורמת לחשיפת תאים אחרים או מפקדות. כמו כן, כל תא שנחשף ניתן להחלפה במהירות בשל הגמישות הרבה של הארגון ואי־התלות שלו במפקדים. מוטיבציה נוספת היא שבאמצעות המבנה הזה נפתח כר רחב ליוזמות ולפעולות עצמאיות במידה רבה, כלומר המבנה מאפשר ומעודד גידול וריבוי פעילות טרור בלי לשאת בסיכונים הרגילים הכרוכים בגידול כזה (בעיקר סיכוני חשיפה).

האינטרנט הוא אמצעי התקשורת האידאלי למבנה זה של ארגון הטרור המודרני: האופי הגמיש והפומבי של הרשת מאפשר קיומם של תאים שונים, הפועלים באופן סמי־עצמאי ומסתפקים בהנחיות כלליות באמצעות פרסומים וכרוזים המתפרסמים באינטרנט.[160] כמו כן, היכולת להחליף כינויים ולשמור על קשר שאינו היררכי בין התאים קלה הרבה יותר באמצעות הרשת – למשל באמצעות פורומים שונים ותוכנות מסרים מידיים. הטרור הבינלאומי החדש, החוצה גבולות ומקיים קשרים בין ארגונים שונים, מושפע ישירות מהפשטות של יצירת קשר בינלאומי בעידן האינטרנט. אפשר לטעון שה"אבולוציה" שעוברים ארגוני הטרור מושפעת ישירות מקיומה של רשת האינטרנט, וייתכן שהרשת היא אחת הסיבות לשינוי שעוברים היום ארגוני הטרור.

שינוי המבנה הארגוני של הטרור מקשה מאוד על עבודת המודיעין. ארגון מסודר, שבו ההוראות יורדות בסדר היררכי ברור, הוא קל יותר לפיקוח, להבנה, לחשיפה ולמעקב לשם התרעה וסיכול. בעידן של ארגון הטרור הישן אפשר היה לעקוב אחרי פעילי הטרור באמצעות מעקב אחר המפקדות ושרשרת הפיקוד (למשל באמצעות מספרי טלפון או כתובות דואר אלקטרוני ספציפיים) ועל ידי כך לספק תמונת מצב של הארגון ולתת התרעה על פיגוע עתידי במקרה הצורך.

159 S. Shavit, "Contending with International Terrorism", *Journal of International Security Affairs* 6 (2004), p. 65

160 Weiman, **לעיל** הערה 34, עמ' 25.

ארגון הטרור החדש, שאינו פועל בצורה היררכית, מקשה מאוד על מעקב מסודר. יש לעקוב בו־זמנית אחרי תאים שונים – שאינם פועלים בתיאום מלא, שאינם מקבלים הוראות ישירות ושיכולים להיות "רדומים" לאורך שנים. לעתים המאפיין החשוד ביותר של תא כזה יהיה דווקא גלישה לאתרי אינטרנט של הארגון (לשם קבלת הנחיות כלליות בפרסומי הארגון), או העובדה שהתא אוסף מודיעין חשוד באינטרנט, מקיים קשר רופף עם תאים אחרים (לפי תוכן ההתקשרויות), מגייס כספים וכולי.

אפשר לטעון אפוא שהיום, כשמבנה הארגונים "שטוח" ולא היררכי, מתחייב שינוי בגישה המסורתית כדי לאפשר מעקב מודיעיני יעיל אחרי ארגון הטרור. השיטה המתבססת על מעקב לפי מספרי טלפון או כתובות דואר אלקטרוני ספציפיות, המשמשות פעילים החשודים בטרור, אינה יעילה עוד. כדי לזהות ולהתריע על קיומם של תאים הפועלים כמעט באופן עצמאי, ייתכן שיש לעקוב אחר **הרגלי גלישה** בשילוב עם מעקב אחר תכתובות דואר אלקטרוני לפי **תוכנן**. בכל אופן, גם אם אין זו בהכרח הדרך היעילה היחידה לעקוב אחרי ארגון הטרור החדש, יש לשים לב ששינוי המבנה של ארגוני הטרור פגע ביעילותו של המעקב המסורתי. מתחייבת אפוא מחשבה חדשה והכרחי לשקול את שינוי נוסחאות האיזון שהיו קיימות בעבר לגבי האזנות סתר. גם אם יוכרע לבסוף שהפגיעה החמורה בפרטיות – הכרוכה בשימוש בתכונות רחרחניות – אינה מוצדקת, תהיה הכרעה זו מבוססת על מודעות למחיר הכרוך בה ועל מוכנות לשאת במחיר זה. על כל פנים, אין הצדקה לקבל כמובנות מאליהן את נוסחאות האיזון הישנות.

