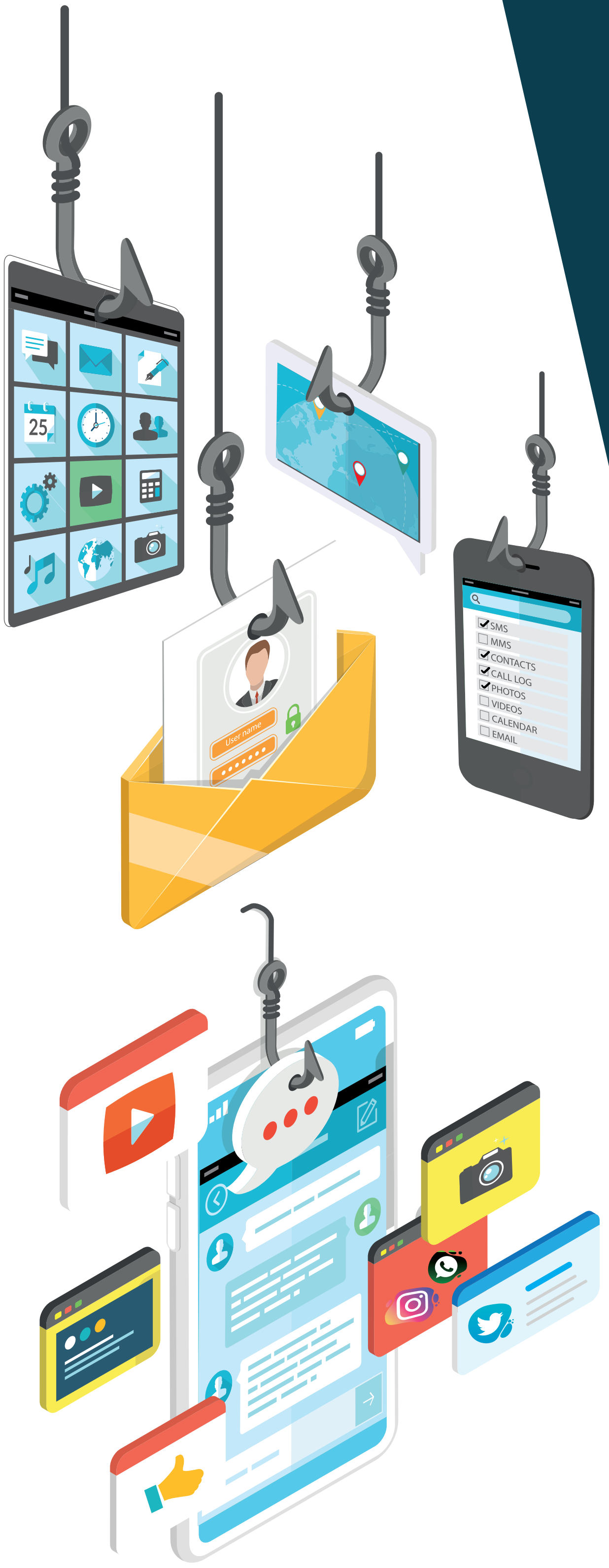
איגוד האינטרנט הישראלי
ISOC-IL

טכנולוגיות חדירה וחיפוש במכשירים חכמים ונכסים דיגיטליים על ידי רשויות האכיפה בישראל

סקירה מקצועית מיוחדת



מחברים: ד"ר אסף וינר, עו"ד הדס תמם בן-אברהם

אישור מקצועי: עו"ד יורם הכהן

ביקורת עמיתים (מדעי המחשב ופורנזיקה):
פרופ' אור דונקלמן, דנית לייבוביץ'-שאטי

ביקורת עמיתים (משפטים): פרופ' מיכאל בירנהק,
פרופ' יואב ספיר, ד"ר עמרי רחום-טוויג

ינואר 2023

איגוד האינטרנט הישראלי
ISOC-IL

איגוד האינטרנט הישראלי (ע"ר) הוא ארגון ללא כוונת רווח אשר פועל למעלה מ-25 שנה להטמעת השימוש באינטרנט לטובת הציבור בישראל ומפעיל תשתיות אינטרנט חיוניות בישראל: מרשמי שמות המתחם (domain names) המדינתיים ".il" ו-".ישראל" ומחלף האינטרנט הפנים מדינתי (IIX). הידע והניסיון המקצועי של איגוד האינטרנט הישראלי במחקר, בפיתוח ובהפעלה של טכנולוגיות אינטרנט עבור הציבור הישראלי משמש בסיס לפעילות מחקר, מדיניות והעצמת הקהילה שמבצע האיגוד. בכלל זה, איגוד האינטרנט הישראלי מפעיל את מיזם Block.org.il המספק לציבור הרחב ידע וכלים להגנת סייבר; את מיזם data.isoc.org.il האוסף ומנגיש נתונים כמותיים-סטטיסטיים על האינטרנט הישראלי ומשתמשיו; ומפרסם מחקרי מדיניות מקצועיים המיועדים ליידע ולטייב את זירת האינטרנט הישראלית והגלובלית בצמתים מגוונים של משפט וטכנולוגיה.

סקירה מקצועית זו נכתבה בידי ד"ר אסף וינר (סמנכ"ל רגולציה ומדיניות באיגוד האינטרנט הישראלי; מרצה למשפט וטכנולוגיות מידע באוניברסיטת תל אביב ובאוניברסיטת בן גוריון; עמית בכיר במרכז הנשיא שמגר למשפט דיגיטלי וחדשנות באוניברסיטת תל אביב) ועו"ד הדס תמם בן-אברהם (מרצה וחוקרת בתחומי המשפט, הטכנולוגיה והליכי קבלת החלטות; סגנית דקן וראשת המכון לסיכוני סייבר למנהלים, הפקולטה למנהל עסקים בקריה האקדמית אונו; בעבר כיהנה כקצינה ביחידת להב 433 במשטרת ישראל). עוזרי מחקר: נופר קדוש ועדו אילי.

פרקים א–ג בסקירה זו עברו ביקורת עמיתים על ידי פרופ' אור דונלקמן (מדעי המחשב, אוניברסיטת חיפה) ודנית ליבוביץ-שטי (Alpha Forensics).

פרקים ד–ו בסקירה זו עברו ביקורת עמיתים על ידי פרופ' מיכאל בירנהק (משפטים, אוניברסיטת תל אביב), פרופ' יואב ספיר (משפטים, אוניברסיטת תל אביב), וד"ר עמרי רחום-טוויג (מרכז הנשיא שמגר למשפט דיגיטלי וחדשנות באוניברסיטת תל אביב).

איגוד האינטרנט הישראלי מבקש להודות לעמיתים נוספים שלקחו חלק בהערות ובתשומות לטיוטות מוקדמות של מסמך זה: אייל זילברמן (מדיניות ציבורית, אוניברסיטת סטנפורד), ד"ר דלית קן-דרור פלדמן (הקליניקה למשפט, טכנולוגיה וסייבר, אוניברסיטת חיפה), עו"ד עמית אשכנזי (המרכז למשפט טכנולוגיה, אוניברסיטת חיפה) ואביה גל (איגוד האינטרנט הישראלי).

© כל הזכויות שמורות לאיגוד האינטרנט הישראלי (ע"ר), 2023.
ליצירת קשר ושיתופי פעולה מחקריים: policy@isoc.org.il
עיצוב החוברת: www.7design.co.il

תקציר מנהלים ועיקרי ממצאים

משטרת ישראל ורשויות אכיפה נוספות, כגון מצ"ח, הרשות לניירות ערך, רשות המיסים ואף הרשות להגנת הפרטיות, מפעילות מזה כעשור כלי פורנזיקה דיגיטלית מתקדמים לפריצה וחיפוש במחשבים אישיים וטלפונים ניידים שנתפסו במסגרת חקירה. כלים אלו מספקים גישה לכמות עצומה של נתונים חושפניים, הנצברים אגב שימוש יומיומי במכשיר, כגון התכתבויות, תמונות וסרטונים, רשימות אנשי קשר, היסטוריית גלישה, נתוני מיקום ובמקרים רבים מסוגלים לגשת גם להרשאות גישה (credentials) לשירותים מרוחקים, כגון רשתות חברתיות ושירותי ענן. במקביל, בתי המשפט בישראל הכירו בשנים האחרונות בכך שחדירה לטלפונים חכמים מאפשרת לרשויות אכיפת חוק גישה למידע אישי ורגיש בהיקף חסר תקדים, וכי דיני החיפוש המיושנים אינם כוללים פיקוח וביקורת מספקים נגד שימוש מופרז או לא־מידתי בכלים טכנולוגיים רבי עוצמה לחילוץ נתונים אישיים ממכשירים חכמים ומחשבונות הענן המקושרים אליהם. למרות זאת, נכון למועד כתיבת מסמך זה, לא עודכנו הדינים הנוגעים לשימוש בכלים אלו.

סקירה מקצועית זו נועדה לספק נתונים ועובדות מהימנים על אופן הפעולה והיכולות של כלים טכנולוגיים המופעלים כיום בישראל, לצד מיפוי מפורט של מסגרת הדין ונוהלי המשטרה להפעלתם. המסמך נועד להציב בסיס עובדתי לדיון ולעיצוב מדיניות בידי נבחרי הציבור, מערכת אכיפת החוק ומערכת המשפט, בין היתר על רקע קריאות ציבוריות ושיפוטיות לעדכון דיני החיפושים והראיות והתאמתם למציאות הטכנולוגית העכשווית בעידן האינטרנט של הדברים ומחשוב ענן.

הטכנולוגיה של אמצעי החדירה והחיפוש שמפעילות הרשויות בישראל

יכולות הכלים לחדירה, העתקה וחיפוש במכשירים חכמים באמצעות תפיסה פיזית שלהם

מחשבים אישיים ומכשירים חכמים אחרים, ובפרט טלפונים ניידים, אוצרים כמויות מידע עצומות על משתמשיהם וסביבתם. מידע זה כולל לרוב גם פרטים אישיים ולעיתים פרטים אינטימיים ממש. רשויות האכיפה בישראל משתמשות בטכנולוגיה עוצמתית, המאפשרת לפרוץ, להעתיק ולנתח את כלל הנתונים הנגישים ממכשירים שנתפסו במהלך חקירה, כגון:

נתונים מתוכנות ייעודיות ויישומונים (אפליקציות): מרבית התוכנות הייעודיות והאפליקציות בטלפונים חכמים יוצרות ושומרות נתוני משתמשים – היסטוריית גלישה, נתונים ומדדים רפואיים, מידע פיננסי והיסטוריית תשלומים, תכתובות, שיחות צ'ט ועוד. הטכנולוגיות הפורנזיות שמפעילות הרשויות יכולות להעתיק נתונים מתוכנות ואפליקציות פופולריות, ומתעדכנות בקביעות לתמיכה באפליקציות נוספות.

מטא־נתונים (metadata): כלי זיהוי פלילי למכשירים חכמים יכולים לחלץ רשומות של מועדי ההתקנה, השימוש והמחיקה של תוכנות ואפליקציות, וכן תדירות השימוש, ואף להראות מתי המכשיר הופעל או כובה, מתי המשתמשת קראה הודעה, האם ומתי בוצעה התחברות להתקני Bluetooth או Wi-Fi ופרטיהם, חיפושים ברשת או במכשיר, ועוד.

נתונים ש"נמחקו": לעיתים כלים אלו יכולים לגשת לנתונים ש"נמחקו", שכן מחיקת קובץ לא בהכרח מעלימה אותו מהמכשיר, ובוודאי לא מהענן או משירותים אחרים שבהם הוא שמור או מגובה.

סיסמאות ופרטי התחברות לשירותים: במרבית המכשירים החכמים נשמרות סיסמאות המשתמש לשירותים ציבוריים ומסחריים רבים, וטכנולוגיות אלו יכולות לחלץ את הסיסמאות ולנצלן לדליית מידע מכל שירות שאליו הן מקושרות.

תהליך מיצוי נתונים וראיות ממכשירים חכמים כגון טלפונים ניידים במסגרת תהליך החקירה הגלויה נעשה בארבעה שלבים עיקריים:

1. תפיסת המכשיר ע"י גורם האכיפה
2. שכפול נתוני המכשיר, לרבות פריצת מנגנוני נעילה
3. ניתוח והצלבה של המידע
4. העברת פלט מיצוי לתביעה ולהגנה

לאחר תפיסת המכשיר, חיפוש וחילוץ הנתונים ממנו יכולים להיעשות בכמה דרגות טכנולוגיות:

דפדוף ידני – במכשיר כמשתמש רגיל

LOGICAL EXTRACTION – אוטומציה של חילוץ נתונים הנגישים למשתמש הרגיל

FILE SYSTEM EXTRACTION – העתקת מערכת הקבצים המלאה של המכשיר (עשויה לכלול נתונים שהמשתמש אינו חשוף להם, כגון קבצים זמניים ותיעוד תהליכים במערכת ההפעלה)

PHYSICAL EXTRACTION – העתקה פיזית המשכפלת את כל הנתונים שעל החומרה (bit-by-bit)

טכנולוגיות לחדירה, העתקה וחיפוש במכשירים חכמים באופן סמוי (רוגלות)

משטרת ישראל מבצעת חדירה, פריצה, חיפוש, האזנה והעתקה של חומר לא רק באמצעות תפיסה פיזית, אלא גם באמצעות רוגלות המותקנות מרחוק ובסתר במערכות מחשוב ובמכשירים חכמים. רוגלה שהותקנה בהצלחה מאפשרת גישה מלאה לתוכן שנאגר במכשיר לאורך זמן (בדומה לחיפוש במכשירים שנתפסו), וכן מעקב אחר השימוש הרציף בו, ביצוע פעולות בתוכנה או הפעלת החומרה ללא ידיעת המשתמש. לכן, רוגלות כגון פגסוס שמפעילה משטרת ישראל מעוררות חששות ייחודיים שאין להם מענה בדין הישראלי:

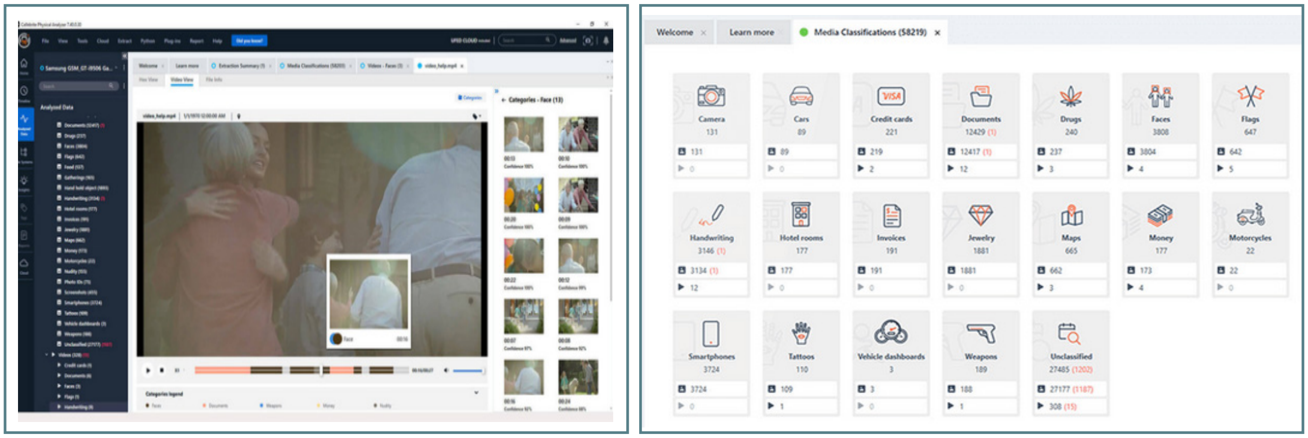
- **להבדיל מחיפוש או האזנת סתר, רוגלות לא מוגבלות לאיסוף מידע רק מיום אישור ה"האזנה"** ויכולות לגשת לכלל המידע וחומר המחשב שזמינים דרך המכשיר, גם אם הופק או נצבר לפני שנים רבות או על ידי צדדים שלישיים.
- **להבדיל מחיפוש או האזנת סתר, רוגלות חושפות את בעל המכשיר לפגיעות סייבר נוספות מצד גורמים זדוניים ומעוררות קשיים עקרוניים בכל הנוגע להבטחת הליך הוגן, אי־פגיעה בשרשרת הראייתית ואמינות המידע המופק בחדירה.** מכיוון שחדירה לטלפון חכם באמצעות רוגלה נעשית באופן סמוי, ביצוע של חדירה או חיפוש מרחוק כרוך בשינוי נתונים ונטרול או עקיפה של מערכות אבטחת המידע המובנות בחומרה ובמערכת ההפעלה של

איגוד האינטרנט הישראלי
ISOC-IL

המכשיר. יש גם חשש מ"זיהום" של נתוני המכשיר, ברשלנות או בזדון, עקב חוסר היכרות של המפעיל עם המערכת הנתקפת, תקלות במערכת החדירה, או שינויי מידע במכשיר במסגרת מערך ההגנה שלו. וכמובן, גורמי החקירה יכולים ליזום תקשורת בשם בעל המכשיר או לשנות את תוכנו בסתר.

