הזכות לפרטיות מול ביטחון המדינה:

הצעת חוק הפצחנות, הרוגלה והנוזקה



מגיש: אורי קליין

מתרגלת: הדר קורן

תאריך הגשה: 20.6.2022

תוכן עניינים

[פרק 1 – מבוא 3](#_Toc106639928)

[פרק 2 – רקע: פרטיות, טכנולוגיה וביטחון 3](#_Toc106639929)

[2.1 – הזכות לפרטיות: צידוקים, רקע, הגדרה וחקיקה. 3](#_Toc106639930)

[2.2 – מציאות טכנולוגית עכשווית: אתגרים וסכנות. 4](#_Toc106639931)

[2.3 – אינטרס השמירה על הביטחון הלאומי, אמצעי רוגלה ופגיעה בפרטיות. 4](#_Toc106639932)

[פרק 3 – הדין המצוי 5](#_Toc106639933)

[3.1 – הזכות לפרטיות והיקפה: חקיקה 5](#_Toc106639934)

[3.2 – הזכות לפרטיות והיקפה: פסיקה 7](#_Toc106639935)

[פרק 4 – הדין הרצוי 8](#_Toc106639936)

[4.1 – הפער הקיים: היעדר חקיקה המתירה רוגלה ופצחנות לצרכי מאבק בטרור. 8](#_Toc106639937)

[4.2 – קריאה לחקיקה: גבולות והיקף תחולה רצוי, איזון ערכי-חוקתי ודגשים ליישום. 9](#_Toc106639938)

[4.3 – ביקורות ושיקולי נגד להצעת החקיקה 11](#_Toc106639939)

[פרק 5 – סיכום והכרעה 12](#_Toc106639940)

# פרק 1 – מבוא

הזכות לפרטיות היא מהחשובות בחירויות הפרט. מאז חקיקת חוק-יסוד: כבוד האדם וחירותו עלתה הזכות לפרטיות למעמד חוקתי, ולצדה משלימים את הדין ישראלי עוד מספר חוקים והלכות המגינים על היבטים שונים של הפרטיות. בעידן המודרני מנוהלים חיינו במרחב הרשתי החכם ומתועדים דיגיטלית, ושימור הפרטיות הופך למורכב. לצד זכות זו עומד אינטרס הביטחון הלאומי, הזוכה לעליונות בחקיקה ובפסיקה, בהיותו תנאי לקיום. בישראל נכון הדבר שבעתיים לאור האיום התמידי והמחיר ההרסני של ״טעויות״ ביטחוניות. לכן קובע החוק שלצורך שמירה על הביטחון ומניעת פשיעה וטרור ניתן לפגוע בפרטיות בתנאים מסוימים.

כפי שאראה במאמר – בחוק הישראלי כיום לא קיים אף היתר לפרוץ למכשיר סלולרי או למחשב מרחוק ללא ידיעת הנפרץ לצורך השתלטות על המכשיר ו/או שאיבת מידע ממנו. מדובר במצב בעייתי, שכן הרבה מהטרור מתרחש כיום במרחב הרשתי, ובו אף מתבצע תכנון הטרור הפיזי. כפי שמעידים גורמים ביטחוניים, שימוש באמצעי סייבר הכרחי כנגד הטרור כיום. במאמר זה אציע חקיקה להסדרת שימוש בפעולות פצחנות (״האקינג״) רוגלה, ונוזקה. החקיקה תציע נוסחה לאיזון מידתי בין השמירה על הזכות החוקתית לפרטיות לבין שמירה על האינטרס הביטחוני בכלי סייבר. אראה שההצעה עומדת בדרישות פסקת ההגבלה שבחוק היסוד, אסקור טיעוני-נגד לה ואשיב להם.

# פרק 2 – רקע: פרטיות, טכנולוגיה וביטחון

## 2.1 – הזכות לפרטיות: צידוקים, רקע, הגדרה וחקיקה.

הזכות לפרטיות מופיעה במשפט העברי הקדום, כגון בדיני שכנות[[1]](#footnote-1), נושים[[2]](#footnote-2) והסגת גבול[[3]](#footnote-3). בחוקות ובאמנות בין-לאומיות רבות כיום מוכרת הזכות לפרטיות כזכות יסוד[[4]](#footnote-4), אך הדבר לא תמיד היה כך. למעשה, הפעם הראשונה בה הוזכרה הפרטיות כזכות משפטית הייתה במאמר משנת 1890 של צמד עורכי דין אמריקניים בשם וורן וברנדייס[[5]](#footnote-5), שהסבירוה בתור ״הזכות להיעזב במנוחה״. מאז היא עוגנה בחוק[[6]](#footnote-6) ובפסיקה בארה״ב[[7]](#footnote-7), אך לענייננו – היא הוכרה בחקיקה ובפסיקה הישראלית.

בשנת 92׳ עלו חלק מזכויות האדם למעמד חוקתי בישראל עם ״המהפכה החוקתית״, שהעניקה להן עליונות נורמטיבית במשפט הישראלי. בסעיף 7 לחוק-יסוד: כבוד האדם וחירותו נקבע: ״כל אדם זכאי לפרטיות ולצנעת חייו״. משכך הפכה הזכות לפרטיות לזכות יסוד חוקתית. החוק בישראל לא מגדיר מהי פרטיות[[8]](#footnote-8), אך בפסיקה אומצה הגדרתם של וורן וברנדייס למושג. כדברי הנשיאה ביניש[[9]](#footnote-9): ״זכותו של אדם להיוותר לנפשו״[[10]](#footnote-10)*.* חוקים נוספים שחוקקו בישראל מעגנים היבטי פרטיות ועליהם ארחיב בהמשך. בישראל אף הוקמה ב-2006 הרשות להגנת הפרטיות. חלק מסמכויותיה מעוגנות בחוק[[11]](#footnote-11), ובין סמכויותיה: ניהול חקירות מנהליות ופליליות וקידום תיקוני חקיקה בנושא פרטיות.

לקיומה של הפרטיות כזכות קיימים מספר צידוקים מרכזיים. ניתן לחלקם לשתי קטגוריית: צידוקים הנגזרים מכבוד האדם, וצידוקים הנגזרים מצרכים פסיכולוגיים[[12]](#footnote-12). ראשית, הכרה בפרטיות משמעה הכרה באדם כיחיד אוטונומי בעל ייחוד מאחרים, ייחוד קריטי לקיום אישיות הזכאית לכיבוד[[13]](#footnote-13). שנית, הפרטיות מאפשרת לאדם להיעזב לנפשו ולמנוחתו ולהיות עם עצמו – אינטרס אישי אוטונומי הנחוץ ליצירת מרחב אישי[[14]](#footnote-14). רק כך האדם יכול לקבוע לעצמו את אופן פעולתו האישית באזור מחייתו במנותק ממעורבות החברה, תוך הגנה מעיני זרים[[15]](#footnote-15).

## 2.2 – מציאות טכנולוגית עכשווית: אתגרים וסכנות.

בפרפרזה על תָאלֶס[[16]](#footnote-16) שקבע: ״הכול מים״ – היום, בחברה המודרנית – ״הכול חכם״. הטלפונים שלנו חכמים, כנ״ל הבתים ומכשירי המטבח, ואף הערים והתשתיות[[17]](#footnote-17). ״חוכמת״ מכשירים אלו היא ״היכולת לאסוף, לחבר, לנתח ולשתף במידע ברציפות ובהיעדר אמצעיות״[[18]](#footnote-18). ככל שהטכנולוגיה החכמה פורצת לתחומים נוספים בחיינו, יותר מפעולותיו הופכות למֵידָעִיוֹת וליצרניוֹת מידע ומכשירינו החכמים אוספים אותו[[19]](#footnote-19). לצד עושר המידע והנוחות האדירה שמאפשרת מציאות החיים הטכנולוגית החכמה, היא מכילה גם סכנות ואיומים כלפי פרטיות האדם. מחברות וגופים פרטיים וממשלתיים האוספים עלינו מידע, ועד לעבריינות סייבר: על אף שהשמירה על בטחון המידע האישי ועל זכות היסוד לפרטיות הופכת למאתגרת, אין משמעות הדבר שעל השמירה עליה להיעלם כליל[[20]](#footnote-20).