ג. שינוי אופי התקשורת

השימוש המגוון שעושים ארגוני הטרור באינטרנט (כמפורט לעיל) מהווה אתגר גדול לרשויות אכיפת החוק. לעומת איסוף המודיעין המסורתי ואמצעי התקשורת האחרים, האופי הגמיש והאנונימי של הרשת הפך את התוכנות הרחרחניות לדרך היעילה ביותר ליירט תקשורת, מסיבות אלה:

- בניגוד למספרי טלפון, שהחלפתם כרוכה בזמן וכסף ולעתים היא מוגבלת מבחינה טכנית, הדואר האלקטרוני הוא משאב שנחשב היום כבלתי מוגבל. חברות רבות מספקות דואר אלקטרוני בחינם ואינן מגבילות את מספר הכתובות למשתמש. למעשה, ניתן להחליף כתובות ללא כל הגבלה. מעבר

לכך, בניגוד למספר טלפון המשמש משתמש ספציפי או מספר מצומצם של משתמשים, דואר אלקטרוני יכול להיות קיבוצי ולשמש משתמשים רבים בפינות שונות של העולם.

- התקשורת באמצעות צ׳טים ופורומים – שגם הם אינם דורשים שם קבוע של משתמש ספציפי – מספקת לארגוני הטרור כלי יעיל ומהיר שלא היה קיים בעבר.
- ההתקשרות באמצעות פרסום כרוזים פומביים ברשת, גלויים או חסויים, מאפשרת העברת מסרים בלי להפנותם ישירות אל כתובת ספציפית. הדרך היחידה ״ליירט״ מסר כזה היא באמצעות מעקב אחר המתפרסם באתרי האינטרנט של ארגוני הטרור, וכן מעקב אחר גולשים שנכנסים לאתרים אלה.

בניגוד לאמצעי התקשורת הישנים, התקשורת באינטרנט הופכת את יחידת הקצה (מכשיר הטלפון, כתובת הדואר האלקטרוני) לפחות קבועה ומזוהה, ולכן קשה יותר לעקוב אחרי התקשורת ולאתרה. כדי ליירט תקשורת של פעילות חשודה אין מנוס מזיהוי הפעילות החשודה על סמך **תוכנה** החשוד, ואי־אפשר להסתפק **בזיהוי יחידת הקצה** המשויכת למשתמש החשוד.

ד. שינוי טכנולוגיית ההאזנה

יש אפוא מקום לחשיבה מחדש על כללי ההאזנה הקיימים, ובעיקר על הדרישה שכל צו האזנה יהיה ספציפי, לגבי אדם או מספר טלפון מסוים. הרציונל העומד מאחורי כללים אלה הוא הגבלת הרשויות מפני האזנות רחבות מדי, העלולות לגרום פגיעה חמורה מדי בפרטיות. אך יש לזכור שכללים אלה עוצבו בעבר, כאשר אמצעי ההקלטה וההאזנה היו שונים לחלוטין.

ניתן לדמיין מצב (שעם ההתקדמות הטכנולוגית, ייתכן שהוא אינו רחוק) שבו אפשר להאזין לכל שיחות הטלפון שמתקיימות; מעבר לכך, כל שיחות הטלפון נסרקות (סריקה ממוחשבת) ונשלפות מתוכן רק שיחות בעלות תוכן פלילי חמור, או שיחות של בני אדם ספציפיים שהמערכת יודעת לזהות את קולם. אילו הייתה בידינו מערכת כזו, ששיעור ההצלחה שלה כמעט מושלם, ייתכן שעיצוב הכלל המשפטי לגבי צו ההאזנה היה אחר. במצב זה אפשר היה לעצב שני סוגים של צווי האזנה: צו האזנה המאשר להאזין לאדם ספציפי (בכל מספר טלפון שבו המערכת מזהה את קולו) וצו האזנה המאשר להאזין לכל

שיחה שבה נמצא תוכן חשוד על פי משוואות (המגדירות מהו חומר חשוד) שאושרו על ידי בית המשפט. מובן שצווים כאלה צריכים להיות מגובים במעקב אחר השיחות שעולות מתוכן כדי לוודא שאין בהן שיעור גבוה של שיחות תמימות. אילו הייתה מערכת כזו עובדת ביעילות, רשויות האכיפה היו מקבלות כיסוי טוב יותר של הפעילות הפלילית, וגם מבחינת הפגיעה בפרטיות ייתכן שהיה בכך יתרון.