טכנולוגיות לניתוח והצלבה של עושר המידע המחולץ ממכשירים חכמים

פיתוחים מהשנים האחרונות אף מאפשרים לרשויות להשתמש בטכנולוגיות בינה מלאכותית (AI) ולמידת מכונה (Machine Learning), לרבות זיהוי פנים ועצמים, לצורך ניתוח והצלבה של מידע העתק המחולץ מהמכשיר, והצגה אוטומטית של דפוסים ותובנות מעשיות על פעילותו של החשוד, לרבות מידע נרחב על קשריו החברתיים ואנשים שאיתם שוחח, גם אם אינם בגדר חשודים.



תמונות 6–7: צילומי מסך מתוך מערכת Cellebrite Physical Analyzer המסווגת תמונות בעזרת בינה מלאכותית, ומאתרת ומסווגת מדיה על בסיס העדפות נבחרות (מקור/קרדיט: cellebrite.com/en/physical-analyzer)

כמפורט במסמך, כלים ויכולות אלו מחייבים את מעצבי המדיניות להתמודד עם הסיכון הכללי של הטיות פסולות (bias), המאפיינות רבים מהשימושים של רשויות האכיפה בטכנולוגיות בינה מלאכותית ולמידת מכונה; ועם היכולת המוגבלת של גופי החקירה ורשויות התביעה להתחקות אחר אופן יצירת הפלט של מנגנוני AI.

מהימנות, אמינות וחולשות של הכלים הטכנולוגיים אותן מפעילות הרשויות

כלים פורנזיים לחילוץ ועיבוד מידע, ובפרט אלו המשמשים את רשויות החקירה בישראל, מנצלים חולשות אבטחה במערכת ההפעלה, בחומרה, באמצעי התקשורת או בתוכנה של מכשירים חכמים כדי לשבש או לעקוף את מנגנוני הנעילה והאבטחה המובנים בהם. גם תוכנות ייעודיות לחיקור טלפונים ניידים עשויות לכלול חולשות שאינן ידועות למפתחים או למפעילים.

ב־2021 התגלו חולשות אבטחה נרחבות ומטרידות בכלים UFED ו־Physical Analyzer, הנמצאים בשימוש נרחב של רשויות אכיפת החוק בישראל לאורך העשור האחרון. חולשות אלו אפשרו לבעלי מכשירים שהכירו אותן לפגוע בתהליך חילוץ ועיבוד המידע. זאת באמצעות הכנת קובץ מבעוד מועד, אשר בעת הפעלת כלי UFED על המכשיר, ישבש את הדו"ח הפורנזי של הסריקה ואף ישנה נתונים של מכשירים אחרים השמורים במערכת (הוספה או הסרת טקסט, דוא"ל, תמונות, אנשי קשר ועוד), לרבות מכשירים עתידיים.

איגוד האינטרנט הישראלי ISOC-IL

גם כלים פורנזיים לחדירה מרחוק, כגון סייפן או פגסוס, מבוססים על תוכנה וקוד העשויים לכלול חולשות שאינן ידועות. אך עיקר הבעייתיות שבהם נובעת מכך שהפעלתם כרוכה, בהגדרה, בשינוי נתונים במכשיר היעד ומערכות אבטחת המידע המובנות במערכת ההפעלה או החומרה של המכשיר – ללא ידיעת המשתמש – על מנת להסתיר את ההדבקה והגישה הנמשכת. בשל הצורך בהסתרה, על כלים אלה לשנות את התיעוד האוטומטי (log) במערכת ההפעלה או במערכת הקבצים של המכשיר, מה שעשוי ליצור קושי ראייתי מהותי. וכאמור, ישנו חשש כי גורמי החקירה יתחזו לבעל המכשיר או ישנו את תוכנו.

למרות החולשות העשויות להשפיע על מהימנותם או אמינותם של תוצרי הכלים הללו, אין בישראל הליך מובנה לבחינה ואישור של תקינות פעולתם בידי צד שלישי ניטרלי. זאת בשונה ממערכות טכנולוגיות אחרות, דוגמת הממל"ז או א־3 שבשימוש המשטרה, שנבחנו בידי בית המשפט ומומחים מטעמו. אי־בחינתם המקצועית של כלי רוגלה בידי צד שלישי מומחה מהווה ליקוי מהותי, ויש להסדיר נושא זה.

מיפוי הדין הקיים לחדירה וחיפוש במכשירים חכמים ומשאבי ענן

הדין הקיים, המבוסס על חקיקה, הנחיות פרקליט המדינה ונוהלי רשויות האכיפה, מאפשר לרשויות האכיפה להשתמש בכלים הנידונים באופן סמוי וגלוי בתהליכי חקירה. החקירה מתחילה לרוב בחשאי, ומתבססת על האזנות סתר לשיחות ולתקשורת מחשבים של החשוד (שמיעה, קליטה או העתקה של "שיחה" באמצעות מכשיר). בהמשך, תהליך החקירה הגלויה מתמקד בתפיסה, חיפוש וחדירה למכשירים ולחומר מחשב.

1. מסגרת הדין בתהליך החקירה הגלויה: תפיסה וחיפוש מכוח הסדרי פקודת סדר הדין הפלילי

כמתואר בהרחבה במסמך, מסגרת החיפוש המשטרתי במחשב או חומר מחשב מעוגנת בפקודת סדר הדין הפלילי ומורכבת מהשלבים הבאים: (א) הנפקת צו חדירה למחשב או קבלת הסכמה מדעת של החשוד; (ב) תפיסה פיזית של המכשיר החכם; (ג) פריצה, העתקת וניתוח החומרים באמצעות טכנולוגיה פורנזית; (ד) העברת חומרי החקירה והראיות לתביעה ולהגנה. כל אחד משלבים אלו מעורר שאלות משפטיות־חוקיות, חברתיות ומוסריות רבות, המפורטות במסמך.

שאלות אלו מעסיקות גם את בתי המשפט בישראל, המכירים בכך שחדירה של רשויות האכיפה למכשירים חכמים מאפשרת להן גישה להיקף חסר תקדים של מידע אישי ורגיש, אולם הדינים הנוגעים לשימוש בכלים טכנולוגיים לפורנזיקה דיגיטלית עדיין לא עודכנו.

2. מסגרת הדין בתהליך החקירה הסמויה: "האזנת סתר לתקשורת בין מחשבים"

החל משנת 1995 הורחבה ההגדרה של "שיחה" בחוק האזנת סתר, והוחלה גם על "תקשורת בין מחשבים", כמפורט בהרחבה במסמך. מסקירת המצב המשפטי הקיים בעניין זה עולה שהסמכות לביצוע האזנת סתר חלה על ניטור התעבורה של תקשורת בין מחשבים בעת ה"שיחה" (In Transit), ואילו חדירה מרחוק למידע שנאגר במחשב קודם למועד החדירה היא חיפוש. חומר מחשב שנאגר במכשיר חכם (In Rest), גם אם הגיע אליו באמצעות תקשורת בין מחשבים (למשל דוא"ל שהמשטרה מבקשת לגשת אליו בדיעבד), נחשב "חפץ", ונדרש צו חיפוש במחשב כדי לגשת לנתונים הצבורים במכשיר שנתפס. על כן, לפי עמדת פרקליטות המדינה, איסוף מידע שלא הועבר בתקשורת בין מחשבים, או שנאגר קודם למועד התקנת הכלי, איננו האזנת סתר המותרת לפי חוק, אלא חיפוש סמוי במחשב, שאינו בסמכות המשטרה.

איגוד האינטרנט הישראלי ISOC-IL

נתונים ופערי מידע על חקירות וחיפושים בטלפונים חכמים וחשבונות ענן

חדירה וחיפוש במכשירים חכמים הם פרקטיקה נפוצה ברשויות החקירה:

- **למעלה מ־20,000 צווי חיפוש במחשבים – ובכלל זה בטלפונים ניידים – ניתנים מדי שנה.** ובשנת 2019 לבדה התבקשו וניתנו כ-24,000 צווי חיפוש בטלפונים ניידים, נוסף על מקרים רבים של חדירה וחיפוש בחומר מחשב על בסיס הסכמת הנחקר.
- **גם המשטרה הצבאית מבצעת חדירה וחיפוש בטלפונים בהיקפים נרחבים,** כאשר רוב החיפושים נעשו בהסכמת הנחקר וללא צו, גם כאשר מדובר במכשירים אישיים-אזרחיים ולא צבאיים.
- **בקשות לצווים לפי חוק האזנת סתר זוכות לאישור שיפוטי נרחב:** מתוך 3,692 בקשות שהוגשו ב־2020 נדחו 26 בלבד (0.7%). ב־2021 הגישה המשטרה 3,359 בקשות להאזנת סתר, שמהן התקבלו 3,350 – יותר מ־99%.

נתונים אלו מציגים על קצה המזלג את היקף התופעה וממחישים את היקף ופוטנציאל הפגיעה בזכויות וחירויות אזרח של עשרות אלפי אנשים בשנה. כפי שאנו מסבירים, מעגל הפגיעה של טכנולוגיות מתקדמות לחדירה וחיפוש בטלפונים ניידים אינו מוגבל לאדם הנחקר, נוכח העובדה שמכשירים אלו מאחסנים לרוב מידע ונתונים רגישים של צדדיים שלישיים, כגון תמונות או סרטונים המתעדים גורמים בלתי תמימים בלתי-מעורבים, כגון בני/בנות זוג וילדים או התכתבויות ומידע פנימי של ארגונים וחברות. מדובר במספר עצום של אזרחים שמושפעים מהשימוש המשטרתי בטכנולוגיות אלו.

אילו נתונים חשובים עדיין איננו יודעים?

דיון אחראי וממצה במסגרת הדין והנוהל להפעלת כלים מתקדמים לפריצה, העתקה וחיפוש במכשירים חכמים מחייב ידע על ההיקף והאופן של ביצוע חיפושים בחומר מחשב בשנים האחרונות, ובפרט בטלפונים ניידים, ועל תועלתם לאינטרס הציבורי באכיפת הדין, למשל – בכמה מקרים של חיפושים כאלה החקירה לא הובילה לכתב אישום. מטבע הדברים, נתונים אלו זמינים לרשויות האכיפה בלבד ולא נחשפו מעולם במלואם ובשיטתיות. דיון ציבורי וחקיקתי דורש מענה, בין היתר, לשאלות אלו:

הפעלת כלים טכנולוגיים למיצוי נתונים ממכשירים חכמים שנתפסו

- ? **מה היקף ההפעלה של כלים פורנזיים לחדירה וחיפוש בטלפונים חכמים, דוגמת מוצרי Cellebrite, בידי רשויות החקירה והאכיפה בישראל?** בכמה מקרים הדבר נעשה באמצעות צו שיפוטי, ובכמה על בסיס הסכמה? האם הפעלתם מוגבלת רק לעבירות חמורות או לעבירות מסוג מסוים? אם לא, כמה שכיח השימוש בכלים אלו בסוגי עבירות שונים?
- ? **האם לגופי חקירה שמפעילים כלים כאלה יש מדיניות ברורה לשימוש בהם, למשל לגבי סוג העבירות או מידת הנחיצות של הכלי?** בפרט, יש לבחון האם נקבעו כללים שונים למידע רגיש, וכמה גורמי חקירה מקבלים גישה למידע.

הפעלת כלים טכנולוגיים מסוג "הדבקה מרחוק" כלפי מכשירים חכמים

- ? **מה היקף השימוש בכלים להאזנת סתר לתקשורת בין מחשבים באמצעות "הדבקה מרחוק", דוגמת סייפן, בידי רשויות האכיפה בישראל?**

איגוד האינטרנט הישראלי ISOC-IL

- ? **מה התוקף הממוצע של צווים להאזנת סתר לתקשורת בין מחשבים, וכיצד מובטחת הסרת הגישה בסיום תקופת הצו?**
- ? **האם גופי האכיפה מיישמים טכנולוגיות נוספות של האזנת סתר מסוג זה?**
- ? **מה פוטנציאל זיהום החקירה של מערכות אלו הכרוכות בשיבוש פעילותו התקינה של המכשיר, ובפרט של מערכות אבטחת המידע שלו?**

הפעלת טכנולוגיות לחדירה, חיפוש או האזנת סתר על מכשירים חכמים

- ? **כמה מהחיפושים שבוצעו בטלפונים ניידים כללו גם מיצוי מידע מחשבונות ענן המקושרים למכשיר?** במקרים רבים הפעלת הכלים הפורנזיים למיצוי מידע מטלפונים חכמים כוללת שימוש גם ביכולת זו, אך היקף התופעה לוט בערפל.
- ? **כמה מהחיפושים במכשירים חכמים, וטלפונים ניידים בפרט, מניבים כתבי אישום והרשעות?**
- ? **באיזו מידה בתי משפט נענים לבקשות חיפוש בטלפונים ניידים?** יש להבחין בין קבלה מלאה, קבלה הכוללת קביעת תיחום נוסף לבקשה, ודחייה.
- ? **מה עולה בגורל הנתונים המחולצים ממכשירים חכמים ומחשבונות ענן לאחר החקירה?** האם הם נשמרים כחומר מודיעיני פוטנציאלי לחקירות אחרות? האם הם נמחקים במידה שתיק החקירה נסגר מחוסר אשמה? האם עקרון צמידות המטרה, המוכר לנו מדיני הגנת הפרטיות, חל גם על השימוש בחומרים שנאספים במסגרת החקירה (החשאית והגלויה)?
- ? **האם לספקיות הכלים הטכנולוגיים יש גישה למידע שמתקבל או למידע על הפעלתם ויעדיהם?** זאת בעקבות ממצאי ועדת מררי לבדיקת האזנות סתר לתקשורת בין מחשבים, לפיהם סיפקה חברת NSO נתונים לגבי "כל הדבקה שבוצעה באמצעות המערכת לאורך כל שנות פעילותה במשטרה; המועד המדויק שבו בוצעה ההדבקה; והטלפון הנייד שנדבק".

הצורך בעדכון מסגרת הדין והנוהל לחדירה וחיפוש במכשירים חכמים

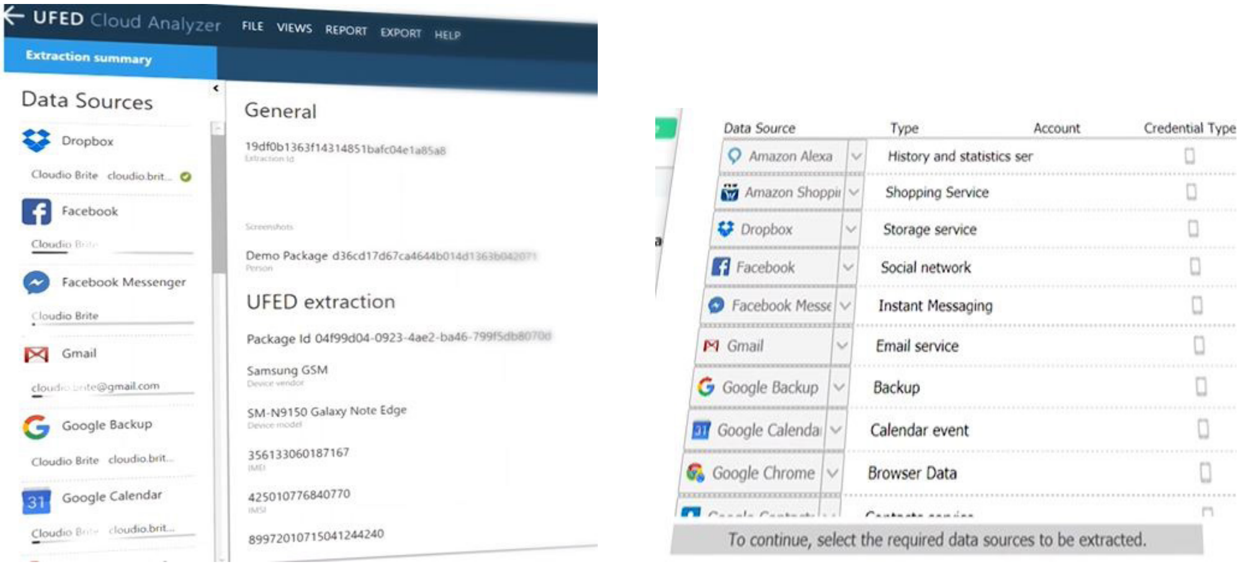
א. הבטחת הליך הוגן והגנה על זכויות אזרח מול פוטנציאל הפגיעה של חדירה וחיפוש במכשירים אישיים

המסגרת החקיקתית המיושנת של דיני החיפוש בישראל אינה מאפשרת מנגנוני פיקוח וביקורת מספקים נגד שימוש חורג או בלתי-הכרחי של רשויות האכיפה השונות בכלים טכנולוגיים רבי עוצמה לחילוץ נתונים אישיים ממכשירים חכמים ומחשבונות הענן המקושרים אליהם.