## 2.3 – אינטרס השמירה על הביטחון הלאומי, אמצעי רוגלה ופגיעה בפרטיות.

תופעת הטרור בעולם היא עתיקה ואקטואלית כאחד. בישראל היא אקטואלית עד כאב: בכל 74 שנות המדינה, לא הייתה ולו שנה אחת בה לא נהרג אף ישראלי מטרור[[21]](#footnote-21), ורק מתחילת 2022 נרצחו 20 ישראלים[[22]](#footnote-22). כפי שאף קבע בג״ץ, המצב הביטחוני בישראל שונה מהמצב ביתר העולם, גם באופי הסיכונים ואי-צפיותם, וגם בהשלכות מרחיקות הלכת שיהיו ״לטָעות״ ביטחונית בישראל[[23]](#footnote-23).

חוק המאבק בטרור[[24]](#footnote-24) מגדיר משפטית ״טרור״ דרך ארבעה מרכיבים מצטברים: המעשה, המניע, מטרתו ונזקו. למונח ״ביטחון לאומי״ אין הגדרה מוסכמת בחקיקה או בפסיקה בישראל[[25]](#footnote-25), אך מקובל בפסיקה שכשנדרש לאזן בין אינטרסים, זוכה הביטחון לעליונות על אינטרסים אחרים[[26]](#footnote-26). שהרי הביטחון הוא תנאי לקיום, ושמירה עליו היא שמירה על חייהם וגופם של האזרחים. יצוין אף שבס׳ 4 לחוק-יסוד: כבוד האדם וחירותו, תחת הכותרת ״הגנה על החיים, הגוף והכבוד״ נקבע: ״כל אדם זכאי להגנה על חייו, על גופו ועל כבודו״ – זכות חיובית שעל המדינה לספק לכל אזרח. אלא שכפי שנפסק: ״ביטחון המדינה איננו מילת קסם, ועדיפותו אינה קמה בכל מקרה ובכל נסיבות שהן״[[27]](#footnote-27). לצד הנחיצות שבפעולה נחושה נגד הטרור, יש חשש שהפעולה תפגע בזכויות אדם[[28]](#footnote-28).

כיום משמשת הרשת אף כאמצעי לטרור. ממתקפת סייבר של החמאס נגד ישראל[[29]](#footnote-29) ועד להאקרים איראניים הסוחטים כסף באיומים[[30]](#footnote-30). ישראל נחשבת מהמתקדמות בעולם בתחום[[31]](#footnote-31), ולה מערך סייבר לאומי. כדי למגר עבירות סייבר וטרור, מנצלות רשויות הביון והאכיפה פרצות טכנולוגיות שבשימוש העבריינים, לרבות פריצה למידע אישי של משתמשים[[32]](#footnote-32).

# פרק 3 – הדין המצוי

## 3.1 – הזכות לפרטיות והיקפה: חקיקה

בסקירת המסגרת הנורמטיבית בנוגע לזכות לפרטיות בישראל, אתחיל מחוק-יסוד: כבוד האדם וחירותו[[33]](#footnote-33). בסעיף 7 לחוק נכתב, תחת הכותרת ״פרטיות וצנעת הפרט״, כי ״כל אדם זכאי לפרטיות ולצנעת חייו״. הסעיף אף הקובע שאין להיכנס לרשות היחיד שלא בהסכמתו, ואוסר לערוך חיפוש ברשות היחיד של האדם ולפגוע בסוד שיחו, כתביו ורישומיו. משכך, לזכות לפרטיות מעמד חוקתי. משכך, לזכות לפרטיות יש עליונות נורמטיבית, ובעת התנגשות עם נורמות אחרות כגון חקיקה ראשית או תקנות היא תגבר. ניתן לפגוע בה רק בהתאם ל-4 התנאים המצטברים שבפסקת ההגבלה המופיעים בס׳ 8 לחוק: ע״י חוק, ההולם את ערכי המדינה, שנועד לתכלית ראויה, ובאופן מידתי.

אם חוק-יסוד: כבוד האדם וחירותו מחייב את המדינה ומוסדותיה לשמור על פרטיות האזרח, הרי שחוק הגנת הפרטיות[[34]](#footnote-34) מ-1981 מסדיר את הסוגיה במשפט הפרטי וקובע חובות ונהלי שמירת פרטיות גם ביחסים שבין אדם לחברו[[35]](#footnote-35) וביחסים שבין אנשים לתאגידים[[36]](#footnote-36). חוק זה קובע שפגיעה בפרטיות היא גם עבירה פלילית גם ועוולה אזרחית[[37]](#footnote-37). החוק מגדיר מהי פגיעה בפרטיות ומונה 11 חלופות. היריעה קצרה מלסכם את החוק, אך אציין שבין היתר מפרט החוק מהם החובות המוטלות על אבטחת מידע[[38]](#footnote-38) ומונה הגנות ופטוֹרים בהפרת פרטיות[[39]](#footnote-39). חוק המחשבים[[40]](#footnote-40) מגדיר מושגים כגון מחשב ומחשב עזר, מידע ותוכנה[[41]](#footnote-41), ואוסר חדירה למחשב שלא כדין[[42]](#footnote-42) או פעולה לשיבוש פעילותו[[43]](#footnote-43).

בחוק האזנת סתר[[44]](#footnote-44) מוגדרת מהי ״שיחה״ – כל דיבור, כתב, שֶמע, אותות, צורות או מידע העוברים בין מכשירים כגון טלפון חוטי ואלחוטי, נייד, מחשב ואחרים; ומהי ״האזנה״ – האזנה, קליטה או העתקה של שיחת הזולת באמצעות מכשיר[[45]](#footnote-45). החוק אוסר על האזנת סתר שלא כדין, לרבות בהסכמת צד אחד[[46]](#footnote-46), מטיל עונשי מאסר ניכרים על המפרים אותו[[47]](#footnote-47) וקובע כלל פסלות ראיות[[48]](#footnote-48). החוק נוגע במפגש בין הפרטיות לבין הביטחון, כשמתיר בתנאים מסוימים האזנות סתר למטרת ביטחון המדינה[[49]](#footnote-49) והאזנות למניעת עבירות וגילוי עבריינים[[50]](#footnote-50), כשבכל סוג קיימות הגבלות ונהלים שונים.

בתחום הפלילי – מניעת עבירות וגילוי עבריינים, תתאפשר האזנת סתר בצו מנשיא בימ״ש מחוזי או סגנו המוסמך לכך[[51]](#footnote-51), כשאת הבקשה הגיש קצין משטרה מוסמך בדרגת סנ״צ ומעלה והבקשה באה לגילוי, חקירה או מניעה של עבירה מסוג פשע או בהקשרים של עבירות פשע[[52]](#footnote-52). הבקשה תוגש בטופס מסודר ותתאר פרטים רלוונטיים להאזנה[[53]](#footnote-53). השופט רשאי לסרב, ועל סירוב קיים נוהל ערעור[[54]](#footnote-54). בהיתר ההאזנה יצוין משך הזמן בו תותר ההאזנה, אשר לא יעלה על שלושה חודשים[[55]](#footnote-55). בתחום הביטחוני – היתר להאזנת סתר למטרות ביטחון המדינה[[56]](#footnote-56) יינתן בכתב ע״י שר[[57]](#footnote-57), לאחר שקיבל בקשה לכך בכתב מראש אמ״ן או ראש השב״כ[[58]](#footnote-58). גם כאן, בָבקשה יפורט המידע הרלוונטי כמצוין לעיל, וגם כאן יש הגבלת משך זמן זהה[[59]](#footnote-59). על השר לדווח על ההיתר ליועמ״ש אחת ל-3 חודשים, ואם היה זה שר הביטחון – עליו לדווח על כך מיידית לרה״מ[[60]](#footnote-60).

במקרי צרכי ביטחון או פלילים דחופים[[61]](#footnote-61), החוק מאפשר ״מסלול מהיר״ להיתר להאזנת סתר: ״במקרים דחופים״ בהם ״שוכנע ראש רשות ביטחון כי ביטחון המדינה מחייב האזנת סתר שאינה סובלת דיחוי״, הוא רשאי להתיר בכתב את ההאזנה – בתוקף של עד 48 שעות[[62]](#footnote-62). היתר שכזה מחייב לכתוב על כך מיידית לשר ולהודיע ליועמ״ש, וכל אחד מהללו רשאי לבטל את ההיתר[[63]](#footnote-63).

