דין וחשבון

הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים

חברי הצוות:

עו״ד עמית מררי, המשנה ליועצת המשפטית לממשלה (משפט פלילי), יו״ר הצוות

מר איל דגן, ראש אגף חקירות בשירות הביטחון הכללי בדימוס

מר צפריר כץ, ראש האגף הטכנולוגי בשירות הביטחון הכללי בדימוס

ירושלים, אב התשפ״ב - אוגוסט 2022

תוכן עניינים

תקציר 1

1. **מבוא** 10

1.1 הקמת צוות הבדיקה 10

1.2 פירוט הישיבות והדוברים שהופיעו בפני צוות הבדיקה 12

2. **רקע נורמטיבי** 14

2.1 חוק האזנת סתר – רקע כללי 14

2.2 ההגדרות הקבועות בחוק לעניין האזנת סתר לתקשורת בין מחשבים 18

2.3 סוגי היתרים להאזנות סתר 19

2.4 ייחודה של האזנת סתר 20

2.5 הבחנה בין האזנת סתר לתקשורת בין מחשבים לבין חיפוש במחשב, המצאה ותפיסה 21

3. **רוגלות** 25

4. **בדיקת הטענות לכך שהמשטרה מבצעת האזנות סתר ללא צווי בית משפט כנדרש בחוק** 29

4.1 בדיקת מערכת סייפן 31

4.1.1 אופן הבדיקה וממצאים 31

5. **בדיקת הטענות לכך שבמסגרת האזנת סתר המשטרה חורגת מסמכויותיה ואוספת מידע שאינו מהווה תקשורת בין מחשבים** 33

5.1 מידע האגור על מכשיר הטלפון 34

5.1.1 אישורים משפטיים לקבלת מידע אגור 36

5.1.2 עמדת הצוות לעניין קבלת מידע אגור 37

5.2 סוגי מידע שאינם מהווים תקשורת בין מחשבים 38

5.2.1 רשימת האפליקציות המתקבלת באופן אוטומטי 38

5.2.2 מידע נוסף שלא מהווה תקשורת בין מחשבים המתקבל במערכת סייפן 39

5.2.3 האם ניתנו אישורים משפטיים לאיסוף סוגי מידע שאינם מהווים תקשורת בין מחשבים 41

5.3 בדיקות מדגמיות בכל הנוגע להפקת המידע החורג 41

5.4 המלצות הצוות לעניין הפעלה מחודשת של המערכות 41

6. **נוסח הבקשות לצווי האזנת סתר** 44

6.1 רקע נורמטיבי לעניין הוראות הדין בדבר בקשה להיתר להאזנת סתר 44

6.2 ממצאים והמלצות 46
7. **שרשרת האזנה** 49
7.1 מהי שרשרת האזנה? 49
7.2 השלבים השונים בשרשרת ההאזנה 50
7.3 ממצאים והמלצות בעניין שרשרת ההאזנה 52
8. **בחינת הליכי האישור ביחס למערכות להאזנה לתקשורת בין מחשבים המותקנות על מכשיר קצה** 53
8.1 בחינת הליכי האישור 54
8.1.1 מעבר ראשון מהאזנת סתר בתווך התעבורה לשימוש באמצעים המותקנים על מכשיר קצה 54
8.1.2 אישורים משפטיים והנחיות שניתנו למערכת סייפן 54
8.1.3 דיונים משפטיים שהתקיימו במשרד המשפטים 57
8.2 ממצאים 58
8.3 המלצות 59
8.3.1 המלצות ביחס להליכי הטמעת מערכות טכנולוגיות חדשות במשטרת ישראל 59
8.3.2 המלצות בעניין הייעוץ המשפטי לחטיבת הסייבר והייעוץ המשפטי למשטרה 60
8.4 הליכי פיקוח ובקרה בחטיבת הסייבר 62
8.5 המלצות לעניין הליכי פיקוח ובקרה 64
9. **יועצים חיצוניים** 65
10. **פיקוח משרד המשפטים על האזנות סתר של משטרת ישראל** 66
10.1 פיקוח היועץ המשפטי לממשלה על האזנות סתר - רקע 66
10.2 ממצאים והמלצות 67
11. **המלצות לתיקוני חקיקה** 69
נספחים 71
נספח א' - ממצאי צוות הבדיקה בעניין האזנות סתר בדרך של תקשורת בין מחשבים לעניין הפרסום באתר "כלכליסט" מיום 7.2.22 72
נספח ב' - עמדה משפטית 77
נספח ג' – כתב מינוי 97

תקציר

הקמת הצוות ומטרותיו

הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים מונה ביום 31 בינואר 2022 על ידי היועץ המשפטי לממשלה (דאז), פרופ׳ אביחי מנדלבליט, נוכח טענות שעלו בסדרת פרסומים בעיתון ״כלכליסט״, ולפיהן משטרת ישראל מבצעת פעולות למעקב טכנולוגי אחר אנשים באמצעות תוכנת פגסוס של חברת NSO (להלן – **החברה**), על מנת לקבל מידע מודיעיני ללא קשר לחקירה מתנהלת או לברור חשדות לביצוע עבירות פליליות, וממילא מבלי שהתקבל צו שיפוטי. עוד נטען כי בעת ביצוע האזנת הסתר לתקשורת בין מחשבים של טלפונים ניידים, מתקבל מידע אשר חורג מהמותר על פי חוק האזנת סתר, התשל״ט-1979 (להלן – **חוק האזנת סתר**). בהמשך לכך, ביום 7 בפברואר 2022 פורסמה רשימת שמות של אנשים שנטען כי משטרת ישראל חדרה לטלפונים הניידים שלהם ושאבה מהם מידע ללא צו בית משפט.

טענות אלה נוגעות בליבת שלטון החוק במדינה דמוקרטית, וככל שיש בהן ממש, פוגעות פגיעה חמורה במרחב הפרטיות הנתון לכל אדם בה. יש בטענות אלה כדי לערער את אמון הציבור במשטרת ישראל, גוף האכיפה המרכזי במדינה האמון על שמירה על שלטון החוק, וברשויות האכיפה בכלל.

כאמור, נוכח חומרת הטענות, החליט היועץ המשפטי לממשלה דאז על מינוי צוות לבדיקת האזנות סתר לתקשורת בין מחשבים בראשות המשנה ליועצת המשפטית לממשלה (משפט פלילי), עמית מררי. כחברים בצוות מונו שני ראשי אגפים בדימוס בשב״כ: צפריר כץ, שעמד בראש האגף הטכנולוגי, ואיל דגן שעמד בראש אגף החקירות.

בעקבות בירור ראשוני שנערך עם המשטרה, עלה כי בעת השימוש במערכת נקלטים חומרים מעבר לאלה שהוצגו תחילה ליועץ המשפטי לממשלה עם פרסום הכתבות. לפיכך, ביום 31 בינואר 2022, עם הקמת צוות הבדיקה, הנחה היועץ המשפטי לממשלה דאז את משטרת ישראל להשעות את השימוש במערכת עד שייקבע על-ידו או על ידי מי מטעמו כי אין מניעה לשוב ולהשתמש בה. משכך הפסיקה המשטרה את השימוש במערכת. בעקבות הפרסום מיום 7 בפברואר, התבקש הצוות לבחון בשלב ראשון האם בוצעה חדירה באמצעות תוכנת פגסוס שבשימוש משטרת ישראל, למכשירי טלפון ניידים (להלן - **הדבקה**) השייכים אל מי מבין האנשים ששמותיהם פורסמו, וזאת ללא צו שיפוטי המתיר זאת.

לצורך בדיקת הטענות, ובהתאם לכתב המינוי, צוותו לצוות הבדיקה עובדי שירות הביטחון הכללי והמוסד למודיעין ולתפקידים מיוחדים, המומחים בתחום הטכנולוגיה הרלוונטית. יודגש כי המומחים לא פעלו כנציגי הגופים בהם הם מועסקים ולא הונחו על ידם. צוות הבדיקה, בסיועם של המומחים הטכנולוגיים, ערך בדיקה טכנולוגית יסודית וממוקדת של מספרי הטלפון של רשימת האנשים אל מול נתונים הנמצאים בבסיס הנתונים הפנימי של המערכת אשר לא ניתן לשינוי או למחיקה ואשר משקף את הפעולות שבוצעו באמצעות המערכת (Audit Log). יצוין כי המערכת מותקנת במתקני משטרת ישראל, ואולם גישה לשכבה זו של המערכת מחייבת ידע טכני כמו גם נתוני אימות המצויים ברשות החברה ולא בידי המשטרה. מכאן שבסיס הנתונים הפנימי של המערכת אינו זמין למשתמש, אלא יכול להיות מונגש במתקני המשטרה על ידי חברת NSO בלבד.

ביום 21 בפברואר 2022 פורסמו ממצאי הבדיקה שביצע הצוות ביחס לרשימת האנשים שהתפרסמה ואשר נטען לגביהם כי המשטרה הדביקה את הטלפונים הניידים שלהם ללא צו בית משפט. הבדיקה העלתה כי אין כל אינדיקציה לכך שמשטרת ישראל הדביקה באמצעות מערכת פגסוס שבידיה, (המכונה על ידי המשטרה "**סייפן**"), ללא צו שיפוטי, מכשיר טלפון נייד של מי מבין רשימת האנשים שפורסמו בתקשורת. כמו כן, נבדקה מערכת נוספת שבידי משטרת ישראל, ולא היו כל אינדיקציות להדבקות או ניסיונות הדבקה של המכשירים של מי מבין רשימת האנשים האמורה.

להרחבה ראו "ממצאי צוות הבדיקה בעניין האזנות סתר בדרך של תקשורת בין מחשבים לעניין הפרסום באתר "כלכליסט" מיום 7.2.22" המצורף כנספח א' לדוח זה.

לאחר פרסום הממצאים הראשוניים המשיך הצוות בבדיקה מעמיקה ומקיפה של הסוגיות הנוגעות להאזנת סתר לתקשורת בין מחשבים, בין היתר בנוגע לטענה הכללית כי משטרת ישראל חודרת לטלפונים ניידים אף בהיעדר קיומו של חשד פלילי וללא צו בית משפט ושואבת את תוכנם, לרבות תוך שימוש ב"האקרים" חיצוניים; בחינת הסוגיה של עצם השימוש ברוגלות על ידי משטרת ישראל; בדיקה של מאפייני מערכות האזנת סתר לתקשורת בין מחשבים של טלפונים ניידים שבשימוש משטרת ישראל ומידת התאמתן לחוק - בשים לב לעמדה המשפטית שגובשה; בחינת התמונה המוצגת לבתי המשפט במסגרת בקשה להאזנת סתר לתקשורת בין מחשבים של טלפונים ניידים; בחינת הליך שרשרת ההאזנה והליכי הפיקוח והבקרה; וכן בחינה כללית של הליכי האישור המשפטי בנוגע לשימוש במערכות אלו על ידי הייעוץ המשפטי למשטרה ומשרד המשפטים, ככל שניתנו, על מנת להתוות עקרונות ודרכי פעולה לעתיד.

עבודת הצוות ערכה מאות שעות של עבודה. מאז מונה הצוות ועד למועד פרסום הדוח נערכו כ- 50 ישיבות צוות שחלקן ארכו ימים שלמים. כמו כן, הגורמים שסייעו לצוות הבדיקה הגיעו באופן תדיר למטה חטיבת הסייבר וביצעו בדיקות שנמשכו מספר חודשים.

כפי שיפורט בהמשך, צוות הבדיקה ערך בדיקות טכנולוגיות מקיפות, נפגש עם גורמים רלוונטיים שונים במשטרת ישראל בעבר ובהווה, ביניהם ראשי ומנהלי חטיבת הסייבר הגורמים האמונים בפועל על הפעלת הכלים והגורמים האמונים על הפקת המידע הנאסף על ידי המערכות והעברתו ליחידה החוקרת.

יודגש כי לאורך כל תקופת עבודתו של צוות הבדיקה משטרת ישראל שיתפה עימו פעולה בפתיחות מלאה ואפשרה לצוות הבדיקה ולמומחים הטכנולוגיים שסייעו בידו להיחשף למערכות הטכנולוגיות, לקיים מפגשים עם בעלי התפקידים הנוגעים בדבר, וכן העמידה לרשותו את כל המידע שהתבקש.

כחלק מבחינת מאפייני המערכות שבידי משטרת ישראל שפותחו על ידי חברות פרטיות, נפגש צוות הבדיקה עם נציגים של חברת NSO בכל הנוגע למאפייני מערכת סייפן, ועם נציגי חברה נוספת שמערכת בפיתוחה הייתה טרם הקמתו של הצוות בשימוש בשלבי פיילוט במשטרה (להלן יחד – **החברות**). יודגש כי נציגי החברות שיתפו פעולה עם צוות הבדיקה והיו זמינים לכל שאלה או הבהרה בנוגע למערכות שהתבקשו על ידי צוות הבדיקה.

ביחס לטענות שפורסמו על ידי עיתון "כלכליסט", נפגש צוות הבדיקה עם עורכת העיתון, הגב' גלית חמי, ועם סגן העורכת, מר אמיר זיו.

הצוות קיים סדרת פגישות עם גורמים שונים באשר לסוגיות העקרוניות המתעוררות בעניין הפעלת רוגלות (תוכנות המותקנות באופן סמוי על מערכות מיחשוב), ובכלל זה גופים ציבוריים - הסנגוריה הציבורית והרשות להגנת הפרטיות, וארגוני חברה אזרחית.

כחלק מבחינת סוגיות הנוגעות למעמד הייעוץ המשפטי למשטרה ותפקידו ולדפוסי העבודה מול הייעוץ המשפטי לממשלה, לבקשת הצוות התקיימה פגישה מקצועית עם כב׳ השופט בדימוס פרופ׳ יצחק זמיר, אשר כיהן בתפקיד היועץ המשפטי לממשלה בין השנים 1978-1986 וכשופט בית המשפט העליון בין השנים 1994-2001.

בכל הנוגע לעמדות המשפטיות המפורטות בדוח זה ובנספח המשפטי, אלו נבחנו בנפרד לעבודת הצוות על ידי גורמי הייעוץ המשפטי לממשלה ואושרו על ידי היועצת המשפטית לממשלה, לאחר שהובאו בפניה ממצאי הצוות ועמדת המשנה ליועצת המשפטית לממשלה (משפט פלילי) וצוותה.

תקציר ממצאי הצוות

<u>רקע נורמטיבי</u>

כפי שמפורט בהרחבה בפרק הרקע הנורמטיבי בדוח, חוק האזנת סתר נועד מצד אחד לקבוע בחקיקה הגנה איתנה מפני חדירה לצנעת הפרט על ידי האזנה לשיחותיו של אדם ללא ידיעתו, ומן הצד השני להסדיר את ההליכים להאזנה כשזו מחויבת מטעמים של ביטחון המדינה או מניעת עבירות וגילוי עבריינים. בכל הנוגע לסמכות המשטרה לפי החוק, זו מוסמכת לבצע האזנת סתר לצורך מניעה, גילוי או חקירה של עבירות פשע, זאת בכפוף לאישור של נשיא בית משפט מחוזי או סגנו. כמו כן, למפכ״ל המשטרה סמכות לתת היתר כאמור ל-48 שעות בלבד במקרים שאינם סובלים דיחוי (כאשר לא ניתן לקבל בעוד מועד היתר מבית משפט), בכפוף לתנאים נוספים. בהתאם לחוק, על המפכ״ל להעביר דיווח ליועץ המשפטי לממשלה אחת לחודש, ובו פירוט של כלל היתרי האזנת הסתר שניתנו ותנאיהם. במסגרת זו מפורטים העבירה שביסוד הבקשה; זהותו של האדם שביחס אליו בוצעה ההאזנה; סוג ההאזנה שבוצעה; משך ההיתר שניתן; הנימוקים להאזנה שהוצגו לבית המשפט והחלטת בית המשפט.

בכל הנוגע להאזנה לתקשורת בין מחשבים, ובכלל זה האזנה לתקשורת בין מחשבים של טלפונים ניידים, סמכות זו נשענת על ההגדרות הקבועות בחוק האזנת סתר. האזנה כאמור מוגבלת להאזנה למידע המועבר בתקשורת בין מחשבים מיום מתן ההיתר ואילך ועד לתום התקופה הנקובה בהיתר שניתן.

לצד זאת, למשטרה סמכות נפרדת לקיים חיפוש **גלוי** במחשב (ובכלל זה טלפון נייד) של המידע האגור בו, וזאת לפי הוראות פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש] התשכ״ט-1969.

מכאן שלמשטרה אין סמכות לבצע חיפוש סמוי במחשב ובכך לשאוב את המידע האגור על הטלפון הנייד באופן סמוי, אלא רק לבצע האזנה ממועד מתן הצו ואילך של מידע המועבר בתקשורת בין מחשבים. לעניין זה ראו הרחבה בפרק הרקע הנורמטיבי וכן בנספח המשפטי.

<u>בדיקות הצוות ביחס להאזנות סתר שבוצעו על ידי משטרת ישראל</u>

בדיקת הצוות נעשתה בשני מישורים: **האחד**, האם בוצעה האזנה לאנשים שאין בעניינם צו בית משפט המתיר האזנה לתקשורת בין מחשבים של טלפונים ניידים ובהתאם למועדים הקבועים בו.

השני, האם במסגרת ביצוע האזנת הסתר, הייתה חריגה בהיקף המידע שהתקבל המותר לפי חוק האזנת סתר, המהווה חריגה מסמכות.

להלן יפורטו הממצאים ביחס לבדיקות:

(1) בדיקת הטענות לעניין הדבקת טלפונים ניידים בהיעדר צו שיפוטי

במסגרת הטענות שפורסמו, נטען כי קיים דפוס פעולה שיטתי לפיו משטרת ישראל מדביקה באמצעות מערכת פגסוס שברשותה טלפונים ניידים של אנשים שאין בעניינם חשד פלילי ובהיעדר צו שיפוטי בניסיון לקבל מידע מודיעיני.

בשים לב לחומרת הטענות, הרחיב הצוות את הבדיקה הראשונית וביצע בדיקה טכנולוגית מעמיקה ביחס לכל מכשירי הטלפון הניידים שהודבקו מיום התקנתה של המערכת במשטרת ישראל. בדיקה זו נשענה על נתונים הנמצאים בליבת מערכת סייפן (Audit Log) ונשלפו על ידי חברת NSO לבקשת צוות הבדיקה. כפי הנמסר מחברת NSO אלה לא ניתנים לשינוי או למחיקה, והם נתונים מלאים של כל הדבקה שבוצעה באמצעות המערכת לאורך כל שנות פעילותה במשטרה; המועד המדויק שבו בוצעה ההדבקה; והטלפון הנייד שנדבק באותו מועד. ביחס לכל נתון כאמור, צוות הבדיקה בחן האם קיים צו בית משפט המתיר את ההאזנה שבוצעה, סוג היתר בית המשפט שניתן, ומועד תוקפו.

מבדיקת הצוות ביחס לכלל המספרים שקיימים בבסיס הנתונים הפנימי של מערכת סייפן, נמצא כי אין כל אינדיקציה לנכונות הטענות לפיהן הודבקו טלפונים ללא צו. ביחס לכלל המספרים עלה כי משטרת ישראל פעלה כשברשותה היתר כדין, למעט 4 מקרים, בהם ניסיון ההדבקה לא צלח, וממילא לא התקבלו תוצרים. אשר לחריגים אלה – שני מקרים בהם עלה כי בוצע ניסיון הדבקה כאשר צו בית המשפט שניתן מתיר האזנת סתר, אולם אינו מתיר האזנה מסוג תקשורת בין מחשבים לטלפון נייד; מקרה אחד בו בוצע ניסיון הדבקה זמן קצר לאחר פקיעת תוקפו של הצו; מקרה נוסף בו בוצע ניסיון הדבקה, אך מבדיקות הצוות לא אותר ההיתר הנדרש לפי הנהלים להעלאת יעד נוסף בהתאם לצו שניתן (ראו פירוט בפרק 4). לטענת המשטרה מדובר בטעויות בתום לב.

צוות הבדיקה הרחיב את בדיקתו למערכות נוספות שבידי המשטרה שלהן יכולת להאזנה לתקשורת בין מחשבים של טלפונים ניידים, וגם בעניינן לא נמצאה אינדיקציה להדבקה ללא צו. בכלל זה נשלפו נתונים גם מבסיס הנתונים של מערכת נוספת שבידי משטרת ישראל שבפיתוח חברה פרטית, שגם הוא כפי שנמסר מהחברה אינו ניתן לשינוי או למחיקה. גם לגבי מערכת זו לא נמצאה כל אינדיקציה כאמור.

שתיים מהמערכות שהיו בשימוש בעבר פותחו על ידי משטרת ישראל, ומובהקות הבדיקה הטכנולוגית לגביהן נמוכה יותר. יחד עם זאת יש להדגיש את הדברים שלהלן:

למערכת אחת המכונה "חלוץ" הייתה היכולת לבצע האזנה רק לטלפונים <u>ממספר מצומצם של דגמים ישנים</u>, וההדבקה באמצעותה היתה אפשרית <u>רק בנגישות פיזית</u> אל הטלפון הנייד שהוא יעד ההאזנה (אין למערכת זו אפשרות לביצוע הדבקה מרחוק). מערכת נוספת, המכונה "דייזי", נבדקה על אף שלה היכולת לבצע האזנה <u>למחשבים</u> בלבד, ובעניינה, כפי שנמסר מהמשטרה, ניתן היה לבצע הדבקה <u>רק בנגישות פיזית</u>. כאמור, מהבדיקה הטכנולוגית שבוצעה גם בעניינן של מערכות אלה לא נמצאה אינדיקציה להאזנה ללא צו בית משפט.

לאור האמור לעיל, לא נמצא בסיס לטענה כי משטרת ישראל מדביקה טלפונים ניידים של אנשים שאין בעניינם חשד פלילי ובהיעדר צו שיפוטי. בניגוד לנטען, התרשמות הצוות בעקבות הבדיקות שנערכו היא כי קיימת בחטיבת הסייבר הקפדה על ביצוע האזנה רק לאחר קבלת צווים כדין.

(2) <u>בדיקת הטענות לפיהן במסגרת הדבקה המשטרה אוספת מידע שאינו מותר על פי דין</u>

במסגרת הפרסומים נטען כי משטרת ישראל מבצעת שאיבה של כל החומר האגור על הטלפון הנייד בניגוד לסמכות הקבועה בחוק האזנת סתר. לאור זאת, ביצע צוות הבדיקה בדיקות מקיפות לעניין מאפייני המערכות שבשימוש משטרת ישראל להאזנה לתקשורת בין מחשבים של טלפונים ניידים באמצעות הדבקה.

ככלל הבדיקה העלתה כי מערכות אלה פועלות בדרך של איסוף תוצרים חדשים אשר עברו בתקשורת בין מחשבים מרגע הדבקת הטלפון הנייד.

עם זאת, נמצא כי אכן קיימות חריגות ביכולות הטכנולוגיות של מערכת סייפן שבידי משטרת ישראל המאפשרת לקבל סוגי תוצרים מסוימים שאינם מותרים לפי חוק האזנת סתר. יכולות טכנולוגיות אלה חורגות בשני מישורים:

האחד, מערכת סייפן מאפשרת למשטרה לקבל מידע האגור על מכשיר היעד <u>אשר נוצר קודם למועד ההדבקה ואף קודם למועד הצו.</u> קבלת המידע האגור אפשרית באמצעות הפעלה אקטיבית של יכולת זאת. באופן קונקרטי, הופעלה יכולת זאת במסגרת האזנות בהן ביקשה המשטרה להשלים פערי זמן של האזנה שנוצרו בתוך תקופת ההיתר של בית המשפט, במקרים בהם הכלי חדל לפעול מסיבות טכנולוגיות שונות והותקן מחדש. לשם המחשה: אם ניתן צו בית משפט להאזנה לתקשורת בין מחשבים ליעד מסוים לחודשים ינואר-פברואר, ובוצעה הדבקה ביום 1.1, אך הכלי חדל לפעול מסיבה זו או אחרת ביום 2.1 ורק ביום 10.1 הצליחו לבצע הדבקה חדשה, פעלו המפעילים לקבלת המידע האגור במכשיר שבין ה-2.1 ל-10.1. לעניין זה, עד אפריל 2020 לא ניתן היה להגביל את המועד אשר החל ממנו יתקבל מידע אגור, ועל כן התקבל במקרים רבים מידע הקודם למועד ההתקנה הראשון ואף הקודם למועד צו בית המשפט.

בשימוש המשטרה מערכת נוספת בפיתוח חברה פרטית, אשר אוספת מידע מרגע ההדבקה ואילך ולה היכולת במקרים קונקרטיים להביא מידע אגור בכפוף להכנסת תאריכים מדויקים שמהם רוצים לקבל את המידע בשלב ההדבקה.

השני, למערכת סייפן היכולת לקבל מידע שאינו מהווה תקשורת בין מחשבים כגון פרטי יומן, אנשי קשר ופתקים האגורים במכשיר, ורשימת האפליקציות המותקנות. ואכן, במקרים רבים התקבל מידע כאמור במסגרת ביצוע האזנת סתר. גם לעניין זה, רק באפריל 2020 ניתן היה לבחור להגביל מראש את סוגי התוצרים שיתקבלו במסגרת האזנת הסתר ולמנוע קבלת אותם חומרים אסורים.

לא נחסמה טכנולוגית היכולת לקבל מידע אגור או מידע שאינו בגדר תקשורת בין מחשבים, ומידע כזה אכן התקבל במערכות המשטרה. עם זאת, קיימים נהלים בחטיבת הסייבר האוסרים על <u>הפקת</u> מידע שאינו מהווה תקשורת בין מחשבים וכן מידע הקודם למועד ההתקנה הראשון. צוות הבדיקה התרשם כי קיימת הפנמה ומשמעת של הגורמים הרלוונטיים ביחס לגדרי המותר והאסור לשימוש. כמו כן, מ-25 בדיקות מדגמיות שבוצעו, עלה כי לא בוצעה הפקה בכתב של תוצרים אלה.

עמדת צוות הבדיקה היא שנדרש היה לבצע את החסימות הטכנולוגיות (להלן גם – ניוונים) במלואן בטרם כניסת המערכות לשימוש במשטרת ישראל על מנת להתאימן לסמכויות המוקנות למשטרה לפי חוק האזנת סתר.

ומבלי להקל ראש בהיקף הפגיעה בפרטיות, ראוי לציין עם זאת, יש להדגיש כי לפי בדיקת מסמכים טרם רכישת המערכת ולאחר מכן, ומהתרשמות של צוות הבדיקה מהגורמים שאיתם נפגש עלה כי אי ניוון המערכת באופן מלא לא נבע מרצון המשטרה לעשות שימוש במידע החורג, אלא, הנחת המוצא של חטיבת הסייבר הייתה כי בשים לב לאיסור הנוהלי על הפקת המידע, יש בכך כדי להוות תנאי מספק להתאמת חריגות המערכת לסמכות לפי חוק האזנת סתר.

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. זאת, אף אם למשטרת ישראל לא הייתה כוונה לעשות שימוש בפועל במידע העודף שהתקבל בידה, ואף שעיגנה בנהליה איסור לעשות שימוש במידע עודף כאמור. לעמדת הצוות לא היה די בהסדרה בנהלים, והיה צורך לבצע ניוון טכנולוגי של היכולות העודפות.

<u>אשר לטענות בדבר הטעיית בית המשפט במסגרת בקשות להאזנת סתר</u>: הצוות מצא כי בבקשות שהוגשו לבית המשפט הוצג המידע בדבר סוגי התוצרים אשר עתידים להתקבל אגב ביצוע האזנת סתר אשר ייעשה בהם שימוש. הצוות לא מצא כי המשטרה פעלה כדי להסתיר מידע מבית המשפט. יתר על כן, כאשר בית המשפט דרש במקרים קונקרטיים פרטים נוספים מעבר לאמור בבקשה, הפרטים הנוספים הועברו. יחד עם זאת, נוכח מאפייני המערכת, בראיה לאחור, סבור הצוות כי היה מקום להרחיב עוד בפני בית המשפט באשר לשיטת הפעולה להאזנה, וכן באשר לסוג המידע שעשוי להתקבל במסגרת ההאזנה ואשר לא יופק (וזאת מבלי לגרוע מהעמדה לעיל לפיה היה מקום לכתחילה לנוון את המערכת).

תקציר המלצות הצוות

התאמת הכלים לסמכויות הנתונות למשטרה: יש לוודא במבט צופה פני עתיד כי מערכות טכנולוגיות אשר בשימוש משטרת ישראל תואמות את הסמכויות המעוגנות בחקיקה.

נדרש ליווי משפטי צמוד על ידי הייעוץ המשפטי למשטרה לאורך תהליך הטמעת מערכות חדשות מראשיתו ועד סופו: הצוות מצא כי סוגיות הנוגעות לשורש גדרי הסמכויות הנתונות למשטרה על פי דין לא הובאו על ידי חטיבת הסייבר לידיעה מפורשת ומלאה של הייעוץ המשפטי למשטרה כפי שהיה נדרש. יש להבטיח כי כלל התנאים הנדרשים מבחינה משפטית מתקיימים עוד טרם הפעלת הכלי. כמו כן נדרש יידוע ושיתוף מלא של הייעוץ המשפטי למשטרה ביחס לסוגיות המתעוררות אגב השימוש בטכנולוגיה.

אישור הייעוץ המשפטי לממשלה לכלים שלהם יכולות טכנולוגית מסוג חדש:

לאורך השנים היה ידוע לייעוץ המשפטי לממשלה, ולמחלקת הסייבר בפרקליטות המדינה, שקיימת מערכת להאזנת סתר בשם "סייפן", אשר מבצעת האזנת סתר על ידי חדירה למכשיר קצה. מבירור הצוות, על אף מערכת היחסים ההדוקה וההתייעצויות השוטפות של משטרת ישראל עם מחלקת הסייבר בפרקליטות, והייעוץ המשפטי לממשלה, לא עלה כי הועברו לידי משרד המשפטים בדרך זו או אחרת כלל מאפייני המערכת, ובאופן ספציפי מידע ביחס ליכולות הטכנולוגיות של המערכת אשר חורגות מהסמכות לפי חוק האזנת סתר. משלא הובאה המערכת לאישור הייעוץ המשפטי לממשלה, על כלל מאפייניה, כפי שהיה נדרש, ממילא לא התקיים דיון עקרוני בנושא בייעוץ המשפטי לממשלה. למעלה מכך, אף סוגיות עקרוניות שהתעוררו במהלך הפעלת הכלי, ואושרו משפטית על ידי הייעוץ המשפטי למשטרה, לא הובאו לידיעת הייעוץ המשפטי לממשלה.

על המשטרה לוודא כי כל מערכת טכנולוגית שלה יכולת חדשה מבחינת איסוף או עיבוד המידע, ושהיא בעלת פוטנציאל לחריגה מהסמכות הקבועה בחוק, תועבר לאישור הייעוץ המשפטי לממשלה, טרם השימוש בה. זאת, תוך פירוט כלל מאפייני המערכת והתנאים להפעלתה, בצירוף עמדה משפטית בדבר מקור הסמכות.

הבניה של מנגנוני פיקוח ובקרה מקצועיים: קיימת חשיבות להקמת שני מנגנוני פיקוח על מערכות להאזנת סתר. הראשון הוא מנגנון פיקוח תהליכי לפיו תבחן המשטרה באופן עיתי ושיטתי האם הפעלת האמצעי להאזנת הסתר והשימוש בתוצרים הם בהתאם להוראות החוק, צו בית המשפט והנהלים. השני הוא מנגנון פיקוח טכנולוגי ולפיו כל מערכת להאזנת סתר תכלול בסיס נתונים שאינו ניתן לשינוי אשר ניתן יהיה להפיק ממנו מידע לצורך בקרה ומעקב בקלות, ביחס לכל אחד משלבי תהליך ההאזנה.

טיוב נוסח הבקשות לבית המשפט להיתרי האזנת סתר לתקשורת בין מחשבים: כאמור לעיל, הצוות מצא כי אכן צוין בפני בית המשפט סוגי המידע שיתקבלו וכי מדובר בהאזנה הדורשת התקנת תוכנה במכשיר. מוצע להרחיב בטופס הבקשה באשר לשיטת ההאזנה (למשל שמדובר בהדבקה מרחוק של מכשיר טלפון נייד). עוד במסגרת בדיקת הצוות עלה כי ככלל, כאשר מבוקשת האזנה לתקשורת בין מחשבים של טלפונים ניידים מבוקש באופן גורף כלל סוגי המידע המהווה תקשורת בין מחשבים. נכון שהמשטרה תקפיד לבחון בכל מקרה ביחס לכל אחד מסוגי המידע, האם הוא נדרש לחקירה הקונקרטית.

הצורך בבחינת המבנה הארגוני של הייעוץ המשפטי במשטרה: הגורמים האמונים על מתן ייעוץ משפטי בחטיבות השונות במשטרה, ובכלל זה באגף החקירות והמודיעין אליה משתייכת גם חטיבת הסייבר, אינם כפופים מקצועית ופיקודית ליועץ המשפטי למשטרה, על אף שבהקשרים רבים קיימת עבודה צמודה ומתואמת ביניהם. גם היועצים המשפטיים במחוזות השונים במשטרת ישראל כפופים מקצועית בלבד ליועץ המשפטי למשטרת ישראל. צוות הבדיקה מצא כי בענייננו לא היה שיתוף מספק של הייעוץ המשפטי למשטרה, והנחיותיו לא יושמו כנדרש. הייעוץ המשפטי למשטרה עצמו לא היה אקטיבי דיו על מנת לוודא שהנחיותיו מבוצעות. הצוות סבור כי יש קושי בהיעדר כפיפות מקצועית ופיקודית לייעוץ המשפטי למשטרה. בכפיפות כאמור יש כדי לבסס ייעוץ משפטי עצמאי בעל ראיית רוחב ביחס לכלל הנעשה במשטרת ישראל. הצוות ממליץ כי נושא זה ייבחן בעבודת מטה שתערך בהקדם.

טיוב הליכי הפיקוח של משרד המשפטים והעמקת המומחיות המשפטית-טכנולוגית: נוסף על המלצת הצוות המפורטת לעיל לעניין אישור היועצת המשפטית לממשלה לשימוש בכלים טכנולוגיים חדשים, מוצע בין היתר כדלקמן:

יש להשתמש בהליכי הפיקוח הקיימים לפי החוק על מנת להרחיב את תשתית הפיקוח הקיימת ולייצר הזדמנויות נוספות לבחינת שאלות משפטיות הנוגעות לשימוש בטכנולוגיות חדשות. לצורך כך נדרש, בין היתר, לציין בדיווח העתי את האמצעי הספציפי שבאמצעותו בוצעה ההאזנה.

נוסף על כך, נדרשת העמקה של הידע המשפטי הטכנולוגי של הגורמים הרלוונטיים בייעוץ המשפטי לממשלה, בין היתר, בנוגע לאיסוף שימוש ועיבוד מידע פרטי על אודות אדם על ידי גופי האכיפה. העמקה כאמור תאפשר לטייב את היכולות לאתר ולטפל בסוגיות משפטיות המתעוררות אגב היבטים טכנולוגיים ולהתעמק בהם, תוך התייחסות מראש להתפתחויות צפויות באופן שיצמצם ככל האפשר את הפער בין ההסדרה בדין לבין המציאות הטכנולוגית הקיימת באותה עת.

יש להדגיש כי אין בכל אלה כדי לגרוע מכך שהאחריות להצגת תמונה עובדתית מלאה באשר ליכולות טכנולוגיות המובאות בפני משרד המשפטים, היא על משטרת ישראל.

תנאים לשימוש במערכות שבידי משטרת ישראל:

רוגלה היא תוכנה המותקנת באופן סמוי על גבי מערכת מחשוב (בין אם מרחוק או באופן פיזי), ומאפשרת לצד התוקף נגישות למערכת המחשוב הנתקפת. צוות הבדיקה קיים דיון בכל הנוגע לעצם השימוש ברוגלות להאזנת סתר על ידי גורמי אכיפת חוק משטרתיים הפועלים למול גורמים חשודים בפלילים. עמדת הצוות היא שלא ניתן להתייחס למונח "רוגלה" כאל סוגיה אחידה. קיים ספקטרום רחב של היקף היכולות הקיימות לכל מערכת. מכאן שלא ניתן לקבל עמדה השוללת כל פעולה של האזנת סתר הדורשת חדירה למחשבים או טלפונים ניידים (להלן גם – **מכשיר קצה**) לצורך ביצוע האזנה. אלא יש לבחון כל אמצעי להאזנת סתר לגופו.

לצד האמור, השאלה המשפטית לעניין הסמכות מכוח חוק האזנת סתר להתקנת אמצעי להאזנת סתר על מכשיר טלפון, היא שאלה המעוררת סוגיות משפטיות כבדות משקל וזו נבחנה בנפרד כמפורט בהרחבה בנספח המשפטי. עמדת היועצת המשפטית לממשלה, לאחר שהובאה בפניה עמדת המשנה ליועצת המשפטית לממשלה (משפט פלילי) וצוותה, היא כי ניתן לפרש את חוק האזנת סתר ככזה המתיר חדירה למכשיר טלפון לצורך התקנת אמצעי לביצוע האזנת סתר בכפוף לתנאים ולמגבלות נוקשות המפורטות שם, ובכלל זה, בין היתר, שימוש במערכת בה מנוטרל טכנולוגית כל חשש לחריגה מגבולות סמכות המשטרה לפי החוק.

מובן כי הסוגיה העקרונית ביחס לשימוש ברוגלות, ובפרט מערכת פגסוס, מעוררת שיח ער ונוקב ברחבי העולם. לכך יש להוסיף כי מדינות שונות מסדירות סוגיות הנוגעות לענייננו באופן מפורש בחקיקה, כגון בריטניה וצרפת[1]. משום כך, נדרשת בחינה זהירה באשר לסמכויות המשטרה בהקשר זה.

---

[1] בצרפת: Code de Procédure Pénale [C. Pr. Pén.]; בבריטניה: Investigatory Powers Act (2016).

צוות הבדיקה ממליץ כי נוכח הממצאים שעלו בבדיקה, וכן העמדה המשפטית המפורטת בנספח, המשטרה תהיה רשאית לעשות שימוש במערכות להאזנה לתקשורת בין מחשבים של טלפונים ניידים אשר כוללות הדבקה של מכשיר הטלפון. ואולם מאחר שחוק האזנת סתר לא נדרש במפורש לשאלה זו, מתחייבת זהירות ביחס לאמור ובחינת כל מערכת מחייבת דקדוק קפדני ביחס לגבולותיה. השימוש יהיה אפשרי בכפוף לקיומם של תנאים מצטברים שיבטיחו שימוש זהיר ומידתי בסמכות, ובכלל זה:

(א) יש לוודא כי יבוצעו כל החסימות הטכנולוגיות הנדרשות בכלל המערכות שבידי משטרת ישראל על מנת להבטיח כי אלו מבצעות אך ורק האזנת סתר כפי שהותר בחוק.

(ב) נוסף על כך, יש להבטיח כי השימוש במערכות יהיה בכפוף לקיומם של נהלים ברורים אשר יאושרו על ידי הייעוץ המשפטי לממשלה תוך אפשרות אפקטיבית לפעולות פיקוח המבוססת על דוחות שיופקו מבסיס הנתונים.

(ג) יש לבחון האם יש מקום להטיל מגבלות או תנאים מיוחדים להגשת בקשות להאזנת סתר לגבי יכולות מסוימות במקרים פרטניים.

(ד) פיקוח פרטני הדוק של משטרת ישראל, תוך פיקוח מוגבר לגבי השימוש במערכת במסגרת הדיווחים העתיים ליועצת המשפטית לממשלה לפי סעיף 6(ו)

תיקון חוק האזנת סתר: מבלי לגרוע מהעמדה המשפטית לפיה יש סמכות להתקין אמצעי להאזנת סתר על מכשיר קצה, אין ספק שקיים צורך ממשי לערוך תיקוני חקיקה לחוק האזנת סתר על מנת להתאימו למציאות הטכנולוגית של היום. חוק האזנת סתר תוקן בשנת 1995 לעניין תקשורת בין מחשבים, ואין חולק כי באותה עת לא ניתן היה להידרש לכלל ההיבטים הייחודיים הנובעים מהתפתחותה של הטכנולוגיה מאז. נדרשת חקיקה עדכנית, אשר תסדיר באופן רוחבי סוגיות של מעקב בעידן הדיגיטלי. על חקיקה זו להסדיר בברור את גבולות הסמכות והפעלתה, בשים לב למאפיינים הייחודיים של הפגיעה בפרטיות במקרים אלו.

נוסף על דוח זה המפורסם לציבור, מוגש דוח חסוי ליועצת המשפטית לממשלה הכולל פרטים רגישים הנוגעים לשיטות עבודה ואמצעים של משטרת ישראל ולסודות מסחריים של החברות. פרט לאלה, כלל ממצאי צוות הבדיקה מפורטים בדוח זה.

יצוין כי במקביל למינוי הצוות, הודיע מבקר המדינה מר מתניהו אנגלמן, כי בין היתר יבדוק את השימוש של גורמי אכיפת החוק במערכת. ממצאי הצוות יועברו למבקר המדינה.

1. מבוא

1.1 הקמת צוות הבדיקה

ביום 31 בינואר 2022 מונה על ידי היועץ המשפטי לממשלה (דאז), צוות בראשות המשנה ליועצת המשפטית לממשלה (משפט פלילי), עו״ד עמית מררי, לבדיקת האזנות סתר לתקשורת בין מחשבים (להלן – **צוות הבדיקה או הצוות**). הצוות הוקם נוכח טענות שעלו בסדרת פרסומים בעיתון ״כלכליסט״ על אודות שימוש לא חוקי של משטרת ישראל באמצעים לביצוע האזנת סתר לטלפונים סלולריים, ומכח הסמכות הנתונה ליועץ המשפטי לממשלה לפיקוח על האזנות סתר שמבצעת משטרת ישראל לפי סעיף 6(ו) לחוק האזנת סתר, התשל״ט-1979. כחברים בצוות מונו שני ראשי אגפים בדימוס בשירות הביטחון הכללי, מר צפריר כץ, שעמד בראש האגף הטכנולוגי של שירות הביטחון הכללי, ומר איל דגן, שעמד בראש אגף חקירות של שירות הביטחון הכללי.

בסדרת הפרסומים בעיתון ״כלכליסט״ נטען שמשטרת ישראל מבצעת פעולות למעקב טכנולוגי אחר אנשים באמצעות חדירה למכשירי הטלפון שלהם תוך שימוש בתוכנת פגסוס של חברת NSO (להלן – **החברה**) על מנת לדוג מידע מודיעיני ללא קשר לחקירה מתנהלת או לברור חשדות לביצוע עבירות פליליות, וממילא מבלי שהתקבל צו שיפוטי. עוד נטען, כי בעת ביצוע האזנת הסתר לתקשורת בין מחשבים של טלפונים ניידים, מתקבל מידע אשר חורג מהמותר על פי חוק האזנת סתר. בהמשך לכך, ביום 7 בפברואר 2022 פורסמה רשימת שמות אנשים שנטען לגביהם כי משטרת ישראל חדרה לטלפונים הניידים שלהם ושאבה מהם מידע ללא צו בית משפט.

טענות אלה נוגעות בליבת שלטון החוק במדינה דמוקרטית, וככל שיש בהן ממש, פוגעות פגיעה חמורה במרחב הפרטיות הנתון לכל אדם בה. בטענות אלה יש כדי לערער את אמון הציבור במשטרת ישראל, גוף האכיפה המרכזי במדינה האמון על שמירה על שלטון החוק, וברשויות האכיפה בכלל.

בעקבות בירור ראשוני שנערך עם המשטרה עלה כי בעת השימוש במערכת נקלטים חומרים מעבר לאלה שהוצגו תחילה ליועץ המשפטי לממשלה עם פרסום הכתבות. לפיכך ביום 31 בינואר 2022, עם הקמת צוות הבדיקה, הנחה היועץ המשפטי לממשלה דאז את משטרת ישראל להשעות את השימוש במערכת, וזאת עד שייקבע על ידי היועץ המשפטי לממשלה או מי מטעמו כי אין מניעה לשוב ולהשתמש בה. משכך הפסיקה המשטרה את השימוש במערכת.

בעקבות הפרסום מיום 7 בפברואר 2022, התבקש הצוות לבחון בשלב ראשון האם בוצעה חדירה למכשירי טלפון ניידים השייכים אל מי מבין רשימת האנשים שפורסמו, באמצעות תוכנת פגסוס שבשימוש משטרת ישראל, המכונה במשטרה סייפן (להלן גם – **סייפן**), וזאת ללא צו שיפוטי המתיר זאת.

לצורך בדיקת הטענות ובהתאם לכתב המינוי צוותו לצוות הבדיקה עובדי שירות הביטחון הכללי והמוסד למודיעין ולתפקידים מיוחדים, המומחים בתחום הטכנולוגיה הרלוונטית. יודגש כי המומחים לא פעלו כנציגי הגופים בהם הם מועסקים ולא הונחו על ידם. צוות הבדיקה, בסיועם של המומחים הטכנולוגיים, ערך בדיקה טכנולוגית יסודית וממוקדת של מספרי הטלפון של רשימת האנשים אל מול נתונים הנמצאים בבסיס הנתונים הפנימי של המערכת אשר לא ניתן לשינוי או למחיקה ואשר משקף את הפעולות שבוצעו באמצעות המערכת (Audit Log). המערכת מותקנת

במתקני משטרת ישראל, ואולם גישה לשכבה זו מחייבת ידע טכני כמו גם נתוני אימות שמצויים ברשות החברה ולא בידי המשטרה. מכאן שבסיס הנתונים הפנימי של המערכת אינו זמין למשתמש, ויכול להיות מונגש על ידי חברת NSO בלבד.

ביום 21 בפברואר 2022 פורסמו ממצאי הבדיקה שביצע הצוות ביחס לרשימת האנשים שהתפרסמה ואשר נטען לגביהם כי המשטרה הדביקה את הטלפונים הניידים שלהם ללא צו בית משפט. הבדיקה העלתה כי אין כל אינדיקציה לכך שמשטרת ישראל הדביקה באמצעות מערכת פגסוס שבידיה, ללא צו שיפוטי, מכשיר טלפון נייד של מי מבין רשימת האנשים שפורסמו בתקשורת. כמו כן, נבדקה מערכת נוספת שבידי משטרת ישראל, ולא היו כל אינדיקציות להדבקות או ניסיונות הדבקה אל מי מבין רשימת האנשים האמורה (להרחבה ראו נספח א').

לאחר פרסום הממצאים הראשונים כמפורט לעיל, המשיך צוות הבדיקה בבדיקה מעמיקה ומקיפה של הסוגיות הנוגעות להאזנת סתר לתקשורת בין מחשבים במשטרת ישראל, בין היתר לאור הטענות שפורסמו בתקשורת.