נחזור מהדמיון למציאות. במצב הנוהג היום, שלפיו ההאזנה היא לקווים ספציפיים, התוצאה הבלתי נמנעת היא ששיחות פרטיות רבות של בני משפחה, עמיתים לעבודה ואחרים מוקלטות ונשמעות על ידי רשויות האכיפה. במצב הדמיוני שתואר למעלה רק השיחות הרלוונטיות ביותר היו מוקלטות, נשמרות ונשמעות. לו היינו חיים במצב דמיוני זה (שכאמור אפשר שהוא קרוב), ייתכן מאוד שהאיזון היה מעוצב בצורה שונה. אך משום שבזמן שעוצבו הכללים, אמצעי ההאזנה וההקלטה של הרשויות היו מוגבלים למספר קווים ולא היה אפשר לבצע סינון מכני אלא רק על ידי בני אדם, הדרך היחידה להגביל את הרשויות משרירותיות הייתה להגבילן להאזנה לקווים ספציפיים, על פי חשד נגד אדם ספציפי.

נוסחאות האיזון הקיימות מתאימות אפוא, עדיין, להאזנה לטלפונים. אך יש לבדוק אותן שוב באשר להאזנה לרשת האינטרנט. ראשית, יש לשים לב שמגבלת האגירה, ההקלטה, והסינון לפי תוכן של דואר אלקטרוני (ואף יותר מזה של פרטי גלישה אחרים) כמעט שלא קיימת, לעומת המגבלה הקיימת לגבי שיחות טלפון. התעבורה ברשת עוברת בצורת טקסט, ולכן אגירתה פשוטה הרבה יותר. מעבר לכך, האפשרות לשלוף ידיעות לפי תוכנן כבר איננה דמיונית אלא קיימת במציאות. נוסף על כך, בעוד שזיהוי על פי קול הוא מסובך ודורש משאבים עצומים, זיהוי גולש לפי חתימה, סגנון הכתיבה או "לחיצת ידיים" וירטואלית (חתימה, סיסמה) הוא פשוט הרבה יותר. מכאן שבאינטרנט ניתן לעצב כלל איזון אחר שאינו מגביל את רשויות האכיפה לפי יחידת הקצה דווקא (כתובת הדואר האלקטרוני), אלא מאפשר לה "עוגנים" אחרים – לפי תוכן או לפי זיהוי המשתמש בדרך אחרת.

אפשרות נוספת להציג טיעון זה היא להרהר בשאלה עד כמה החיפוש באמצעות מחשב אכן פוגע בפרטיות. כאמור, כמעט כל הודעת דואר אלקטרוני

שלנו עוברת סינון ממוחשב לאיתור "דואר זבל", ואנו לא רואים בכך פגיעה בפרטיות. כאשר תוכנה עוברת על הודעות הדואר שלנו ומאתרת רק את ההודעות החשודות בטרור, הפגיעה בפרטיות היא פחותה מאשר בהאזנה הקלסית.[161] האיזון הישן היה מבוסס על כך שכדי להאזין יש צורך באדם שיישב וישמע שיחות או יקרא התכתבויות ויברור את החומר החשוד. ויטס משווה את פעולת התוכנה החדשה (הרחרחנית) לפעולת ההשוואה של DNA שנמצא בזירת פשע עם מאגר ה־DNA הקיים אצל רשויות האכיפה. לכאורה **כל** האנשים הכלולים במאגר עוברים סוג של חקירה (אפשר להשוות את זה למסדר זיהוי המוני), ובכל זאת איננו רואים כל בעיה בכך. עם זאת יש כמובן הבדל, מבחינת הפגיעה באינטרס הפרטיות, בין קריאת תוכן התקשרות ובין נתוני DNA.

