



ח"כ שמחה רוטמן, יו"ר ועדת חוקה חוק ומשפט של הכנסת

**חברי ועדת חוקה חוק ומשפט של הכנסת**

**הנדון: דיון בדו"ח האזנות סתר 2021, לאור מסקנות דו"ח ועדת מררי**

1. אנו מברכים על קיומו של הדיון. בשנים האחרונות ביצענו כמה מחקרים בעניין פיקוח על מעקבים מקוונים<sup>1</sup>, פרסמנו חוות דעת בעניין הפיקוח על היצוא של טכנולוגיות מעקב וכן כינסנו קבוצת מומחים על מנת לנסות להתוות מסגרת לחוק מעקבים חדש. תהליך זה עודנו בעבודה.
2. בדיון וחשבון הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים (דו"ח ועדת מררי) שהתפרסם באוגוסט 2022<sup>2</sup>, נכתב באותיות בולטות: "במבט לאחור הצוות סבור כי המשמעות הדרמטית של הכנסה לשימוש של מערכת בעלת יכולות טכנולוגיות רחבות היקף המהווה נקודת מפנה מבחינת עולם האזנות הסתר, לא הובנה לאשורה על ידי גורמי המשטרה הרלוונטיים. לאורך השנים לא יוחסה מלוא המשמעות המתבקשת להיקף היכולות הפוטנציאלי של המערכת ולעצם כניסת חומרים אסורים מתוך טלפונים ניידים אל מחשבי המשטרה, ולנגישותם של החומרים שהתקבלו במערכות המשטרה"<sup>3</sup>.
3. ואכן, אין מדובר אך בסוגיה "איזוטרתית" של פגיעה בפרטיות. יכולתה של משטרת ישראל להחזיק ברשותה טכנולוגיה רבת עוצמה המאפשרת להיכנס מרחוק ובאופן סמוי למכשיר טלפון, לשאוב את כל תכולתו ובכלל זה מידע האגור בו וביישומי ענן הקשורים אליו (data at rest), וכמובן מידע עתידי (data in transit) – ולהחזיק אותו בשרתיה "לעת מצוא" - היא ערעור משמעותי של הפרדת הרשויות. די אם נחשוב על

<sup>1</sup> תהילה שוורץ אלטשולר ורחל ארידור הרשקוביץ, הצעת חוק הגנת הפרטיות התשע"ט-2019 (2019) <https://www.idi.org.il/books/27125>; עמיר כהנא ויובל שני, רגולציה של מעקב מקוון בדיון הישראלי ובדיון המשווה (2019) <https://www.idi.org.il/books/25754>; עמיר כהנא ויובל שני, פיקוח על מעקב מקוון בישראל (2020) <https://www.idi.org.il/books/32264>, בעמ' 201-200 (להלן: כהנא ושני, פיקוח).

<sup>2</sup> [https://fs.knesset.gov.il/25/Committees/25\\_ci\\_bg\\_1962239.pdf](https://fs.knesset.gov.il/25/Committees/25_ci_bg_1962239.pdf)

<sup>3</sup> סעיף 6 לדו"ח.

**אמיר אלשטיין**

יו"ר הוועד המנהל

**הנשיא העשירי ראובן ריבלין**

יו"ר של כבוד

**יוחנן פלסנר**

נשיא

**ברנד מרכוס**

יו"ר בינלאומי

**חברי הוועד המנהל**

אלי גרונר

פרופ' ירד וניצקי-טרוסי

ד"ר חן ליכטנשטיין

מזל מועלם

שגריר לשעבר סלי מרידור

פרופ' פאדיה נאסר אבו-אלהיג'א

עו"ד אבי פישר

ד"ר מיכל צור

יוסי קוצ'יק

**המועצה הבינלאומית**

פרופ' רונלד דניאלס, יו"ר

השופטת רוזלי סילברמן אבול, קנדה

אליט אברמס, ארה"ב

שגריר לשעבר מרטין אינדיק, ארה"ב

אן אמלבלאום, ארה"ב

פרופ' יורנו בגדנור, בריטניה

השופטת דורית ביניש, ישראל

השופט סטיבן ברייר, ארה"ב

השופט סלים ג'ובראן, ישראל

ד"ר ג'וזף ג'וספה, גרמניה

פרופ' משה הלברטל, ישראל

פרופ' מייקל וולצר, ארה"ב

פרופ' רוברט מנקין, ארה"ב

פרופ' כריסטוף מרקשיס, גרמניה

השופט אברהם סופר, ארה"ב

ברט טפטנס, ארה"ב

פרופ' ארווין קוטלר, קנדה

פרופ' גרהרד קספר, ארה"ב

פרופ' יהודה ריינהרץ, ארה"ב

פרופ' גבריאלה שלו, ישראל

**סגני נשיא**

פרופ' סוזי נבות, מחקר

פרופ' קרנית פלוג, מחקר

ד"ר ישי ג'סיץ, פרס, אסטרטגיה

**עמיתים בכירים**

פרופ' איסמעיל אבו סעד

פרופ' תמר הרמן

פרופ' נתן זוסמן (אורח)

פרופ' עמית כהן

פרופ' יותם מרגלית

פרופ' דניאל סטטמן

פרופ' בני פורת

פרופ' יובל פלדמן

פרופ' מרדכי קרמניצר

פרופ' גדעון רהט

ד"ר תהילה שוורץ אלטשולר

פרופ' יובל שני

**מייסדים**

ד"ר אריק כרמון

מזכיר המדינה ג'ורג' שולץ (1920-2021)



## המכון הישראלי לדמוקרטיה

- שימוש שעושה המשטרה בטכנולוגיה כזאת כנגד פוליטיקאים ואישי ציבור אחרים והכוח שהיא צוברת בשל כך שאגרה את "המוח והלב הדיגיטליים" שלהם בשרתיה; ולחילופין, על מקרה שבו שר, המבקש לבצע התערבות פוליטית בעבודת המשטרה, דורש ממנה להפעיל טכנולוגיות כאלה כנגד מתנגדיו הפוליטיים.
4. אין מדובר באפשרויות מופרכות. בשנים האחרונות מתרבות העדויות על שימושים לרעה במערכת "פגסוס" ובמערכות של חברות אחרות על ידי משטרים שרכשו רישיונות להפעלתה, ובכלל זה משטרים שאינם דיקטטוריים, כמו מקסיקו, הונגריה והודו.
5. במכתבנו אליכם נתייחס לשני עניינים. האחד הוא הצורך הבווער לעדכן את חובות הדיווח על האזנות סתר ומעקבים דיגיטליים כך שאתם, חברי הכנסת, תוכלו להפוך את הדיווח לכלי פיקוח אפקטיבי. השני הוא הצורך לחוקק חוק מעקבים דיגיטליים חדש.
6. נשמח לעמוד לרשותכם בכל עניין שיידרש

בברכה,

עו"ד עמיר כהנא

ד"ר תהילה שוורץ אלטשולר

התוכנית לדמוקרטיה בעידן המידע

המכון הישראלי לדמוקרטיה



## חלק ראשון: חובות הדיווח על האזנות סתר

1. חוק האזנת סתר<sup>4</sup> מורה כי על המשטרה למסור לוועדת החוקה של הכנסת דוח שנתי על הפעלת הסמכויות תחת פרק ג' לחוק (האזנת סתר למטרת מניעת עבירות וגילוי עבריינים). ברם, לאורך השנים הוועדה מיעטה לדון בדיווחים אלה ולא שימשה מערך פיקוח אפקטיבי על האזנות סתר.<sup>5</sup> על רקע החשיפות ביחס לשימוש שעושה המשטרה ברוגלות לשם מעקב אחר אזרחים, התחדש העניין הפרלמנטרי בדיווחי המשטרה לפי החוק והתקיים דיון בחודש מרץ 2022.
2. בדו"ח מררי נקבע כי במשטרה קיימת מערכת מבצעית לאיסוף מידע באמצעות פריצה מרחוק לטלפונים סלולריים. עוד נקבע כי מערכת שמירת הסף והפיקוח לא פעלה, ו"לא הועבר המידע הנדרש בעניין מערכת סייפן, על כלל מאפייניה, לידיעת הייעוץ המשפטי לממשלה, וממילא לא התקיים דיון משפטי עקרוני בנושא"<sup>6</sup>.
3. כעולה מן הדברים, מערך הפיקוח והבקרה על שימוש בטכנולוגיות מעקב בישראל – כשל. השאלה היא כיצד לתקן את הדברים. **לדעתנו, הצעד ההכרחי הראשון הוא לשפר מאד את יכולת הבקרה של הכנסת על האזנות סתר.**
4. לשון סעיף 6(ז) לחוק מורה כי "שר המשטרה ימסור, מדי שנה, דין וחשבון לוועדת החוקה חוק ומשפט של הכנסת, שיכלול את מספר הבקשות שהוגשו ואת מספר ההיתרים שניתנו לפי פרק זה, בציון מספר האנשים, וכמות קווי הבזק ומתקני הבזק, אשר האזנה אליהם הותרה". ברבות השנים התווסף לדוחות מידע על התפלגות מספר הצווים לפי סוגי העבירות.
5. אבל, כפי שענייכם רואות מן הדו"ח לשנת 2021 הנמצא לפניכם, הפרמטרים שבדיווח הקיים אינם **מספיקים על מנת לעמוד על האופן בו המשטרה מפעילה את סמכויותיה תחת החוק והדיווחים במתכונתם הנוכחית אינם מאפשרים לכם, כחברי הוועדה נציגי הציבור, ללמוד על המצב לאשורו.**
6. בראש ובראשונה, בינואר 2022 דיווחה המשטרה אך ורק על מספרי בקשות, מספרי מואזנים, ומספרי קווי בזק שאליהם היתה האזנה. כפי שאנו כבר יודעים עכשיו ואושר על ידי וועדת מררי, בשנת 2021 הפעילה המשטרה את מערכת סייפן/פגסוס, וביקשה צווי האזנת סתר כדי להפעיל את המערכת. בכל זאת, בדו"ח שלפניכם אין זכר למספרי האזנות שאינן דרך קווי בזק וליתר דיוק – שכל תכליתן לעקוף את חוסר היכולת להאזין דרך קווי בזק.
7. בדו"ח מררי נכתב בעניין הדיווח המשטרתי לשופטים בזמן הבקשות לקבל צווי האזנות סתר, כי בניגוד לאמור בסעיף 6(ד) לחוק האזנת סתר המחייב לפרט את דרכי ההאזנה שהותרו – לא נמצא פירוט כזה בצווים רבים. הדבר מלמד על כך שלא פורטה בבקשות העובדה שהאזנה תתבצע באמצעות רוגלה וכי הבקשה להפעלת סמכות עזר לא כללה הבהרה ש"צו כניסה למקום" כוונתו הדבקת הטלפון ברוגלת סייבר ולא כניסה פיזית

<sup>4</sup> חוק האזנת סתר, התשל"ט-1979, ס"ח 938, 118

<sup>5</sup> לפי הנתונים באתר הוועדה, נראה כי טרם הדיון מיום 1.3.2022, הדיון האחרון שעסק בדיווח השנתי של המשטרה לפי סעיף 6(ז) התקיים ביום 28.11.2006.