בשלב זה מטרות הצוות היו לבחון את הסוגיות שלהלן:

1. בדיקה רוחבית ומעמיקה בנוגע לטענה כי משטרת ישראל חודרת לטלפונים ניידים ללא צו בית משפט ושואבת את תוכנם.
2. בדיקה של מערכות האזנת סתר לתקשורת בין מחשבים של טלפונים ניידים, שבשימוש משטרת ישראל, על מנת לבחון האם הן עומדות בתנאים של חוק האזנת סתר.
3. בחינת התמונה המוצגת על ידי המשטרה לבתי המשפט בכל הנוגע להאזנה לתקשורת בין מחשבים של טלפונים ניידים, בדגש על נוסח הצווים המוגשים לבתי המשפט.
4. בחינת הליך שרשרת ההאזנה של האזנות סתר לתקשורת בין מחשבים של טלפונים ניידים במשטרת ישראל.
5. בחינת הליכי פיקוח ובקרה לעניין אופן הפעלת אמצעים להאזנה לתקשורת בין מחשבים של טלפונים ניידים בכלל ומערכת סייפן בפרט.
6. בחינה כללית של הליכי האישור המשפטי בנוגע לשימוש במערכות טכנולוגיות לשם ביצוע האזנת סתר לתקשורת בין מחשבים של טלפונים ניידים, על ידי הייעוץ המשפטי למשטרה והייעוץ המשפטי לממשלה, על מנת להתוות עקרונות ודרכי פעולה לעתיד.

יובהר כי לצוות הבדיקה לא היו נתונות סמכויות חקירה מכוח הדין. על פי כתב המינוי של הצוות, ככל שתמצא התנהלות פסולה שיש בה חשד לעבירה פלילית, הטיפול בעניין יועבר לרשויות המוסמכות על-פי דין.

בדיקת הצוות ביחס לטענות בדבר האזנה ללא צו בית משפט וקבלת מידע החורג מהסמכויות על פי דין, הסתמכה בין היתר על בדיקת המערכות הטכנולוגיות ובדיקת אופן השימוש בהן אשר מבוססת על נתונים שהתקבלו מבסיס הנתונים של מערכות שהן בפיתוח של חברות פרטיות, זאת על מנת לקבל תמונה אובייקטיבית שלמה ומקיפה ככל הניתן בדבר השימוש בהן. עוד נסמכה הבדיקה על פגישות עם גורמים רלוונטיים, בדיקות של צווי בית משפט וביקורים ביחידות המשטרתיות הרלוונטיות, כפי שיפורט בהרחבה בהמשך.

יצוין כי לאורך כל תקופת עבודתו של צוות הבדיקה, משטרת ישראל שיתפה עימו פעולה בפתיחות מלאה ואפשרה לצוות, למומחים הטכנולוגיים ולגורמים הנוספים שסייעו בידו להיחשף למערכות הטכנולוגיות, לקיים מפגשים עם בעלי התפקידים הנוגעים בדבר, וכן העמידה לרשותו את כל המידע שהיה בידיה.

את עבודת הצוות ריכזה עו״ד אפי טפליץ. השתתפו בדיוני הצוות באופן קבוע עו״ד גבריאלה פיסמן, ראשת אשכול סמכויות שלטוניות, עו״ד אסתר זנזורי-פריאל, עוזרת למשנה ליועצת המשפטית לממשלה (משפט פלילי) ועו״ד רותם רייבי, כולן מהמחלקה למשפט פלילי בייעוץ וחקיקה במשרד המשפטים. כמו כן סייעה לעבודת הצוות באופן צמוד, הגב׳ טל דעבול, סטודנטית למשפטים העובדת במחלקה. בנוסף, המומחים הטכנולוגים המשיכו לסייע לצוות בתחום הטכנולוגי לאורך כל עבודתו.

1.2 פירוט הישיבות והדוברים שהופיעו בפני צוות הבדיקה

עבודת הצוות כללה מאות שעות של עבודה. מאז מונה הצוות ועד למועד פרסום הדוח התקיימו כ-50 ישיבות צוות שחלקן ארכו ימים שלמים. כמו כן, הגורמים שסייעו לצוות הבדיקה הגיעו באופן תדיר למטה חטיבת הסייבר לבדיקות שנמשכו מספר חודשים.

צוות הבדיקה קיים ישיבות רבות עם גורמים שונים במשטרת ישראל בעבר ובהווה, בין היתר נפגש הצוות עם גורמים מהייעוץ המשפטי למשטרה ומהייעוץ המשפטי לחטיבת הסייבר; מנהלי חטיבת הסייבר; גורמים במחלקת התעצמות בחטיבת הסייבר האחראים בין השאר על הכוונה מקצועית; גורמים במחלקת טכנולוגיות בחטיבת הסייבר האמונים על הפעלת הכלים להאזנת סתר מסוג תקשורת בין מחשבים; גורמים במחלקת מ״מ (מקורות מיוחדים) בחטיבת הסייבר האחראים על התכלול בין היחידה בשטח לבין חטיבת הסייבר בכל הנוגע לבקשות להאזנות סתר מסוג תקשורת בין מחשבים, כתיבת פקודות המבצע והפקת התוצרים של האזנות סתר מסוג תקשורת בין מחשבים; גורמים אשר היו מועסקים על ידי משטרת ישראל ופיתחו מערכות להאזנת סתר שהיו בשימוש המשטרה בעבר, וכן הגורמים שהיו אחראים על הפעלתם.

מלבד הישיבות שקיים צוות הבדיקה עם גורמים שונים במשטרה, קיים הצוות בדיקות טכנולוגיות בחטיבת הסייבר על מנת להכיר ולבחון לעומק את היכולות הטכנולוגיות של המערכות שבידי משטרת ישראל ועמדות ההפקה שלהן. כמו כן ביקר הצוות בימ״ר שבו מוצבת אחת מעמדות ההפקה של מערכת סייפן.

צוות הבדיקה נפגש גם עם מנהל מחלקת הסייבר בפרקליטות המדינה, ד״ר חיים ויסמונסקי, וכן עם עו״ד רביד דקל, ראש אשכול לשעבר במחלקה למשפט פלילי בייעוץ וחקיקה שהייתה אמונה על נושאי האזנות הסתר.

כחלק מבחינת מאפייני המערכות שבידי משטרת ישראל אשר בפיתוח חברות פרטיות, נפגש צוות הבדיקה עם נציגים של חברת NSO בכל הנוגע למאפייני מערכת סייפן, ועם נציגי החברה הנוספת (להלן יחד – **החברות**) שמערכת בפיתוחה נמצאה טרם הקמתו של הצוות בשימוש בשלבי פיילוט במשטרה. יודגש כי נציגי החברות שיתפו פעולה עם צוות הבדיקה והיו זמינים לכל שאלה או הבהרה בדבר המערכות שהתבקשו על ידי צוות הבדיקה.

ביחס לטענות שפורסמו על ידי עיתון "כלכליסט", נפגש צוות הבדיקה עם עורכת העיתון, הגב' גלית חמי, וכן עם סגן העורכת מר אמיר זיו.

באשר לסוגיות העקרוניות המתעוררות בעניין הפעלת רוגלות, הצוות קיים סדרת ישיבות שבמהלכן שמעו חבריו גורמים שונים הרלוונטיים לנושא:

- הסנגוריה הציבורית – עו"ד גיל שפירא ועו"ד יגאל בלפור.
- הרשות להגנת הפרטיות – עו"ד גלעד סממה, ראש הרשות להגנת הפרטיות, עו"ד ראובן אידלמן, היועץ המשפטי, עו"ד ניר גרסון, סגן היועץ המשפטי ועו"ד אפרת חושן, הממונה על החקירות הפליליות.
- האגודה לזכויות האזרח בישראל – עו"ד אבנר פינצ'וק ועו"ד גיל גן-מור.
- המכון הישראלי לדמוקרטיה – ד"ר תהילה אלטשולר ועו"ד עמיר כהנא.
- פרופ' אמנון רייכמן, אוניברסיטת חיפה.

כחלק מבחינת סוגיות הנוגעות למעמד היועץ המשפטי למשטרה ותפקידו, ולדפוסי העבודה מול הייעוץ המשפטי לממשלה, התקיימה לבקשת הצוות פגישה מקצועית עם כב' השופט בדימוס פרופ' יצחק זמיר, אשר כיהן בתפקיד היועץ המשפטי לממשלה בין השנים 1978-1986 וכשופט בית המשפט העליון בין השנים 1994-2001.

נוסף על דוח זה המפורסם לציבור, מוגש ליועצת המשפטית לממשלה דוח חסוי הכולל פרטים רגישים הנוגעים לשיטות עבודה ואמצעים של משטרת ישראל וכן לסודות מסחריים של החברות. פרט לאלה, כלל ממצאי צוות הבדיקה מפורטים בדוח זה.

יצוין כי במקביל למינוי הצוות, הודיע מבקר המדינה, מר מתניהו אנגלמן, כי בין היתר יבדוק את השימוש של גורמי אכיפת החוק במערכת. ממצאי הצוות יועברו למבקר המדינה.

תודות

לא יכולנו לעמוד במשימה המורכבת שהוטלה עלינו ללא הסיוע והליווי המקצועי של הצוות ממחלקת ייעוץ וחקיקה (משפט פלילי) ושל המומחים הטכנולוגים. אנחנו מבקשים להודות ולבטא את הערכתנו הרבה אליהם. השילוב של מקצועיות מהמעלה הראשונה יחד עם מחויבות ומסירות אין קץ שלהם תרמו תרומה משמעותית לעבודת הצוות.

תודה מיוחדת לעו"ד אפי טפליץ, אשר ריכזה את עבודת הצוות ואת גיבוש הדוח במקצועיות, במסירות וביעילות והתעמקה באופן יוצא דופן בכלל הפרטים הטכניים והמשפטיים המורכבים של הסוגיה.

2. רקע נורמטיבי

2.1 חוק האזנת סתר – רקע כללי

האזנת סתר מהווה כלי מרכזי למלחמה בפשיעה חמורה. אמצעי זה, ובכלל זה אמצעי להאזנת סתר לתקשורת בין מחשבים, מהווה לא פעם חוליה הכרחית ומרכזית במסגרת סמכויות החקירה השונות לצורך מניעת עבירות פשע וחקירתן. כפי שהעולם בכללו עבר לביצוע פעולות רבות במרחב המקוון, כך גם תקשורת בין גורמי פשיעה פועלת במרחב זה. מכאן שעל אף היותה של האזנת סתר אמצעי הפוגע בליבת הפרטיות של אדם, אין ספק כי זו נדרשת למשטרה לצורך מימוש תפקידה לשמור על שלום הציבור וביטחונו.

בשים לב לכך, חוק האזנת סתר, התשל"ט-1979 (להלן – **חוק האזנת סתר** או **החוק**), נועד מצד אחד לעגן בחקיקה את ההגנה מפני חדירה לצנעת הפרט הנגרמת מהאזנה לשיחותיו ללא ידיעתו, ולהבטיח את ההגנה על ידי קביעת עבירה פלילית ספציפית של האזנה אסורה, ומן הצד השני - להסדיר את ההליכים להאזנה כשזו מחויבת מטעמים של ביטחון המדינה או מטעמים של מניעת עבירות וגילוי עבריינים.[2] נוכח תכלית זו, החוק קובע עבירה פלילית בגין האזנת סתר לשיחת הזולת כאשר לא ניתנה הסכמת אף אחד מבעלי השיחה, אך לצד זאת קובע חריגים לאיסור, המתירים לגורמי אכיפת החוק לבצע האזנות סתר בנסיבות שבהן הפגיעה בזכות לפרטיות מוצדקת לשם הגנה על הציבור או על ביטחון המדינה. ביסוד ההסדר הקבוע בחוק האזנת סתר עומד אפוא האיזון בין זכותו החוקתית של היחיד לפרטיות אשר היא מהחשובות שבזכויות האדם במדינה דמוקרטית והוכרה בישראל כזכות יסוד חוקתית בחוק יסוד: כבוד האדם וחירותו, לבין חובתן של הרשויות להגן על הציבור מפני פשיעה ופגיעה בביטחון המדינה.

הוראות חוק האזנת סתר מגלמות את התפישה כי האזנה לסוד שיחו של אדם מהווה פגיעה חמורה ביותר בפרטיותו, ועל כן קבועים הסדרים נוקשים לקבלת היתר להאזנת סתר, הן בהיבט המהותי והן בהיבט הפרוצדורלי. לעניין מידת הפגיעה בפרטיות הגלומה בהאזנת סתר ואיזונה מול תכליות אחרות יפים דבריו של בית המשפט העליון בע"פ 1302/92 **מדינת ישראל נ' נחמיאס** (21.6.1995):

> "האזנת סתר היא התערבות חריפה בזכותו של אדם להיות עם עצמו. היא מהווה חדירה קשה לפרטיותו של האדם. היא שוללת מהאדם את מנוחת נפשו, את ביטחונו בחופש רצונו. היא הופכת את מבצרו לכלאו. עם זאת הזכות לפרטיות אינה מוחלטת. ניתן לפגוע בה לשם מניעת עבירות, אשר סופן הגנה על הפרטיות של אחרים, ועל כבודם וחירותם."[3]

כך גם עולה מפסק הדין שניתן לאחרונה בעניין **אטיאס**:[4]

> "האזנה לסוד שיחו של אדם, מבלי שידע על כך, פוגעת קשות בהגנה על המרחב הפרטי שלו, באוטונומיה שלו להחליט לחשוף על דעת עצמו פרטים על אודותיו עם אחרים, בצנעת הפרט ואף בצדדים שלישיים, ששיחותיהם נקלטות ללא ידיעתם וללא הסכמתם [...]. החשש מפני פגיעה בפרטיות גובר שבעתיים נוכח האמצעים הטכנולוגיים הקיימים המשמשים לביצוע האזנות סתר, בין אם בדרך של האזנה לטלפון נייד או קווי ובין אם בדרך של "האזנת נפח". [...]

[2] דברי ההסבר להצעת חוק דיני העונשין (האזנת סתר), התשל"ח-1978.
[3] ראו עמ' 353 לפסק הדין של המשנה לנשיא ברק (כתוארו דאז).
[4] רע"פ 1089/21 **מדינת ישראל נ' אטיאס** פסקאות 25-26 לפסק הדין של השופט אלרון (14.3.2022).

> נוכח הפגיעה בפרטיות הנלווית לביצועה של האזנת סתר, ביצועה מותר רק מקום בו הדבר נועד לשמירה על אינטרס ציבורי כבד משקל. תכליתו של החוק, היא ליצור מערכת משולבת ומתואמת של הוראות המאזנת כראוי בין הצורך להגנה על שלום הציבור, מניעת עבריינות ושמירה על ביטחון המדינה, לבין הגנה על הפרטיות (ע"פ 639/79 אפללו נ' מדינת ישראל, פ"ד לד(3) 561, 570 (1980))."[5]

יצוין כי מידת הפגיעה בפרטיות הנובעת מהאזנת סתר מקבלת משנה תוקף כאשר מדובר בהאזנה לתקשורת בין מחשבים, בעידן שבו התקשורת בין אנשים על סוגיה השונים והמתפתחים, הלכה למעשה, מתקיימת כמעט כולה במרחב המקוון. למעלה מכך, מאפייניהם הייחודיים של טלפונים חכמים, והיקף השימוש שנעשה בהם בחיי היומיום עשויים להוביל לפגיעה חריפה בפרטיותו של אדם בהשוואה להאזנת השמע "המסורתית", ולא ניתן להמעיט במשמעות ובהשלכות של חשיפה להיקף ולסוג תכנים אלה. ראו לעניין מאפייניו הייחודיים של חומר מחשב, דבריו של כב' השופט עמית בעניין **פישר**:[6]

> "מאפיין נוסף של חומר מחשב, לרבות הטלפון הנייד, הוא שניתן לדלות ממנו חומרים אובייקטיביים מזמן אמת, ראיות עוצמתיות שיכולות לשרת הן את התביעה והן את ההגנה. אך פוטנציאל ראייתי זה הוא בבחינת אליה וקוץ בה. מדובר בחומר רב שדרכו ניתן ללמוד גם על "סיפור חייו" של המשתמש. למעשה לא מדובר רק בסיפור חיים המשורטט בקווים כלליים, אלא בפרטי הפרטים של חיי היומיום של האדם – מקומו בבוקר ועד לכתו לישון דרך המקומות בהם שהה, האנשים עימם שוחח ותכני השיחה ("סוד השיח"), רעיונות, הגיגים, תחביבים, חברים, ידידים, מידע אינטימי ומידע עסקי, תחומי עניין וסקרנות (האתרים אליהם גולש המשתמש) ועוד [...].

יודגש כי הדברים האמורים לעיל בעניין **פישר** נוגעים לסמכות החיפוש במחשב ביחס לכלל המידע האגור בו ולא להאזנת סתר, ואולם המאפיינים הייחודיים של חומר מחשב, ובפרט ביחס לטלפון נייד, רלוונטיים, בשינויים המחויבים, גם בכל הנוגע להאזנת סתר לתקשורת בין מחשבים.[7] ראו הרחבה מטה לעניין ייחודה של האזנת סתר.

---

5 ראו גם בג"ץ 5207/04 **אפל נ' היועץ המשפטי לממשלה** פסקה 7 לפסק הדין של השופטת פרוקצ'יה (20.5.2007): "[...] חוק האזנת סתר מגלם בתוכו איזון בין שני אינטרסים מתנגשים: מצד אחד, ניצב אינטרס קידום ההליך הפלילי באמצעות השגת ראיות נגד חשודים בביצוע פשעים, ולצורך מלחמה בעבריינות; מצד שני, עומד אינטרס ההגנה על הפרטיות ועל צנעת חייו של האדם, שהאזנת הסתר פולשת לחייו הפרטיים, וחודרת גם לפרטיות צדדים שלישיים, ששיחותיהם משתלבות בהאזנה בלי ידיעתם ובלי הסכמתם. חוק האזנת סתר טומן בחובו איזון בין הצורך להגן על הפרט מפני התערבות בצנעת חייו על ידי האזנה לשיחותיו ללא רצונו וללא ידיעתו, לבין צרכי החברה בקיום אמצעי האזנת הסתר בשל שיקולים של מלחמה בפשע."

[6] בש"פ 6071/17 **מדינת ישראל נ' פישר**, פס' 10 (27.8.2017). ראו גם דברי בית המשפט העליון בדנ"פ 1062/21 **אוריך נ' מדינת ישראל** (11.1.2022), בכל הנוגע לחיפוש במחשב, ובשינויים המחויבים, בהבדל בין סמכות החיפוש בכל המידע האגור בפלאפון לבין האזנה לתקשורת בין מחשבים בתקופת זמן מסוימת צופה פני עתיד: "[...] מאפייניהם הייחודיים של מכשירים אלה יש בהם כדי להשפיע על הפרשנות הראויה לסעיף 23א לפקודה. חדירה למחשב או לטלפון החכם יכולה לחשוף נפח עצום של פרטים מתוך סיפור חייו של אדם; עובדה זו, בצירוף היכולות הטכנולוגיות שבאמצעותן ניתן להרכיב פרופיל שלם לגבי אדם תוך שימוש במידע המצוי במכשירים אלה, מוליכות אל המסקנה שפוטנציאל הפגיעה בפרטיות עקב חיפוש במחשב הוא, במקרים רבים, גבוה לאין שיעור בהשוואה לחיפוש "המסורתי" בחצרו או בכליו של אדם, והוא נוגע גם לצדדים שלישיים רבים שחייהם נקשרו בצורה כזו או אחרת – ולו לרגע – עם המחזיק במחשב או בטלפון החכם..." (ראו פסקה 29 לפסק הדין של כב' הנשיאה חיות). עוד ראו דבריו של השופט אלרון בעניין **אוריך**: "מאז תוקן סעיף 23א(ב) לפקודת החיפוש בשנת 2005 ועד היום, התחדדה עוד יותר החשיבות של עריכת איזון עדין ומדויק בין הצורך לבצע חיפושים במחשבים לשם קידום חקירות פליליות, לבין הזכות לפרטיות של בעל המחשב ואלו הנמנים עם מעגליו החברתיים. זאת, מאחר שהשימוש במחשבים – ובפרט במכשירי טלפון ניידים חכמים – הפך לנפוץ במיוחד. מכשירים אלו מצויים כעת בידיו של כמעט כל אדם, ואוצרים בחובם מידע בלתי נדלה על בעל המכשיר והקרובים לו. באמצעות מחשבו ומכשיר הטלפון הנייד החכם של אדם ניתן לא פעם ללמוד על עברו ועל תכניותיו לעתיד, כמו גם על תחביביו, לבטיו, רחשי ליבו, מכריו, אהוביו ושונאיו. מקומות בהם שהה מתועדים עם ציון גיאוגרפי מדויק, לעיתים בליווי תמונות, ונאגרים מידי יום במכשיריו ובחשבונותיו במרשתת; ובמקרים רבים, סודותיו וסודות חבריו שמורים במכשיר הטלפון החכם או במחשב שברשותו." (ראו פסקה 4 לפסק הדין של כב' השופט אלרון).

[7] לעניין ההבחנה בין חיפוש במחשב לבין האזנת סתר ראו בהמשך.

אל מול הפגיעה החמורה בזכות החוקתית לפרטיות הנובעת מהאזנת סתר, הכיר המחוקק באינטרסים נוספים אשר עומדים כנגדה. האיזון בין הזכות לפרטיות של החשוד ושל צדדים שלישיים, לבין האינטרס הציבורי בהגנה על ביטחון הציבור עובר כחוט השני בהוראותיו של חוק האזנת סתר. במסגרת כך, חוק האזנת סתר קובע תנאים בהם רשות ביטחונית תהא מוסמכת לבצע האזנת סתר כשהדבר דרוש מטעמי ביטחון המדינה,[8] ותנאים בהם משטרת ישראל תהא מוסמכת לבצע האזנת סתר כשהדבר דרוש למניעת עבירות ולגילוי עבריינים.[9]

סמכות המשטרה לבצע האזנת סתר מוסדרת בסעיף 6 לחוק. היתר להאזנת סתר ניתן על ידי נשיא בית משפט מחוזי או סגן נשיא שהסמיכו הנשיא לעניין זה, לפי בקשתו של קצין משטרה מוסמך, אם שוכנע – לאחר ששקל את מידת הפגיעה בפרטיות – שהדבר דרוש לגילוי, לחקירה או למניעה של עבירות מסוג פשע, או לגילוי או לתפיסה של עבריינים שעברו עבירות כאמור, או לחקירה לצרכי חילוט רכוש הקשור בעבירה שהיא פשע.

בהיתר להאזנת סתר יש לתאר את זהות האדם אשר האזנה לשיחותיו הותרה, או זהות הקו או המיתקן המשמשים או המיועדים לשמש לקליטה, להעברה או לשידור של בזק, ואשר האזנה אליהם הותרה ומקום השיחות או סוגן, הכל אם הם ידועים מראש. כמו כן, יש לפרט את דרכי ההאזנה שהותרו,[10] ותקופת תקפו של ההיתר, אשר לא תעלה על 3 חודשים מיום מתן ההיתר.[11]

אל הוראות אלו מתווספות ההוראות המשלימות הקבועות בתקנות האזנת סתר (בקשה להיתר האזנה), התשס"ז-2007, הקובעות את סדרי הדין בדיון בבקשה להאזנת סתר והפרטים שיש לכלול בבקשה ובהיתר להאזנה (ראו הרחבה בהמשך).

בכל הנוגע לבסיס העובדתי והשיקולים שיש לשקול בעת מתן היתר להאזנה, בהתאם לע"פ 2286/91 **מדינת ישראל נ' אילוז** (31.7.1991), אין להתיר האזנה בעלמא ללא קיומו של בסיס ראשוני רק כדי לדוג אחר מידע, אלא על בית המשפט להשתכנע, בהתבסס על המידע המובא בפניו, כי אכן יש צורך אמיתי בנקיטת האמצעי מרחיק הלכת של פגיעה בצנעת הפרט, כדי למנוע עבירה או לגילוי העבריין. כל זאת, בין היתר, בשים לב לחומרת העבירה. לצורך כך, על המשטרה להקפיד בתיאור מדויק של נתוני היסוד במסגרת הבקשה להאזנת סתר, הן בפרטים התמציתיים שנרשמים בטופס והן בדיון בעל פה בפני בית המשפט, שכן כל אלה משמשים מצע להפעלת שיקול הדעת על ידי השופט.

לשלמות התמונה יצוין כי לפי סעיף 7 לחוק, למפכ"ל משטרת ישראל סמכות לתת היתר להאזנת סתר לשם מניעת פשע או גילוי מבצעיו, אם יש צורך בהאזנת סתר שאיננה סובלת דיחוי, ולא ניתן לקבל בעוד מועד היתר מבית משפט. משך תוקפו של היתר כאמור לא יעלה על 48 שעות. על המפכ"ל להודיע מיד ליועצת המשפטית לממשלה על היתר שניתן, ולה נתונה הסמכות לבטל את ההיתר.

האזנת סתר לשיחה ברשות הרבים איננה טעונה היתר (בכפוף לתנאים הקבועים בסעיף 8 לחוק), כאשר לעניין זה רשות הרבים היא מקום שאדם סביר יכול היה לצפות ששיחותיו יישמעו ללא הסכמתו, וכן מקום שבו מוחזק אותה שעה עצור או אסיר.[12]

---

[8] ראו פרק ב' לחוק.
[9] ראו פרק ג' לחוק.
[10] סעיף 6(ד) לחוק האזנת סתר.
[11] סעיף 6(ה) לחוק; ההיתר ניתן לחידוש מפעם לפעם.
[12] סעיף 8(1) לחוק.

ביחס להליכי פיקוח ובקרה של היועצת המשפטית לממשלה, לפי סעיף 6(ו) לחוק על המפכ״ל להגיש מדי חודש דין וחשבון ליועץ המשפטי לממשלה על היתרי האזנת סתר שניתנו ועל תנאיהם. אם כן, לפי החוק, על היועצת המשפטית לממשלה לערוך פיקוח בדיעבד על האזנות סתר פרטניות שבוצעו. במסגרת הדיווח העיתי שמועבר ליועצת המשפטית לממשלה מפורטים העבירה שביסוד הבקשה להאזנה שהוגשה; זהותו של האדם שביחס אליו בוצעה ההאזנה;[13] סוג ההאזנה שבוצעה (למשל האזנת שמע לטלפון נייד); משך ההיתר שניתן על ידי בית המשפט; תמצית הנימוקים להאזנה שהוצגו בפני בית המשפט והחלטת בית המשפט (ראו בהרחבה בפרק 6).

נוסף על תפקידה של היועצת המשפטית לממשלה לבצע פיקוח ובקרה בדיעבד המוסדר בסעיף 6(ו) לחוק, המחוקק קבע נסיבות מסוימות בהן על המשטרה לקבל אישור של היועצת המשפטית לממשלה או של פרקליט המדינה בטרם פניה לבית משפט להוצאת צו האזנת סתר מסוים, למשל בכל הנוגע לבקשה להאזנה לשיחות חסויות לפי סעיף 9א לחוק,[14] או לפי סעיף 2א לחוק חסינות חברי כנסת, התשי״א -1951 כאשר מבוקש להאזין לחבר כנסת, שר או סגן שר.

שלא בשולי הדברים יצוין כבר בשלב זה, כפי שיפורט בהמשך בפרק 10 לדוח, כי מעורבות גורמי הייעוץ המשפטי לממשלה בנושא האזנות סתר אינה מוגבלת אך לפיקוח הנובע מקבלת הדיווח בהתאם לחוק. במסגרת מערכת היחסים השוטפת עם משטרת ישראל, כפי שאף נהוג אל מול יתר רשויות השלטון, מובאות על ידי הייעוץ המשפטי למשטרה סוגיות המעוררות שאלה משפטית מורכבת או השלכות רוחב הדורשות את עמדת הייעוץ המשפטי לממשלה. דיון בסוגיות משפטיות עשוי אף להתעורר באופן יזום על ידי גורמי הייעוץ המשפטי לממשלה ככל שסוגיות אלו מובאות לידיעתם בדרך אחרת, כגון בפניית ציבור או בפרסום בתקשורת. לא אחת, נדונות במסגרת זו שאלות משפטיות הנוגעות להיבטים טכנולוגים של הכלים המופעלים לביצוע האזנות סתר ודורשות את עמדת הייעוץ המשפטי לממשלה.

<u>ועדות חקירה קודמות</u>

לסיומו של חלק זה נבקש לציין דוחות נוספים אשר עסקו בסוגיות הנוגעות להאזנת סתר:

- דין וחשבון צוות הבדיקה בנושא האזנות סתר (אפריל 2005) בראשות עו״ד לבנת משיח, המשנה ליועץ המשפטי לממשלה (תפקידים מיוחדים) דאז. דוח זה בחן את הצורך בשינויי חקיקה ונהלים, ובמסגרתו הומלץ, בין היתר, על עיגון נהלים הקשורים בהגשת בקשה להאזנת סתר; קביעת בקרה להאזנות ארוכות; טיוב הבקשות המוגשות לבית המשפט; קביעת נהלים שמטרתם להבטיח ביצוע האזנה לפי המגבלות הקבועות בהיתר; פיתוח מנגנון להטמעת הנהלים; השלמת ההסדר החקיקתי הנוגע להאזנה לשיחות בעלי מקצוע ששיחותיהם חסויות; האזנה בצירוף תיעוד חזותי ועוד. בהמשך לדוח צוות משיח גיבשה המשטרה כ-40 נהלים המסדירים נושאים שונים הקשורים להאזנת סתר, ביניהם נהלים המסדירים האזנות ייחודיות לפי החוק, הפקת התוצרים ועוד. בעקבות ההמלצות גובשה וקודמה הצעת חוק האזנת סתר (תיקון מס׳ 6) התש״ע-2009, שלא הבשילה לכדי חקיקה.

---

[13] ככל שזהותו ידועה מראש. כך למשל יתכן כי בעת הגשת הבקשה להאזנה היה ידוע רק מספר הטלפון שקשור לעבירה אך טרם היה מידע לעניין זהותו של המשתמש באותו מספר טלפון.

[14] אישור כאמור נדרש כאשר מבוקש להאזין לשיחה שהעדות עליה חסויה לפי סעיפים 51-48 לפקודת הראיות [נוסח חדש], התשל״א 1971 (דהיינו שיחה שמתקיימת תוך מתן השירות המקצועי של עורך-דין, רופא, פסיכולוג, עובד סוציאלי וכהן דת).

- דוח בדיקה של כב׳ השופט (בדימוס) שלום ברנר, בנושא העברת תוצרי האזנת סתר בת.פ 5461/06 מ״י נ׳ ח״כ חיים רמון משנת 2007. דוח זה בחן את תהליכי ההעברה לעורכי הדין של ההגנה של תוצרי האזנת הסתר שהיוו חלק מחומר החקירה בתיק הנדון והסיבות שבעטיין חלק מהחומר לא הועבר במועד.
- ועדת החקירה הפרלמנטרית בעניין האזנות סתר משנת 2009. תפקידיה וסמכויותיה של הוועדה כפי שנקבעו בהחלטת הכנסת כללו את בחינת התשתית החוקית והאיזונים שנקבעו בחקיקה בין הזכות לפרטיות לבין אינטרסים ציבוריים אחרים; חקירת סוגיית האזנות הסתר המבוצעות על ידי גורמי אכיפת החוק על כל היבטיה: יישום החוק בידי רשויות החקירה, התביעה ובידי בתי המשפט, לרבות תפיסת ההפעלה, המקצועיות, בעלי התפקידים, מנגנוני הבקרה והתפוקות של מערך האזנות הסתר. בין היתר, דנה הוועדה בנושאים הבאים: ההליך שמתנהל בבית המשפט; אחזקה, ביעור ומחיקה של חומרי האזנה; הקשר שבין צו חיפוש וצו האזנה; הפקת מידע מודיעיני; צו האזנת סתר ותמלול; האזנה לשיחות של בעלי מקצוע; אמצעים טכנולוגיים לביצוע האזנת סתר.
- חוות דעת מבקר המדינה בעניין האזנות סתר בחקירות פליליות משנת 2010. חוות דעת זו עניינה נושא האזנות הסתר בחקירות פליליות, דרכי הביצוע, השימוש בהן ובתוצריהן, נוכח תלונות שנשמעו בנושא זה בשנים שקדמו לכתיבת חוות הדעת. חוות הדעת סוקרת את הליכי ההסדרה של האזנות הסתר בישראל ויישום הנורמות בתחום זה בידי רשויות האכיפה.

2.2 ההגדרות הקבועות בחוק לעניין האזנת סתר לתקשורת בין מחשבים

הגדרת ״האזנת סתר״ קבועה בסעיף 1 לחוק. הגדרה זו חלה הן לעניין העבירה הקבועה בחוק והן לעניין הסמכות הנתונה לגורמים השונים לבצע האזנת סתר. החוק קובע כי האזנת סתר היא האזנה ללא הסכמה של אף אחד מבעלי השיחה, כאשר הגדרה זו מורכבת מכמה רכיבים נוספים המוגדרים בחוק:

> ""שיחה" – בדיבור או בבזק, לרבות בטלפון, בטלפון אלחוטי, ברדיו טלפון נייד, במכשיר קשר אלחוטי, בפקסימיליה, בטלקס, בטלפרינטר או בתקשורת בין מחשבים;
>
> "בעל שיחה" – כל אחד מאלה:
>
> (1) המדבר;
>
> (2) מי שהשיחה מיועדת אליו;
>
> (3) המשדר בבזק;
>
> (4) מי שהמסר המועבר בבזק מיועד להיקלט אצלו;
>
> למעט הנותן שירות של העברת מסר בבזק, למען זולתו או מטעם זולתו;
>
> "האזנה" – האזנה לשיחת הזולת, קליטה או העתקה של שיחת הזולת, והכל באמצעות מכשיר;
>
> "האזנת סתר" – האזנה ללא הסכמה של אף אחד מבעלי השיחה;

"בזק" – סימנים, אותות, כתב, צורות חזותיות, קולות או מידע, המועברים באמצעות תיל, אלחוט, מערכת אופטית או מערכת אלקטרומגנטית אחרת;"

בנוסח החוק המקורי טרם תיקונו, ההגדרה של שיחה הייתה "בדיבור או בדרך תקשורת אחרת". בעת התיקון לחוק בשנת 1995 נוסף, בין היתר, הרכיב של "תקשורת בין מחשבים" להגדרה של שיחה, והובהר כי הסמכות לבצע האזנת סתר כוללת את הסמכות להאזין לתקשורת המועברת בין מחשבים. זאת, מתוך התפיסה כי ההגנה על סוד השיח אינה צריכה להיות תלויה בטכניקה של העברת המסרים.

כמו כן, לאור הכללתן של טכנולוגיות שונות של "שיחה" אשר אינן נוגעות רק לדיבור, שונתה בשנת 1995 ההגדרה של "האזנה" כך שתחול במפורש הן על שמיעת שיחה והן על קליטתה או העתקתה של שיחה.[15]

הגדרה מקובלת למונח מחשב קבועה בחוק המחשבים, התשנ"ה-1995.[16] יובהר כי טלפון נייד נכלל בגדרי ההגדרה של מחשב. על כן במסגרת דוח זה השימוש במונח תקשורת בין מחשבים כולל גם טלפון נייד.

2.3 סוגי היתרים להאזנות סתר

כאמור לעיל, היתר להאזנת סתר יכול להינתן כאשר יש חשד לעבירות פשע, על ידי נשיא או סגן נשיא של בית משפט מחוזי. לפי סעיף 6(ד) לחוק האזנת סתר יש לפרט בהיתר בית משפט כדלקמן:

"בהיתר לפי סעיף זה יתוארו זהות האדם אשר האזנה לשיחותיו הותרה, או זהות הקו או המיתקן המשמשים או המיועדים לשמש לקליטה, להעברה או לשידור של בזק, ואשר האזנה אליהם הותרה ומקום השיחות או סוגן, **<u>הכל אם הם ידועים מראש</u>**; כן יפורטו דרכי ההאזנה שהותרו".

מכאן שככלל, נדרש שצווי האזנת סתר ינקבו ביעד ההאזנה ומספר הטלפון המפורש שאליו הותרה ההאזנה. ואולם, המחוקק הכיר בכך שלעיתים, קיימות נסיבות בהן חלק מהמידע אינו ידוע מראש בשלב הגשת הבקשה ומתן ההיתר השיפוטי. בנסיבות אלו, ובכפוף לשיקול הדעת של בית המשפט, אפשר שיינתן צו שיפוטי המתיר האזנה אף אם לא כל המידע שלעיל ידוע מראש.

כך למשל, במסגרת מתן צו בית משפט להאזנה ליעד מסוים, ניתן להתיר מראש גם האזנה לטלפונים נוספים אשר עולה כי נמצאים בשימושו של היעד במהלך תקופת ההיתר. יודגש כי סוג היתר כאמור, אשר אינו מוגבל רק למספר הטלפון המסוים שצוין בהיתר, צריך להינתן במפורש על ידי בית המשפט, על בסיס כלל המידע הרלוונטי לעניין זה. נוסף על כך, ככל שניתן היתר משפטי מפורש כאמור, ובתקופת ההאזנה עלה כי בידי יעד ההאזנה טלפון נוסף בו הוא עושה שימוש, האזנה לאותו טלפון נוסף מחייב לקבל אישורים של גורמים מסוימים במשטרת ישראל ורק בנסיבות הקבועות בנהלים.

---

[15] להלן ההגדרה טרם התיקון משנת 1995: "האזנה - האזנה לשיחת הזולת באמצעות מכשיר".
[16] "מחשב" – מכשיר הפועל באמצעות תוכנה לביצוע עיבוד אריתמטי או לוגי של נתונים, וציודו ההיקפי, לרבות מערכת מחשבים, אך למעט מחשב עזר.

נוסף על כך, במקרים חריגים ניתן, בנסיבות מסוימות, לבקש היתר מפורש מבית משפט כי נוסף על היעדים שהותר להאזין להם במסגרת צו בית המשפט, יותר להעלות יעדים נוספים ככל שיעלה חשד כי הם מעורבים באותה פרשייה הנחקרת ושהם אינם ידועים בשלב זה. יודגש כי המדובר רק במקרים ייחודיים וחריגים, בין היתר בשים לב לחומרת העבירה ומסוכנותה, בהם צפויה דחיפות מידית להעלאת יעד נוסף שלא היה ידוע מראש (ואף אין די בסמכות המפכ"ל לתת היתר הקבוע בסעיף 7 לחוק). גם לעניין זה, סוג היתר כאמור צריך להינתן במפורש על ידי בית המשפט, על בסיס כלל המידע הרלוונטי ובכלל זה כלל המעורבים הידועים למשטרה במועד הגשת הבקשה והנסיבות הייחודיות המצדיקות מתן היתר חריג כאמור. נוסף על כך, ככל שניתן היתר משפטי מפורש ובתוך תקופת ההאזנה שהותרה עלה צורך מידי כאמור, נדרש קודם ביצוע ההאזנה לקבל אישורים של גורמים במשטרת ישראל ורק בנסיבות הקבועות בנהלים. למותר לציין כי האזנה במקרים המפורטים לעיל, מוגבלת אך ורק לתקופת ההיתר שניתן ולסוג ההיתר שניתן (למשל האזנת שמע לעומת האזנה לתקשורת בין מחשבים). יוער כי קיימת ביקורת מוקפדת של הייעוץ המשפטי לממשלה, במסגרת הדיווחים העתיים לפי סעיף 6(ו) בכל הנוגע לצווים מסוג זה. נבחן הצורך הראשוני שבעתו התבקש מלכתחילה צו מהסוג האמור, וכן במקרים בהם אכן בפועל הועלה יעד נוסף במסגרת ההאזנה נבחן הצורך הקונקרטי שלא איפשר פניה מבעוד מועד לבית המשפט להוצאת היתר ספציפי בענייננו.

2.4 ייחודה של האזנת סתר

ייחודה של האזנת סתר בהיבט של סמכויות אכיפה נובעת ממספר מאפיינים:

א. **פגיעה בסוד שיחו של אדם** – המחוקק ביקש לייחד הוראות בכל הנוגע לסוג מסוים של פגיעה בפרטיות, הכוללת חדירה לתוך סוד שיחו של אדם ללא ידיעתו. מובן כי בעת חקיקת החוק המחוקק ביקש להגן על שיחה במובנה הקלאסי, המתבצעת בין שני אנשים בדיבור. ואולם עם תיקון החוק להאזנה ל"תקשורת בין מחשבים", הורחבה הסמכות לתקשורת נוספת. בעקבות השינויים הטכנולוגים הרבים מאז שנת 1995, והשינוי בפלטפורמות של העברת תוכן וכן בסוג התוכן, עולות סוגיות הנוגעות להיקף המונח "תקשורת בין מחשבים" ככל שלא מדובר בשיחה בין אדם לאדם. למשל, האם תכלית חוק האזנת סתר חלה גם במקרים בהם אדם שולח מייל לעצמו, או מתכתב עם בוט.

ב. **פעולת חקירה סמויה** – האזנת הסתר אינה ידועה ליעד ההאזנה בעת ביצועה, ולעיתים ייתכן כי אף לא יידע על אודותיה לעולם.

ג. **פעולת חקירה הצופה פני עתיד** – פעולות מעקב ככלל, והאזנת סתר בפרט, ייחודיות במובן זה שפעולת האכיפה מתנהלת סימולטנית תוך כדי התרחשות הדברים, ולא בדיעבד במסגרת איסוף ראיות לאחר ביצוע העבירה. משום שמדובר בפעולת אכיפה סימולטנית, לא ניתן לצפות מראש איזה מידע יתקבל במסגרתה, מה יהיה היקפו, ומה מידת הפגיעה בפרטיות הנובעת ממנו ליעד ההאזנה או לצדדים שלישיים.

ד. **פעולת חקירה מתמשכת** – האזנת סתר היא פעולת חקירה המבוצעת באופן מתמשך, במסגרתה נאסף מידע לאורך כל תקופת ההיתר שניתן. זאת, בשונה למשל מפעולת חקירה חד פעמית, כגון חיפוש בביתו של אדם.

ה. **נדיפות הראיה** – מאפיין זה נובע מנדיפותה של הראיה העוברת בתקשורת בין בעלי השיחה, קרי העובדה שתיעודה של הראיה נוצר מלכתחילה רק בשל פעולת ההאזנה, ואלמלא אותה הפעולה – לא היה נותר לה תיעוד. מאפיין זה בא לידי ביטוי באופן מובהק כאשר מדובר בהאזנת שמע, שכן אלמלא מכשיר ההקלטה לא היה נותר תיעוד לשיחה שהתקיימה (אלא אם אחד מבעלי השיחה הקליט אותה). לעומת זאת, בכל הנוגע לתקשורת הכוללת העברת מסרים כתובים, למשל בהודעות טקסט או במסגרת אחרת של תקשורת בין מחשבים, בשלב קבלת חומרי המחשב במכשיר הקצה, הרי שממילא הם נאגרים וקיים תיעוד שלהם, ועל כן חומר זה חשוף מטבעו ככל חומר מחשב.

2.5 הבחנה בין האזנת סתר לתקשורת בין מחשבים לבין חיפוש במחשב, המצאה ותפיסה

כמפורט לעיל, חוק האזנת סתר חל גם על האזנה לשיחה בדרך של "תקשורת בין מחשבים". ייחודו של חומר מחשב המועבר בתקשורת בין מחשבים עומד, בין היתר, על כך שהוא נתפש בחקיקה הישראלית באופנים שונים ביחס למועד והאופן בו הוא נאסף על ידי גופי החקירה. כפי שנפרט להלן, תוכן זהה של חומר מחשב עשוי, בנסיבות מסוימות, לדרוש צו האזנת סתר סמוי לצורך גישה אליו, בנסיבות אחרות להיחשב "חפץ" ולדרוש צו חיפוש גלוי ובנסיבות אחרות לדרוש צו המצאת מסמכים. לא אחת נדונה שאלת מיקומו של קו הגבול בין הוראות נורמטיביות אלו, נוכח ייחודו של חומר המחשב אשר כאמור לעיל, בגלגוליו השונים – וזאת מבלי שהשתנה התוכן עצמו – עשוי בכל פעם, בשים לב לאופי הפעולה, להיכנס תחת מטריה משפטית שונה.

ההבחנה המקובלת בין הסמכויות השונות בדין הישראלי, נשענת על ההבחנה בין stored communication, מידע אגור, הכפוף לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 (להלן – **פקודת סדר הדין הפלילי** או **הפקודה**),[17] לבין communication in transit, תקשורת בתעבורה או בתווך, הכפופה לחוק האזנת סתר. דהיינו, מקובל לראות בסמכות לבצע האזנת סתר ככזו שחלה על ניטור התעבורה של תקשורת בין מחשבים בעת ביצוע ה"שיחה", בעוד שחדירה מרחוק למידע שנאגר במחשב קודם למועד החדירה מהווה פעולה מסוג חיפוש.

להבחנה זו נפקות מעשית לעניין המקור הנורמטיבי והתנאים הקבועים בחקיקה לאיסוף המידע על ידי רשויות החקירה. ודוק: חומר מחשב אשר אגור במכשיר הקצה כגון טלפון נייד או מחשב אישי, גם אם הגיע אל מכשיר הקצה על ידי תקשורת בין מחשבים (למשל מייל שהועבר בתקשורת בין מחשבים אך מבוקש לגשת אליו בדיעבד לאחר שנאגר במחשב), נתפש מהותית כ"חפץ" ועל כן גישה אליו אפשרית על ידי המשטרה רק באמצעות צו חיפוש במחשב לפי סעיף 23א לפקודת סדר הדין

[17] חומר מחשב אשר אגור במכשיר הקצה, גם אם הגיע אל מכשיר הקצה על ידי תקשורת בין מחשבים (למשל מייל שהועבר בתקשורת בין מחשבים אך כעת הוא שמור בתיבת המייל), נתפש מהותית כ"חפץ" ועל כן גישה אליו אפשרית על ידי המשטרה רק באמצעות צו חיפוש במחשב לפי סעיף 23א לפקודת סדר הדין הפלילי (מעצר וחיפוש) תוך ביצוע החיפוש באופן גלוי, או על ידי מתן הוראה להציג את חומר המחשב מכוח צו המצאת מסמכים לפי סעיף 43 לפקודה.

הפלילי, תוך ביצוע החיפוש באופן גלוי, או על ידי מתן הוראה להציג את חומר המחשב מכוח צו המצאת מסמכים לפי סעיף 43 לפקודה.[18]

יש להדגיש כי למשטרת ישראל אין סמכות בהתאם להוראות הקבועות היום בדין הישראלי, לבצע פעולה של חיפוש סמוי במחשב (ובכלל זה בטלפון נייד). כאשר מדובר בחיפוש בחומרי מחשב האגורים במחשב, סמכותה כפופה לפקודת סדר הדין הפלילי – דהיינו על החיפוש להיערך באופן גלוי ובידיעת בעל המחשב.