כפי שאנחנו מדגימים לאורך הדו"ח, חדירה וחיפוש בטלפון חכם פוגעים בחריפות בחירות האזרח והזכות להליך הוגן, עקב המציאות הטכנולוגית העכשווית בה הטלפון החכם הוא למעשה המחשב האישי הנפוץ ביותר בחיינו ובשל התפתחויות טכנולוגיות המרחיבות את סוגי והיקפי הנתונים שהוא אוצר. לפיכך נדרש עדכון של הדין הקיים, שיתמקד באתגרים הבאים:

- להבדיל מחיפוש במרחב הפיזי, שמוגבל לתפיסה של חומרים רלוונטיים לחקירה, טכנולוגיות לחיפוש במכשירים חכמים ומשאבי ענן המקושרים אליהם מבוססות על חילוץ המידע כולו, ללא סינון מראש לתקופה מסוימת או לסוג חומר רלוונטי בלבד.
- הטלפון החכם הוא שער לשלל נכסיו הדיגיטליים של האדם, כגון חשבונות ברשתות חברתיות, דואר אלקטרוני, מידע רפואי ופיננסי ונכסים קריפטוגרפיים, ואיסוף נתונים אלה אינו דורש צווים נפרדים או תוכנית חקירה מיוחדת.
- חיפוש בטלפונים חכמים אינו פוגע רק בזכויות בעל המכשיר הנחקר, אלא כרוך לרוב גם בפגיעה ניכרת בפרטיותם של צדדים שלישיים, למשל מידע עסקי-סודי על מקום עבודתו של בעל המכשיר, או מידע מידע אישי כגון תמונות והתכתבויות עם חברים קרובים, בני ובנות זוג, כמו גם ילדים וקטינים הנמצאים בסביבתו של בעל המכשיר.
- יכולתו של החשוד לעיין בהגשת מיצוי החקירה הפורנזית של החיפוש בטלפון החכם מוגבלת מאוד יחסית לחומרי חקירה אחרים, הן בשל תלותו בגופי האכיפה לשם אספקת חומרי חקירה והן בשל המומחיות הנדרשת להבנת התהליך של חילוץ המידע ופענוחו.

הצורך בעדכון מסגרת הדין והנוהל להפעלת אמצעים טכנולוגיים לחדירה ולחיפוש בטלפונים ניידים בוער במיוחד כיום, בעידן מחשוב הענן, שכן יכולתם של גופי האכיפה לחדור ולחפש בחשבונות ענן הנגישים מהמכשיר היא הרחבה עצומה של סמכויות החקירה וחודרנותה.



מערכת UFED Cloud Analyzer (ראו פרק ב)

ב. התמודדות עם אתגרי האמינות והמהימנות של ראיות שהופקו באמצעים בעלי מעמד פורנזי

בחינת מסגרת הדין לחדירה וחיפוש במכשירים חכמים נדרשת לא רק מטעמי הגנה על פרטיות וכבוד האדם, אלא בראש ובראשונה מטעמי הליך הוגן ואמינות הראיות המופקות באמצעות הכלים הטכנולוגיים המופעלים בעת חקירה. כמפורט במסמך, בשנים האחרונות תועדו חולשות אבטחה בכלים UFED ו־Physical Analyzer, שאפשרו לבעל המכשיר לשבש את פעילותו התקינה של תהליך חילוץ ועיבוד המידע, לרבות שינוי הדו"ח הפורנזי של הסריקה ואף את הנתונים של מכשירים אחרים השמורים במערכת, לרבות מכשירים עתידיים.

על רקע זה, נדרש עדכון מסגרת הדין והנוהל לחדירה וחיפוש במכשירים חכמים כדי להבטיח את זכות האזרח להליך הוגן, ולשמור על האינטרס הציבורי להבטחת אמינות ומהימנות הראיות המובאות בפני בית המשפט – הן ביחס לאמינות הכלים הטכנולוגיים, והן ביחס לשרשרת הראייתית והגנה מפני זיהום.

ג. מתן מענה לכך שחיפוש בטלפונים חכמים פוגע במיוחד באוכלוסיות מוחלשות

מערכת המשפט הפלילי מאופיינת בפערים בשיעורי המעצר, וסביר להניח שהחיפושים בטלפונים סלולריים כבר משקפים פערים דומים. בנוסף, חיוני להכיר במגבלות ההסכמה של מיעוטים הסובלים מאכיפת יתר כתוצאה של חוסר סימטריה משמעותי בסמכויות ובמעמד. בית המשפט העליון קבע שאי אפשר לכפות הסכמה, במפורש או בעקיפין – אולם הניסיון ופסיקות משפטיות מהעת האחרונה מלמדים כי אינטראקציה של גורמי אכיפה עם מיעוטים תרבותיים הנתונים לאכיפת יתר, מתאפיינת בתחושת איום או אסימטריה קיצונית בסמכויות ובמעמד, שעלולה לגרום לאנשים להרגיש שאין באפשרותם או בטובתם לסרב לבקשת חיפוש מצד שוטרים.

לכן, השימוש הנרחב של רשויות החקירה בישראל בטכנולוגיות לחדירה וחיפוש בטלפונים חכמים פוגע במיוחד באוכלוסיות מוחלשות או מיעוטים הנתונים לשיטור יתר בישראל, כגון יוצאי אתיופיה ולא-יהודים; ובאוכלוסיות עניות מכלל החברה הישראלית – שכל פעילותם המקוונת והנתונים והמידע האישי שהם צוברים מבוססים על הטלפון החכם, בהיעדר מחשב אישי.

ד. היעדר אסדרה בחקיקה של הסמכות לבצע חדירה למידע בענן כפעולה חוץ-טריטוריאלית

התרחבות השימוש באחסון מבוסס־ענן במכשירים חכמים מעוררת קושי משפטי בנוגע לסמכותן של רשויות האכיפה לבצע חדירה או חיפוש במידע המאוחסן מחוץ לשטחה הריבוני של המדינה. כמפורט במסמך, בשני העשורים האחרונים רווחת במדינות דמוקרטיות התפיסה כי רשויות האכיפה אינן רשאיות לחפש בנתונים או במאגרי מידע שלא בשטחן הטריטוריאלי ללא הסדר חקיקתי ייעודי.

אם כן, הפרקטיקה של חדירה לחומר מחשב האגור מחוץ לישראל ללא הסמכה מפורשת בחקיקה, על בסיס היתר של פרקליטות המדינה, אינה עולה בקנה אחד עם עקרון הטריטוריאליות ועם ההכרה של מדינות דמוקרטיות בצורך לעדכון דיני החיפושים לעידן הנוכחי, שבו כמעט כל חיפוש במכשיר חכם כרוך בגישה לנתונים שמאוחסנים מחוץ לגבולות המדינה.

איגוד האינטרנט הישראלי ISOC-IL

מתווה לפיתוח הדין והנוהל של חיפושים בחומר מחשב וטלפונים חכמים בישראל

בשונה מן התפיסה הרווחת, הזכות להליך הוגן בכל הנוגע למידע המוחזק במכשיר חכם תלויה במידה רבה ב"שופטי השטח", היושבים בערכאות השלום ובתורנויות המעצרים, ולא בפסקי דין עקרוניים של בית המשפט העליון. לתפיסתנו, הבטחת איזון בין האינטרס הציבורי בחקר האמת ואכיפת הדין לבין זכויות היסוד לפרטיות, הליך הוגן וכבוד האדם, דורשת מהמחוקק ובתי המשפט לשקול כמה עקרונות:

חובת תיעוד מוגברת של פעילות הכלים הפורנזיים לפריצה ולחיפוש במכשירים חכמים: ראוי לקבוע בחקיקה כי הכלים שרשויות האכיפה מפעילות על מכשירים חכמים יכללו פונקציות לניהול רשומות, ובייחוד יומני ביקורת (audit logs) מפורטים והקלטות מסך אוטומטיות.

חובות לגבי טיפול במידע שנאסף ממכשירים חכמים: שמירת מידע שאינו מוגדר בצו חיפוש דומה לשמירת זכותן של רשויות אכיפת החוק לבצע חיפוש בבית עד עולם, ולכן ראוי לחייב אותן למחוק כל נתון שמוצה מהמכשיר ואינו קשור למטרה של צו החיפוש תוך חודשים ספורים מיום קבלת המידע. בנוסף, ראוי לקבוע כי אם רשויות החקירה מפעילות כלים טכנולוגיים למיצוי נתונים ממכשירים חכמים ו/או מחשבונות הענן המקושרים אליהם, רק פריטי מידע שסוננו ונמצאו רלוונטיים בידי גורמי החקירה יוזנו למערכת ויישמרו על ידי הגורם החוקר, להבדיל מהנוהל הקיים להעתיק את כלל המידע הזמין מהמכשיר.

קביעת חובות שקיפות על רשויות חקירה (לא בטחוניות) המפעילות טכנולוגיות לחדירה, חיפוש והעתקה ממכשירים אישיים: נתונים ועובדות על היקפי ההפעלה של טכנולוגיות עוצמתיות בידי רשויות החקירה השונות הם תנאי חיוני לביקורת פרלמנטרית ואמון ציבורי. בפרק ג' פירטנו את סוגי הנתונים אותם ראוי לפרסם פומבית, הן לשם פיקוח ציבורי והן כתשתית חיונית עבור עורכי דין, חוקרים, וקובעי מדיניות.

אסדרת מערכת היחסים והגישה לנתונים בין רשויות החקירה לספקי טכנולוגיות פורנזיות: אסדרה עתידית חייבת לקבוע בחקיקה כללי סף להתקשרות גורמי האכיפה עם חברות פרטיות המספקות שירותי פריצה לטלפונים חכמים או "האזנה לתקשורת בין מחשבים". בבסיס כללים אלו יעמוד איסור גורף על כל אפשרות גישה של הגורם הפרטי למידע הנאסף בעזרת הכלים שסיפק, ועיקרון שלפיו המידע המופק מהכלים והמידע המתעד את הפעלתם יישמר רק במאגרים מדינתיים.

הגבלת כוחה של "הסכמה" לחיפוש בטלפונים ניידים ובמשאבי ענן בהיעדר צו שיפוטי: "הסכמה" להפעלת כלים טכנולוגים רבי עצמה לחדירה והעתקה של נתוני טלפוניים חכמים אישיים, ניתנת לא אחת בסיטואציה של פערי כוחות וסמכות בין חוקר לנחקר/חשוד שמנסה לרצות אותו, ומעוררת חששות עקרוניים ומעשיים נוספים: (א) באין צו חיפוש המגדיר את תכליות החיפוש ומטרותיו, החוקר איננו מוגבל לנושאי החקירה, והפגיעה בפרטיות איננה מידתית ואיננה מפוקחת; (ב) לא ניתן להניח שבעל המכשיר מודע להיקף ואינטימיות המידע שרשויות החקירה מסוגלות להפיק ממכשירו, ולכן "הסכמה" בסיטואציה של פערי מידע כאלו אינה בעלת משמעות; (ג) כאשר החדירה והחיפוש למכשיר מתבצעים "בשטח" או "בזמן אמת", היכולת להבטיח את אמינות מיצוי הנתונים או לשלול זיהום (מכוון או רשלני) של הנתונים היא מוגבלת מאוד. על כן, יש לבחון מחדש בישראל את גבולות הלגיטימיות של הפעלת הפעלת כלים טכנולוגים אלו על בסיס הסכמה בלבד.

איגוד האינטרנט הישראלי
ISOC-IL

תוכן עניינים

מבוא 14

א. טלפונים "חכמים" כמקור עתק של מידע אישי ורגיש: סקירה טכנולוגית 16

ב. כלים פורנזיים של רשויות החקירה בישראל להפקת ראיות ממכשירים חכמים 21

ב.1 חדירה, העתקה וחיפוש במכשירים חכמים באמצעות תפיסה פיזית שלהם 21

ב.2 חדירה, חיפוש והאזנה למכשירים חכמים באופן סמוי (רוגלות) 27

ב.3 טכנולוגיות לניתוח ולהצלבה של מידע העתק שניתן לחלץ מחדירה לטלפון חכם 31

ב.4 חולשות, מהימנות ואמינות של טכנולוגיות חדירה למכשירים חכמים 32

ג. נתונים על חדירה וחיפוש בטלפונים חכמים וחשבונות ענן בישראל: תמונת מצב 34

ג.1 משטרת ישראל ורשויות נוספות משתמשות בטכנולוגיות פריצה וחיפוש מתקדמות 34

ג.2 טכנולוגיות פורנזיות לפריצה ולחיפוש בטלפונים חכמים מופעלות בהיקף עצום 34

ג.3 אילו נתונים חשובים עדיין איננו יודעים 35

ד. מסגרת הדין ונוהלי משטרת ישראל לפריצה ולחיפוש במכשירים חכמים 38

ד.1 מסגרת הדין בתהליך החקירה הסמויה: האזנת סתר לשיחות ותקשורת מחשבים 38

ד.2 תהליך החקירה הגלויה: תפיסה, חיפוש וחדירה למכשירים וחומר מחשב 41

ד.2.א שלב ההרשאה: הנפקת צו חדירה למחשב או קבלת הסכמה 43

ד.2.ב שלב התפיסה הפיזית של המכשיר הנחפש 46

ד.2.ג שלב הפריצה והעתקת נתונים מהמכשיר התפוס 49

ד.2.ד שלב הניתוח והעיון באמצעות טכנולוגיה פורנזית 49

ד.3 שלב ההליך הפלילי: חסיונות והעברת חומרי חקירה וראיות לתביעה ולהגנה 51

ד.4 שמירת ראיות וחומרי חקירה על ידי רשויות החקירה ושימוש עתידי בהם 54

ה. הצורך בעדכון מסגרת הדין והנוהל לפריצה ולחיפוש במכשירים חכמים ובמשאבי ענן 55

ה.1 התפתחויות טכנולוגיות המעצימות את היקף ורגישות המידע שניתן לחלץ מטלפונים 55

ה.2 שאלת אמינות ומהימנות ראיות שהופקו באמצעים בעלי מעמד פורנזי 56

ה.3 חיפוש בחומרי ענן ושרתים מרוחקים כפעולה חוץ-טריטוריאלית 57

ה.4 הגידול בהיקף החיפושים בטלפונים חכמים פוגעני במיוחד בקרב אוכלוסיות מוחלשות 59

ו. במקום סיכום: מתווה לפיתוח האסדרה של חיפוש במכשירים חכמים אישיים 60

הגבלת האפשרות לחיפוש בטלפונים ניידים ובמשאבי ענן על בסיס הסכמה וללא צו שיפוטי 60

חובת תיעוד (AUDIT LOGS) של פעילות הכלים הפורנזיים לחדירה ולחיפוש במכשירים חכמים ... 61

הסדרת היכולת של חוקרים להשתמש במידע מחוץ למטרת החיפוש הספציפי: צמידות מטרה? ... 62

חובות לגבי טיפול במידע שנאסף ממכשירים חכמים: חתימה ומחיקה 62

חובות שקיפות על רשויות החקירה 63

אסדרת מערכת היחסים והגישה לנתונים בין רשויות החקירה לספקי טכנולוגיות פורנזיות דיגיטליות . 64

הדרכות והשתלמויות לשופטים על טכנולוגיות פורנזיות ויכולותיהן 64

מבוא

חוק המחשבים נחקק לפני למעלה מ-25 שנים. עידנים שלמים בתחום המחשבים חלפו מאז. המחשבים שעמדו נגד עיניו של המחוקק אז והיום אינם אותם מחשבים, גם אם הם מתוארים באמצעות אותה מילה... בשנים שחלפו השימושים במחשבים הפכו מגוונים יותר, כי היקף הזיכרון של מחשבים הוא נרחב לאין שיעור, וכי במקרים רבים צווי חדירה אף חורגים מגבולותיו הפיזיים של המחשב (למשל, אל קובצי "ענן"). מורכבותו הרבה של הנושא, שבגינה לא מתאפשרת במקרה זה פעולה של 'קריאה לתוך החוק'... מדגישה את הצורך לעדכן את החוק למחשבים של ימינו אנו ומציאות השימוש בהם, ויפה שעה אחת קודם.