כדי לאפשר לרשויות שימוש בתוכנות הרחרחניות, נהיה חייבים להתגבר על הבעיות העיקריות שהועלו כנגדן: ה־false positive וקשיי הפיקוח על הרשות, כולל האפשרות של ניצול התוכנות לשם profiling, וכן עניין "המדרון החלקלק" – המעבר משימוש בתוכנה למניעת טרור לשימוש בה לשם מניעת פשיעה באופן כללי. אם נצליח לנטרל קשיים אלה, ייתכן שאפשר יהיה, בהקשר של האזנה לאינטרנט, להמליץ על השימוש בתוכנות אלה.

ה. תוכן התקשורת מול נתוני התקשורת

כפי שפורט לעיל, בכל הקשור ל"נתוני תקשורת" קיים בעולם קונצנזוס שפרטיותו של אדם היא אינטרס חלש לעומת אינטרס הפרטיות שלו בתוכן ההתקשרות. גם בעבר המשטרה הייתה יכולה לקבל פירוט של שיחות טלפון, ובשנים האחרונות היא יכולה לקבל אף מיקומים של טלפונים סלולריים, ללא צורך לעמוד בתנאי חוק האזנת סתר. בהמשך לאותו קו, ההפרדה בין תוכן לנתוני תקשורת היא שהולידה את המגמה שכל מה שאיננו תוכן – ובימינו: פירוט ההתקשרויות והקשרים בדואר האלקטרוני, וגם נתוני הגלישה באינטרנט – כפוף לסטנדרטים אחרים, מקלים הרבה יותר. עם זאת לדעתי מוטב לחשוב שנית על הבחנה זו

161 Witten, **לעיל** הערה 127, עמ' 249–250.

ולשאול עד כמה היא מהותית ואם באמת יש הבדל תהומי, מבחינת הפגיעה באינטרס הפרטיות, בין נתוני התקשורת לבין תוכן ההתקשרות.

בימינו – באמצעות נתוני התקשורת – ניתן לדעת **עם מי** דיברנו, **מתי** דיברנו **והיכן היינו**. באמצעות נתוני הגלישה ניתן לדעת פרטים רבים על עיסוקנו המקצועי, עיסוקינו בשעות הפנאי, העדפות ותחביבים, רכישות שאנו מבצעים, מטרות ותנועות שאנו מזדהים אתן, אתרים שבהם אנו רשומים ושיכולים להצביע על הזדהות פוליטית, על מצב בריאותי, על קשיים אישיים ועוד. באמצעות נתוני התקשורת של הדואר האלקטרוני אפשר ללמוד את שמותיהם של חברינו ובני משפחתנו.

לדעתי, אף שההבדל בין תוכן לבין נתוני תקשורת איננו חסר משמעות, יש לחשוב שנית אם הבדל זה מצדיק גישה כל כך מתירנית לגבי נתוני התקשורת מחד גיסא, וגישה כל כך שמרנית וזהירה לגבי התוכן (כאשר אין חשד ספציפי) מאידך גיסא.

ברור שטיעון זה אינו מצדיק כשלעצמו את השימוש בתוכנות רחרחניות ואת הסינון לפי תוכן. ייתכן שהמסקנה מביקורת זו היא שיש דווקא להילחם בהרחבת הגישה של רשויות הביטחון לנתוני התקשורת. בלי להרחיב בעניין זה, משום שלא זה הנושא שבו אני מתמקד, אומר רק שחוק נתוני תקשורת הישראלי הוא בהחלט רחב ופוגע יותר מדי בזכות לפרטיות – בעיקר בשל העובדה שהוא מופעל לגבי עבֵרות רבות מדי, כולל עבֵרות עוון (כאשר ניתן צו שופט) ועבֵרות פשע קלות (כל עבֵרת פשע), אף ללא צו של שופט.

עם זאת הטיעון יכול גם להצדיק חשיבה מחודשת על "קדושת" התוכן מול חילול נתוני התקשורת. ייתכן שדווקא ההגנה החזקה על תוכן ההתקשרויות היא שהולידה את הצורך לפגוע קשות בפרטיות בכל הקשור לנתוני התקשורת. לכן טיעון זה יכול לחזק גישה האומרת שבמקביל להקשחת התנאים המאפשרים קבלת נתוני תקשורת באופן כללי, ייתכן שיש לאפשר באופן מוגבל ומפוקח את השימוש בסינון על פי תוכן על מנת לתת לרשויות כלי אפקטיבי במלחמתן בטרור.