בחוק נתוני תקשורת[[64]](#footnote-64) קיימות הוראות חוק דומות, אך במיקוד במאגרי מידע. כאן מדובר בהיתר שיכול ביהמ״ש לתת לקצין משטרה מוסמך לצורך קבלת מידע ממאגר מידע, תוך הגדרת פרמטרים להיתר סביב צורך, מראה, תוקף ותוכן הבקשה וכו׳[[65]](#footnote-65). גם חוק זה מכיל ״ערוץ מהיר״ עבור ״מקרים דחופים״, המאפשר השגת מידע גם ללא צו ותוך הגבלות מסוימות[[66]](#footnote-66).

החוק האחרון שאסקור בפרק זה הוא חוק השב״כ[[67]](#footnote-67) מ-2002[[68]](#footnote-68), לו השלכות על סוגיית הפרטיות. בחוק מוגדרים יעוד השב״כ ותפקידיו[[69]](#footnote-69), שתכליתם היא התמודדות עם איומים ביטחוניים. החוק מקנה לשב״כ כלים נרחבים לביצוע תפקידיו, כגון היתר ״לקבל ולאסוף מידע״ למילוי תפקידי הארגון[[70]](#footnote-70), על אף הפגיעה בפרטיות הנגרמת מכך[[71]](#footnote-71). סעיף 11 לחוק מקנה לרה״מ סמכות לקבוע כללים לפיהם סוג מידע מסוים יועבר ממאגרי מידע אל השב״כ, באישור ראש השב״כ, תוך פירוט מסוים ולזמן של עד 6 חודשים[[72]](#footnote-72). כללים אלו מתוקף סעיף 11 הינם חסויים ואין לנו גישה אליהם[[73]](#footnote-73).

סוגיית העברת המידע מגוף לגוף היא ליבתית בסוגיית הפרטיות, ועלתה בפס״ד מה-CJEU[[74]](#footnote-74), מקרה שנדון בביהמ״ש העליון באירלנד ובבית הדין של האיחוד האירופי. המקרה עסק באזרח אוסטרי בשם שרֶמס שתבע על כך שפרטיו האישיים הועברו מחברת פייסבוק אירלנד לפייסבוק ארה״ב. זאת לאור הסטנדרטים הנמוכים יותר של ארה״ב בנושא ביטחון מידע ופרטיות המידע ביחס לאלו באיחוד האירופי. לאחר מספר ערעורים, ערכאות ושמיעת עדים רבים, התקבלו טענות שרמס ונקבע כי לא ניתן להעביר מידע אישי של אדם למדינה בה מידע זה לא יוגן כראוי[[75]](#footnote-75).

לאחר האזנת סתר לתקשורת בין מכשירים (מידע בתנועה) ולשימוש במאגרי מידע (מידע במנוחה), הדרך השלישית שמתיר החוק פגיעה בפרטיות היא תפיסה. לפי פקודת הסד״פ[[76]](#footnote-76), צו חיפוש מתיר לשוטר לתפוס חפץ ולקחתו[[77]](#footnote-77), ואם חושד שנעברה או מתוכננת להיעבר בו עבירה, או שעשוי לשמש כראיה בהליך משפטי – אף ללא צו[[78]](#footnote-78). כהוראה משלימה, קובעת הנחיית פרקליט המדינה[[79]](#footnote-79) כי לאחר תפיסת טלפון או מחשב, ובהינתן צו מתאים, ניתן ליצור העתק של תוכנם ולעיין בו[[80]](#footnote-80).

## 3.2 – הזכות לפרטיות והיקפה: פסיקה

בפסיקה הישראלית אין הגדרה אחת מאוגדת למושג ״פרטיות״, אך קיימים מספר פס״דים והלכות מרכזיות שקבעו את האיזונים בדיני הפרטיות. עניין ידיעות[[81]](#footnote-81) מ-2003 עסק במקרה של גברת לוין שתבעה את ׳ידיעות אחרונות׳ בגין לשון הרע. לצורך בירור אמיתוּת הנכתב עליה בעיתון, נדרשה גישה לתיקהּ הרפואי – והיא סירבה בטענה שנפגעת פרטיותה. לבסוף הותרה גישה חלקית, אך להלכה נקבע שהזכות לפרטיות היא יחסית, ומשכך – יש לאזנה כנגד עקרונות היסוד האחרים[[82]](#footnote-82). כשמאפשרים גישה למידע פרטי, יש להפעיל את *מבחן הרלוונטיות* של המידע הפוטנציאלי שמבקשים לחשוף, וכן את *מבחן ההכבדה* הבודק כמה תכביד חשיפת המידע על האדם הנחשף.

בעניין האגודה למען זכויות האזרח נ׳ משטרת ישראל[[83]](#footnote-83) מ-2009 הוגשו עתירות נגד חוק נתוני תקשורת המאפשר לרשויות החקירה גישה לנתוני תקשורת מכלל חברות וספקי התקשורת, הסלולר והאינטרנט, בטענה לפגיעה בזכות החוקתית לפרטיות. ביהמ״ש דחה את העתירות וקבע שהחוק עומד בדרישות פסקת ההגבלה, לרבות דרישת המידתיות: רשויות החקירה מבקשות ומקבלות צווי חיפוש רק לגילוי עבירות או עבריינים קונקרטיים, ולא לצרכי פעילות מודיעינית כללית.

מקרה אקטואלי של פגיעה בפרטיות שהעלה את שאלת איזון האינטרסים: פרטיות מול ביטחון, הוא פרשת איכוני ומעקבי השב״כ בקורונה[[84]](#footnote-84). אחת מדרכי הממשלה להתמודד עם התפרצות נגיף הקורונה, אי שם במרץ 2020, הייתה להיעזר בשב״כ ולהסמיכו למעקב אחר אזרחים לאיתור מיקום חולי קורונה ואנשים שבא עמם במגע. העתירה עצמה התמקדה בשאלת הסמכות השיורית מכוח סעיף 32 לחוק-יסוד: הממשלה בנושא הסדרים ראשוניים, אך בפסק הדין התחדדה שאלת האיזון בין הצורך הלאומי לבין הזכות לפרטיות. לגבי איכוני השב״כ בקורונה נקבע כי מכיוון שהיו צורך לאומי בעת חירום יש לאפשר פגיעה זו בפרטיות. אולם נקבע שמעתה והלאה יידרש לאשרם גם בכנסת שכן זהו הסדר ראשוני מובהק.

המקרה האחרון שאסקור כעת הוא עניין אוריך[[85]](#footnote-85). פס״ד אוריך הוא שילוב של מספר מקרים, אך לגוף העניין: אוריך היה עוזרו של רה״מ לשעבר בנימין נתניהו, והוגשה נגדו ונגד אחרים תלונה בגין הטרדת עד ע״י מר פילבר, עד בפרשה המכונה ״תיק 4000״. המשטרה חקרה את התלונה ובחקירה ביצעה חיפוש במכשיר הנייד של אוריך ללא צו מתאים וללא שהוסבר לנחקרים שזכותם להתנגד לחיפוש. רק לאחר מכן פנתה המשטרה לביהמ״ש לקבלת צו חיפוש, מה שעורר את התנגדות אוריך. בימ״ש השלום נתן את הצו בדיעבד, החלטה עליה ערער אוריך למחוזי, ובהמשך לעליון ואף לדנ״פ. שופטי הרוב פסקו כי חיפוש שהתבצע שלא כדין לא בהכרח יביא לדחיית בקשת מתן הצו, אלא רק במקרים חריגים. זאת משום שמנגד עומד אינטרס בירור הדין והאמת. אם לאחר מתן הצו יוגש כתב אישום, משקל הראיות שהושגו שלא כדין יקבע לפי הלכת יישכרוב[[86]](#footnote-86).

# פרק 4 – הדין הרצוי

## 4.1 – הפער הקיים: היעדר חקיקה המתירה רוגלה ופצחנות לצרכי מאבק בטרור.

על אף עליונות אינטרס הביטחון על הפרטיות, המתבטאת בהסדרי החוק שלעיל המתירים פגיעה בפרטיות בהאזנת סתר, בהשגת מידע ממאגרים ובתפיסת מכשיר, קיים תחום רלוונטי, מרכזי וחיוני במרחב הדיגיטלי אותו החוק בישראל אינו מתיר כיום – ומכוח *עיקרון חוקיות המנהל* ולאור הזכות החוקתית לפרטיות – אף אוסר, והוא תחום הסייבר: רוֹגלָה, נוֹזקוֹת ופָצחָנוּת.