בית המשפט העליון, ינואר 2022[1]

רשויות אכיפת החוק משתמשות בטכנולוגיה רבת עוצמה להפקת מידע מטלפונים ניידים ומכשירי קצה חכמים[2] שנתפסו במהלך החקירה. הכלים הטכנולוגים שמפעילות הרשויות בישראל לצורך חקירה והפקת ראיות מאפשרים לפרוץ, להעתיק ולנתח את כלל הנתונים שאליהם ניתן לגשת ממכשירים חכמים אישיים: דואר אלקטרוני, מסרונים, תמונות, סרטונים, מיקומים, מידע מאפליקציות (לרבות חשבונות ענן) ועוד. מרכזיותו של הטלפון החכם בחיינו, יחד עם התפתחויות טכנולוגיות המגבירות את סוג והיקף הנתונים שהוא אוצר, הופכים את החדירה והחיפוש בו על ידי רשויות המדינה לפגיעה כבדה במיוחד בזכויות החוקתיות להליך הוגן, כבוד האדם והזכות לפרטיות.[3]

עם זאת, חדירה וחיפוש משטרתי בטלפונים ניידים מתבצעים כעניין שבשגרה עבור רשויות אכיפת החוק בישראל. בשנים האחרונות משטרת ישראל מרחיבה את השימוש בכלים טכנולוגיים מתקדמים לקצירה ולעיבוד של מידע ממכשירים ניידים (באמצעות תפיסתם ועריכת חיפוש או באמצעות פריצה נסתרת מרחוק אליהם), שבעבר היה נמנע בגין שיקולי עלות. בממוצע, עשרות צווי חיפוש במכשירים ניידים המאושרים על ידי שופטים בבתי משפט השלום ניתנים מדי יום, זאת בנוסף למקרים רבים שבהם חיפושים אלה מתקיימים על בסיס הסכמת הנחקר וללא צו שיפוטי.[4]

1 דנ"פ 1062/21 אוריך נ' מדינת ישראל (11.1.2022), פס' 21 לחוות דעתה של השופטת ברק-ארז.

2 חקיקת המחשבים והחיפושים בישראל אינה מבחינה בין חיפוש במחשב שולחני לחיפוש בטלפון נייד או בטלוויזיה חכמה, אלא חלה באופן אחיד על כל חדירה או חיפוש ב"מחשב". על רקע זה, הסקירה הטכנולוגית בפרק זה מתמקדת בטלפונים ניידים, שהם למעשה ה"מחשבים" והמצלמות הנפוצים בישראל, והמונח "מכשירים חכמים" מתייחס לקבוצה רחבה של מכשירים בעלי יכולת עיבוד נתונים וגישה לאינטרנט, כגון טאבלטים, שעונים חכמים, עוזרים ביתיים כגון Alexa או Google Home ועוד.

3 "השימוש הרווח במכשיר הטלפון הנייד כאמצעי גישה לאינטרנט (מרשתת) פותח צוהר נוסף לעיון בנסתרות ליבו של בעל המכשיר, בעמדותיו הפוליטיות, בתחביביו ובתוכניותיו לעתיד... לא אחת מכשירי הטלפון הניידים כוללים תיעוד מדויק של המקומות שבהם שהה בעל המכשיר, התכתבויות אישיות ואינטימיות, ומידע על חבריו ועל טיב הקשר עימם, לצד מידע עסקי רגיש... אולם לפעולה זו מחיר כבד: היא פוגעת באופן חמור ביותר בפרטיותו של הנחקר... מעבר לפגיעה העצמאית בפרטיותם של הנחקר ושל מכריו, הנחקר אף עלול לחשוש כי חוקר המשטרה יעשה שימוש במידע רגיש המתגלה בהודעותיו בכדי לגרום לו לשתף פעולה בחקירה". בש"פ 7917/19 אוריך נ' מדינת ישראל (25.12.2019), פס' 19 לפסק דינו של כבוד השופט אלרון.

4 בש"פ 5105/20 שמעון נ' מדינת ישראל, פסקה 24 לפסק דינו של השופט אלרון (25.5.2021) ("כ-24,000 צווי חיפוש במכשירי טלפון נייד התבקשו – וניתנו – בשנת 2019").

איגוד האינטרנט הישראלי ISOC-IL

למרות תפוצתם הרחבה ופרק הזמן הארוך שרשויות החקירה בישראל מפעילות בו טכנולוגיות פורנזיות מתקדמות לחדירה, להעתקה ולחיפוש בטלפונים חכמים ובחשבונות הענן המקושרים אליהם, אין כמעט שקיפות ציבורית בנוגע לתדירות או לאופי המקרים שבהם רשויות אכיפת החוק משתמשות בכלים כאלה, למעט כאשר זו מופעלת נגד חשודים בעלי נראות ציבורית גבוהה. כמו כן, בכל הנוגע לחדירה ולחיפוש בחומר מחשב, ובטלפונים חכמים בפרט, לא מתקיים דיווח מספק על יכולותיהם ועל היקפי השימוש בכלים אלה, ולרוב הם זוכים לחיסיון, גם כאשר מוגש כתב האישום.[5]

באופן כללי יותר, החשיבות של דיון ציבורי ורפורמה משפטית בכל הנוגע לחדירה ולחיפושים של רשויות חקירה בטלפונים ניידים ובחשבונות ענן מתחדדת עוד יותר נוכח היוזמה העכשווית של משרד המשפטים לחיזוק זכויות חשודים ונחקרים בישראל,[6] ומול קריאתו הטרייה של בית המשפט העליון לרפורמה חקיקתית של דיני החיפושים והראיות בעידן מחשוב הענן.[7]

על כן, מטרתו של מסמך זה היא לספק למעצבי מדיניות, לשופטים ולציבור הרחב מקור מהימן של נתונים ועובדות בשני תחומים: (א) אופן הפעולה והיכולות של טכנולוגיות הפריצה והחיפוש המופעלות כיום בישראל; (ב) מיפוי תיאורי של מסגרת הדין ונוהלי משטרת ישראל להפעלת טכנולוגיות מתקדמות אלו, כמערכת לביצוע איזונים בין האינטרס הציבורי באכיפה אקטיבית לבין זכויות היסוד להליך הוגן ולפרטיות של האזרחים והגופים שכלים אלו מופעלים עליהם.

5 ראו להלן פרק ד.

6 דברי שר המשפטים גדעון סער בדיון שהתקיים ביום 2.2.2022 בוועדת חוקה חוק ומשפט (קישור); הצעת חוק-יסוד: זכויות בהליך הפלילי (קישור); דברי ההסבר להצעת חוק לתיקון פקודת הראיות (מס' 18), התשפ"ב-2021 (קישור).

7 דנ"פ אוריך, לעיל ה"ש 1.

א

טלפונים "חכמים" כמקור עתק של מידע אישי ורגיש: סקירה טכנולוגית

מחשבים אישיים, מכשירים חכמים אחרים וטלפונים ניידים בפרט, אוצרים בחובם מידע בלתי נדלה על משתמשיהם וסביבתם. מטבע הדברים, מידע זה כולל לרוב גם מידע אישי רב ולעיתים מידע אינטימי ממש.

חקיקת המחשבים והחיפושים בישראל אינה מבחינה בין חיפוש במחשב שולחני לחיפוש בטלפון נייד או בטלוויזיה חכמה, אלא חלה באופן אחיד על כל חדירה או חיפוש ב"מחשב".[8] על רקע זה, הסקירה הטכנולוגית בפרק זה מתמקדת בטלפונים ניידים, שהם למעשה ה"מחשבים" והמצלמות הנפוצים בישראל,[9] והמונח "מכשירים חכמים" מתייחס לקבוצה רחבה של מכשירים בעלי יכולת עיבוד נתונים וגישה לאינטרנט, כגון טאבלטים, שעונים חכמים, עזרים ביתיים כגון Alexa או Google Home ועוד.

זאת, בהינתן שטלפונים ניידים מספקים שילוב נוח בין אמצעי תקשורת, מצלמה, פנקס, יומן, מכשיר ניווט, דפדפן, ארנק חכם ועוד. טכנולוגיות פורנזיקה דיגיטלית לחיפוש בטלפונים חכמים מאפשרות לרשויות אכיפת החוק גישה לכל הנתונים הללו ואחרים, בין אם אנשים שומרים את המידע הזה בטלפון במודע ובין אם המידע נוצר ונשמר תוך כדי פעילותם היומיומית. בכלל זה, אנשים שומרים בטלפון החכם לא רק כמויות עצומות של מידע, אלא גם תיעוד גאוגרפי מלא של תנועותיהם, לעיתים מבלי לדעת. כפועל יוצא, טלפונים ניידים ומכשירים חכמים מתעדים כמויות עצומות של מידע שמוגדר על ידי גורמי חקירה כמכרה זהב דיגיטלי.

כלים פורנזיים לחדירה ולחיקור של טלפונים ומכשירים חכמים אחרים מספקים גישה להיקפים עצומים של נתונים שאומנם נצברו אגב השימוש, אבל הם חושפניים באופן בלתי צפוי. כמפורט בהרחבה בפרק הבא, השימוש העיקרי של הכלים הוא איסוף וארגון יומני שיחות, רשימות אנשי קשר, מסרונים ותמונות. עם זאת, מכשירים חכמים אוצרים מידע נוסף שאותו ניתן לחלץ באמצעות הטכנולוגיות הפורנזיות הקיימות, כגון:

נתונים מתוכנות ייעודיות ויישומים (אפליקציות): מרבית התוכנות הייעודיות והאפליקציות בטלפונים חכמים יוצרות ושומרות נתוני משתמשים, כגון היסטוריית גלישה, נתונים ומדדים רפואיים, מידע פיננסי והיסטוריית תשלומים המתבצעים באמצעות הטלפון הנייד, תכתובות, שיחות באפליקציות היכרויות ועוד. הטכנולוגיות הפורנזיות שרשויות החקירה בישראל מפעילות יכולות להעתיק ולמשוך נתונים מהתוכנות והאפליקציות הפופולריות ביותר, והן מתעדכנות בקביעות לתמיכה במגוון אפליקציות חדשות.

נכון לשנת 2020 דווח כי הכלים של חברת Cellebrite, למשל, יכולים לחלץ ולנתח נתונים מלפחות 181 אפליקציות אנדרואיד, ולפחות 148 אפליקציות iOS: כלים כמו גוגל מפות, גוגל תמונות ו-Gmail; אפליקציות היכרויות כמו טינדר, גרינדר

8 סעיף 1 לחוק המחשבים, התשנ"ה-1995 (להלן: "חוק המחשבים), מגדיר מחשב כך: "מכשיר הפועל באמצעות תוכנה לביצוע עיבוד אריתמטי או לוגי של נתונים וציודו ההיקפי, לרבות מערכת מחשבים, אך למעט מחשב עזר (מחשב המסוגל לבצע פעולות חיפוש אריתמטיות בלבד ופעולות הכרוכות בביצוע פעולות כאמור)".

9 על פי נתוני הלמ"ס, נכון לשנת 2020, ל-88% מהאוכלוסייה בישראל היה טלפון חכם, ונכון לשנת 2021, רק 70% מהציבור הישראלי עשה שימוש במחשב אישי ול-17.5% ממשקי הבית אין מחשב אישי כלל. על פי הערכות משנת 2017, כ-85% מכלל התמונות בעולם צולמו בטלפונים חכמים, ומספר התמונות שצולמו מדי שנה בעולם הוכפל מ-660 מיליארד בשנת 2013 ל-1.2 טריליון בשנת 2017. ראו: Felix Richter, "Smartphones Cause Photography Boom" (31.8.2017).

ו-OkCupid; אפליקציית Nike + Run; אפליקציות מדיה חברתית, כמו פייסבוק, אינסטגרם, טוויטר וסנאפצ׳ט; דפדפנים כמו כרום ופיירפוקס; ואפילו אפליקציות מסרים מיידיים מוצפנות, כמו סיגנל וטלגרם.[10]

נתונים ש"נמחקו": כלי זיהוי פלילי למחשבים ומכשירים ניידים יכולים לעיתים לגשת לנתונים ש"נמחקו" מהמכשיר.[11] בדומה לאופן שבו קבצים שנמחקים במחשב מועברים בדרך כלל ל"סל המִחזור", כך גם קובץ שנמחק מהטלפון על ידי המשתמש ניתן לעיתים לשחזור ואחזוק. יתרה מכך, מחיקת הקובץ מהטלפון עצמו לא תמיד מוחקת אותו מגיבוי הענן של המשתמש, או ממגוון המקומות האחרים שבהם הוא נשמר או מגובה.

נתונים על אודות המידע (metadata): טלפונים מתעדים כמויות עצומות של נתונים הנוגעים לאופן שבו אנשים מתקשרים עם המכשיר – מידע שמוגדר על ידי יצרנים של כלים פורנזיים כ"מכרה זהב דיגיטלי".[12] כלי זיהוי פלילי למכשירים ניידים יכולים לחלץ רשומות שמראות מתי אפליקציות הותקנו, היו בשימוש ונמחקו, כמו גם באיזו תדירות השתמשו בהן. נתונים אחרים מגלים מתי המכשיר הופעל או כובה, מתי המשתמשת קראה הודעה, האם ומתי בוצעה התחברות להתקני Bluetooth / Wi-Fi ופרטיהם, מילים שנוספו למילון המשתמשת (לרבות סיסמאות שלעיתים נוספות למילון המקומי), תוכן של התראות או חיפושים בשירות החיפוש Spotlight המובנה במכשירי אייפון, שמציג תוצאות מהמכשיר ומהאינטרנט. טלפונים עשויים לאחסן צילומי מסך של אפליקציות פתוחות המוצגות למשתמשים כאשר הם עוברים בין יישומים פתוחים.[13] כל הנתונים הללו נשמרים "מאחורי הקלעים" כדי לשפר את ביצועי הטלפון או כדי לשרת את צורכי היצרנים, אך הם משאירים עקבות מפורטים להפליא שטכנולוגיות החקירה יכולות לנתח בעתיד.[14]

סיסמאות ופרטי התחברות לשירותים ציבוריים ומסחריים: במרבית המחשבים והמכשירים הניידים והדפדפנים המותקנים עליהם נשמרות סיסמאות המשתמש לאינספור שירותים ציבוריים ומסחריים, כך שטכנולוגיות פורנזיות לחדירה וחיפוש בטלפונים חכמים עשויות לחלץ את הסיסמאות ולנצלן עבור חילוץ מידע מאותם שירותים או משירותים אחרים שבהם נעשה שימוש באותן סיסמאות.[15]

על רקע זה, גם ערכאות המשפט בישראל החלו להכיר בכך שההתקדמות הטכנולוגית ביכולותיהם של טלפונים ניידים, יחד עם תפקידם ההולך וגובר בביצוע פעולות יום-יומיות, הופכת אותם למקור של מידע אישי בהיקפים חסרי תקדים.[16] לא רק תמונות, הודעות דואר אלקטרוני, יומן אישי, מידע רפואי, היסטוריית גלישה באינטרנט וכיו"ב, אלא גם מידע פרטי בעל רגישות גבוהה שבעל המכשיר לעיתים אינו מודע אליו כלל, כגון מידע הנשמר באמצעות האפליקציות או בשרתיהן ומידע הנאגר על ידי מוצרי האינטרנט של החפצים שאליהם המכשיר מקושר (כגון עוזרים קוליים, שעוני כושר, שירותי בית חכם וכו').[17]

---

10 Koepke et al., Upturn Report: Mass Exctraction (2020) (קישור) (להלן: Upturn Report).
11 Upturn Report, שם, בעמ' 21; Cellebrite UFED product overview (קישור).
12 Mati Goldberg, "How a Suspect's Pattern-of-life Analysis is Enhanced with Data" (13.6.2019).
13 Upturn Report, לעיל ה"ש 10, בעמ' 22; Cellebrite, "UFED, UFED Physical Analyzer, UFED Logical Analyzer, & Cellebrite Reader v7.28", Release Notes (2020).
14 Upturn Report, שם, בעמ' 22.
15 להרחבה ראו להלן פרק ב.
16 ע"פ 8627/14 דביר נ' מדינת ישראל, פס' 7 (2015).
17 ראו למשל: בש"פ 6071/17 מדינת ישראל נ' פישר, פס' 10 ("**מדובר בחומר רב שדרכו ניתן ללמוד גם על 'סיפור חייו' של המשתמש... 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...").

