

חוק השב"כ – בין פרטיות לביטחון

מאת

הלל זרם*

מבוא

בשנים האחרונות, בעקבות ההתפתחות המואצת של האמצעים הטכנולוגיים, התגבר המתח בין הזכות לפרטיות של אזרחי מדינת ישראל ובין הביטחון הלאומי. מאמר זה יתמקד במתח ובאיזונים הנדרשים בסוגיה זו. מחד גיסא, השמירה על האינטרס הציבורי של ביטחון המדינה מעוררת לעיתים צורך לבצע חדירה לפרטיות של אזרחים חשודים בטרור. כמו כן, הטכנולוגיה הקיימת מאפשרת למדינה לבצע חיפוש ומעקב אחר גורמים החותרים תחתיה, על ידי חדירה למחשבים וטלפונים.¹ מאידך גיסא, האפשרויות הטכנולוגיות בכלל, והאפשרות לחדירה למחשבים בפרט, מקנות למדינה פוטנציאל לפגיעה בזכותם של האזרחים בפרטיות, זכות שעוגנה בחוק יסודי: כבוד האדם וחירותו.² המאמר יסקור את דרכי ההתמודדות של מדינת ישראל עם מתח זה, ואת הדין המצוי בנושא. בתוך כך יתמקד המאמר בחוק השב"כ.³ חוק זה מסמיך את גוף הביון הישראלי לחיפוש ולמעקב אחר חשודים בטרור, על מנת למנוע את פעילותם הבלתי חוקית. עם זאת אין התייחסות מפורשת בחוק לאפשרות של חדירה למחשבים וטלפונים, כחלק מהליך החיפוש והמעקב. בפרט, ינסה מאמר זה לענות על השאלה, האם נוסח החוק הקיים מסמיך את רשויות הביון לבצע פעילות של תקיפת מחשבים על מנת למנוע פעילויות טרור, ואם לא, מה נדרשת מדינת ישראל לעשות על מנת לבצע פעולות אלה באופן חוקי ותוך פגיעה מצומצמת בזכות לפרטיות. לצורך כך, המאמר יתייחס לאיזון הקיים בין האינטרס הציבורי בביטחון לאומי ובין הזכות לפרטיות, בתחומים משיקים

* תלמיד תואר ראשון בפקולטה למשפטים ותואר שני למדעי המדינה באוניברסיטת בראילן.

¹ מיכאל בירנהק "פרטיות: תמונת מצב" משפט, חברה ותרבות ב 9 עמ' 10-12 (2019).

² ס' 7 לחוק יסודי: כבוד האדם וחירותו.

³ ס' 10-7 לחוק שירות הביטחון הכללי, התשס"ב-2002. (להלן: חוק השב"כ).

במשפט הישראלי. בסוף המאמר אעלה את הצעתי להתמודדות עם הסוגיה, שלפיה על ידי חקיקה מפורשת וסמכות מפקחת, המדינה יכולה להיאבק בטרור תוך פגיעה מוצדקת ומידתית בזכות לפרטיות.

א. הזכות לפרטיות בחקיקה ובפסיקה

הזכות לפרטיות מעוגנת בסעיף 7 לחוק־יסוד: כבוד האדם וחירותו,⁴ כזכות חוקתית, שכל פגיעה בה תיעשה אך ורק לפי פסקת ההגבלה שבסעיף 8 לחוק.⁵ כלומר, "בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שאינה עולה על הנדרש או לפי חוק כאמור מכוח הסמכה מפורשת בו". לאחר עיגונה של הזכות לפרטיות במפורש בחוק־יסוד: כבוד האדם וחירותו, התייחסה הפסיקה לזכות לפרטיות בתור זכות בעלת מעמד חוקתי על־חוקי.⁶ הזכות לפרטיות הוכרה בפסיקה עוד לפני עיגונה בחוקי היסוד. אומנם בתחילת ימיה של המדינה סירב בית המשפט להכיר בעוולה על בסיס הזכות לפרטיות,⁷ אך מסוף שנות ה־70 ניתנו פסקי דין אשר פסלו הוראות מינהליות על סמך פגיעה בזכות לפרטיות.⁸