<sup>6</sup> ראו פרק 8.1.3 לדו"ח והציטוט מתך תחילת פרק 10.2 לדו"ח.



- למקום. דבר זה ניכר גם בדו"ח שלפניכם ולמעשה בדיוק כפי שהשופטים לא קיבלו את תמונת המצב המלאה, גם אתם, חברי הכנסת, לא מקבלים אותה.
8. וועדת מררי אימצה פרשנות מרחיבה לסעיף 10(א) לחוק האזנת סתר, הקובע כי "מי שמוסמך להתיר האזנת סתר לפי חוק זה, רשאי להתיר גם כניסה למקום לצורך התקנת אמצעים הנדרשים להאזנה, פירוקם או סילוקם". הוועדה סברה כי ניתן לראות הדבקות מכשיר ברוגלה כ"כניסה למקום". איננו מתייחסים כרגע כלל לשאלת הפרשנות הזאת, אבל גם אם נניח שהיא תקפה, מכל מקום יש צורך לעדכן את חובת הדיווח בנוגע לחוק האזנות סתר, כך שתכלול לפחות סיכום מספרי של המקרים שבהם נעשה שימוש ברוגלות ולא בהאזנה לקווי בזק.
9. עוד קבעה הוועדה כי בהיעדר נהלים כאלה ובהיעדר היכרות של חלקים במשטרה עם הנהלים הקיימים<sup>7</sup>, יש לקבוע הנחיות ונהלים פנימיים שיחייבו ניוון של חלק מן היכולות של מערכות המעקב וכן יקבעו מגבלות על שימוש במידע עודף שהושג במהלך ההדבקה ברוגלה. ניתן להתווכח גם על השאלה האם נהלים פנימיים הם תחליף להסמכה מפורשת בחוק, אבל בכל מקרה יש מקום לדרוש שחברי הכנסת יחשפו נהלים אלה והמשטרה תהיה חייבת לדווח הן על תוכן הנהלים הן על עדכונם או שינויים.
10. לכן, עוד לפני חקיקת חוק מעקבים רחב, אנחנו מציעים כבר כעת לפעול כדי להגביר באופן משמעותי את הפירוט הנדרש בדיווחים השנתיים של המשטרה מכוח החוק, וזאת בין השאר על בסיס השוואה עם הדיווחים הפומביים הנוהגים בבריטניה ובארצות הברית ביחס להפעלת סמכויות מעקב על ידי סוכנויות הביטחון ואכיפת החוק.<sup>8</sup> נקדים ונדגיש כי מכיוון שחלק מפרטים אלו עשויים לחשוף יכולות מבצעיות (ר' לדוגמה להלן בס' 1.4, 2.11, 8.7), מוצע שלדיווחים תהא גרסה מסווגת וגרסה פומבית ללא המידע המסווג.
11. הואיל והדו"ח נשלח אל הכנסת בינואר 2022 והדיון בו נעשה רק עתה, לאחר שהתפרסם דו"ח מררי, אנו מציעים לכם בעת הזאת לבקש תשובות גם לשאלות הבאות:
- 11.1 האם מאז פרסום דו"ח מררי הוכנו נהלים להפעלת רוגלות או למעקב באמצעות כלי סייבר (בנפרד מהנוהל של האזנות סתר)? מכוח איזה חוק? (נתוני תקשורת/פקודת סדר הדין הפלילי מעצר וחיפוש)
- 11.1.1 האם הנוהל כולל רשימה של עבירות שבעטיין ניתן להפעיל את אותם הכלים?

<sup>7</sup> ראו פרק 8 לדו"ח.

<sup>8</sup> ר' דו"ח נציב סמכויות חקירה הבריטי IPCO, Annual Report of the Investigatory Powers Commissioner 2020 (2022), [https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020\\_Web-Accessible-version.pdf](https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf); דו"ח הנהלת בתי המשפט הפדראליים ביחס לבית הדין למודיעין זר (FISC) Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2020 (16.07.2021) [https://www.uscourts.gov/sites/default/files/fisc\\_annual\\_report\\_2020.pdf](https://www.uscourts.gov/sites/default/files/fisc_annual_report_2020.pdf) (להלן: FISC report 2020); דו"ח האזנות הסתר הפדרלי השנתי, United States Courts, Wiretap Report 2020 (31.12.2020) <https://www.uscourts.gov/statistics-reports/wiretap-report-2020> (להלן: Wiretap report 2020)



## המכון הישראלי לדמוקרטיה

- 11.1.2 האם הנוהל כולל רשימה או איפיון של הכלים המותרים בהפעלה?
- 11.1.3 האם ישנו מתאם בנוהל בין חומרת העבירה לבין הכלי שבו נעשה השימוש?
- 11.2 בהינתן הקביעה בדו"ח מררי שלפיה הייעוץ המשפטי במשטרה לא הכיר לפחות חלק מן הנהלים של יחידת הסיגינט במשטרה - מי במשטרה אחראי להפעיל כלי סייבר לפריצה לטלפונים, ומי הסמכות במשטרה המפקחת עליו?
- 11.3 כפי שנכתב בדו"ח מררי<sup>9</sup>, בידי המשטרה כלי רוג'לה נוספים. אלו כלים משטרה רכשה ב-5 השנים האחרונות כלים מחברות נוספות על חברת NSO (למשל – Cellebrite)?
- 11.4 האם ישנם מקרים בהם המשטרה מתקינה כלי סייבר על טלפונים של אזרחים בהסכמתם?
- 11.5 האם לאחר דו"ח מררי המשטרה פנתה ליועמ"ש לבקש הנחיות לשימוש בפריצת כלי סייבר לטלפונים והאם נוסחו כבר נהלים חדשים או הנחיות מטעם היועמ"ש?
- 11.6 האם ניתן להציג אותם?
12. לתפיסתנו, על הכנסת לדרוש, באמצעות תקנות או באמצעות חקיקה, כי להבא הדו"חות הנוגעים לחוק האזנת סתר יכללו להבא את הפרטים הבאים:

### א. שקיפות נתוני המשטרה

1. אמצעי המעקב
- 1.1 מספר האזנות באמצעות התקני ציתות פיזיים במקום השיחה (Bugging)
- 1.2 מספר האזנות באמצעות קווי בזק/סלולר
- 1.3 מספר האזנות באמצעות רוג'לות
- 1.4 מספר האזנות באמצעים טכנולוגיים אחרים (פירוט בדו"ח המסווג)
2. סוג התוכן המבוקש בצו/היתר שהמשטרה מגישה לבית משפט
- 2.1 מספר צווים/היתרים שבהם התבקש תוכן שיחה טלפונית
- 2.2 מספר צווים/היתרים שבהם התבקש תוכן תקשורת דוא"ל
- 2.3 מספר צווים/היתרים שבהם התבקש תוכן מסרים מדיים
- 2.4 מספר צווים/היתרים שבהם התבקש תוכן SMS
- 2.5 מספר צווים/היתרים בהם התבקשו נתוני תקשורת במקביל לנתוני תוכן
- 2.6 מספר צווים/היתרים בהם התבקש תוכן תקשורת בפקסימיליה
- 2.7 מספר צווים/היתרים בהם התבקש תוכן תקשורת בטלפרינטר
- 2.8 מספר צווים/היתרים בהם התבקש תוכן תקשורת בין מחשבים
- 2.9 מספר צווים/היתרים בהם התבקש תוכן תקשורת במכשיר קשר אלחוטי
- 2.10 מספר צווים/היתרים בהם התבקש תוכן שיחה בדיבור (ולא בבזק)
- 2.11 מספר צווים/היתרים בהם התבקש סוג נתונים אחר (פירוט, בדו"ח המסווג)
3. מספר הצווים/היתרים בחתך של היחידה המשטרתית והמחוז שהגיש אותם
4. מספר האזנות לפי סוג העבירה הנחקרת
5. מושאי המעקב
- 5.1 מספר ההאזנות לחשודים
- 5.2 מספר האזנות לאזרחים שאינם חשודים

<sup>9</sup> עמודים 5-6 לדו"ח.



- 5.3. מספר האזנות לתקשורת חסויה
6. משך תקופת האזנה
- 6.1. בחתך אמצעי מעקב
- 6.2. בחתך סוג נתונים
- 6.3. בחתך מושאי המעקב
7. נוכח קיומו של מסלול הסמכה עוקף בית משפט, תחת ס' 7 לחוק, במסגרתו רשאי המפקח הכללי של המשטרה לאשר **האזנות סתר דחופות לתקופה שאינה עולה על 48 שעות**, מן הראוי לקבל דיווח שנתי על היתרים לשימוש בסמכויות אלו, ועל אישורם או ביטולם לאחר מעשה.

## ב. שקיפות נתוני הפיקוח שיפוטי

האזנות סתר למניעת עבירות וגילוי עבריינים מותנות בצו מאת נשיא בית המשפט המחוזי או סגנו שהסמיך לכך. נתונים בדבר כמות הבקשות לצווים, כמות הצווים שניתנו וכמות הצווים שנדחו, מדווחים מדי שנה תחת ס' 6(ז) לחוק. בדיווחים אלה שיעור הבקשות הנדחות נמוך עד אפסי,<sup>10</sup> ועלול ליצור את רושם שמא בתי המשפט משמשים כחותמת גומי לבקשות המשטרה.<sup>11</sup>

ואולם, יש הטוענים כי שיעור הדחייה הנמוך של צווי האזנת סתר (או צווי מעקב מקוון אחרים, בבתי משפט אחרים) משקף דווקא את האפקטיביות של הערכאה השיפוטית כגורם מפקח – אם באמצעות הרתעת רשויות אכיפת החוק מלבקש צווים ללא הצדקה וביסוס חוקיים, ואם בשל צמצום של צווים על ידי בית המשפט.<sup>12</sup> נוכח ביקורת דומה על שיעור הדחייה של בית המשפט למוזדעין זר (FISC) בארצות הברית, התווסף לדיווחים הסטטיסטיים השנתיים שלו, לצד הנתונים על מספר הצווים שנדחו,<sup>13</sup> פרמטר של **מספר הצווים ששונו על ידי בית המשפט**, באופן המאפשר לבחון את מידת המעורבות של הבית המשפט בתכני צווים. אנו מציעים להוסיף פרמטר דומה, ואף לפרט במסגרתו את **סוגי השינויים** הנפוצים שמורה בית המשפט לבצע בבקשות להאזנת סתר טרם הוא מאשר אותן.