המכנה משותף לרוב תוכנות הריגול והסייבר הוא היותן תוכנות מחשב זדוניות אותן מחדירים למחשבים ומערכות מחשוב ללא הסכמה, למטרות איסוף מידע. יש אף נוזקות התוקפות מערכות מחשב ופוגעות בחוּמרה ובתוֹכנה. פצחנים (״האקרים״) כיום מסוגלים לעשות את מה שבוצע בעבר רק בסרטים. בפרשת תוכנת ״פגסוס״ של חברת NSO Group הישראלית שנחשד שנמכרה לממשלת מקסיקו שדיכאה דרכה מתנגדי משטר ועיתונאים[[87]](#footnote-87) פורסם שהמערכת מסוגלת להשתלט מרחוק על מכשיר סלולרי עד כדי הפעלה ושימוש במצלמה, במיקרופון, בשירותי המיקום ובכל יתר היישומונים (״אפליקציות״) שלו[[88]](#footnote-88), מבלי להשאיר סימנים או עקבות. יש תוכנות רבות כאלו, אך לא ארחיב כעת אודות הבדלים בין סוגי התוכנות השונים, שאין זו מטרת המאמר[[89]](#footnote-89).

מכיוון שהזכות לפרטיות היא חוקתית, פגיעה בה תתאפשר רק לפי פסקת ההגבלה – ע״פ חוק מפורש[[90]](#footnote-90). אך אשוב ואדגיש – לא קיים כיום בדין הישראלי אף היתר לחדור מרחוק ללא ידיעת האזרח לתוכן מכשירו הסלולרי ו/או לעשות בו וביישומיו שימוש פצחני, לא בהקשרי ביטחון לאומי ולא בהקשרים פליליים. פקודת הסד״פ מאפשרת רק תפיסה של טלפון או מחשב, ובהתאם להנחיית פרקליט המדינה – צו בית משפט יכול להתיר העתקת תוכנו ועיון בהעתק. גם חוק האזנת סתר הארכאי, שחוקק ב-79׳ בטרם באו אמצעי הרוגלה והפצחנות לעולם, לא מכסה תוכנות פצחנות. חוק זה מאפשר ניטור רק תקשורת בין מכשירים, על סוגיה השונים, אך לא איסוף נתונים שהם מעבר לשיחה. ההיתר בחוק נתוני תקשורת מצומצם למידע מוגבל על קו הטלפון מושא הצו – פלט מספרי טלפון של שיחות נכנסות ויוצאות ואיכון המכשיר ובעליו. רוגלה ופצחנות? לא בדיוק.

היו ניסיונות להסדרת חקיקה בנושא[[91]](#footnote-91). ב-2011 עלתה הצעת חוק המאבק בטרור, התשע״א-2011, שכללה את סעיף 131 שהציע תיקון לחוק השב״כ להסמכת הארגון לתקוף מחשבים לסיכול טרור וריגול נגד המדינה. נציג השב״כ בדיונים בכנסת הסביר כי: ״החוק שאנו עובדים איתו היום מתאים לאיומים שהיו לפני חמישים שנה ולא לעידן הטכנולוגי והרשתות החברתיות״. לבסוף הוחלט לפצל סעיף 131 מההצעה לאור מורכבותו. ב-2017 עבר החוק בכנסת, וכיום סעיף 131 עדיין תלוי ועומד[[92]](#footnote-92).

## 4.2 – קריאה לחקיקה: גבולות והיקף תחולה רצוי, איזון ערכי-חוקתי ודגשים ליישום.

איני מתיימר לקבוע האם גופי הביטחון בישראל עושים שימוש בתוכנות רוגלה ופצחנות או לא. בהינתן המצב הביטחוני, סביר שהתשובה היא כן. איני מכנה גופים אלה כפורעי חוק. אדרבא, בתור אזרח אני שמח שהמדינה פועלת לשימור הביטחון. אך לאור *עיקרון החוקיות המנהל* לפיו לרשויות מותר רק מה שהחוק מתיר להן במפורש, סבורני שאת המצב הנוכחי יש לשנות בהקדם ולהסדיר פצחנות בחקיקה. ״צורך״ אינו מקור סמכות, וכפי שאף נפסק בעבר[[93]](#footnote-93) נדרשת הסמכה בחוק. הצעתי היא לחוקק או לתקן את החוק הקיים כך שיותר לגופי הביטחון האמונים על המלחמה בטרור – המוסד, השב״כ ואגף המודיעין בצה״ל – שימוש בתוכנות רוגלה, נוזקה וכלי פצחנות לצורך המאבק בטרור. או ע״י תיקון חוק האזנת סתר דרך הוספת נספח או פרק לחוק, או דרך חוק עצמאי חדש (הצעת שם: ״חוק הפצחנות, הרוגלה והנוזקה״). בדומה להסדרי חוק האזנת סתר, גם החקיקה המוצעת תקבע תנאים ונהלים להיתר. כעת אפרט את עיקרי הצעת החקיקה:

 א. כנגד טרור בלבד – שימוש בפצחנות פוגע קשות בזכות לפרטיות. מחשבו ומכשירו הסלולרי של האדם מכילים את כלל המידע המתועד בחייו, לרבות מידע אינטימי. אם לא די בכך, חלק מאמצעי הרוגלה מאפשרים שליטה מרחוק במכשיר הנפרץ, לרבות ביצוע פעולות אקטיביות ממנו. לכן בשביל שהחוק יתיר לאנשי זרועות הביטחון גישה ישירה לליבת פרטיותם של אזרחים, במיוחד במצב בו הדבר נעשה ללא ידיעת מושא הפריצה, נדרש שבמאזן הערכי יעמוד מנגד ערך עליון.

כמצוין לעיל, החוק והפסיקה בישראל מעניקים לאינטרס הביטחון עליונות כמעט מוחלטת[[94]](#footnote-94). בהיות הטרור האיום הפיזי המרכזי על חיי אזרחי המדינה, ובהנתן שהלוקח חלק בטרור מאבד מזכויותיו האישיות – מצויה ההצדקה הערכית לפגיעה החוקתית הנלווית לפעולות פצחנות ורוגלה.

אולם לגבי עבירות שאינן טרור, שעל אכיפתן אָמונה המשטרה, אין הדבר כך. מעשי שוד, הסגות גבול או נהיגה בשכרות הם מזיקים, אך לא מאיימים על קיום המדינה. מדינות העולם מתקיימות על אף העבריינות הפלילית בגבולן. לכן בעיניי אין להתיר למשטרה, האמונה על השיטור והסדר החברתי, גישה לאמצעי הפצחנות והרוגלה, אלא לייחדם להתמודדות עם הטרור ולהקצותם לגופי הביטחון הרלוונטיים בלבד. אגב, אעיר כי ״טרור הוא טרור הוא טרור״, כך שהחקיקה המוצעת לא תבחין בין שימוש באמצעי פצחנות כנגד בעלי ת״ז כחולה לבין כאלה שאינם. עוסק בטרור הוא עוסק בטרור, ללא קשר לאזרחותו. ניתן אף להציע אחרת, אך מקוצר היריעה לא אאריך כאן בדיון זה.

 ב. הגדרת דרג מאשר, וצורת והיקף האישור – אין הצדקה שמעצם העובדה שגופי הביטחון מתמודדים עם טרור יוענק להם היתר גורף לשימוש בכלים אלה. כפי שקובע חוק האזנת סתר דרג נדרש לאישור כל סוג האזנה, החקיקה המוצעת תגדיר את רוֹם-הדֶרג הנדרש להיתר פעולה פצחנית. בחוק האזנת סתר הוגדר שקצין משטרה מוסמך הוא קצין בדרגת נצ״מ ומעלה שהוסמך ע״י המפכ״ל[[95]](#footnote-95). אציע ששימוש באמצעי הפצחנות יותנה באישור של קצין בדרג זהה בהתאם לארגון: אל״מ בצה״ל, ודרג מקביל במוסד ובשב״כ[[96]](#footnote-96). הקצין יאשר רק כשיראה זאת נחוץ, בהתקיים קשר רציונלי בין האמצעי למטרה הנדרשת. אף בהתאם לדרישת החתימה הקיימת בחוק האזנת סתר, על אישור זה להיות חתום. בהתאם לחוק, גם היתרי הפצחנות יוגבלו בזמן. אציע שהיתר יהיה בתוקף ל-48 שעות, הסף המחמיר בחוק האזנת סתר, שכן מדובר בפגיעה חמורה יותר בפרטיות[[97]](#footnote-97).