עוד בטרם עוגנה הזכות לפרטיות בתור זכות חוקתית, הכנסת חוקקה גם את חוק הגנת הפרטיות שקבע שפגיעה בזכות היא עבירה פלילית ועוולה אזרחית.⁹ החוק אינו מגדיר את היקף הזכות, ובמקום זאת מציין מספר התנהגויות שייחשבו לפגיעה בפרטיות. עם זאת החוק מחריג את רשויות הביטחון מתחולת החוק, בתנאי שפגיעתן בפרטיות תיעשה באופן סביר ולשם מילוי תפקידם.

ב. האיזון המצוי בין הזכות לפרטיות לאינטרס הציבורי בשמירה על הביטחון

מהפכת המידע והטכנולוגיה הביאה עימה יתרונות רבים וחשובים, כמו שימוש בטלפון נייד, גלישה באינטרנט לחיפוש מידע ועוד שלל יכולות שהפכו לחלק בלתי נפרד מחיינו. האפשרויות הרבות שמציעה הגלישה באינטרנט, יחד עם הנוחות בשימוש והעלות הנמוכה, סייעו להפיכתה לתקשורת אטרקטיבית ובינלאומית. כחלק מכך, כמעט כל פעולה של גלישה באינטרנט מותירה אחריה עקבות

⁴ ס' 7 לחוק־יסוד: כבוד האדם וחירותו.

⁵ שם, בס' 8.

⁶ בש"פ 537/95 גנימאת נ' מדינת ישראל, פ"ד מט(3) 375, 355 (1995).

⁷ ע"א 68/56 רבינוביץ נ' מירלין, פ"ד יא 1224 (1957): "גם 'זכות הפרטיות' לא יכלה לעמוד למערערת כעילת תביעה לפי המשפט הישראלי. אין לזכות מעין זו זכר ברשימת מעשי העוולה האזרחיים שבפקודת הנוזקים האזרחיים, ואשר לשאלת ה'יבוא' של עילה כזאת מן המשפט המקובל האנגלי, מכל מקום אין מה לייבא משם, כי עד כה לא הכירו בתייהמשפט באנגליה בסוג תביעה כזה, בה מבקש אדם להגן על עצמו כנגד פגיעה על־ידי פרסום תמונתו ברבים ללא נטילת רשות ממנו".

⁸ בג"ץ 355/79 קטלן נ' שירות בתי הסוהר, פ"ד לד(3) 294, 308 (1980), בדברי הנשיא לנדוי: "כללו של דבר, גם לי נראה שאת הנושא הזה אין להסדיר, מפאת הפגיעה בזכות לפרטיות גופו של אדם, בדרך הנחיות מינהליות ואף לא בדרך חקיקת משנה אלא רק בדרך חקיקה ראשית או מכח הסמכה ברורה בחקיקה ראשית". ראו גם בג"ץ 259/84 מ.ג.ל.ן בע"מ – מכון ישראלי למוצר ולעסק הנבחר בע"מ נ' רשות השידור, פ"ד לח(2), 673 (1984).

⁹ ס' 4 לחוק הגנת הפרטיות, התשמ"א-1981, ס"ח 128.