לשם חידוד ההבחנה הנורמטיבית והפרוצדורלית בין הסמכויות השונות הנתונות למשטרת ישראל, להלן נסכם בקצרה את המסגרת הנורמטיבית שחלה בדין הישראלי נוסף על חוק האזנת סתר הרלוונטית לסוגיית המחשבים (ובכלל זה טלפונים ניידים):

1. פקודת סדר הדין הפלילי:

א. <u>חדירה לחומר מחשב (חיפוש במחשב)</u> – כאמור, סעיף 23א לפקודה קובע את המסגרת הנורמטיבית לחדירה לחומר מחשב האגור במחשב. חיפוש בחומר מחשב היא סמכות הנתונה למשטרה כיום רק בכפוף לקיומו של צו בית משפט המתיר את החיפוש והמפרט את מטרות החיפוש ותנאיו אשר עליהם להיקבע באופן שלא יפגע בפרטיותו של אדם מעבר לנדרש. סמכות החדירה לחומר מחשב משמעה סמכות לעיין בחומר המחשב אשר אגור בו, ואין בה כדי לאפשר מעקב מתמשך ב"זמן אמת". כאמור, סמכות החדירה לחומר מחשב אינה כוללת סמכות לחיפוש סמוי במחשב, מכאן שעל החיפוש במחשב להיעשות בידיעת הבעלים של המחשב.

ב. <u>סמכות תפיסה</u> – סעיף 32 לפקודת סדר הדין הפלילי קובע את הסמכות של שוטר לתפוס חפץ אם יש לו יסוד סביר להניח כי באותו החפץ נעברה או עומדים לעבור עבירה, או שהוא עשוי לשמש ראיה בהליך משפטי בשל עבירה, או שניתן כשכר בעד ביצוע עבירה או כאמצעי לביצועה. בהתאם להגדרות הקבועות בחוק, "חפץ" הוא לרבות "חומר מחשב". אם כן, סעיף זה מסמיך את המשטרה אך ורק לתפוס את המחשב. על מנת לחדור למחשב ולעיין בחומר המחשב המצוי בו ולבצע חיפוש בו נדרש צו בית משפט לפי סעיף 23א לפקודה. לשון אחר – סעיף 32 מסדיר אך ורק את ההיבט החפצי של תפיסת המחשב כחפץ, אך אין בו כדי להעניק סמכות לעיין בתוכן האגור במחשב.[19]

ג. <u>הצגת חפץ (המצאה)</u> – סעיף 43 לפקודת סדר הדין הפלילי קובע את הסמכות של בית המשפט להורות לאדם על הצגת חפץ הנחוץ לצרכי חקירה או משפט, אשר לפי ההנחה החפץ נמצא בהחזקתו או ברשותו. כאמור לעיל, לעניין תפיסת חפץ הכולל מחשב, גם הסמכות בסעיף זה הנוגעת ל"חפץ" כוללת בין היתר "חומר מחשב" בהתאם להגדרה הקבועה בסעיף 1 לפקודה. בשונה מסמכות החיפוש, סמכות התפיסה או הסמכות לבצע האזנת סתר אשר מאופיינות בפעולות המבוצעות על ידי הרשות החוקרת לצורך איסוף הראיה, הסמכות להמצאת חומר מחשב היא

---

[18] ראו בהרחבה: חיים ויסמונסקי, **חקירה פלילית במרחב הסייבר**, פרק ד (2015).

[19] עוד ראו סעיף 32(ב) לפקודת סדר הדין הפלילי בכל הנוגע לתפיסת חומר מחשב מוסדי, וסעיף 32א לפקודה בעניין העתקת חומר מחשב לבקשת אדם המשתמש במחשב שנתפס.

פעולה שאינה מבוצעת בפועל על ידי הרשות החוקרת. אלא, בהינתן צו שיפוטי המורה על המצאת חומר המחשב, האדם המחזיק בו הוא זה שאמור להציגו לבית המשפט. נוסף על כך, בשונה מצו חיפוש במחשב אשר יכול להתיר גישה אל כלל חומרי המחשב האגורים במחשב, צו המצאה נוגע לחומר מחשב מסוים.

2. חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007 (להלן – **חוק נתוני תקשורת**) – חוק נתוני תקשורת קובע את הסמכות של משטרת ישראל לקבל נתוני תקשורת מבעל רישיון בזק.[20] חשוב לחדד את ההבחנה בין סמכות זו לבין הסמכות להאזנת סתר: בכפוף לעילות הקבועות בחוק, חוק נתוני תקשורת מסמיך את המשטרה לקבל נתוני תקשורת של מי שמקבל שירות בזק, כאשר נתוני תקשורת כוללים אך ורק נתוני מנוי,[21] נתוני מיקום ונתוני תעבורה.[22] בשונה מחוק האזנת סתר, חוק נתוני תקשורת אינו כולל את קבלת תוכנם של המסרים המועברים.[23]

להשלמת הדיון ברקע הנורמטיבי של סוגיית האזנת סתר, יש להביא, בתמצית, גם את הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, תפישה וחיפוש), התשע"ד-2014 (להלן – **הצעת חוק החיפוש**), אשר הונחה על שולחן הכנסת ה-19 והכנסת ה-20. זוהי הצעת חוק ממשלתית במסגרתה הוצעה רפורמה כוללת בדיני החיפוש, ההמצאה והתפיסה של רשויות האכיפה בהליכים פליליים, שנועדה להחליף את ההוראות הנורמטיביות הקבועות בפקודת סדר הדין הפלילי לעניין זה. בפרט הוצע להסדיר בהצעה זו באופן נרחב את כלל הפעולות הנוגעות לחומר מחשב אשר כיום מוסדרות בפקודה, שכן המצב החוקי הנוהג לעניין חיפוש במחשבים אינו נותן מענה מספק בכל הקשור לחדירה לחומר מחשב.

פרק ו' להצעת החוק מבטא את ההכרה כי מתחייבת התייחסות מיוחדת למחשב ולחומר מחשב בדיני החיפוש, התפיסה וההמצאה. הכרה זו מתחייבת במיוחד לאור היקף המידע הגלום בחומר מחשב, שכיחות השימוש בו בחיים המודרניים, והקלות היחסית שבה אפשר לחדור לחומר כאמור, ולדלות ממנו מידע תוך פגיעה בפרטיותו של האדם.[24] בהצעת החוק הוצע לקבוע איזון קפדני נוכח מאפייניו הייחודיים של חומר המחשב, בין צרכי המשטרה והאינטרס הציבורי של חשיפת עבירות, מניעתן והבאת עבריינים לדין לבין זכויות החשוד וגורמים שלישיים.

נוסף על הניסיון לעגן אמות מידה מהותיות, הכוונת שיקול הדעת והתנאים הפרוצדורליים של הפעלת סמכויות הנתונות כבר היום לגופי החקירה, הוצע בהצעת החוק להסדיר סמכויות נוספות שאינן מוסדרות כיום בדין הישראלי בכל הנוגע לחומרי מחשב. בין השאר הוצע לעגן את סמכות המשטרה לבצע חיפוש סמוי בחומר מחשב, סמכות שכאמור כיום – אינה נתונה למשטרה.

[20] בעל רישיון בזק מוגדר בסעיף 1 לחוק נתוני תקשורת.

[21] פרטים מזהים של המנוי, אמצעי התשלום שלו על השירות, הכתובת שבה הותקן מתקן הבזק בו הוא משתמש ועוד.

[22] פרטים לגבי סוג המסר המועבר (למשל הודעה לעומת שיחה), משכו והיקפו, מועד השידור ועוד.

[23] ראו דיון נרחב על אודות חוק נתוני תקשורת בבג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (28.5.2012).

[24] כמפורט בהצעת החוק, לחומר מחשב מאפיינים ייחודיים הן מההיבט של צרכי החקירה והן מן ההיבט של האינטרסים של החשוד וצדדים שלישיים. מחד גיסא, יכולת ההסוואה של הפעילות העבריינית באמצעות המחשב על דרך של הצפנה, הגנת סיסמה, פעולה באמצעות מחשב מרוחק וכדומה; נדיפותה של הראיה האלקטרונית, שמטבע הדברים עלולה להימחק או להשתנות באופן שלא ניתן יהיה לשחזרה בדיעבד; והפן הבינלאומי המובנה ברשתות תקשורת בין מחשבים, בפרט ברשת האינטרנט. מאידך גיסא, הפגיעה הצפויה בפרטיות הנחקר וצדדים שלישיים שחומר המחשב נוגע להם, נוכח היקף החומר האגור במחשב והעובדה שלצד מסמכים הדרושים לחוקר יכול שימצאו גם מסמכים רבים שאינם רלוונטיים אך הם בעלי אופי אישי ביותר; חשיבותו של המחשב וחומר המחשב לצורך ניהולו התקין של העסק שממנו נתפס החומר; וחשיבותו של חומר המחשב לצורך תפקודם היומיומי של החשוד ובני ביתו.

לסיום חלק זה יצוין כי מטרת הצעת החוק היתה להסדיר מחדש את הסמכויות שנוגעות לחיפוש, המצאה ותפיסה בלבד, ולא להחליף את ההסדרים הנוגעים לסמכות לקבלת נתוני תקשורת לפי חוק נתוני תקשורת או לסמכות להאזנת סתר ובכלל זה האזנת סתר לתקשורת בין מחשבים לפי חוק האזנת סתר. יצוין כי נכון להיום פועלים הגורמים הרלוונטיים במשרד המשפטים לעדכון הצעת החוק.

3. רוגלות

רוגלה היא תוכנה המותקנת באופן סמוי על גבי מערכת מחשוב (בין אם מרחוק או באופן פיזי), ומאפשרת נגישות לצד התוקף למערכת המחשוב הנתקפת. לרוגלות שונות יכולות שונות ומאפייני פעולה שונים. קיים ספקטרום רחב של פעולות שרוגלות שונות מסוגלות לבצע, החל מרוגלה אשר מסוגלת אך ורק לנטר הודעות IM (Instant Messaging) הנכנסות ויוצאות ממכשיר הטלפון, דרך רוגלות אשר להן יכולת לשאוב את כלל המידע האגור בתוך המחשב או הטלפון הנייד, לבצע פעולות מעקב רחבות היקף, וכלה במחיקת חומרים ועוד.[25]

ברי כי לענייננו מסגרת הדיון נוגעת אך ורק לרוגלות אשר מבצעות האזנת סתר.

במסגרת ישיבות צוות הבדיקה שהתקיימו עם הסנגוריה הציבורית, הרשות להגנת הפרטיות וארגוני חברה אזרחית, אחת הטענות המרכזיות שהועלתה בפני הצוות הייתה כנגד עצם הסמכות להתקין רוגלה על מכשיר קצה לצורך ביצוע האזנת סתר ללא הסמכה מפורשת בחוק. נציין בתמצית כי עמדה זו נשענת בין היתר על כך שרוגלה מאפשרת למשטרה לקבל בקלות רבה היקף מידע עצום על אודות כלל פעולותיו של מושא ההאזנה וכן גורמים שלישיים. פגיעה בפרטיות הנובעת משימוש ברוגלה היא חמורה במיוחד ובכך שונה מהאזנת סתר במובנה המוכר, ועל כן היא מחייבת הסמכה מפורשת בחקיקה לאחר קיום דיון השקוף לציבור. בהקשר זה הודגש כי לעצם החדירה למכשיר הקצה יש כשלעצמה פוטנציאל לאיסוף מידע באופן נרחב ולפגיעה משמעותית בפרטיות, אשר חורג מסמכויות המשטרה, במיוחד כאשר החריגה על פניה מתאפשרת רק בלחיצת כפתור. למעלה מכך, נטען כי השאלה אינה נוגעת אך לגדרי לשון החוק, אלא מחייבת אף בחינה במישור הערכי-עקרוני. דהיינו, יש לצאת מהפריזמה הצרה של שאלת הסמכות מבחינת החוק, ולבחון ברמה העקרונית מה המשמעות של טכנולוגיה מהסוג האמור הנתונה בידי משטרת ישראל, כאשר לעניין זה רלוונטי לבחון לא רק את היכולת הטכנולוגית לאיסוף המידע והיקפה, אלא גם את יכולת העיבוד של המידע לאחר איסופו, אופן השימוש בו והסקת המסקנות על בסיסו.

מובן כי בכל הנוגע לסוגיות המפורטות לעיל, מתעוררת שאלה משפטית כבדת משקל בדבר הסמכות הנתונה למשטרה מכוח חוק האזנת סתר, וזו נבחנה בנפרד כמפורט בהרחבה בנספח המשפטי. בכל הנוגע לשאלה הקונספטואלית-עקרונית-ערכית בדבר סוגיית השימוש ברוגלות להאזנת סתר על ידי גורמי אכיפת חוק משטרתיים, הפועלים למול גורמים פליליים במדינת ישראל, צוות הבדיקה קיים דיונים שונים.

הצוות סבור כי יש לחלק את הדיון המשפטי העקרוני למספר רכיבים, הנדרשים לצורך קביעת ממצאיו –

- ראשית, האם ניתן לאפשר למשטרת ישראל לחדור מרחוק אל מכשיר קצה לצורך ביצוע האזנת סתר (וזאת כשאלה מקדימה ובמנותק מהשאלה הנוספת והעוקבת של היקף היכולות הטכנולוגיות של הרוגלה לאיסוף מידע).
- שנית, ככל שהתשובה לשאלה לעיל חיובית – מהן יכולות איסוף מידע שנכון שיהיו בידי משטרת ישראל במסגרת האזנת סתר.

[25] למען הסר ספק, במסגרת האזנת סתר אין למשטרת ישראל הסמכות לבצע חיפוש סמוי או למשל למחוק מידע.

- שאלה נוספת נוגעת לאופן השימוש במידע בשלבים מאוחרים יותר על ידי, למשל, עיבודו או הצלבתו עם מידע אחר. סוגיה זו חורגת בעיקרה מהמסגרת שצוות הבדיקה התבקש לבחון, ויהיה מקום לבחון אותה בהמשך לעבודתו ולהמלצות המפורטות בדוח זה.

כאמור לעיל, סוגיות אלו כרוכות בשאלות משפטיות כבדות משקל, אשר נבחנו על ידי היועצת המשפטית לממשלה בהתבסס על ממצאי הצוות, ומפורטות בנספח המשפטי.

בכל הנוגע לשאלה הראשונה, הנוגעת רק לסוגיה העקרונית האם ניתן לאפשר למשטרת ישראל להדביק מרחוק מכשיר קצה, ומבלי להתייחס בשלב זה להיקף איסוף המידע האפשרי על ידי המערכת – ראו העמדה המשפטית לעניין מקור הסמכות לפי סעיף 10א לחוק האזנת סתר כמפורט בנספח המשפטי.

בכל הנוגע לתפישה העקרונית, יש לציין כי העמדה המשפטית היא שלא ניתן לקבל עמדה גורפת השוללת כל פעולה של האזנת סתר הכוללת חדירה למכשיר הקצה לצורך ביצוע האזנה. נכון להיום מרבית התעבורה מועברת בדרך מוצפנת, על כן משמעות עמדה עקרונית זו, השוללת כל חדירה מרחוק למכשיר קצה לצורך התקנת אמצעי להאזנת סתר, ואשר מחייבת רק האזנה לתווך התעבורה, עשויה לפגוע פגיעה קשה ביכולתה של המשטרה לבצע את תפקידיה, ולממש את התכליות שלשמן המחוקק התיר האזנה לתקשורת בין מחשבים ל למניעת עבירות פשע וחקירתן. ודוק: כפי שהעולם בכללו עבר לביצוע פעולות רבות במרחב המקוון, כך גם תקשורת בין גורמי פשיעה לצורך קידומה וביצועה מצויה במרחב זה.

עם זאת, לא ניתן לחלוק על כך שקיים צורך ממשי לבצע תיקוני חקיקה לחוק האזנת סתר על מנת להתאימו למציאות הטכנולוגית של היום. ההסדרה הנורמטיבית הקיימת כיום אינה מספקת מסגרת כוללת בעת המעבר מהעולם הישן של האזנת סתר לשיחה טלפונית לעולם הטכנולוגי החדש אשר השתנה ללא היכר. נדרשת חקיקה עדכנית אשר תסדיר באופן רוחבי סוגיות של מעקב בעידן הדיגיטלי בשים לב לכך שמנוטרת לא רק תקשורת בין אנשים אלא מידע רחב היקף המעיד על "סיפור חייו" של אדם. על החקיקה להסדיר את גבולות הסמכות והפעלתה בבירור בשים לב למאפיינים הייחודיים של הפגיעה בפרטיות בכל הנוגע למעקב אחר פעולות המבוצעות במרחב המקוון. ברי כי מדובר בסוגיות אשר המחוקק בשנת 1995 לא יכול היה להידרש אליהן.

לצד האמור, כמפורט לעיל, בעת הדיון בשאלת השימוש ב"רוגלות" להאזנת סתר, יש לבחון את רכיביה השונים של הקונספציה הכללית על אודות המשמעות של התקנת רוגלה, העשויה לערבב בין השאלה של עצם הסמכות להתקין אמצעי על מכשיר קצה לצורך ביצוע האזנת סתר, לבין השאלה של היקף היכולת הטכנולוגית לביצוע האזנת סתר לאחר התקנת האמצעי על מכשיר הקצה.

אכן, חלק מהחששות המועלים על ידי הארגונים השונים הם מהותיים והכרחיים לדיון, ואף יש בהם ממש. יש משמעות קרדינלית לעצם החדירה למכשיר קצה ופוטנציאל היכולת לאיסוף מידע על ידי כך, אשר עשוי להיות זמין, ודי לעניין זה בפעולה פשוטה. על כן, על אף שלעמדת הצוות לא ניתן לשלול מראש ובאופן גורף כל שימוש באמצעי להאזנת סתר המותקן על גבי מכשיר הקצה, אכן מחויבת בחינה פרטנית ביחס לכל רוגלה, בשים לב לספקטרום היכולות הטכנולוגיות שעשויות להיות לאותו כלי ספציפי. דהיינו, דומה כי עיקר כובד המשקל נעוץ לא בשאלה האם ניתן להחדיר רוגלה באופן כללי למכשיר קצה, אלא מה היכולות הטכנולוגיות של אותה רוגלה ספציפית.

כמפורט בנספח המשפטי, וכן כפי שיובא בהרחבה מטה, יש לבחון בצורה קפדנית ומחמירה ביחס לכל רוגלה המותקנת על מכשיר קצה לצורך ביצוע האזנת סתר, לפי היקף המידע שהיא מאפשרת לאסוף וטיבו ובהתאם לסמכויות הנתונות על פי דין. ואולם מאחר שהחוק לא עיגן באופן מפורש חדירה למחשב לשם התקנת אמצעי להאזנת סתר, נדרשת התייחסות זהירה לכל סוגיה שמועלית.

מובן כי הסוגיה העקרונית ביחס לשימוש ברוגלות, מעוררת שיח ער ונוקב ברחבי העולם. כך למשל קיימת חוות דעת של ה- European Data Protection Supervisor מפברואר 2022 בעניין שימוש ברוגלות ובאופן פרטני לעניין מערכת פגסוס והקשיים העולים בעניינה.[26] לכך יש להוסיף כי מדינות שונות מסדירות סוגיות הנוגעות לנושא זה באופן מפורש בחקיקה, כגון בריטניה וצרפת.[27]

בשים לב לאמור לעיל ולעמדה המשפטית – יש לשים את הדגש על כך שבחינת כל רוגלה ומאפייניה תבוצע תוך דיקדוק קפדני ביחס לגבולותיה, קביעת נהלים ופעולות לפיקוח ובקרה. לפיכך, המלצת הצוות כי השימוש במערכות אלה יהיה אפשרי רק בכפוף לקיומם של תנאים מצטברים כמפורט בהרחבה בפרק 5.4 לדוח.

<u>אחרית דבר לעניין תוכן מוצפן</u>

לסיכום חלק זה, יבקש הצוות אף להתייחס לטענות שהועלו על ידי חלק מגופי החברה האזרחית בכל הנוגע לקושי בעקיפה של מידע מוצפן על ידי התקנת רוגלה על מכשיר הקצה:

התקנת אמצעי על גבי מכשיר מושא ההאזנה לצורך ביצוע האזנת סתר מאפשרת לרוב לקבל תוכן אשר לו היה מנוטר בתווך התעבורה לא ניתן היה לגשת אליו היות שהוא מועבר בצורה מוצפנת. בהקשר זה נטען על ידי נציגי המכון הישראלי לדמוקרטיה כי כאשר אדם פועל בתווך המוצפן הציפיה הסבירה לפרטיות גבוהה יותר ומכאן שעומק הפגיעה בפרטיות חזק יותר, ועל כן יש בכך כדי להשליך באופן עקיף על שאלת הסמכות. לעמדת הצוות אין בעובדה זו כשלעצמה כדי להשליך על השאלה העקרונית בכל הנוגע לביצוע האזנת סתר לתקשורת בין מחשבים על ידי התקנת אמצעי על גבי מכשיר יעד ההאזנה.

אף אם אדם פעל באופן אקטיבי להגנה מוגברת על תוכן המידע על ידי הצפנתו על מנת לבצר ככל הניתן את אפשרות הגישה אליו על ידי גורמים בלתי מורשים, הרי שמבחינה נורמטיבית אין בשל כך לחסום את הגישה של רשויות החקירה אל המידע – בהינתן קיומו של חשד לעבירה פלילית והיתר להאזנת סתר כדין. יודגש כי שאלה זו אינה ייחודית להתקנת רוגלה לבדה, אלא עשויה אף להתעורר במקום שבו ההאזנה מבוצעת מרחוק דרך ניטור תעבורת הנתונים בטכנולוגיה המאפשרת לפרוץ את ההצפנה של תוכן המידע המועבר.

ככל שאכן קיים חשד לביצוע עבירה פלילית מסוג פשע המבוסס על תשתית ראייתית קונקרטית, וניתן היתר מבית המשפט לפגיעה בפרטיותו של אדם על ידי ביצוע פעולת חקירה של האזנת סתר – פעולת ההצפנה לא יכולה כשלעצמה להקנות "מעמד על" למידע, ולחסום את הגישה של רשויות החקירה אליו.

כאמור לעיל, שאלת הסמכות של גופי החקירה לגשת אל מידע על אף פעולות להגנה מוגברת על פרטיות תוכן המידע אינה שאלה חדשה – היא מתעוררת גם בהיבטים של ניטור נתוני תקשורת

[26] European Data Protection Supervisor (the EU's independent data protection authority, Preliminary Remarks on Modern Spyware (15 February 2022).

[27] בצרפת: Code de Procédure Pénale [C. Pr. Pén.]; בבריטניה: Investigatory Powers Act (2016).

בתווך התעבורה המועבר בצורה מוצפנת. שאלה זו אף מתעוררת בהקשרים אחרים כגון בעת הפעלת סמכות חיפוש במחשב במסגרתה נדרש להפעיל אמצעים על מנת לפצח סיסמת כניסה למחשב נעול אשר נתפס כדין וניתן צו חיפוש במחשב בענייננו. שאלה זו עשויה להתעורר גם בעולם הפיזי הישן כאשר אדם פעל להגן על תוכן מידע מסוים באמצעות שמירת מסמכים בכספת ויש לפרוץ אל הכספת.

העובדה שאדם ביצע פעולות להגנת הפרטיות המובילות לכך שנדרש לעקוף את ההצפנה, לפצח את הסיסמה, או לפרוץ את הכספת לצורך גישה למידע, על אף שניתן לטעון כי היא מבססת ציפייה מוגברת לפרטיות, אין בה כדי להקנות לאדם חסיון בפני גישה למידע על ידי רשויות האכיפה באמצעות הרשאה כדין. עוד לשם השוואה, ניתן להפנות לעניין זה לסוגיה דומה (אם כי לא זהה) אשר נדונה בבג"ץ **האגודה לזכויות האזרח**[28] בעניין חוק נתוני תקשורת. במסגרת העתירה נטען על ידי העותרות כי אין להעביר נתוני זיהוי כהגדרתם בחוק למאגר הנתונים שבידי משטרת ישראל של מי שמספר הטלפון שלו חסוי. בית המשפט קבע כי אין במחויבות חברת התקשורת כלפי הלקוח לספק לו מספר חסוי כדי להקים חיסיון ללקוח מפני רשויות אכיפת החוק.

סיכומו של פרק זה, לעמדת צוות הבדיקה לא ניתן להתייחס למונח "רוגלה" כאל סוגיה אחידה, שכן קיימים מאפיינים שונים לרוגלות שונות. קיים ספקטרום רחב של היקף היכולות הקיימות לכל רוגלה ורוגלה. מכאן שלא ניתן לקבל עמדה השוללת מניה וביה כל פעולה של האזנת סתר הדורשת חדירה למכשיר קצה לצורך ביצוע ההאזנה. בהינתן האמור, יש לבחון כל רוגלה לגופה כאשר מרכז כובד המשקל שיש ליתן בעת בחינת הרוגלה, נוגע להיקף הפעולות והמידע שהרוגלה יכולה לבצע ולאסוף. בחינה זו צריכה להיעשות באופן קפדני ומחמיר, בשים לב לפוטנציאל החריגה הנובע מעצם העובדה שהאזנת הסתר מבוצעת על ידי התקנת תוכנה סמויה למכשיר הטלפון או למחשב, ומתוך בחינה של היקף הפגיעה הפוטנציאלי בזכויות הפרט. ודאי בכל הנוגע לטלפונים ניידים, אשר להם היכולת לספר את "סיפור חייו" של אדם.

---

[28] בג"ץ 3809/08 ***האגודה לזכויות האזרח בישראל נ' משטרת ישראל*** (28.5.2012).

4. בדיקת הטענות לכך שהמשטרה מבצעת האזנות סתר ללא צווי בית משפט כנדרש בחוק

במסגרת הפרסומים בתקשורת, נטען, בין השאר, כי למשטרת ישראל דפוס פעולה שיטתי לפיו היא מדביקה טלפונים ניידים באמצעות מערכת פגסוס שפותחה על ידי חברת NSO, לעתים ללא קשר לחקירה מתנהלת או לבירור חשדות לביצוע עבירות פליליות, ומבלי שהתקבל צו שיפוטי המאשר זאת, תוך ניסיון לדוג מידע מודיעיני. בהמשך לפרסומים אלה, ביום 7 בפברואר פורסמה רשימת אנשים שביחס אליה נטען כי משטרת ישראל ביצעה הדבקה של מכשירי הטלפון שלהם באמצעות מערכת פגסוס שבידיה, ללא צו בית משפט.

בדוח הביניים של צוות הבדיקה שפורסם ביום 21 בפברואר 2022, נבדקו הטענות ביחס לרשימת האנשים שפורסמה ביום 7 בפברואר, שלגביה נטען כי הטלפונים הסלולריים שלהם הודבקו ללא צו בית משפט באמצעות מערכת 'סייפן'. הבדיקה הטכנולוגית העלתה כי אין כל אינדיקציה לכך שמשטרת ישראל הדביקה באמצעות מערכת 'סייפן' שבידיה ללא צו שיפוטי, מכשיר טלפון של מי מבין רשימת האנשים שפורסמה בתקשורת. יתרה מזאת, על בסיס בדיקה שנערכה בכל המקרים בהם המידע שנשלף מהמערכת אפשר לבדוק זאת, לא נמצאה גם כל אינדיקציה לניסיונות הדבקה. כמו כן, במסגרת אותה בדיקה נבדקה גם מערכת נוספת שפותחה על ידי חברה פרטית ושבשימוש בשלבי פיילוט של משטרת ישראל, וגם בעניינה לא הייתה כל אינדיקציה להדבקות או לניסיונות הדבקה אל מי מבין רשימת האנשים שפורסמה.

לאחר פרסום הממצאים הראשונים, ובשים לב לחומרת הטענות, הרחיב הצוות את הבדיקה הראשונית וביצע בדיקה טכנולוגית מעמיקה ביחס לכל מכשירי הטלפון הניידים שהודבקו מיום התקנתה של המערכת במשטרת ישראל. בדיקה זו נשענה על נתונים הנמצאים בליבת מערכת סייפן (Audit Log) ונשלפו על ידי חברת NSO, אשר על פי הנמסר מחברת NSO אינם ניתנים לשינוי או למחיקה. נתונים אלה הם נתונים מלאים, בין היתר, של כל הדבקה שבוצעה באמצעות המערכת לאורך כל שנות פעילותה במשטרה; המועד המדויק שבו בוצעה ההדבקה; והטלפון הנייד שנדבק באותו מועד. ביחס לכל נתון כאמור, צוות הבדיקה בחן האם קיים צו בית משפט המתיר את ההאזנה שבוצעה, סוג היתר בית המשפט שניתן, ומועד תוקפו.

כפי שעולה מבדיקת הצוות, ביחס לכלל המספרים שקיימים בבסיס הנתונים הפנימי של מערכת סייפן, נמצא כי אין כל אינדיקציה לנכונות הטענות שלעיל. ביחס לכלל המספרים – עלה כי משטרת ישראל הדביקה את מכשירי הטלפון הניידים לפי היתר כדין, למעט 4 מקרים.. בהם ניסיונות ההדבקה לא צלחו, וממילא לא התקבלו תוצרים:

2 מקרים בהם עלה כי בוצע ניסיון הדבקה כאשר צו בית המשפט שניתן מתיר האזנת סתר, אולם אינו מתיר האזנה מסוג תקשורת בין מחשבים לטלפון נייד; מקרה אחד בו בוצע ניסיון הדבקה זמן קצר לאחר פקיעת תוקפו של הצו;[29] מקרה אחד בו בוצע ניסיון הדבקה אך מבדיקות הצוות לא

[29] לעניין מקרה זה הייתה הארכה של צו האזנת הסתר לתקופה שבה בוצע ניסיון ההדבקה, ואולם צו בית המשפט לא התיר האזנה לתקשורת בין מחשבים של טלפון נייד.

אותר ההיתר הנדרש לפי הנהלים להעלאת היעד הנוסף בהתאם לצו שניתן; לטענת המשטרה מדובר בטעויות בתום לב.

נוסף על כך, לפי בדיקה מסוימת שנערכה לגבי פקודות ההסרה, עלה כי באחד המקרים ניתנה פקודה להסרת הכלי המאוחרת ב-3 ימים למועד הצו. כפי שיפורט בהמשך בפרק 5, ניתן באמצעות המערכת להגביל את מועדי ההאזנה ולקבוע מועד התחלה ומועד סיום להאזנה, וכך המערכת לא תבצע האזנה מעבר לתקופת זמן זו, אף אם הכלי לא הוסר לחלוטין מהטלפון באופן אקטיבי. כפי הנמסר מהמשטרה, בשים לב לאמור, גם במקרה זה לא התקבלו תוצרים בתקופת זמן חורגת זו.

יודגש שוב כי הבדיקה של מועדי ההדבקה וניסיונות ההדבקה התבססה על נתונים הנמצאים בליבת המערכת אשר לפי שנמסר מהחברה לא ניתנים לשינוי או למחיקה. על כן זוהי בדיקה אובייקטיבית, אשר בהכרח מקיפה את כל יעדי ההאזנה להם בוצעה הדבקה, לרבות כל המועדים המדויקים בהם ההדבקה בוצעה.

צוות הבדיקה הרחיב את בדיקתו אף למערכות נוספות המאפשרות לבצע האזנה לתקשורת בין מחשבים באמצעות הדבקה של מכשיר קצה, וגם בעניינם לא נמצאה כל אינדיקציה לנכונות הטענות הנטענות.

ביחס למערכת שפותחה על ידי חברה פרטית ושבידי משטרת ישראל בשלבי פיילוט, נשלפו אף בעניינה נתונים מבסיס הנתונים של המערכת שכפי שנמסר מהחברה אינו ניתן לשינוי או למחיקה על ידי המשתמש, ולא נמצאה כל אינדיקציה כאמור.

יצוין כי קיימות שתי מערכות שבפיתוח של משטרת ישראל שהיו בעבר בשימוש המשטרה, שלגביהן מובהקות הבדיקה הטכנולוגית נמוכה יותר. יחד עם זאת יש להדגיש את הדברים שלהלן:

למערכת אחת המכונה "חלוץ" הייתה היכולת לבצע האזנה רק לטלפונים ממספר מצומצם של דגמים ישנים, וההדבקה באמצעותה היתה אפשרית רק בנגישות פיזית אל הטלפון הנייד שהוא יעד ההאזנה (אין אפשרות להדבקה מרחוק). למערכת נוספת, המכונה "דייזי", היתה היכולת לבצע האזנה למחשבים, ובעניינה, כפי שנמסר מהמשטרה, ניתן היה לבצע הדבקה רק בנגישות פיזית. כאמור, מהבדיקה הטכנולוגית שבוצעה גם בעניינן של שתי מערכות אלה, לא נמצאה אינדיקציה להאזנה ללא צו בית משפט.

לשלמות התמונה נציין כי קיימים מספרי טלפון נוספים שלגביהם בוצעה הדבקה או ניסיון הדבקה, אך לפי בדיקות הצוות מדובר במספרי טלפון שנועדו לבדיקת המערכות ומשויכים לחברות הפרטיות, או למשטרת ישראל. כמו כן קיימים מספרים בודדים אשר לפי מאפייניהם ונתונים שנשלפו מבסיס הנתונים לגביהם שוכנע הצוות שגם לגביהם מדובר במספרי בדיקה.

לאור האמור לעיל, לא נמצא בסיס לטענה כי משטרת ישראל מדביקה טלפונים ניידים של אנשים שאין בעניינם חשד פלילי ובהיעדר צו שיפוטי. בניגוד לנטען, בדיקות הצוות העלו כי קיימת בחטיבת הסייבר משמעת להאזנה בכפוף להיתר כדין.

4.1 בדיקת מערכת סייפן

להלן יפורטו הליך הבדיקה וממצאי צוות הבדיקה בכל הנוגע לקיומם של צווי האזנת סתר ביחס להדבקות או לניסיונות הדבקה באמצעות מערכת סייפן.

4.1.1 אופן הבדיקה וממצאים

הבדיקה נעשתה ביחס לנתונים אשר נשלפו מליבת המערכת:

הבדיקה נעשתה מול בסיס הנתונים הפנימי של המערכת (Auditlog), בו נשמרים כלל הרשומות הנוגעות להדבקה לאורך כל תקופת פעילותה של המערכת במשטרה (בין השנים 2016-2021). המערכת פרוסה במתקני משטרת ישראל, ואולם מהמידע שנמסר על ידי נציגי חברת NSO לצוות הבדיקה, השכבה של בסיס הנתונים הפנימי של המערכת אינה זמינה למשתמש, אלא יכולה להיות מונגשת על ידי החברה בלבד, וכן אינה ניתנת לשינוי או מחיקה על ידו.

רשימת מספרי הטלפון שנבדקו

הבדיקה נעשתה על בסיס רשומות שנשלפו מבסיס הנתונים של המערכת (Audit log), אשר כוללות את כלל מספרי הטלפון אשר ביחס אליהם נעשתה הדבקה שצלחה, וכן במקרים בהם התאפשר אף ביחס לניסיון הדבקה שלא צלח. יודגש, כי אין מדובר ברשימת מספרי טלפון שגובשה או הועברה על ידי המשטרה, אלא מספרים אשר חולצו מליבת המערכת עצמה.

אופן בדיקת ההדבקות וניסיונות ההדבקה

ביחס לכל מספר טלפון אשר מופיע ברשימת המספרים אשר חולצה לעיל, חולצו מבסיס הנתונים כלל התאריכים והשעות בהם בוצעו הדבקה או ניסיון הדבקה באמצעות המערכת. ביחס לכל מספר טלפון עשויות להיות מספר הדבקות או ניסיונות הדבקה – כל אלה נבדקו על ידי צוות הבדיקה.

אל מול נתונים אלה, נבדק ביחס לכל מספר טלפון, שלגביו נעשו הדבקות או ניסיונות הדבקה, האם יש באותו מועד צו בית משפט בתוקף, המתיר האזנת סתר בדרך של תקשורת בין מחשבים לפי חוק האזנת סתר. קרי, נבדקו הפרטים שלהלן:

א. פירוט מספר הטלפון הספציפי המופיע בצו בית המשפט (לעניין זה ראו הרחבה בהמשך תחת סוגי ההיתרים שקיימים);
ב. מועד תחילת הצו ומועד סיומו;
ג. האם הצו התיר האזנה מסוג תקשורת בין מחשבים.

סוגי ההיתרים שקיימים

היתר להאזנת סתר יכול להינתן כאשר יש חשד לעבירות פשע, על ידי נשיא או סגן נשיא של בית משפט מחוזי. לפי סעיף 6(ד) לחוק האזנת סתר יש לפרט בהיתר בית משפט כדלקמן:

> "בהיתר לפי סעיף זה יתוארו זהות האדם אשר האזנה לשיחותיו הותרה, או זהות הקו או המיתקן המשמשים או המיועדים לשמש לקליטה, להעברה או לשידור של בזק, ואשר האזנה אליהם הותרה ומקום השיחות או סוגן, **הכל אם הם ידועים מראש**; כן יפורטו דרכי ההאזנה שהותר".

עוד ראו בתקנות האזנת סתר (בקשה להיתר האזנה), התשס"ז-2007, את הטופס המפורט בתוספת לעניין נוסח הבקשה וההיתר.

מכאן שככלל, נדרש שצווי האזנת סתר ינקבו ביעד ההאזנה ומספר הטלפון המפורש שאליו הותרה ההאזנה. ואולם, המחוקק הכיר בכך כי לעיתים, קיימות נסיבות בהן חלק מהמידע אינו ידוע מראש בשלב הגשת הבקשה ומתן ההיתר השיפוטי. בנסיבות אלו, ובכפוף לשיקול הדעת של בית המשפט, אפשר שיינתן צו שיפוטי רחב יותר המתיר האזנה אף אם לא כל המידע שלעיל ידוע מראש. כמפורט בהרחבה בפרק 2 לעניין סוגי היתרים להאזנות סתר.

לפי בדיקת הצוות, באחוז גורף של המקרים מספרי הטלפון שקיימים בבסיס הנתונים של המערכת מופיעים באופן מפורש בצווי בית המשפט שניתנו.

במקרים בהם מספר הטלפון לא מופיע בצו, צוות הבדיקה בחן האם מדובר בצו אשר התיר במפורש להאזין למספרי טלפון נוספים אשר לא היו ידועים מראש במועד מתן ההיתר (כמפורט בהרחבה בפרק 2 לעניין סוגי ההיתרים השונים),. במקרים אלו נבחנה בצורה מדוקדקת על ידי צוות הבדיקה, האם קיים אישור בכתב של הגורמים הרלוונטיים בחטיבת הסייבר, בהתאם לנהלים בנושא, המתירים האזנה ביחס לאותו מספר טלפון נוסף. לעניין זה נבדק האם האישור שניתן קודם למועד ההדבקה או לניסיון ההדבקה.

כפי שעולה מבדיקת הצוות, ביחס לכלל המספרים קיים היתר כדין כמפורט לעיל. זאת למקרים המפורטים לעיל.

עוד יצוין כי קיימים מספר מקרים של טעויות סופר, בהם במסגרת הזנת המספר להדבקה באמצעות המערכת, ברור כי הייתה טעות באופן הזנת המספר.[30] גם בכל המקרים האמורים נמצא שמדובר בניסיונות הדבקה שלא צלחו.

יצוין כי הבדיקה השיטתית שבוצעה על ידי צוות הבדיקה נוגעת למועדי <u>הדבקה וניסיונות הדבקה</u>. נוסף עליה, בוצעו בדיקות מסוימות לעניין מועד הפסקת האזנת הסתר. בשים לב לסד הזמנים שהיה בידי צוות הבדיקה לא נעשתה בדיקה בעניין זה ביחס לכלל האזנות הסתר. במקרים בהם ניתן היה להשלים בדיקה זו, נמצא כי ההאזנה הייתה בתוך תקופת צו בית המשפט, למעט המקרה המתואר לעיל.

סיכומם של דברים, כפי שעולה מבדיקת הצוות, ביחס לכלל המספרים שקיימים בבסיס הנתונים הפנימי של מערכת סייפן, נמצא כי אין כל אינדיקציה לכך שמשטרת ישראל הדביקה באמצעות מערכת סייפן שבידיה מכשירי טלפון ניידים ללא היתר כדין. זאת למעט 4 מקרים כפי שפורט לעיל, בעניינם ההדבקה לא צלחה וממילא לא התקבלו תוצרים, ולטענת המשטרה מדובר בטעות בתום לב.

---

[30] למשל – במקום 050-000123 נכתב 050-000132.

5. בדיקת הטענות לכך שבמסגרת האזנת סתר המשטרה חורגת מסמכויותיה ואוספת מידע שאינו מהווה תקשורת בין מחשבים

במסגרת הפרסומים נטען בין היתר כי משטרת ישראל שואבת את כל החומר האגור על הטלפון הנייד של יעד האזנת הסתר בניגוד לסמכות הקבועה בחוק האזנת סתר. צוות הבדיקה ביצע בדיקות מקיפות לעניין מאפייני המערכות שבשימוש משטרת ישראל להאזנה לתקשורת בין מחשבים של טלפונים ניידים באמצעות הדבקה.

כפי שיפורט בהרחבה להלן, ככלל המערכות פועלות לאיסוף תוצרים חדשים, אשר עברו בתקשורת בין מחשבים, מרגע ההתקנה ואילך. לצד האמור, נמצא כי אכן קיימות חריגות ביכולות הטכנולוגיות של מערכת סייפן המאפשרות לקבל סוגי תוצרים שאינם מותרים לפי חוק האזנת סתר. צוות הבדיקה סבור כי טרם תחילת שימוש המשטרה במערכת נדרש היה לוודא את התאמתה לסמכויות המוקנות למשטרה בחוק האזנת סתר, באמצעות חסימה טכנולוגית של כל אפשרות לקבלת תוצרים אלה.

עם זאת, ועוד טרם נרחיב על אודות החריגות, ומבלי להקל ראש בהיקף הפגיעה בפרטיות, ראוי לציין כי לפי בדיקת מסמכים, הן ממועדים הקודמים לרכישת המערכת והן לאחריה, ומהתרשמות צוות הבדיקה מהגורמים שאיתם נפגש – הנחת המוצא של חטיבת הסייבר הייתה כי בשים לב לאיסור הנוהלי על הפקת המידע החורג, יש בכך כדי להוות תנאי מספק להתאמת חריגות המערכת לסמכות לפי חוק האזנת סתר, ולא הייתה כוונה לעשות שימוש במידע חורג.

נפרט:

היכולות הקיימות במערכת המשטרתית מפורטות בנוסח החסוי של דוח זה, כמתואר במבוא, על מנת שלא לחשוף שיטות עבודה ואמצעים של משטרת ישראל, וכן סודות מסחריים של החברות.

היכולות הטכנולוגיות הקיימות במערכת סייפן חורגות בשני מישורים מסמכויות המשטרה:

האחד, מערכת סייפן מאפשרת למשטרה לקבל מידע האגור על מכשיר היעד ושנוצר קודם למועד ההדבקה. קבלת המידע האגור אפשרית באמצעות הפעלה אקטיבית של יכולת זאת. באופן קונקרטי, הופעלה יכולת זאת במסגרת האזנות בהן ביקשה המשטרה להשלים פערי זמן של האזנה שנוצרו בתוך תקופת ההיתר של בית המשפט, במקרים בהם הכלי חדל לפעול מסיבות טכנולוגיות שונות והותקן מחדש. עם ההתקנה המחודשת, ביקשה המשטרה באמצעות פעולה אקטיבית במערכת ("פיקוד אקטיבי") לקבל מידע אגור על מנת להשלים את אותו פער זמנים. לעניין זה, עד אפריל 2020[31] בפועל לא ניתן היה להגביל את התקופה אשר החל ממנה יתקבל מידע אגור, ועל כן התקבל במקרים רבים מידע הקודם למועד ההתקנה הראשון ואף הקודם למועד צו בית המשפט.

---

[31] ראו בהמשך פירוט על אודות הוספת מודול ה warrant באפריל 2020.

בשימוש המשטרה מערכת נוספת בפיתוח חברה פרטית, אשר אוספת מידע מרגע התקנת הכלי ואילך ולה היכולת במקרים קונקרטיים להביא מידע אגור בכפוף להכנסת תאריכים מדויקים שמהם רוצים לקבל את המידע בשלב התקנת הכלי.

השני, לא נוונה במערכת סייפן היכולת לקבל מידע שאינו מהווה תקשורת בין מחשבים כגון פרטי יומן, אנשי קשר פתקים האגורים במכשיר, ורשימת האפליקציות המותקנות. ואכן, במקרים רבים התקבל מידע כאמור במסגרת ביצוע האזנת סתר. גם לעניין זה, רק באפריל 2020 ניתן היה לבחור להגביל מראש את סוגי התוצרים שיתקבלו במסגרת האזנת הסתר ולמנוע קבלת אותם חומרים אסורים.

מבלי לגרוע מחומרת הדברים האמורים, יודגש כי קיימים נהלים בחטיבת הסייבר האוסרים על הפקת מידע שאינו מהווה תקשורת בין מחשבים וכן מידע הקודם למועד ההתקנה הראשון. לעניין זה יש להוסיף כי מהתרשמות צוות הבדיקה, עלה כי קיימת הפנמה ומשמעת של הגורמים הרלוונטיים ביחס לגדרי המותר והאסור לשימוש. כמו כן, מ-25 בדיקות מדגמיות שבוצעו על ידי הצוות כפי שיפורט בהמשך, עלה כי לא בוצעה הפקה בכתב של תוצרים אלה. לכך יש להוסיף עוד 23 בדיקות שבוצעו על ידי הפרקליטות שגם בהן לא נמצא כי בוצעה הפקה בכתב של תוצרים אלה.

נציין כי בהתאם להנחיית פרקליט המדינה, הפרקליטות בודקת תיקים פליליים שבהם נעשה שימוש במערכות לגבי תיקים תלויים ועומדים, בין היתר תיקים בהם הוגש כתב אישום ונעשתה פניה על ידי ההגנה, על מנת לבחון האם נעשה שימוש במערכות וככל שכן האם הופקו התוצרים.

הצוות לא הגיע לממצאים ברורים בעניין הצפייה בחומרים שהתקבלו, ולא נמצא שהיו נהלים שהתייחסו באופן מפורש לעניין זה. לפי הנמסר באופן עקבי מהמשטרה, משמעות האיסור על הפקה היא שזו חלה גם על צפייה במידע.

כפי שיפורט מטה, עמדת צוות הבדיקה היא שהנהלים אשר רק אוסרים על שלב הפקת המידע, על אחת כמה וכמה משאינם מלווים בהליכי בקרה תכופים וקפדניים כדי לוודא את יישומם, אינם יכולים להוות חסם מספק למקרים בהם קיימת מערכת אשר ביכולתה לאסוף מידע החורג מהיקף הסמכויות הנתונות למשטרה. לפיכך נדרש היה לוודא כי אין יכולת טכנולוגית לקבלת המידע העודף.