9. סיכום והמלצות

א. הערה על הרלוונטיות הטיעונים לגבי ישראל

האם הטיעונים שהועלו במאמר זה רלוונטיים לישראל ולמאבקה בטרור? הרי הטיעון לגבי מבנה ארגוני הטרור והשימוש שעושים הארגונים באינטרנט מבוסס בעיקר על ארגון אל־קאעדה ולא על ארגוני הטרור הפלסטיניים או חזבאללה. המענה לשאלה זו מחולק לכמה רבדים.

ראשית, יש לציין שגם ארגוני הטרור הפלסטיניים וחזבאללה, שעמם מתמודדת ישראל באופן תדיר, מקיימים פעילות ענפה ברשת האינטרנט, בהיקף הולך וגובר. הטיעונים באשר להתעצמות הטרור ומשמעותו האזורית וכן הטיעון לגבי השינוי באמצעי ההאזנה תקפים אף הם לגבי ארגונים אלה. יוצא אפוא שהטיעון היחיד שאיננו רלוונטי לגבי ישראל הוא שינוי המבנה הארגוני, שתקף בעיקר לגבי ארגוני הג׳האד העולמי ובראשם אל־קאעדה. אכן יש בכך כדי להחליש את הטיעון, ככל שמדובר בישראל.

שנית, חשוב לזכור שגם ארגון אל־קאעדה שם לו כמטרה אסטרטגית את הפגיעה בישראל. ארגון זה מצהיר תדיר, בכלל זה על ידי מנהיגיו אוסאמה בן לאדן ואימן אלט׳ואהרי, על הצורך להילחם ולפגוע בישראל (בציונים־ביהודים). במסמך ההקמה שלו נקרא הארגון "החזית העולמית האסלאמית למאבק בצלבנים וביהודים", וכמה פיגועים אף בוצעו בפועל נגד מטרות ישראליות, בהם הפיגוע במומבסה בשנת 2002 והפיגוע המשולב בשנת 2004 בסיני ובטאבה. כמו כן סוכלו מספר התארגנויות שכוונו כנגד תיירים ישראלים, ובהם התארגנות בטורקיה. ככל שאיום הג׳האד העולמי על ישראל ייהפך למוחשי וקונקרטי יותר, ייתכן שהטיעונים שהועלו בעד שימוש בתוכנות רחרחניות יכריע את הכף אל מול הפגיעה בפרטיות הנובעת משימוש זה. בכל אופן, מטרת הטיעונים היא לקבוע שהאיזון הקיים היום בין פרטיות להאזנות אינו מקודש, ואפשר להשתחרר ממנו כאשר הנסיבות מצדיקות זאת.

שלישית, גם אם יתברר שהשינוי המחשבתי שאני מציע אינו רלוונטי לישראל, עדיין הטיעון שהוצג תקף כשלעצמו לגבי מדינות הרואות עצמן כנפגעות מהג׳האד העולמי – בראשן ארצות הברית, הודו ומדינות אירופה. המאמר מעלה טיעון תאורטי שאין הכרח להפעילו בהקשר הישראלי דווקא.

ב. סיכום הטענה: הצורך בשקילה מחדש של האיזון המסורתי בין פרטיות לבין ביטחון

הטענה העיקרית שאותה ביקשתי להעלות במאמר היא שיש מקום לחשיבה מחודשת על נקודת האיזון בין הזכות לפרטיות לבין צורכי הביטחון, ככל שמדובר במניעת מעשי טרור. אין פירוש הדבר שכל הנעשה בימים אלה הוא מוצדק (בעיקר בכל הקשור לחקירות **שאינן** קשורות בטרור, למשל על פי חוק נתוני תקשורת), ולכן אני סבור שראוי לבקר ואף להצר את צעדיהן של הרשויות במקרים המתאימים.

עם זאת שילוב הטיעונים שהצגתי – התעצמות הטרור, השינוי במבנה הארגוני של ארגוני הטרור, והשינוי במאפייני התקשורת ובאמצעי ההאזנה – מחייב מחשבה על איזון חדש בין ההגנה על הביטחון לבין הזכות לפרטיות.