דיגיטליים המאפשרים לתעד פעולות רבות בחיינו.¹⁰ לצד זאת, הרשת מאפשרת לאנשים לפעול באנונימיות ובכך מעניקה פלטפורמה נוחה לעבריינים ולפעילי טרור, שיכולים לאסוף מידע רב ברשת ולתכנן את מעשיהם הבלתי חוקיים. בשל בעיה זו, רשויות הביטחון בעולם ובישראל הבינו כי על מנת להתחקות אחר גורמים אלה ולסכל את פעולתם, עליהם לפעול דרך הרשת ובכך לנצל את היתרונות הטכנולוגיים הגלומים בה. פעולות איסוף המודיעין של רשויות הביטחון, נעשות בדרך כלל תוך סריקה מקיפה של המידע וההודעות הקיימות במכשירים של החשודים, ולכן לעיתים נדרשת סריקה גם של הודעות של אזרחים תמימים. איסוף מסוג זה, אומנם תורם לאינטרס הציבורי בשמירה על הביטחון, אך פוגע בזכות לפרטיות.¹¹

מדינת ישראל מנסה לאזן מתח זה מבחינה משפטית על ידי חקיקה המעניקה סמכות לשירותי הביטחון לפעול בזירות הטכנולוגיות, אך באותה נשימה גם מגבילה את אותן רשויות.

1. חוק האזנת סתר

חוק אחד שנכלל בניסיון לאיזון, הוא חוק האזנת סתר.¹² חוק זה מסדיר במפורש האזנות לשיחות הכוללות שיחות בטלפונים, במכשירי קשר ובפקסים, וכן מסדיר האזנה לתקשורת בין מחשבים.¹³ החוק מצד אחד קובע איסור כללי, לפיו האזנה לשיחה ללא הסכמת השותפים לה, היא עבירה פלילית שדינה חמש שנות מאסר. מאידך, החוק קובע מספר חריגים לאיסור זה, הנוגעים לביטחון המדינה. סעיף 4 לחוק מעניק לשר הביטחון או לראש הממשלה סמכות לאשר בקשת האזנת סתר שהתקבלה מאגף המודיעין בצה"ל או מהשב"כ, אם שוכנע שההאזנה באותו מקרה נדרשת לטובת שמירה על ביטחון המדינה.¹⁴ בהיתר מסוג זה דרוש תיאור של זהות האדם או הקו או המתקן שעליהם תבוצע האזנה וכן פירוט לגבי שיטות האזנה שהותרו. ההיתר קצוב לעד 3 חודשים, אך ניתן לחידוש. בנוסף, ישנה חובת דיווח לוועדה משותפת של ועדת חוקה חוק ומשפט ושל ועדת החוץ והביטחון של הכנסת אודות מספר ההיתרים שניתנו על פי סעיף 4. סעיף 5 לחוק מתיר לראש אגף המודיעין בצה"ל או לראש השב"כ להעניק היתר לביצוע האזנת סתר במקרים דחופים.¹⁵ עם זאת, תוקף ההיתר הוא ל-48 שעות, ויש לעדכן מיד את שר הביטחון או ראש הממשלה והיועץ המשפטי לממשלה ולשניהם קיימת הסמכות לבטל את ההיתר.

2. חוק השב"כ

חוק מרכזי נוסף שמתעסק באפשרויות ובמגבלות אלו הוא חוק השב"כ. חוק זה מעגן את סמכותו של השב"כ לקבל נתונים מספקי אינטרנט כולל כתובות, דואר אלקטרוני, מספרי טלפון ועוד, למעט תוכן שיחה, אם ראש הממשלה קבע שפעולה זו נחוצה למילוי תפקידו של שירות הביטחון הכללי. שימוש בנתונים אלה יעשה

¹⁰ עמיר פוקס "טרור ופרטיות" פרטיות בעידן של שינוי 231-232 (תהילה שוורץ-אלטשולר עורכת, 2012).

¹¹ שם.

¹² חוק האזנת סתר, תשל"ט-1979.

¹³ שם, בס' 1.

¹⁴ שם, בס' 4.

¹⁵ שם, בס' 5.