5.1 מידע האגור על מכשיר הטלפון

בהתאם לבדיקות הצוות, לא נוונה טכנולוגית במערכת סייפן וכן במערכת נוספת שבידי משטרת ישראל היכולת לבקש באופן אקטיבי מהמערכת מידע הקודם למועד ההתקנה.

להלן נפרט על אודות יכולות המערכת והפרקטיקה שנהגה במשטרת ישראל לקבלת מידע הקודם למועד ההתקנה אשר נועדה ליתן מענה לפער הזמנים שנוצר בין התקנה להתקנה בפרק הזמן שבו הכלי חדל לפעול בתוך תקופת הצו. עוד נפרט בהמשך על האישורים המשפטיים שניתנו בעניין :

עם התקנת סייפן על מכשיר טלפון, הכלי פועל בדרך של איסוף תוצרים חדשים הנוצרים על גבי מכשיר הטלפון אליו מאזינים מרגע ההתקנה ואילך. ואולם, נוסף על כך, קיימת אפשרות טכנולוגית למפעיל לבצע פעולה אקטיבית במסגרת האזנה מסוימת, המבקשת מהכלי לאסוף מידע אשר אגור על גבי מכשיר יעד ההאזנה, דהיינו מידע אשר נוצר טרם התקנת הכלי ואף קודם למועד צו בית

המשפט כפי שיפורט להלן. יודגש כי משמעות הדברים היא כי מידע האגור על המכשיר והקודם למועד ההתקנה לא נאסף אוטומטית, אלא רק אם ניתן פיקוד אקטיבי לשם כך.

למען הסר ספק יובהר כי איסוף מידע האגור על מכשיר הטלפון ואשר קודם למועד ההתקנה, אינו מהווה האזנת סתר, אלא חיפוש סמוי במחשב – שכפי שפירטנו בפרק 2, אינו בסמכות המשטרה.

הפרקטיקה: בהקשר זה הוסבר על ידי משטרת ישראל כי במקרים בהם בוצעה התקנה ולאחריה הכלי חדל לפעול לתקופה מסוימת, הייתה קיימת פרקטיקה במסגרתה לאחר ההתקנה המחודשת, נשלח פיקוד אקטיבי לקבלת מידע אגור על מנת להשלים את הפער שנוצר בשל נפילת הכלי, בתקופה שבה היה צו בית המשפט בתוקף. לשם המחשה: אם ניתן צו בית משפט להאזנה לתקשורת בין מחשבים ליעד מסוים לחודשים ינואר-פברואר, ובוצעה הדבקה ביום 1.1, אך הכלי חדל לפעול מסיבה זו או אחרת ביום 2.1 ורק ביום 10.1 הצליחו לבצע הדבקה חדשה, פעלו המפעילים לקבלת המידע האגור במכשיר שבין ה-2.1 ל-10.1. זאת מתוך התפישה כי כל עוד מדובר במידע שהועבר בתקשורת בין מחשבים בתוך תקופת הצו, הדבר מותר לפי חוק האזנת סתר, כמפורט בהמשך.

מודול ה- warrant:

במרבית תקופת פעילותה של מערכת סייפן (החל משנת 2016 ועד אפריל 2020), כאשר בוצעה פעולה לקבלת מידע אגור כאמור לעיל, לא ניתן היה להגביל את המועד אשר החל ממנו יתקבל המידע, ולהבטיח כי יהיה זה רק מידע שנוצר לאחר מועד ההתקנה הראשון (שנעשה בתקופת הצו). מכאן שהלכה למעשה היה מתקבל מידע אגור אשר נוצר קודם למועד ההתקנה הראשון ואף קודם להיתר שניתן על ידי בית המשפט.

רק באפריל 2020 לערך, בגרסה מתקדמת יותר של המערכת, נכלל מודול חדש בממשק המשתמש שבידי המשטרה, שמכונה "**מודול ה- warrant**". מודול זה איפשר להזין את התאריכים לביצוע ההאזנה (בהתאם לתוקפו של צו בית המשפט). כך ניתן היה, במקרים בהם ניתן פיקוד אקטיבי לקבלת מידע אגור, להגביל את המועד שהחל ממנו יתקבל מידע ולקבוע כי זה יתקבל רק החל ממועד ההתקנה הראשון של הכלי על מכשיר הטלפון.[32]

מכאן שעד לאפריל 2020, ולהכנסת מודול ה- warrant, בכל פעם שבוצעה פעולה אקטיבית לקבלת מידע אגור מסוג מסוים, על מנת להשלים את אותו "פער זמנים" שבו הכלי חדל לפעול בתוך תקופת הצו, התקבל מידע אשר נאסף על מכשיר היעד קודם למועד ההתקנה וממילא קודם להיתר בית המשפט. יש להדגיש כי אין הכוונה כי עשויה היתה להתקבל במקרים אלו כל תכולת המכשיר הסלולרי, אלא רק מידע אגור מסוג המידע שהמערכת מסוגלת לאסוף ואשר ביחס אליו התבקש באופן אקטיבי לקבל מידע אגור לצורך השלמת פער הזמנים שבו הכלי חדל לפעול.

יודגש שוב כי קיימים נהלים האוסרים על הפקת מידע הקודם למועד ההתקנה. לפי התרשמות של צוות הבדיקה כאמור לעיל, אי ניוון המערכת באופן מלא לא נבע מרצון המשטרה לעשות שימוש במידע אגור הקודם למועד התקנת הכלי. אלא, הנחת המוצא של חטיבת הסייבר הייתה כי בשים לב לאיסור הנוהלי על הפקת המידע ושימוש בו, יש בכך כדי להוות תנאי מספק להתאמת חריגות המערכת לסמכות משטרת ישראל לפי הוראות חוק האזנת סתר.

---

[32] יוזכר שוב, כי אף לפני תקופת ה warrant המערכת פעלה כברירת מחדל באופן של איסוף תוצרים רק מרגע ההתקנה ואילך, ומידע אגור הקודם למועד זה התקבל רק אם בוצעה בקשה אקטיבית לכך.

השימוש במודול ה- warrant לא מהווה תנאי הכרחי טכנולוגית להדבקה בסייפן: אף לאחר הטמעת מודול ה- warrant באפריל 2020, ממשק ה- warrant לא היה ממשק שהיווה תנאי הכרחי מבחינה טכנולוגית לצורך ביצוע הדבקה.

לפי בדיקת הצוות, גם לאחר אפריל 2020 אכן היו מקרים רבים בהם בוצעה הדבקה ללא הזנה של warrant אשר מאפשר להגביל את המועד ממנו יתקבל מידע אגור, ככל שישלח פיקוד לכך. יש לציין כי כפי שנבדק על ידי צוות הבדיקה בעזרת נתונים שנשלפו מבסיס הנתונים של המערכת, אף לאחר שנוסף מודול ה- warrant באפריל 2020, לא החל שימוש מידי וגורף בממשק זה.[33] כפי שנמסר לצוות הבדיקה מנציגי חברת NSO, בחודש עד חודשיים הראשונים לאחר הוספת המודול למערכת היו בעיות תפעוליות של המודול שבגינן לא ניתן היה לעשות שימוש קבוע בממשק זה. כך גם לדברי נציגי המשטרה.

מערכת נוספת שבידי משטרת ישראל: היכולת הטכנולוגית לקבלת מידע אגור קיימת גם במערכת נוספת שבשימוש משטרת ישראל. ואולם בעניינה החל מתקופת ראשית פעילותה ניתן היה להגביל מראש את התקופה אשר החל ממנה יתקבל מידע אגור בהתאם לפרקטיקה האמורה לעיל. גם כאן, הפרקטיקה הייתה לבקש באופן אקטיבי מידע אגור על מנת לגשר על פער הזמנים שבו הכלי חדל לפעול, בתוך תקופת הצו.

5.1.1 אישורים משפטיים לקבלת מידע אגור

בשנת 2018 ניתן אישור מטעם הייעוץ המשפטי למשטרה לבצע פעולה לקבלת מידע אגור ממכשיר היעד לגבי התקופה שבה נוצר פער זמנים בתוך תקופת הצו, כאמור. לפי האישור הנ״ל, הותר לקבל מידע אגור בתוך תקופת צו בית המשפט, אך רק החל ממועד תחילת ההאזנה הראשונה בפועל (אף אם היתר בית המשפט הוא קודם לכן), ובכפוף לכך שקיימת האזנה נוספת לתקשורת בין מחשבים במקביל. עוד הובהר באישור המשפטי כי פעולה זו אפשרית רק כאשר מתעורר צורך זמני וכי לא ניתן לאשרה כדפוס פעולה או פרקטיקה קבועה ושגרתית בה ישנה הסתמכות לפרקי זמן ממושכים על קיומה של האזנה מקבילה.

נבקש לציין מספר נקודות לעניין אישור משפטי זה:

- הפרקטיקה החלה עוד לפני האישור המשפטי: לפי הנתונים שנשלפו על ידי חברת NSO מבסיס הנתונים של המערכת, עולה כי הפרקטיקה לקבלת מידע אגור החלה למעשה בשנת 2016, עוד לפני שניתן האישור המשפטי המפורט לעיל.

- לא הייתה קיימת במערכת באותו הזמן אפשרות טכנולוגית להגביל את המועד ממנו יחל להיאסף מידע אגור: האישור המשפטי בעניין ניתן בשנת 2018, בתקופה שבה לא ניתן היה מבחינה טכנולוגית להגביל את המועד ממנו יתקבל מידע אגור, כך שיכלול רק מידע החל ממועד ההתקנה הראשון. כאמור לעיל, משמעות הדברים היא כי על בסיס אישור זה בוצעו פעולות אשר הלכה למעשה כללו איסוף מידע אגור הקודם למועד הצו ומהוות חיפוש סמוי. מכאן שהאישור המשפטי עליו נסמכה הפעולה, לא מתייחס לסוגיה המשמעותית של קבלת

[33] למען הסר ספק, הכוונה רק לשימוש בממשק, ולא לשאלה האם ההאזנה בוצעה בכפוף לצו בית משפט.

מידע הקודם למועד ההתקנה הראשון, וודאי למועד תחילת הצו. כפי שנמסר מהייעוץ המשפטי למשטרה, עובדה טכנולוגית זו לא הובאה לידיעתו.

- לא קיימים נהלים לגבי קבלת מידע הקודם למועד ההתקנה: מבדיקה שערך הצוות נמצא כי לא נקבעו נהלים שהסדירו את המקרים והנסיבות בהם ניתן לבצע פעולה לקבלת מידע אגור ממכשיר היעד. עובדה זו הובילה לכך שהלכה למעשה לא הייתה הסדרה ברורה וחד משמעית למפעילים באשר לתנאים בהם ניתן לעשות שימוש בטכנולוגיה זו. ההשלכות לכך היו כי הפרקטיקה אכן הייתה שונה מזו שהותוותה באישור המשפטי כפי שיפורט להלן.

- הפרקטיקה הייתה שונה מזו שהותוותה באישור המשפטי: אף לאחר האישור המשפטי שניתן בשנת 2018, הפרקטיקה בפועל בחטיבת הסייבר לא תאמה את המתווה אשר בכפוף אליו הותר קבלת מידע אגור. כאמור, האישור המשפטי חייב קיומם של שני תנאים: האחד, קיימת האזנה מקבילה לכל משך התקופה שלגביה מבוקש לקבל מידע אגור והשני, מתווה זה לא יהיה בבחינת פרקטיקה שגרתית.

בפועל, הפרקטיקה הייתה שונה מזו שאושרה על ידי הייעוץ המשפטי למשטרה. כפי שנמסר לצוות הבדיקה, בפועל בקשות אקטיביות מהמערכת לקבלת מידע אגור נעשו בין אם הייתה האזנה מקבילה ובין אם לאו. כמו כן, גם לאחר שכבר נוסף מודול ה – warrant למערכת, הייתה תקופה שבה לא הזינו במערכת את מועד ההתקנה הראשון (קרי מועד תחילת ההאזנה כמפורט בעמדת היועץ המשפטי למשטרה), אלא את מועד תחילת צו בית המשפט, אף אם ההתקנה הראשונה הייתה מאוחרת אליו.

עוד יצוין, כי כפי שעולה מבסיס הנתונים של המערכת השנייה שבשימוש משטרת ישראל שגם לה יכולת זו, מידע אגור התבקש אף במקרים מסוימים בהם הייתה זו ההדבקה הראשונה באמצעות אותה מערכת. כפי שנמסר מהמשטרה, הבקשה לקבל מידע אגור בהקשר זה התבססה על כך שבוצעה הדבקה בעבר על ידי מערכת אחרת להאזנה מאותו סוג, בתוך תקופת הצו.

5.1.2 עמדת הצוות לעניין קבלת מידע אגור

כמפורט בפרק 2, איסוף מידע האגור על מכשיר הטלפון קודם למועד ההתקנה, אינו מהווה האזנת סתר, אלא חיפוש סמוי במחשב – שאינו בסמכות המשטרה.

ואולם יודגש שוב כמפורט בהרחבה לעיל, כעולה ממסמכי המשטרה הקודמים למועד רכישת המערכת והן ממועדים מאוחרים יותר, ומהתרשמות צוות הבדיקה מהגורמים שאיתם נפגש, עלה כי היעדר ניוון המערכת בהקשר זה, והשימוש בפרקטיקה לקבל מידע אגור, לא נבעו מרצון המשטרה לעשות שימוש במידע הקודם למועד צו בית המשפט.

בכל הנוגע לחומרת הדברים, יש מקום להבחין בין מידע אגור שהתקבל בתוך תקופת צו בית המשפט, לבין מידע אגור שהתקבל והוא קודם לתקופה שנקבעה בצו בית המשפט. בכל הנוגע לקבלת מידע הקודם למועד צו בית המשפט, מדובר בפגיעה בפרטיות שנעשתה בחוסר סמכות– וזאת אף ללא תלות בשאלה האם הפיקו מידע זה בפועל ואם לאו. כמפורט בנספח המשפטי, הפגיעה בפרטיות נעשית עוד החל משלב איסוף המידע, אף אם המידע אינו חשוף בפני כל ולא נעשה בו

שימוש. לעניין זה יש להפנות לדבריה של כב׳ השופטת דפנה ברק-ארז בבג״ץ **האגודה לזכויות האזרח**[34] בעניין איכוני השב״כ בקורונה:

> "ראוי להדגיש כי הזכות לפרטיות כוללת בחובה לא רק הגנה מפני "גילוי" מידע הנוגע לאדם לצדדים שלישיים. ההגנה על זכות זו חייבת להתייחס גם לפעולות הקודמות לגילוי במישור הזמן – איסוף המידע [...]. הטלת הגבלות על איסוף מידע הנוגע לאדם ועל אגירתו באופן אלקטרוני היא חלק אינטגרלי מהזכות לפרטיות אף כאשר הוא אצור במאגר המידע ואינו נחשף בפני כול. מטעם זה חוק הגנת הפרטיות כולל פרק מיוחד שעניינו פיקוח על מאגרי מידע (פרק ב׳ לחוק זה). כמו כן, חוקים רבים נוספים כוללים הגבלות על איסוף חומר אישי הנוגע לאדם. ייתכן למשל שהשימוש במידע גנטי היה יכול להרים תרומה נוספת למאבק בפשיעה אילו כל אזרחי המדינה היו נדרשים למסור דגימה למאגר כללי שישמש את המשטרה. אולם, מחשבה זו כלל אינה עולה על הדעת. ובצדק רב."

לגבי איסוף מידע האגור על המכשיר אך נוצר אך ורק לאחר מועד ההתקנה הראשון – כמפורט בנספח המשפטי, העמדה המשפטית היא כי גם פעולה זו אינה מהווה פעולה מסוג האזנת סתר ועל כן אינה מותרת. לצד האמור, יש להדגיש כי זו פעולה אשר באותו זמן עמדת הייעוץ המשפטי למשטרה לגביה הייתה כי היא מותרת על פי החוק (בהינתן התנאים שנקבעו במתווה המשפטי שפורט לעיל המחייב חזרה למועד ההתקנה הראשון, וקיומה של האזנה חלופית).

5.2 סוגי מידע שאינם מהווים תקשורת בין מחשבים

הצוות מצא כי לא נוונה באופן מלא היכולת הטכנולוגית במערכת לקבל סוגי מידע מסוימים שאינם מהווים תקשורת בין מחשבים. להלן יפורטו סוגי מידע אשר אינם מהווים מידע מסוג ״תקשורת בין מחשבים״ לפי החוק, ומשכך איסופם מהווה, למעשה, חיפוש סמוי.

בהקשר זה נדרש להבחין להלן בין יכולות טכנולוגיות של המערכת שלא נוונו, אשר אף לעמדת הייעוץ המשפטי למשטרה באותו הזמן לא עמדו בתנאי חוק האזנת סתר, לבין סוגי מידע המתקבלים באמצעות המערכת שלגביהם לא הייתה עמדה של הייעוץ המשפטי למשטרה כי אין סמכות לאספם, אך לאחר שנבחנו כיום על ידי הייעוץ המשפטי לממשלה, העמדה היא כי הם אינם מותרים (כמפורט בנספח המשפטי).

בכל הנוגע לסוג הראשון, היו נהלים האוסרים את הפקת המידע, ואכן לפי בדיקות מדגמיות ספורות של צוות הבדיקה עלה כי מידע זה לא הופק בכתב ולא הועבר במסגרת הפרפרזה הכתובה ליחידה החוקרת.

5.2.1 רשימת האפליקציות המתקבלת באופן אוטומטי

בכל פעם שבו מערכת סייפן מותקנת על גבי מכשיר הטלפון של יעד מסוים, מוצגת באופן אוטומטי בממשק המשתמש שבידי המשטרה רשימת האפליקציות המותקנת על גבי המכשיר (קרי, שמות האפליקציות המותקנות בלבד) באופן דומה, גם במערכת הנוספת שבשימוש המשטרה מתקבלת באופן אוטומטי רשימת האפליקציות עם ההתקנה.

במערכות אלה רשימת האפליקציות מוצגת הן למפעיל, שאחראי על התקנת הכלי, והן למפיק שאחראי על הפקת התוצרים שמתקבלים מהכלי. בהקשר זה נטען על ידי משטרת ישראל כי רשימת

---

34 בג״ץ 6732/20 **האגודה לזכויות האזרח נ׳ הכנסת**, פסקה 12 לפסק הדין של השופטת ברק-ארז (1.3.2021).

האפליקציות נדרשת לצורך ביטחון הכלי ותפעולו, על מנת לוודא כי לא מותקנת אפליקציה העשויה לסכן את אמצעי ההאזנה על גבי מכשיר הטלפון, ובכך לחשוף שיטות ואמצעים וכן את קיומה של חקירה פלילית סמויה, על כל המשתמע מכך. על כן לעמדת המשטרה נדרש לקבל מידע זה והסמכות לכך נעוצה בסעיף 10א לחוק האזנות סתר, בדבר סמכויות העזר. לצד האמור ציינה המשטרה כי בהתאם לנהלי חטיבת הסייבר, חל איסור על הפקת רשימת האפליקציות והעברת המידע ליחידה החוקרת – דהיינו, השימוש נועד רק לשימוש הגורמים הטכנולוגיים במשטרה האחראים על התקנת ותפעול הכלי.

בכל הנוגע לשאלה העובדתית האם אכן נעשה בפועל שימוש ברשימת האפליקציות לצורך התכלית של ביטחון הכלי, כפי שנמסר מהגורמים הרלוונטיים בחטיבת הסייבר, לא נעשה בכך שימוש בפועל לצורך תכלית זו. כפי שעולה מבדיקות הצוות, בפועל עד היום, המפעילים לא בדקו את רשימת האפליקציות על מנת לבדוק האם יש חשש לחשיפת הכלי, אלא הסתמכו על הבדיקה הממוכנת שנעשית על ידי המערכת באופן אוטומטי. לעומת זאת, באחד מביקורי הצוות במתקני המשטרה, הוזכרה כדוגמא ביחס למקרים בהם התקבל במערכת מידע על אפליקציה חדשה שהתעדכנה, האפשרות לעשות שימוש לצרכים מודיעיניים כגון מידע ביחס לכך שאותו יעד האזנה עושה שימוש באפליקציה הסוחרת בביטקוין.

<u>העמדה המשפטית כפי שנבחנה במהלך עבודת הצוות</u>: בכל הנוגע לשאלה המשפטית, בדבר הסמכות לפי סעיף 10א לחוק לקבל מידע שאינו מהווה תקשורת בין מחשבים, ראו פירוט בנספח המשפטי. בתמצית, עמדת היועצת המשפטית לממשלה, בהתבסס על ממצאי צוות הבדיקה, היא כי קבלת המידע היא בגדר סעיף 10א לחוק האזנת סתר, מאחר שהמידע אכן נדרש למערכת סייפן והמערכת הנוספת שבשימוש המשטרה לצורך ביטחון הכלי לבחינה אוטומטית וממוכנת. מכאן שהסמכות מוגבלת לכך שהבדיקה נעשית באופן ממוכן ואוטומטי, וכי רשימת האפליקציות אינה חשופה לעיני אדם, ראו הרחבה בנספח המשפטי.

5.2.2 מידע נוסף שלא מהווה תקשורת בין מחשבים המתקבל במערכת סייפן

נוסף על רשימת האפליקציות המתקבלת באופן אוטומטי, במערכת סייפן קיימים סוגי מידע נוספים שניתן לקבל, אולם נכון להיום (לאחר כניסת מודול ה- warrant בשנת 2020) הם אינם מתקבלים באופן אוטומטי, אלא על המפעיל לסמן אקטיבית בשלב ההתקנה האם מדובר במידע שהוא מבקש שהכלי יעביר למערכת במסגרת פעולת ההאזנה. חלק מסוגי המידע הנוספים אשר המפעיל יכול לסמן ולקבל, אינם נכללים במסגרת הסמכות הנתונה למשטרת ישראל לפי החוק, שכן לא מדובר במידע המועבר בתקשורת בין מחשבים, אלא במידע האגור על גבי המכשיר (ראו בנספח המשפטי), כגון פתקים אנשי קשר ופריטי יומן.

כאמור בראשיתו של פרק זה, נבחין בין מידע אשר אף לשיטת המשטרה חל איסור משפטי לקבלו, לבין יכולות טכנולוגיות שלא הייתה לגביהן עמדה של הייעוץ המשפטי למשטרה כי אין סמכות בעניינן, ושעמדת היועצת המשפטית לממשלה, בהתבסס על ממצאי הצוות, היא כי הן אינן עומדות בתנאי החוק.

בשים לב להבחנה זו: פתקים, אנשי קשר ופרטי יומן הם מסוגי המידע אשר לכל אורך תקופת פעילותה של מערכת סייפן לא היה חולק בייעוץ המשפטי למשטרת ישראל כי אין סמכות לקבלם. אף על פי כן, בפועל, לא נוונו טכנולוגית יכולותיה של המערכת לקבלת מידע מסוג זה, והנחת

העבודה של חטיבת הסייבר הייתה כי די בקביעת איסור נוהלי על הפקתם. בשיחה שקיים צוות הבדיקה עם גורמים בחטיבת הסייבר לצורך בירור משמעות ההנחיה בעניין, הובהר על ידי גורמים בחטיבת הסייבר, כי האיסור בנהלים חל לא רק על הפקה אלא גם על צפייה במידע.

יצוין כי קיימים סוגי מידע מסוימים נוספים, אשר נבחנו על ידי היועצת המשפטית לממשלה על בסיס ממצאי צוות הבדיקה, ונמצא כי הם אינם מהווים תקשורת בין מחשבים. הדברים מפורטים בדוח החסוי.

<u>הבהרה לעניין מאפייני מערכת סייפן בכל הנוגע לסוגי מידע שאינם מהווים תקשורת בין מחשבים</u>: המערכת אוספת תוצרים חדשים שנוצרו מרגע ההתקנה ואילך, וכך גם לעניין סוגי המידע המפורטים לעיל – משמעות הדברים היא כי ככל שאכן סומן אחד מסוגי המידע האמורים לעיל, המערכת קיבלה את אותו סוג מידע רק אם נוצר מידע חדש מסוג זה מרגע ההתקנה. כך למשל, יתקבלו רק אנשי קשר חדשים שנשמרו במכשיר ממועד ההתקנה.

עד למודול ה warrant לא ניתן היה להגביל בסייפן את סוגי המידע שיתקבלו: במרבית תקופת פעילותה של מערכת סייפן (החל משנת 2016 ועד 2020), לא ניתן היה להגביל את האפשרות לקבל אנשי קשר, פתקים ויומן. כפי שהוסבר לעיל, רק סביב אפריל 2020, נכנס לפעולה מודול ה- warrant אשר אפשר את הגבלת טווח התאריכים שהחל ממנו יתקבלו תוצרים, וכן אפשר להגביל את סוגי התוצרים שמבוקש שהכלי יאסוף ויעביר למשטרה. רק באמצעותו ניתן היה להגביל את האפשרות לקבל אנשי קשר, פתקים ויומן.

כמפורט לעיל, כפי שנבדק על ידי צוות הבדיקה בעזרת נתונים שנשלפו מליבת המערכת, אף לאחר שנוסף מודול ה- warrant באפריל 2020, לא החל שימוש מיידי וגורף בממשק זה. כאמור, כפי שנמסר לצוות מנציגי חברת NSO, עד כחודש או חודשיים לאחר הוספת המודול למערכת היו בעיות תפעוליות של המודול שבגינן לא ניתן היה לעשות שימוש בממשק זה. כך גם נמסר מנציגי המשטרה. אכן, לפי בדיקת הצוות, לאחר אפריל 2020 היו קיימים מקרים רבים בהם בוצעה הדבקה ללא הזנה של warrant, אשר מאפשר להגביל את קבלת התוצרים יומן, אנשי קשר ופתקים.

דהיינו, מתחילת פעולתה של המערכת בשנת 2016 ועד להטמעת מודול ה- warrant באפריל 2020, נוכח מאפייני המערכת, התקבל בהכרח מידע שאינו מהווה תקשורת בין מחשבים מהסוג המפורט לעיל. כמו כן, אף לאחר אפריל 2020, הגבלה של סוגי התוצרים הייתה מותנית בכך שאכן נעשה שימוש בכל מקרה ומקרה במודול ה- warrant בעת הדבקה, וכן בכפוף לכך שלא הוזנו במודול ה- warrant בקשה לאסוף סוגי תוצרים אסורים.

מבדיקת הצוות לפי נתונים שהתקבלו מליבת המערכת, אכן, לאחר ה- 1.4.20, באחוז לא מבוטל מהמקרים, מתוך סך ההדבקות שבוצעו התקבל מידע מסוג אנשי קשר, פתקים ופריטי יומן.

יצוין כי לאורך כל תקופת פעילותה של המערכת הייתה אפשרות בה באופן פאסיבי ייחשף מידע למפיק: המערכת פועלת כך שלעתים תוצר יופיע למפיק על הצג גם אם המפיק לא נכנס באופן אקטיבי לצפייה באותו פריט מידע. כך למשל, עם הכניסה של המשתמש לממשק התוצרים שהתקבלו, הפריט עם התאריך הכי קרוב יופיע ראשון עבור המטרה שצופים בה במסך.

5.2.3 האם ניתנו אישורים משפטיים לאיסוף סוגי מידע שאינם מהווים תקשורת בין מחשבים

לעמדת המשטרה באותה העת היה נהיר כי לא הייתה סמכות לקבל יומן, אנשי קשר ופתקים ועל כן חל איסור על הפקתם. כפי שצוין בפרק 8, בשנת 2012 עת נבחן השימוש הפוטנציאלי של מערכת סייפן, הייתה מעורבות של הייעוץ המשפטי למשטרה לעניין היקף היכולות של המערכת ונדון הצורך בהתאמה לסמכויות הנתונות למשטרה לפי חוק האזנת סתר, כך שהמערכת תוכל להבחין בין תכנים הנמצאים במכשיר עצמו ושאינם חלק מסמכויות המשטרה, לבין תכנים המהווים תקשורת בין מחשבים. על אף שבתחילת הדרך נדון הצורך בניוונים טכנולוגיים, דה פקטו, המערכת הופעלה ללא ניוון טכנולוגי של היכולות העודפות.

יצוין כי ביחס לסוג מידע מסוים נוסף, ניתן אישור משפטי של הייעוץ המשפטי למשטרה, אך זה התייחס רק למאפיין אחד הנוגע אליו. מאפיין נוסף הנוגע לסוג מידע זה לא הוצג לייעוץ המשפטי למשטרה, אך יכול שהדבר נבע מהיעדר היכרות מלאה יחד עם הבנה מוטעית של הגורמים הרלוונטיים על אודות הטכנולוגיה המסוימת. כתוצאה מכך היה שימוש בפונקציה מסוימת אשר לאור ממצאי הצוות, ולאחר שאלו הובאו בפני היועצת המשפטית לממשלה, העמדה היא כי אין לעשות שימוש בפונקציה זו.

5.3 בדיקות מדגמיות בכל הנוגע להפקת המידע החורג

מטעם הצוות נערכו 25 בדיקות מדגמיות על מנת לבחון האם ביעדי האזנה לגביהם התקבלו תוצרים שאינם מהווים תקשורת בין מחשבים, או תוצרים הקודמים למועד ההתקנה הראשון, ואף ידוע (לפי המידע שבבסיס הנתונים) כי תוצרים אלה סומנו על ידי המערכת כנצפו, והאם המידע הופק ונכלל בפרפרזה שהועברה ליחידה המזמינה. בדיקת הצוות בעניין זה התמקדה בבחינת טבלאות ההפקה אשר המפיקים ממלאים בשלב המעבר על תוצרי האזנת הסתר שהתקבלו, וכן מעבר על הפרפרזות המועברות ליחידה החוקרת.

יודגש כי מדובר בבדיקה מדגמית. עוד יודגש כי בשים לב למגבלות בדיקת הצוות, בדיקה זו נוגעת למידע שתועד בכתב בטבלת ההפקה ובפרפרזות.

מבדיקות מדגמיות אלה לא עלתה אינדיקציה כי הופקו נתונים הקודמים למועד הצו או סוגי נתונים שלא מהווים תקשורת בין מחשבים, וכן לא עלתה אינדיקציה כי המידע הועבר ליחידה המזמינה במסגרת הפרפראזה שהוכנה. לכך יש להוסיף, כי פרקליטות המדינה ביצעה מטעמה עד כה עוד 23 בדיקות וגם בעניינן נמצא כי על אף שמידע כאמור התקבל, מידע עודף זה לא הופק ולא הועבר לצוות החקירה. בצד זאת, יודגש כי מדובר בבדיקות מדגמיות ספורות בלבד, ואשר נוגעות להעברת מידע בכתב בלבד אל טבלת ההפקה וממנה אל היחידה החוקרת במסגרת הפרפרזה הכתובה.

5.4 המלצות הצוות לעניין הפעלה מחודשת של המערכות

איסוף מידע אשר אינו מידע שמועבר בתקשורת בין מחשבים, וכן מידע אשר קודם למועד התקנת הכלי, אינו מהווה פעולה של האזנת סתר המותרת לפי החוק, אלא חיפוש סמוי במחשב – שאינו בסמכות המשטרה. על אף שלא נמצאה אינדיקציה לכך שהמידע החורג הופק, איסוף מידע שאינו

במסגרת הסמכויות הנתונות על פי דין מהווה פעולה הפוגעת בפרטיותו של אדם בהיעדר סמכות, וזאת ללא תלות בשאלה האם לאחר איסופו המידע נצפה או הופק והועבר ליחידה החוקרת.

בעמדת היועצת המשפטית לממשלה כמפורט בנספח המשפטי, ובעמדה בפרק 3 לדוח בעניין רוגלות, מפורטת בהרחבה הזהירות הנדרשת בבואנו לבחון האם ניתן להתיר שימוש באמצעי להאזנת סתר המותקן על הטלפון הנייד, ומודגש כי פרשנות זו מחייבת זהירות ביחס לגבולותיה בהיעדר חקיקה מפורשת. כמפורט שם בהרחבה.

בשים לב לכך, עמדת צוות הבדיקה היא כי ניתן להחזיר לשימוש את שתי המערכות האמורות, בכפוף לתנאים המפורטים להלן:

התאמות טכנולוגיות

א. העמדה המשפטית לפיה משטרת ישראל רשאית לעשות שימוש להאזנת סתר במערכות באמצעות חדירה למכשיר קצה, נוגעת אך ורק למערכות אשר בוצעו בהן כלל החסימות הטכנולוגיות הנדרשות על מנת לוודא כי אלו מבצעות האזנת סתר כפי שהותר בחוק בלבד, על פי הפרשנות שאושרה. לפיכך יש לנטרל יכולות לקבל מידע אגור, ולוודא כי במערכות המותקנות במשטרה יהיו יכולות טכנולוגיות לאסוף מידע מסוג תקשורת בין מחשבים רק מרגע ההתקנה ואילך.

ב. יש לנוון כל יכולת טכנולוגית לקבל סוג מידע שאינו מועבר בתקשורת בין מחשבים, אשר לא אושר בנספח המשפטי ובנספח המשפטי לדוח החסוי.

ג. לעניין רשימת האפליקציות המתקבלת באופן אוטומטי בשים לב לעמדה המפורטת בנספח המשפטי, יש לנוון את הצגת רשימת האפליקציות בממשק המשתמש המשטרתי, ולהבטיח כי זו אינה חשופה לעיני אדם. עוד יש לוודא כי רשימת האפליקציות לא תשמר במערכת לאחר שמסתיימת האזנת הסתר.

ד. על מנת שתתאפשר בקרה אובייקטיבית בהתבסס על בסיס הנתונים של המערכות, יש לוודא כי המערכות יאפשרו הפקת דוחות פעולה לצורך ביצוע בקרה בדיעבד בקלות, תוך אינדיקציה ברורה לעניין כל אחד משלבי התהליך. לצורך כך נדרש שיופיע בדוחות הפעולה המופקים מבסיס הנתונים, שדות הכוללים בין השאר את: מספר הצו, טלפון יעד ההאזנה, מועדי הצו שהוזנו, סוג הפעולה שבוצעה ביחס ליעד ומועדה, מועד הסרת הכלי, והמשתמש שביצע כל אחת מהפעולות. נדרש כי ניתן יהיה להפיק את הדוח באופן המאפשר מיון לפי כל אחד מהשדות הנ"ל. נוסף על האמור לעיל, יש להבטיח קיומם של גיבויים לבסיס הנתונים, ככל שאינם.

מבלי לגרוע מהאמור בסעיפים שלעיל ככל שמסיבה טכנולוגית לא ניתן לבצע את השינויים הטכנולוגיים באופן מלא ביחס לסעיפים ב׳–ד׳ המפורטים לעיל, ממליץ הצוות כי המשטרה תהיה רשאית להביא לבחינת היועצת המשפטית לממשלה מתווה חלופי המבוסס על חוות דעת משפטית של היועץ המשפטי למשטרה ועל חוות דעת טכנולוגית לפיהן מתווה מוצע המונע חריגה מסמכות. הצוות ממליץ כי לאור ממצאיו ונוכח העמדה המשפטית שגובשה, ומאחר שהחקיקה הנוגעת לעניין טרם תוקנה – מתווה כאמור יובא לבחינה רק ככל שמוצו באופן מוחלט כלל המאמצים לניוון המערכת, ורק אם המשטרה שוכנעה כי המתווה מבטיח פעולה כדין, בשים לב להמלצות הצוות וממצאיו ולעמדה המשפטית.

יצוין כי נדרש בירור עובדתי ומשפטי נוסף של משטרת ישראל לגבי מאפיין מסוים נוסף במערכת לעניין עמידתו בדרישת הסימולטניות בהתאם לעקרונות שהותוו בנספח המשפטי החסוי.

תנאים נוספים נדרשים

א. בשים לב לכך שמדובר בפרשנות תכליתית של חוק האזנת סתר, ונוכח היקף הפגיעה בפרטיות הפוטנציאלי בעת שימוש במערכות להאזנת סתר המותקנות על גבי המחשב או הטלפון הנייד, יש להבטיח כי שימוש במערכות אלה יהיה כפוף לקיומם ויישומם של נהלים ברורים המבהירים את גדר הסמכויות וכוללים הנחיות מפורטות לעניין אופן השימוש, תוך נקיטת זהירות מיוחדת. הצוות ממליץ כי נהלים אלה יאושרו על ידי היועץ המשפטי למשטרה והייעוץ המשפטי לממשלה.

ב. יש לבחון במסגרת גיבוש הנהלים אם יש מקום להטיל תנאים או מגבלות מיוחדים להגשת בקשות להאזנת סתר לגבי הפעלת יכולות שעל אף שנמצא כי הן בסמכות לפי חוק האזנת סתר, יש להן פוטנציאל לפגיעה משמעותית במיוחד בפרטיותו של יעד ההאזנה. הגבלות ותנאים כאלה יכול שיהיו לגבי סוג מסויים של האזנה או לסוגי מקרים.

ג. נדרש פיקוח פרטני הדוק של משטרת ישראל. כן יש מקום גם לתת את הדעת באופן מיוחד למקרים בהם היה שימוש במערכות אלה במסגרת הפעלת סמכות הפיקוח הקבועה ליועצת המשפטית לממשלה לפי סעיף 6(ו) לחוק האזנת סתר.

ד. נדרש לבחון בהקדם אם יש צורך בקביעת כללים ייחודיים, נוסף על אלו הקיימים כיום, לעניין ביעור ומחיקה של מידע שהתקבל במסגרת האזנת סתר לתקשורת בין מחשבים, וכן תיעוד של פעולת מחיקה כאמור.

6. נוסח הבקשות לצווי האזנת סתר

בין הטענות השונות שהועלו בעקבות הפרסומים בתקשורת בדבר השימוש המשטרתי במערכת סייפן, נטען כי משטרת ישראל לא פירטה בפני בית המשפט במסגרת הבקשות להאזנת סתר מסוג תקשורת בין מחשבים, כי ההאזנה תבוצע באמצעות מערכת זו; כי האזנת הסתר כוללת חדירה מרחוק למכשיר יעד ההאזנה; ומהו היקף היכולות של המערכת וסוג התוצרים שיתקבלו עם ביצוע האזנה מהסוג האמור.

צוות הבדיקה בחן את נוסח הבקשות להאזנת סתר מסוג תקשורת בין מחשבים המוגשות לבתי המשפט, על מנת לבדוק אילו פרטים מוצגים לבית המשפט בטרם קבלת החלטתו להתיר האזנה.

הבדיקה כללה בחינה של תבנית הצווים והנימוקים שמוגשים לבית המשפט בהקשר הנדון. שלא בשולי הדברים יצוין כי נוסח בקשות להאזנות הסתר של תקשורת בין מחשבים היו מוכרים עוד בעבר לגורמי הייעוץ המשפטי לממשלה, שכן אלה הוצגו במסגרת הדיווחים העתיים שהוגשו לייעוץ המשפטי לממשלה מכוח סעיף 6(ו) לחוק. ואולם נוסח הצווים נבחן עתה מחדש על ידי צוות הבדיקה לאחר שנבחנו כלל היכולות הטכנולוגיות של המערכות ובראי אותן יכולות.

יש לציין כי צוות הבדיקה בחן רק את המסמכים המוגשים לבית המשפט, ולא את פרוטוקולי הדיונים עצמם. כמו כן, בשים לב ללוח הזמנים שעמד לרשות הצוות והצורך למקד ככל הניתן את היקף הבדיקה, לא הרחיב הצוות את בדיקתו בעניין זה ולא נפגש עם הנהלת בתי המשפט או שופטים המוסמכים להתיר ביצוע האזנות סתר. משכך, המלצות הצוות נוגעות רק לסוגיית נוסח הבקשות שיש להביא בפני בית המשפט.

6.1 רקע נורמטיבי לעניין הוראות הדין בדבר בקשה להיתר להאזנת סתר

בהתאם לסעיף 6(ד) לחוק האזנת סתר, בהיתר להאזנת סתר יש לתאר את "זהות האדם אשר האזנה לשיחותיו הותרה, או זהות הקו או המיתקן המשמשים או המיועדים לשמש לקליטה, להעברה או לשידור של בזק, ואשר האזנה אליהם הותרה ומקום השיחות או סוגן, הכל אם הם ידועים מראש; כן יפורטו דרכי ההאזנה שהותרו." כמו כן, לפי סעיף 6(ה) לחוק, יש לפרט בהיתר את תקופת תקפו, אשר לא תעלה על 3 חודשים מיום מתן ההיתר, ואולם ההיתר ניתן לחידוש על ידי בית המשפט.

את הוראות החוק הנ"ל משלימות תקנות האזנת סתר (בקשה להיתר האזנה), התשס"ז-2007.[35] התקנות קובעות, בין השאר, כי הדיון בבקשה יערך במעמד צד אחד וכי הדיון יתועד בפרוטוקול שישקף את כל הנאמר בדיון.[36] במסגרת הדיון, על הקצין או הנציג המתייצב בפני בית המשפט להצהיר על העובדות התומכות בבקשה ועל אמיתותן, להציג לבית המשפט חומר הנוגע לבקשה, וכן לצרף העתקים מבקשות קודמות הנוגעות לאותו אדם באותו תיק חקירה והחלטות בית המשפט

---

[35] התקנות תוקנו בשנת 2007 וזאת לאחר דוח צוות הבדיקה בנושא האזנות סתר משנת 2005 (דו"ח לבנת משיח שהוזכר לעיל), אשר עסק בין היתר בפרטי הבקשה להאזנות סתר ונימוקיה וההליך המתנהל בבית המשפט. הצוות הוקם על ידי היועץ המשפטי לממשלה דאז (מר אליקים רובינשטיין), בעקבות בחינתו את תיק מח"ש 2403/02 בפרשת האזנות הסתר ביאחב"ל שנפתח נגד ניצב משה מזרחי, והממצאים שעלו מהחקירה, לצור הפקת לקחים ולשם בחינת הצורך בשינוי חקיקה או נהלים בנושא האזנות סתר.

[36] סעיף 3 לתקנות האזנת סתר (בקשה להיתר האזנה), התשס"ז-2007.

בבקשות אלה, לרבות החומר שהוגש לבית המשפט. כאשר מדובר בבקשה לחידוש היתר, ידווח לבית המשפט על ההאזנות שנערכו בעבר ועל המידע שהופק מהן.[37]

עוד נקבע בתקנות נוסח הטופס להגשת בקשה להאזנת סתר לבית המשפט.[38] בטופס האמור על המשטרה לפרט את שם האדם ופרטיו או פרטי מידע על המקום שבו מותקן הטלפון, או המקום שלגביו מתבקשת ההאזנה. יש לפרט את מהות החשד וסעיף העבירה, את הקו או המיתקן שאליו מבוקשת ההאזנה. נוסף על כך יש לפרט את משך ההיתר המבוקש (אשר לא יעלה על 3 חודשים).

כמו כן, התקנות מנחות את המשטרה לעניין הפירוט הנדרש במסגרת הנימוקים לבקשה. בין היתר יש לציין את התשתית העובדתית שעליה מבוססת הבקשה ואת טעמי הבקשה, הנימוקים שהובילו להחלטה על הגשת בקשה להאזנת סתר, לאחר שנשקל הצורך מול הפגיעה הצפויה בפרטיות בשים לב לחומרת העבירה; הסיכוי לאיסוף מידע רלוונטי באמצעות ההאזנה; עוצמת החשד והתשתית הראייתית אשר מצדיקים האזנת סתר; מידת הקשר בין המואזן לעבירה; מידת הפגיעה הצפויה במי שאינו חשוד ומשך ההאזנה הדרוש. עוד יש לתאר את אפיון המקום או הקו שבו מתבקשת האזנת הסתר (בית פרטי, עסק, רכב וכו'), פרטי המחזיק ככל שהוא ידוע ואת הקשר בינו לבין יעד ההאזנה.

יצוין כי התקנות קובעות אף את נוסח טופס ההיתר שעל בית המשפט למלא במסגרת החלטתו.

נשוב ונזכיר לעניין זה את פסק הדין בעניין אילוז[39] עוד משנת 1991, בו נקבע כי בכל הנוגע לבסיס העובדתי והשיקולים שיש לשקול בעת מתן היתר להאזנה, על בית המשפט להשתכנע, בהתבסס על המידע המובא בפניו, כי אכן יש צורך אמיתי בנקיטת האמצעי מרחיק הלכת של פגיעה בצנעת הפרט כדי למנוע עבירה או לגילוי העבריין. כל זאת בין היתר בשים לב לחומרת העבירה. לצורך כך, על המשטרה להקפיד בתיאור מדויק של נתוני היסוד במסגרת בקשה להאזנת סתר, הן בפרטים התמציתיים שנרשמים בטופס והן בדיון בעל-פה בפני בית המשפט, שכן כל אלה משמשים מצע להפעלת שיקול הדעת על ידי השופט.

קיימת חשיבות לקיומו של פירוט נרחב במסגרת בקשה להאזנת סתר בכלל, ולהאזנה מסוג תקשורת בין מחשבים בפרט. הבנת בית המשפט את היקף הפגיעה הפוטנציאלי בפרטיות הנובע ממתן היתר להאזנה מסוג מסוים, הכרחי על מנת לאפשר לו לשקול באופן מלא את ההצדקה לשימוש באמצעי חקירה הפוגע באופן כה דרמטי בפרטיותו של אדם, ויערוך את האיזון הנדרש בין הצורך החקירתי אל מול מידת הפגיעה בפרטיות במקרה הקונקרטי. לא זו אף זו, הבסיס העובדתי המצדיק את סוג ההאזנה המבוקש והיקף המידע שיתקבל עם ביצוע ההאזנה חיוני על מנת שבית המשפט יוכל, במסגרת החלטתו, לבחון האם ניתן לקבוע גדרות ומגבלות להיתר אשר יפחיתו את מידת הפגיעה בפרטיות ככל הניתן.

זוהי אם כן הנחת המוצא ממנה יצא צוות הבדיקה בעת בדיקת הטפסים המוגשים לבית המשפט.

יצוין כי הדברים האמורים נכונים באשר לפירוט אשר יש בו כדי להוות בסיס עובדתי אשר הכרחי לצורך עריכת האיזון הנדרש על ידי בית המשפט בין הצורך בהאזנה לבין מידת הפגיעה בפרטיות,

---

[37] שם, בסעיף 4.
[38] שם, בתוספת לתקנות.
[39] ע"פ 2286/91 **מדינת ישראל נ' אילוז**, מה(4) 289 (31.7.1991).