איגוד האינטרנט הישראלי ISOC-IL

המשמעות המשפטית של הגידול החד בהיקף ובאינטימיות המידע שניתן להפיק מטלפונים חכמים, כפי שציין בית המשפט העליון בשנים האחרונות,[18] היא הצורך להתמודד עם הפגיעה חסרת התקדים של חיפוש משטרתי כלפי מי שמופעלות טכנולוגיות חדירה וחיפוש בנתונים הזמינים ממכשיר הטלפון הנייד שלו:

- בעוד שהחיפוש בביתו של אדם מוגבל באופן פיזי לתפיסה וחקירה בחומרים הרלוונטיים לחקירה בלבד, הטכנולוגיות הקיימות לחיפוש במכשיר הטלפון הנייד החכם שברשותו חושפות מידע עתק באשר למעשיו ומחשבותיו על פני תקופה ממושכת, המספרת לא רק על תחומי העניין של המשתמש או פעולות שביצע אלא גם על הנעשה במוחו, וכל זאת ללא יכולת סינון מראש בטרם התפיסה באופן המאפשר חשיפה ועיון בחומרים נרחבים הפורצים, באופן בוטה, את גבולות החקירה המבוצעת.

- שפע המידע האישי והחושפני הנאגר במכשירו של המשתמש, הנוצר מעצם השימוש התכוף בטלפון, ייתכן שאף מבלי שהאדם מודע לכך או שאף אינו בעל האפשרות הממשית להפסיק את איסוף הנתונים עליו בעת השימוש במכשיר, מביא לחשיפת פרטי אישיות, פנטזיות כמוסות וקווי מחשבה החורגים משליטתו של הנחקר כאדם באיסוף המידע, באופן העשוי לפגוע בכבודו.

- טלפונים ניידים מהווים כיום גם מפתח גישה לשלל נכסיו הדיגיטליים של האדם: חשבונות ברשתות חברתיות, דואר אלקטרוני, מידע רפואי, חשבונות בנק, מטבעות קריפטוגרפיים, אחסון קבצים מרוחק ועוד מבלי להזדקק לצווים נפרדים או לקביעת תוכנית חקירה מיוחדת עבור איסוף נתונים אלה, ובכך לחרוג מהגדרת החקירה ובמקרים רבים אף לחרוג ממטרתה.

- החיפוש במחשב ובמכשיר הטלפון חוצה אף מעבר לפגיעה בזכותו האישית לפרטיות של בעליו או של המחזיק בו, וכרוך לרוב גם בפגיעה ניכרת בפרטיותם של צדדים שלישיים, למשל מידע עסקי-סודי על מקום עבודתו של בעל המכשיר, מידע אישי כגון תמונות והתכתבויות עם חברים קרובים, בני ובנות זוג, כמו גם ילדים וקטינים ממשפחתו של בעל המכשיר.

- יכולת העיון של החשוד בהגשת מיצוי החקירה הפורנזית הנעשית בטלפון החכם מוגבלת באופן משמעותי מיכולתו לעיין בחומרי חקירה אחרים. זאת, הן נוכח תלות החשוד באספקת חומרי החקירה המוגשים לו על ידי גופי האכיפה, כאשר לרוב מדובר בתמצית בלבד, והן בשל המומחיות המקצועית הנדרשת לשם הבנת תהליך חילוץ המידע והבנתו.

18 ראו למשל עניין פישר, שם; עניין שמעון, לעיל ה"ש 4, בפס' 2 לפסק דינה של השופטת ברון. עם זאת, ראוי להדגיש כי קריאתו של בית המשפט העליון לחיזוק ההגנה מפני הפולשנות והחודרנות של חדירה וחיפוש במכשירים חכמים מכוונת לגופי האכיפה (משטרה, רשויות המס וכו'), להבדיל מגופי הביטחון כגון שב"כ או מוסד.

איגוד האינטרנט הישראלי ISOC-IL

התפתחות טכנולוגית נוספת המחייבת עדכון של הדין וההלכה לגבי חיפושים במחשב ובחומר מחשב מכוח פקודת החיפוש,[19] היא המעבר הנרחב למחשוב ענן, המעצים את היקף המידע הנתונים האישיים שאליהם ניתן לגשת באמצעות חיפוש בטלפון נייד.

המונח "מחשוב ענן" (Cloud Computing) מתאר מודל לשירותי תקשוב (ICT) מבוססי רשת מחשבים, המאפשר גישה למאגר משותף של משאבי מחשוב המצויים בשרתים מרוחקים, כגון אחסון מרוחק של קבצים ונתונים או יישומים ותוכנות שמשתמשי הענן יכולים להפעיל ללא צורך בהתקנתם על מכשירי הקצה (SaaS – Software as a Service).

היישום המוכר והנפוץ של מחשוב ענן הוא אחסון קבצים ומידע באופן מרוחק, כדוגמת השירותים DROPBOX, גוגל דרייב ואחרים, להבדיל מהמודל המסורתי של מחשבים ומכשירים חכמים שבו הקבצים והמידע שהמשתמש יוצר או "מוריד" מאוחסנים על גבי מכשירי הקצה שברשותו (מחשבים וטלפונים חכמים של המשתמש הרגיל, ושרתים מקומיים בארגונים). יישום נפוץ נוסף של טכנולוגיית מחשוב ענן הוא בתחום התוכנה והעיבוד, כאשר ניתן להשתמש ביישומים ולבצע פעולות עיבוד מידע באמצעות יישומים המופעלים על גבי שרתים מרוחקים, שאינם בבעלותו של משתמש הקצה. באופן זה, משתמשי קצה יכולים להפעיל תוכנות מורכבות באמצעות מכשירים "רזים" או "חלשים" אשר אינם נדרשים לכוח עיבוד או אחסון משמעותיים. כלומר, מחשבים רבי עוצמה בכל רחבי העולם הם שמבצעים את פעולות העיבוד והאחסון, ולא מכשירי הקצה של המשתמשים.

כך, מחשוב ענן משנה באופן יסודי את פרדיגמת טכנולוגיות המחשוב והמידע, מסביבת חישוב אישית/ארגונית לסביבת חישוב מבוזרת, כאשר רשת האינטרנט מספקת לרוב את עמוד השדרה הנדרש כדי לספק את שירותי הענן. מחשוב הענן צובר חשיבות במהירות, כפי שמעידים היקפי הפריסה והצמיחה של פלטפורמות ענן, כגון Azure של חברת מייקרוסופט, AWS של חברת אמזון ו-Google Cloud Platform, שהם ספקי שירותי ענן הגדולים ביותר, המשרתים מספר עצום של משתמשים פרטיים, ארגונים וגופי ממשל.[20]

המשמעות העיקרית של מהפכת מחשוב הענן בנוגע לחיפושים במחשבים ובמכשירים חכמים היא היכולת לגשת במחי "לחיצת כפתור" להיקף אדיר של נתונים אישיים של בעל המכשיר (וצדדים שלישיים), גם אם הם לא נוצרו במכשיר בו נערך החיפוש או נשמרו על גביו. בעידן מחשוב הענן הנוכחי, נתונים שנוצרו במכשיר אחר עשויים להיות שמורים או זמינים לצפייה בטלפון, ונתונים מהטלפון עשויים להיות מגובים בענן – כאשר ניתן לגשת בפשטות לנתונים ומשאבי ענן נוספים דרך רשת האינטרנט באמצעות אימות המורשים לגישה.

כלי החקירה הפורנזיים מביאים בחשבון את כל האפשרויות, וספקים רבים מציעים תכנות או מוצרים ייעודיים לחילוץ גיבויים משירותי ענן ופרטי חשבון אחרים, כמפורט בהרחבה בפרק הבא.

19 פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 (להלן: פקודת החיפוש).
20 דוגמה ליישום של ארכיטקטורת מחשב ענן על ידי גופי ממשל בישראל היא פרויקט "נימבוס" (קישור).

כפי שציין לאחרונה בית המשפט העליון, שינויים מרחיקי לכת אלו באשר להיקף ולאופן שבו מופקים ונשמרים "חומרי מחשב" הכוללים פרטים אישיים ואינטימיים על מחזיקיהם של מכשירים חכמים מחייבים עדכון של המסגרת המשפטית לאסדרת החיפוש והחדירה אליהם:[21]

> "למרבה הצער החקיקה הקיימת בכל הנוגע לחיפוש במחשבים נשרכת אחרי המציאות הטכנולוגית, המתפתחת בקצב מהיר מאוד... נוכח קיומן של טכנולוגיות שבאו אל חיינו בשנים האחרונות ושינו ללא היכר את גישתנו למידע מקוון. אם בעבר היה המידע המקוון נשמר על כוננים פיזיים שהיו מצויים בהישג ידו של בעל המידע, כיום טכנולוגיית ה"ענן" מאפשרת שמירת מידע על שרתים מרוחקים (לרבות כאלו הממוקמים מחוץ לגבולות ישראל), והגישה למידע זה אפשרית ממגוון מקורות, ואף ממספר מחשבים בו-זמנית."

עם זאת, בעוד שבתי המשפט מכירים בכך שחדירה וחיפוש בטלפונים חכמים מאפשרת לרשויות החקירה גישה להיקף חסר תקדים של מידע אישי ורגיש, המסגרת החקיקתית המיושנת של דיני החיפוש בישראל אינה מספקת פיקוח וביקורת מספקים כנגד שימוש מופרז, לא-מידתי או לא-מפוקח דיו בכלים טכנולוגיים רבי עוצמה לפריצה ולחיפוש במכשירים חכמים ובחשבונות הענן המקושרים אליהם, כמפורט להלן בפרקים ה–ו.

21 דנ"פ אוריך, לעיל ה"ש 1, בפס' 64 לפסק דינה של הנשיאה חיות ובפס' 7 לפסק דינו של השופט סולברג.

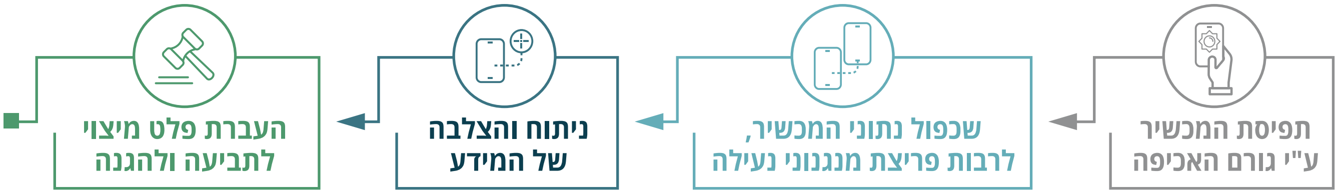
ב כלים פורנזיים של רשויות החקירה בישראל להפקת ראיות ממכשירים חכמים

ב.1 חדירה, העתקה וחיפוש במכשירים חכמים באמצעות תפיסה פיזית שלהם

חלק זה של הסקירה עוסק בטכנולוגיות לחדירה ולחילוץ נתונים לאחר תפיסה פיזית של המכשיר הנייד, להבדיל מחדירה מרחוק למכשיר הנעשית ללא ידיעת בעליו, שבה עוסק תת-הפרק הבא.

ההליך הפורנזי הדיגיטלי, שבמסגרתו משתמשים גופי החקירה בכלים פורנזיים שונים, מאפשר להפיק באופן אוטומטי את מסת המידע האדירה המצויה במכשיר הנייד, לרבות המידע הגלוי והידוע למשתמש הקצה, כגון תכתובות ומדיה, כמו גם מידע שאינו גלוי בהכרח למשתמש ואשר נשמר באופן אוטומטי על גבי המכשיר או בחשבונות ענן המקושרים אליו (דוגמת היסטוריית המיקומים המדויקת שלו, מועדי הפעלה וכיבוי, הזמנים שבהם המכשיר היה מחובר להתקנים חיצוניים ועוד).[22]

תהליך מיצוי נתונים וראיות ממכשירים חכמים כגון טלפונים ניידים במסגרת תהליך החקירה הגלויה נעשה בארבעה שלבים עיקריים:



לאחר תפיסת המכשיר, חיפוש וחילוץ הנתונים ממנו יכולים להיעשות בכמה דרגות טכנולוגיות:

22 Upturn Report, לעיל ה"ש 10.

לפי נוהלי משטרת ישראל, חיפוש בחומר מחשב (לרבות טלפונים חכמים) יתבצע באמצעות שכפול מלא של הנתונים השמורים על גבי החומרה של המכשיר (physical extraction), כך שפעולות החדירה והחיפוש הפורנזיות נעשות לאחר מכן כלפי הנתונים המשוכפלים, אם כי נוהלי משטרת ישראל מאפשרים "דפדוף" בזמן אמת על ידי כל שוטר, גם אם אין לו מיומנות והכשרה ייעודית לחיפושים בחומרי מחשב.[23]

טכנולוגיות פורנזיות להפקת ראיות ממכשירים ניידים מאפשרות את מיצוי הנתונים בכל הרמות, תוך התמודדות עם תכונות האבטחה וההצפנה של מרבית הטלפונים הניידים. יצרני טלפונים כמו אפל, סמסונג, גוגל ואחרים משלבים במכשירים אמצעי אבטחה מתוחכמים שנועדו להגן על פרטי המשתמשים במקרה של אובדן או גנבה. היצרנים מפתחים שיטות שמאזנות בין נוחות השימוש לבין אבטחה ופרטיות, אולם האיזון הזה עלול לגרום לפגמים בתכנון, לבאגים בתוכנה או לפרצות אבטחה אחרות שטכנולוגיות פורנזיות לפריצה ולחיפוש במכשירים חכמים יכולות לנצל. לכן, כמתואר בהמשך פרק זה, הכלים הטכנולוגיים כדוגמת אלו שמספקת חברת Cellebrite מסוגלים במקרים רבים לפרוץ או לשבש את אמצעי האבטחה המובנים בטלפונים ולחלץ נתוני משתמשים, לרבות היסטוריית שיחות, מיקומים, אנשי קשר, מסרונים, תמונות, סרטונים ועוד.

מבחינה טכנית, הכלים הפורנזיים להפקת ראיות ממכשירים ניידים באמצעות גישה פיזית אליהם משלבים לרוב תוכנה וציוד היקפי (כבלים, אמצעי אחסון חיצוני וכו'), המאפשרים לפרוץ את מנגנון הנעילה או ההצפנה של המכשיר, לפרוץ את הגנות מערכת ההפעלה ולייצר העתק מלא של המידע הזמין בו.

תמונה 1: מערכת UEFD מתוצרת חברת סלברייט המשמשת לפריצה והעתקה של נתונים מטלפונים חכמים שנתפסו על ידי גורמי אכיפה[24]

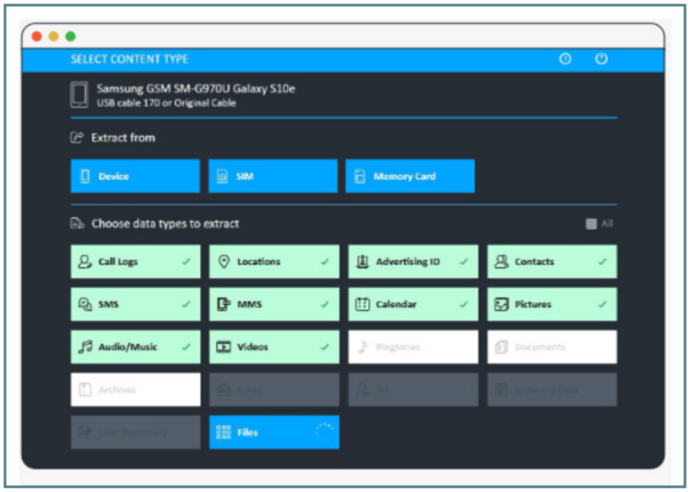
מידע פומבי על אודות פעילות הרכש של רשויות הממשל השונות חושף כי בשנים האחרונות נעשה שימוש בכלים של חברת Cellebrite לחדירה ומיצוי נתונים בקרב שורה ארוכה של רשויות בישראל. מסמך רשמי של משטרת ישראל מיום 5.7.2021 מלמד כי Cellebrite מספקת למשטרת ישראל מגוון שירותים בתחום "מיצוי מידע פורנזי ואנלאיטיקה [כך במקור] ממרבית סוגי המכשירים הדיגיטליים בהם אגור מידע".[25] באופן ספציפי, משטרת ישראל משתמשת בכלים הטכנולוגיים הבאים המסופקים דרך חברת סלברייט (המבוססים על תפיסה פיזית של המכשיר, להבדיל מגישה לנתונים מרחוק):

23 ראו להלן בפרק ד.2.
24 צילום: Yaniv Shif. מקור התמונה: The Intercept (קישור).
25 בקשה לפרסום התקשרות עם חברת סלברייט (קישור). להרחבה, ראו להלן פרק ג.1.