8. צווים שיפוטיים
- 8.1. כמות צווים שניתנו
- 8.2. כמות צווים שנדחו
- 8.3. כמות צווים חוזרים (הארכות)
- 8.4. כמות צווים ששונו בעקבות הוראת בית המשפט
- 8.4.1. בחלוקה לפי סוגי שינויים נפוצים

<sup>10</sup> ר' כהנא ושני, פיקוח, בה"ש 1 לעיל בעמ' 201-200.

<sup>11</sup> ר' כהנא ושני, פיקוח, בה"ש 1 לעיל, בעמ' 153, 89.

<sup>12</sup> ר' למשל David Rudenstine, THE AGE OF DEFERENCE: THE SUPREME COURT, NATIONAL SECURITY, AND THE CONSTITUTIONAL ORDER, 148-149 (2016)

<sup>13</sup> ר' FISC Report 2020, בה"ש 8 לעיל.



- 8.4.1.1. צמצום משך הצו
- 8.4.1.2. צמצום מספר הנעקבים
- 8.4.1.3. אחר (פירוט)
- 8.5. כמות צווים כוללת
- 8.6. בחתך בית משפט
- 9. האזנת סתר ללא פיקוח שיפוטי
- 9.1. מספר היתרים שניתנו להאזנת סתר בחירום לפי ס' 7(א) לחוק
- 9.2. מספר היתרים שבוטלו על ידי היועץ המשפטי לפי ס' 7(ב) לחוק
- 9.3. מספר היתרים שאושרו בדיעבד על ידי בית המשפט לפי ס' 7(ג) לחוק

### ג. אפקטיביות מודיעינית

האם כלי האזנת הסתר והמעקב שנמצאים בשימוש המשטרה משיגים את מטרתם? אינדיקציה לכך יכולה להיות בחינה של התוצאות של היתרים וצווים שניתנו תחת החוק – האם אלו הבשילו לכדי הרשעה או סיכול פשיעה?

אנו מציעים לבחון זאת גם בחתך של סוג הנתונים המבוקש ושל סוגי התוכן המבוקשים, על מנת ללמוד על מיצוי יכולות החקירה במשטרה. כמו כן, יש להביא לידיעת הוועדה מידע ביחס לחסמים טכניים לביצוע האזנות, דוגמת קשיים בפינוח חומר מוצפן.<sup>14</sup>

- 10. אפקטיביות
- 10.1. מספר צווים/היתרים בתוקף בחקירה פעילה
- 10.2. מספר צווים/היתרים בחקירות שהסתיימו
- 10.2.1. ללא הרשעה
- 10.2.2. בהרשעה
- 10.3. מספר עבירות שנמנעו/סוכלו בעקבות צו
- 10.4. מספר עבירות שנמנעו/סוכלו בעקבות היתר תחת ס' 7 לחוק
- 10.5. [בחתך אמצעי מעקב]
- 10.6. [בחתך סוג תוכן]
- 10.7. כמות האזנות סתר שאושרה אך לא ניתן היה להפיק מידע בפועל
- 10.7.1. בשל התווך הטכנולוגי
- 10.7.2. בשל שימוש באמצעי הצפנה
- 10.7.3. סיבות אחרות (פירוט)

<sup>14</sup> ר' לדוג' Wiretap Report 2020, בה"ש 8 לעיל.



המכון הישראלי  
לדמוקרטיה

#### ד. פיקוח על השומרים

סעיף 6(ד) לחוק מורה למפכ"ל המשטרה להגיש דיווחים חודשיים ליועץ המשפטי לממשלה על היתרים שניתנו לפי פרק זה, וכן על האזנות לשיחות חסויות ועל האזנות לפי חוק חסינות חברי הכנסת. במסגרת הדיווח השנתי לוועדת חוקה חוק ומשפט, יש מקום להוסיף:

- 12.1 מספר הישיבות החודשיות שנערכו באותה שנה של נציגי המשטרה עם נציגי משרד המשפטים והתאריכים שלהם.
- 12.2 פירוט סוגיות שהתעוררו מול משרד המשפטים הנוגעות להאזנות סתר
- 12.3 פירוט נהלים חדשים שנכנסו לתוקף לאור כניסת טכנולוגיות מעקב חדשות





## 1. הקדמה

בחודש ינואר 2022, התפרסמה סדרה של פרסומים בעיתון כלכליסט בהם נטען שהמשרה עושה שימוש ברוגלת 'פגסוס' של חברת NSO.<sup>15</sup> דו"ח מררי, שהתפרסם באוגוסט 2022, אימת את הטענות לשימוש ברוגלה. פרשת הרוגלות בשירות משרתת ישראל משמשת תזכורת לכך שדיני המעקב המקוון בישראל הם מיושנים, וטעונים התאמה למציאות הטכנולוגית בת זמננו, לצרכי המודיעין של רשויות אכיפת החוק, וכן לסטנדרטים מתקדמים של הגנה על פרטיות וזכויות אדם. המסגרת המשפטית הקיימת רזה וחסרה,<sup>16</sup> וראשיתה בשלהי שנות השבעים. התאמת דינים המתייחסים בין השאר להאזנה לתקשורת "בפקסימיליה, בטלקס, בטלפרינטר..."<sup>17</sup> למציאות בה רשויות אכיפת החוק נדרשות למידע המצוי בשכבות שונות של תקשורת וברבדים שונים של תנועה (הצפנה, תקשורת בתיווך פלטפורמות בינלאומיות שאינן בעלי רישיון בזק, גישה לנתונים שמאוחסנים בענן), אינה יכולה להיעשות רק על בסיס פרשנות יצירתית הקבורה בנהלים פנימיים של משרתת ישראל ומשרד המשפטים, אלא יש לתת לה בסיס סטטוטורי.

אשר על כן, נדרשת לתפיסתנו עבודה על חוק מעקבים דיגיטליים חדש שייצור מסגרת חקיקה רחבה שתעסוק בעולם הסייבר האיסופי או המעקבים הדיגיטליים.

## 2. סמכויות מעקב דיגיטליות של משרתת ישראל ורשויות החקירה: תמונת מצב

### 2.1 חוק האזנת סתר: יירוט נתוני תוכן in transit

חוק האזנת סתר מסדיר יירוט של נתוני תוכן בזמן אמת.<sup>18</sup> תחת חוק האזנת סתר, המשטרה מוסמכת לבצע האזנות סתר בכפוף לצו מאת נשיא בית המשפט המחוזי או סגנו שהוסמך לכך, אם שוכנע שהדבר דרוש לגילוי, חקירה או מניעה של עבירות מסוג פשע, או לגילוי ותפיסת עבריינים שעברו עבירות כאמור.<sup>19</sup> האזנת סתר מוגדרת בחוק כהאזנה או הקלטה של שיחת הזולת באמצעות מכשיר, ושיחה היא "בדיבור או בבזק, לרבות בטלפון, בטלפון אלחוטי, ברדיו טלפון נייד, במכשיר קשר אלחוטי, בפקסימיליה, בטלקס, בטלפרינטר או בתקשורת בין מחשבים".<sup>20</sup>

<sup>15</sup> תומר גנון, "חברת NSO בשירות משרתת ישראל: פריצות לטלפון של אזרחים ללא פיקוח או בקרה", כלכליסט (18.1.2022) [https://www.calcalist.co.il/local\\_news/article/s1b1xwx6y](https://www.calcalist.co.il/local_news/article/s1b1xwx6y)

<sup>16</sup> ר' עמיר כהנא ויובל שני, [רגולציה של מעקב מקוון בדיון הישראלי ובדיון המשווה](#) 274-295 (המכון הישראלי לדמוקרטיה, 2019)

<sup>17</sup> ס' 1 לחוק האזנת סתר, התשל"ט-1979, ס"ח 938, 118 (להלן: חוק האזנת סתר)

<sup>18</sup> ר' גם כהנא ושני, בה"ש 16 לעיל, בעמ' 42-52

<sup>19</sup> ס'6(א) לחוק האזנת סתר.

<sup>20</sup> ס' 1 לחוק האזנת סתר



בקשות לצו האזנת סתר ידונו במעמד צד אחד.<sup>21</sup> האזנה לפי היתר מתבצעת ביחס לאדם, קו, מתקן או מקום מוגדרים, ולפי דרכי האזנה מוגדרות.<sup>22</sup> היתר להאזנת סתר לא יינתן לתקופה העולה על שלושה חודשים, וניתן לחדשו מפעם לפעם.<sup>23</sup>

במקרים דחופים, בהם המפכ"ל שוכנע שלשם מניעת פשע או גילוי מבצעיו יש צורך בהאזנת סתר שאינה סובלת דיחוי, הוא רשאי לאשר האזנת סתר אף בלא צו שופט, לתקופה בת 48 שעות. על היתר כאמור יש לדווח ליועץ המשפטי לממשלה, שרשאי לבטל את ההיתר.<sup>24</sup>

האזנה לשיחה ברשות הרבים ("מקום שאדם סביר יכול היה לצפות ששיחותיו יישמעו ללא הסכמתו") מותרת אם נעשתה על ידי מי שהוסמך לכך על ידי קצין משטרה מוסמך לשם מניעת עבירות או גילוי עבריינים.<sup>25</sup>

החוק מכיל כלל פסילה ראייתית מפורשת, לפיו דברים שנקלטו בדרך של האזנת סתר בניגוד להוראותיו לא יהיו קבילים כראיה בבית המשפט אלא בהליך פלילי בשל עבירה לפי חוק האזנת סתר או בהליך פלילי בשל פשע חמור, אם בית המשפט הורה על קבילותה לאחר ששוכנע מטעמים מיוחדים שיפורטו כי בנסיבות העניין הצורך להגיע לחקר האמת גובר על הזכות לפרטיות.<sup>26</sup> לאחרונה, בית המשפט קבע כי ראיות שמקורן בהאזנת סתר כדן יהיו קבילות גם לצורך הוכחת עבירות שאינן מסוג פשע.<sup>27</sup>