לדעתי, בעתיד הקרוב תיאלץ ישראל ככל הנראה לאמץ את המסקנה שסינון על פי תוכן באמצעות תוכנות רחרחניות הוא הכרחי, למרות הפגיעה בפרטיות, משום שתמונת האיומים תכלול איום ממשי מצד הג׳האד העולמי, או משום שהארגונים האחרים שעמם מתמודדת ישראל יהפכו דומים לארגוני הג׳האד העולמי. בהקשר של הלחימה בטרור נראה שעדיף להתמקד ולצמצם את הפגיעה בפרטיות שנובעת מהשימוש[162] בתוכנות אלה, אך לא לוותר על הפעולה החיונית שלהן בגילוי ובמעקב אחר ארגוני הטרור. כיצד אפשר אפוא למזער את הפגיעה בפרטיות בלי לוותר על השימוש בתוכנות רחרחניות?

ג. אמצעים למזעור הפגיעה בפרטיות על אף השימוש בתוכנות רחרחניות

הגבלת השימוש לגוף מוגדר ומצומצם

יש להגביל את השימוש בתוכנות רחרחניות למספר מצומצם של אנשים ברשות הביטחונית שיעברו הליכים קפדניים של מיון (לרבות בדיקות פוליגרף), לשם הבטחת אמינותם ומחויבותם לשמירת סוד. אנשים אלה יהיו אחראים בלעדית על המעקב והפיתוח של התנאים הלוגיים שלפיהם יתבצע סינון התוכן והרגלי הגלישה.

162 **שם**, עמ׳ 240.

מניעת זליגה של מידע

יש למנוע זליגת חומרים ש"נתפסו" על ידי התוכנה הרחרחנית לכלל המערכת הביטחונית – כולל חומר שמעיד על פשיעה (שאיננה טרור). יש לאכוף איסורים אלה על ידי סנקציות מרתיעות.

מעבר למסלול הרגיל

לאחר אפיון של קבוצה חשודה (והצטברות ראיות מפלילות), אם לפי כתובת הדואר האלקטרוני ואם לפי כתובת ה־IP של מחשב מסוים, ניתן להעביר את הפיקוח – לאחר קבלת צו כמקובל לפי חוק האזנת סתר – להמשך מעקב ב"מסלול הרגיל", על פי כתובות דואר אלקטרוני חשודות.

הגבלה לשימוש ביטחוני בלבד

שימוש בתוכנות רחרחניות יכול להביא תועלת רבה גם בחקירת פשיעה רגילה, אולם הצידוקים שלעיל, החלים כלפי ארגוני טרור, לא חלים לגבי פשיעה רגילה. בפשיעה המאורגנת לא קיימים עדיין, למיטב ידיעתי, מאפיינים של מעבר מובהק לשימוש ברשת האינטרנט כאמצעי תקשורת, או תאים רדומים והיעדר היררכיה. עם זה ברור שהפגיעה בפרטיות הגולשים תהיה קשה ביותר אם המשטרה תיעזר באופן רגיל בתוכנות רחרחניות לשם איתור פשעים וחקירתם. לכן יש להבטיח שהשימוש בתוכנות רחרחניות יהיה רק במסגרת המאבק בטרור.

פיקוח רצוף על פעילות התוכנה

ישנם אמצעים שונים של פיקוח שאפשר להשתמש בהם בנפרד או במשולב כדי למזער את השימוש לרעה בתוכנות הרחרחניות ואת הבעיות הנוספות שעולות בהפעלתן. אין בדעתי להעלות הצעה מפורטת בעניין זה, אך ראוי שהפיקוח יתמקד ברבדים אלה:

פיקוח משפטי

גוף מצומצם – שיכלול את היועץ המשפטי, שופט בית המשפט העליון בדימוס ועורך דין בכיר מהמגזר הפרטי – יפקח ויבקר את השאילתות הניתנות לתוכנות הרחרחניות (ובכך יוודא, למשל, שלא נעשה בהן שימוש לצורכי profiling). גוף

זה יראה דוגמאות של החומר שנאסף ויקפיד על כך שלא ייעשה שימוש לרעה בתוכנה. ראוי שתהיה לגוף זה סמכות להורות על הפסקת השימוש בתוכנות, הגבלתן ומחיקת חומר שנאסף שלא כדין.