 ג. מנגנוני ביקורת ופיקוח – כל גוף מרשויות המדינה חייב שיעמוד בפני פיקוח וביקורת. חזקת תקינות המנהל אינה מספיקה במציאות מורכבת ובוודאי בתחום הבטחוני. בחקיקה המוצעת יהיה מנגנון פיקוח וביקורת בדומה לחוק האזנת סתר, כגון אישור שופט או חובת דיווח לשר[[98]](#footnote-98). יש להעיר כי מטבע הפעילות הביטחונית כנגד הטרור, קיימת באופן מובנה דחיפות בפעילות גופי הביטחון הרלוונטיים. מי שמכיר את אופי פעילויות הארגונים הביטחוניים יודע שלעתים לא נדירות יכולות התרחשויות חשובות לקום וליפול על חודן של דקות. על כן, מנגנוני הפיקוח שאציע הם שניים:

מנגנון ראשון: פיקוח תמידי מובנה. בפעולות רוגלה ופצחנות יש פגיעה קשה במיוחד בפרטיות שכן מדובר בפעולה מתמשכת. לכן נדרש פיקוח תמידי. בעיניי, באופן פרדוקסלי, דווקא הפיקוח התמידי הוא שיאפשר פעילות ביטחון שוטפת ותקינה. הרי אם בכל פעם שתתבצע פעולת פצחנות יידרש פיקוח נקודתי מחדש, לרבות אישורים וביקורות, תיווצר ״תקיעת מקלות בגלגלים״ אופרטיבית.

מעשית, הדבר יוכל להתבצע ע״י הרשות להגנת הפרטיות. אציע שלרשות זו, העוסקת אף בחקירות ובעניינים מסווגים, יהיה תקן של ממונה על פרטיות בסייבר בכל ארגון: בצה״ל, בשב״כ ובמוסד. נדרש שלנציג זה יהיו גם ״שיניים״, ושבמקרי חריגה מהחוק וממתחם הסבירות שיוגדר לפעילות הביטחונית – הטיפול יועבר ליועמ״ש שיחליט מה דין החריגה ואם להגיש כתב אישום להבאת הגורמים החורגים לביהמ״ש (פיקוח שיפוטי). פיקוח תמידי זה מקביל לדרישת חוק האזנת סתר לכך שכל צו יאושר ויעבור תחת בקרה – דרישה שלא ניתן לקיים במלואה בארגוני ביטחון נגד טרור.

מנגנון שני: פיקוח תקופתי. לרוב פיקוח תמידי הוא בסיסי בלבד, והשגרה הביטחונית לא תמיד מאפשרת התעמקות יסודית. אולם דו״ח תקופתי מאפשר להעמיק ולבחון מקרים ביסודיות. לכן החקיקה תיקבע הסדר פיקוח לפיו תקופתית, למשל אחת לחודש או רבעון, יגיש גוף הביטחון דו״ח המפרט את פעולות הפצחנות שביצע באותה תקופה. אציע כי הדו״ח יוגש לרשות להגנת הפרטיות מהיותה אמונה על שמירת הפרטיות במדינה; ליועמ״ש בתור הנציג המשפטי; ולשר הביטחון מהיותו נציג הציבור בתחום הביטחון. הפיקוח התקופתי מקביל להסדר חוק האזנת סתר לפיו מוגש מדי חודש דו״ח דומה ליועמ״ש[[99]](#footnote-99). גם כאן, במקרים בהם אחד או יותר משלושת גורמי הדיווח יזהה בדו״ח מעשה חריג – הדבר יגרור סנקציה משפטית, לרבות הבאת המקרה בפני ביהמ״ש.

הצעת החקיקה עומדת בדרישות פסקת ההגבלה[[100]](#footnote-100): חקיקה ראשית שתעבור בכנסת ותקיים את הרציונל הדמוקרטי והמוסדי; החקיקה לא סותרת את ערכי מדינת ישראל כיהודית ודמוקרטית[[101]](#footnote-101); חקיקה לתכלית ראויה – הגנה על ביטחון וקיום המדינה וחיי אזרחיה; ומעל הכול – החקיקה היא מידתית, מוכוונת רק כנגד מניעת טרור ומתירה שימוש באמצעים הכרחיים טכנולוגית. היא עומדת *במבחן ההתאמה* ומקיימת קשר רציונלי בין האמצעי (פצחנות) לבין המטרה (ביטחון). היא עומדת *במבחן האמצעי שפגיעתו פחותה* – לא ניתן להשיג את התכלית הביטחונית-טכנולוגית דרך אמצעים אחרים הפוגעים פחות בפרטיות[[102]](#footnote-102). קיימת *מידתיות במובן הצר –* יחס ראוי בין תועלת (מניעת טרור) לנזק (פגיעה בפרטיות הנחשדים או העוסקים בטרור). כהערת אגב אעיר שיש חשיבות גם לאופן העלאת הצעת החקיקה, שכמובן תהיה מפורטת. הדרך בה תונגש ההצעה לציבור ולנבחריו וזֶהות מעלֶה ההצעה ישפיעו על סיכויי ההצעה להתקבל בכנסת[[103]](#footnote-103).

## 4.3 – ביקורות ושיקולי נגד להצעת החקיקה

הצעה זו אינה חפה מביקורת. אדרבא, העלאת ביקורות ושיקולי יכולה להביא לטיוב ודיוק ההצעה. ראשית, ביקורת מהותית נגד היתר לשימוש בפצחנות לצרכי ביטחון תטען שמהיבטי ליברליזם וחירויות פרט, בדגש על הזכות לפרטיות וקדושת מרחבו האישי של האדם, אין להתיר אמצעים שכאלה. תשובה לביקורת זו מצויה בחלקי המאמר לעיל: העובדה שקיום וחיים קודמים לכל ושאמצעים אלה הכרחיים במציאות הביטחונית כיום. כעת אציג ביקורות נקודתיות יותר:

 א. פגיעה בפרטיות צדדים שלישיים – כחלק מפעילות פצחנות שגרתית עלול להיחשף מידע אישי של צדדים שלישיים, כגון מידע אינטימי של חברי ומשפחת יעד הפריצה, או אף לקוחות אם מדובר בבעל מקצוע. נגד אותם אנשים אין כל חשד לטרור. אעיר שטענה זו בדין היא, אולם בעיניי מנגד עומד הצידוק ״הרוּבָּני״. הדמוקרטיה מצדיקה הכרעה לטובת הרוב היחסי. הטרור מכוון כנגד הציבור, סיכולו טוב לכול, והדבר מצדיק הפגיעה בצדדי ג׳. אך כן ניתן לקבוע הסדרים שיצמצמו פגיעה בצדדי ג׳, כגון קביעת זמן מירבי להחזקה במידע לפני שיימחק.

 ב. פגיעה מתמשכת כלפי העתיד – ביקורת זו עלתה בדיונים בתיקון שהוצע לחוק השב״כ ע״י האגודה לזכויות האזרח[[104]](#footnote-104). נטען שהיתר לשימוש ברוגלות יאפשר לגופי הבטחון לנהל מעקב אחר פעולות עתידיות של חשודים. התוכנות יותקנו בָמכשיר לאיסוף מידע עתידי שיתקבל, והדבר ״דומה להתקנת מצלמה בביתו של אדם המבצעת מעקב על המתרחש בבית, תוך הארכת החיפוש לזמן בלתי מוגבל״. אשיב שמדובר בביקורת שביסודה חשש נכון. אולם היתר לשימוש ברוגלות לא יתיר פגיעה חופשית כלפי העתיד. לכן אציע שהחקיקה תכלול נהלי פיקוח על מעקבים מתמשכים. תוגדר תקופה כגון אחת לשבוע, בה יוגשו דו״חות על מעקבים מתמשכים עם בקשה להמשך הפעילות וההצדקה להמשכה, והממונה ייבחר אם לאשר את הבקשה. כך תימנע פגיעה בפרטיות עתידית.