לצורך החלטה בעניין מתן היתר להאזנת סתר. לעמדת צוות הבדיקה המצע העובדתי הנדרש להפעלת שיקול הדעת השיפוטי אינו מחייב פירוט בפני בית המשפט בעניין כלל מאפייניה של המערכת הספציפית באמצעותה תבוצע האזנת הסתר, פירוט יצרני המערכת או כינויה. אין בפרטים אלה כשלעצמם כדי להעלות או להוריד לעניין הבחינה של מידת הפגיעה בפרטיות. לצד האמור, יש חשיבות יתרה שבעת הפעלתה של מערכת חדשה לה יכולות חדשות, תוצג בפני בית המשפט אופן ביצוע ההאזנה (למשל שמדובר בהאזנה הדורשת הדבקה מרחוק של מכשיר טלפון נייד ברוגלה) והיקף המידע שעשוי להתקבל באמצעותה (בין אם מדובר במידע הנדרש לצורך תפעול וביטחון הכלי, ובין אם מדובר במידע המופק ומועבר ליחידה החוקרת).

6.2 ממצאים והמלצות

בשים לב לדברים האמורים ובכפוף לתפישה העקרונית שהוצגה לעיל, צוות הבדיקה בחן את נוסח הצווים שמועבר לבית המשפט בעניין האזנת סתר מסוג תקשורת בין מחשבים לטלפונים ניידים.

נוסח הבקשות לצווים קבוע בתקנות האזנת סתר (בקשה להיתר האזנה), תשס״ז-2007, וכן בנהלים של חטיבת הסייבר ועליו להופיע בבקשות הנוגעות להאזנה לתקשורת בין מחשבים של מכשיר טלפון סלולרי או מחשב. לאחר שנבחנו היכולות הטכנולוגיות של המערכת, נבקש לציין את הנקודות שלהלן:

פירוט על אודות העובדה כי לצורך האזנה נדרשת חדירה למכשיר הסלולרי/המחשב:

נוסח הבקשה לצווים אכן מפרט כי לצורך האזנת הסתר ייתכן ויהיה צורך להתקין או להסיר את התוכנה מהמכשיר.

כמו כן, בבקשות לצווים, הנוסח אותו הציגה המשטרה בפני בית המשפט, כולל במסגרתו גם את סוגי התוצרים אשר עתידים להתקבל אגב ביצוע האזנת הסתר ואשר ייעשה בהם שימוש, כמפורט בדוח החסוי.

משכך, הצוות לא מצא כי המשטרה פעלה כדי להסתיר מידע מבית המשפט. יתר על כן, כאשר בית המשפט דרש פרטים נוספים מעבר לאמור בבקשה, הפרטים הנוספים הועברו[40].

יחד עם זאת, בבחינה בדיעבד, נוכח מאפייני המערכת, הצוות סבור כי עם כניסתה של המערכת לפעולה היה מקום גם להרחיב בפני בית המשפט באשר לשיטת הפעולה להאזנה, סוג המידע החורג הצפוי להתקבל במסגרת ההאזנה אשר לא יופק, ובכלל זאת הפרקטיקה שהייתה נוהגת המפורטת בפרק 5 המובילה לכך שעשוי להתקבל מידע אגור הקודם למועד ההדבקה ולמועד צו בית המשפט.

ואולם יש להדגיש כי הצוות סבור שממילא אין מקום לאשר את השימוש במערכות בהיעדר ניוון של יכולות טכנולוגיות לקבלת תוצרים החורגים מהסמכויות לפי חוק האזנת סתר, כמפורט בהרחבה בפרק 5. משכך, לא נדרש לשנות את נוסח הבקשות לעניין מידע חורג שעשוי להתקבל. זאת, משום שממילא מידע חורג מסוג זה לא יתקבל עוד.

[40] כך למשל בשנת 2018 ביקש בית המשפט עמדה לעניין סמכותה של המשטרה לבצע פעולה של חדירה סמויה למחשבים ולטלפונים סלולריים לצורך ביצוע פעולה של האזנת סתר.

לאור האמור, עם קליטתה והכנסתה לפעולה של מערכת חדשה, הצוות סבור כי יש לפרט פרטים נוספים בפני בית המשפט בעניין, כמפורט להלן:

- **יש לוודא שבמסגרת הבקשה, ההתייחסות לשיטת ההאזנה תשקף לבית המשפט את כניסתה לפעולה של מערכת חדשה ואת שיטת ההאזנה בפועל** (למשל כשמדובר בהאזנה הדורשת הדבקה מרחוק של מכשיר טלפון נייד ברוגלה).
- נכון להיום, המשטרה מבקשת היתר לכניסה למקום פיזי יחד עם בקשה להתקנת תוכנה, ללא הבחנה ברורה. **הצוות סבור כי נכון להפריד בין בקשה להיתר כניסה למקום פיזי לבין בקשה להיתר חדירה למחשב לצורך התקנת תוכנה להאזנת סתר מכוח סעיף 10א לחוק.**

הצורך בשינוי התפישה של הגשת בקשה לכלל סוגי התקשורת בין מחשבים באופן גורף

כפי שעולה מהטופס האחיד לבקשות להאזנת סתר של תקשורת בין מחשבים הקבוע בהנחיית העבודה של חטיבת הסייבר, ההנחיה עד היום הייתה כי בכל פעם בו יש צורך להאזנת סתר מסוג תקשורת בין מחשבים, יש לבקש מבית המשפט את כלל סוגי התקשורת. פרקטיקה זו היתה ידועה למשרד המשפטים. לגבי יכולת מסוימת הונחתה המשטרה לשקול את נחיצותו במקרים הקונקרטיים ולא לבקשו בכל צו, וכן לגבש נוהל שיתווה את שיקול הדעת בשימוש בו.

לאחר בחינת סוגיה זו על ידי צוות הבדיקה, ונוכח היקף הפגיעה המשמעותית בפרטיות הנגרמת לנשוא הצו כאשר מדובר בתקשורת בין מחשבים, הצוות סבור כי יש לשנות פרקטיקה זו. **הצוות ממליץ שהמשטרה תבחן בעת גיבוש האזנת הסתר בנפרד לגבי כל אחד מסוגי התקשורת בין מחשבים, האם הוא נדרש לצורך החקירה הקונקרטית. הצוות סבור כי יש להסביר בבקשה לבית המשפט, מדוע נדרשת דווקא האזנה לסוג התקשורת המבוקש. לגבי יכולות מסוימות יש להבהיר בבקשה את הנסיבות בהן מבוקש להפעילן, על מנת שבית המשפט יתווה את התנאים לכך, כמפורט בהרחבה בדוח החסוי.**

השתלמויות לשופטים בעניין סוגי הכלים באמצעותם מבוצעת האזנת סתר

צוות הבדיקה מציע, כי נוסף על הפירוט בבקשה להיתר לצו האזנת סתר של מאפייני ההאזנה והיקף המידע שצפוי להתקבל במסגרתה, לקיים השתלמויות עתיות במסגרתן הגורמים הטכנולוגיים במשטרת ישראל יציגו לשופטי בתי המשפט המחוזי המוסמכים להתיר האזנות סתר, את כלל הכלים הטכנולוגיים באמצעותם ניתן לבצע האזנת סתר, מאפייניהם, והיקף המידע המתקבל באמצעותם. פירוט כאמור יחזק בדרך נוספת את האפשרות של בתי המשפט במקרים הקונקרטיים לבצע איזון בין הצורך החקירתי למידת הפגיעה בפרטיות, ואף לבחון האם קיים אמצעי להאזנה שפגיעתו פחותה.

בקשות לחיפוש בחומר מחשב העוקבות לפעולה של האזנת סתר לתקשורת בין מחשבים ביחס לאותו מכשיר

לעמדת צוות הבדיקה, במבט צופה פני עתיד נכון כי במקרים בהם בוצעה האזנה לתקשורת בין מחשבים של מכשיר טלפון נייד או מחשב של יעד מסוים, ותוצרי האזנת הסתר הניבו מידע שהוביל לחקירה גלויה ולביצוע החיפוש גלוי באותו חומר מחשב, כי משטרת ישראל תביא לידיעת בית המשפט אשר דן בצו לחיפוש במחשב את העובדה כי בוצעה האזנה כאמור. הדברים עולים אף מפסק

הדין של בית המשפט העליון בדנ״פ **אוריך**,[41] שם נקבע מפי כב׳ הנשיאה חיות, כי במסגרת הגשת בקשה לבית המשפט לקבלת צו חיפוש לפי סעיף 23א לפקודת סדר הדין הפלילי, על מגישי הבקשה לכלול במסגרתה בין היתר פרטים בדבר בקשות חיפוש קודמות וההחלטות שניתנו בהן, ואשר בינן ובין בקשת החיפוש יש קשר ענייני. לעניין זה נקבע כי אין מדובר ברשימה סגורה, ועל רשויות החקירה להביא לידיעת בית המשפט כל פרט נוסף שיש לו רלוונטיות לחיפוש ואשר עשוי להשפיע על ההחלטה בבקשה.

[41] דנ״פ 1062/21 **יונתן אוריך נ׳ מדינת ישראל** פסקה 69 לפסק הדין של הנשיאה חיות (11.01.2022).

7. שרשרת האזנה

7.1 מהי שרשרת האזנה?

בפרק זה נסקור את תהליך שרשרת ההאזנה כפי שהוא כיום, בכל הנוגע לאמצעי תקשורת בין מחשבים, ובפרט ביחס למערכת סייפן. לצורך בדיקת הצוות, "שרשרת ההאזנה" הוגדרה ככלל השלבים השונים במסגרת ביצוע האזנת סתר, אשר ראשיתם בשלב העלאת הצורך הראשוני על ידי היחידה המזמינה לביצוע האזנת סתר ביחס ליעד מסוים, ועד לשלב הפקת התוצרים שהתקבלו מהמערכת בעניין אותו יעד.

מובן כי עשויות להתעורר סוגיות נוספות בכל הנוגע לתוצרי האזנת סתר, ביחס לשלבים מאוחרים יותר, כגון השימוש והעיבוד של ידיעות מודיעיניות המופקות מתוצרי האזנת סתר שבוצעו כדין על כל המשתמע מכך. ואולם יודגש כי צוות הבדיקה נדרש רק לשלבים האמורים לעיל, נוכח ייעודו הממוקד לבחון סוגיות הנוגעות להאזנה ללא סמכות.

הסקירה המובאת להלן לעניין שרשרת ההאזנה מבוססת על מסמכים שהועברו על ידי משטרת ישראל לצורך עבודת צוות הבדיקה, נוהלי האזנת סתר של חטיבת הסייבר במשטרת ישראל, וכן ישיבות של הצוות עם גורמים שונים במשטרה על מנת לבחון במבט כולל את הליך שרשרת ההאזנה.

נוכח מגבלות היכולת לבדוק האם ככלל אכן התהליך מבוצע בפועל כנדרש בנהלים – זאת הן נוכח היעדר סמכויות לצוות הבדיקה והן נוכח מגבלות משאבי הצוות ומיקודו – הבדיקה התמקדה בבחינת ההוראות והנהלים הקיימים לצורך מתן המלצות במבט צופה פני עתיד. מכאן, שבשונה מבדיקות אחרות של צוות הבדיקה בהן נבחנה האם בעבר בוצעו חריגות, אין בסקירה המפורטת מטה כדי למצות את הבדיקה בעניין זה ולהעיד האם תהליך שרשרת ההאזנה מראשיתו ועד סופו התקיים בהכרח בהתאם לנהלים, אלא אך לסקור מהו התהליך בפועל כפי שעלה בהתאם לבדיקת הצוות.

הגורמים הרלוונטיים בשרשרת ההאזנה

קיימים מספר גורמים רלוונטיים המעורבים בשרשרת ההאזנה:

1. <u>היחידה המזמינה</u> – היחידה בה נחקרת הפרשייה הקונקרטית במסגרתה מבוצעת האזנת סתר לתקשורת בין מחשבים. כפי שיפורט להלן, היחידה המזמינה שמביאה בפני חטיבת הסייבר את הצורך המבצעי להאזנה מסוג תקשורת בין מחשבים. ראש הדסק ביחידה אחראי על תכלול פעולות החקירה, ובכלל זה הפעולות מול חטיבת הסייבר לצורך האזנה לתקשורת בין מחשבים.
2. <u>מחלקת טכנולוגיות בחטיבת הסייבר (המפעילים)</u> – אחראית בין היתר על ביצוע התקיפה בפועל, ההתקנה של הכלי על מכשיר הטלפון ותפעולו של הכלי.
3. <u>מחלקת מענה מבצעי בחטיבת הסייבר (מ"מ)</u> – אחראית על הפקה של תוצרי האזנת סתר מסוג תקשורת בין מחשבים ברמת המענה הארצי (ככל שאין צוות סיגינטי משולב - צס"מ ליחידה המזמינה). מחלקה זו אחראית גם על תכלול הבקשות להאזנות סתר מסוג תקשורת בין מחשבים מהיחידות המזמינות ותיווכם אל הגורמים הרלוונטיים בחטיבת

הסייבר, ביניהם מחלקת טכנולוגיות. כמו כן אחראית על הכנת פקודת המבצע טרם ההתקנה.

4. צוות סיגינטי משולב (צס״מ) – יחידות הצס״מ הן חלק מיחידת השטח וכפופים פיקודית למפקד הימ״ר (יחידה מרכזית) ומקצועית לחטיבת הסייבר. בצס״מ יושבים המפיקים האחראים על הפקת התוצרים הסיגינטיים של היחידה המזמינה.

7.2 השלבים השונים בשרשרת ההאזנה

יצוין שוב, כי הדברים המפורטים להלן הם כעולה מהמסמכים שהועברו וכפי שנמסר מהגורמים השונים במשטרה ביחס לשרשרת ההאזנה נכון להיום.

שלב א׳ – העלאת צורך מבצעי להאזנה מסוג תקשורת בין מחשבים מהיחידה החוקרת אל חטיבת הסייבר

במסגרת חקירה משטרתית, במקרים בהם עולה צורך מבצעי לבצע האזנת סתר מסוג תקשורת בין מחשבים ליעד מסוים, היחידה החוקרת פונה אל חוליית מ״מ במחלקת מענה מבצעי בחטיבת הסייבר. במסגרת פניה זו על היחידה המזמינה לפרט על אודות החשד, מטרת ההאזנה, הראיות הקיימות בשלב זה, המכשיר שאליו מבוקש להאזין וכיו״ב. בשלב זה נבדק האם האזנת סתר לתקשורת בין מחשבים במקרה הנדון יכולה להוות מענה מתאים לפער החקירתי שהוצף על ידי היחידה החוקרת.

שלב ב׳ – בדיקת היתכנות טכנולוגית

ככל שהצורך המבצעי מאושר על ידי ראש חוליית מ״מ, מבוצעת על ידי החוליה הטכנולוגית במחלקת טכנולוגיות בחטיבת הסייבר בדיקה בדבר ההיתכנות הטכנולוגית לבצע האזנה מסוג תקשורת בין מחשבים ביחס למכשיר אליו מבוקש להאזין. בדיקות היתכנות אלו מבוצעות טרם הוצאת צו האזנת סתר מסוג תקשורת בין מחשבים, יובהר כי בשלב זה לא מתבצעת האזנה או חדירה לטלפון הנייד.

שלב ג׳ – הכנות לביצוע פעולת התקנה

אם נמצא כי קיימת אפשרות טכנולוגית להתקנה, מונחית היחידה החוקרת על ידי חוליית מ״מ לפנות לבית המשפט להוציא צו שיפוטי להאזנת סתר מסוג תקשורת בין מחשבים ביחס למכשיר בעניינו בוצעה הבדיקה.

לאחר שניתן צו שיפוטי הוא נבחן שוב על ידי חוליית מ״מ (למשל האם נקבעו מגבלות במסגרת ההיתר שניתן), ובהתאם אליו, נכתבת על ידי חוליית מ״מ פקודת מבצע המועברת לאישורו של רמ״ח מענה מבצעי בחטיבת הסייבר (דרגת נצ״מ).

שלב ד׳ – תהליך ההתקנה

ההתקנה מבוצעת על ידי חוליית טכנולוגיה.

טרם ההדבקה, נציג חוליית טכנולוגיות יחד עם נציג חוליית מ״מ עוברים על הצו השיפוטי ומזינים אותו אל המערכת מבחינת טווח הזמנים של הצו שניתן (בכל הנוגע לתאריך התחילה – לפי הנחיות

הייעוץ המשפטי למשטרה, כמפורט בנספח המשפטי, יש להזין את תאריך ההתקנה בפועל גם אם תאריך הצו השיפוטי קודם לתאריך ההתקנה). בהקשר של סייפן, בשלב זה מסומנים על ידי המפעיל ונציג חוליית מ"מ סוגי התוצרים אשר מבוקש שהמערכת תביא (כאמור, שלב זה החל רק עם הוספת מודול ה- warrant למערכת).

שלב ה' – הפקת התוצרים שהתקבלו

ההפקה של תוצרי האזנת הסתר לתקשורת בין מחשבים נעשית על ידי מפיקים שהוסמכו לכך. תפקידו של המפיק הוא לעבור על התוצרים שהתקבלו במסגרת האזנת הסתר, ולהזין אותם אל "טבלת הפקה" המהווה תמצית של תוכן התוצרים הרלוונטיים, התאריך בו התקבלו והסוג שלהם. בשלב ההפקה המפיק בוחן את מידת הרלוונטיות של התוצרים לצו ההאזנה שברשותו, ומפיק את התוצרים הרלוונטיים והמותרים להפקה בהתאם להנחיית העבודה בנושא

כפי שנמסר מהמשטרה, טבלת ההפקה הנוגעת לתוצרי האזנת סתר מסוג תקשורת בין מחשבים אינה מועברת אל היחידה המזמינה, אלא על בסיסה מבוצע על ידי המפיק זיקוק של המידע שנמצא כי הוא רלוונטי וזה מועבר בתצורת פרפראזה מודיעינית. עוד כפי שנמסר, יכול ויועבר מידע מודיעיני מהמפיק אל היחידה גם בעל פה במסגרת השיח השוטף ביניהם, כפי שגם עולה מהנחיית העבודה של חטיבת הסייבר. לאחר שהפרפראזה המודיעינית מועברת ל"דסק" שביחידה המזמינה, הדסק מפיק מהפרפראזה ידיעה מודיעינית, וזו מועברת לגורמי החקירות ביחידה.

בהתאם להנחיית העבודה של חטיבת הסייבר, חל איסור על הפקת התוצרים, בין היתר מהסוג שלהלן:

- אנשי קשר;
- פתקים;
- יומן;
- רשימת האפליקציות;

יצוין כי בממשק המשתמש של הרשאת המפיקים במ"מ ובצס"מ הם חשופים לא רק למידע המהווה תוצרי האזנת הסתר, אלא לכל המידע המגיע מהמערכת, הכולל אפילו מידע המוגדר על ידי המשטרה ככזה הנדרש למפעילים לצורך תפעול וביטחון הכלי, כגון רשימת האפליקציות ורשימת הקבצים. יצוין כי בהתאם להנחיית העבודה, חל איסור על הפקה של רשימת האפליקציות.

עמדות הפקה: ככלל, ההפקה של תוצרי תקשורת בין מחשבים מהמערכות השונות מבוצעת בעמדות המוצבות בחטיבת הסייבר. בכל הנוגע למערכת סייפן, תחילה ההפקה בוצעה אך ורק על ידי מפיקים השייכים לחוליית מ"מ ואשר יושבים בחטיבת הסייבר. עם התרחבות הפעילות הוסמכו גם מפיקים מהצס"מ להפקת תוצרים ממערכת סייפן שנמצאת בחטיבת הסייבר, כפי שנמסר על ידי המשטרה, לפני כשנה וחצי החל תהליך ביזור של פריסת עמדות הפקה למספר צס"מים וההפקה התקיימה בעמדות המוצבות בהם. ביזור פריסת עמדות ההפקה נועד ליתן מענה להתרחבות הצורך והשימוש באמצעי האזנה מסוג זה, וכן לתעל את היתרון המבצעי לשיטת המשטרה של עבודה צמודה בין המפיק ליחידה החוקרת. כך, היות שהמפיק מבצע את עבודת ההפקה במקום בו נמצאת היחידה המזמינה (ולא בעמדות המוצבות בחטיבה), מתאפשר לקיים שיח רציף בין המפיק ליחידה

על אודות הצ״ח, התפתחות החקירה וכיו״ב, ובכך מתאפשר הן עדכון בזמן אמת של היחידה החוקרת על אודות תוצרי האזנת הסתר, והן דיוק עבודת ההפקה ויעילותה בזמן אמת.

7.3 ממצאים והמלצות בעניין שרשרת ההאזנה

כאמור, עמדת צוות הבדיקה היא כי יש לוודא בטרם מתן אישור להפעלת המערכות, כי אלה תואמות מבחינת היקף היכולות הטכנולוגיות את הסמכויות שהמחוקק עיגן בחוק, ולא די לעניין זה בגידור נוהלי בלבד. בהינתן עמדה זו, במבט צופה פני עתיד, צוות הבדיקה אינו סבור כי נדרש שינוי מהותי בשרשרת ההאזנה במובנה הרחב מבחינת החשש לזליגת מידע האסור על פי דין אל היחידה החוקרת.

לצד האמור, יש לחדד בנהלים כי הדבקת יעד יכולה להיעשות רק לפי צו בית משפט יש להבטיח כי גדרי הצו מובאים באופן סדור, אל המפעיל בשלב ההדבקה, כפי שייקבע בנהלים, על מנת להבטיח כי כלל נתוני הצו נבדקים שוב על ידו בטרם ההדבקה ומוזנים למערכת באופן מדוקדק בהתאם לקבוע בצו.

בשים לב להיקף הפגיעה בפרטיות, נכון לצמצם ככל הניתן את הגורמים החשופים לתוכן המידע המתקבל. לדעת הצוות נכון כי יהיה מידור בין הגורמים הטכנולוגיים המפעילים את המערכת לבין הגורמים האמונים על הפקת המידע. יש לקבוע הפרדה ברורה בנהלים בין הגורם הטכנולוגי לבין הגורם שאחראי על מיצוי המידע שמתקבל, כך שעיון בתוצרים ייעשה אך ורק על ידי המפיק.

8. בחינת הליכי האישור ביחס למערכות להאזנה לתקשורת בין מחשבים המותקנות על מכשיר קצה

הצוות בחן את הליכי האישור וההנחיות המשפטיות שניתנו ביחס למערכות להאזנה לתקשורת בין מחשבים בדרך של הדבקת מכשיר קצה. בפרק זה נסקור את הליכי האישור וההנחיות המשפטיות שניתנו ביחס למערכת סייפן. הבדיקה נערכה על סמך מסמכים שהגישה המשטרה לבקשת הצוות, וכן מפגישות שערך הצוות עם גורמים רלוונטיים מהמשטרה - הן הממלאים תפקידים כיום והן מי שמילאו תפקידים בחטיבת הסייבר בעבר, וכן מהפרקליטות. יובהר כי מטרת בדיקה זו הייתה לבחון את השתלשלות האירועים המשמעותיים בעניין זה לאורך השנים, במבט על, בשים לב למאפייני עבודת הצוות כפי שנכתבו במבוא.

כפי שעלה מהמידע שנאסף על ידי הצוות, ניתנו ביחס למערכות שנבדקו מספר אישורים משפטיים והנחיות עבודה מטעם גורמים שונים במשטרה. ביניהם, הייעוץ המשפטי למשטרה והייעוץ המשפטי של חטיבת הסייבר. עוד קיימות הנחיות עבודה אשר ניתנו על ידי מחלקת הכוונה מקצועית בחטיבת הסייבר.

נמצא כי על אף שהייתה ידיעה בראשית הדרך לבעלי התפקידים הבכירים בחטיבת הסייבר והייעוץ המשפטי למשטרה ולחטיבה, כי למערכת סייפן יכולות החורגות מהסמכויות הנתונות למשטרה לפי חוק האזנת סתר, וכי נדרשים בענייה ניוונים טכנולוגיים לצורך התאמת מאפייניה לחוק, הלכה למעשה לא בוצעו הניוונים הנדרשים כתנאי מקדים להפעלתה.

במבט לאחור, הצוות סבור כי המשמעות הדרמטית של הכנסת מערכת בעלת יכולות טכנולוגיות פוטנציאליות רחבות היקף המהווה נקודת מפנה מבחינת עולם האזנות הסתר לתקשורת בין מחשבים לא הובנה לאשורה על ידי הגורמים הבכירים במשטרה. לאורך השנים לא יוחסה מלוא המשמעות המתבקשת להיקף היכולות הפוטנציאליות של המערכת ולעצם הכנסת חומרים אסורים אל מערכות המשטרה ומשמעות החריגה מסמכות, אף אם לא ייעשה בהם שימוש בפועל.

בכלל השלבים האמורים סוגיות עקרוניות אלה לא הובאו לאישור הייעוץ המשפטי לממשלה. כמו כן עלה כי על אף מעורבות של הייעוץ המשפטי למשטרה בהקשרים אחרים, סוגיות הנוגעות לשורשה של שאלת הסמכות לא הובאו לידיעה מפורשת של הייעוץ המשפטי למשטרה כפי שיפורט להלן.

נוכח ממצאים אלו, וכפי שיפורט בהמשך, ממליץ הצוות כדלקמן:

- על משטרת ישראל לוודא טרם רכישת מערכות טכנולוגיות או פיתוח עצמאי שלהן, ווּדאי שטרם השימוש בהן, כי מערכות אלה תואמות מבחינת הפוטנציאל הטכנולוגי את סמכויות המשטרה. לצורך כך נדרשת מעורבות משפטית הדוקה של הייעוץ המשפטי למשטרה. לעמדת הצוות, אין לעשות שימוש במערכות שיש חשש או פוטנציאל לכך ששימוש בהן, ובכלל זה איסוף מידע או עיבודו, יחרוג מגדרי סמכויות המשטרה – אלא באישור הייעוץ המשפטי לממשלה, ולאחר שנעשו כלל הצעדים הנדרשים כדי לוודא ששימוש במערכת לא תביא לחריגה מסמכות.

- הצוות מצא קושי משמעותי בהעדר כפיפות ישירה מקצועית ופיקודית של היועצים המשפטיים במשטרה ליועץ המשפטי למשטרה, וממליץ כי נושא זה ייבחן על רבדיו השונים בעבודת מטה שתערך בהקדם.
- קיימת חשיבות יתרה בביצוע פעולות פיקוח ובקרה אפקטיביות בכל הנוגע לאופן הפעלת האמצעים להאזנת סתר מסוג תקשורת בין מחשבים, על מנת לבחון האם הפעלת האמצעי והפקת התוצרים היא בהתאם להוראות החוק, היתר בית המשפט והנהלים.

להלן נפרט מבחינה כרונולוגית את השתלשלות האירועים העיקריים בעניין, ממצאי הצוות והמלצותיו.

8.1 בחינת הליכי האישור

8.1.1 מעבר ראשון מהאזנת סתר בתווך התעבורה לשימוש באמצעים המותקנים על מכשיר קצה

האזנת סתר לתקשורת בין מחשבים על ידי משטרת ישראל מבוצעת הן על ידי האזנה 'קלאסית' לתווך התעבורה של התקשורת, והן על ידי האזנה לתקשורת בין מחשבים באמצעות חדירה למכשיר קצה. ראו בפרק 2 פירוט על אודות ההבחנה בין האזנה לתווך התעבורה לבין האזנה באמצעות מכשיר המותקן על מכשיר קצה.

הבחינה המשפטית במשטרת ישראל בנושא ביצוע האזנת סתר באמצעות כלי שוהה על מכשיר קצה החלה עוד בשנת 2010 לקראת הפעלת מערכת "דייזי" אשר מותקנת על מחשבים. במסגרת המעבר להאזנה מסוג חדש, על ידי החדרת כלי שוהה על מכשיר קצה, התעוררו שאלות משפטיות עקרוניות אליהן נדרש הייעוץ המשפטי של המשטרה. חלק מהסוגיות שנדונו היוו מבחינת חטיבת הסייבר בסיס משפטי לשימוש בשנים מאוחרות יותר במערכת סייפן.

לא נמצאו מסמכים המעידים על דיון עקרוני בנושא זה במשרד המשפטים. אולם ידוע כי הפרשנות המפורטת בנספח המשפט לדוח זה, לפיה ישנה סמכות לחדירה למכשיר קצה לצורך האזנת סתר הייתה מקובלת על משרד המשפטים (ראו בהמשך בפרק 8.1.3).

<u>שימוש ראשון בכלי האזנת סתר השוהה על טלפון סלולרי</u>: בשנת 2013 פותחה במשטרה מערכת "חלוץ", אשר באמצעות נגישות פיזית מאפשרת חדירה לטלפונים ניידים ממספר מצומצם של דגמים ישנים, וביצוע האזנת סתר. לצוות הבדיקה לא נמסרו מסמכים בנוגע לאישורים משפטיים ביחס למערכת זו. נמסר לצוות הבדיקה מגורמים בחטיבת הסייבר, כי פעילות המערכת לוותה על ידי הייעוץ המשפטי למשטרה.

8.1.2 אישורים משפטיים והנחיות שניתנו למערכת סייפן

<u>הצורך בהתאמת המערכת לסמכויות המשטרה</u>

לכל המאוחר בסוף שנת 2012 הייעוץ המשפטי למשטרה והייעוץ המשפטי של חטיבת הסייבר בחנו את האפשרות המשפטית של שימוש המשטרה בסייפן בשים לב להיקף יכולות המערכת כפי שהיא, והצורך להתאמתה לסמכויות המשטרה מכוח חוק האזנת סתר. כפי שעולה מהמסמכים, היה ברור עוד באותו שלב כי מדובר באמצעי החורג מסמכויות משטרת ישראל בשל הפוטנציאל הטכנולוגי לאסוף מידע, שכן הוא מאפשר לקבל מידע אגור הקודם למועד האזנת הסתר וכן לקבל מידע שאינו

מהווה תקשורת בין מחשבים. על כן העמדה המשפטית הייתה כי יש לפעול על מנת להתאים את היכולות הטכנולוגיות של המערכת לסמכויות המשטרה הקבועות בחוק.

ממסמכי המשטרה השונים, עולה כי גם בשנים הבאות לפחות עד שנת 2015, ישנן התייחסויות מגורמים שונים במשטרה בנוגע לצורך לבצע התאמות טכנולוגיות הנדרשות מהמערכת, הן ביחס לסוגי תוצרים והן ביחס למידע אגור.

העקרונות שנדרשו באותו שלב מהמערכת, לפי מסמכי המשטרה, היו כי זו תהיה רלוונטית בעיקר לתעבורה המשודרת לרשת חיצונית וכי מידע השוהה במכשיר טרם התקנת הכלי לא ייאסף. כמו כן, נדרש כי על היירוט להתבצע קרוב מאד לזמן אמת לשידור התקשורת, וללא יכולת לקבלת מידע אגור או מסמכים.

בצד זאת, עולה מהמסמכים כי אותו זמן היה ברור לגורמים המעורבים, כולל הייעוץ המשפטי לחטיבה והייעוץ המשפטי למשטרה, כי המערכת מביאה מידע אגור, וכן מידע שאינו מהווה תקשורת בין מחשבים ואינו נכלל בגדרי הסמכות לפי החוק.

לא ידוע לצוות הבדיקה באיזה שלב הוחלט להפעיל את המערכת ועל ידי מי, על אף שלא בוצעו כלל הניוונים הטכנולוגיים הנדרשים על מנת שהמערכת לא תאפשר לאסוף מידע אגור טרם התקנת הכלי, וכן סוגי מידע מסוימים שאינם מועברים בתקשורת בין מחשבים (כגון אנשי קשר, יומן ופתקים). אולם ידוע כי דה פקטו, עם תחילת השימוש במערכת, לערך בתחילת שנת 2016 וכן לאורך תקופת פעילותה עד היום, המערכת הופעלה ללא ניוון טכנולוגי של היקף היכולות הפוטנציאליות האמורות לעיל, אשר אינן בסמכות משטרת ישראל להאזנת סתר לפי החוק. במקום ניוון טכנולוגי מלא, הפעלת המערכת, שלה יכולות עודפות, בוצעה תוך הסתמכות על נהלים והנחיות פנימיים אשר נועדו להתוות את המותר והאסור בנוגע לשימוש במערכת, ובהמשך, בשנת 2020, תוך הסתייעות במודול ה- warrant.

יודגש שוב, כי לפי בדיקת המסמכים טרם רכישת המערכת ולאחריה, ומהתרשמות צוות הבדיקה מהגורמים שאיתם נפגש – עלה כי העדר ניוון המערכת באופן מלא לא נבע מרצון המשטרה לעשות שימוש במידע החורג.

<u>**מודול ה- warrant**</u>**:** באפריל 2020 לערך, נכנס למערכת מודול ה-warrant אשר מאפשר למפעיל להגביל את סוגי התוצרים שיתקבלו לאורך תקופת ההאזנה. מודול זה איפשר למפעיל לסמן אילו סוגי תוצרים מבוקש לקבל במסגרת תקופת האזנת הסתר, וככל שלא סימן בשלב ההדבקה את הבקשה לקבל תוצרים מסוימים, למשל אנשי קשר או יומן – תוצרים אלו לא היו מתקבלים. כמו כן, מודול ה warrant איפשר, במקרים בהם הופעלה יכולת המערכת לקבלת מידע האגור (בהתאם לפרקטיקה המפורטת בפרק 5), להגביל את המועד שהחל ממנו יתקבל מידע ולקבוע כי זה יתקבל רק החל ממועד ההתקנה הראשון של הכלי על מכשיר הטלפון. יוזכר שוב, כמפורט בפרק 5, כי אף לפני תקופת ה warrant המערכת פעלה כברירת מחדל באופן של איסוף תוצרים רק מרגע ההתקנה ואילך, ומידע אגור הקודם למועד זה התקבל רק אם בוצעה בקשה אקטיבית לכך. יצוין כי אף מודול ה-warrant אינו מהווה ניוון טכנולוגי, אלא ממשק המאפשר למשתמש להגביל את עצמו. מכאן שהיקף היכולות הטכנולוגיות של המערכת גם לאחר אפריל 2020 נותר כמות שהוא, והגבלת קבלת סוגי מידע אסורים עודנה נותרה כפופה לנהלי חטיבת הסייבר.

נהלי חטיבת הסייבר

לחטיבת הסייבר נהלים אשר נועדו להתוות את דרכי העבודה לגורמים השונים בהליך ביצוע האזנת הסתר, החל משלב העלאת הצורך, הוצאת צו בית משפט, וכלה באופן הפקת התוצרים.

כאמור, לפי נוהלי חטיבת הסייבר משנת 2015, שעיקרם מפורט בדוח החסוי, ישנם, בין היתר, איסור על הפקת מידע הקודם למועד ההתקנה, ואיסור על הפקת פתקים, אנשי קשר ויומן. הנוהל עודכן בשנת 2017, ובמסגרת זו נוסף איסור על הפקה של רשימת האפליקציות.

לא היו הנחיות עבודה שהסדירו מהקצה אל הקצה את אופן הפעלת המערכת על ידי המפעילים האמונים על ביצוע ההדבקה, והסוגיות הייחודיות הנוגעות לשלב זה ורלוונטיות לעצם ביצוע האזנת הסתר (לעומת ההנחיות שהתייחסו לשלב ההפקה). הנחיות אלו מחויבות על מנת להתוות את המותר והאסור בשלב הפעלת הסמכות.

אם כן, אף מנוהלי החטיבה עולה בבירור כי היה ידוע שמערכת סייפן אוספת מידע החורג מהסמכויות הנתונות למשטרת ישראל על פי דין ועל כן נקבעו איסורים להפקה, הן לעניין סוגי התוצרים והן לעניין המועד שהתיר את ההפקה רק לגבי תוצרים שנקלטו במועד ההקלטה בפועל (מכאן למדים שהיה ברור כי למערכת יכולת לקבל מידע אגור הקודם למועד ההקלטה, שאם לא כן אין משמעות לקביעת מגבלה זו). לא ניתן לקבוע האם הייעוץ המשפטי של המשטרה הכיר נהלים אלה, ואולם כפי שנמסר לצוות הבדיקה על ידי הייעוץ המשפטי למשטרה – הם לא הכירו חריגות מגבולות הסמכות על פי חוק האזנות סתר, והניחו כי היכולות החורגות של המערכת נוונו באופן טכנולוגי.

דיונים פרטניים ביחס לסוגיות משפטיות שהתעוררו במהלך הפעלת המערכת

במהלך השנים התקיימו מספר דיונים בין חטיבת הסייבר לייעוץ המשפטי למשטרה לגבי סוגיות עקרוניות שהתעוררו בקשר לסייפן, בין היתר כמפורט להלן:

- ביום 20.8.2017 ניתנה הנחייה מטעם הייעוץ המשפטי למשטרה לפיה ניתן לקבל נתונים מהמערכת רק מרגע ההיתכנות הטכנולוגית לקליטת החומר ולא מרגע מועד תחילת תוקפו של צו בית המשפט. כלומר, ניתן היתר לקבלת חומרים ממועד ההדבקה בפועל, ולא ממועד תחילת תוקפו של הצו אשר עשוי היה להיות קודם למועד ההדבקה. סוגיה זו נדונה שוב בשנת 2019.
- ביום 23.5.2018 הייעוץ המשפטי למשטרה הנחה כי ניתן לקבל מידע אגור בתוך תקופת צו בית המשפט, אך רק החל ממועד תחילת ההאזנה הראשונה בפועל (אף אם היתר בית המשפט הוא קודם לכן), ובכפוף לכך שקיימת האזנה נוספת לתקשורת בין מחשבים במקביל ברקע. עוד הובהר באישור המשפטי כי פעולה זו אפשרית רק כאשר מתעורר צורך זמני ולא ניתן לאשרה כדפוס פעולה או פרקטיקה קבועה ושגרתית בה ישנה הסתמכות לפרקי זמן ממושכים על קיומה של האזנה מקבילה.

ראו בפרק 5 הרחבה בדבר הפרקטיקה שהחלה עוד לפני שניתן האישור המשפטי, פירוט על כך שהאישור ניתן בתקופה שבה לא ניתן היה מבחינה טכנולוגית להגביל את המועד שהחל ממנו יתקבל המידע, ועל כך שעובדה זו לא הובאה לידיעת הייעוץ המשפטי למשטרה. יתרה

מזאת, גם לאחר שניתן האישור המשפטי הפרקטיקה הייתה שונה מהמתווה שאושר, ולמעשה הנחיית הייעוץ המשפטי לא יושמה כלשונה.
הצוות לא מצא אינדיקציה לכך שאי קיום ההנחיה המשפטית נבע מכוונה לפעול בניגוד מפורש להן, אלא בשל העדר הקפדה על קבלת הנחיות באופן סדור והטמעתן.

עוד התקיימו דיונים בין חטיבת הסייבר לבין הייעוץ המשפטי למשטרה ביחס ליכולות קונקרטיות של המערכת והתנאים להפעלתן, כפי שמפורט בדוח החסוי.

<u>**מערכת נוספת להאזנת סתר לתקשורת בין מחשבים שבשימוש המשטרה**</u>

בשנת 2021 החל פיילוט בחטיבת הסייבר ביחס למערכת נוספת להאזנת סתר לתקשורת בין מחשבים. המערכת אושרה כפיילוט על ידי הייעוץ המשפטי למשטרה. מערכת זו אוספת מידע מרגע התקנת הכלי ואילך ולה היכולת במקרים קונקרטיים לקבל מידע אגור בכפוף להכנסת תאריכים מדויקים שמהם רוצים לקבל את המידע בשלב התקנת הכלי.

8.1.3 דיונים משפטיים שהתקיימו במשרד המשפטים

לאורך השנים היה ידוע לייעוץ המשפטי לממשלה, ולמחלקת הסייבר בפרקליטות המדינה, שקיימת מערכת להאזנת סתר בשם "סייפן", אשר מבצעת האזנת סתר על ידי חדירה למכשיר קצה. מבירור הצוות, על אף מערכת היחסים ההדוקה וההתייעצויות השוטפות של משטרת ישראל עם מחלקת הסייבר בפרקליטות ועם הייעוץ המשפטי לממשלה, לא נמצא מסמך או גורם שאיתו שוחח צוות הבדיקה (במשטרה או במשרד המשפטים), אשר מהם עולה כי הועבר לידי משרד המשפטים מידע בדרך זו או אחרת בדבר כלל מאפייני המערכת, ובאופן ספציפי מידע ביחס ליכולות הטכנולוגיות של המערכת אשר חורגות מהסמכות לפי חוק האזנת סתר.

באופן פרטני, בשנת 2018 נדונה יכולת מסוימת הנוגעת למערכת סייפן. לעניין זה התבקשה חטיבת הסייבר להציג בישיבת הדיווח העתית בראשות המשנה ליועצת המשפטית לממשלה (משפט פלילי) את הטכנולוגיה והנוהל המסדיר סוגיה זו. בהמשך לבקשה זו, הוסבר על ידי הייעוץ המשפטי לחטיבת הסייבר כי אין נוהל המסדיר ספציפית את הסוגיה וכי נוהל כאמור יגובש ויועבר למחלקת ייעוץ וחקיקה. כן עלה, כי במסגרת בקשות להאזנת סתר מתבקש באופן גורף מבית המשפט, במקרים בהם מבוקשת האזנה לתקשורת בין מחשבים לטלפונים ניידים, אף היתר לטכנולוגיה מסוג זו. הובהר על ידי המשנה ליועצת המשפטית לממשלה (משפט פלילי) כי אין מקום לבקש מבית המשפט היתר לטכנולוגיה ספציפית זו בכל פעם שבו מבוקש היתר כאמור, אלא רק במקרים בהם הדבר נדרש, ולאחר שנשקלו כלל ההיבטים. ביולי 2021 הועברה למחלקת ייעוץ וחקיקה הנחיית חטיבת הסייבר בנושא. לאחר שהועברו הערות מחלקת ייעוץ וחקיקה להנחיה, ובמסגרת ישיבת הדיווח העתית בראשות היועץ המשפטי לממשלה דאז, נקבע שוב כי אין לבקש האזנת סתר מסוג זה באופן אוטומטי עם הבקשה להאזנת סתר לתקשורת בין מחשבים של טלפונים ניידים, אלא יש להפעיל שיקול דעת בטרם הגשת הבקשה לבית משפט בשים לב למקרה הקונקרטי והאיזון הנדרש בנסיבות העניין.

מחלקת ייעוץ וחקיקה לא הכירה אף את המערכת הנוספת שנמצאת בשלבי פיילוט בשימוש המשטרה, וממילא לא את יכולתה לאסוף מידע הקודם למועד התקנת הכלי.

מעבר לדברים האמורים לעיל, לא הועבר לידיעת מחלקת ייעוץ וחקיקה פירוט על אודות כלל הסוגיות המשפטיות המפורטות לעיל, וממילא לא התקיים דיון משפטי עקרוני בנושא.

בכל הנוגע לפרקליטות, באוגוסט 2017 נערכה התייעצות של הייעוץ המשפטי למשטרה עם מחלקת הסייבר בפרקליטות המדינה לגבי שתי סוגיות שהתעוררו אגב חקירה קונקרטית, בה ניתנה עמדת הפרקליטות בכל הנוגע ליכולת מסוימת שקיימת למערכת.

נוסף על כך, באוגוסט 2018, במסגרת דיון בבית משפט במעמד צד אחד לקבלת היתר להאזנת סתר מסוג תקשורת בין מחשבים, הועברה חוות דעת מטעם מחלקת הסייבר בפרקליטות המדינה, אשר עולה כי נוגעת למערכת סייפן, ובה הובהר כי למשטרה יש סמכות לחדור למכשיר קצה מכוח סעיף 10א לחוק האזנת סתר אך הובהר כי אין בכך כדי להקנות למשטרה סמכות לחיפוש סמוי. מעבר לכך לא התקיים דיון מעמיק יותר על אודות אופייה ויכולותיה של המערכת, וממילא לא התקיים דיון על השלכות אפשריות על תיקים פליליים.

8.2 ממצאים

להלן יפורטו ממצאי צוות הבדיקה בכל הנוגע להליך האישורים כפי שנעשה בעבר, ובפרט ביחס למערכת סייפן.

1. **היעדר ניוונים טכנולוגיים מתחייבים למערכת סייפן:** הייתה ידיעה בראשית הדרך לכל הפחות לבעלי התפקידים הבכירים בחטיבת הסייבר ולייעוץ המשפטי למשטרה כי המערכת של חברת NSO היא מערכת בעלת יכולות לקבלת מידע האגור על מכשיר הטלפון הנייד ואותו "מוצר מדף" בעל יכולות טכנולוגיות החורגות מהסמכויות הנתונות למשטרת ישראל ועל כן נדרשים ניוונים טכנולוגיים. כפי שנמסר מהייעוץ המשפטי למשטרה לצוות הבדיקה, אלו הנחו את חטיבת הסייבר להתאים את המערכת לסמכויות המשטרה לפי חוק, ולאחר מכן לא היו מוכרות להם חריגות מגבולות סמכויות המשטרה לפי חוק האזנת סתר. הלכה למעשה לא נוונו יכולות טכנולוגיות אשר חורגות מהסמכויות על פי דין (כגון היכולת לקבל מידע אגור, וכן סוגי מידע שאינם תקשורת בין מחשבים, ביניהם אנשי קשר, יומן ופתקים). לעמדת צוות הבדיקה, ככל שלא הובהר לייעוץ המשפטי למשטרה כי בפועל לא בוצעו הניוונים ליכולות הטכנולוגיות על מנת להתאים את המערכת לסמכויות על פי דין, וכי הדרך להתאמת המערכת לחריגות מבחינת פוטנציאל היכולות היא בגידור נוהלי של שימוש במידע - היה על חטיבת הסייבר ליידע פוזיטיבית בעובדות אלו את הייעוץ המשפטי למשטרה, בטרם הפעלת המערכת, על מנת לבקש אישור משפטי להפעלת המערכת בהיעדר ניוון טכנולוגי מלא.

2. **נדרשו הנחיות משפטיות מובהקות ומפורטות כתנאי מקדמי להפעלת המערכת על מנת שזו תותאם לסמכויות על פי הדין:** מבלי לגרוע מהאמור לעיל בדבר הצורך בעדכון של חטיבת הסייבר את הייעוץ המשפטי למשטרה על החריגות של המערכת, סבור הצוות כי היה על הייעוץ המשפטי למשטרה לוודא כי הנחיותיו מיושמות. נוכח היקף הפגיעה הפוטנציאלי בזכויות יסוד, יש הכרח ליתן הנחיות משפטיות מדויקות ומפורטות לגבי התנאים הספציפיים הנדרשים לכניסת המערכת לתוקף מבחינת מאפייני המערכת. תנאים משפטיים מפורטים כאמור היו עשויים להבטיח כי ככל שיש פער בין ההנחיה המשפטית

לבין מאפייני המערכת או אופן הפעלתה, הייעוץ המשפטי למשטרה יעודכן ויהיה צורך לקבל את אישורו.