## 2.2 חוק נתוני תקשורת: השגת נתוני תקשורת at rest

חוק נתוני תקשורת מסדיר השגת נתוני תקשורת (המוגדרים בחוק כנתוני זיהוי, נתוני מיקום ונתוני תעבורה)<sup>28</sup> מבעלי רישיון בזק על ידי המשטרה ורשויות חוקרות אחרות. המשטרה רשאית לקבל צו מאת בית משפט השלום המורה לבעל רישיון בזק להעביר לידיה נתוני תקשורת, אם הדבר נדרש להצלת חיי אדם, גילוי עבירות, חקירתן או מניעתן, גילוי עבריינים או חילוט רכוש על פי דין.<sup>29</sup> החוק מכיל הוראות לגבי המידע המפורט שיופיע בבקשה ולגבי מסמכים המצורפים

<sup>21</sup> ס'6(ב) לחוק האזנת סתר

<sup>22</sup> ס'6(ד) לחוק האזנת סתר

<sup>23</sup> ס'6(ה) לחוק האזנת סתר

<sup>24</sup> ס'7 לחוק האזנת סתר

<sup>25</sup> ס'8 לחוק האזנת סתר

<sup>26</sup> ס'13 לחוק האזנת סתר

<sup>27</sup> רע"פ 1089/21 מדינת ישראל נ' אליצור אטיאס (14.3.2022)

<sup>28</sup> ס' 1 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007, ס"ח 2122, 72 (להלן: **חוק נתוני תקשורת**)

<sup>29</sup> ס' 3 לחוק נתוני תקשורת.



## המכון הישראלי לדמוקרטיה

לה, <sup>30</sup> ומתווה את תוכן הצו עצמו. <sup>31</sup> ניתן לבקש נתוני תקשורת עתידיים (ובלבד שהתקופה המירבית לקבלתם לא תעלה על שלושים ימים מיום קבלת הצו). <sup>32</sup> צו יהיה בתוקף לשלושים ימים. <sup>33</sup> במקרים דחופים רשאי קצין מוסמך לאשר קבלת נתוני תקשורת ללא צו שיפוטי אם הדבר נדרש בלא דיחוי לא מניעת עבירה מסוג פשע או לשם הצלת חיי אדם. <sup>34</sup>

בעניין האגודה לזכויות אזרח, <sup>35</sup> נקבע כי אין לעשות שימוש בחוק נתוני תקשורת לצורך 'מסעות דיג' ולא לתכליות של איסוף גורף. רשויות החקירה מוסמכות לפנות לבית המשפט בבקשה לקבלת צו על-פי חוק נתוני תקשורת אך לצורך גילוי עבירות או עבריינים קונקרטיים, ולא לצרכי פעילות מודיעינית כללית ביחס לעבירות או עבריינים.

בנוסף, חוק נתוני תקשורת מסדיר הקמת מאגר מידע משטרתי של נתוני זיהוי, <sup>36</sup> ונהלי שיתוף במידע שמקורו במאגר עם רשויות חוקרות אחרות. <sup>37</sup>

בשונה מס' 6 לחוק האזנת סתר, אין בחוק נתוני תקשורת חובת דיווח לוועדת הכנסת הרלוונטית או ליועץ המשפטי לממשלה. תוקפה של הוראת השעה הסטטוטורית שבחוק פג לפני כעשור. <sup>38</sup>

במהלך הגל הראשון של מגיפת הקורונה, הותקנו תקנות שעת חירום לתיקון זמני של חוק נתוני תקשורת באופן שאפשר למשטרה לקבל נתוני מיקום אחרון של מבודדים לצורך פיקוח קיום הוראות הבידוד. <sup>39</sup>

### 2.3 חדירה לחומר מחשב: בחינה של נתוני תוכן at rest

חוק המחשבים מגדיר חדירה לחומר מחשב כ"חדירה באמצעות התקשורת או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר." <sup>40</sup>

<sup>30</sup> ס' 3(ד), (ו) לחוק נתוני תקשורת.

<sup>31</sup> ס' 3(ח) לחוק נתוני תקשורת.

<sup>32</sup> ס' 3(ז) לחוק נתוני תקשורת.

<sup>33</sup> ס' 3(י) לחוק נתוני תקשורת.

<sup>34</sup> ס' 4(א) לחוק נתוני תקשורת.

<sup>35</sup> בג"ץ 3809/08 [האגודה לזכויות אזרח נ' משטרת ישראל](#), פס' 37 (פורם באר"ש, 28.5.2012), פד' 16 לפסק דינה של הנשיא (בדימ') ביניש.

<sup>36</sup> ס' 6-7 לחוק נתוני תקשורת.

<sup>37</sup> ס' 8 לחוק נתוני תקשורת.

<sup>38</sup> ס' 14 לחוק נתוני תקשורת. ר' כהנא ושני, בה"ש 16 לעיל בעמ' 35

<sup>39</sup> תקנות שעת חירום (נתוני מיקום), התש"פ-2020, ק"ת 8390 (16.3.2020). ר' גם פס' 4(ד) להחלטת הביניים בעניין בג"ץ 2109/20 [בן מאיר נ' ראש הממשלה](#) (פורסם באר"ש, 19.3.2020); וכן בג"ץ 2109/20 [בן מאיר נ' ראש הממשלה](#) (פורסם באר"ש, 26.4.2020) בעמ' 3.



סעיף 23א לפקודת סדר הדין הפלילי (חיפוש ומעצר)<sup>41</sup> קובע כי חדירה לומר מחשב יראו אותן כחיפוש הטעון בצו. סעיף זה מאפשר חיפוש במחשבים ומכשירי סלולר שנתפסו פיזית, באופן ממוקד וחד פעמי.

בעניין **אוריך**<sup>42</sup> נקבע כי נוכח החששות מפני סיכול חקירה באמצעות גילוי הכוונה לערוך חיפוש במכשיר נייד, דיון בבקשה לצו חיפוש תחת ס' 23א לפסד"פ חיפוש ומעצר יתקיים במעמד צד אחד. כן נקבע כי משיקולי יעילות החקירה לא יתאפשרו הליכי השגה וערעור על צווי חיפוש. ביחס להשלכות של חיפוש בלתי חוקי בטלפון סלולרי או בחומר מחשב, קבע בית המשפט כי שאלת קבילות הראיות תיעשה במסגרת ההליך העיקרי, והיא תיבחן לאורה של דוקטרינת הפסילה הפסיקתית (הלכת יששכרוב).<sup>43</sup>

רחום טוויג סבור שהגם שהסעיף אינו מאפשר חיפוש מתמשך, נראה כי "בקשה לצו חיפוש בחומר מחשב מרחוק באמצעות כלי רוג'לה, גם אם אפשרית מבחינה טכנית ולפי לשון החוק, חייבת להיות תחומה למועד גישה מסוים, לסוגי מידע מסוימים, לשימושים הטכנולוגיים המתאפשרים במסגרת החיפוש ולאופן שבו ניתן להבטיח את פרטיותו של הנחקר ביחס למידע שאינו קשור לחקירה."<sup>44</sup>

יוער כי במסגרת הדיון המשפטי-טכנולוגי בהיקף פרישתו של סעיף 23א לפסד"פ חיפוש ומעצר לא נבחנה השאלה של גישה אקטיבית לחומר מחשב בענן תוך שימוש בסיסמאות שמקורן בהעתקת חומר מחשב ממכשירי טלפון נייד.<sup>45</sup>

להבדיל מחוק האזנות סתר, בהסדר זה אין חובת דיווח ליועמ"ש או לועדת חוק חוקה ומשפט, בדומה להסדר שבס' 6 לחוק האזנת סתר.

#### 2.4 אינטראקציה עם פלטפורמות וספקים: השגת נתוני תוכן at rest

<sup>40</sup> ס' 4 לחוק המחשבים, תשנ"ה-1995, ס"ח 1534 בעמ' 366 (להלן: **חוק המחשבים**)

<sup>41</sup> פקודת סדר הדין הפלילי (חיפוש ומעצר) [נוסח חדש], תשכ"ט-1969 (להלן: **פסד"פ חיפוש ומעצר**)

<sup>42</sup> דנ"פ 1062/21 אוריך נ' מדינת ישראל (11.1.2022)

<sup>43</sup> לביקורת, ר' מיכאל בירנהק, "[מאורך לפגסוס: על פרטיות חוקתית בחקירות משטרה](https://www.idi.org.il/articles/38112)", **ICON-S-II Blog**, (23.1.2022); עמיר כהנא, "פרשת הטלפונים ויועצי רה"מ לשעבר: עלות, יעילות ופרטיות בחקירה פלילית" **המכון הישראלי לדמוקרטיה** (17.1.2022) <https://www.idi.org.il/articles/38112>

<sup>44</sup> עמרי רחום טוויג, "חיפוש ממוחשבים – על סמכויות חקירה בגישה מרחוק למחשבים ומידע דיגיטלי" **תגובות משפט** (31.1.2022) <https://www.taulawreview.sites.tau.ac.il/post/raham-twaig>