 ג. סיכון יחסי החוץ של המדינה – הביקורת עלתה ע״י פרופ׳ ג׳אפור על הצעת תיקון חוק בארה״ב שביקשה להרחיב את סמכויות ה-FBI בתחום הפצחנות ורלוונטית לענייננו. צווים המתירים תקיפות ופריצות מחשבים עלולים להביא להפעלת סמכויות שיפוט חוץ-טריטוריאליות. דרג זוט לא-מדיני ולא-נבחר זוכה לשיקול דעת רחב בתחום המעצב מדיניות חוץ. זה בעייתי דמוקרטית – בשאלת זהות מעצבי מדיניות ציבורית, וגם מעשית-קונקרטית – בפגיעה במדיניות החוץ עצמה. גם טענה זו בדין. לכן אין מניעה לקיים שת״פ בין-ארגוני לגיבוש כללי פעולה מנחים לפצחנות. אציע שמשרד החוץ ייוצג בגופי הביטחון ויוודא שלא נפגעת מדיניות החוץ הממשלתית[[105]](#footnote-105).

# פרק 5 – סיכום והכרעה

אין להקל ראש בפגיעה בפרטיות, שהיא זכות חוקתית מהחשובות בזכויות האדם. לא בכדי היבטיה השונים מוגנים בחקיקות רבות. כפי שנפסק בבג״ץ הזכות לפרטיות היא יחסית ויש לאזנה בכל מקרה למול האינטרס הספציפי, ופגיעה בה תתאפשר כשמנגד עומד הביטחון והדבר יעמוד בפסקת ההגבלה[[106]](#footnote-106). הצעתי לחקיקה מקיימת איזון חוקתי-ערכי זה וקוראת להתאים את היתרי הפגיעה בפרטיות למציאות המודרנית, באימוץ קווי החוק הקיים והתרה רק בטרור, לפי מבחן הרלוונטיות ורק במקרים קונקרטיים.

הביקורות שעלו בתחומי הפגיעה בחירות הפרט בהווה ובעתיד, בפרטיות צדדים שלישיים ובתחום מדיניות החוץ של המדינה, נוגעות כולן בנקודות חשובות. כפי שכתבתי לעיל – חלק מהן יש לאמץ. במאזן הסופי בין הכנסת הצעת החקיקה לספר החוקים בישראל לבין דחייתה, סבורני שיש לאמצה ויפה שעה אחת קודם. על נהלי ופיקוח חקיקה זו יש להקפיד בדקדקנות, אך בזירה הטכנולוגית העכשווית אין למדינה פריבילגיה שלא לפעול באמצעים שכאלה. אם הם כבר בשימוש, יש להסדירם בכנסת בהתאם לפסקת ההגבלה, שהרי מדובר בפגיעה בזכות יסוד חוקתית.

|  |  |  |  |
| --- | --- | --- | --- |
| קריטריון | ניקוד | ניקוד בפועל | הערות |
| הגשת ראשי פרקים  | 20 | 20 | ר' הערותיי בראשי הפרקים.  |
| מבנה וחלוקה לפרקים | 10 | 10 | השער מושקע, הכותרת מעניינת ותוכן העניינים מסודר – כל הכבוד! בנוסף, עבודתך בנויה באופן מסודר וקוהרנטי המשרת את טיעונך.  |
| ניסוח | הגהה ואזכור אחיד | 10 | 10 | 18 | עבודתך כתובה בשפה ברורה. באשר להערות השוליים, ככלל, הערות שוליים טובות. עם זאת, היו מספר טעויות. במיוחד יש להקפיד על כללי האזכור החוזר. בנוסף, נדרשת להפנות לפסקאות/עמודים ספציפיים. |
| אופן הצגת הטיעון והתמודדות עם טיעוני נגד | 30 | 28 | הצגת את טיעונך באופן מסודר וברור. הסברת כראוי מה הקושי במצב הקיים ומתוך כך הצגת את הצעתך. כמו כן, הסברת יפה מדוע יש לאפשר פגיעה בפרטיות רק במקרים של טרור. בנוסף, הקפדת להתמודד עם טענות נגד אפשריות. עם זאת, היו מספר נקודות שמצאתי לנכון להעיר לגביהן:* היה מקום להסביר מעט על מהי רוגלה ופצחנות ומדוע יש צורך בכך כדי להתמודד עם פעילות הטרור. בהיעדר הסבר כאמור, קיים קושי להבין כיצד הוספת סמכויות לבצע רוגלה תוסיף לחוק הקיים ותסייע במאבק בטרור. עולה התהייה האם לא מדובר בפגיעה שאינה נחוצה בפרטיות (למשל: מדוע יש צורך להיחשף לגלריה של הפלאפון כדי להיאבק בטרור?).
* היה מקום להרחיב על מקרי הבוחן ולהתייחס לנקודות המהותיות כגון התייחסות השופטים לפגיעה בפרטיות אל מול האינטרס הציבורי.
* לא פעם לא נימקת את טענותיך ומסקנותיך. כך למשל, כאשר טענת כי החוק המוצע עומד בתנאי פסקת ההגבלה, עלייך להסביר מדוע. כמו כן, היה עלייך לנמק ולהרחיב בתגובותייך לביקורות.
* כאשר אתה מציג את דעתך, יש להקפיד על שפה מסויגת (לדעתי, לדידי, לגישתי) שכן אין מדובר בעובדה חד משמעית.
* עליך להקפיד לעגן את טיעוניך (ר' הערותיי בגוף העבודה).
 |
| יישום וניתוח דוגמאות ושימוש במקורות החובה | 20 | 20 |  עשית שימוש בכל מקורות החובה וניתחת את המקורות כראוי.  |
| מקוריות ושימוש במקורות נוספים (בונוס) | 5 | 5 | השתמשת במקורות נוספים שהעשירו את עבודתך וסייעו בביסוס טענותיך.  |
| סה"כ | 105 | 101 | אורי, כתבת עבודה יפה מאוד. הקפדת על סדר ועל הניסוח. הצגת באופן מעולה את הדין הקיים וכן את החוסרים בו. כך, הנחת תשתית טובה לטיעונך בדבר הצורך במתווה המוצע. כמו כן, הקפדת לנמק את עמדתך ולהסביר את הרציונלים לגישתך. כאמור, לעתים דעותייך הוצגו ללא נימוק מספק וכעובדה. בהצלחה!הדר.  |

1. בבלי, בבא בתרא ס׳, עמוד א׳. [↑](#footnote-ref-1)
2. דברים כ״ד י׳-י״א. [↑](#footnote-ref-2)
3. פסיקתא זוטרתא, ויקרא א׳, א׳. [↑](#footnote-ref-3)
4. 4 מיכאל בירנהק [מרחב פרטי] הזכות לפרטיות בין משפט לטכנולוגיה 9 (2011). [↑](#footnote-ref-4)
5. Samuel D. Warren and Louis D. Brandeis “The Right to Privacy” Harvard Law Review Vol. 4 No. 5, 193-220 (1890). [↑](#footnote-ref-5)
6. The Privacy Act 1974, 5 U.S.C. § 552a. [↑](#footnote-ref-6)
7. כגון Roe v. Wade, 410 U.S. 113 (1973) שם נפסק שהתיקון השלישי לחוקה מגן על אזור הפרטיות בבית המגורים. [↑](#footnote-ref-7)
8. אולם החוק כן מגדיר מהי פגיעה בפרטיות, למשל בסעיף 2 לחוק הגנת הפרטיות, תשמ״א-1981. [↑](#footnote-ref-8)
9. בג״ץ 3809/08 האגודה למען זכויות האזרח נ׳ משטרת ישראל, 9 פס׳ 5 לפסק דינה של הנשיאה ביניש (נבו 28.05.2012). [↑](#footnote-ref-9)
10. הגדרה זו התקבלה אף במקומות נוספים, כגון ע"פ 1302/92 מדינת ישראל נ' נחמיאס פ"ד מט(3) 209, 353 פס׳ 24 לפסק דינו של השופט (כתוארו דאז) ברק (1995), וכן בבג"ץ 2481/93 יוסף דיין נ' ניצב יהודה וילק פ"ד מח(2) 456, 470 פס׳ 16 לפסק דינו של השופט (כתוארו דאז) ברק (1994). [↑](#footnote-ref-10)
11. כגון בסעיף 10(א) לחוק הגנת הפרטיות תשמ״א-1981, לפיו רשות זו תגיש לוועדת חוק, חוקה ומשפט דו״ח פעם בשנה על פעולות האכיפה והפיקוח בתחום הפרטיות בשנה החולפת. [↑](#footnote-ref-11)
12. מיכאל בירנהק [מרחב פרטי] הזכות לפרטיות בין משפט לטכנולוגיה 115 (2011). [↑](#footnote-ref-12)
13. ע"פ 2963/98 גלעם נ' מדינת ישראל, 11 פס׳ 9 לפסק דינו של השופט ח׳ אריאל (נבו 13.06.1999). [↑](#footnote-ref-13)
14. ע"א 8483/02 אלוניאל בע"מ נ' מקדונלד, פ"ד נח(4) 314, 348 פס׳ 33 לפסק דינו של השופט א׳ ריבלין. [↑](#footnote-ref-14)
15. בג״ץ 6650/04 פלונית נ' בית הדין הרבני האיזורי בנתניה, 10 פס׳ 10 לפסק דינו של הנשיא ברק. [↑](#footnote-ref-15)
16. תָאלֵס איש מילֵטוֹס, ‏624 לפנה"ס עד 546 לפנה"ס בקירוב, פילוסוף ומתמטיקאי יווני מהאסכולה המילֵטית. נחשב לפילוסוף המוכר הראשון בתולדות הפילוסופיה המערבית. [↑](#footnote-ref-16)
17. להמחשה: לפי מכון המחקר הבינלאומי IoT Analytics, בשנת 2021 היו בעולם 12.2 מיליארד מכשירים חכמים המחוברים לאינטרנט, והתחזית היא כי עד לסוף שנת 2022 יהיו 14.4 מיליארד כאלו. ראו:

Mohammad Hasan ״State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion .globally״ IOT ANALYTICS 18.05.2022 https://bit.ly/3HkrydK [↑](#footnote-ref-17)
18. אסף לובין ״תקיפות מחשבים למטרות איסוף מודיעין כחלק מהמאבק בטרור בדין הישראלי, המשווה והבין-לאומי״ חוקים יג 255 (2020). [↑](#footnote-ref-18)
19. כפי שמסביר בירנהק, ״מהפכת הפס הרחב״ העצימה את התופעה בכך שהגבירה את מהירות זרימת המידע ואפשרה גישה לכל מידע, מכמעט כל מקום בעולם, בכל רגע נתון. ראו:: מיכאל בירנהק "פרטיות: תמונת מצב" משפט, חברה ותרבות ב 9, 11 (2019). [↑](#footnote-ref-19)
20. מיכאל בירנהק, "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" משפט וממשל כרך י"א 9, עמ' 18-19 (2008). [↑](#footnote-ref-20)
21. הכנסת, מכון המחקר והמידע, ״נתונים על חללי מערכות ישראל וחללי פעולות איבה בשנים 1947–2017״ (23.05.2017) https://docdro.id/LYbiMEk. [↑](#footnote-ref-21)
22. ״דוחות חודשיים״ אתר השב״כ (2022) https://bit.ly/2Jhtd7m. [↑](#footnote-ref-22)
23. בג"ץ 4541/94 אליס מילר נ' שר הביטחון, מט(4) 094, 118 פס׳ 1 לפסק דינו של השופט י׳ קדמי (1995). [↑](#footnote-ref-23)
24. חוק המאבק בטרור, תשע"ו-2016. [↑](#footnote-ref-24)
25. בג"ץ 2109/20 עו״ד שחר בן מאיר נ' ראש הממשלה, 13 פס׳ 16 לפסק דינה של הנשיאה חיות (נבו 26.04.2020). [↑](#footnote-ref-25)
26. למשל בבג״ץ 73/53 חברת ״קול העם״ בע״מ נ׳ שר הפנים, פ״ד ז 871, 880 פס׳ 3 לפסק דינו של השופט אגרנט, וכן בג״ץ 680/88 שניצר נ׳ הצנזור הצבאי הראשי, 642 פס׳ 27 בפסק הדין של אהרן ברק. [↑](#footnote-ref-26)
27. בג"ץ 4541/94 אליס מילר נ' שר הביטחון, מט(4) 094, 125 פס׳ 12 לפסק דינו של השופט י׳ קדמי (1995). [↑](#footnote-ref-27)
28. יצחק זמיר ״זכויות האדם וביטחון המדינה״ 18 (1988). [↑](#footnote-ref-28)
29. ״מתקפת הסייבר שהחמאס מבצע נגד ישראל״ iCapital https://bit.ly/3N2bkaB. [↑](#footnote-ref-29)
30. אסף גלעד וניצן שפיר ״האקרים איראניים: נדליף מידע אישי נוסף אם לא נקבל מיליון דולר תוך 48 שעות״ גלובס 31.10.2021 https://bit.ly/3zACFgF [↑](#footnote-ref-30)
31. Gil Press "Israeli Startups Shine In The $92 Billion Cybersecurity Market" Forbs 29.02.2019 https://bit.ly/39iH2ST [↑](#footnote-ref-31)
32. אסף לובין ״תקיפות מחשבים למטרות איסוף מודיעין כחלק מהמאבק בטרור בדין הישראלי, המשווה והבין-לאומי״ חוקים יג 255 (2020). [↑](#footnote-ref-32)
33. חוק-יסוד: כבוד האדם וחירותו. [↑](#footnote-ref-33)
34. חוק הגנת הפרטיות, תשמ"א-1981. [↑](#footnote-ref-34)
35. שם, פרקים א׳ ו-ג׳. סעיף 1 בחוק קובע: ״לא יפגע אדם בפרטיות של זולתן ללא הסכמתו״, וסעיף 4 בחוק קובע כי ״פגיעה בפרטיות היא עוולה אזרחית״. [↑](#footnote-ref-35)
36. שם, בדגש על פרק ב׳. [↑](#footnote-ref-36)
37. חוק הגנת הפרטיות, התשמ"א–1981, סעיפים 4-5. [↑](#footnote-ref-37)
38. שם, סעיף 17. [↑](#footnote-ref-38)
39. שם, פרק ג׳. [↑](#footnote-ref-39)
40. חוק המחשבים, תשנ״ה-1995. [↑](#footnote-ref-40)
41. שם, סעיף 1. [↑](#footnote-ref-41)
42. שם, סעיף 4. [↑](#footnote-ref-42)
43. שם, סעיף 6(א)(1). [↑](#footnote-ref-43)
44. חוק האזנת סתר, תשל"ט-1979. [↑](#footnote-ref-44)
45. שם, סעיף 1. [↑](#footnote-ref-45)
46. שם, סעיף 3. [↑](#footnote-ref-46)
47. שם, סעיף 2 רבתי. [↑](#footnote-ref-47)
48. שם, בסעיף 13(א) נקבע שמידע שנקלט בהאזנת סתר פסולה אינו קביל כראיה בביהמ״ש, לצד חריגים לכלל זה. [↑](#footnote-ref-48)
49. חוק האזנת סתר 1975, פרק ב׳. [↑](#footnote-ref-49)
50. שם, פרק ג׳. [↑](#footnote-ref-50)
51. ביהמ״ש מאשר למשטרה צווי האזנת סתר בשיעורים של 99.5 אחוזים. ראו: יהושע (ג׳וש) בריינר ״בכירים במשטרה: שופטים שמאשרים האזנה לא יודעים באיזה כלי המשטרה תשתמש״ הארץ 19.01.2022 https://bit.ly/3xOMPJs [↑](#footnote-ref-51)
52. שם, סעיף 6(א)(ב). [↑](#footnote-ref-52)
53. שם, כגון בסעיף 6(ד) הדורש לפרט את זהות האדם והמכשיר בו הותר להאזין. [↑](#footnote-ref-53)
54. שם, סעיף 6(ג). [↑](#footnote-ref-54)
55. שם, סעיף 6(ה). [↑](#footnote-ref-55)
56. ראו לעיל פרק 2.3. [↑](#footnote-ref-56)
57. חוק האזנת סתר, סעיף 4(א). [↑](#footnote-ref-57)
58. שם, סעיף 1. [↑](#footnote-ref-58)
59. שם, סעיף 4(ג). [↑](#footnote-ref-59)
60. שם, סעיף 4(ד). [↑](#footnote-ref-60)
61. שם, סעיף 7(א). [↑](#footnote-ref-61)
62. שם, סעיף 5(א). [↑](#footnote-ref-62)
63. שם, סעיפים 5(ב)(ג). [↑](#footnote-ref-63)
64. חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת) 2007. [↑](#footnote-ref-64)
65. שם, סעיפים 3(א)(ב)(ג)(ד)(ה)(ו)(ז)(ח)(י). [↑](#footnote-ref-65)
66. שם, סעיף 4. למשל: סעיף 4(ב) הקובע הגבלת תוקף לעד 24 שעות. [↑](#footnote-ref-66)
67. חוק שירות הביטחון הכללי, תשס"ב-2002. [↑](#footnote-ref-67)
68. עד שנה זו פעל השב״כ ללא סמכות מוסדרת בחוק. ראו: אריאל צימרמן ״הצעת חוק השב״כ: ניתוח משווה״ המכון הישראלי לדמוקרטיה (1997). [↑](#footnote-ref-68)
69. חוק השב״כ, סעיף 7(א)(ב). [↑](#footnote-ref-69)
70. שם, סעיף 8(א)(1). [↑](#footnote-ref-70)