3. **מעורבות הייעוץ המשפטי למשטרה בסוגיות עקרוניות**: עולה כי ישנן סוגיות המחייבות ידיעה מפורשת ומעורבות של הייעוץ המשפטי למשטרה שלא הובאו לידיעתם. כמו כן עולה כי סוגיות עקרוניות הנוגעות לשורשן של שאלות הסמכות, ושאף יש בהן רגישות ציבורית מיוחדת, הוסדרו בהנחיות עבודה פנימיות ללא אישור משפטי של הייעוץ המשפטי למשטרה. בנוסף, למשל, הפעולה של קבלת מידע אגור הקודם למועד התקנת הכלי, בוצעה עוד טרם שניתן לכך אישור על ידי הייעוץ המשפטי למשטרה. עוד באותו הקשר, בנוגע לאישור המשפטי מיום 23.5.2018 של הייעוץ המשפטי למשטרה אשר הותיר קבלת מידע אגור עד למועד תחילת ההאזנה, בכפוף לתנאים – לא הובהרה לייעוץ המשפטי למשטרה עובדה מהותית הרלוונטית לצורך גיבוש העמדה המשפטית, בעניין מתן היתר לקבלת מידע אגור בתוך תקופת הצו כמפורט בהרחבה בפרק 5, לפיה אין אפשרות באותו זמן להגביל את המועד שהחל ממנו יתקבל המידע.

4. **היעדר הנחיות מספקות לשלב הפעלת המערכת:** לא היו הנחיות עבודה שהסדירו מהקצה אל הקצה את אופן הפעלת המערכת על ידי המפעילים האמונים על ביצוע ההדבקה, והסוגיות הייחודיות הנוגעות לשלב זה ורלוונטיות לעצם ביצוע האזנת הסתר. הנחיות אלו מחויבות על מנת להתוות את המותר והאסור בשלב הפעלת הסמכות. ההנחיות שהוצאו היו בעיקרן לגבי תהליך הנדרש עד להוצאת צו בית משפט, והנחיות לעניין אופן הפקת המידע, אך לא לשלב הפעלת המערכת. אף כאשר ניתנה הנחיה משפטית על ידי הייעוץ המשפטי למשטרה בעניין מסוים, הייעוץ המשפטי למשטרה וחטיבת הסייבר לא וידאו את יישומן.

5. **היעדר יידוע של הייעוץ המשפטי לממשלה**: אופן פעולת המערכת והיקף פוטנציאל היכולות של המערכת מבחינת החריגה מהסמכויות הנתונות לפי דין לא הועבר לידיעת הייעוץ המשפטי לממשלה. משלא הובאו הדברים לידיעת הייעוץ המשפטי לממשלה, ממילא לא התקיים דיון עקרוני בנושא במשרד המשפטים, והמערכת הופעלה מבלי שניתנה התייחסות משפטית כנדרש. למעלה מכך, אף סוגיות עקרוניות שהתעוררו במהלך הפעלת הכלי ואושרו משפטית על ידי הייעוץ המשפטי למשטרה לאורך השנים לא הובאו לידיעת הייעוץ המשפטי לממשלה.

8.3 המלצות

8.3.1 המלצות ביחס להליכי הטמעת מערכות טכנולוגיות חדשות במשטרת ישראל

1. **כלים התואמים את הסמכויות הנתונות למשטרה:** כמפורט בנספח המשפטי ובפרק 5 באופן כללי, יש לוודא במבט צופה פני עתיד כי מערכות טכנולוגיות אשר בשימוש משטרת ישראל תואמות את הסמכויות הקבועות בחקיקה. במקרה מושא ענייננו, גידור נוהלי אינו יכול להוות חסם מספק על מנת שניתן יהיה לראות בפעולות שבאופן גורף אינן מותרות לפי החוק כעומדות בתנאים.

2. **נדרשים נהלים נרחבים לאופן הפעלת מערכות טכנולוגיות:** נדרשים נהלים הנוגעים לכלל ההיבטים של שימוש במערכות, ובפרט הנחיות מפורטות לעניין אופן הפעלתן. הנחיות אלו מחויבות על מנת להתוות את המותר והאסור בשלב הפעלת הסמכות.

3. **נדרשת מעורבות משפטית הדוקה:** נדרש ליווי משפטי צמוד של הייעוץ המשפטי למשטרה לאורך תהליך הטמעת מערכות חדשות מראשיתו ועד סופו. זאת החל משלב אפיון הצורך, הבנת אופן הפעילות של המערכת, שדות התוצרים המתקבלים, ההשלכה על פלטפורמת הקצה עליו היא פועלת, ומאפייני השימוש השונים. תהליך זה מחייב שיח צמוד בין הגורמים הרלוונטיים בחטיבת הסייבר, ובכלל זה הגורם הטכנולוגי שתפקידו הבנת הטכנולוגיה לעומק על כלל רבדיה, לבין הייעוץ המשפטי המוודא כי הטכנולוגיה מותאמת לסמכויות המוקנות למשטרה על פי החוק. בהקשר זה יש להבטיח כי כלל התנאים הנדרשים מבחינה משפטית מתקיימים עוד טרם הפעלת הכלי.

4. **אישור הייעוץ המשפטי לממשלה על אודות כלים שלהם יכולות טכנולוגית מסוג חדש:** בשים לב לצורך לבחון בקפידה את התאמתם של כלים טכנולוגיים לסמכויות המשטרה נוכח היקף הפגיעה בזכויות יסוד, על המשטרה לוודא כי טרם רכישה או פיתוח עצמאי של מערכת טכנולוגית שלה יכולת חדשה מבחינת איסוף או עיבוד המידע, ושהיא בעלת פוטנציאל לחריגה מהסמכות הקבועה בחוק, וודאי שטרם השימוש בה, זו תועבר לאישור הייעוץ המשפטי לממשלה. זאת תוך פירוט כלל מאפייני המערכת והתנאים להפעלתה, בצירוף עמדה משפטית מטעם המשטרה בדבר מקור הסמכות.

5. **החלת העקרונות באופן רוחבי:** על המשטרה לוודא כי כלל הפיתוחים או הרכש הנוגעים בין היתר לסוגיות של סיגינט או סייבר מאושרים על ידי גורם מרכזי במטה ועל ידי הייעוץ המשפטי למשטרה. יש להחיל את כל הכללים הנדרשים כמפורט בדוח זה, על מקרים כאמור, גם אם לא פותחו או נרכשו על ידי חטיבת הסייבר.

8.3.2 המלצות בעניין הייעוץ המשפטי לחטיבת הסייבר והייעוץ המשפטי למשטרה

בשים לב לממצאים המפורטים לעיל בכל הנוגע להיעדר מעורבות משפטית הדוקה בסוגיות שונות הן טרם הפעלת הכלי והן במהלכו, אישור נהלים וכן סוגיות אשר חייבו ידיעה מפורשת ומעורבות של הייעוץ המשפטי למשטרה, צוות הבדיקה בחן את הנסיבות המבניות שעשויות היו להוביל לפער כאמור.

תפקיד הייעוץ המשפטי למשרדי הממשלה מוסדר בהנחיית היועץ המשפטי לממשלה מס' 9.1000[42] בפתחה נקבע כי תפקידו "לייעץ ולהנחות את כלל גורמי המשרד בהיבטים המשפטיים של פעולתם. במסגרת זו עליו, בין השאר, לסייע ולהעמיד לרשות המשרד את הכלים והאמצעים המשפטיים הדרושים ליישום מדיניות המשרד. במילוי תפקידו זו, עליו לשמש גם "שומר סף", כדי להבטיח כי פעילות המשרד ונושאי המשרה בו תתבצע על-פי הדין וכללי המינהל התקין. ככלל, על היועץ המשפטי למשרד לפעול לשם קיומו וחיזוקו של שלטון החוק."

[42] הנחיית היועצת המשפטית לממשלה מס' 9.1000 בדבר היועצים המשפטיים למשרדי הממשלה משנת 2002 (עודכן לאחרונה בשנת 2015)

בכל הנוגע לפניות ליועצת המשפטית לממשלה ולמחלקת ייעוץ וחקיקה, בהנחיה 9.1000 נקבע כי ככלל יש לעודד פעילות עצמאית של היועצים המשפטיים למשרדי הממשלה בענייני משרדיהם, וזאת מבלי לפגוע בכפיפותם המקצועית ליועצת המשפטית לממשלה, ובתיאום הנדרש של עבודתם עמה. בצד זאת, ניתן או יש להפנות לגורמים האמורים סוגיות הדורשות אישור, הכרעה או התייעצות. בפרט, ניתן או יש להפנות לאישור בעיות ונושאים בעלי רגישות מיוחדת, ציבורית או אחרת, או שאלות עקרוניות בעלות השלכות רוחב משמעותיות על משרדים נוספים, או בעלות השלכות בתחומי העונשין, וכן לשם קבלת גיבוי מקצועי בשל קושי פנימי מול הנהלת המשרד.

במסגרת עבודת הצוות, כחלק מבחינת סוגיות הנוגעות למעמד היועץ המשפטי למשטרה ותפקידו ולדפוסי העבודה מול הייעוץ המשפטי לממשלה, לבקשת הצוות התקיימה פגישה מקצועית עם כב' השופט בדימוס פרופ' יצחק זמיר, אשר כיהן בתפקיד היועץ המשפטי לממשלה בין השנים 1986-1978 וכשופט בית המשפט העליון בין השנים 1994-2001. פגישה זו חיזקה את עמדת הצוות בעניין חשיבות המשך עידוד פעילות עצמאית של הייעוץ המשפטי למשטרה, תוך אחריות להיותו "שומר הסף" של המשטרה. במקביל התחזקה עמדת הצוות ביחס לחשיבות קיומה של כפיפות מקצועית היוצרת ציר ישיר לאורך כל שרשרת הייעוץ המשפטי למשטרה ועד ליועצת המשפטית לממשלה: דהיינו, בהמשך לכך שמקצועית היועץ המשפטי למשטרה כפוף לעמדת היועצת המשפטית לממשלה, נדרש להבטיח כי יתר הגורמים האמונים על ייעוץ משפטי במשטרה יהוו המשך ישיר של ציר זה.

נוכח הדברים האמורים – הן לעניין תפקידו של הייעוץ המשפטי למשטרה מול הגורמים השונים בתוך המשטרה והן בדבר אחריותו להבאת נושאים בעלי רגישות מיוחדת לאישור היועצת המשפטית לממשלה, וכל זאת בשים לב לממצאים אשר פורטו בהרחבה לעיל, צוות הבדיקה גיבש את ההמלצות כדלקמן:

1. **הצוות מצא קושי משמעותי בהעדר כפיפות ישירה מקצועית ופיקודית של היועצים המשפטיים במשטרה ליועץ המשפטי למשטרה, וממליץ כי נושא זה ייבחן על רבדיו השונים בעבודת מטה שתערך בהקדם**: בהקשרים רבים קיימת עבודה צמודה ומתואמת בין הייעוץ המשפטי למשטרת ישראל לבין הייעוץ המשפטי לחטיבת הסייבר. עם זאת, בפועל הייעוץ המשפטי לחטיבת הסייבר אינו כפוף פיקודית ומקצועית לייעוץ המשפטי למשטרה. אין זה ייחודי במשטרת ישראל לעניין חטיבת הסייבר בלבד. גורמים האמונים על מתן ייעוץ משפטי בחטיבות השונות במשטרה ובכלל זה באגף החקירות והמודיעין אליה משתייכת גם חטיבת הסייבר, אינם כפופים באופן ישיר, פיקודית ומקצועית, ליועץ המשפטי למשטרה, זאת בשונה מהכפיפות הישירה בצה"ל של מערך הייעוץ המשפטי לפרקליט הצבאי הראשי, ומכפיפות מקצועית של מערך הייעוץ המשפטי ליועץ המשפטי של שירות הביטחון הכללי. עמדת הצוות לעניין הצורך בבחינה של נושא זה נובעת ממספר טעמים:

   ראשית, צוות הבדיקה סבור כי לאור ממצאי בדיקת הליכי האישור של מערכת סייפן ואופן הפעלתה, כמקרה בוחן באופן כללי לסוגיות הנוגעות לקשרי העבודה בין הייעוץ המשפטי לחטיבה למול הייעוץ המשפטי למשטרה - היעדר כפיפות ישירה עלולה להוביל שוב לכך שסוגיות המחייבות ידיעה ומעורבות של הייעוץ המשפטי למשטרה, לא יובאו לידיעתם המפורשת. שנית, מן העבר השני, כפיפות זו תחזק את המעורבות היזומה של היועץ

המשפטי למשטרה ביחס לנעשה בחטיבות, ותשפר את יכולתו לשמש כשומר סף, וכן את יכולתו של היועץ המשפטי לחטיבה. שלישית, כפיפות כאמור תוודא אחידות בעמדות המשפטיות הניתנות. רביעית, בשונה מהיועץ המשפטי לחטיבה, לייעוץ המשפטי למשטרה ראיית הרוחב ביחס לכלל הנעשה במשטרת ישראל לצורך גיבוש עמדה רוחבית ביחס לסוגיות עקרוניות המתעוררות ביחידות השונות.

2. **נדרש ליווי משפטי הדוק אף לאחר הטמעת מערכות חדשות:** בהמשך ישיר לאמור לעיל ונוסף על המפורט בהמלצות בדבר הצורך במעורבות משפטית הדוקה בהליכי הטמעת מערכות טכנולוגיות חדשות במשטרת ישראל - נוכח העובדה כי האזנת סתר מהווה פגיעה חריפה בפרטיותו של אדם, נדרש יידוע ושיתוף של הגורמים המשפטיים אף ביחס לסוגיות המתעוררות אגב השימוש בטכנולוגיה. יש הכרח להציף באופן שוטף בפני הגורמים המשפטיים את כלל המאפיינים, היכולות והמשמעויות של הפעולות השונות המבוצעות באמצעות מערכות טכנולוגיות. זאת לתכלית כפולה: הן על מנת שכאשר מובאת בפני הייעוץ המשפטי סוגיה משפטית הם יוכלו לבחון אותה על בסיס תשתית עובדתית מלאה ולשקול את ההשלכות המשפטיות העולות ממנה, והן בכדי שהייעוץ המשפטי יוכל לזהות באופן אקטיבי נקודות המעוררות שאלה משפטית.

3. **מעורבות הייעוץ המשפטי למשטרה בהנחיות חטיבת הסייבר**: נוהלי עבודה או הנחיות עקרוניות הנוגעות להפעלת סמכות, ודאי סמכות כה פוגענית כמו האזנת סתר, מחייבים את אישור הייעוץ המשפטי למשטרה. זאת בין אם ההנחיה מוסדרת במדרג נורמטיבי של נוהלי משטרה, ובין אם במדרג נורמטיבי אחר כמו הנחיית עבודה.

4. **דיון בשאלות עקרוניות הנוגעות לפרשנות החוק:** הייעוץ המשפטי לממשלה הוא הגורם המוסמך במשרד המשפטים למתן ייעוץ בעניין סוגיות עקרוניות המעוררות שאלה משפטית בכל הנוגע להיקף הסמכות של משטרת ישראל, ובכלל זה סוגיות כאמור המתעוררות אגב תיק פלילי מסוים.

8.4 הליכי פיקוח ובקרה בחטיבת הסייבר

בהינתן העובדה כי לא בוצע ניוון טכנולוגי מלא למערכות, והגידור לעניין היקף הסמכות נותר גידור נוהלי בלבד, ביקש צוות הבדיקה לבחון אילו הליכי פיקוח ובקרה בוצעו לאורך השנים במשטרת ישראל על מנת לוודא כי אכן הפעלת הכלי ואופן הפקתו תואם את המגבלות שהותוו בנהלים. באופן ספציפי ביקש הצוות לבחון האם הייתה בקרה בכל הנוגע להפעלת המערכת שלא בהתאם להנחיות המקצועיות והמשפטיות שניתנו, קבלת מידע החורג מהסמכויות הנתונות לפי דין, וכן בקרה לעניין צפייה במידע או הפקתו בניגוד לנהלים.

כפי שנמסר מהמשטרה, קיימות שלוש סוגי בקרות בעניין האזנה לתקשורת בין מחשבים:

1. בקרת מפקד – בקרה על חוליית מ״מ.
2. בקרה מקצועית – בקרה על חוליית מ״מ וצס״מ מחוזי בתחום התקשורת בין מחשבים.
3. בקרת אבטחת מידע במסגרת הבקרות העיתיות.

מבחינת הבקרות הפיקודיות, הוסבר כי רמ"ד הפקה ורמ"ד החוליה ביצעו בקרות יומיומיות על החוליה והיחידות (בהתאמה); זאת עד לביזור הפקת התוצרים למחוזות, בעת הקמת הצס"מים בשנת 2021. מאז, בוצעו בצס"מים בקרות על ידי חוליית מ"מ. באשר לבקרות שבוצעו על ידי מדור הכוונה מקצועית, נמסר כי החל משנת 2017 בוצעו בקרות שנתיות במ"מ ובצס"מים לאחר הקמתם. בקרות אבטחת מידע בוצעו מעת לעת על ידי ראש חוליית ביטחון מקורות מידע במ"מ ובצס"מים. כמו כן, בנוגע לפיקוח ובקרה ביחס למערכת הפיילוט, נמסר כי בוצעה בקרה של ראש חוליית מ"מ וכן סטטוסים שבועיים לבחינת הפיילוט בהשתתפות גורמי טכנולוגיות, הכוונה מקצועית, חוליית מ"מ ומחלקת מענה מבצעי.

צוות הבדיקה בחן באופן מדגמי שני דוחות בקרה מהסוגים המפורטים מעלה. כפי שעולה מהדוחות שנבדקו, אלו אינם נוגעים לסוגיות המפורטות מעלה, אלא ליעילות השימוש בכלי וסוגיות של אבטחת מידע.

נוסף על כך, הצוות ביקש מהמשטרה לקבל דוגמאות לבקרות הנוגעות באופן פרטני לפיקוח בדיעבד על אודות היכולות החורגות של המערכת, דהיינו בקרות אשר מטרתן לבדוק האם השימוש במערכת ובכלל זה הפקת התוצרים המתקבלים ממנה נעשה בהתאם לנהלים אשר היוו החסם היחיד מפני שימוש במערכת על כלל יכולותיה. כפי הנמסר מהמשטרה לא היו בקרות אשר בחנו היבט מסוים זה בכל הנוגע להאזנת תקשורת בין מחשבים.

בידיעה כי המערכת לא נוונה מבחינה טכנולוגית, וכי עודנה קיימת יכולת טכנולוגית להפעיל את המערכת על שלל יכולותיה (קבלת סוגי תוצרים אסורים וקבלת מידע האגור על הטלפון הנייד), המשטרה שמה את מרכז יהבה על נהלי עבודה והנחיות פנימיות שיהוו את החסם מפני שימוש בלתי חוקי במערכת והגבלת הפקת התוצרים העודפים שמתקבלים על ידה.

בהינתן שלא בוצעו ניוונים טכנולוגיים, חשיבות קיומה של בקרה כאמור לאורך השנים במשטרת ישראל, מקבלת משנה תוקף נוכח כך שבלחיצת כפתור ניתן פוטנציאלית לקבל היקף מידע החורג באופן משמעותי מזה המותר על פי דין. לא זו אף זו, פיקוח בדיעבד לעניין עיון והפקת התוצרים הוא הכרחי, שכן לכל הפחות עד אפריל 2020, בשים לב למאפייני המערכת והיעדר מודול ה-warrant עד לאותו שלב (אשר איפשר להגביל את סוגי התוצרים שיתקבלו), במסגרת האזנת הסתר התקבלו בהכרח תוצרים אשר אף לשיטת המשטרה אותו זמן היו אסורים (כמו אנשי קשר, יומן ופתקים).

יודגש כי צוות הבדיקה שותף לעמדת המשטרה אשר הוצגה בפניו, לפיה מתחייבת הנחת המוצא במסגרת תפישת הפעלת סמכויות באופן כללי, וכן במסגרת ביצוע האזנת סתר מסוג תקשורת בין מחשבים באופן פרטני, כי הגורמים במשטרת ישראל האמונים על הפעלת המערכת והפקת התוצרים המתקבלים ממנה, פועלים בהתאם לסמכות ולנהלים. כפי שהודגש על ידי המשטרה, קיימים מקרים רבים בהם מסגרת ביצוע האזנות סתר, לשוטר שיקול דעת ויש לצאת מנקודת מוצא כי זה מפעיל אותו בהתאם לתנאים אשר הותוו והוגדרו. כך לשם דוגמא, כאשר מפיק שמע מאזין להאזנת סתר ומסתבר כי מדובר בשיחה חסויה עם עורך דין – עליו שלא להאזין לשיחה. גם כאן, האיסור בחוק על האזנה לשיחות חסויות עם עורך דין, מותנית ביישומה בפועל על ידי השוטר הספציפי.

ואולם לעמדת צוות הבדיקה אין בהנחת מוצא זו כדי לגרוע מהצורך בביצוע פיקוח בדיעבד. ודאי במקרה מושא עניינו, כאשר הוחלט לעשות שימוש במערכת אשר הלכה למעשה אוספת מידע אשר אינו מותר לפי החוק, ואף ניתן באמצעותה, בקלות שבלחיצת כפתור, לשאוב מידע רחב האגור על הטלפון הסלולרי של יעד ההאזנה.

אף על פי כן, המשטרה לא ביצעה הליכי פיקוח ובקרה שיבטיחו את הפעלת המערכת בהתאם לנהלים שנקבעו.

8.5 המלצות לעניין הליכי פיקוח ובקרה

כאמור בפרק 5, הצוות סבור כי על מנת לפעול בהתאם לסמכויות הנתונות למשטרה על פי דין, יש הכרח לנוון את המערכות כך שאלו לא יאספו מידע החורג מזה המותר לפי חוק האזנת סתר וודאי שלא תהיה סמכות לאסוף מידע האגור על הטלפון הנייד.

לצד האמור, עודנה קיימת חשיבות יתרה בביצוע פעולות בקרה לעניין כלים רגישים ופוגעניים אלה, על מנת לוודא כי הפעלת הכלי והפקתו היא בהתאם לנהלים, ובהתאם לצו בית המשפט שניתן. כך גם לעמדת חטיבת הסייבר, כפי שהוצג לצוות הבדיקה, נכון במבט צופה פני עתיד לייחד בקרות מסוגים שונים על אודות הפעלת הכלים והפקתם. לעניין זה הוקם לאחרונה צוות פיקוח ובקרה הכפוף לראש חטיבת הסייבר אשר ייעודו לבצע בקרה בציר הטכנולוגי, מתודולוגי ומבצעי.

נוסף על כך, על מנת שתתקיים בקרה אובייקטיבית בהתבסס על בסיס הנתונים של המערכות, יש לוודא כי מערכות יאפשרו שליפת דוחות פעולה שיאפשרו ביצוע בקרה בדיעבד בקלות, תוך אינדיקציה ברורה לעניין כל אחד משלבי התהליך. לצורך כך נדרש שיופיע בדוחות הפעולות המופקים מבסיס הנתונים, שדות הכוללים בין השאר את: מספר הצו, טלפון יעד ההאזנה, מועדי הצו שהוזנו, סוג הפעולה שבוצעה ביחס ליעד ומועדה, מועד הסרת הכלי, והמשתמש שביצע כל אחת מהפעולות. נדרש כי ניתן יהיה להפיק את הדוח באופן המאפשר מיון לפי כל אחד מהשדות הנ"ל.

עוד לשם ביצוע בקרה אפקטיבית, נדרש כי ביחס לכלל המערכות שבידי משטרת ישראל להאזנת סתר, לכלל המשתמשים במערכת לא תהיה האפשרות לבצע מחיקות ושינויים בדיעבד בבסיס הנתונים. לצד זאת, במקרים בהם קיימות טעויות בהזנת פרטים למערכת, נדרשת יכולת לתעד את הסיבה לטעות.

9. יועצים חיצוניים

נבקש להתייחס בתמצית לטענות שעלו בפרסומים בכלכליסט באשר לשימוש המשטרה ב"האקרים" חיצוניים לצורך תקיפת מכשירי קצה. לאחר שיחות שהתקיימו עם בעלי תפקידים רלוונטיים בחטיבת הסייבר בהווה ובעבר, וכן כפי שעולה מהתייחסות שהועברה בכתב על ידי חטיבת הסייבר, עלה שאכן קיימים יועצים חיצוניים המועסקים על ידי משטרת ישראל.

ביום 18.1.22 עם פרסום הטענות בתקשורת, הועברה התייחסות כתובה של משטרת ישראל אל המשנה ליועצת המשפטי לממשלה (משפט פלילי), בה הובהר כי הפעלת מערכת סייפן נעשית רק על ידי שוטרים המוסמכים לכך במשטרת ישראל.

עוד נמסר במכתב זה כי היועצים החיצוניים מועסקים על ידי המשטרה לאחר שעברו את כל הסיווגים הנדרשים לשם עבודתם בחטיבה, בהתאם לאופי פעילותם, וכי עבודתם התבצעה תחת הוראות ופיקוח של המשטרה.

דברים אלה תואמים את אשר נמסר לצוות הבדיקה במהלך הישיבות שקיים עם גורמים שונים במשטרת ישראל בעבר ובהווה. בפגישות אלה נמסר כי היועצים החיצוניים לא נטלו חלק בהפעלת מערכת סייפן, או מערכות אחרות שמטרתן האזנה למכשיר קצה, למעט האזנה לתקשורת בין מחשבים של מצלמות אבטחה. לעניין זה עלה בישיבות הצוות כי היועצים החיצוניים סייעו במקרים קונקרטיים ביחס לפעילות טכנולוגית מסוימת, לעיתים פיזית ולעיתים מרחוק, וזאת בליווי שוטר. כמו כן, סייעו היועצים החיצוניים במחקר רשת לגבי סוגיות טכנולוגיות עקרוניות שעלו. עוד נמסר כי ישנם יועצים חיצוניים העוסקים בניהול פרויקטים במשטרה, למשל, בהתנהלות מול חברות התקשורת בתחומים שונים.

עם זאת, יש לציין כי בשיחה עם גורם אחד מכלל הגורמים שעמם נפגש צוות הבדיקה, נטען לנכונות הטענות שפורסמו בתקשורת בהקשר מסוים זה. צוות הבדיקה לא התרשם מכך שהמידע שנמסר נובע מהיכרות ישירה של אופי הפעילות של היועצים החיצוניים. נוסף על כך, בכל הנוגע להיקף הסיווג הביטחוני, אף אם הליך סיווג שונה מזה של שוטרים במשטרת ישראל, אין בכך כדי לקבוע כי מדובר בסיווג לא מספק. לטענת הגורמים הבכירים במשטרה מדובר בהליך סיווג והכשרה המספק לאופיו של התפקיד.

לא למותר לציין כי לעמדת הצוות יש חשיבות לכך שכלל הגורמים במשטרת ישראל, בין אם אלו שוטרים או יועצים חיצוניים, אשר מעורבים בהפעלת סמכויות יעברו את ההכשרה הנדרשת להטמעת סוגיות משפטיות הנוגעות לגבולות סמכות משטרת ישראל.

לסיכום, הצוות לא מצא מידע המבסס את הטענות שהתפרסמו בהקשר זה. נוכח האמור, ומיקוד עשייתו של הצוות בטענות המרכזיות שנטענו, לא מצא הצוות מקום להרחיב מעבר לבדיקות שבוצעו.

10. פיקוח משרד המשפטים על האזנות סתר של משטרת ישראל

10.1 פיקוח היועץ המשפטי לממשלה על האזנות סתר - רקע

כאמור בפרק 1 לדוח, לפי סעיף 6(ו) לחוק האזנת סתר, על המפכ״ל להגיש מדי חודש דין וחשבון ליועץ המשפטי לממשלה על היתרי האזנת סתר שניתנו ועל תנאיהם.[43] אם כן, לפי חוק האזנת סתר, על היועץ המשפטי לממשלה לערוך פיקוח בדיעבד על היתרים להאזנות סתר פרטניות שניתנו למשטרת ישראל (האזנות לשם גילוי, חקירה או מניעה של עבירה מסוג פשע, לגילוי או תפיסה של עבריינים שעברו עבירות פשע או לחקירה לצרכי חילוט רכוש הקשור בעבירת פשע).[44]

במסגרת הדיווח העיתי שמועבר ליועץ המשפטי לממשלה, מפורטים ביחס לכל האזנה שנתבקשה מבית המשפט (גם אם זו סורבה), העבירה שביסוד הבקשה להאזנה שהוגשה; זהותו של האדם שביחס אליו בוצעה ההאזנה;[45] סוג ההאזנה שהותרה (למשל האזנת שמע לטלפון נייד או האזנה לתקשורת בין מחשבים); משך ההיתר שניתן על ידי בית המשפט; תמצית הנימוקים להאזנה שהוצגו בפני בית המשפט והחלטת בית המשפט.

לאחר קבלת הדיווח, מתקיימות ישיבות תחילה בראשותה של המשנה ליועצת המשפטית לממשלה (משפט פלילי) יחד עם נציגות מחלקת ייעוץ וחקיקה במשרד המשפטים, נציגי חטיבת הסייבר, נציגי הייעוץ המשפטי למשטרה ונציגי הפרקליטות. ישיבות אלו נערכות לאחר שבוצעה בחינה ראשונית של תמצית <u>כלל</u> הבקשות וההיתרים להאזנת סתר לתקופת הדיווח על ידי ייעוץ וחקיקה, ונדונים במהלכן היתרים אשר עוררו שאלה עובדתית או משפטית. במסגרת בחינה זו מוצגות על ידי המשטרה – לגבי ההיתרים שעוררו שאלות – הבקשות שהוגשו לבית המשפט, ובכלל זה הנימוקים המפורטים שבבסיסן, פרוטוקול הדיון וכן החלטת בית המשפט.

נוסף על האמור, אגב ישיבות הדיווח מתעוררות לעיתים סוגיות עקרוניות אשר אינן נוגעות למקרה קונקרטי, ואף הן נבחנות במסגרת הישיבות או לחלופין מתקיים לגביהן דיון נפרד ספציפי ככל שהן דורשות בחינה פרטנית. במסגרת כך יכול שיתקיים דיון בסוגיות הנוגעות לפרשנות משפטית של הוראות החוק השונות, נוהלי המשטרה בכל הנוגע להאזנות סתר, ועוד. בעקבות ישיבות אלה, במקרים בהן נדרש, ניתנות הנחיות או דגשים למשטרת ישראל על ידי המשנה ליועצת המשפטית לממשלה (משפט פלילי).

לאחר ישיבות הדיווח בראשות המשנה ליועצת המשפטית לממשלה (משפט פלילי), מתקיימת אחת לתקופה ישיבה בראשות היועצת המשפטית לממשלה, במסגרתה מועלים לעדכון הבקשות וההיתרים להאזנת סתר אשר עוררו שאלות או דיון. במקרה הצורך מובאות בדיון זה סוגיות להכרעתה המשפטית של היועצת, וככל הנדרש ניתנות הנחיות למשטרת ישראל.

---

[43] יצוין כי עד לאחרונה היה פיגור במועד העברת הדיווחים לפי סעיף 6(ו).
[44] היועץ המשפטי לממשלה מפקח בנוסף לכך גם על היתרים שניתנו לתכליות של ביטחון המדינה ומניעת דלף ביטחוני.
[45] אם הוא ידוע מראש. כך למשל ייתכן כי אותה של הגשת הבקשה להאזנה היה ידוע רק מספר הטלפון אשר קשור בעבירה אך טרם יש מידע לעניין זהותו של המשתמש באותו מספר טלפון.

יוער כי מעורבות גורמי הייעוץ המשפטי לממשלה אינה מוגבלת אך לישיבות הדיווח להאזנות סתר. במסגרת שגרת העבודה השוטפת עם משטרת ישראל, כפי שאף נהוג אל מול יתר הלשכות המשפטיות במשרדי הממשלה, מובאות על ידי המשטרה באופן שוטף סוגיות המעוררות שאלה משפטית מורכבת הדורשת את עמדת הייעוץ המשפטי לממשלה. דיון בסוגיות משפטיות עשוי אף להתעורר באופן יזום על ידי גורמי הייעוץ המשפטי במשרד המשפטים ככל שסוגיות אלו מובאות לידיעתם בדרך אחרת, כגון בפניית ציבור או בעקבות פרסום בתקשורת, בהן עולות סוגיות טכנולוגיות עקרוניות המעוררות שאלה הדורשת קבלת עמדה משפטית בנושא.

לסיום חלק זה, ולצורך שלמות התמונה, יצוין כי נוסף על תפקידה של היועצת המשפטית לממשלה לבצע פיקוח ובקרה בדיעבד המוסדר בסעיף 6(ו) לחוק האזנת סתר, המחוקק קבע נסיבות מסוימות בהן על המשטרה לקבל אישור של היועצת המשפטית לממשלה או של פרקליט המדינה בטרם פניה לבית משפט להוצאת צו האזנת סתר, למשל בכל הנוגע לבקשה להאזנה לשיחות חסויות לפי סעיף 9א לחוק,[46] או לפי סעיף 2א לחוק חסינות חברי הכנסת, זכויותיהם וחובותיהם, התשי״א-1951, כאשר מבוקש להאזין לחבר כנסת, שר או סגן שר.

10.2 ממצאים והמלצות

כמפורט בהרחבה בפרק 8.1.3, לא הועבר המידע הנדרש בעניין מערכת סייפן, על כלל מאפייניה, לידיעת הייעוץ המשפטי לממשלה, וממילא לא התקיים דיון משפטי עקרוני בנושא.

להלן יפורטו ההמלצות בנושא.

אישור הייעוץ המשפטי לממשלה על אודות כלים שלהם יכולות טכנולוגית מסוג חדש: בשים לב לצורך לבחון בקפידה את התאמתם של כלים טכנולוגיים לסמכויות המשטרה נוכח היקף הפגיעה בזכויות יסוד, על המשטרה לוודא כי <u>טרם</u> רכישה או פיתוח עצמאי של מערכת טכנולוגית שלה יכולת חדשה מבחינת איסוף או עיבוד המידע, ושהיא בעלת פוטנציאל לחריגה מהסמכות הקבועה בחוק, וודאי שטרם השימוש בה, זו תועבר לאישור הייעוץ המשפטי לממשלה. זאת תוך פירוט כלל מאפייני המערכת והתנאים להפעלתה, בצירוף עמדה משפטית בדבר מקור הסמכות.

פיקוח לפי סעיף 6(ו) לחוק האזנת סתר: לעמדת צוות הבדיקה, נוסף על ההמלצה להבאת כלים טכנולוגיים חדשים לידיעת משרד המשפטים, יש להשתמש בהליכי הפיקוח הקיימים לפי סעיף 6(ו) לחוק על מנת להרחיב את תשתית הפיקוח הקיימת על אמצעים טכנולוגיים בהם נעשה שימוש במסגרת האזנות סתר, וכן לייצר הזדמנויות נוספות לבחינת שאלות משפטיות הנוגעות לשימוש בטכנולוגיות חדשות. לצורך כך נדרש, בין היתר, לציין בדיווח העתי את האמצעי הספציפי שבאמצעותו בוצעה ההאזנה.

הצורך באוריינות טכנולוגית: מחלקת ייעוץ וחקיקה במשרד המשפטים עוסקת באופן יומיומי בסוגיות טכנולוגיות. הצוות סבור כי נדרשת העמקה של הידע המשפטי הטכנולוגי בדבר מגמות והתפתחויות טכנולוגיות בעולם, בין היתר, בנוגע לאיסוף, שימוש ועיבוד מידע פרטי על אודות אדם על ידי גופי האכיפה. העמקה כאמור תאפשר לטייב את היכולות לאתר ולטפל בסוגיות משפטיות

[46] אישור כאמור נדרש כאשר מבוקש להאזין לשיחה שהעדות עליה חסויה לפי סעיפים 51-48 לפקודת הראיות [נוסח חדש], התשל״א-1971 (דהיינו שיחה שנערכה תוך מתן השירות המקצועי של עורך-דין, רופא, פסיכולוג, עובד סוציאלי וכהן דת).

המתעוררות, תוך התייחסות מראש להתפתחויות צפויות, באופן שיצמצם ככל האפשר את הפער בין ההסדרה בדין לבין המציאות הטכנולוגית הקיימת באותה עת, כמו גם לזהות ולנתח מגמות ולהמליץ על תיקוני חקיקה בהתאם, במיוחד לאור מהירות התפתחות הטכנולוגיה מול קצב התקדמות החקיקה.

יש להדגיש כי אין בכל אלה כדי לגרוע מכך שהאחריות להצגת תמונה עובדתית מלאה באשר ליכולות טכנולוגיות ואופן השימוש המבוקש המובאות בפני ייעוץ וחקיקה, היא על משטרת ישראל.

הסדרה בנהלים כתנאי להמשך הפעלת הסמכות: צוות הבדיקה דן בהשתלשלות האירועים המתוארת בפרק 8.1.3, בכל הנוגע לאותה יכולת ואשר ניתנה הנחיה על ידי המשנה ליועצת המשפטי לממשלה (משפט פלילי), ובהמשך לכך אף על ידי היועץ המשפטי לממשלה דאז, לפיה לא ניתן לבקש מבית המשפט באופן גורף להפעיל יכולת זו בכל המקרים בהם מבוקשת האזנה לתקשורת בין מחשבים לטלפונים ניידים. כאמור, נוהל בנושא הועבר רק 3 שנים לאחר בקשת מחלקת ייעוץ וחקיקה לקבלו. לא ניתן לחלוק על החשיבות בהסדרה ברורה של שימוש באמצעים הפוגעים בפרטיותו של אדם בהתאם לנהלים סדורים המתווים את שיקול הדעת. במבט צופה פני עתיד, על מנת להבטיח שימוש מידתי במערכות אלה, יש מקום להתנות את הפעלתן בקביעת נהלים באישור היועץ המשפטי למשטרה והייעוץ המשפטי לממשלה.

חיסיון: לצוות הבדיקה נמסר כי ככל שהשימוש במערכות להאזנת סתר לתקשורת בין מחשבים באמצעות הדבקה התבצע במסגרת חקירות שהתגלגלו לכדי תיקי חקירה שהובאו לפתחה של התביעה, עלה הצורך לפעול להוצאתה של תעודת חיסיון לפי סעיף 45 לפקודת הראיות [נוסח חדש], התשל"א – 1971 על השימוש במערכות כמו גם על כלל תוצריהם. זאת, לצורך הגנה על "שיטה ואמצעים" חסויים שבשימושה של משטרת ישראל. בתהליך הבחינה של תעודת החיסיון, מובא דבר השימוש בכלי ותוצריו בפני פרקליט המחוז, מנהל המחלקה בפרקליטות המדינה, או גורם בכיר אחר בתביעה שהוסמך לכך, לצורך בחינה האם יש בחיסויו של עצם השימוש בכלי, ובחיסוי התוצרים שנאספו באמצעות הכלי, כדי לפגוע בהגנת נאשם באופן שעשוי לערער את האפשרות לחסותו במלואו. בהקשר זה לעמדת צוות הבדיקה, יש ליידע את הפרקליט הרלוונטי בדבר האפיון הכללי של הכלי (למשל שמדובר בהאזנה הדורשת הדבקה מרחוק של מכשיר סלולרי ברוגלה).

על פי הנוהג שהשתרש בעניין זה, גורמי המשטרה, במסגרת "ישיבת חסיונות" בה נבחנת שאלת תעודת החיסיון, נהגו להביא בפני גורמי התביעה את הפרפראזות שנערכו על ידי המפיקים, ולא את יומני ההפקה במלואם, שבהם פירוט נרחב יותר על התוצרים שהתקבלו.

הצוות סבור, כי נכון לקבוע כי יש להציג במסגרת "ישיבת חסיונות" בנוגע לשימוש בכלים את "יומני ההפקה", לנוכח הפירוט הנרחב יותר שיש בהם. בכך יתאפשר לגורמי התביעה לערוך בחינה מיטבית, כצעד מקדים לבחינתו של הממונה על החסיונות, של הפוטנציאל לפגיעה בהגנת הנאשם.

עמדת הפרקליטות שהוצגה בפני הצוות הייתה כי הדברים מקובלים עליהם.

11. המלצות לתיקוני חקיקה

כאמור פרק 3 לדוח, השאלה לעניין הסמכות מכוח חוק האזנת סתר להתקנת רוגלה על מכשיר טלפון לצורך ביצוע האזנת סתר, היא שאלה המעוררת סוגיות משפטיות כבדות משקל וזו נבחנה בנפרד, כמפורט בהרחבה בנספח המשפטי. בכפוף לעמדה המשפטית הנ"ל, אשר מצאה כי ניתן לפרש את חוק האזנת סתר ככזה המתיר חדירה למכשיר טלפון לצורך התקנת אמצעי לביצוע האזנת סתר, צוות הבדיקה קיים דיון בכל הנוגע לשאלה הקונספטואלית בדבר סוגיית השימוש ברוגלות להאזנת סתר באופן כללי על ידי גורמי אכיפת חוק משטרתיים הפועלים למול גורמים חשודים בפליליים. לעמדת צוות הבדיקה לא ניתן להתייחס למונח "רוגלה" כאל סוגיה אחידה, שכן קיים ספקטרום רחב של היקף היכולות הקיימות לכל רוגלה ורוגלה. מכאן שלא ניתן לקבל עמדה השוללת כל פעולה של האזנת סתר הדורשת חדירה למכשיר קצה לצורך ביצוע האזנה. אלא, יש לבחון כל רוגלה לגופה, כאשר מרכז כובד המשקל שיש ליתן בעת בחינת הרוגלה, נוגע להיקף הפעולות והמידע שהרוגלה יכולה לבצע ולאסוף. כל זאת כמפורט בהרחבה בפרק 3.

מבלי לגרוע מהעמדה המשפטית ומעמדת צוות הבדיקה ביחס לסוגיה המפורטת לעיל, לא ניתן לחלוק על כך שקיים צורך לבצע תיקוני חקיקה לחוק האזנת סתר על מנת להתאימו למציאות הטכנולוגית של היום.

חוק האזנת סתר נחקק לראשונה בשנת 1979, ומאז תוקן פעמים ספורות. התיקון הרלוונטי לענייננו נערך בשנת 1995, במסגרתו הוגדר כי "שיחה" היא בין היתר גם "תקשורת בין מחשבים".[47] אין חולק על כך שהמחוקק בשנת 1995 לא יכול היה לראות לנגד עיניו את היקף השינויים הטכנולוגיים וסוגי הפלטפורמות השונות בהן מבוצעת תקשורת בין מחשבים כיום. מובן כי נוכח היקף השינויים מאז תיקון החוק בשנת 1995, יש להסדיר באופן רוחבי סוגיות של מעקב בעידן הדיגיטלי בשים לב לכך שלא רק תקשורת אלא פעולות נוספות רבות של אדם מבוצעות במרחב המקוון. על החקיקה להסדיר את גבולות הסמכות והפעלתה בבירור, בשים לב למאפיינים הייחודיים של הפגיעה בפרטיות הנובעת משינויים אלה.

בחוות דעת מבקר המדינה משנת 2010 שעסקה בהאזנות סתר בחקירות פליליות, המליץ מבקר המדינה כי נוכח השינויים הטכנולוגיים המתחוללים בעולם, המעבר לתקשורת מחשבים ולטלפונים ניידים, כמו גם התחכום הגובר שלארגוני הפשיעה, כלל מערכות אכיפת החוק ייערכו הן מהבחינה הנורמטיבית והן מהבחינה הטכנולוגית כדי לאפשר למשטרה לקיים האזנת סתר במקרים הראויים לשם מאבק בפשיעה, בעיקר בפשיעה החמורה.

יודגש כי במהלך העשור האחרון (לערך) התעורר דיון ציבורי, פוליטי ומשפטי בסוגיית המעקבים המקוונים במדינות שונות בעולם. בעקבות כך, ישנן מדינות שהחלו בשנים האחרונות להסדיר באופן מפורש ונרחב את ההסדרים הנוגעים לשימוש ברוגלות (ראו למשל את החקיקה בצרפת

[47] סעיף 1 לחוק האזנת סתר.

ובריטניה).[48] אין חולק כי דיון ציבורי בנושא, בצד תיקוני חקיקה מפורשים הנוגעים לגדרי הסמכויות הרלוונטיות בעניין, נדרשים להתקיים גם בישראל.

יצוין כי במסגרת עבודת הצוות, נפגש הצוות עם גורמים שונים העוסקים בנושא, בהם הסנגוריה הציבורית, הרשות להגנת הפרטיות, המכון הישראלי לדמוקרטיה, האגודה לזכויות האזרח ופרופ׳ אמנון רייכמן. ככלל, הוצגה על ידי גורמים אלה העמדה כי נדרשת הסמכה מפורשת בחקיקה בנושא, לאחר קיום דיון ציבורי. כמו כן, הובאו מטעם גורמים אלה עמדות שונות לעניין ההסדרים הרלוונטיים שיש להוסיף לחוק האזנת סתר, וביניהם:

- הרחבת חובת הדיווח של משטרת ישראל לכנסת וליועצת המשפטית לממשלה.
- חובת פרסום של נתונים סטטיסטיים לגבי ביצוע האזנות סתר (כגון באילו סוגי עבירות נעשה שימוש בכל אמצעי האזנה, כמה אנשים היו חשופים להאזנת סתר ועוד).
- הסדרת סוגיות אשר נוגעות לא רק להיקף המידע המותר לאיסוף על ידי המשטרה, אלא הסדרה רוחבית הנוגעת גם לגדרי סמכויות השימוש במידע שיתקבל, ובכלל זה הסדרת הסמכות לעבד את המידע באמצעות כלים אחרים או להצליב אותו עם מידע אחר.
- עיגון זכות היידוע של מי שהיה יעד להאזנת סתר בתום החקירה בעניינו.
- הקמת גוף עצמאי שתפקידו יהיה, בין היתר, לפקח על אופן הביצוע של האזנות סתר.

מבלי להביע עמדתו ביחס להצעות המפורטות לעיל, צוות הבדיקה ממליץ על קידום תיקון חקיקה מקיף לחוק האזנת סתר בהקדם. בדעת מחלקת ייעוץ וחקיקה במשרד המשפטים לעסוק בכך מיד לאחר הגשת הדוח, תוך בחינת כלל הסוגיות הנוגעות לעניין יחד עם הגורמים הממשלתיים הרלוונטיים ובשיתוף ארגוני חברה אזרחית וגורמי אקדמיה, נוכח השלכות הרוחב של סוגיה זו על זכויות היסוד של הפרט. במסגרת זו יהיה מקום גם לעסוק בהמלצות לתיקוני חקיקה בדוחות קודמים שעסקו בנושא האזנות הסתר ושלא קודמו, כמו גם בהצעות לתיקונים נוספים לחוק האזנת סתר שהצורך בהם עלה במהלך השנים האחרונות.

עמית מררי
המשנה ליועצת המשפטית לממשלה
(משפט פלילי), יו״ר הצוות

צפריר כץ
חבר צוות הבדיקה

איל דגן
חבר צוות הבדיקה

[48] בצרפת: Code de Procédure Pénale [C. Pr. Pén.]; בבריטניה: Investigatory Powers Act (2016).