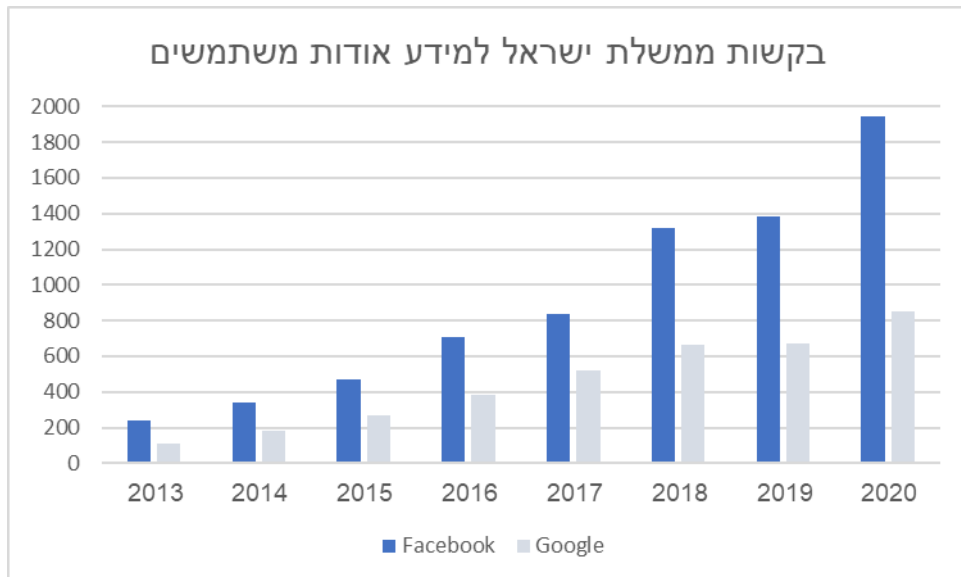
<sup>45</sup> אם כי נראה מהערת אגב של גביראלה פיסמן, ראש אשכול סמכויות שלטוניות במשרד המשפטים, כי בהינתן צו חיפוש במכשיר, לפי פרשנות משרד המשפטים, ניתן לחפש גם בחומרים בענן שנגישים דרכו. "ברגע שיש חיפוש פיזי אז גם אפשרי חיפוש שהוא מעבר למכשיר הקצה." "....יש לך כרגע את המכשיר שלי ביד, כשאת לוחצת על תמונה את לא יכולה לדעת אם היא נמצאת אצלי במחשב או רק בענן." פרוטוקול מס' 194 משיבת ועדת חוק, חוקה ומשפט של הכנסת ה-24, 12-13 (1.2.2022)



נראה כי התפתחה פרקטיקה לפיה מכוח ס' 43 לפסד"פ חיפוש ומעצר, לפיו "ראה שופט שהצגת חפץ נחוצה או רצויה לצרכי חקירה או משפט, רשאי הוא להזמין כל אדם, שלפי ההנחה החפץ נמצא בהחזקתו או ברשותו, להתייצב ולהציג את החפץ, או להמציאו, בשעה ובמקום הנקובים בהזמנה," מוגשים צווים שיפוטיים לחברות טכנולוגיות שמאחסנות מידע ולבקש ממנה את התכנים.<sup>46</sup>

השימוש בס' 43 על מנת להשיג נתוני תוכן רגישים ללא בקרות מקבילות לאלו המצויות בחוק האזנת סתר, במעמד צד אחד, וללא דיווח שקוף לועדה פרלמנטרית מפקחת, היועץ הממשלתי לממשלה והציבור, טעון בירור יסודי ובחינה מחדש.

ואולם, דוחות השקיפות של ספקי שירותי אחסון בענן ופלטפורמות בינלאומיים, מלמדים כי ממשלת ישראל מבקשת מספר הולך וגדל של נתונים מחברות אלו (ר' תרשים מטה). אין אנו יודעים אם בקשות אלו כוללות בקשות למידע על מכוח ס' 43 לפסד"פ או בהסתמך על בסיס סטטוטורי אחר, ואילו רשויות הן המבקשות אותן. ואולם יש בכך כדי להעיד על חור שחור הקורא לאסדרה.<sup>47</sup>



מקור: דוחות השקיפות של חברות גוגל ומטא.<sup>48</sup>

## 2.5 פטור לרשויות ביטחון

<sup>46</sup> פרוטוקול מס' 194 מישיבת ועדת חוק, חוקה ומשפט של הכנסת ה-24, 13-17 (1.2.2022).

<sup>47</sup> ר' לדוגמא כהנא ושני, בה"ש 16 לעיל בעמ' 279-277.

<sup>48</sup> עבור חב' מטא ר' <https://transparency.fb.com/data/government-data-requests>; עבור חב' גוגל ר' <https://transparencyreport.google.com/user-data/overview?hl=en>. יצוין כי לחברת אמזון אין נתונים אודות ישראל. חברת אפל מדווחת על מספר בקשות נמוך מדי שנה (למטה מ-10).



3 המצב החוקי הקיים מול שימוש ברוגלה כגון "פגסוס"

מכרזות רוגלה מופעלות מרחוק ושואבות את כלל המידע מהמכשיר	פס"פ מעצר וחיפוש (תיקון 1995) - נתפס ככניסה לחצרים/הסגת גבול	חוק האזנת סתר (תיקון 1995)	
	כמו חיפוש. על-ידי בעל תפקיד המיומן לביצוע פעולות כאלה.	מניעת עבירות מסוג פשע (סעיפים 6-7)	תכלית ביצוע
פגסוס מאפשרת גם חיפוש בקיים וגם האזנה להבא לכן יש בעיה להפעיל פגסוס רק על סמך צו מסוג אחד. פגסוס היא ההיפך מחיפוש ממוקד.	חומר קיים. אין לתת צו מתמשך לחיפוש עתידי (פס"ד פילוסוף). החיפוש הוא נקודתי ובידיעת החשוד ומתבצע בחשוד וחפציו ואינו משליך לרוב על צדדים שלישיים. (פס"ד פילוסוף).	מכאן ולהבא. תחום וממוקד.	חומר קיים או רק מכאן ולהבא
פגסוס בנויה על גישה מרחוק ולכן צו האזנה בטוח מספיק, שאלה לגבי צו חיפוש.	לא ברור	כן	האם מאפשר גישה מרחוק
פתיח ליצירת "פורום שופינג" - לא ברור ממי יושג צו וכן האם שופט מחוזי יודע על צו של שופט שלום ולהיפך.	כל בית משפט (כלומר, בימ"ש שלום)	קצין משטרה מוסמך לנשיא/ס. נשיא בימ"ש מחוזי בבקשה להיתר	הליך אישור
שימוש בפגסוס לצרכי דייג אינו נכלל באף אחד מן החוקים. איסוף כל השיחות, כולל ביישומים, מעורר חשש שלא מדובר בחיפוש ממוקד. איסוף כל המידע על המכשיר מעורר חשש שלא ניתן לומר מהן מטרות החיפוש.	האם ההיתר הוא לחדור לחומר מחשב או להפיק פלט מהן מטרות החיפוש.	זהות האדם או הקו לו מתבקש ההיתר להאזין אופי השיחות שנדרש להאזין להן משך ההאזנה דרכי ההאזנה	מה נדרש לפרט בבקשה ומה צריך לכלול ההיתר?
קשה לומר ששימוש בפגסוס עולה בקנה אחד עם תנאים לשמירה על פרטיות.	יש לקבוע ולפרט תנאים כדי שלא תיפגע פרטיותו של אדם מעבר לנדרש.	על השופט להשתכנע שההאזנה נדרשת לגילוי, חקירה או מניעה של עבירות	מסגרת השיקולים

<sup>49</sup> ס' 9 לחוק הגנת הפרטיות, התשמ"א-1981, ס"ח 1011, 128



## המכון הישראלי

### לדמוקרטיה

		מסוג פשע. יש לשקול את מידת הפגיעה בפרטיות.	
לא ידוע מהחלק הגלוי בדו"ח מררי אם נעשה שימוש בחריג ביחס לפגסוס.	אין	מפכ"ל המשטרה מוסמך להורות על ביצוע האזנת סתר במקרים דחופים ללא צו שיפוטי, מקסימום ל - 48 שעות.	<b>חריגים</b>
בדו"חות אין פירוט מה מתוך ההאזנות נעשה באמצעות רוגלה.	אין	יש, אחת לשנה	<b>חובת דיווח לכנסת?</b>
	94% נזכיר שהצווים אינם ניתנים לערעור (דנ"פ אוריך)	92%	<b>נתונים אחרונים לגבי אחוזי היענות לבקשות</b>
הואיל ומדובר ברוגלה סמויה, אם חקירה לא מבשילה לאישום, לא ניתן יהיה לדעת על השימוש בכלי או לבקש למחוק את המידע שנאסף.	אין (ייתכן שמפני שהתפיסה היתה שבשביל חיפוש במחשב צריך לבקש אותו מבעליו).	אין	<b>חובת יידוע של הנחקר</b>
אם המשטרה מתקינה פגסוס על בסיס צו האזנת סתר, הראיות שהושגו ייבחנו רק בשלב המשפט עצמו, אם יהיה כזה. (דנ"פ אוריך). זהו תמריץ שלילי.	אין כלל פסלות ראיות. לערכאה הדיונית במסגרת ההליך הפלילי עצמו יהיה שיקול דעת האם לתת משקל מופחת לראיות שהושגו בחקירות פסולות (דנ"פ אוריך).	כן. למעט במקרים של עבירות פשע חמור ומטעמים שיירשמו.	<b>האם קיים כלל פסלות ראיות?</b>

#### 4 סוגיות שאינן מוסדרות בדן הקיים

כאמור, המסגרת המשפטית הנוגעת למעקבים דיגיטליים אינה משקפת את ההתפתחויות הטכנולוגיות בנות זמננו. להלן תיאור של מספר סוגיות שאינן מוסדרות בדן הישראלי, שיש לשקול להתייחס אליהן במסגרת חוק מעקבים דיגיטלי.

##### 4.1 רוגלות

גם אם השימוש ברוגלות יהיה מנוון (ולא צופה פני עבר), וגם אם הוא נועד להתגבר על אתגרים ביישום חוק האזנת סתר בסביבה בה המשתמשים נוטשים בהדרגה את התווך הטכנולוגי של בעלי רישיון בזק ועוברים לתקשורת המבוססת על תווך טכנולוגי של פלטפורמות (כגון תוכנות



מסרים, VoIP, שיחות וידאו), יש לאסדר אותו בנפרד, תוך צמצום היקף העבירות שבגינן תוכל המשטרה לבקש צו סייבר.<sup>50</sup>

#### 4.2 אסדרת אוסינט

אוסיןט (Open Source Intelligence, OSINT), או מודיעין גלוי, היא דיסציפלינה מודיענית ותיקה, המתבססת על מידע בלתי מסווג שאותר במכוון, סונן, זוקק והופץ לצרכנים ספציפיים על מנת לענות על שאלה מסוימת. ידיעות אוסינטיות יכולות 'להלבין' ידיעות שהושגו באמצעים מסווגים או על-ידי מקורות חשאיים מסווג מבלי ל'שרוף' אותם. אוסינט מאפשר גם הקצאה יעילה יותר של משאבי האיסוף המודיעיניים, באמצעות ניצול מידע נגיש שלא נדרש להפעיל מאמצים מיוחדים כדי להשיגו.<sup>51</sup>