71. שם, בסעיף 11(א) מחדד החוק כי אותו ״מידע״ לא כולל ״תוכן שיחה״ ע״פ חוק האזנת סתר. כלומר ההיתר הוא לאיסוף מידע בלבד, ואם ברצון הארגון להאזין לשיחה – עליו לפעול בערוץ של חוק האזנת סתר. [↑](#footnote-ref-71)
72. שם, סעיף 11(ב)(ג). [↑](#footnote-ref-72)
73. עמיר כהנא ויובל שני ״רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה״ המכון הישראלי לדמוקרטיה 52 (2019). [↑](#footnote-ref-73)
74. CJEU, C-311/18, Maximillian Schrems v. Data Protection Commissioner (16.7.2020). [↑](#footnote-ref-74)
75. בפסק הדין אף נדונה שאלת שיתוף מידע אישי של אזרחים עם מדינות צד ג׳ לצרכי שמירה על הביטחון של אותן מדינות מקבילות. מדובר בדיון נפרד ומרתק, עליו ראוי להרחיב במועד אחר. [↑](#footnote-ref-75)
76. פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט-1969. [↑](#footnote-ref-76)
77. שם, סעיף 24(א)(1) [↑](#footnote-ref-77)
78. שם, סעיף 32(א). [↑](#footnote-ref-78)
79. הנחיית פרקליט המדינה 7.14 ״עקרונות הפעולה בנוגע לאופן התפיסה, החיפוש, ההעתקה והעיון במחשבים ובחומרי מחשב, תיעודם והעמדת התוצרים המהווים "חומר חקירה" לעיון ההגנה״ (21.02.2021). [↑](#footnote-ref-79)
80. בעידן הדיגיטלי, זוהי דרך הפעולה המניבה את המידע הרב ביותר, שכן כמות המידע הקיימת במחשב או בטלפון גדולה בהרבה מזו העולה מהאזנת סתר או מקבל מידע ממאגר. [↑](#footnote-ref-80)
81. רע"א 8019/06 ידיעות אחרונות בע"מ נ' מירב לוין (נבו 23.10.2009). [↑](#footnote-ref-81)
82. שם, עמ׳ 10, פסקה 22 לפסק דינו של השופט ס׳ ג׳ובראן. [↑](#footnote-ref-82)
83. בג״ץ 3809/08 האגודה למען זכויות האזרח נ׳ משטרת ישראל (נבו 28.05.2012). [↑](#footnote-ref-83)
84. בג"ץ 2109/20 עו״ד שחר בן מאיר נ' ראש הממשלה (נבו 26.04.2020). [↑](#footnote-ref-84)
85. דנ"פ 1062/21 יונתן אוריך נ' מדינת ישראל (נבו 11.01.2022). [↑](#footnote-ref-85)
86. בפרשת יששכרוב (ע"פ 5121/98 טור' רפאל יששכרוב נ' התובע הצבאי פ"ד סא(1), 461 (04.05.06)) חייל הואשם בהחזקת סם, ונגבתה ממנו עדות מפלילה בטרם שבושר לו כי יכול להתייעץ עם עו״ד, כמחויב בסעיף 12 לפקודת הראיות. ביהמ״ש פסק כי יש לפסול את ההודאה שנגבתה מהנאשם שלא כדין, לאור הזיקה לזכות החוקתית לכבוד ולחירות. נקבע כי לביהמ״ש מרחב שיקול נרחב בהתאם לנסיבות כל מקרה, ובהתאם לשאלות הנזק מול התועלת החברתית בפסילת הראיה, וחומרת אי-החוקיות שבהשגת הראיה ומרכזיותה בהשגה. [↑](#footnote-ref-86)
87. בר לביא ורועי ברק ״הדלפת ענק חושפת: תוכנת הריגול של NSO עקבה אחר עיתונאים, ראשי מדינות ופעילי זכויות אדם״ גלובס 19.07.2021 https://bit.ly/3O76SZ6 [↑](#footnote-ref-87)
88. אסף לובין ״תקיפות מחשבים למטרות איסוף מודיעין כחלק מהמאבק בטרור בדין הישראלי, המשווה והבין-לאומי״ חוקים יג 253 (2020). [↑](#footnote-ref-88)
89. להרחבה על סוגי הרוגלות, נוזקות ותוכנות הפצחנות השונות: אסף לובין ״תקיפות מחשבים למטרות איסוף מודיעין כחלק מהמאבק בטרור בדין הישראלי, המשווה והבין-לאומי״ 257 חוקים יג (2020). [↑](#footnote-ref-89)
90. חוק-יסוד: כבוד האדם וחירותו, סעיף 8. [↑](#footnote-ref-90)
91. מיכאל בירנהק ״מאוריך לפגסוס: על פרטיות חוקתית בחקירות משטרה / מיכאל בירנהק״ ICON-S-IL Blog 31.01.2022 https://bit.ly/3HKYQDa [↑](#footnote-ref-91)
92. דוגמת נוספת לניסיון הסדרה היא תזכיר חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה) מ-2011 שעבר ב-2014 כהצעת חוק בקריאה ראשונה בלבד, אשר ביקש לייחד פרק נפרד לחדירה מרחוק לחומרי מחשב. בעקבות פיזורי כנסות הליך החקיקה לא המשיך לקריאה שנייה ושלישית. [↑](#footnote-ref-92)
93. רע"א 2558/16 פלונית נ' קצין התגמולים – משרד הביטחון, פס' 58 לפסק הדין של השופטת ברק-ארז (נבו 5.11.2017). שם מדובר היה בפרטיות מידע רפואי. [↑](#footnote-ref-93)
94. ראו דיון מפורט לעיל בפרק 2.3. [↑](#footnote-ref-94)
95. חוק האזנת סתר תשל״ט-1979, סעיף 1. [↑](#footnote-ref-95)
96. העובדה שהחיפוש שלי בדבר מבנה הארגון והדרגות בשב״כ ובמוסד העלה חרס היא משמחת. [↑](#footnote-ref-96)
97. יש לקיים אף דיון בהיקף היתר המעשה הפצחני והגישה למידע שניתן לאסוף, אולם אין זה המקום להאריך. [↑](#footnote-ref-97)
98. ראו פירוט לעיל בפרק 3.1. [↑](#footnote-ref-98)
99. חוק האזנת סתר תשל״ט-1970, סעיף 6(ו). [↑](#footnote-ref-99)
100. חוק-יסוד: כבוד האדם וחירותו, סעיף 8. [↑](#footnote-ref-100)
101. דרישה שלא קיבלה ביטוי משמעותי בפסיקה, אשר שמה דגש לרוב על יתר המבחנים. [↑](#footnote-ref-101)
102. כפי שהוסבר לעיל ע״י נציג השב״כ בדיון על תיקון 131 לחוק השב״כ. [↑](#footnote-ref-102)
103. אריסטו רטוריקה עמ׳ 24–35 (מהדורת ספרית פועלים) 2002. [↑](#footnote-ref-103)
104. זיו קריסטל "מדינת משטרה? מבט לעתיד של חוק החיפוש החדש" פוסטה: אתר לענייני חברה חוק 277 ומשפט (15.2.2018) 15916/https://posta.co.il/article.. [↑](#footnote-ref-104)
105. פיקוח נציג נבחרי הציבור שהצעתי לעיל מסייע אף בנושא. [↑](#footnote-ref-105)
106. בג״ץ 3809/08 האגודה למען זכויות האזרח נ׳ משטרת ישראל, 19 פס׳ 11 לפסק דינה של הנשיאה ביניש (נבו 28.05.2012). [↑](#footnote-ref-106)