איגוד האינטרנט הישראלי
ISOC-IL

:CELLEBRITE UFED 4PC \ Touch

התקני החומרה והתוכנה הבסיסיים של חברת Cellebrite לפריצה וחיקור של מכשירים ניידים שנתפסו פיזית על ידי רשויות החקירה, המאפשרים לעקוף סיסמאות והצפנה ממכשירי אנדרואיד ו-iOS. כלי זה מאפשר לבצע בממשק אחד פעולות של חדירה, העתקה וניתוח של נתונים מתוך מכשירים ניידים. התוכנה מאפשרת גם לבצע סינונים וחיתוכים בחומר (logical extraction capabilities). לתוכנה יכולות שחזור, חדירת מחסומי הצפנה ואיסוף תוכן שנמחק או מוגדר כ-unknown.[26] לכלי זה יכולת גישה למידע במכשירים נעולים על ידי עקיפה, חשיפה או השבתה של קוד נעילת המשתמש,[27] והוא מאפשר גישה, העתקה וניתוח של נתוני אפליקציות, סיסמאות, דוא"ל, היסטוריית שיחות, SMS, אנשי קשר, לוח שנה, מסמכי מדיה (תמונות, וידאו, אודיו) ומידע על מיקום באמצעות רישומי GPS לכתוב מחדש: ממערכת ההפעלה של המכשיר, כרטיס ה-SIM ומרכיבי חומרה נוספים.



איור 2: ממשק מערכת UFED מתוצרת סלברייט המאתר את סוגי המידע השונים שביכולתה לחלץ מטלפונים חכמים[28]

CELLEBRITE PREMIUM[29]

כלי תוכנה זה מאפשר ביטול נעילה במכשירי iOS ואנדרואיד, ומבצע העתקה מיידית ראשונית של חלק מהמידע שאינו מוצפן, למניעת פגיעה במידע בהמשך. עם השתכללותם של מנגנוני ההגנה של מכשירי האייפון הפועלים על מערכת iOS המשתמשת במנגנוני הצפנה מובנים ומנעולים מורכבים, עלה הצורך בפיתוח תוכנה ייעודית לחדירה למערכת ה-iOS. התוכנה מאפשרת לשחזר סיסמאות, לחדור לכל קובצי אפל ואף לגשת לאזורים מוגנים ביותר כגון "secure folder" או "iOS keychain" שבהם נשמר מאגר הסיסמאות של המשתמש לשירותים שונים, כגון רשתות חברתיות, שירותים רפואיים, פיננסיים ועוד.

התוכנה מאפשרת גישה לנתוני אפליקציות של צדדים שלישיים, סיסמאות שמורות, שיחות צ'אט (כגון ווטסאפ, פייסבוק, טלגרם ועוד), נתוני מיקום, דואר אלקטרוני וצרופותיו; גישה לתוכן שנמחק; גישה לסיסמאות שמורות ב-Keychain; שחזור

26 Cellebrite UFED product overview (קישור).
27 במכשירי אנדרואיד: יכולת לעקוף מערכות לנעילת המכשיר, לרבות נעילת תבנית (pattern lock), סיסמה מספרית, וקוד PIN. במכשירי BlackBerry: יכולת לחדור לנתוני BBM, דוא"ל, אפליקציות, נתוני בלוטות' ועוד. במכשירי נוקיה: יכולת חילוץ סיסמאות ממכשיר נעול. במכשירי אייפון: יכולות מיצוי ודי-קודינג. בצ'יפים סיניים: יכולות מיצוי.
28 מקור: Upturn Report, לעיל ה"ש 10.
29 Cellebrite PREMIUM solution overview (קישור).

נתונים מאפליקציות המערבות צד שלישי; נתוני מיקום הן מ-Wifi והן מיקומים סלולריים (אנטנות סלולריות); גישה לנתוני שימוש במערכת ובאפליקציות (System and Applications Logs).

בצד אלו, רשויות האכיפה בישראל משתמשות בכלים נוספים לחדירה וחיפוש במחשבים שולחניים, אך אליהם לא נתייחס בסקירה זו.[30]

יצרני הטלפונים מצידם מגיבים בעדכוני תוכנה שחוסמים פרצות אבטחה ידועות וממשיכים לפתח אמצעי אבטחה מתקדמים, שנועדו לסכל גישה לא רצויה – כולל כזו שמתבצעת באמצעות כלי זיהוי פלילי למכשירים ניידים. לדוגמה, חברת אפל הודיעה בשנת 2022 על "מצב הנעילה" אשר מיועד להתמודד עם תוכנות הפריצה למכשירים החכמים מתוצרתה.[31] "משחק החתול והעכבר" הזה מתרחש כבר שנים, כאשר כלים טכנולוגיים לפריצה וחקירה של טלפונים חכמים משתמשים באינספור טקטיקות לקבלת גישה לנתוני המשתמש: ניחוש סיסמאות, ניצול פרצות אבטחה או כלי פיתוח, ואפילו התקנת תוכנות ריגול.[32]

למעט מקרים נדירים ויוצאי דופן, כלים טכנולוגיים לפריצה וחקירה של טלפונים חכמים כמעט תמיד יכולים לקבל גישה ולהעתיק לפחות חלק מהנתונים המאוחסנים בטלפון.

הודות להצפנה או לאמצעי אבטחה אחרים, כלי זיהוי פלילי למכשירים ניידים לא תמיד מצליחים לחלץ נתונים ממכשיר באופן מיידי. במקרים כאלה הם נוקטים אסטרטגיה אחרת: מנסים סיסמאות אקראיות עד שהם מצליחים לנחש את הסיסמה הנכונה (brute force) ולקבל גישה לנתונים שבמכשיר. אם הסיסמה מורכבת לפיצוח, הכלים הללו יכולים לחפש נתונים לא-מוצפנים שמאוחסנים בטלפון.[33] המפתח לפיענוח ההצפנה בטלפונים רבים מבוסס על סיסמת המכשיר, כך שעוצמת ההגנה שההצפנה מספקת נגזרת ישירות מאורך וממידת המורכבות של סיסמת המשתמש. קל יותר לנחש קוד גישה קצר או נפוץ. לפי נתונים של חוקרי הצפנה משנת 2018, פריצת קוד גישה לאייפון תושלם בתוך 13 דקות אם מדובר בארבע ספרות, 22 שעות בשש ספרות ו-92 ימים בשמונה ספרות. אורך ברירת המחדל ב-iOS הוא שש ספרות.[34] המשמעות היא שתוכנות נפוצות מתקדמות כמו GrayKey או Cellebrite Premium יוכלו לנחש קוד גישה למכשיר תוך פחות מיממה. בנוסף, Cellebrite, לדוגמה, טוענת ש-UFED Premium יכול לחלץ נתונים גם ממכשירי אייפון נעולים (באמצעות ניצול חולשות אבטחה או ניחוש סיסמאות שיטתי).[35]

30 לפי מסמכי הרכש של רשויות אכיפת החוק בישראל (ראו להלן בפרק ג.1) נמצאים ברשותן גם הכלים הבאים: **Cellebrite Macquisition \ Digital Collector**: תוכנה לחדירה למכשירים מתוצרת אפל. בעזרת התוכנה ניתן לחדור למחשב, להשיג נגישות לתיקיית הקבצים ולהעתיק כמויות גדולות של מידע (לא רק קבצים ספציפיים אלא גם בלוקים שלמים של נתונים). התוכנה מאפשרת חיפושים מושכלים בתוך מקבצי המידע ומאפשרת לעיין בתצוגה מקדימה של קבצים נבחרים גם טרם העתקת החומרים, וכן להציג בחינה מדגמית של החומר בהתאם לקריטריונים רלוונטיים ולאסוף מידע המתקבל בזמן אמת כאשר הטלפון מוחזק בידי רשויות החקירה (קישור לפרטי הכלי באתר Cellebrite); **Cellebrite Black Light \ Inspector**: תוכנה לעיבוד וניתוח של נתוני פעילות משתמש ממערכות הפעלה Windows ו-Mac OS למחשבים אישיים: שחזור היסטוריית הפעילות והשימוש במכשיר, שחזור זיכרון, גישה לגיבויים ומידע שהתקבל במכשיר תוך אפשרויות חיפוש מתקדמות. כלי זה כולל גם אפשרות למצות נתונים ומידע מאפליקציות ממערכות ההפעלה iOS ואנדרואיד למכשירים חכמים, לרבות: שיחות והודעות, לוח שנה, העברות בארנק הדיגיטלי, מידע בריאותי ועוד (קישור לפרטי הכלי באתר Cellebrite).

31 (קישור לפרסום באתר Apple).

32 מישור התמודדות נוסף של חברות הטכנולוגיה עם כלים פורנזיים המבוססים על פריצה או ניצול חולשות אבטחה במערכותיהם הוא תביעות משפטיות בגין חדירה לא מורשית למערכת מחשבים. ראו למשל תביעת חברת Apple נגד NSO משנת 2021 (קישור); תביעת חברת Meta נגד NSO משנת 2022 בעקבות פריצה למערכת WhatsApp (קישור).

33 Upturn Report, לעיל ה"ש 10, בעמ' 27.

34 D. Pegg & S. Cutler, What is Pegasus spyware and how does it hack phones, The Guardian, 2021 (link).

35 Cellebrite PREMIUM solution overview (קישור).

איגוד האינטרנט הישראלי
ISOC-IL

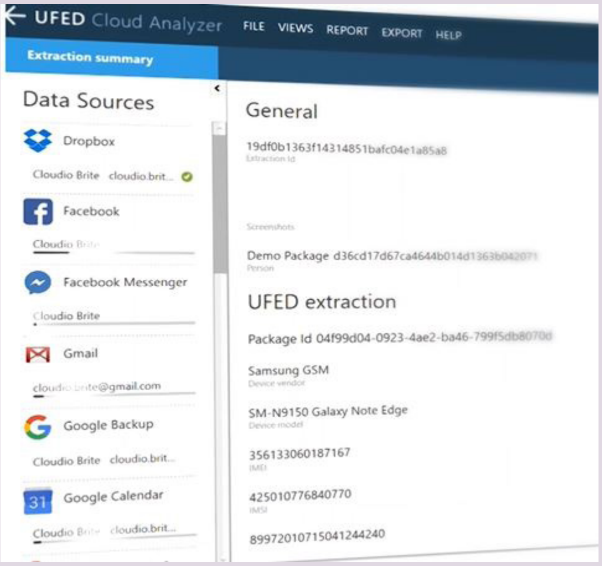
כלים טכנולוגיים לפריצה וחקירה של טלפונים חכמים לא תמיד נדרשים לפצח את הסיסמה, ומנצלים את העובדה שכדי לאזן בין נוחות לבין ביטחון הטלפונים אינם מצפינים את כלל הנתונים במכשיר. רוב האנשים עדיין רוצים לקבל שיחות ומסרונים ולשמוע התראות לאחר שהפעילו את המכשיר וטרם פתחו את הנעילה, לכן נתונים מסוימים אינם מוצפנים בעת ההפעלה, לרבות פרטים הדרושים לקבלת התראות. כמובן יש גישות בסיסיות יותר. לעיתים קרובות רשויות אכיפת החוק מבקשות את ״הסכמתו״ של החשוד לביצוע "חיפוש מרצון" בטלפון, מבלי שהחשוד יודע שיש לו יכולת לסרב. להרחבה, ראו להלן פרק ד, הסוקר את מסגרת הדין והנוהל להפעלת אמצעי מעקב דיגיטליים בישראל.

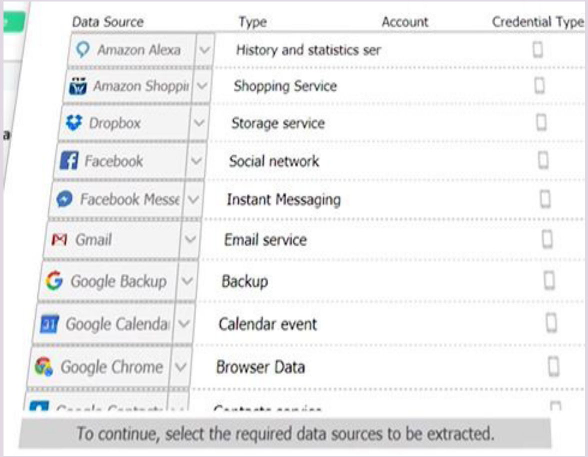
נוסף על הכלים הטכנולוגיים לחדירה ולחיפוש בטלפונים חכמים שנתפסו (אותם מפעילות כאמור רשויות האכיפה בישראל שנים רבות), ראוי להתייחס לטכנולוגיות פורנזיות חדשות שמצטרפות לסדרת ה-UFED, **המאפשרות מיצוי וניתוח של מידע אישי מחשבונות ענן ושרתים מרוחקים שלמכשיר הטלפון קיימת גישה אליהם, כגון גיבויים של מכשירים ניידים קודמים, תמונות וקבצים "כבדים" שזיכרון האחסון של המכשיר צר מלהכיל, ולעיתים גם מידע של משתמשים אחרים שמחזיקים בבעלות משותפת על חשבון הענן משיקולי עלות או עבודה משותפת.**

אחת הדרכים שבהן כלי זיהוי פלילי למכשירים ניידים ניגשים למידע מרוחק היא באמצעות העתקת פרטי החיבור לחשבון השמורים בטלפון, והתחזות למכשיר של המשתמש. גופי החקירה מקבלים כך גישה לרוב נתוני הענן של המשתמש, לרבות מידע ממדיה חברתית, דוא"ל או גיבויים של תמונות ונתונים אחרים, אשר לרוב אינם מוצפנים. הכלים מנצלים את האפשרות להוריד את כל הנתונים המקושרים לחשבון המשתמש (שירות שמציעות למשל גוגל או פייסבוק) כדי לקבל גישה למגוון רחב אף יותר של נתונים ומקורות מידע. יכולות חסרות תקדים אלו של גישה לנתונים הנמצאים בשרתים מרוחקים (להבדיל מנתונים המאוחסנים על מכשיר הטלפון שנתפס) מעוררות שאלות משפטיות רבות, כמפורט להלן בפרק ה.3.

משנת 2020, חברת סלברייט מציעה ללקוחותיה את הכלי UFED CLOUD,[36] המאפשר לחלץ ולנתח מידע באופן אוטומטי מלמעלה מ-50 שירותי ענן ומקורות מקוונים באמצעות פרטי ההתחברות של בעל המכשיר:[37]

- שירותי אחסון בענן, כגון Dropbox, OneDrive, Google Drive, Google Photos ועוד.
- שירותי גיבוי מקוונים, כגון Google Backup, iCloud ועוד.
- חשבונות דואר אלקטרוני ויומן, כגון Gmail, Google Calander ועוד.
- אפליקציות מסרים מיידיים, כגון Whatsapp, Facebook Messenger ועוד.
- רשתות חברתיות (לרבות היסטוריית שיחות, מידע על פעילות ומיקומים), כגון Facebook, YouTube, Ok Cupid, Instagram, Twitter ועוד.
- חשבונות גוגל/אנדרואיד, הכוללים לרוב גיבויים, שמירת סיסמאות, תיעוד של חיפושים, פעילות, מיקומים, אנשי קשר ועוד.
- חשבונות בדפדפנים, כגון Google Chrome או FireFox (הכוללים לרוב היסטוריית גלישה וסיסמאות שמורות).





צילומי מסך של מערכת UFED Cloud Analyzer כפי שהוצגו בסרטון מידע מטעם חברת סלברייט[38]

36 Cellebrite UFED CLOUD product overview (קישור).

37 מקור: https://cellebrite.com/en/ufed-cloud-analyzer-5. פעולה זו נעשית לרוב באמצעות האפשרות של שירותים מקוונים רבים לאפשר למשתמש להוריד את כל המידע האגור עליו.

38 קרדיט: Cellebrite, שם.