בהיתר מיוחד מראש השב"כ, ולמשך זמן מוגבל שלא יעלה על שישה חודשים.¹⁶ לפי סעיף 9 לחוק, מוסמך השירות לבצע חיפוש על גופו של אדם, בכליו, במטענו, בכלי רכבו או בטובין אחרים שבידיו, ולתפוס חפץ או לאסוף מידע למטרות מודיעין במעברי גבול. לפי סעיף 10 לחוק, השירות מוסמך לבצע חיפוש סמוי בכלי רכב ובחצרים למטרות מודיעין. בשני סעיפים אלה, המתייחסים לחיפוש בדברים שברשותו של אדם, ובשאר החוק, אין התייחסות ספציפית ומפורשת לחיפוש במחשבים וטלפונים, בניגוד לחוק האזנת סתר, בו קיימים הסדרים מפורשים. בפועל, לפי פרסומים שונים, השב"כ מבצע חדרות למחשבים וטלפונים, תוך שימוש בסמכות הכללית המוענקת לו בחוק, אך ללא הסמכה מפורשת.¹⁷

ג. השוואה לתחומים משיקים

1. תקנות הקורונה

הניסיון לאזן את המתח בין האינטרס הציבורי ובין הגנה על זכויות הפרט, קיים במחוזות משפטיים נוספים. לאחרונה, בשל התפרצות נגיף הקורונה במדינת ישראל, החליטה הממשלה כי יש להסמיך את שירות הביטחון הכללי על פי סעיף 7(ב)(6) לחוק השב"כ, לבצע איסוף, עיבוד ושימוש ב"מידע טכנולוגי" הנוגע לחולים מאומתים בנגיף הקורונה וכן לאנשים שבאו עימם במגע. על החלטה זו הופנתה ביקורת מצד חברי כנסת והאגודה לזכויות האזרח,¹⁸ שבהמשך הגישה עתירה לבג"ץ כנגד החלטה זו.¹⁹ ההכרעה שעלתה מפסק הדין הייתה כי על הממשלה לפעול לעיגון הבסיס למעורבות השב"כ בשימוש במידע טכנולוגי בחקיקה ראשית, שתהא זמנית ותיחקק כהוראת שעה. בעקבות דרישה זו, נחקק "חוק להסדרת האמצעים טכנולוגיים לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה", על מנת לצמצם את התפשטות המגפה. על פי אותו החוק, השב"כ רשאי לעבד מידע טכנולוגי לגבי החולה שהבקשה נוגעת אליו, ולגבי האנשים שבאו במגע קרוב עם החולה, רק לתקופה מסוימת ולפי ההנחיות המקצועיות של משרד הבריאות.²⁰ סעיף ההגדרות בחוק קובע מפורשות כי המידע הטכנולוגי אותו רשאי לעבד השב"כ כולל נתוני מיקום, ומגדיר שנתוני המיקום הם נתוני איכון של טלפון נייד.²¹ החוק מגדיר בנוסף את ההגבלות על השב"כ לשימוש במידע, כך שהשימוש יעשה לצורך ביצוע פעולות הסיוע בלבד.²² כמו כן, בחוק מפורטים נתונים רבים עליהם ישנה חובת דיווח לוועדת חוץ וביטחון וליועמ"ש, בניהם מידע אודות מספר החולים והבאים עם חולים במגע, שלגביהם התבקש השב"כ לעבד מידע טכנולוגי.²³

¹⁶ ס' 11 לחוק השב"כ.

¹⁷ רונן ברגמן ועידו שברצטוך "מאגר המידע הסודי של השב"כ" ידיעות אחרונות (25.03.2020); אריק ברברנינג "התמודדות השב"כ עם טרור הבוודדים" מרכז דדו (01.12.2019).

¹⁸ איתמר אייכנר "תקנות המעקב הסלולרי" ynet (17.03.2020).

¹⁹ בג"ץ 2109/20 בן מאיר נ' ראש הממשלה (נבו) (26.04.2020).

²⁰ ס' 5(א)(1) חוק להסדרת האמצעים טכנולוגיים לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הסמכת שירות הביטחון הכללי ופיתוח טכנולוגיות אזרחיות לאיתור מגעים (הוראת שעה), התש"ף-2020.