בשנים האחרונות נראה כי גופים ממשלתיים שונים בישראל מגלים עניין רב במודיעין גלוי המבוסס על מקורות מקוונים ועל ניטור רשתות חברתיות בפרט (SOCMINT),<sup>52</sup> לתכליות מגוונות, ובכלל זה משטרת ישראל.<sup>53</sup> ואולם, לצד התועלת המגוונת הרבה שבאיסוף אוסינטי – בין אם במסגרת חקירה ממוקדת או במסגרת איסוף גורף לצרכי חיזוי וסיכול איומים, יש לתת לדעת גם על הפגיעות הפוטנציאליות שלו בזכויות אדם, ובכלל זה הזכות לפרטיות וחופש הביטוי.<sup>54</sup> נוכח

---

<sup>50</sup> חוק סמכויות חקירה הבריטי, למשל, כולל פרק העוסק בצווים 'להתערבות בצידוד' (שימוש באמצעי סייבר) כדי להשיג מידע. צו התערבות בצידוד יינתן לתכליות מניעה או גילוי של פשע חמור. הצו ניתן מאת ראש רשות אכיפת חוק (כגון מפכ"ל משטרה) ובאישור נציב שיפוטי מנציבות סמכויות החקירה. במקרים דחופים ניתן לאשר את הצו ללא אישור נציב שיפוטי, ובתנאי שהוא יאושר בדיעבד תוך שלושה ימי עבודה. ר' כהנא ושני, בה"ש 16 לעיל, בעמ' 156-162. קוד סדר הדין הפלילי הגרמני מתיר שימוש ב'אמצעים טכניים' לתכליות של 'חיפוש חשאי מרחוק במערכות מידע' (ס' 100b), בחקירות פשע חמור במיוחד (רשימה סגורה המוגדרת בסעיף). אמצעים טכניים אלו יופעלו ככלל רק כנגד החשוד. ניתן להתערב בצידוד מחשב של אחרים רק כשיש בסיס עובדתי המאפשר להניח כי החשוד עושה שימוש בצידוד מחשב של אותם אחרים ושההתערבות בצידוד של החשוד לבדו לא יוביל לבירור עובדתי. ר' כהנא ושני, בה"ש 16 לעיל, בעמ' 201. הוראות דומות מצויות גם בחוק המשטרה הפדראלית (ס' 49), המתיר שימוש באמצעים טכניים אלו רק כאשר נשקפת סכנה לחיי אדם, לגופו או לחירותו, או לטובין ציבוריים שנשקף להם איום המשפיע על יסודות הקיום של הממשלה, המדינה או המין האנושי, ובכפוף לצו בית משפט לבקשת ראש המשטרה הפדראלית.

<sup>51</sup> Robert David Steele, *Open Source Intelligence* in HANDBOOK OF INTELLIGENCE STUDIES 129-147 (Loch K. Johnson, Ed., 2006); אפרים לפיד, "אתגרי המודיעין הגלוי בעידן המידע" **אתגרי קהילת המודיעין בישראל** 123 (2017).

<sup>52</sup> David Omand, *Social Media Intelligence (SOCMINT)* in THE PALGRAVE HANDBOOK OF SECURITY, RISK AND INTELLIGENCE 355-371 (Robert Dover, Huw Dylan and Michael S. Goodman, Eds., 2017)

<sup>53</sup> יהושוע (ג'וש) בריינר, " המשטרה רוצה לרכוש מערכת לאיסוף מודיעין על גולשים ב-40 מיליון שקל - ללא מכרז" **הארץ** (7.6.2019)

<sup>54</sup> ר' לדוגמא Alison Lyle, *Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism Data* in OPEN SOURCE INTELLIGENCE INVESTIGATION - FROM STRATEGY TO IMPLEMENTATION 277-294 281 (AKHGAR, BAYERL AND SAMPSON, Eds., 2016)





העניין הגובר של רשויות בישראל בכלים אוסינטיים עולה בצורך באסדרה פרטנית – שאינה קיימת<sup>55</sup> - של המותר והאסור במסגרת מתודולוגיה מודיעינית זו.<sup>56</sup>

### 4.3 היתוך מידע ובינה מלאכותית

ברחבי העולם מצטיידות רשויות אכיפת החוק בכלים נבונים לניתוח מידע. את הדימוי של המפה העירונית המעטרת את קירות תחנות המשטרה ועליה מסומנים אזורי הפשיעה בחוטים וסיכות, החליפו זה מכבר מערכות מידע גאוגרפי (GIS), המעבדות נתוני פשיעה ממוכנים ומשרטטות על מסך המחשב "נקודות חמות" (hot spots) או "אזורים עתירי פשיעה" (high crime areas).<sup>57</sup>

גישה נוספת לחיזוי פשיעה הוא באמצעות מערכת דירוג חברתי (social scoring).<sup>58</sup> אין הכוונה בהכרח למערכת דרוקנית דוגמת זו המצויה בשימוש בסין, לה מטרות אחרות,<sup>59</sup> אך העקרון המנחה הוא זהה: ההנחה שהרשת החברתית של אדם – מכריו, חבריו, משפחתו – משמשת אינדיקציה לרמת העבריינות הפוטנציאלית שלו. כאן מודל השיטור הוא אינו ביצוע פטרולים הרתעתיים באזורים מועדי פשיעה, אלא זיהוי ישיר של חשודים סטטסטיים. גישה זו עודנה בחיתוליה מבחינת יישום נרחב, אך ברחבי ארצות הברית ניתן לראות ניצנים של פרויקטים בתחום.<sup>60</sup>

מערכות חיזוי פשיעה המבוססות על מתודולוגיות אלו עשויות בין השאר להתבסס על נתונים שמקורם באיסוף סיגנטי, בצירוף היסטוריה הפלילית המתועדת במערכות המשטרה. היתוך מידע

---

<sup>55</sup> ר' למשל כהנא ושני, בה"ש 16 לעיל, בעמ' 277; מפקדה לשעבר של יחידת האסינטי חצ"ב מצוין כי "מדובר בתחום בו ההסדרה החוקית נמצאת בחיתוליה. במצב כזה מתעוררות סוגיות חוקיות ואתיות, כגון יצירת דמויות פיקטיביות ('אווטארים') והפרה של תנאי השימוש ברשתות החברתיות לצורכי איסוף מודיעין. יש לציין, עם זאת, כי לא כל מה שמותר לגוף מודיעין רשמי לעשות מתוקף סמכותו החוקית, מותר לחברה אזרחית או מסחרית". סא"ל ר' "אתגרים במיצוי מודיעין מהמדיה החברתית" **אתגרי קהילת המודיעין בישראל** 129, 135 (שמואל אבן ודוד סימן טוב עורכים, 2017).

<sup>56</sup> ר' למשל (24.4.2012) DEMOS #Intelligence, Omand, David <https://demos.co.uk/project/intelligence>

<sup>57</sup> על טכנולוגיות מיפוי קרימינולוגיות, ר' Andrew Guthrie Ferguson, *Crime Mapping and the Fourth Amendment - Redrawing "High-Crime Areas"*, 63 HASTINGS L. J. 179 (2011). כן ר' Andrew G. Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109 (2017).

<sup>58</sup> ר' Ferguson (2017), שם, בעמ' 1137.

<sup>59</sup> ר' כהנא ושני, בה"ש 16 לעיל, בעמ' 22; רשות הגנת הפרטיות, דירוג חברתי בראי הזכות לפרטיות: סקירת רקע בעניין שימוש במערכות לדירוג חברתי (21.4.2020). בס' 5(1)(c) להצעת תקנות הבינה המלאכותית באירופה, בה"ש **שגיא! הסימניה אינה מוגדרת**. לעיל, מוצע לאסור שימוש במערכות דירוג חברתי שעשויות להביא לתוצאות שליליות בהקשרים אחרים מאלו שלשמן נאסף המידע או ליחס בלתי צודק או שלילי לאנשים פרטיים או לקבוצות באופן שאינו הולם את התנהגותם החברתית או את חומרתה. על מדינת המעקב הסינית, ר' GEOFFREY CAIN, *THE PERFECT POLICE STATE: AN UNDERCOVER ODYSSEY INTO CHINA'S TERRIFYING SURVEILLANCE DYSTOPIA OF THE FUTURE* (2021).

<sup>60</sup> לסקירה ר' Ferguson (2017), בה"ש 57 לעיל בעמ' 1138-1143.



זה, ללא בקרה ועקרונות ממשל נתונים (data governance), עשוי להביא להפעלת סמכויות שיטור באופן מוטא, מפלה, ולא אפקטיבי.<sup>61</sup>

אשר על כן יש לשקול להתייחס במסגרת חוק מעקבים דיגיטליים גם להיבטים של החלטות אוטומטיות המבוססות על עיבוד מידע ממקורות סיגינטיים.

#### 4.4 התמודדות עם טכנולוגיות חדשות

בארצות הברית ישנה מגמה של הגברת הפיקוח הקהילתי על שימוש ורכישה של טכנולוגיות מעקב חדשות על ידי המשטרה המקומית. ב-15 גופי ממשל מקומי בארצות הברית, לרבות בערים כגון סן פרנסיסקו וניו יורק, ישנה כעת חקיקה המגבילה את השימוש בטכנולוגיות מעקב חדשות על ידי המשטרה המקומית. ברוב המקרים, רכש של טכנולוגיות מעקב חדשות כפוף לאישור המועצה המקומית. לפני אימוץ של טכנולוגיות כאלו, על המשטרה לדווח על היכולות של האמצעים בהם היא מבקשת לעשות שימוש, על אופן השימוש, ועל ההשפעה הפוטנציאלית שלהן על אזרחים. על פי רוב, ישנן הוראות של דיווח שנתי ופומבי על השימוש באמצעים אלו.<sup>62</sup>

נוכח תופעות במסגרתן גופי החקירה בישראל מאמצים טכנולוגיות מעקב חדשות כאשר המסגרת המשפטית המסמיכה את השימוש בהן מתגלה בדיעבד כשנויה במחלוקת,<sup>63</sup> רצוי יהיה להציג הסדרי פיקוח סטטוטוריים על אימוצן. הסדרי הפיקוח המקומיים בגופי הממשל המקומי בארצות הברית שמים דגש על יידוע הקהילה הנעקבת על אמצעי המעקב החדשים, ועל היבטים של שיתוף הציבור, וזכו בהתאמה לביקורת על העדר שיניים וחוסר אפקטיביות.<sup>64</sup> ואולם ביקורת זו מתייחסת בעיקר למעמדם של גופים קהילתיים מייצגים במסגרת הליכי אישור הכנסת

---

<sup>61</sup> כך למשל, ייצוג יתר של אוכלוסייה עשוי לשקף הטייה. ייצוג יתר זה בבסיס נתונים מסויים עשוי כשלעצמו לשקף הטייה מבנית או הפלייה היסטורית. כך למשל, נתוני העבריינות בארצות הברית, העשויים לגלם הטיות מערכתיות של מערכת האכיפה נגד אפרו-אמריקאים (בדיווח ואכיפה מוגברים של עבירות בקרב שחורים, לדוגמא), עלולים גם – בשל ייצוג יתר של אוכלוסייות מיעוטים בתוכם – להביא להטיות במודלים המפותחים על בסיסם ומשמשים במערכות של חיזוי פשיעה, הערכת סיכון ורצידיביזם. בהקשר זה ר' Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CA. L. REV. 687 (2016).