2.ב חדירה, חיפוש והאזנה למכשירים חכמים באופן סמוי (רוגלות)

שלב החקירה הסמויה מתאפיין בעיקר בהפעלת כלים לאיסוף ראיות אשר מושא החקירה איננו מודע להם, ואיננו מעומת איתם כמפורט להלן, ולכן הוא בעל השפעה עצומה על זכות האזרח להליך הוגן. מרבית השיטות והאמצעים הטכנולוגיים של המשטרה מוגדרים על ידה כבעלי חיסיון, אולם הואיל ואלו נבחנים שוב ושוב בפסיקה ובפרקטיקה הנוהגת, הרי שמרביתם הפכו גלויים והמתודה שביסודם גם הפכה גלויה, וההתייחסות להלן כולה מקורה במקורות גלויים. כלל השיטות שנסקור בפרק זה יכולות להיות מופעלות החל משלב החקירה המודיעינית אשר מתבצעת ביחידות המודיעין השונות וביניהן יחידת הסיגנט ויחידת הסייבר, והן בשלב החקירה הסמויה על בסיס בקשת היחידה החוקרת.

רוגלה (spyware) היא תוכנה המותקנת באופן סמוי על גבי מערכת מחשוב (לרבות מכשירים חכמים), לרוב באמצעות תקיפה המנצלת חולשות במנגנוני אבטחה קיימים של מכשירים ותוכנות אחרות, המעניקה לתוקף המפעיל אותה גישה למערכת המחשוב שעליה הותקנה.[39] קיים ספקטרום רחב של פעולות שרוגלות שונות מסוגלות לבצע. לצורך סקירה זו נבחין בין רוגלות שיכולותיהן מוגבלת ל"האזנת סתר" בלבד, קרי ניטור שיחות קוליות והודעות מיידיות (instant messaging) של מכשיר יעד, שהיו נפוצות בעשור הקודם,[40] לבין רוגלות מודרניות דוגמת Pegasus מתוצרת חברת NSO, המספקות גישה מלאה לנתונים הקיימים במכשיר היעד, לרבות אפשרות להעתיק/למחוק מידע או ליזום גישה למידע נוסף (מחיישני המכשיר או מחשבונות ענן המקושרים אליו).

במהלך שנת 2022 נמצא כי משטרת ישראל מפעילה מזה תקופה כלי סייבר התקפי מתוצרת חברת NSO המכונה "סייפן", המאפשר לגורמי החקירה חדירה נמשכת ונסתרת לטלפון החכם של הנעקב, וגישה למכלול הנתונים הזמינים בו או באמצעותו. לפי דו"ח מררי,[41] השימוש בתוכנה לצורך ביצוע "האזנת סתר לתקשורת בין מחשבים" (חדירה נמשכת, נסתרת ומרחוק לטלפונים חכמים והנתונים הקיימים בהם, לרבות נתוני עבר ועתיד) "החל לערך בשנת 2016".[42]

תת-פרק זה מציג את הטכנולוגיה והיכולות של כלים מסוג זה, להבדיל מפריצה וחיפוש במכשירים שנתפסו שבהם עסק תת-הפרק הקודם. מכיוון שלא נחשפו לציבור פרטים על מערכת NSO המכונות "סייפן", הסקירה בחלק זה מתבססת על מקורות מוסמכים ליכולותיו של הכלי Pegasus שאותו מספקת NSO, ואשר לו יכולות ומנגנוני פעולה דומים.[43]

כלי ריגול כדוגמת פגסוס, או מערכות דומות המופעלות בשלב החקירה הסמויה, נועדו לתקוף בהצלחה כמעט כל טלפון חכם עם מערכת הפעלה iOS או אנדרואיד, על פי הנתונים הספציפיים של היעד – כגון מספר הטלפון הסלולרי. **באופן בלתי נראה לעין לבעל המכשיר, כלים אלה יכולים להפוך טלפון סלולרי למכשיר מעקב הפועל 24 שעות, בעודם**

39 **דין וחשבון הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים** (אוגוסט 2022) (להלן: דו"ח מררי) בעמ' 25 ("רוגלה היא תוכנה המותקנת באופן סמוי על גבי מערכת מחשוב (בין אם מרחוק או באופן פיזי), ומאפשרת נגישות לצד התוקף למערכת המחשוב הנתקפת"); דו"ח נציב הגנת הפרטיות באיחוד האירופי מיום 15.2.2022 (קישור) (להלן: דו"ח נציב הגנת הפרטיות-2022).

40 דוגמה לרוגלות מוגבלות אלו היא מערכת "חלוץ" שפותחה בשנת 2013 על ידי משטרת ישראל, אשר באמצעות נגישות פיזית מאפשרת חדירה לטלפונים חכמים וביצוע האזנת סתר (דו"ח מררי, בעמ' 14).

41 דו"ח מררי, לעיל ה"ש 39.

42 שם, בעמ' 31 ("לאורך כל תקופת פעילותה של המערכת במשטרה (בין השנים 2016-2021)").

43 על פי דו"ח ועדת מררי, מערכת סייפן אינה מוגבלת בפועל לאיסוף תוצרים חדשים בלבד (כפי שהאזנת סתר "רגילה" מוגבלת): **ראשית, מערכת סייפן מאפשרת למשטרה לקבל מידע האגור על מכשיר היעד ושנוצר קודם למועד ההדבקה**; יכולת זו הופעלה במקרים מספר על ידי חוקרי משטרת ישראל והתקבל באמצעותה מידע שנוצר טרם מועד ההדבקה הראשון, ואף קודם למועד צו בית המשפט. **שנית, במערכת הסייפן לא נוונה היכולת לקבל מידע שאינו מהווה תקשורת בין מחשבים כגון פרטי יומן, אנשי קשר, פתקים או רשימת האפליקציות המותקנות**, וגם מידע זה התקבל פעמים רבות במסגרת הפעלת הכלי. שם, בעמ' 33.

איגוד האינטרנט הישראלי ISOC-IL

משיגים גישה מלאה לכל חיישני הטלפון והנתונים השמורים בו. בנוסף, רוגלות מסוג זה מאפשרות לקרוא, לשלוח או לקבל הודעות שאמורות להיות מוצפנות מקצה לקצה, להוריד תמונות שמורות בטלפון ולהאזין לשיחות קוליות/וידאו, ולהקליט אותן.[44] לשם כך, רוגלות כגון פגסוס מנצלות נקודות תורפה בטלפונים ניידים של אנשים מזוהים מראש, אינה זקוקה למעורבות של ספקי שירותי תקשורת אלקטרוניים, ומשלבת מגוון כלי מעקב אלקטרוניים.[45] הרוגלה **נטענת ומותקנת** באופן אוטומטי במכשיר של היעד אחרי שמפעיל התוכנה (1) גורם ליעד ללחוץ על קישור תמים למראה (SMS phishing link – קישור דיוג בהודעת טקסט), או (2) גורם למכשיר של היעד להתחבר לרשת סלולרית מזויפת שידועה בשם IMSI catcher (network injection – הזרקה לרשת), או (3) מנצל נקודת תורפה לא ידועה (zero-click exploit – פריצה ללא לחיצה), כלומר ללא כל פעולה מצד היעד.[46]

ככל שהרוגלה נטענת ומותקנת בהצלחה על מכשיר היעד מרחוק היא מאפשרת למפעילה גישה מלאה לתוכן ההיסטורי שנאגר במכשיר וחומרתו, וזו מאפשרת לחוקרים להשתמש במצלמה או במיקרופון של הטלפון הנייד בחשאי כדי לצלם את המשתמש ואת סביבתו או כדי להפעיל את המיקרופון ולהקליט שיחות בעולם האמיתי (למשל של אנשים בקרבת המשתמש). בין היתר, לכלים אלו יש גישה מלאה גם למודול המיקום הגאוגרפי של הטלפון, כלומר הם יודעים היכן נמצא הטלפון הנעקב (וככל הנראה גם בעליו) בכל רגע נתון, והם מסוגלים להקליט גם את השינויים במיקום הטלפון לאורך זמן.[47]

בנוסף על כך שכלים כגון Pegasus או "סייפן" אינם מוגבלים לאיסוף מידע רק מיום תחילת ה"האזנה",[48] הם נבדלים מטכנולוגיות האזנה מסורתיות של רשויות האכיפה, במישורים נוספים:

- **רוגלות מעקב לטלפונים חכמים דוגמת פגסוס מאפשרות גישה מלאה ובלתי מוגבלת למכשיר היעד ולכל חשבונות הענן שיש לו גישה אליהם.** על פי מחקר שערכה מעבדת האבטחה של אמנסטי אינטרנשיונל, תוכנת ריגול זו מאפשרת לתוקף לקבל מה שמכונה "הרשאות שורש", או הרשאות ניהול, במכשיר: "פגסוס מסוגלת לעשות יותר במכשיר מאשר בעל המכשיר עצמו".[49] לאור היכולות חסרות התקדים הללו, אי אפשר לשלול את האפשרות של שימוש בפגסוס מעבר להאזנה לשיחות. לדוגמה, הכלי יכול לאפשר לתוקף לקבל גישה לאישורים דיגיטליים או לאפליקציות זהות דיגיטלית, ובאמצעותם ניתן להתחזות לקורבן ולקבל גישה לנכסים הדיגיטליים והפיזיים שלו, או לבצע פעילויות דומות אחרות.[50]
- **יכולת לבצע "הדבקה" מרחוק של טלפונים ללא צורך בפעולה של המשתמש (Zero-Click), כך שאפילו משתמש בעל ידע רב באבטחת סייבר אינו מסוגל לעשות דבר כדי למנוע את המתקפה.** יתר על כן, אפילו הספקים הגדולים ביותר של מכשירים, כגון אפל וגוגל, אינם מסוגלים בהכרח לתת הגנה מלאה לאנשים פרטיים מפני תוכנות זדוניות (זדונה) מודרניות כמו פגסוס – על אף מאמציהם הבלתי נלאים לשפר את האבטחה של התוכנות שלהם. על פי דו"ח נציב הגנת הפרטיות של האו"ם משנת 2022, לחברות פריצה פרטיות, כגון קבוצת NSO, יש עוצמה פיננסית

44 סקירת היכולות ואופן הפעולה של רוגלות דוגמת פגסוס של חברת NSO נסמכת על המקורות הבאים: דו"ח נציב הגנת הפרטיות באיחוד האירופי מיום 15.2.2022, לעיל ה"ש 39; דו"ח פורנזי של Amnesty International's Security Lab מיום 18.7.2021 (קישור) (להלן: דו"ח אמנסטי-2021); דו"ח פורנזי של Citizens Lab מיום 18.9.2018 (קישור).

45 European Parliamentary Research Service, Europe's PegasusGate (2022) (link).

46 שם, בפרק 2.

47 שם.

48 לגבי Pegasus, ראו שם. לגבי "סייפן", ראו דו"ח מררי, לעיל ה"ש 39, בעמ' 33 ("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").

49 דו"ח נציב הגנת הפרטיות, לעיל ה"ש 39, בעמ' 3.

50 שם.

המאפשרת להן לשכור מהנדסי תוכנה מבריקים, שתפקידם היחיד הוא לחפש נקודות תורפה (אלה תמיד קיימות) ולפתח אמצעים רבי עוצמה, כך שיכולותיהן של חברות אלה אינן שונות באופן מהותי מאלה של מדינת לאום.[51]

- **כמעט בלתי אפשרי לגלות את פעולתה של פעולת פגסוס בזמן אמת או בעבר, אלא אם כן מערכת ההפעלה כוללת מנגנוני רישום מערכתיים מאובטחים.**[52] חוקרי אבטחה חושדים שגרסאות עדכניות של פגסוס שוכנות רק בזיכרון הזמני של הטלפון, ולא בכונן הקשיח שלו, כלומר: ברגע שהטלפון כבוי, למעשה כל זכר לתוכנה נעלם.[53] יתר על כן, ההטמעה של מחשוב ענן מאפשרת לחברות פרטיות המוכרות תוכנות זדוניות ותוכנות ריגול לספק ללקוחותיהן גישה למכשירו של הקורבן דרך אתר אינטרנט, מבלי שהלקוח יצטרך לרכוש חומרה או להתקין תוכנה כלשהי על מערכות המחשוב שלו.[54]

על רקע זה, חשוב להבין כי ביצוע של "האזנת סתר לתקשורת בין מחשבים" באמצעות רוגלות כדוגמת Pegasus לרוב כרוך בביצוע העבירות הפליליות שקובע חוק המחשבים: שיבוש או הפרעה למחשב או לחומר מחשב; חדירה לחומר מחשב; כתיבה או העברה של תוכנה שתוצאתה תהיה מידע כוזב או פלט כוזב; או פעולות אסורות בתוכנה.[55] דוגמה ממחישה לכך היא פרשת ריגול מסחרי שכונתה פרשת "הסוס הטרויאני", בה הורשעו מי שפיתחו והפעילו תוכנה סמויה שעם חדירתה למחשב כלשהו מבעד לאינטרנט יש ביכולתה לקבל ולהעביר למפעיליה נתונים שונים המצויים במחשב שאליו חדרה.[56]

על כן, אין להשוות את פגסוס לכלֵי האזנה "מסורתיים" המשמשים את רשויות האכיפה; נראה שפגסוס דומה יותר לפתרונות "טרויאניים" או לפתרונות "חיפושים מקוונים"[57] שהופעלו בעבר על ידי ממשלות והעלו חששות משפטיים ומוסריים בלתי מבוטלים.[58] בשל התכונות הייחודיות שלה, תוכנת הריגול פגסוס ודומותיה מהוות נקודת מפנה המשלבת דרגת פולשנות חסרת תקדים בהשוואה ליכולות עבר, עם תכונות המסוגלות להפוך רבים מאמצעי הנעילה והאבטחה של המכשירים החכמים לבלתי יעילים ולחסרי משמעות. כמובן פגסוס אינה יחידה מסוגה, וחברות נוספות מפתחות כלי סייבר התקפי עבור רשויות אכיפת חוק מדינתיות.

51 שם. ראו גם: L.H. Newman, Google Warns That NSO Hacking Is On Par With Elite Nation-State Spies, Wired (15.12.2021) (קישור).
52 דו"ח נציב הגנת הפרטיות-2022, לעיל ה"ש 39.
53 שם; Pegg & Cutler, לעיל ה"ש 34.
54 דו"ח נציב הגנת הפרטיות 2022-ודו"ח אמנסטי-2021, לעיל ה"ש 39.
55 סעיפים 2–6 לחוק המחשבים.
56 לתיאור פרטי הפרשה, שעסקה בין היתר בעבירות של חדירה לחומר מחשב, החדרת נגיף מחשב והאזנת סתר שלא כדין, ראו: בש"פ 7368/05 זלוטובסקי נ' מדינת ישראל (4.9.2005).
57 להרחבה על אודות המונח Government Trojan ועוצמת החודרנות של כלים אלו, ראו בקישור.
58 GFF Challenge to use of government spyware, Privacy International (2021) (link).

עם חתימה, נציין כי ייתכן מצב שבו כלי הסייבר ההתקפי שמפעילה משטרת ישראל יוגבל באופן אפקטיבי ממימוש היכולות חסרות התקדים של פגסוס. אולם, נכון למועד כתיבת שורות אלו, במרבית תקופת פעילותה של מערכת סייפן משנת 2016, ולפחות עד אפריל 2020, לא ניתן היה להגביל את המועד אשר החל ממנו יתקבל המידע או תבוצע הגישה למידע נוסף מהטלפון החכם שאינו "שיחה". על פי דו"ח מררי, החל מאפריל 2020 נכלל "מודול" חדש בממשק המשתמש של מערכת NSO שברשותה המאפשר להגביל את המידע המתקבל לתאריכים תחומים ומוגבלים, או את סוגי התוצרים שיתקבלו במסגרת הפעלת הרוגלה.[59] עם זאת, כפי שהדו"ח מציין, גם לאחר הטמעת המודול החדש והאפשרות להגביל את יכולות הכלי לא היה ממשק שהיווה תנאי הכרחי מבחינה טכנולוגית לביצוע ההדבקה.[60]

על כן, אנו סבורים כי בעת הזו ראוי להתייחס מבחינה תאורית ליכולות הפוטנציאליות של מערכת "סייפן" כדומות במהותן לאלו של רוגלות דוגמת Pegasus. זאת, בין היתר, בהסתמך על הממצאים שלפיהם במערכת "סייפן" ובמערכות דומות נוספות שבידי משטרת ישראל לא נוונה באופן מלא היכולת הטכנולוגית לקבל את סוגי המידע הבאים שאינם מהווים מידע מסוג "תקשורת בין-מחשבים", כגון רשימת אפליקציות המותקנות על גבי המכשיר המודבק,[61] ונתונים אישיים מסוג פתקים, אנשי קשר או פרטי יומן[62] החורגים מסמכות המשטרה לפי חוק האזנות סתר, שאינה כוללת אפשרות לגשת למידע האגור במכשיר.[63] מידע מסוג זה אף התקבל בפועל לא אחת אצל המשטרה,[64] ואף לאורך תקופת פעילותה של המערכת הייתה אפשרות שבה "באופן פאסיבי ייחשף מידע למפיק... גם אם המפיק לא נכנס באופן אקטיבי לצפייה באותו פריט מידע".[65]

---

59 דו"ח מררי, לעיל ה"ש 39, בעמ' 35 ("רק באפריל 2020 לערך, בגרסה מתקדמת יותר של המערכת, נכלל מודול חדש בממשק המשתמש שבידי המשטרה, שמכונה "מודול ה-warrant". מודול זה אפשר להזין את התאריכים לביצוע ההאזנה ("בהתאם לתוקפו של צו בית המשפט").