נספחים

מדינת ישראל

משרד המשפטים

ירושלים: כ׳ אדר א׳ תשפ״ב

21 פברואר 2022

ממצאי צוות הבדיקה בעניין האזנות סתר בדרך של תקשורת בין מחשבים לעניין הפרסום באתר ״כלכליסט״ מיום 7.2.22

ביום 31 בינואר 2022 מונה על ידי היועץ המשפטי לממשלה (דאז), צוות, בראשות המשנה ליועצת המשפטית לממשלה (משפט פלילי), עו״ד עמית מררי, לבדיקת האזנות סתר בדרך של תקשורת בין מחשבים (להלן - ״**צוות הבדיקה**״); זאת מכח הסמכות הנתונה ליועץ המשפטי לממשלה לפיקוח על האזנות סתר שמבצעת משטרת ישראל לפי סעיף 6(ו) לחוק האזנת סתר, התשל״ט-1979, ונוכח טענות שעלו בפרסומים בתקשורת על אודות שימוש לא חוקי לכאורה באופן בו משטרת ישראל מפעילה אמצעים לביצוע האזנת סתר בדרך של תקשורת בין מחשבים (להלן גם – **הדבקה**). כמו כן מונו כחברים בצוות שני ראשי אגפים בדימוס בשב״כ, מר צפריר כץ שעמד בראש האגף הטכנולוגי של השב״כ ומר איל דגן שעמד בראש אגף חקירות של השב״כ.

הצוות מונה בעקבות טענות שונות שפורסמו ביחס לחריגה מהסמכויות הנתונות למשטרת ישראל בכל הנוגע להאזנות לתקשורת בין מחשבים, ובכלל זה טענות לפיהן בעת ביצוע האזנת סתר כאמור מתקבל בידי משטרת ישראל חומר החורג מהמותר על פי דין. בהמשך לפרסומים אלו, ביום 7.2.2022 פורסם כי משטרת ישראל מבצעת פעולות אקטיביות עצמאיות למעקב טכנולוגי אחר אנשים, לעיתים אף ללא קשר לחקירה מתנהלת או לברור חשדות לביצוע עבירות פליליות, וממילא מבלי שהתקבל צו שיפוטי (להלן - **הטענות הנוספות**). אם כן, ביחס לטענות הנוספות, נטען כי: (1) הפעולות הנטענות נעשו על ידי משטרת ישראל; (2) הפעולות נעשו באמצעות תוכנת פגסוס שבידי משטרת ישראל שפותחה על ידי חברת NSO; (3) ההדבקה בוצעה למכשירי טלפון של רשימת אנשים אשר פורסמה.

קשה להפריז בחומרתה של הפגיעה הנטענת. טענות אלה, נוגעות בליבת שלטון החוק במדינה דמוקרטית, ויש בהן כדי לערער את תחושת הביטחון האישי של כל אדם ואזרח במדינה, כמו גם את אמון הציבור במשטרת ישראל, כגוף האכיפה המרכזי במדינה, האמון על שמירה על שלטון החוק.

נוכח האמור, הונחה צוות הבדיקה בשלב ראשון לקיים בדיקה ממוקדת ויסודית ביחס לטענות הנוספות, וזאת על פי שלושת המאפיינים שתוארו לעיל. היינו, הצוות התבקש לבחון **האם בוצעה הדבקה על ידי משטרת ישראל למכשירי טלפון ניידים השייכים אל מי מבין רשימת האנשים שפורסמו, באמצעות תוכנת פגסוס שפותחה ע"י חברת NSO, ללא צו שיפוטי. בשלב זה לא נדרש הצוות לבדוק את השאלות הנוספות שנדרשות לבדיקה המפורטות להלן בסעיף 18, ובכלל זה אופן מימוש צווי האזנה וחומרים שהתקבלו.**

לצורך בדיקת הטענות, צוותו לצוות הבדיקה עובדי שירות הביטחון הכללי והמוסד לתפקידים מיוחדים, המומחים בתחום הטכנולוגיה הרלוונטית (להלן – **המומחים הטכנולוגיים**). המומחים מסייעים לצוות בהתאם לכתב המינוי של הצוות, לפיו "הצוות רשאי לשמוע ולהסתייע בגורמים נוספים, לרבות מומחים בתחום המשפט ובתחום הטכנולוגיה". המומחים אינם פועלים כנציגי הגופים בהם הם מועסקים ואינם מונחים על ידם.

להלן יפורטו הליך הבדיקה וממצאי צוות הבדיקה בכל הנוגע לשאלה שהונחה הצוות לבחון בשלב זה כאמור לעיל.

<u>**בסיס הליך הבדיקה**</u>

1. **רשימת מספרי הטלפון שנבדקה**: הבדיקה נעשתה על בסיס רשימה מורחבת שגובשה על ידי משטרת ישראל, של מספרי טלפון אשר בשימוש רשימת האנשים שהתפרסמה (להלן – **הרשימה המורחבת**). יצוין כי רשימה זו נבדקה מול מספרי טלפון של מרבית האנשים ששמותיהם פורסמו, אשר אומתו על ידי צוות הבדיקה באופן בלתי אמצעי. המספרים שנבדקו אכן נכללו ברשימת מספרי הטלפון הרחבה שגיבשה המשטרה לצורך הבדיקה.

2. **מאפיינים כלליים של המערכת:** הבדיקה נעשתה מול ממשק המשתמש ומול בסיס הנתונים הפנימי של המערכת. בסיס הנתונים הפנימי נמצא בשרתים המותקנים במשטרת ישראל, ואולם מהמידע שנמסר על ידי נציגי חברת NSO לנציגי צוות הבדיקה, השכבה של בסיס הנתונים הפנימי של המערכת אינה זמינה למשתמש, אלא יכולה להיות מונגשת על ידי החברה בלבד. גישה לשכבה זו מחייבת ידע טכני כמו גם נתוני אימות שמצויים ברשות החברה בלבד ולא בידי המשטרה.

3. **אופן הבדיקה:** הבדיקה נעשתה על ידי הצלבת כלל מספרי הטלפון והמזהים שעלו מתוך בסיס הנתונים הפנימי של המערכת, אל מול רשימת מספרי הטלפון המורחבת. ככל שלא עלו מספרי טלפון אלא מזהים אחרים, כגון מזהה כרטיס סים, ביצעה המשטרה תרגום של מזהים אלה למספרי טלפון. על חלק מהמזהים בוצעה בקרה מדגמית על ידי צוות הבדיקה.

4. **סוגי הבדיקות שבוצעו**: צוות הבדיקה למד את המערכת על רבדיה השונים ואופן פעולתה הטכנולוגי והמבצעי. הבדיקות שנעשו על ידי צוות הבדיקה נעשו הן על גבי ממשק המשתמש והן על בסיס נתונים שהחברה סיפקה לבקשת הצוות מבסיס הנתונים הפנימי המהווה את ליבת המערכת. על פי המידע שנמסר מהמשטרה ומהחברה, הבדיקה כיסתה את כלל שיטות הפעולה המשמשות את המשטרה, על כלל תרחישי השימוש השונים במערכת. לשלמות התמונה יצוין כי המערכת מאפשרת למשתמש לבצע תחזוקה הכוללת

מחיקה של רשומות. הצוות ביצע את הבדיקות גם למול רשומות שנמחקו על מנת לכסות גם תרחיש זה, וזאת, בין היתר, באמצעות שליפות שהחברה ייצרה, מהאזור בבסיס הנתונים הפנימי שלא ניתן למחיקה על ידי המשתמש. בדיקות מעמיקות ומקיפות אלה חייבו מספר סבבי בדיקה גם אל מול החברה והאריכו את הליך הבדיקה מעבר למתוכנן.

5. יודגש כי הבדיקה שבוצעה היא טכנולוגית בלבד. צוות הבדיקה לא נחשף לתכנים שהופקו מהאזנות סתר שבוצעו באמצעות המערכת. כמו כן, הצוות לא נחשף בשלב זה לזהות האנשים שבעניינם בוצעה האזנת סתר באמצעות המערכת, למעט אלה הנכללים ברשימה.

<u>תהליך הבדיקה</u>

6. בימים 7-8 בפברואר 2022 קיימה משטרת ישראל בדיקה עצמאית על גבי ממשק המשתמש של המערכת ביחס לטענות הנוספות שפורסמו. לאחר בדיקה שערכה המשטרה על בסיס רשימת מספרי הטלפון המורחבת, מסרה המשטרה לצוות הבדיקה כי לגבי שלושה אנשים מתוך הרשימה קיימים צווים להאזנת סתר מסוג תקשורת בין מחשבים לפי חוק האזנת סתר, רק לגבי שניים מתוכם בוצע ניסיון הדבקה ורק לגבי אחד מהשניים ההדבקה הצליחה. ביחס ליתר האנשים נמסר על ידי המשטרה כי לא קיימים בעניינם צווי האזנת סתר מסוג תקשורת בין מחשבים וכן לא בוצעה בפועל הדבקה של מכשירי הטלפון הסלולריים שלהם באמצעות המערכת וכן מערכות נוספות הקיימות ברשותם.

7. בימים 9-20 בפברואר 2022 קיים צוות הבדיקה, בסיוע המומחים הטכנולוגיים, בחינה של הטענות הנוספות שפורסמו. תחילה נבדקו הטענות על גבי ממשק המשתמש במערכת פגסוס שבידי המשטרה תחת הרשאות המנגישות תיעוד מלא של הפעולות במערכת שאינו נתון לשינויים במערכת. זאת במטרה לבחון את כלל ניסיונות ההדבקה וההדבקות המוצלחות שבוצעו במערכת למול רשימת הטלפונים המורחבת. בדיקות אלה העלו כי למעט לגבי שני אנשים אשר בעניינם הוצא צו, לא היו הדבקות ולא עלו אינדיקציות לניסיונות הדבקה ביחס לרשימת המספרים המורחבת, ובפרט גם למול רשומות שנמחקו על ידי המשתמש.

8. על מנת לייצר תובנות ברמת סמך גבוהה ככל הניתן, בוצעה פנייה אל חברת NSO בבקשה לשליפת הנתונים מבסיס הנתונים הפנימי של המערכת. בהמשך לכך הגיעו נציגי חברת NSO אל מתקני משטרת ישראל ונפגשו עם חלק מנציגי הצוות ושלפו נתונים בהתאם לשאלות שהועברו על ידי צוות הבדיקה מבסיס הנתונים הפנימי המצוי בשרתים שהותקנו במשטרת ישראל. כאמור לעיל, מהמידע שנמסר על ידי נציגי חברת NSO לנציגי צוות הבדיקה, שכבה זו של המערכת נגישה לחברה בלבד ואינה זמינה למשתמש. גישה לשכבה זו מחייבת ידע טכני כמו גם נתוני אימות שמצויים ברשות החברה בלבד ולא בידי המשטרה.

9. הרציונאל שעמד בבסיס השאלות שהועברו לחברת NSO לצורך שליפת נתונים מבסיס הנתונים הפנימי, נועד לקבל פירוט נתונים של כלל השימושים שנעשו במערכת מאז מועד

הפעלתה הראשונית בידי משטרת ישראל ועד היום, אל מול כל תרחישי השימוש השונים האפשריים על שלביהם השונים במערכת.

10. על מנת לתת מענה לכל תרחישי השימוש השונים במערכת, ננקטו על ידי צוות הבדיקה שתי גישות שונות: **האחת**, כללה בדיקה של כל ההדבקות שהסתיימו בהצלחה (קרי הדבקה בפועל של מכשיר טלפון) על ידי המערכת. יצוין כי בדיקה זו מקיפה את כל תרחישי השימוש השונים במערכת. **השנייה**, במטרה לייצר תמונה רחבה אף יותר, כללה בדיקה של כלל ניסיונות ההדבקה במערכת ללא תלות בשאלת הצלחתן בפועל. בדיקה זו בוצעה כל אימת שהמידע שנשלף מהמערכת איפשר זאת.

11. הגישה הראשונה לבדה, מאפשרת לתת מענה באופן מלא לטענות לעניין הדבקה בפועל של מכשירי טלפון ניידים השייכים לרשימת האנשים שפורסמו בתקשורת.

12. כמו כן, נבחנה מערכת נוספת שנכנסה לשימוש לאחרונה ומשמשת להאזנה לתקשורת בין מחשבים של מכשירי טלפון נייד. הבדיקה נעשתה על בסיס רשימת המספרים המורחבת ואל מול פלט מבסיס הנתונים הפנימי של המערכת אשר הועבר על ידי החברה הפרטית ממנה נרכשה המערכת. כפי שנמסר מהחברה, בסיס נתונים פנימי זה אינו נגיש למשתמשים ואינו ניתן לשינוי.

13. יצוין כי ביום 15 בפברואר 2022 בוצעה מטעם הצוות בדיקה פרטנית למספרי הטלפון שהועברו על ידי שלושת המנהלים הכלליים לשעבר של משרדי הממשלה, ששמותיהם הופיעו בפרסום: שי באב״ד, אמי פלמור וקרן טרנר. אלה העבירו לידי הצוות בעקבות פנייתנו מזהים של מכשירי הטלפון שלהם, ונוסף על כלל הבדיקות שבוצעו באופן רוחבי, מזהים אלו נבדקו באופן ישיר. מזהים אלה לא עלו בנתוני המערכות שנבדקו.

14. כלל הבדיקות וההשלמות השונות שנדרשו נמשכו עד ליום 20 בפברואר 2022.

<u>ממצאים</u>

15. כפי שעולה מבדיקת הצוות, ביחס לכלל המספרים שקיימים בבסיס הנתונים הפנימי של מערכת פגסוס, נמצא כי לגבי שני אנשים שלגביהם ניתן צו בית משפט להאזנה לתקשורת בין מחשבים, בוצע ניסיון הדבקה, ולעניין אחד מהשניים שלגביהם ניתן צו בית משפט - ההדבקה הצליחה. יתר המספרים שיוחסו לאנשים שברשימת המספרים המורחבת אינם מופיעים בבסיס הנתונים של המערכת, קרי אין כל אינדיקציה לכך שנדבקו. ממצא זה אושש בכל אחד מסוגי הבדיקות שבוצעו למול בסיס הנתונים הפנימי של המערכת.

16. ביחס למערכת הנוספת שפורטה בסעיף 12 לעיל, אף אחד מהמספרים שיוחסו לכלל האנשים שברשימת המספרים המורחבת אינם מופיעים בפלט בסיס הנתונים הפנימי של המערכת כפי שנשלף על ידי החברה.

17. **<u>סיכומם של דברים</u>: הבדיקה הטכנולוגית העלתה כי אין כל אינדיקציה לכך שמשטרת ישראל הדביקה באמצעות מערכת פגסוס שבידיה ללא צו שיפוטי, מכשיר טלפון של מי מבין רשימת האנשים שפורסמו בתקשורת. יתרה מזאת, על בסיס בדיקה שנערכה בכל**

המקרים בהם המידע שנשלף מהמערכת אפשר לבדוק זאת, לא נמצאה גם כל אינדיקציה לניסיונות הדבקה. בכל הנוגע למערכת הנוספת שבידי משטרת ישראל ונבדקה בידי צוות הבדיקה, לא היו כל אינדיקציות להדבקות או ניסיונות הדבקה אל מי מבין רשימת האנשים שפורסמה.

<u>סוגיות להמשך בחינה</u>

18. אלה הם ממצאי הצוות הכוללים את ממצאי הבדיקה הטכנולוגית שמאפייניה פורטו לעיל. עד כה בוצעה בדיקה טכנולוגית ביחס לטענה שפורסמה ביום 7.2.22 לפיה המשטרה מבצעת מעקב טכנולוגי אחר אזרחים באמצעות תוכנת פגסוס, ללא חקירה וללא צו שיפוטי. הבדיקה צפויה להימשך. ככל שלא יוחלט על ידי הגורמים המוסמכים על מתווה בדיקה שונה, הצוות עתיד להמשיך את עבודתו ביחס לבחינת העיסוק והטיפול המשטרתי בהאזנות סתר בדרך של תקשורת בין מחשבים, לרבות הרחבת הבדיקה בדבר הטענות לשימוש במערכות ללא צו מעבר לרשימת האנשים שפורסמו, על בסיס הנתונים שנותחו ונאספו על ידי המומחים הטכנולוגים עד כה; מידת ואופן התאמתם של הכלים המצויים בידי המשטרה לסמכויות הנתונות לה על-פי דין ואופן השימוש שנעשה בכלים אלה, לרבות במערכות נוספות בעלות מאפיינים שונים המאפשרות האזנה לתקשורת בין מחשבים המצויות או שנמצאו בשימוש משטרת ישראל; קיומן של אינדיקציות לחריגה מסמכות; פיקוח ובקרה בזמן אמת ובדיעבד על כלל שלבי עבודת המשטרה בתחום, והיבטים נוספים.

ממצאים מפורטים ביחס לתהליך הבדיקה בשלמותו מצויים בדו״ח חסוי של צוות הבדיקה.

עמית מררי
המשנה ליועצת המשפטית לממשלה
(משפט פלילי),
יו״ר צוות הבדיקה

צפריר כץ
חבר צוות הבדיקה

איל דגן
חבר צוות הבדיקה

נספח ב׳ - עמדה משפטית

להלן תפורט העמדה המשפטית בכל הנוגע לאפשרות השימוש במערכות לתקשורת בין מחשבים המודבקות על מחשב, ובכלל זה טלפון נייד, כפי שהוצגה ליועצת המשפטית לממשלה על ידי מחלקת ייעוץ וחקיקה (משפט פלילי), והתקבלה על ידה.

הדיון המשפטי דורש בחינה בשלושה רבדים:

ראשית, יש לבחון האם עצם הסמכות של משטרת ישראל לשימוש ב״רוגלה״ המותקנת על מכשיר הקצה של יעד ההאזנה הינה בגדר האזנת סתר לפי החוק בנוסחו כיום. בשים לב לכך, נדרש לבחון את השיטה לקבלת מידע שיש לראות בה כ״פעולת האזנה״ לאור הוראות החוק, תכליותיו והפסיקה.

שנית, יש לבחון אילו סוגי מידע נכנסים לגדרי ״שיחה״ באמצעות ״תקשורת בין מחשבים״ לפי החוק, ואילו סוגי תוצרים אינם חלק מסמכויות המשטרה. בתוך כך, יש לבחון האם ואיזה סוג מידע עודף בסמכות המשטרה לקבל, גם אם אינו מהווה תקשורת בין מחשבים, לצורך תפעול וביטחון הכלי, לפי סעיף 10א לחוק האזנת סתר.

יובהר בראשית הדברים כי הדיון כולו מוגבל לסמכות לבצע ״האזנת סתר״ כהגדרתה בחוק ולא לביצוע פעולות אחרות החורגות מהאזנת סתר.

יש אפוא ליתן מענה לשאלות המשפטיות שלהלן:

1. **האם חוק האזנת סתר מסמיך את המשטרה לבצע חדירה סמויה למכשיר קצה על מנת להתקין אמצעי להאזנת סתר?**
2. **מהם התנאים לקביעה האם פעולה מהווה האזנת סתר לתקשורת בין מחשבים לפי החוק?**
3. **אילו סוגי מידע ניתן לקבל במסגרת האזנת סתר כהגדרתה בחוק והאם יש תוצרים שאינם האזנת סתר אך ניתן לקבלם מכוח סמכויות העזר המוגדרות בחוק לצורך ביטחון ותפעול הכלי?**[49]

רקע - חוק האזנת סתר

1. חוק האזנת סתר נועד לתת בסיס משפטי איתן להגנה על אדם מפני פגיעה בפרטיותו על ידי האזנה לשיחותיו ללא ידיעתו, ולהבטיח את ההגנה על ידי הוראה המענישה האזנה אסורה. בד בבד החוק מסדיר את ההליכים להאזנת סתר כשזו מחויבת מטעמים של בטחון המדינה או מטעמים של גילוי, חקירה או מניעה של עבירות מסוג פשע וגילוי עבריינים.[50] נוכח תכלית זו, החוק קובע איסור על האזנת סתר, ולצד זאת קובע חריגים לאיסור המתירים לגורמי אכיפת החוק לבצע האזנות סתר בנסיבות שבהן הפגיעה בזכות לפרטיות מוצדקת לשם הגנה על הציבור או על בטחון המדינה. ביסוד ההסדר הקבוע בחוק האזנת סתר עומד אפוא האיזון בין זכותו החוקתית של היחיד לפרטיות לבין זכותו של הציבור לביטחון.

---

[49] שאלה זו נידונה בהרחבה בנפרד במסגרת הדו״ח החסוי.
[50] ראו דברי ההסבר להצעת חוק דיני העונשין (האזנת סתר), התשל״ח-1978.

2. הוראות חוק האזנת סתר מגלמות את התפישה כי האזנה לסוד שיחו של אדם מהווה פגיעה חמורה ביותר בפרטיות ועל כן קבועים הסדרים נוקשים לקבלת היתר להאזנת סתר, הן בהיבט המהותי והן בהיבט הפרוצדורלי. הפסיקה שבה והבהירה את מידת הפגיעה בפרטיות הגלומה בהאזנת סתר. יפים לעניין זה דבריו של המשנה לנשיא (כתוארו אז), כב' השופט ברק בעניין **נחמיאס**[51]:

> "האזנת סתר היא התערבות חריפה בזכותו של אדם להיות עם עצמו. היא מהווה חדירה קשה לפרטיותו של האדם. היא שוללת מהאדם את מנוחת נפשו, את ביטחונו בחופש רצונו. היא הופכת את מבצרו לכלאו. עם זאת הזכות לפרטיות אינה מוחלטת. ניתן לפגוע בה לשם מניעת עבירות, אשר סופן הגנה על הפרטיות של אחרים, ועל כבודם וחירותם".

3. יצוין כי מידת הפגיעה בפרטיות הנובעת מהאזנת סתר מקבלת משנה תוקף כאשר מדובר בהאזנה לתקשורת בין מחשבים, בעידן שבו מרבית התקשורת, הלכה למעשה, מתקיימת במרחב המקוון. למעלה מכך, מאפייניהם הייחודיים של טלפונים חכמים, והיקף השימוש שנעשה בהם בחיי היומיום עשויים להוביל לפגיעה חריפה בפרטיותו של אדם בהשוואה להאזנת השמע "המסורתית", ולא ניתן להמעיט במשמעות הייחודית של חשיפה להיקף וסוג תכנים אלו. ראו לעניין מאפייניו הייחודיים של חומר מחשב, דבריו של השופט עמית בעניין **פישר**:[52]

> "מאפיין נוסף של חומר מחשב, לרבות הטלפון הנייד, הוא שניתן לדלות ממנו חומרים אובייקטיביים מזמן אמת, ראיות עוצמתיות שיכולות לשרת הן את התביעה והן את ההגנה. אך פוטנציאל ראייתי זה הוא בבחינת אליה וקוץ בה. מדובר בחומר רב שדרכו ניתן ללמוד גם על "סיפור חייו" של המשתמש. למעשה לא מדובר רק בסיפור חיים המשורטט בקווים כלליים, אלא בפרטי הפרטים של חיי היומיום של האדם – מקומו בבוקר ועד לכתו לישון דרך המקומות בהם שהה, האנשים עימם שוחח ותכני השיחה ("סוד השיח"), רעיונות, הגיגים, תחביבים, חברים, ידידים, מידע אינטימי ומידע עסקי, תחומי עניין וסקרנות (האתרים אליהם גולש המשתמש) ועוד [...]".

4. יודגש כי הדברים האמורים לעיל בעניין **פישר** נוגעים לסמכות החיפוש במחשב ביחס לכלל המידע האגור בו ולא להאזנת סתר, ואולם המאפיינים הייחודיים של חומר מחשב, ובפרט ביחס לטלפון נייד, רלוונטיים בשינויים המחויבים גם בכל הנוגע להאזנת סתר לתקשורת בין מחשבים. ראו הרחבה מטה לעניין ייחודה של האזנת סתר.

5. סעיף 6 לחוק האזנת סתר מסדיר את סמכות המשטרה לבצע האזנת סתר לשם גילוי, חקירה או מניעה של עבירות מסוג פשע, בצו שיפוטי בהיתר של נשיא בית משפט מחוזי או סגנו, כאשר גדרי הסמכות נשענים בין היתר על ההגדרות המנויות בסעיף 1 לחוק. בשנת 1995 תוקן חוק האזנת סתר כך שהובהרה ההגדרה של "שיחה", ונוספה לה, בין היתר, גם האזנה לשיחה באמצעי של "תקשורת בין מחשבים". כמו כן, לאור הכללתן של טכנולוגיות שונות של "שיחה" אשר אינן נוגעות רק לדיבור, שונתה ההגדרה של "האזנה" כך שתחול במפורש הן על שמיעת שיחה והן על קליטתה או העתקתה של שיחה.[53] בדברי ההסבר לתיקון משנת 1994 הבהירה

---

[51] ע"פ 1302/92 **מדינת ישראל נ' נחמיאס** (1995).

[52] בש"פ 6071/17 **מדינת ישראל נ' פישר**, פס' 10 (27.8.2017).

[53] להלן ההגדרה טרם התיקון משנת 1995: "האזנה - האזנה לשיחת הזולת באמצעות מכשיר".

הממשלה כי התיקון נועד לכלול את כל אמצעי הטלקומוניקציה ונועד להסיר ספקות שעלו מן הפסיקה בנושא, במיוחד בכל הנוגע לתקשורת אלחוטית.[54]

להלן הוראות החוק הרלוונטיות:

> ""שיחה" – בדיבור או בבזק, לרבות בטלפון, בטלפון אלחוטי, ברדיו טלפון נייד, במכשיר קשר אלחוטי, בפקסימיליה, בטלקס, בטלפרינטר או בתקשורת בין מחשבים;
>
> "בעל שיחה" – כל אחד מאלה:
>
> (1) המדבר;
>
> (2) מי שהשיחה מיועדת אליו;
>
> (3) המשדר בבזק;
>
> (4) מי שהמסר המועבר בבזק מיועד להיקלט אצלו;
>
> למעט הנותן שירות של העברת מסר בבזק, למען זולתו או מטעם זולתו;
>
> "האזנה" – האזנה לשיחת הזולת, קליטה או העתקה של שיחת הזולת, והכל באמצעות מכשיר;
>
> "האזנת סתר" – האזנה ללא הסכמה של אף אחד מבעלי השיחה;
>
> "בזק" – סימנים, אותות, כתב, צורות חזותיות, קולות או מידע, המועברים באמצעות תיל, אלחוט, מערכת אופטית או מערכת אלקטרומגנטית אחרת;"

6. סעיף 10א לחוק נחקק בשנת 1995 והוסיף את סמכות העזר שמאפשרת כניסה למקום לשם התקנת אמצעים שנדרשים להאזנה, פירוקם או סילוקם:

> 10א. "מי שמוסמך להתיר האזנת סתר לפי חוק זה, רשאי להתיר גם כניסה למקום לצורך התקנת אמצעים הנדרשים להאזנה, פירוקם או סילוקם; פרטי המקום שאליו הותרה הכניסה יפורטו בהיתר."

7. בשנת 1995 נחקק חוק המחשבים, התשנ"ה-1995 (להלן – **חוק המחשבים**) אשר הסדיר את העבירות הפליליות המרכזיות הנוגעות למחשב, וכן ביצע תיקונים עקיפים בהיבטים שונים (דיני ראיות וסמכויות). לענייננו, נחקק תיקון עקיף לפקודת סדר הדין הפלילי (מעצר וחיפוש), תשכ"ט-1969 (להלן –**פקודת סדר הדין הפלילי**) אשר הוסיף את הסמכות **לחיפוש** במחשב בסעיף 23א לפקודת סדר הדין הפלילי:

> 23א. "(א) חדירה לחומר מחשב וכן הפקת פלט תוך חדירה כאמור, יראו אותן כחיפוש וייעשו על-ידי בעל תפקיד המיומן לביצוע פעולות כאמור; לענין זה, "חדירה לחומר מחשב" – כמשמעותה בסעיף 4 לחוק המחשבים, תשנ"ה-1995.
>
> (ב) על אף הוראות פרק זה, לא ייערך חיפוש כאמור בסעיף קטן (א), אלא על-פי צו של שופט לפי סעיף 23, המציין במפורש את ההיתר לחדור לחומר מחשב או להפיק פלט, לפי הענין, והמפרט את מטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש.
>
> (ג) קבלת מידע מתקשורת בין מחשבים אגב חיפוש לפי סעיף זה לא תיחשב כהאזנת סתר לפי חוק האזנת סתר, תשל"ט-1979."

[54] דברי ההסבר להצעת חוק האזנת סתר, תיקון, התשנ"ד – 1994, ה"ח 2292, ה' באב התשנ"ד, 157, 1994.

לעניין ההגדרה של "חדירה לחומר מחשב", חוק המחשבים קובע כך:

> 4. "החודר שלא כדין לחומר מחשב הנמצא במחשב, דינו – מאסר שלוש שנים; לענין זה" , חדירה לחומר מחשב – "חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר, התשל"ט-1979."

ייחודה של האזנת סתר

8. ייחודה של האזנת סתר בהיבט של סמכויות אכיפה נובעת ממספר מאפיינים:

ו. **פגיעה בסוד שיחו של אדם** – המחוקק ביקש לייחד הוראות בכל הנוגע לסוג מסוים של פגיעה בפרטיות, הכוללת חדירה לסוד שיחו של אדם ללא ידיעתו. מובן כי בעת חקיקת החוק המחוקק ביקש להגן על שיחה במובנה הקלאסי, המתבצעת בין שני אנשים. ואולם עם תיקון החוק להאזנה ל"תקשורת בין מחשבים", הורחבה הסמכות לסוגי תקשורת נוספים. בהמשך לשינויים הרבים בטכנולוגיה מאז שנת 1995, והשינוי בפלטפורמות של העברת תוכן עולות סוגיות הנוגעות להיקף הגדרת "תקשורת בין מחשבים" ככל שלא מדובר בשיחה בין אדם לאדם. למשל, האם תכלית חוק האזנת סתר חלה גם במקרים בהם אדם שולח דוא"ל לעצמו, או מתכתב עם בוט.

ז. **פעולת חקירה סמויה** – האזנת הסתר אינה ידועה ליעד ההאזנה בעת ביצועה, ולעיתים ייתכן כי אף לא יידע על אודותיה לעולם.

ח. **פעולת חקירה הצופה פני עתיד** – פעולות מעקב ככלל, והאזנת סתר בפרט, ייחודיות במובן זה שפעולת האכיפה מתנהלת סימולטנית תוך כדי התרחשות הדברים, ולא בדיעבד. משום שמדובר בפעולת אכיפה סימולטנית, לא ניתן לצפות מראש איזה מידע יתקבל במסגרתה, מה יהיה היקפו, ומה מידת הפגיעה בפרטיות הנובעת ממנו ליעד ההאזנה או לצדדים שלישיים. ברי כי ביחס לפעולה עתידית יש קושי לבצע סינון של המידע מראש בטרם יגיע לרשויות החקירה.

ט. **פעולת חקירה מתמשכת** – האזנת סתר היא פעולת חקירה המבוצעת באופן מתמשך במסגרתה נאסף מידע לאורך תקופת ההיתר שניתן. זאת בשונה למשל מפעולת חקירה חד פעמית כגון חיפוש בביתו של אדם.

י. **נדיפות הראיה** - ייחוד זה נובע מנדיפותה של הראיה העוברת בתקשורת בין בעלי השיחה, קרי העובדה שתיעודה של הראיה נוצר מלכתחילה רק בשל פעולת ההאזנה ואלמלא היא לא היה נותר תיעוד לה. מאפיין זה מובהק כאשר מדובר בהאזנת שמע, שכן אלמלא מכשיר ההקלטה לא היה נותר תיעוד לשיחה שהתקיימה (אלא אם אחד מבעלי השיחה מקליט אותה). לעומת זאת, בכל הנוגע לתקשורת הכוללת העברת מסרים כתובים, למשל בהודעות טקסט או במסגרת תקשורת בין מחשבים, בשלב קבלת חומרי המחשב במכשיר הקצה, הרי שממילא הם נאגרים וקיים תיעוד שלהם, ועל כן חומר זה חשוף מטבעו לסיכונים ככל חומר מחשב.

ייחודו של חומר מחשב בעולם סמכויות האכיפה[55]

9. ייחודו של חומר מחשב המועבר בתקשורת בין מחשבים עומד בין היתר על כך שהוא נתפש בחקיקה הישראלית באופנים שונים ביחס למועד ולאופן בו הוא נאסף על ידי גופי החקירה. להבחנה זו נפקות מעשית לעניין המקור הנורמטיבי והתנאים בחוק לאיסוף המידע בידי רשויות החקירה. אותו תוכן של חומר מחשב עשוי בנסיבות מסוימות לדרוש צו האזנת סתר סמוי לצורך גישה אליו, בנסיבות אחרות להיחשב "חפץ" ולדרוש צו חיפוש במחשב ובנסיבות אחרות - צו המצאת מסמכים. לא אחת נדון קו הגבול בין ההוראות הנורמטיביות השונות החלות על חומר מחשב.

10. ככלל, ההבחנה המקובלת בין הסמכויות השונות בדין הישראלי, נשענת על ההבחנה בין stored communication הכפוף לפקודת סדר הדין הפלילי,[56] לבין communication in transit הכפוף לחוק האזנת סתר. דהיינו, מקובל לראות בסמכות לבצע האזנת סתר ככזו שחלה על ניטור התעבורה של תקשורת בין מחשבים בעת ביצוע ה"שיחה" במבט צופה פני עתיד, בעוד שחדירה מרחוק למידע אגור במחשב במבט צופה פני עבר מהווה פעולה מסוג חיפוש.

שאלה I - האם חוק האזנת סתר מסמיך את המשטרה לבצע חדירה סמויה למכשיר קצה על מנת להתקין אמצעי להאזנת סתר?

ראשית דבר לעניין הדיון על אודות שימוש ב"רוגלות"

11. רוגלה היא תוכנה המותקנת באופן סמוי על גבי מערכת מחשוב (בין אם מרחוק או באופן פיזי), ומאפשרת נגישות לצד התוקף למערכת המחשוב הנתקפת. לרוגלות שונות יכולות להיות מאפיינים שונים ויכולות שונות. קיים ספקטרום רחב של פעולות שרוגלות שונות מסוגלות לבצע, החל מרוגלה אשר מסוגלת אך ורק לנטר הודעות IM (Instant Messaging) הנכנסות ויוצאות ממכשיר הטלפון, רוגלות אשר להן יכולת לשאוב את כלל המידע האגור בתוך המחשב או הטלפון הנייד, לבצע פעולות מעקב רחבות היקף וכלה ביכולות למחיקת חומרים ועוד[57].

12. בטרם נרחיב בשאלה שבכותרת, יש להדגיש כי חלק זה מתייחס אך ורק לסוגיה של עצם הסמכות לחדור למחשב על מנת לבצע האזנת סתר. אין בחלק זה כדי להתייחס לסוג ההאזנה המותר ולהיקף המידע שניתן לקבל מכוח חוק האזנת סתר, אלא אך לשאלה הקונקרטית הנוגעת לפרשנות סעיף 10א לחוק בכל הנוגע לסמכויות העזר הנתונות למשטרת ישראל לחדור מרחוק או על ידי גישה פיזית אל מחשב על מנת להתקין אמצעי להאזנת סתר.

13. עוד יובהר כי הדיון כולו מוגבל לסמכות לבצע "האזנת סתר" כהגדרתה ולא לכלל הפעולות האפשריות לביצוע באמצעות רוגלה.

---

[55] ראו בהרחבה חיים ויסמונסקי, **חקירה פלילית במרחב הסייבר**, פרק ד (2015).
[56] חומר מחשב אשר אגור במכשיר הקצה, גם אם הגיע אל מכשיר הקצה על ידי תקשורת בין מחשבים (למשל מייל שהועבר בתקשורת בין מחשבים אך כעת הוא שמור בתיבת המייל), נתפש מהותית כ"חפץ", ועל כן גישה אליו אפשרית על ידי המשטרה רק באמצעות צו חיפוש במחשב לפי סעיף 23א לפקודת סדר הדין הפלילי, תוך ביצוע החיפוש באופן גלוי, או על ידי מתן הוראה להציג חומר מחשב מסוים מכוח צו המצאת מסמכים לפי סעיף 43 לפקודה.
[57] למען הסר ספק, במסגרת האזנת סתר אין למשטרת ישראל הסמכות לבצע חיפוש סמוי או למשל למחוק מידע.

14. בהמשך לדברים האמורים, יוער כי במסגרת ישיבות צוות הבדיקה שהתקיימו עם הסנגוריה הציבורית, הרשות להגנת הפרטיות וארגוני חברה אזרחית, אחת הטענות המרכזיות שהועלתה בפני הצוות הייתה כנגד עצם הסמכות להתקין רוגלה על מכשיר קצה ללא הסמכה מפורשת בחוק. עמדה זו נשענת בין היתר (בתמצית) על כך שרוגלה מאפשרת למשטרה לקבל בקלות רבה היקף מידע עצום על אודות כלל פעולותיו של יעד ההאזנה וכן גורמים שלישיים, ועל כן, לפי עמדה זו, מדובר בפגיעה חמורה בפרטיות המחייבת הסמכה מפורשת בחקיקה, לאחר קיום דיון השקוף לציבור על ידי המחוקק ואין די בהסמכה כללית בחוק לביצוע האזנת סתר. בהקשר זה הודגש על ידי הארגונים הנ״ל כי לעצם החדירה למכשיר הקצה כשלעצמה יש פוטנציאל לאיסוף מידע באופן נרחב ולפגיעה משמעותית בפרטיות, כזה אשר חורג מסמכויות המשטרה, במיוחד כאשר החריגה מתאפשרת רק בלחיצת כפתור. למעלה מכך, נטען כי בחינת השאלה אינה מתמצית במישור בחינת הסמכות הקבועה בחקיקה, אלא גם מחייבת בחינה במישור הערכי-עקרוני. דהיינו, יש לצאת מהפריזמה הצרה של שאלת הסמכות המעוגנת בחוק, ולבחון ברמה העקרונית מה משמעות של שימוש בטכנולוגיה מסוג זה בידי משטרת ישראל, כאשר לעניין זה רלוונטי לבחון לא רק את היכולת הטכנולוגית לאיסוף המידע והיקפה, אלא גם את יכולת העיבוד של המידע לאחר איסופו, אופן השימוש בו והסקת המסקנות על בסיסו.

15. אין חולק על כך שההסדרה הנורמטיבית הקיימת כיום בכל הנוגע להאזנת סתר חסרה בעניין שימוש ברוגלות לצורך האזנת סתר ואינה מספקת מסגרת המתייחסת למעבר מהעולם הישן של האזנת סתר לשיחה טלפונית לעולם הטכנולוגי החדש. על כן, נדרשת חקיקה עדכנית אשר תסדיר באופן רוחבי סוגיות של מעקב בעידן הדיגיטלי, בו לא רק התקשורת אלא פעולות רבות של האדם מבוצעות במרחב המקוון. על החקיקה להסדיר את גבולות הסמכות בבירור בשים לב למאפיינים הייחודיים של הפגיעה בפרטיות בכל הנוגע למעקב אחר פעולות המבוצעות במרחב המקוון. אלה סוגיות אשר המחוקק בשנת 1995, אשר הסדיר את הסוגיה של תקשורת בין מחשבים, לא יכול היה להידרש אליהן. השאלה היא האם וכיצד חסר זה משליך על גבולות הסמכות כיום.

16. לצד האמור, בעת הדיון בשאלת השימוש ב״רוגלות״ לצורך האזנת סתר, אנו סבורים כי יש להבחין בין השאלה של עצם הסמכות להתקין אמצעי על מכשיר קצה לצורך ביצוע האזנת סתר, לבין השאלה של היקף המידע המותר לקבל במסגרת האזנה מסוג זו. עוד נציין, כי לתפיסתנו הסדרת הסמכות בדין אינה נוגעת להסדרת השימוש בכלי ספציפי אלא להקניית סמכות כללית לביצוע פעולות מסוג מסוים.

17. אכן, החששות המועלים על ידי הארגונים השונים הם מהותיים ויש להם משקל של ממש. **ברי, כי עצם החדירה למכשיר קצה ופוטנציאל היכולות לאיסוף מידע על ידי כך יש בהם כדי להשליך על מידת הזהירות שיש לנקוט בעת בחינת השאלות המשפטיות להלן.**

18. בהמשך לכך יצוין כי עמדה גורפת לפיה ניתן לפעול אך ורק דרך ניטור התעבורה ללא אפשרות לביצוע האזנת סתר על ידי התקנת אמצעי האזנה במכשיר הקצה (ויודגש שוב כי אין הכוונה לביצוע פעולה של חיפוש סמוי, אלא לפעולות האזנת סתר בלבד), עשויה להוביל לפגיעה קשה ביכולת המשטרה לבצע את תפקידיה ולממש את התכליות שלשמן המחוקק התיר האזנה לתקשורת בין מחשבים. שכן, נכון להיום כמעט כל התעבורה מועברת בדרך מוצפנת. ודוק: כפי שהעולם בכללו עבר לביצוע פעולות רבות במרחב המקוון, כך גם תקשורת בין גורמי פשיעה

פועלת במרחב זה, וכן קיימות עבירות המבוצעות על ידי מחשב (למשל לעיתים בעבירות פדופיליה). עמדה לפיה האזנת סתר שתתבצע על ידי המשטרה תהיה ללא כל נגישות אל מכשיר הקצה, אלא אך ורק דרך האזנה לתווך התעבורה המוצפן, יש בה כדי להתעלם מהשינויים הטכנולוגיים המחייבים לעיתים שיטות האזנה לתקשורת בין מחשבים מסוג חדש.

19. בשים לב לצורך האמור, וכפי שיפורט להלן, ניתן לפרש את החוק כמתיר חדירה למחשב לצורך התקנת אמצעי להאזנת סתר, כמפורט מטה. יחד עם זאת, יש לבחון כל אמצעי האזנה כזה, המותקן במכשיר בידי המשטרה לצורך האזנת סתר, לפי היקף המידע שהוא מאפשר לאסוף וטיבו ובהתאם לסמכויות הנתונות על פי דין. ואולם מאחר שהחוק לא נדרש במפורש לשאלה של חדירה למחשב לשם התקנת אמצעי להאזנת סתר, נדרשת התייחסות זהירה במיוחד בבחינה המשפטית בדבר מידת התאמת אמצעי ההאזנה.

20. מובן כי הסוגיה העקרונית ביחס לשימוש ברוגלות, מעוררת שיח ער ונוקב ברחבי העולם. לעניין זה, יש למשל להפנות לחוות הדעת של ה- European Data Protection Supervisor מפברואר 2022 בעניין שימוש ברוגלות ובאופן פרטני לעניין מערכת פגסוס והקשיים העולים בעניינה.[58] לכך יש להוסיף כי במדינות שונות כבר מוסדרות סוגיות הנוגעות לרוגלות באופן מפורש בחקיקה, כגון בריטניה וצרפת[59] .

21. בשים לב לאמור לעיל נבקש להדגיש מספר הנחות יסוד בטרם פירוט הניתוח המשפט כי אף אם ניתן לפרש את סעיף 10א לחוק האזנת סתר ככזה המתיר חדירה למחשב לצורך התקנת אמצעי להאזנת סתר (כמפורט בהרחבה מטה) – יש לשים את הדגש על כך שמדובר בפרשנות המחייבת נוקשות ודיקדוק קפדני ביחס לגבולותיה. השימוש במערכות אלה יהיה אפשרי רק בכפוף לקיומם של התנאים המצטברים הבאים טרם תחילת הפעלתן :

א. העמדה המשפטית לפיה משטרת ישראל רשאית לעשות שימוש להאזנת סתר באמצעות מערכות החודרות למכשיר קצה, נוגעת אך ורק לרוגלות **אשר בוצעו בהן כלל החסימות הטכנולוגיות הנדרשות על מנת לוודא כי אלו מסוגלות לבצע אך ורק האזנת סתר כפי שהותר בחוק**, על פי הפרשנות שאושרה.

ב. בשים לב לכך שמדובר בפרשנות תכליתית של חוק האזנת סתר, ונוכח היקף הפגיעה הפוטנציאלי בפרטיות בעת שימוש במערכות להאזנת סתר המותקנות על גבי המחשב או הטלפון הנייד, יש להבטיח כי שימוש במערכות אלה יהיה בכפוף לקיומם ויישומם של נהלים ברורים המבהירים את גדר הסמכות וכוללים הנחיות מפורטות לעניין אופן השימוש במערכות, תוך נקיטת זהירות מיוחדת. מוצע כי הנהלים יגובשו עם היועץ המשפטי למשטרה, ויהיו באישורו, וכן יועברו לאישור הייעוץ המשפטי לממשלה.

ג. במסגרת הנהלים הנ״ל יש לבחון הטלת תנאים או מגבלות מיוחדים להגשת בקשות להאזנת סתר לגבי הפעלת יכולות שעל אף שנמצא כי הן בסמכות לפי חוק האזנת סתר, יש להן פוטנציאל לפגיעה משמעותית בפרטיותו של יעד ההאזנה – הגבלות ותנאים כאלה יכול שיהיו לגבי סוג מסויים של האזנה או לסוגי מקרים. נדרש פיקוח פרטני הדוק על אופן השימוש במערכות, כמפורט בפרק 5.4 לדוח. במסגרת זו יש גם לתת את הדעת באופן מיוחד

---

[58] European Data Protection Supervisor (the EU's independent data protection authority, Preliminary Remarks on Modern Spyware (15 February 2022).

[59] בצרפת : Code de Procédure Pénale [C. Pr. Pén.] ; בבריטניה : Investigatory Powers Act (2016).

למקרים אלה במסגרת הפעלת סמכות הפיקוח הקבועה ליועצת המשפטית לממשלה לפי סעיף 6(ו) לחוק האזנת סתר.

ד. יש להביא לידיעת בית המשפט בבקשות להאזנת סתר כי הבקשה במקרה הקונקרטי היא לשימוש במערכת באמצעות החדרת רוגלה.

להלן יפורט הניתוח המשפטי:

סמכות המשטרה להתקין אמצעי האזנה לפי סעיף 10א לחוק האזנת סתר

22. כפי שיפורט להלן, ניתן לפרש את חוק האזנת סתר ככזה המתיר לחדור למכשיר קצה על מנת להתקין אמצעי האזנה מכוח סמכויות העזר הקבועות בסעיף 10א לחוק.