²¹ שם, בס' 2.

²² שם, בס' 14(א).

²³ שם, בס' 19(1) ובס' 19(2).

2. הדין הפלילי

תחום משפטי נוסף בו קיים מתח דומה, הוא התחום הפלילי. פקודת סדר הדין הפלילי, המסמיכה את המשטרה למעצר וחיפוש בגין חשד לעבירות פליליות, תוחמת את גבולות הגזרה של חדירה לחומר מחשב, בקביעתה כי חדירה לחומר מחשב וכן הפקת פלט תוך חדירה, יראו אותן כחיפוש, וייעשו על ידי בעל תפקיד המיומן לביצוע הפעולות הללו.²⁴ בהמשך הפקודה קובעת כי חדירה למחשב תבצע על פי צו של שופט בלבד, המציין במפורש את ההיתר לחדור לחומר מחשב או להפיק פלט, ומפרט את מטרת החיפוש ותנאיו כך שלא ייפגעו בפרטיותו של אדם מעבר למידה הנדרשת.²⁵ בנוסף, על מנת לשמור על פרטיותו של החשוד, המפקח הכללי של המשטרה יקבע הוראות נוספות לעניין חדירה למחשב, לצורך שמירה על הפרטיות.²⁶ בעניין המידתיות המצוינת בפקודה, אותה צריכים להביא בחשבון בתי המשפט כאשר הם נותנים צו חיפוש לחדירה למחשב, קבע השופט יוסף אלרון בדיון נוסף בפסק דין אוריך, כי על בית המשפט להפעיל שיקול דעת עצמאי, ולבחון האם מטרותיו ותנאיו של הצו אכן מתוחמים באופן מספק.²⁷ לפי אלרון, על בית המשפט לבחון זאת על פי כמה מדדים, בניהם – טיב ואופי המידע על בסיסו נטען כי הצו נחוץ, המטרה לשמה הצו מתבקש, חומרת העבירה וסוג המידע המצוי על המחשב או הטלפון הנייד.²⁸ בפסק דין האגודה לזכויות האזרח בישראל נ' משטרת ישראל, השופטת דורית ביניש מנתחת את המורכבות שבהצבת הגבולות להגנה על הפרטיות על רקע חשש מפני שימוש לרעה של המדינה במידע שהיא צוברת באמצעות הטכנולוגיה.²⁹ ביניש מנמקת את הסיבות בגינן יש בכל זאת לעשות בטכנולוגיה שימוש, בין היתר גם בחדירה למחשבים. לפי ביניש, הטכנולוגיה היא כלי הכרחי בידי השלטון, ומניעה משימוש בה עלולה לפגוע בחובת המדינה לאכוף את החוק. זאת, נוכח העובדה כי הכלים הטכנולוגיים מצויים אצל עבריינים וארגוני פשיעה ולא רק בידי הרשויות, ואי שימוש בכלים אלו תותיר את ידם של רשויות אכיפת החוק על התחתונה.³⁰ בפסק דין אחר של השופטת ביניש, פסק דין היינץ ישראל בע"מ נ' מדינת ישראל, שעסק באופן ספציפי בשאלת ההסדרה הראויה של חיפוש תוך חדירה למחשב, קבעה ביניש כי עקב הפוטנציאל לפגיעה בזכויות הפרט ביצוע חדירה למחשב, הסדרה חוקית של פעולות מעין אלו חשובה וחיונית.³¹ לפי ביניש השימוש הגובר במחשבים הופך אותם למאגר מידע עצום של ראיות מפלילות, שיכול לשרת את רשויות אכיפת החוק.³² נראה, אפוא, כי בתחומים משיקים אלה, בהם המדינה נאבקת למען שלום אזרחיה, הן בתחום הבריאותי והן בתחום הפלילי, ישנן הסמכות מפורשות במידה רבה יותר מאשר אלה הקיימות בחוק השב"כ בהקשר של מאבק בטרור. כך, על אף שקיימת בחוקים אלה פגיעה בפרטיות, הפגיעה נעשית בצורה מתונה ומבוקרת, ותוך פיקוח מתמיד, היות וגבולות הגזרה של הפגיעה וחובות האישור והדיווח כתובות מפורשות בחוק. לדעתי, טוב תעשה מדינת ישראל אם תפעל בדומה גם בזירת המאבק בפעולות הטרור.