אפשר להציע שרק לוועדה זו תהיה הסמכות לאשר העברת גורם מסוים לפיקוח ב"מסלול הרגיל" ובכך לחשוף את זהות המשתמש. לפי הצעה זו, שמעלה ויטס, ניתן לצמצם את הפגיעה בפרטיות על ידי הגבלת החשיפה של זהות המשתמש באישור גוף שיפוטי. כך תהיה הגישה למידע עצמו קלה יחסית (באמצעות התוכנה), אך הגישה לפרטי המשתמש – בהנחה שאינם גלויים מתוכן ההתקשרות – תצטרך לעבור ביקורת נוספת ותתקבל רק על סמך חשד סביר שעלה מהחומר, שלא היה נתפס ללא השימוש בתוכנה.[163]

פיקוח פוליטי

ראוי שוועדה מיוחדת בכנסת (כגון ועדת חוקה, חוק ומשפט או ועדת חוץ וביטחון) תקבל דיווח שוטף על מספר ההתכתבויות שהתוכנה יירטה, ההישגים שהושגו באמצעותה ומספר הטעויות (false positive) שהיא עושה.

פיקוח תקופתי מקצועי

יש להקים ועדה מקצועית בלתי תלויה שתורכב מאנשים ששירתו בגופי מודיעין וביטחון וגם מאנשים ש"מחוץ למערכת" לצורך הערכה תקופתית של יעילות המערכת ולמענה על השאלה אם הישגיה מצדיקים את מחיריה.

יידוע האוכלוסייה

העובדה שקיימת מערכת שקוראת את כל התעבורה באינטרנט חייבת להיות גלויה לציבור. אמנם יש לכך מחיר – צמצום המודיעין כתוצאה מזהירות יתר של פעילי הטרור בשימוש באינטרנט (אף שאין אפשרות לשמור על אנונימיות מוחלטת כל הזמן, תוך עמידה בעלויות נמוכות ובנוחות הגישה לרשת), ו"האפקט המצנן" על גלישת כלל האזרחים התמימים. אולם לדעתי מכריע את הכף השיקול שאסור לעשות מעשה כה פוגעני בסתר ובלי ידיעתם של האזרחים. כמו כן, הצורך הברור לתקן את חוק האזנת סתר (או לחוקק חוק ספציפי לגבי

163 **שם**, עמ' 251.

האזנה לתקשורת מחשבים) לשם מתן אפשרות לשימוש בתוכנות אלה מחייב דיון ציבורי ופרסום העובדה שקיימת אפשרות לשינוי חקיקה כזה. מובן שאין צורך לפרט את יכולתן של המערכות ואת סוגי החומרים שאותם הן מחפשות.

ד. סיכום

הנימוקים שהצגתי מצביעים על כך שאין מניעה עקרונית ששירותי הביטחון ישתמשו בתוכנות רחרחניות לאיתור פעילי טרור ותעבורה חשודה באינטרנט. יש להדגיש שדרוש לשם כך מעבר על כל תכתובות הדואר האלקטרוני, ככל שהטכנולוגיה מאפשרת זאת. מרגע שאופיינו כתובות האינטרנט או כתובות IP החשודות בטרור (שאינן false positive) יהיה על היחידה המבצעת את המעקב לקבל אישור ספציפי למעקב, כנהוג היום. את הפגיעה בפרטיות ניתן לצמצם באמצעות שימוש מבוקר וממודר (ובאמצעות שאילתות ממוקדות) ובהצטמצמות להגנה מפני טרור בלבד, תוך פיקוח הדוק על פעילות זאת. כמו כן נדרש כאמור יידוע הציבור. עם זאת יש להדגיש שכל עוד לא ניתן להבטיח את צמצום הפגיעה בפרטיות ואת הפיקוח ההדוק על הפעלת התוכנות הרחרחניות (זהו המצב היום, בטרם קיימים מנגנוני הפיקוח הנחוצים) ראוי להשאיר את המצב הקיים על כנו ואין לאפשר האזנה גורפת. בכל הקשור לישראל אפשר לטעון שהאיום עליה מצד ארגוני הטרור העולמיים טרם הגיע לרמה שמצדיקה פגיעה חמורה בפרטיות, הנובעת מהפעלת תוכנות רחרחניות. כאמור, ייתכן שבאשר למדינות אחרות עשויה להתקבל תוצאה שונה.

מובן שאפשר להכריע אחרת, להתנגד נחרצות ולשלול גם בעתיד ובכל צורה את הפגיעה האינהרנטית בפרטיות, המתחייבת מהפעלת התוכנות הרחרחניות. עם זאת חייבים להכיר בתוצאות של הכרעה כזו – פגיעה גדלה והולכת ביכולת המודיעינית של רשויות הביטחון הנלחמות בארגוני הטרור המודרניים.