<sup>62</sup> Stevie Degroff and Albert Fox Cahn, *New CCOPS On the Beat: an Early Assessment of Community Control of Police Surveillance Laws*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (10.2.2021) <https://www.stopspying.org/ccops>

<sup>63</sup> נוסף על פרשת הרוגלות (ר' גנון בה"ש 15 לעיל), ר' גם את פרשת מערכת 'עין הנץ' לזיהוי לוחיות רישוי, שדבר קיומה נחשף בעיתונות לאחר שמונה שנים בהם היתה פעילה. ר' דניאל דולב, "המשטרה מחזיקה מאגר מידע סודי על תנועות אזרחים", וואלה!, <https://news.walla.co.il/item/3355178> (6.5.2020). בעת כתיבת שורות אלו, עתירה נגד המערכת תלויה ועומדת בבית המשפט העליון, ובמסגרתה ניתן צו על תנאי המורה למשטרה לנמק מדוע לעמדתה היא רשאית להמשיך ולהפעיל את המערכת ללא הסמכה מפורשת בחקיקה בג"ץ 641/21 האגודה לזכויות אזרח נ' משטרת ישראל (11.1.2022)

<sup>64</sup> ר' Vincent M. Southerland, *The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies*, 70 UCLA L. REV. (Forthcoming, 2023) (עותק מצוי בדינו)



טכנולוגיות חדשות לגופי שיטור מוניציפליים, ולא לאפקטיביות הפיקוח הפרלמנטרי (שלו ניתן לתת שיניים סטטוטוריות) על המשטרה ברמה הלאומית.

אנו מציעים כי רכש של טכנולוגיות מעקב חדשות יותר באישור ועדת חוק חוקה ומשפט של הכנסת, בכפוף בין השאר למתן פומבי לנהלי ההפעלה שלהן, בפירוט הסמכות המשפטית לשימוש בהן ובנהלי ההפעלה העתידיים שלהן, כמו גם בסקר סיכונים מקדים.

#### 4.5 זכות יידוע לנעקבים

לחובת ההודעה למושא המידע – או הזכות של מושא המידע להיות מידוע – חשיבות רבה, מאחר שבלעדיה קשה לממש עקרונות יסוד בדיני הגנת הפרטיות, ובתוכם היכולת לתת הסכמה מדעת לעיבוד המידע, ולהבטיח שעקרון צמידות המטרה (לפיו מידע שנאסף למטרה מסוימת לא יכול לשמש למטרה אחרת)<sup>65</sup> נשמר.<sup>66</sup>

אמנם, מטיבו וטבעו מעקב חשאי דורש שיהיה ללא הסכמה, אך חובת ההודעה מהווה תמריץ לרשויות החקירה להקפיד שבעתים על הדיון, מאחר שכך עשויים להתגלות בדיעבד מקרים בהם נעשה שימוש באמצעי מעקב שלא לתכליות הסטטוטוריות המצדיקות את השימוש בהן. למשל, רבים מפעילי מחאת 'הדגלים השחורים' קראו לפרסם את שמותיהם של אלו מתוכם אחריהם עקבה המשטרה, לפי הנטען בתחקיר 'כלכליסט', באמצעות הרוגלה של חברת NSO, בשעה שכפי הנראה אין לכך כל בסיס משפטי.<sup>67</sup> מדובר בבקרה על שימוש בסמכות שלא כדין (כמדיניות, או כ'קיצור דרך' של שוטרים להוטים יתר על המידה להגיע לתוצאות) וגם מניצול לרעה של סמכויות (כאשר שוטר בודד משתמש באמצעי מעקב על מנת להשיג שלא כדין מידע למטרותיו האישיות).<sup>68</sup>

החלת חובת יידוע על גופי אכיפת החוק בישראל,<sup>69</sup> לפיה אלו ידווח למושאי המעקב שלהם עם סיומו או במועד הקרוב ביותר לסיומו שאינו מסכל את החקירה, מסכן חיי אדם או את שלמות הגוף, תשמש בקרה נוספת על פעילותם במטרה להבטיח שזו תהיה כדין. כדי שחובת יידוע זו תהיה אפקטיבית יש להשלימה בהעמדת סעדים למושאי המעקב בגין פגיעה בזכויות,<sup>70</sup> ובהצבת

---

<sup>65</sup> ר' ס' 2 (9) לחוק הגנת הפרטיות; רחל ארידור-הרשקוביץ ותהילה שוורץ-אלטשולר, [הצעת חוק הגנת הפרטיות התשע"ט-2019](#); 51-52; Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Art. 5(1), 6(4), 2016 O.J. (L 119) 1 (EU).

<sup>66</sup> ר' מיכאל בירנהק, [מרחב פרטי: הזכות לפרטיות בין משפט וטכנולוגיה](#) 230-232 (2011)

<sup>67</sup> ניצן שפירא, "מובילי מחאת בלפור נגד המשטרה: הפכה בתקופת אוחנה-נתניהו לגוף שרודף אזרחים" **N12** (18.1.2022)

<sup>68</sup> ר' עמיר כהנא ויובל שני, [פיקוח על מעקב מקוון בישראל](#) 31 (המכון הישראלי לדמוקרטיה, 2020) <https://www.idi.org.il/books/32264>. כן ר' להלן בה"ש 79-81.

<sup>69</sup> ר' גם עמיר כהנא, "לא רק אבק על מיטה: על זכות היידוע של נחקרים" **ICON-S-IL Blog** (30.1.2022)

<sup>70</sup> נוכח הוראות הפטור ס' 19 לחוק הגנת הפרטיות, ספק אם ניתן לתבוע מרשויות ביטחון סעד של פיצויים בגין פגיעה בפרטיות.



גוף המפקח על יישום חובה זו.<sup>71</sup> כך למשל ניתן להתנות צווים המתירים איסוף סיגינטי בציון המועדים הצפויים ליידוע הנעקבים, ובהארכתם בכפוף לאישור בית המשפט.

## 5 חוק מעקבים דיגיטליים – קווים לדמותו

נוכח רשימת הסוגיות שבחלק 3 לעיל, אין חולק שיש צורך ברפורמה מקיפה בדיני המעקב המקוון בישראל.<sup>72</sup> בחלק זה נבקש לתאר את עיצובו הרצוי של חוק מעקבים דיגיטלי, ומספר נושאים נוספים שאת אופן הסדרתם יש לשפר במסגרת רפורמה.

### 5.1 הרמוניזציה של חקיקה ויצירת מדרג נורמטיבי

כפי שעולה מהסקירה בחלק 0 לעיל, כיום מעקבים מקוונים יכולים להתבצע במדינת ישראל מכוח שלושה חוקים: חוק האזנות סתר, חוק נתוני תקשורת, ופסד"פ מעצר וחיפוש. אבל, לאמיתו של דבר אף אחד מהחוקים האלה בפני עצמו לא יכול להספיק בשביל שימושים בתוכנה כמו פגסוס, משום שכל אחד מהם נוגע להיבט אחר של איסוף (שיחות טלפון מכאן ולהבא; "מטא דאטה" ונתוני מיקום; חומר שנמצא בתוך מחשב וטלפון חכם).

הואיל ומדובר בשלושה חוקים שונים גם ההסדר המוסדי ביחס לכל אחד מהם הוא שונה, וגם היסטורית כל אחד מהם נחקק בתקופה טכנולוגית שונה. לכן, גם אם היינו מפרשים את המצב המשפטי ככזה שמאפשר שימוש בפגסוס, הרי שלמעשה צריך להוציא צו האזנת סתר, על ידי שופט מחוזי, ובנוסף צו חיפוש בחומר מחשב – על ידי שופט שלום. אולם, המצב שלפיו די בשופט שלום כדי לחטט במחשב אבל על מנת להאזין יש צורך בסגן נשיא מחוזי, יוצר אי הלימה בין סוגי העבירות שבעטיין אפשר להוציא צו כזה או אחר – ומוביל לאנומליות ברמה הנורמטיבית. מעבר לזה, הוא פתח ל"פורום פייסינג" – לא תמיד מספרים לכל שופט אילו בקשות הועברו למקבילו בבס השיפוט, וכל זאת בנוסף להבנה המועטה של שופטים בטכנולוגיה ולאדישות של מערכת המשפט שאנו מכירים לצערנו במקרים של צווים במעמד צד אחד.

ריכוז כלל סמכויות המעקב המקוון תחת דבר חקיקה אחד יקל על הרמוניזציה שלהן, ועל יצירת מדרג נורמטיבי במסגרתו יוחלו בקרות סטטוטוריות נוקשות יותר על סמכויות שפגיעתן פולשנית יותר, דוגמת הגבלת חומרת העבירות שבגינן מותר לעשות שימוש בסמכויות אלו, או התאמת הערכאה המאשרת לסוג הצו המבוקש.

### 5.2 חיזוק הפיקוח השיפוטי

הגם שלהבדיל ממעקבים מקוונים לתכליות של ביטחון לאומי, הפעלת סמכויות לאיסוף סיגינט לתכליות טעונות על פי רוב בצו שיפוטי, יש לשקול לחזק סמכויות אלו.

<sup>71</sup> הכוונה לפיקוח שוטף שמטרתו לוודא כי אכן כל עם תום מעקב מקוון, היעדים המודיעניים שלו מיועדים (בכפוף לסייגים). בעת כתיבת שורות אלו, לא ברורה מידת הכשל בפיקוח שמפעיל משרד המשפטים על אמצעי הסיגינט המשטרתיים בפרשת השימוש המשטרתי ברוגלות. אפשר שגם ביחס לחובת היידוע, הגורם המפקח היעיל ביותר הוא נציבות סיגינט עצמאית (ר' כהנא ושני, בה"ש 68 לעיל, בעמ' 248-258).