²⁴ ס' 23 א(א) לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט 1969.

²⁵ שם, בס' 23 א(ב).

²⁶ שם, בס' 26 (ב).

²⁷ דנ"פ 1062/21 יונתן אוריך נ' מדינת ישראל (נבו) (11.01.2022).

²⁸ שם, בפס' 7 לפסק דינו של השופט אלרון.

²⁹ בג"ץ 3809/08 האגודה לזכויות האזרח בישראל נ' משטרת ישראל (נבו) (20.05.2012).

³⁰ שם, בפס' 5 לפסק דינה של השופטת ביניש.

³¹ רע"פ 8873/07 היינץ ישראל בע"מ נ' מדינת ישראל, בפס' 17 לפסק דינה של השופטת ביניש

(נבו) (02.01.2011).

³² שם, בפס' 17 לפסק דינה של השופטת ביניש.

3. הצעה לתיקון חוק השב"כ

כאמור, סעיף 10 לחוק השב"כ חסר הסמכה מפורשות לחיפוש בטלפונים ומחשבים של חשודים בטרור, בניגוד לתחומים משיקים במשפט הישראלי.³³ במסגרת פרק זה אעלה את העקרונות לפיהם לדעתי יש לתקן את חוק השב"כ, תיקונים המבוססים על סעיף 131 להצעת החוק למאבק בטרור.³⁴

לדעתי, יש לתקן את החוק כך שיהיה כתוב בו במפורש, אילו חיפושים הוא רשאי לעשות במחשבים וטלפונים של חשודים בטרור. סוגי החיפוש ייקבעו על פי עקרונות מגבילים, ובנוסף בקשות לצווי חיפוש יהיו נתונים לאישור ופיקוח של גורמים ממשלתיים, על מנת שהחוק יעמוד בתנאי פסקת ההגבלה.

על מנת לבצע חיפוש ותקיפת מחשבים, על ראש השב"כ יהיה לקבל אישור מראש הממשלה או שר הביטחון. בבקשת האישור יהיה על ראש השב"כ לפרט את חיוניות החיפוש, ולהסביר מדוע אין דרך אחרת להשיג את המידע הנחוץ. בנוסף, על ראש השב"כ יהיה לדווח על שימוש בסמכות זו ליועץ המשפטי לממשלה, בדומה לחובות הדיווח הקיימות בחוק האזנת סתר. בקשות מעין אלו יהיו אך ורק למניעת פעילויות טרור או פגיעה חמורה בביטחון המדינה. כמו כן, הבקשות יאושרו בכפוף לבדיקות תקופתיות של היועץ המשפטי לממשלה, שייבחנו אם השב"כ עומד בכמה עקרונות מגבילים המפורטים להלן:

— **עיקרון המידתיות** – לפיו הפגיעה בפרטיות תעשה רק במידה הדרושה לצורך השגת המידע ומניעת מעשה הטרור, ולא מעבר לכך.³⁵

— **עיקרון השקיפות המינימלית** – השב"כ יהיה מחויב לידע אזרחים אם ביצע חיפוש במחשביהם, אם הדבר לא פוגע בהמשך החקירה ובמניעת פעולות הטרור העתידות להתבצע.³⁶

— **עיקרון החשיפה המצומצמת** – ראש השב"כ ימנה מספר אנשים מצומצם ואמין, שיהיה אחראי בלעדי לחיפוש במחשבים וטלפונים, על מנת שהמידע הסודי והפרטי אודות החשודים לא יזלוג לגורמים זרים.³⁷

בנוסף, מאחר שעשויות להתקיים נסיבות חריגות בהן ביצוע החיפוש נחוץ באופן מיידי, ראש השב"כ יהיה רשאי לאשר פעולות אלה לתקופת זמן מוגבלת שתיקבע בחוק, וידווח על כך באופן מיידי לראש הממשלה.