23. סעיף 10א לחוק האזנת סתר נוסף בשנת 1995, במסגרת התיקון הכולל את הרחבת ההגדרה של "שיחה" והכללת "תקשורת בין מחשבים", לשם הבהרה מפורשת של סמכויות העזר. הסעיף מסדיר את סמכויות העזר לביצוע האזנה וקובע כי מי שמוסמך להתיר האזנת סתר מוסמך להתיר גם "כניסה למקום לצורך התקנת אמצעים הנדרשים להאזנה, פירוקם או סילוקם". זוהי סמכות עזר הנדרשת למימוש תפקידה של הרשות החוקרת לצורך ביצוע האזנת סתר, ואולם ההכרה בצורך בסמכות עזר זו חייבה הסדר סטטוטורי מפורש, בשל כך שהיא כרוכה בפגיעה בזכויות הפרט.[60]

24. חקיקת סעיף 10א לחוק נעשתה בראי הטכנולוגיה שהייתה קיימת באותו הזמן, ועל כן הסדירה את סמכויות העזר אשר עשויות להידרש להאזנה "בעולם הפיזי". מכאן שיש ליתן תשובה לשאלה האם יש בהוראות הסעיף כדי להתיר למשטרה לבצע פעולות עזר להאזנה לא רק במרחב הפיזי, אלא גם לצורך חדירה למחשב על מנת להתקין אמצעי להאזנת סתר.

האם "מקום" כולל מחשב

25. לעניין זה נפנה לפסק הדין בעע"מ 3782/12 **מפקד מחוז תל-אביב יפו במשטרת ישראל נ' איגוד האינטרנט הישראלי**, בו נדונה פרשנות סעיף 229 לחוק העונשין, התשל"ז -1977 (להלן – **חוק העונשין**) בנוסחו דאז, אשר הסמיך את המשטרה לתת צו לסגירת מקום המשמש להימורים. השאלה שהתעוררה בפסק הדין היא האם ניתן להחיל את סעיף 229 לחוק העונשין על אתר הימורים באינטרנט, קרי האם המשטרה מוסמכת להורות על הגבלת גישה לאתר אינטרנט מכוחו. בית המשפט קבע כי על אף שתכליתית ניתן לעיתים לראות גם במרחב הווירטואלי כ"מקום", נדרשת למשטרה הסמכה מפורשת להורות לצד ג' (ספקיות גישה לאינטרנט באותו המקרה) להגביל גישה לאינטרנט, ולכן לא ניתן להיסמך על סעיף 229 לחוק העונשין.[61] דעת המיעוט של כב' השופט סולברג התייחסה לאפשרות היותו של המרחב הוירטואלי באינטרנט

[60] ראו דברי ההסבר לתיקון משנת 1995: "ברוח חוקי היסוד, מוצע לעגן במפורש בחוק את סמכויות העזר הנדרשות לצורך ביצוע האזנת סתר". עוד ראו למשל דפנה ברק-ארז, משפט מינהלי, עמ' 148-147 (כרך א, 2010).

[61] להשלמת התמונה נציין כי בית המשפט פסק כנגד עמדת המדינה בהקשר זה וקבע כי על אף שניתן לראות במרחב הווירטואלי כמקום, הסעיף אינו מסמיך את המשטרה להורות לצד ג' (ספקיות גישה לאינטרנט) להגביל גישה לאינטרנט מכוח הסעיף. בית המשפט פסק כי אמנם, הסתייעות הרשות בגורמים פרטיים בהתייחס להיבטים טכניים של מילוי תפקידם היא מותרת, אך על מנת שהסתייעות כזו תתאפשר עליה להינתן בהסכמה כנה של הגורם הפרטי. במקרה זה, הצו המשטרתי חייב את ספקיות האינטרנט לחסום את האתרים, ללא הסכמתן, ובליווי סנקציה על אי עמידה בחובה. בית המשפט קבע כי בהעדר אסמכתא מפורשת בחוק, אין אפשרות לחייב גורם פרטי לבצע פעולות עבור הרשות, ולכן נדרשת הסמכה חוקית מפורשת שאינה עולה מלשונו של סעיף 229 לחוק.

כ״מקום״ כהגדרתו במקומות שונים בספר החוקים, כאשר לעניין זה ציין כי על אף שלא ניתן לקבוע זאת באופן גורף – הכלל צריך להורות כי אינטרנט בא בגדרו של ״מקום״:

> "מפאת קוצר היריעה ובהעדר טיעון ממצה, אין ניתן לומר באחריות שכל אימת שהמונח "מקום" מופיע בחקיקה ראשית או בחקיקת משנה הרי שמן הראוי להחילו גם על אינטרנט. יתכן ויימצאו יוצאים מן הכלל, זעיר פה זעיר שם, אך הכלל צריך להורות כי אינטרנט בא בגדרו של "מקום". הטיעון של איגוד האינטרנט הישראלי, שהתקבל על דעתו של בית המשפט לעניינים מינהליים, כי לפי האמת, ולפי הגדרתו המילונית, המרחב הוירטואלי איננו "מקום", איננו משכנע דיו.
>
> [...]
>
> הנה כי כן, בבואנו לפרש את הוראת סעיף 229(א)(1) לחוק העונשין אינני רואה הצדקה לגישה דווקנית ומצמצמת, לפרשנות "מקום" כמקום פיזי בלבד. בעת המודרנית הנוכחית, גם אתר אינטרנט הוא סוג של מקום." (פס' 34-36 לפסק הדין, ההדגשה הוספה)."

26. יש לציין כי על אף שעמדתו של השופט סולברג הייתה במיעוט בכל הנוגע להיקף סמכות המשטרה מכוח סעיף 229 לחוק העונשין, גם דעת הרוב אימצה את דבריו לעניין פרשנות תכליתית של ההוראה ״מקום״. ראו פסק דינו של השופט פוגלמן:

> "מוכן אני להניח, כפי שגם מצא חברי השופט נ' סולברג, כי ניתן לראות באתר אינטרנט בבחינת "מקום" כהגדרתו במקומות שונים בספר החוקים; וכן כי אתר הימורים מקוון הוא בבחינת "מקום משחקים אסורים", כהגדרתו בסעיף 229 לחוק העונשין שבו עסקינן. בעניין זה נוטה אני להסכים כי פרשנות תכליתית של החקיקה האמורה, ברוח הזמן והקדמה הטכנולוגית, אכן יכולה להובילנו למסקנה אליה הגיע חברי, שלפיה ניתן להחיל את סעיף 229 לחוק העונשין גם 'בעולם הווירטואלי'״.[62]

27. גם בענייננו ניתן לפרש פרשנות תכליתית את סעיף 10א לחוק האזנת סתר ביחס לסמכויות העזר הנתונות מכוחו, ולראות במונח ״מקום״ לא רק כמקום פיזי, אלא גם כסמכות להתקין אמצעי האזנת סתר על טלפון נייד או מחשב.[63]

28. ככל שהוראת חיקוק יכולה לשאת יותר מפרשנות אחת מבחינה לשונית, יש להוסיף ולתור אחר תכלית החקיקה, ולבחור מבין האפשרויות הלשוניות את האפשרות המגשימה תכלית זו באופן

---

[62] פסקה 9 לפסק דינו של השופט פוגלמן.

[63] ברע״א 129/17 **ריחני, נאמן על נכסי החייב נ׳ סטריקובסקי**, (7.4.2017), כב׳ השופט סולברג בפסק דינו קבע כי סעיף 58 לפקודת פשיטת רגל (שהייתה בתוקף אותו זמן), המסדיר את סמכות כונס הנכסים לעיין בדברי דואר של החייב, כוחו אינו יפה גם לעיון בתיבת הדוא״ל שלו. תיבת הדוא״ל אינה משמשת רק כבסיס שיגור וקליטה של דברי דואר, אלא חלק מרכזי מייעודה הוא ארכיון וירטואלי של מסמכים. היות שהגישה המבוקשת לדוא״ל מבוקשת לצורך עיון בארכיון הקיים בתיבת הדוא״ל, הרי שמבוקש עיון צופה פני עברה ולא צופה פני עתיד. בקשה כזו כמוה כבקשה לעיין בארכיב המכיל מסמכים שאגר החייב, על כן סעיף 58 אינו מסמיך לעניין זה, אלא סמכויות החקירה הכלליות המסורות לכונס. אשר לסמכות הכונס לדרוש מידע מצד שלישי, נקבע כי הביטוי ״כל מידע או מסמך הנוגעים לענייניו של החייב״, אינו כולל העתק או גישה בלתי אמצעית תוכן תיבת הדואר האלקטרוני, אלא ניתן לדרוש מצד שלישי רק מידע או מסמך (ואף אין הכוונה להעתק של כל תיבת הדוא״ל), שכן אין אינדיקציה כי הם עוסקים דווקא בענייניו של החייב במובן של ״הכנסותיו, הוצאותיו, חבויותיו ונכסיו הרלבנטיים לחיקת הכונס. יצוין כי לעמדת ייעוץ וחקיקה אין בפסק דין זה כדי לגרוע מהעמדה לעניין סמכות כניסה למחשב לפי סעיף 10א – שכן אף לעמדת ייעוץ וחקיקה פרשנות זו מוגבלת אך לחדירה למחשב, ואין בה כדי להתיר חיפוש או עיון בחומר המחשב האגור בו אלא אך ורק ביצוע האזנת סתר לתקשורת בין מחשבים. כמו כן, אף בפסק דין זה חוזר השופט סולבר על עמדתו בפסק דין איגוד האינטרנט כפי שצוטטה מעלה.

מיטבי. תכליתו של דבר חקיקה מורכבת מתכלית סובייקטיבית – קרי, המטרה הספציפית שביקש המחוקק להגשים באמצעות החוק – ומתכלית אובייקטיבית, השאובה מעקרונות היסוד של השיטה ומן הערכים והמטרות שאותם נועד כל דבר חקיקה במדינה דמוקרטית להגשים. במסגרת מלאכת הפרשנות, יש לאתר את נקודת האיזון בין כוונת המחוקק ובין עקרונותיה של השיטה.[64]

29. בכל הנוגע לתכלית הסובייקטיבית, סעיף 10א לחוק האזנת סתר, נועד לעגן במפורש בחוק את סמכויות העזר הנדרשות לצורך ביצוע האזנת סתר, אשר אותו זמן נגע לכניסה למקום באופן סמוי על מתן להתקין אמצעים הנדרשים להאזנה, פירוקם או סילוקם – בשל הטכנולוגיה שהייתה רלוונטית אותה עת.

30. בכל הנוגע לתכלית האובייקטיבית, המחוקק ביקש לאפשר למשטרה לבצע האזנות לתקשורת בין מחשבים לצורך מניעה וחקירה של עבירות פשע. בהתאם לכך שהטכנולוגיה לתקשורת בין מחשבים השתנתה ללא היכר, כך גם נדרשים אמצעים אחרים לצורך האזנה לתקשורת בין מחשבים. נכון להיום, האזנה אשר מוגבלת אך ורק לתווך התעבורה, יש בה כדי להקשות באופן ממשי על יכולת המשטרה לבצע האזנה לתקשורת בין מחשבים היות ותווך התעבורה מוצפן. יש בכך, הלכה למעשה, כדי להביא לפגיעה חמורה בתכליות שלשמן המחוקק התיר למשטרה לבצע האזנה לתקשורת בין מחשבים. משכך מתחייבת קריאה תכליתית של סעיף 10א לחוק ככזה המתיר אף חדירה למכשיר קצה לצורך ביצוע האזנת סתר בדרך של תקשורת בין מחשבים, וזאת בכפוף לגדרות והתנאים הנוקשים אשר פורטו בהרחבה לעיל.

היחס בין סעיף 10א לחוק האזנת סתר לבין סעיף 23א לפקודת סדר הדין הפלילי:

31. סעיף 23א לפקודת סדר הדין הפלילי הוא הסעיף המסמיך את המשטרה לערוך חדירה וחיפוש בחומר מחשב. סמכות זו מוגבלת לפעולה גלויה בלבד – ועל כן על פניו ניתן לטעון שאין להיסמך על סמכות העזר לפי חוק האזנת סתר מקום בו המחוקק הסדיר באופן ייחודי בפקודה את ההוראות הנוגעות לחדירה וחיפוש בחומר מחשב. ואולם ביחס לשאלה הראשונה הנוגעת אך ורק לסוגיה האם יש סמכות לחדור מרחוק לחומר מחשב באופן סמוי על מנת להתקין אמצעי אשר מבצע האזנת סתר, יש לעמדתנו להבחין בין פעולת חדירה שתכליתה חדירה וחיפוש בחומר מחשב, לבין פעולה שתכליתה חדירה לצורך התקנת אמצעי האזנה.

32. אין חולק כי על פי הדין הקיים אין למשטרה סמכות לבצע חדירה וחיפוש סמוי בחומר מחשב. זוהי סמכות המחייבת הסמכה מפורשת בחוק, והוצע להסדירה במסגרת הצעת חוק ממשלתית – הצעת סדר הדין הפלילי (סמכויות אכיפה –חיפוש ותפיסה), התשע"ד-2014 שהונחה עוד בכנסת ה- 20 (להלן – **הצעת חוק החיפוש**). אם כן, בהיעדר חוק מסמיך – אין בסמכותה של המשטרה לחדור למחשב ללא ידיעת הבעלים על מנת לעיין ולערוך חיפוש בחומר האגור בו. ואולם, ככל שהחדירה למחשב תכליתה אך ורק להתקין את אמצעי האזנה (בהמשך מסמך זה נתייחס לשאלה הנוספת הנוגעת להגדרה של "אמצעי האזנה"), ואף מעשית אין בה כדי לעלות לכדי חיפוש ועיון בחומרי המחשב האגורים בו, אלא מהותה חדירה לצורך התקנה טכנית גרידא של אמצעי המאפשר לבצע האזנת סתר כהגדרתה בחוק, הרי שאין לראות בה כפעולה של חדירה

[64] ראו בג"ץ 4455/19 **עמותת טבקה נ' משטרת ישראל** (25.1.2021) אהרן ברק פרשנות במשפט כרך שני – פרשנות החקיקה 92 (1993).

וחיפוש בחומר מחשב לפי סעיף 23א לפקודת סדר הדין הפלילי אלא ככזו הנכנסת לגדרי סעיף 10א לחוק האזנת סתר.

33. מבלי לגרוע מהאמור, אין חולק כי יש לקדם חקיקה עדכנית בה יוסדר באופן מפורש וברור היקף סמכויות העזר הנלוות לביצוע פעולות לפי חוק האזנת סתר שיש בהן כדי לפגוע בזכויות הפרט. בכלל זה, יש להסדיר את סמכויות העזר הספציפיות על מאפייניהן הייחודיים.

34. עם זאת, עד לתיקון החוק והתאמתו לטכנולוגיה העדכנית, ניתן לפרש פרשנות תכליתית את סעיף 10א לחוק ככזה המאפשר פעולות מסוימות הדרושות גם במרחב המקוון לצורך התקנת אמצעי האזנה בלבד. יודגש כי פרשנות זו צריכה להיעשות בזהירות, עקב בצד אגודל, תוך בחינה מעמיקה לעניין סוגי הפעולות אשר נכנסות לתוך גדרי סמכות העזר.

35. **לסיכום חלק זה, ניתן לראות את סעיף 10א לחוק כמקור סמכות להתקין אמצעי האזנה על טלפון נייד או מחשב לצורך ביצוע פעולה של האזנת סתר. והכל ככל שהחדירה למחשב נועדה לצורך התקנה של אמצעי שיבצע אך ורק האזנת סתר כהגדרתה בחוק, ואף מעשית לא יהיה בה כדי לעלות לכדי חיפוש ועיון בחומרי המחשב האגורים בו. עם זאת, יש לקדם חקיקה עדכנית שתסדיר נושא זה באופן מפורש.**

שאלה II: מהם התנאים לקביעה האם פעולה מהווה האזנת סתר לתקשורת בין מחשבים?

ההבחנה המקובלת בין stored communication לבין communication in transit המפורטת מעלה, מעלה שאלה ביחס לשיטות עדכניות לביצוע האזנת סתר. להלן תפורט העמדה בדבר קו הגבול בין פעולה של רוגלה המהווה האזנת סתר לבין פעולה של רוגלה המהווה חיפוש סמוי אסור ; זאת בשים לב, בין היתר, לפרשנות של דרישת הסימולטניות כפי שנקבעה בהלכת **צוברי**.[65]

דרישת הסימולטניות כעקרון מנחה להגדרה של האזנת סתר

36. בעניין **צוברי**, נקבעה ההלכה המחייבת קיומו של תנאי ה״סימולטניות״ על מנת לקבוע האם פעולה מהווה האזנת סתר ואם לאו. פסק הדין עסק בנסיבות בהן הנאשמים התקינו אמצעי להקלטה של קו הטלפון של אדם, אך האזינו לחומר המוקלט רק בשלב מאוחר יותר. נדונה השאלה האם מדובר בהאזנת סתר שכן ההאזנה לא הייתה בעת התקיימות השיחה.[66] בית המשפט קבע כי לא רק האזנה בזמן אמת באמצעות מכשיר מהווה האזנת סתר, אלא גם הקלטה של השיחה שאין עמה האזנה. ראו עמ׳ 198 לפסק הדין :

> "היסוד השלישי של ההגדרה בא להרחיב את מערכת הנסיבות שהחוק מבקש להתייחס אליה: לא רק האזנה בו-זמנית – או כלשון העם "בזמן אמת" – באמצעות מכשיר, היא האזנת-סתר, אלא גם הקלטתה של השיחה.
> המחוקק לא בא להוסיף כאן האזנה בו-זמנית אשר גם מוקלטת, אלא התייחס להקלטה בו-זמנית שאין עמה האזנה בו-זמנית, שהרי אחרת מה הרבותא בהוספתה להגדרה של "הקלטה": אם נתקיימה האזנה בו-זמנית כפשוטה, אין צורך להוסיף

[65] ע״פ 1497/92 **מדינת ישראל נ׳ צוברי** (23.8.93).
[66] יצוין כי פסק הדין פרש את ההגדרה שהייתה תקפה דאז (לפני תיקון החוק בשנת 1995) לענין האזנת סתר : ״האזנה ללא הסכמת אף אחד מבעלי השיחה, לרבות הקלטת שיחה כאמור.״ כאשר ההגדרה של ״האזנה״ אותו זמן הייתה : ״האזנה לשיחת הזולת באמצעות מכשיר״.

> *את האזכור הנפרד של הקלטתה, שהרי העבירה כבר נוצרה על-ידי ההאזנה, ותוספת הפעולה של ההקלטה, קרי התימלול או הרישום של השיחה, אינה מוסיפה דבר על העבירה שנעברה כבר ממילא, ועל-כן לא היה בתוספת האמורה כדי "לרבות". במילים אחרות, לא היה צורך להוסיף את "ההקלטה" על "ההאזנה", אלא אם הדברים כוונו להקלטה, באמצעות מכשיר, של שיחת הזולת ללא הסכמת אף אחד מבעלי השיחה, כאשר המדובר על הרחבה הבאה לחבוק הקלטה בלבד, שאין לה מאזין בו זמני. משמע, הפעלת מכשיר הקלטה לשם הקלטתה של שיחה, ללא הסכמת אף אחד מבעלי השיחה, היא בגדר "האזנת סתר", גם אם אין שמיעה (קרי, האזנה) בו-זמנית בעת שההקלטה מתבצעת, ואף אם אין אפשרות טכנית להאזנה בו-זמנית".*

37. סוגיה זו התעוררה שוב בבית המשפט העליון בעניין **בדיר**,[67] ביחס לנסיבות בהן המערערים חדרו לתא קולי והאזינו לשיחות האגורות בו. המדינה חזרה בה מהאישום נוכח השלכות הרוחב על סמכויות המשטרה ככל שיקבע כי מדובר בהאזנת סתר. בית המשפט הותיר בצריך עיון את השאלה העקרונית האם יש לראות בכך האזנת סתר.[68]

38. יוער כי הלכת **צוברי** נקבעה טרם התיקון לחוק האזנת סתר משנת 1995 אשר שמט את רכיב ההקלטה מההגדרה של "האזנת סתר" אך במקביל שינה את ההגדרה של האזנה, כך שתכלול כיום גם "קליטה או העתקה". ניתן למצוא בפסיקת בתי המשפט עמדות שונות לעניין תקפותה של הלכת **צוברי** עם תיקון החוק והוספת הוראות אלה.[69] סוגיה זו התחדדה, בכל הנוגע להבחנה בין חומר מחשב המהווה "חפץ" לבין חומר מחשב המהווה "תקשורת בין מחשבים" בפרט בכל הנוגע לדיון בפסיקה על אודות תקשורת בין מחשבים א-סינכרונית המאופיינת בכך שאין בו-זמניות בין מועד שליחת המסר לבין קליטתו ביעד.

39. באופן ספציפי נציין בקצרה שתי החלטות שקיבל בית המשפט המחוזי במסגרת החלטות ביניים בעניין **פילוסוף** (פרשת הסוס הטרויאני):

    א. הודעות דואר אלקטרוני האגורות אצל ספק שירות הדואר האלקטרוני (עניין **פילוסוף 1**):[70] בית המשפט קבע כי לגבי דואר אלקטרוני שנמצא אצל ספק שירות וטרם נקרא, מדובר בתקשורת בין מחשבים אשר במהותה נמצאת בשלב התעבורה אל מכשיר היעד, ועל כן דינו כדין "שיחה" לפי חוק האזנת סתר.

---

[67] ע"פ 10343/01 **בדיר נ' מדינת ישראל** (30.4.2003).

[68] הנאשמים הורשעו בבית המשפט המחוזי בין היתר בעבירה של האזנת סתר, בגין חדירה לתא קולי של אחר והאזנה להודעות האגורות שם שלא בהסכמתו. במסגרת הערעור בעליון על הרשעת הנאשם, חזרה בה המדינה מהאישום הספציפי של האזנת סתר נוכח השלכות הרוחב על סמכויות המשטרה כאשר מדובר בגישה לחומרים אגורים (ככל שייקבע כי מדובר בהאזנת סתר יהיה על המשטרה להוציא צו לגישה לתוכן שיחה גם אם מדובר בתוכן שיחה אגור, במקום צו חיפוש כפי שנהוג היה. בית המשפט העליון זיכה את הנאשם מהאזנת סתר נוכח הודעת המדינה, ואולם הותיר בצריך עיון את השאלה העקרונית האם יש לראות בחדירה לתא קולי והאזנה להודעות האגורות שם כהאזנת סתר.

[69] לעניין פעולת צילום בסתר של הודעות אגורות בית המשפט קבע כי זו לא האזנת סתר (ראו תיק אזרחי (מחוזי ת"א) 1477/09 **רויכמן נ' שחף אבן ושיש** (16.2.2004)). בעניין העתקת תוכן אגור בתיבת דואר אלקטרוני ללא הסכמה, העיר בית המשפט באמרת אגב כי לגישתו דומה שדרישת הסימולטניות בהלכת צוברי התבטלה עם תיקון החוק בשנת 1995 ויש לראות זאת כהאזנת סתר נוכח תכלית החוק להגן על סוד שיחו של אדם, ואולם לא נקבעו מסמרות בעניין (ראו עמר"מ (מחוזי מרכז) 13028-04-09 **אליהו נ' עיריית טבריה** (11.3.2010)).

[70] ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף** (5.2.2007). במסגרת חקירה פלילית ניתן צו חיפוש אצל שרתי ספקית שירות האינטרנט לקבלת דואר אלקטרוני היסטורי וכן דואר אלקטרוני עתידי שיתקבל במשך 30 ימים מיום הוצאת הצו. עמדת המדינה הייתה כי על מנת שהפעולה תוגדר כהאזנת סתר עליה לעמוד בדרישת הסימולטניות שנקבעה בהלכת צוברי, ועל הפעולה לייצר תיעוד, קרי העתקה, שהוא בו זמני ל"שיחה". מכאן שעמדת המדינה הייתה כי כל עוד מדובר בהעתקה של הודעות דואר אלקטרוני האגורות אצל ספק השירות, מדובר ב"חומר מחשב" ועל כן חל סעיף 23א לפקודת סדר הדין הפלילי, ואין נפקות לשאלה האם מדובר בצו שנועד לקבלת מידע היסטורי או גם מידע עתידי. בית המשפט קבע בניגוד לעמדת המדינה, כי מדובר בהאזנת סתר. לפי בית המשפט, אין לקרוא את החוק באופן דווקני, וגם בנסיבות אלה מדובר בהאזנת סתר משום שאף כאשר הדואר "חונה" אצל ספקיות התקשורת בדרכו אל מחשב היעד, הוא במהותו נמצא בשלב התעבורה אל מכשיר היעד.

ב. הודעות דואר אלקטרוני אגורות במכשיר היעד וטרם נקראו (עניין **פילוסוף 2**):[71] בית המשפט קבע כי עם הגיעה של הודעה ליעדה הסופי (מחשב היעד), אין מדובר עוד בתהליך של "תקשורת בין מחשבים" לפי חוק האזנת סתר, אלא חפץ אגור הדורש צו חיפוש במחשב. המועד הקובע להתגבשות השיחה לכדי חפץ הוא מועד הגעת ההודעה למחשב היעד, ואין נפקות לשאלה האם ההודעה נקראה או לא.

40. דרישת הסימולטניות בהצעת חוק החיפוש: דרישת הסימולטניות באה לידי ביטוי בהצעת חוק החיפוש, אשר במסגרת התיקונים השונים ביקשה להסדיר בצורה ברורה יותר את ההבחנה בין חיפוש במחשב להאזנת סתר. במסגרת הצעת החוק, הוצע לערוך תיקון עקיף לחוק האזנת סתר, בין היתר, במטרה להוסיף עלי ספר את דרישת הסימולטניות כתנאי הכרחי לכניסה אל גדרי חוק האזנת סתר, ולקבוע כי "האזנה" היא "האזנה לשיחת הזולת, קליטה או העתקה של שיחת הזולת, והכל באמצעות מכשיר תוך כדי התרחשות השיחה".

בדברי ההסבר להצעת חוק החיפוש הובהר כי שינוי ההגדרה נועד להבהיר את ההבדל בין האזנה המתקיימת תוך כדי התרחשות השיחה, לבין האזנה להקלטה של שיחה או עיון בחומר שנאגר במחשב קצה לאחר שעבר בתקשורת בין מחשבים. נוסח זה נועד להביא לידי ביטוי את הייחוד של האזנת סתר הנובע מנדיפותה של הראיה העוברת בתקשורת בין בעלי השיחה, ומכך שמדובר בפעולת אכיפה המתנהלת סימולטנית תוך כדי התרחשות השיחה (להבדיל מתפיסת מידע אגור).

פרשנות דרישת הסימולטניות בכל הנוגע לשימוש ברוגלות לצורך האזנה לתקשורת בין מחשבים

41. יישום דרישת הסימולטניות ברורה כאשר מדובר בהאזנה לשיחות המבוצעות בדיבור בין אם באמצעות טלפון ובין אם באופן בלתי אמצעי. בנסיבות אלו, על מנת שפעולה תחשב כ"האזנה" עליה להתבצע באמצעות מכשיר, **תוך כדי** חילופי המילים בין שני הצדדים, כאשר אין נפקות לשאלה האם ההקשבה להאזנה נעשית תוך כדי השיחה או לאחריה, כל עוד פעולת הקליטה נעשתה במקביל.

42. נוכח השאלות המתעוררות בהקשר של שימוש ברוגלות לביצוע האזנת סתר יש אפוא לצקת תוכן לדרישת הסימולטניות בכל הנוגע להאזנה לתקשורת בין מחשבים, ולבחון מהם התנאים ליישום דרישה זו בנסיבות אלו.

43. יש להדגיש כי הדיון בשאלת פרשנות דרישת הסימולטניות, אין בה כשלעצמה כדי להעיד על מידת הפגיעה בפרטיות הנובעת מהכרעה בה. בהתאם לעמדה המפורטת ביחס לשאלה I לנספח זה לפיה יש סמכות לחדירה למחשב מרחוק לצורך התקנת אמצעי להאזנת סתר, מרכז כובד המשקל של שאלת הפגיעה בפרטיות נוגעת בעיקרה להיבטים של היקף המידע המותר לאיסוף מכוח החוק.

44. משזה נאמר, דרישת הסימולטניות מחייבת קליטה או העתקה של המידע בשלב התקיימות ה"שיחה", ואולם יש לקרוא את דרישת הסימולטניות כדרישה מהותית ולא טכנולוגית גרידא, במובן זה שאין לקרוא את הדרישה ככזו שמחייבת שהמידע יועתק בו בשנייה שבה הוא מגיע

[71] ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף** (10.6.2009).

או נשלח. לשון אחר, דרישת הסימולטניות אכן מחייבת את איסוף והעתקת המידע במועד התקיימות השיחה באופן תכליתי, ואולם אין לקרוא דרישה זו בצורה דווקנית אשר נותנת את הבכורה לטכנולוגיה.

45. פרשנות זו מבקשת לתת דגש למהות של דרישת הסימולטניות, ולא לטכניקה כשלעצמה. היא מבקשת לקרוא את דרישת הסימולטניות – אשר נקבעה במקורה בפסיקה ביחס להאזנות שמע ובתקופה שבה הטכנולוגיה הייתה שונה בתכלית – כדרישה מהותית של ייצור התיעוד במועד השיחה. זאת ביחס למקרים בהם קיים פער זמן מינורי, שהוא סמוך למועד קיומה של השיחה עד לכדי כך שמהותית הדבר נחשב להעתקה סימולטנית עם התקיימות השיחה.

46. על פי תפיסה זו "דרישת הסימולטניות", כפי שנקבעה בפסיקה בנוגע להאזנת סתר, צריכה להתפרש כדרישה מהותית לכך שהמידע ייקלט או יועתק "באמצעות מכשיר" סמוך ככל הניתן למועד התקיימות השיחה, במובן של קליטה או העתקה של התקשורת לכל היותר ב- near real-time. בנספח המשפטי החסוי מפורטים עקרונות, אשר מגדרים את האופן לבחון את קיומה של המהותית של דרישת הסימולטניות, בשים לב לסוגיות טכנולוגיות, בדרך שתמנע זליגה של הפרשנות התכליתית מעולם האזנת סתר לחיפוש סמוי אסור.

47. יצוין כי הפרשנות התכליתית של דרישת הסימולטניות כפי שפורטה לעיל, אינה אמורה לפגוע בהבחנה המקובלת בין סמכות החיפוש לבין סמכות להאזנת סתר. דהיינו, ניתן להותיר את ההבחנה המקובלת כהבחנה עקרונית בין מידע היסטורי אגור – שזו פעולת חיפוש, לבין העתקה רציפה בזמן אמת של מידע שמתקבל או נשלח בתקשורת בין מחשבים, אף אם ההעתקה היא של מידע אגור סמוך מאוד לאחר אגירתו – שזו פעולה של האזנת סתר.

48. בהתאם לכך, לא ניתן להכשיר אמצעי להאזנת סתר אשר מאפשר לתת הוראה לשאוב מידע היסטורי האגור על המכשיר, גם אם מדובר במידע אשר נוצר בתוך תקופת הצו של בית המשפט. פעולת ההאזנה יכולה להיות רק פעולה מתמשכת במבט צופה פני עתיד בלבד ועליה להתבצע near real time.

שאלה III - אילו סוגי תוצרים מהווים האזנת סתר כהגדרתה בחוק והאם יש תוצרים שניתן לקבל לצורך ביטחון ותפעול הכלי?

(1) האם ניתן לקבל מידע עודף שאינו מועבר בתקשורת בין מחשבים לצורך ביטחון ותפעול הכלי מכוח סמכויות העזר

49. כפי שעלה במסגרת בדיקת הצוות, עשויים להיות סוגי מידע אשר על אף שלא הועברו במסגרת תקשורת בין מחשבים, אלו נדרשים לצורך ביטחון ותפעול אמצעי האזנת הסתר. בתוך כך, נבחנה השאלה האם **רשימת האפליקציות** נדרשת, לצורך ביטחון ותפעול הכלי במסגרת ביצוע האזנת סתר על ידי התקנת אמצעי על הטלפון הנייד או מחשב. יצוין כי הרחבה בעניין זה מפורטת בדוח החסוי.

50. אכן, במישור התאורטי – סעיף 10א לחוק האזנת סתר יכול להסמיך קבלת מידע עודף שהוא נדרש וחיוני לצורך התקנת אמצעי האזנת הסתר ותפעולו, ובכלל זה על מנת למנוע

חשיפה שלו. כך גם במישור הפיזי, כאשר מבוצעת כניסה למקום לצורך התקנת אמצעים לביצוע האזנת סתר, פירוקם או סילוקם, פעולה זו עשויה לכלול חשיפה למידע עודף על אודות אדם מעצם הכניסה והצורך באיתור מקום להתקנת האמצעים.

ואולם במישור המעשי – יש הכרח לבחון בזהירות ובקפידה ביחס לכל סוג מידע באופן פרטני האם הוא חיוני לעצם פעולת ההתקנה, והאם אין ביחס למידע האמור משום פגיעה בפרטיותו של אדם באופן העולה על הנדרש, וכן, בשים לב למידת הפגיעה הפרטיות – האם לא נדרשת הסמכה מפורשת. בשים לב לכך, הבחינה המשפטית נוגעת לשאלת הצורך והמידתיות של סוגי המידע המסוימים, אשר אף יש בה כדי להשליך על שאלת הסמכות. יש חשיבות לבחון סוגיה זו בזהירות ותוך הקפדה יתרה, ודאי כאשר מלכתחילה הפרשנות על אודות הסמכות לחדור למכשיר קצה לצורך ביצוע האזנת סתר נשענת על פרשנות תכליתית של הוראות החוק כמפורט מעלה. למותר לציין כי אף אם במקרים מסוימים יימצא כי ניתן לקבל מידע עודף לצורך ביטחון הכלי, אזי שניתן לעשות שימוש בו רק לצורך תכלית זו.

51. במסגרת בחינה זו, יש להדגיש כי הפגיעה בפרטיות נובעת מעצם איסוף מידע על אודות אדם (אף בהיעדר חשיפה אליו או שימוש בו בידי גורמי החקירה כטענת המשטרה), נפנה לדבריה של השופטת דפנה ברק-ארז בבג״ץ **האגודה לזכויות האזרח**[72] בעניין איכוני השב״כ בקורונה:

> "ראוי להדגיש כי הזכות לפרטיות כוללת בחובה לא רק הגנה מפני "גילוי" מידע הנוגע לאדם לצדדים שלישיים. ההגנה על זכות זו חייבת להתייחס גם לפעולות הקודמות לגילוי במישור הזמן – איסוף המידע [...]. הטלת הגבלות על איסוף מידע הנוגע לאדם ועל אגירתו באופן אלקטרוני היא חלק אינטגרלי מהזכות לפרטיות אף כאשר הוא אצור במאגר המידע ואינו נחשף בפני כול. מטעם זה חוק הגנת הפרטיות כולל פרק מיוחד שעניינו פיקוח על מאגרי מידע (פרק ב' לחוק זה). כמו כן, חוקים רבים נוספים כוללים הגבלות על איסוף חומר אישי הנוגע לאדם. ייתכן למשל שהשימוש במידע גנטי היה יכול להרים תרומה נוספת למאבק בפשיעה אילו כל אזרחי המדינה היו נדרשים למסור דגימה למאגר כללי שישמש את המשטרה. אולם, מחשבה זו כלל אינה עולה על הדעת. ובצדק רב."

52. מכאן שאין חולק כי הפגיעה בפרטיות נעשית החל משלב איסוף המידע באופן ממוכן על ידי המערכת.

53. באופן פרטני, לעניין היקף הפגיעה בפרטיות הנובעת **מרשימת האפליקציות**, למותר לציין כי מידע פרטי רחב היקף על אודות אדם יכול להתקבל מרשימת האפליקציות המותקנת במכשירו הסלולרי. מידע פרטי מעין זה יכול לכלול מידע על אודות תחביביו השונים, על מידע פרטי ויתכן שאף אינטימי, כמו כן ניתן במקרים מסוימים להסיק מהן דעותיו הפוליטיות. בימינו, נוכח השימוש המוגבר בפלטפורמה האפליקטיבית לניהול מגוון התחומים של החיים, רשימת האפליקציות לבדה יש בה כדי לפגוע בליבת פרטיותו של אדם.

---

72 בג״ץ 6732/20 ***האגודה לזכויות האזרח נ' הכנסת***, פסקה 12 לפסק דינה של השופטת ברק-ארז (1.3.2021).

54. הצורך ברשימת האפליקציות לביטחון הכלי: כפי שנמסר מחברת NSO וכן מהחברה הנוספת שמערכת בפיתוחה נמצאת בידי המשטרה, רשימת האפליקציות נדרשת למערכת לטובת ביטחון הכלי והאפשרות למנוע את גילויו, על ידי בחינה ממוכנת שנעשית על ידי המערכת. כפי שנבדקת על ידי צוות הבדיקה, אכן רשימת האפליקציות נדרשת לצורך אבטחת הכלי על ידי המערכת.

55. ואולם, שימוש במידע על ידי המשטרה בנוסף על כך אינה מידתית. אף אם ניתן להראות קשר רציונאלי בין האמצעי למטרה, הרי שלא מדובר באמצעי שפגיעתו פחותה, וודאי שפעולה זו אינה עומדת במבחן המידתיות במובנו הצר, קרי מידת הפגיעה בפרטיות אינה עומדת ביחס ראוי למול התועלת הנוספת שהיא מביאה על עיבודו באופן ממוכן, להגשמת התכלית של ביטחון הכלי.

על בסיס המידע שהובא בפני צוות הבדיקה, והועבר ליועצת המשפטית לממשלה, אין למשטרה יתרון **טכנולוגי** נוסף, על הפעולות אשר מבוצעות באופן אוטומטי על ידי המערכות הטכנולוגיות, לזיהוי אפליקציות המסכנות את הכלי ועשויות לחשוף אותו.

56. **נוכח כלל הדברים האמורים, העמדה המשפטית היא כי על השימוש ברשימת האפליקציות להיעשות באופן ממוכן שאינו חשוף לעיני אדם. על כן יש לבטל את האפשרות להצגת רשימת האפליקציות ורשימת הקבצים בממשק המשתמש.**

57. יצוין כי נבחנו סוגי מידע נוספים. לגבי נתונים טכניים מסוימים נקבע כי אכן נדרשים למשטרת ישראל לצורך תפעול הכלי ואין בהם פגיעה העולה על הנדרש. כמו כן, נבחנו סוגי נתונים נוספים אשר נקבע כי אין סמכות לקבלם מכוח סמכויות העזר לפי חוק האזנת סתר. הדברים מפורטים בדוח החסוי.

(2) סוגי התוצרים המהווים תקשורת בין מחשבים לפי החוק

58. תנאי בסיסי וראשוני להגדרה האם תוצר מהווה "תקשורת בין מחשבים" הוא שמדובר במידע שהועבר בתקשורת בין מחשב של יעד ההאזנה לבין מחשב אחר. ואולם נקודת מוצא זו אינה ממצה את הדיון המשפטי בכל הנוגע להיקף ההגדרה של תקשורת בין מחשבים.

59. מעבר לשאלת לשון החוק ומעבר לתיחום בפן הטכנולוגי של מידע המועבר בין מחשב אחד למחשב אחר, יש לבחון מבחינה תכליתית את היקף פרישתו של חוק האזנת סתר בכל הנוגע לסוגי התוצרים המותרים במסגרת הסמכות לבצע האזנת סתר. בחינה תכליתית זו מתחייבת במיוחד בעידן הנוכחי, בו המחשב ובכלל זה הטלפון הנייד מכיל את "סיפור חייו" של המשתמש, דרכו הוא מבצע כמעט את כל פעולותיו היומיומיות.

60. עמדה הנצמדת ללשון החוק תוך מתן בכורה לשאלה הטכנולוגית לבדה, ותוך זניחה של בחינה תכליתית של החוק לעניין האם מדובר במידע שנועד להיות מסר (גם אם במובנו הרחב של "סוד שיחו של אדם"), עשויה להוביל לכך שבפועל כל מידע ייכנס לגדרי חוק האזנת סתר. זאת בשים לב להתקדמות הטכנולוגית ולכך שיותר ויותר פעולות של אדם נשענות על טכנולוגיה הנסמכת על תקשורת בין מחשבים. כך למשל, יכולות להיכלל פעולות המייצרות תקשורת מול מחשב, אשר אינן מבוצעות באופן יזום על ידי יעד ההאזנה, אינן בידיעתו או אף אינן בשליטתו. כך למשל, בכל הנוגע למידע האגור על מכשיר היעד אך

מועברת במסגרת סנכרון או גיבוי, על אף שטכנולוגית מדובר בתקשורת בין מחשבים, תכליתית מידע זה חורג מחוק האזנת סתר.

61. באופן כללי, לשלמות התמונה יצוין כי קיימת פרשנות הנוהגת מזה שנים, אשר בהקשרים שונים אף צוינה בדיונים בוועדות הכנסת,[73] לפיה חוק האזנת סתר מתיר ניטור גלישות באינטרנט ככל שניתן צו בית משפט המתיר זאת. על אף שפרשנות זו נוהגת מזה שנים רבות, ועל כן לא נדרשנו אליה במסגרת הבחינה המשפטית בסוגיה זו, ברי כי גם בעניין זה יש מקום לקידום חקיקה לצורך עיגון מפורש לעניין זה בחוק האזנת סתר[74].

62. לסיכום, בשים לב לעמדה המפורטת לעיל, נבחנו כלל סוגי התוצרים המתקבלים על ידי המערכות שבידי משטרת ישראל, ונקבע לגבי חלקם כי אכן מהווים "תקשורת בין מחשבים" ובעניין חלקם נקבע כי אין סמכות למשטרה לקבלם. כמפורט בדוח החסוי.

---

[73] ראו למשל פרוטוקול דיון בוועדת החוקה, חוק ומשפט מיום 19.6.2017 בעניין הצעת חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע"ז-2017 (עמ' 26-18).

[74] הפרשנות הנוהגת מזה שנים, היא כי בהבחנה בין נתוני תקשורת (שחוק נתוני תקשורת חל עליהם) לבין נתוני תוכן, ניטור הגלישות של אדם מהווה תוכן ועל כן נכלל בגדרי חוק האזנת סתר. אחת הטענות שהועלו בפני צוות הבדיקה בדיונים השונים עם הרשות להגנת הפרטיות, וארגוני חברה אזרחית, היא כי לא ניתן לפרש "שיחה" כפעולה שאדם עושה עם עצמו, ועל כן אין סמכות לנטר את הגלישות של אדם. בהקשר זה נטען כי האזנת סתר מתייחסת אך לשיחה בין שני אנשים שכן במקרים אלו רמת הפרטיות היא פחותה לעומת מידע שאני בוחר שלא לשתף עם אדם נוסף. במובן זה, לגישתם, גלישות במהותן דומות יותר לניטור המחשבות והתהיות הפנימיות של אדם ולא למסר שיחה, לפיכך לא ניתן לקרוא סמכות זו מכוח חוק האזנת סתר. יודגש שוב כי הפרשנות לעניין הסמכות לניטור גלישות היא הפרשנות המשפטית הנוהגת מזה שנים. חוק האזנת סתר אינו מוגבל אך ורק לשיחה המתקיימת בין שני אנשים בלבד. **אמנם, אין לקרוא את החוק בצורה לשונית בלבד במובן זה שכל תקשורת בין מחשבים מהווה שיחה, ויש לבחון סוג של תקשורת בין מחשבים לגופו מבחינת תכליות החוק.** בכל הנוגע לתקשורת בין מחשבים קיים ספקטרום של פעולות ביחס לציר הנוגע למהו "סוד שיח". קו הגבול לעניין זה אינו נעצר לעמדתנו רק בשיחה המתנהלת בין שני אנשים. יודגש כי הבחנה זו אף אינה קיימת בכל הנוגע להאזנה השמע הרגילה – כך למשל, אם בעבר אדם היה מחייג מהמכשיר הסלולרי שלו אל הטלפון בבית על מנת להשאיר תזכורת קולית, ניטור השיחה נכללת בסמכות להאזנת סתר – אף שבמקרה זה לא מדובר במסר שהועבר לאדם אחר. עוד לשם המחשה, יש מקרים בהם אדם מבצע פעולות באינטרנט הכוללות התכתבות עם בוט, במסגרתה הוא שולח הודעות ושואל שאלות במקום לחפש את המידע בתוכן האתר עצמו. לעמדתנו ניטור שיחה זו עם בוט, אף היא נכללת בסמכויות להאזנת סתר. בכל הנוגע לציפייה לפרטיות, מן הידועות היא שפעולות חיפוש וגלישה לאתרים באינטרנט הן פעולות המנוטרות פעמים רבות על ידי גופים מסחריים בהתאם לתנאי השימוש שלהם, למשל לצורך שיפור השירות שמספק הגוף ומיקוד פרסום ביחס לאותו אדם, ולכן אף ההשוואה לכך שמדובר בניטור מחשבותיו הפרטיות של אדם מבחינת מידת הציפייה לפרטיות אינה מדויקת.

היועץ המשפטי לממשלה

ירושלים, כ"ט שבט תשפ"ב
31 ינואר 2022

מס' מסמך: 004-99-2022-001896
(בתשובה נא לציין מספרנו)

לכבוד
עו"ד עמית מררי, המשנה ליועץ המשפטי לממשלה (משפט פלילי) – יו"ר הצוות
מר איל דגן– חבר הצוות
מר צפריר כץ– חבר הצוות

<u>כתב מינוי - צוות לבדיקת האזנות סתר בדרך של תקשורת בין מחשבים</u>

נוכח טענות שעלו אודות שימוש לא חוקי לכאורה באופן בו משטרת ישראל מפעילה אמצעים לביצוע האזנת סתר לתקשורת בין מחשבים, כמו גם מכוח הסמכות הנתונה ליועץ המשפטי לממשלה לפיקוח על האזנות סתר שמבצעת משטרת ישראל, לפי סעיף 6(ו) לחוק האזנת סתר, התשל"ט-1979, אני ממנה בזאת צוות לבדיקת האזנות סתר בדרך של תקשורת בין מחשבים.

ככל שיעלו שאלות משפטיות או פרשניות הנוגעות לגדרי סמכות המשטרה, יידונו אלו על ידי המשנה ליועץ המשפטי לממשלה (משפט פלילי) בנפרד מעבודת הצוות.

לשם ביצוע הבדיקה, הצוות יהיה רשאי לשמוע ולהסתייע בגורמים נוספים, לרבות מומחים בתחום המשפט ובתחום הטכנולוגיה.

יובהר כי ככל שבדיקת הצוות תעלה בממצאיה התנהלות פסולה, שיש בה משום חשד לעבירה פלילית, יועבר הטיפול בממצאים הקונקרטיים לרשויות המוסמכות לכך על פי דין.

הצוות יחל בעבודתו באופן מיידי ומתבקש להגיש את ממצאיו עד ליום ב' בתמוז התשפ"ב (1 ביולי 2022).

בראש הצוות תעמוד עו"ד עמית מררי, המשנה ליועץ המשפטי לממשלה (משפט פלילי).

בברכה,
אביחי מנדלבליט

רח' צלאח א-דין 29, ירושלים 91010 ☎ 073-3925511 , 073-3925521 פקס:02-6467001

העתקים: פרקליט המדינה;
מפכ"ל משטרת ישראל;
היועצת המשפטית, משרד המשפטים.

רח' צלאח א-דין 29, ירושלים 91010 ☎ 073-3925511 , 073-3925521 פקס:02-6467001