<sup>72</sup> ור' בעניין זה כהנא ושני, בה"ש 16 לעיל; כהנא ושני, בה"ש 68 לעיל.



ראשית, רצוי לחזק את הסמכות העניינית ביחס לצווי חיפוש בחומר מחשב ובבקשות להשגת תוכן מפלטפורמות. ניתן לעשות זאת הן באמצעות דרישה לאישור מאת שופט בית משפט המחוזי (או נשיא בית משפט השלום וסגנו שהוסמך לכך) תחת אישור מאת כל שופט בית משפט השלום. נוסף על כך, ניתן לשקול שבקשה להארכת תוקפם של צוים אלו, וכן צוים להשגת נתוני תקשורת (או בקשות חוזרות לעיון בחומר או השגת מידע כאמור) יינתנו על ידי ערכאה בכירה יותר מזו שנתנה את הצו המקורי.

שנית, יש לחזק את המומחיות הטכנולוגית של שופטים הדנים בצווי מעקב מקוון.<sup>73</sup> זאת אפשר לעשות באמצעות הכשרה משלימה,<sup>74</sup> או הוספת תקנים למומחים מקצועיים.<sup>75</sup> דרך נוספת לפיתוח מומחית מקצועית היא קיום דיאלוג פתוח עם האקדמיה וארגוני החברה האזרחית – אשר יכולים להעשיר את השיח.<sup>76</sup>

שלישית, מאחר שלפי טבעם וטיבם, הליכים אלו נעשים במעמד צד אחד, יש לשקול הקמת מוסד 'ידידי בית משפט' בדומה לדגם הקיים בבית הדין האמריקאי למודיעין זר (FISC). תחת חוק איסוף מודיעין זר (FISA), על ערכאה זו למנות חמישה ידידי בית משפט שאליהם יהיה אפשר לפנות כאשר במסגרת החלטה או צו שבית המשפט נדרש לתת מתעוררת שאלה משמעותית או חדשנית שבדין. על ידידי בית המשפט להביא בפני בית המשפט טיעונים משפטיים לקידום הגנת הפרטיות וזכויות אזרח, מידע הנוגע לאיסוף מודיעין או לטכנולוגיות מידע או כל טיעון משפטי אחר הנוגע לעניינים רלוונטיים למקרה הנידון.<sup>77</sup> הסדר חלש יותר, המגן על אינטרסים של גופים במשק שעשויים להיות מושפעים מהפעלת סמכויות חקירה, קיים בדין הבריטי.<sup>78</sup>

ידיד בית משפט אפקטיבי, אליו בית המשפט יהיה מחויב לפנות בבסיבות של בקשה לצוים לשימוש בטכנולוגיות חדשות, או במקרים בהם מתעוררת שאלה פרשנית מיוחדת, עשוי לבלום או למתן את אימוצן.

---

<sup>73</sup> על העדר מומחיות טכנית של שופטים, ר' כהנא ושני, בה"ש 68 לעיל, בעמ' 87-88.

<sup>74</sup> ר' לדוג' European Commission For Democracy Through Law, *Report On The Democratic Oversight Of The Security Services*, para. 30, 34 (2015).

<sup>75</sup> אנדרסן ממליץ שגוף הפיקוח יסתייע במומחים משפטיים חיצוניים, ר' DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW, Para 14.99 (2015); להמלצה על הסמכת גופי פיקוח חיצוניים, לרבות ועדות פרלמנטריות, לשכור לפי הצורך את שירותיהם של מומחים חיצוניים (בייחוד בנושאים טכנולוגיים) ראו Council of Europe Commissioner for Human Rights, *Democratic and Effective Oversight of National Security Services* 14(2015).

<sup>76</sup> ראו לדוגמה ANDERSON, שם, שם; EU Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU vol. II*, 11 (2017); Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report* 2016 (2017).

<sup>77</sup> ר' כהנא ושני, בה"ש 68 לעיל, בעמ' 153-155. Chad Squitieri, *The Limits of the FREEDOM Act's Amicus Curiae*, 11 WASH. J. L. TECH. & ARTS 197, 210 (2015); Ben Cook, *The New FISA Court Amicus Should Be Able to Ignore its Congressionally Imposed Duty*, 66 AM. U. L. REV. 539 (2017).

<sup>78</sup> ר' כהנא ושני, בה"ש 68 לעיל. בעמ' 131-132.



### 5.3 הסדרה קונקרטי של חיפוש במכשיר טלפון והשגת מידע מפלטפורמות

אנו סבורים שחוק מעקבים דיגיטליים לכלול הסדר קונקרטי לחיפוש במכשירי טלפון חכם, המתייחס לתוצאה של דנ"פ אורח, ובכלל זה מציג כלל פסלות ראיות נוקשה יותר. השגת מידע מפלטפורמות נדרשת להעשות על בסיס סמכות מפורשת בחוק ובפיקוח של ערכאה גבוהה יותר מבית משפט מחוזי, תוך הקפדה על שיקולי פרטיות.

### 5.4 התמודדות עם שימוש במאגרי מידע פנימיים

הגישה הבלתי מורשית למאגרי מידע משטרתיים היא תופעה מוכרת במשטרת ישראל מזה כעשור.<sup>79</sup> מסקירה שערכנו עולה שכמעט בכל קבצי ההחלטות של בית הדין למשמעת של המשטרה מחמש השנים האחרונות ישנם תיקים העוסקים בגישה בלתי מורשית של שוטרים למערכות המידע המשטרתיות ובשאלות שלא כדין למאגרי מידע משטרתיים.<sup>80</sup> למרבה הצער, הענישה על עבירות חמורות אלה היא מבישה ולעתים מזומנות סופה בעסקת טיעון, הורדה בדרגה לתקופה קצובה בלבד, נזיפות וקנסות ולא מעבר לכך, ובהתחשבות יתר בנסיבות האישיות של השוטרים ולא בחומרת המעשה

יתר על כן, ברור כי תיקים משמעתיים אלו אינם ממצים את כלל המקרים של גישה שלא ברשות למאגרי מידע במשטרה וככל הנראה מדובר בתופעה נרחבת יותר. הוכחה לכך נמצאת במכתב אגף משאבי האנוש של משטרת ישראל לשוטרים לפיו "כל שוטר שיימצא כי ביצע בדיקות במערכות ומאגרי המידע המשטרתיים שלא לצורך תפקידו המשטרת **מכל סיבה שהיא**, החל מיום 1.8.2021 – יועמד לדין בבית הדין למשמעת".<sup>81</sup>

חוק מעקבים דיגיטליים יידרש לכלול בתוכו הוראות ביחס לענישה של בעלי תפקידים שעשו שימוש במאגרי מידע פנימיים שלא כדין, כמו גם הנחיות באשר לתיעוד הפעילות במערכות מידע ומעקב מקוון על מנת שיתאפשר לזהות שימוש חריג בסמכויות.

### 5.5 חיזוק השקיפות והפיקוח הפרלמנטרי

מוצע להגביר באופן משמעותי את הפירוט הנדרש בדיווחים השנתיים של המשטרה מכוח החוק, וזאת בין השאר על בסיס השוואה עם הדיווחים הפומביים המנהיגים בבריטניה ובארצות הברית ביחס להפעלת סמכויות מעקב על ידי סוכנויות הביטחון ואכיפת החוק.<sup>82</sup>

<sup>79</sup> שי לוי "מאגר ביומטרי? השוטרים יכולים להפיץ מידע אישי על כל אחד מאיתנו" **Mako** (21.10.2013) <https://www.mako.co.il/special-mako-news/Article-62fa938b04bd141006.htm>

<sup>80</sup> ר' לדג' ביד"מ 7/19; ביד"מ 72/18; ביד"מ 73/17; ביד"מ 30/18; ביד"מ 34/18; ביד"מ 60/18; ביד"מ 74/18; ביד"מ 50/18; ביד"מ 13/20; ביד"מ 18/21; ביד"מ 32/21; ביד"מ 45/17; ביד"מ 21/17; ביד"מ 17/21

<sup>81</sup> מ"י/מטא"ר/אגף משאבי אנוש, מכתב מיום 29.7.2021, סימוכין 71235521

<sup>82</sup> ר' דו"ח נציב סמכויות חקירה הבריטי IPCO, Annual Report of the Investigatory Powers Commissioner 2020 (2022), [https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020\\_Web-Accessible-version.pdf](https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf); דו"ח הנהלת בתי



## המכון הישראלי לדמוקרטיה

על הדיווחים להתייחס ביתר פירוט לפרמטרים הנוגעים לאמצעי המעקב וסוג התוכן המבוקש, בחתכים רלוונטיים שונים. עליהם לכלול פירוט של מעקבים דחופים שאושרו במסלול שאינו דורש צו מאת בית המשפט (ס' 7 לחוק האזנת סתר, לדוגמא). על הדיווחים לאפשר בחינה של אפקטיביות הפיקוח השיפוטי, ולכלול מידע ביחס לצווים שהוארכו, לבקשות שתוקנו על ידי בית המשפט וסוגי התיקונים, כמו גם להיתרים שניתנו ללא פיקוח שיפוטי ואישורם או ביטולם בדיעבד על ידי הגורם האקזקוטיבי המפקח. מוצע לכלול בדיווחים בחינה של מידת האפקטיביות המודיעינית של הצווים – כמות הצווים שהסתיימו בהרשעה וללא הרשעה, מספר העבירות שסוכלו בעקבות צו, כמות האזנות הסתר שאושרו אך לא ניתן היה להפיק מידע בפועל. כמו כן, נדרש דיווח פרטני על סוגיות מהותיות שעלו בישיבות השוטפות בנושא מול משרד המשפטים, ועל נהלים חדשים שאושרו לאור הכנסת טכנולוגיות מעקב חדשות.

---

המשפט הפדראליים ביחס לבית הדין למודיעין זר (FISC) United States Courts, Report of the  
Director of the Administrative Office of the U.S. Courts on Activities of the Foreign  
Intelligence Surveillance Courts for 2020 (16.07.2021)  
FISC (להלן: [https://www.uscourts.gov/sites/default/files/fisc\\_annual\\_report\\_2020.pdf](https://www.uscourts.gov/sites/default/files/fisc_annual_report_2020.pdf))  
United States Courts, *Wiretap Report 2020*; דו"ח האזנות הסתר הפדרלי השנתי, *Wiretap Report 2020*  
(להלן: <https://www.uscourts.gov/statistics-reports/wiretap-report-2020>) (31.12.2020)  
(Wiretap report 2020)