³³ אריאל צימרמן **הצעת חוק השב"כ: ניתוח משווה עמ' 9** (מחקרי מדיניות 3, 1997). ביקורת כללית ודומה לכך עלתה במאמר זה.

³⁴ ס' 131 להצעת חוק המאבק בטרור, התשע"א-2011, ה"ח 611.

³⁵ מטרתו של עיקרון המידתיות היא איזון בין תכלית ציבורית והאמצעים לקידומה ובין זכות או אינטרס פרטי מוגן. רשויות מינהליות נדרשות לעמוד בעיקרון זה. ראו לדוגמה: בג"ץ 3477/95 **בן עטייה נ' שר החינוך, התרבות והספורט**, פ"ד מט(5) 1, בפס' 2-5 לפסק דינו של השופט אהרון ברק (1996). בפסק דין זה סוקר ברק את תולדות תורת המידתיות במשפט הישראלי.

³⁶ יובל שני ועמיר כהנא "מתחת לרדאר: מערב מקוון בישראל" **המכון הישראלי לדמוקרטיה** (13.3.2017). במאמר זה מציעים שני וכהנא לחזק את הבקרה המוסדית על ידי מינוי של נציב עצמאי להגנת מידע. לפי ההצעה, הנציב יוכל להתייחס לתלונות על שימוש לרעה בסמכויות של רשויות הביטחון, וכך לשמור על עיקרון השקיפות והיידוע.

³⁷ כך, בשילוב עם עקרונות המידתיות והשקיפות המינימלית, תצטמצם הפגיעה בפרטיות למינימום הנדרש.

סיכום

הזכות לפרטיות במדינת ישראל מוכרת כזכות בסיסית, המנויה בחוקי היסוד. עם זאת, לעיתים יש לאזן זכות זו אל מול האינטרס הלאומי בשמירה על הביטחון, במיוחד במדינה בה הטרור האזרחי רווח ולאור ההתפתחות הטכנולוגית התופסת תאוצה בשנים האחרונות, המאפשרת חדירה משמעותית יותר לפרטיות האזרח. כמו כן, לאור סקירת הנושא, ניכר שחסרה פסיקה ונדרשת עבודה תחקיקתית משמעותית בתחום זה, ובפרט בכל הקשור לתחום של חדירה למחשבים וטלפונים של חשודים בטרור. חוסר זה ניכר במיוחד לאור ההשוואה לחוקים דומים בעניין מגבלות הקורונה ומן התחום הפלילי. החוסר בחקיקה מפורשת בולט בעיקר בחוק השב"כ, שכאמור, לוקה בחסר בתחום זה, ולמעשה אינו קובע בכלל סמכויות והגבלות בעניין תקיפת מחשבים. בסיום המאמר, הוצגו עקרונות כלליים ודרכי פיקוח אפשריות לתיקון לחוק השב"כ. הצעה זו מבקשת לענות על הלקונה בחוק, ולאפשר לשב"כ לבצע פעולות של תקיפת מחשבים באופן חוקי ועל ידי הסמכה מפורשת. יחד עם זאת, ההצעה מתייחסת בכובד ראש לפגיעה בזכות לפרטיות, הנפגעת רבות במצב המשפטי כיום, וקובעת איזונים והגבלות לפגיעה.

ציטוט מוצע: הלל זרם "חוק השב"כ – בין פרטיות לביטחון" **רשות הרבים** (1.9.23)