60 דו"ח מררי, שם, בעמ' 36 ("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... 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").

61 דו"ח מררי, שם, בעמ' 38 ("בכל פעם שבה 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").

62 דו"ח מררי, שם, בעמ' 39 ("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") ועמ' 58 ("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... 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").

63 דו"ח מררי, שם, בעמ' 34.

64 שם, בעמ' 35. לפי הדו"ח, אין הכוונה כי עשויה הייתה 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.

65 דו"ח מררי, שם, בעמ' 40 ("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").

ב.3 טכנולוגיות לניתוח ולהצלבה של מידע העתק שניתן לחלץ מחדירה לטלפון חכם

נוסף על פריצה והעתקה של נתונים ממכשירים חכמים, רשויות אכיפת החוק משתמשות גם בכלים טכנולוגיים מתקדמים כדי לנתח ולהצליב ביעילות את כמות העתק של נתונים שניתן להשיג ממכשירים חכמים שנתפסו על ידן. בסופו של דבר, היכולת להעתיק כמות עצומה של נתונים מטלפון סלולרי אינה מועילה אם אי אפשר לחפש בה ביעילות. כלים אלו מאפשרים לגופי החקירה או המודיעין ברשויות אכיפת החוק למיין ולהצליב את שפע הנתונים שניתן לחלץ מטלפונים חכמים על פי שעת ותאריך יצירתם, לפי מיקום, לפי סוג הקובץ או המדיה או על פי האפליקציה שבה נוצרו. החוקרים יכולים לחפש מילות מפתח בטלפון בדומה לחיפוש באינטרנט, למשל על פי שמות של חשודים או מעורבים אחרים, או תוך אפיון קשרים חברתיים מכלל האפליקציות והנתונים של המשתמש.

המשמעות היא שהמשטרה יכולה לקחת נתונים שמקורם באפליקציות שונות ולצפות בהם במרוכז כסדרת אירועים כרונולוגית, או לשלוף את כל הצילומים מהטלפון לצפייה במקום אחד וביצוע פעולות עיבוד מתקדמות כגון זיהוי פנים, ללא קשר לאופן שבו הם מאורגנים במכשיר.[66]

לדוגמה, הכלי Pathfinder של חברת Cellebrite,[67] שרשויות החקירה משתמשות בו לארגון וניתוח הנתונים שנאספו מכלי הפריצה וההעתקה, כולל יכולות בינה מלאכותית (AI) ולמידת מכונה (Machine Learning) המאפשרות לנתח ולהצליב בין החומרים השונים ולהציג באופן אוטומטי דפוסים ותובנות מעשיות להמשך החקירה. התוכנה מסוגלת להצליב ולבצע חיתוכים בין המידע ולהציג את הנתונים הרלוונטיים ביותר. הצגת הנתונים יכולה להיעשות לפי קטגוריות, אנשי קשר והתקשרויות עם צדדים שלישיים. בנוסף, למערכת יכולות זיהוי חזותיות לאיתור תמונות וקטעי וידאו המציגים סמים, נשק, פורנוגרפיית ילדים ועוד. התוכנה יכולה להתאים בין פרופילים מפלטפורמות שונות ולמפות את כלל הקשרים הדיגיטליים של בעל המכשיר.[68]

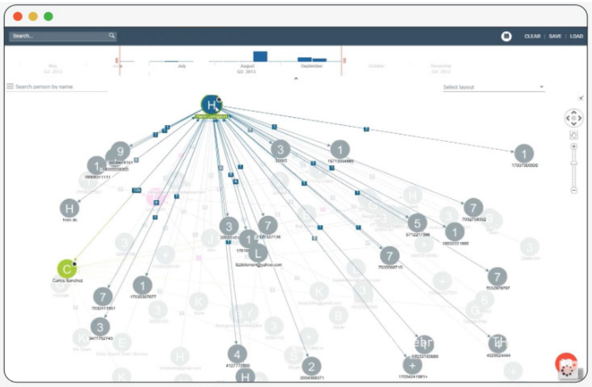


Figure 2.8 shows a screenshot of Cellebrite Analytics, now called Cellebrite Pathfinder, which infers a social graph based on communication events. This graph shows the participants of communications extracted from the phone, as well as a histogram of communication volume over time.[49]

תמונה 4: צילום מסך מתוך מערכת Cellebrite Pathfinder המייצרת מיפוי גרפי של אירועי תקשורת ומיפוי סביבתו החברתית של יעד המעקב (מקור וקרדיט: Cellebrite)

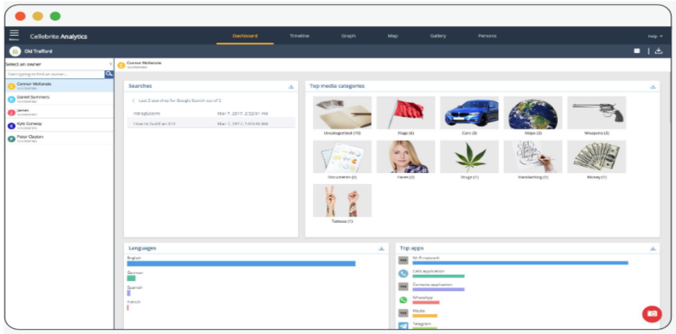


Figure 2.9 sshows Cellebrite Pathfinder, which allows investigators to perform an image-based search using pre-generated filters, like "Flags," "Faces," "Drugs," "Weapons," or "Tattoos." The software also has features, shown at the top, such as "Timeline" (for viewing events on the phone chronologically), "Graph" (to make a social network graph of contacts and communications), "Map" (to display all phone events and media with location data on a map), "Gallery" (to view all media like photos and videos in one place regardless of source), and "Persons" (to view profiles of discrete users on the phone).[53]

תמונה 5: צילום מסך מתוך מערכות הצלבת מידע המאפשרות לחוקרים לבצע חיפוש חזותי בכלל הנתונים (כגון נשק, סמים או קעקועים), לנתח את קשריו החברתיים של אדם מסוים ולבצע חיפושים והצלבות של מכלול הנתונים ביחס למקום גאוגרפי מסוים (מקור וקרדיט: Cellebrite)

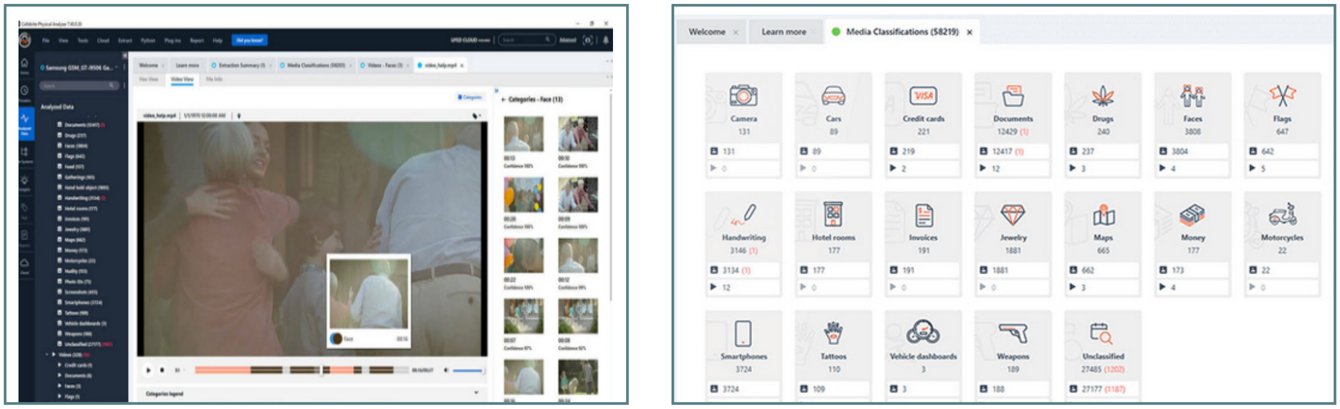
---

66 כוחן המשמעותי ביותר של מערכות אלו הוא ביכולתן לערוך פילוח וניתוח של המידע הגלוי והסמוי שבמכשיר ולאפשר לרשויות החוק ליצור פרופיל משתמש אשר יוצר תמונה מלאה על דעותיו הגלויות והסמויות של האדם, מחשבותיו, תחביביו, נטיותיו המיניות וחולשותיו.

67 Cellebrite PATHFINDER product overview (קישור).

68 בהקשר זה, חשוב להתריע על הסיכון הכללי של הטיות פסולות (bias) המאפיינות רבים מהשימושים של רשויות אכיפת החוק בטכנולוגיות Machine Learning ובינה מלאכותית, ועל מגבלות היכולת להתחקות אחר הדרך שבה הגיעו מנגנוני AI לפלט שהם יוצרים. ראו למשל Yeung et al., Identifying Systemic Bias in the Acquisition of Machine Learning Decision Aids for Law Enforcement Applications, RAND Homeland and Security Research (2021) (link); Will Douglas Heaven, Predictive policing algorithms are racist. They need to be dismantled, MIT Technology Review (2020) (link).

לאחרונה החלה חברת Cellebrite לספק ללקוחותיה כלי טכנולוגי מתקדם בשם Physical Analyzer אשר מסוגל לנתח את כל המידע אשר מגיע מהמוצרים של Cellebrite ומצווי חיפוש.[69] הכלי מייצר לוח זמנים אשר ממקם את כל המידע בצורה נוחה וכרונולוגית. בנוסף, הכלי מסוגל לגשת למידע שנמחק ולמידע שנמצא בענן.



תמונות 6–7: צילומי מסך מתוך מערכת Cellebrite Physical Analyzer המסווגת תמונות בעזרת בינה מלאכותית, ומאתרת ומסווגת מדיה על בסיס העדפות נבחרות (מקור/קרדיט: cellebrite.com/en/physical-analyzer)

כלים אלו הם בעלי חשיבות יתרה במהלך חקירה טרום מעצר, מכיוון שהם מאפשרים ליחידה החוקרת לקבל תמונה מלאה ומפורטת על חייו של החשוד. מעבר לכך, היא נותנת תמונה על קשריו החברתיים, ואף מידע רב על אנשים שאיתם היה בקשר – גם אם הם אינם בגדר חשודים.

בסופו של התהליך, כלי הניתוח של חברת סלברייט מאפשרים למפעיל להפיק פלט של תוצאות החיפוש ומקורות הנתונים, וזה מועבר לידי התביעה וההגנה. ראו דוגמאות בנספח א. עם זאת, כלים אלו מאפשרים למפעיל לבחור איזה מידע ייכנס לכל פלט מוגדר, כך שאם מידע מסוים אינו נמצא בפלט שהועבר לידי ההגנה או התביעה אין זה אומר שהוא אינו נמצא על גבי המכשיר או העותק הפורנזי שלו.

4.ב חולשות, מהימנות ואמינות של טכנולוגיות חדירה למכשירים חכמים

כמתואר בחלקים הקודמים, הכלים הפורנזיים לחילוץ ולעיבוד מידע ממכשירים חכמים כגון אלו של Cellebrite ו-NSO מנצלים חולשות אבטחה במערכת ההפעלה, בחומרה, באמצעי התקשורת או בתוכנה של מערכות המחשבים והטלפונים הניידים כדי לשבש או לעקוף את מנגנוני הנעילה והאבטחה המובנים שלהם. בדומה, גם מרכיבי התוכנה של הכלים הפורנזיים לחיקור טלפונים ניידים שרשויות החקירה משתמשות בהם עשויים לכלול חולשות שאינן ידועות למפתחים או למפעילים של הכלים הפורנזיים.

69 Cellebrite PHYSICAL ANALYZER product overview (קישור).

לדוגמה, בשנת 2021 תועדו חולשות אבטחה בכלים UFED ו-Physical Analyzer (של חברת סלברייט, הנמצאים בשימוש גם בישראל) שאפשרו לבעל מכשיר הטלפון הנייד לשבש את פעילותו התקינה של תהליך חילוץ ועיבוד המידע.[70] חולשות האבטחה שהתגלו בכלים נפוצים אלו היו רחבות ומטרידות בהיקפן עבור טכנולוגיה פורנזית להפקת ראיות. החמורה ביותר נבעה מכך שסביבת התוכנה של מערכת UFED מסתמכת על חבילות קוד חיצוניות לעיבוד קובצי מדיה בקידוד הנפוץ mpeg שלא עודכנו בסביבת התוכנה של הכלים UFED ו-Physical Analyzer מאז שנת 2012, למרות מאות עדכוני אבטחה שפורסמו לחבילה זו מאז. כלומר, כלי סלברייט היו חשופים לכאורה לחולשות אבטחה מרובות וידועות שהתגלו בחבילת הקוד הנפוצה הזו במרוצת השנים.

חולשות אלו, כפי שתועדו בשנת 2021, אפשרו למי שהכיר אותן להכין קובץ שנחזה לפריט מדיה רגיל ושאותו ניתן להפיץ ולשמור על גבי טלפונים ניידים ומכשירים חכמים, אך למעשה מכיל קוד שיופעל בכלים הפורנזיים של סלברייט כאשר יעבדו את הקובץ. באופן זה, מומחי אבטחה הדגימו כיצד ניתן לנצל חולשת אבטחה זו כדי לשבש או לשנות את הדו"ח הפורנזי של הסריקה ואף את הנתונים של מכשירים אחרים השמורים במערכת, לרבות מכשירים עתידיים. בכלל זה, ניתן לשנות את פרטי הדו"חות הפורנזיים של כלל המכשירים במערכת, לרבות הוספה או הסרה של טקסט, דוא"ל, תמונות, אנשי קשר ועוד.

למותר לציין כי ממצאים אלו מעוררים דאגה בנוגע למהימנות הממצאים הפורנזיים שהופקו באמצעות הכלים UFED ו-Physical Analyzer, שבהם משתמשות גם רשויות האכיפה בישראל לאורך העשור האחרון.

כמובן, גם כלים פורנזיים לחדירה מרחוק כגון סייפן או Pegasus מבוססים על תוכנה וקוד העשויים לכלול חולשות שאינן ידועות למפתחים או למפעילים של הכלים הפורנזיים. **בעיקר, הם מעוררים בעיות ראייתיות עמוקות יותר הנובעות מכך שהפעלת כלים אלו מחייבת שינוי של נתונים על גבי מכשיר היעד ללא ידיעת המשתמש** כדי להסתיר את פעולתו מאמצעי אבטחת המידע המובנים במערכת ההפעלה של האמצעי, ומעיני המשתמש. העובדה כי פעילות כלים פורנזיים מסוג זה כרוכה בהכרח בשינוי הנתונים ומערכות האבטחה של מכשיר היעד מהווה שינוי דרמטי מהאופן הפסיבי שבו מתבצעת האזנת סתר מסורתית לשיחה לתקשורת בין מחשבים. זאת, כאשר **אין בישראל תהליך מובנה של אישור משפטי של תקינות הפעולה של מערכות מסוג זה על ידי צד שלישי נייטרלי**, בשונה ממערכות טכנולוגיות אחרות לאכיפת חוק, דוגמת אמצעי אכיפה כגון הממל"ז או מערכת א-3 שבשימוש המשטרה, שנבחנו לעומקן על ידי בתי המשפט ומומחים מטעמו. אי בחינתם המקצועית של כלי חדירה, חיפוש או האזנה שמפותחים ומתוחזקים על ידי גורמים מסחריים היא תקלה מהותית שיש להסדירה.

לכן, כל דיון נורמטיבי בהפעלת כלים כדוגמת "סייפן" נדרש להיעשות בשים לב לפוגענות הייחודית שלהם בשני מישורים: (א) חשיפת המשתמש לפגיעות סייבר אחרות, לרבות גישה למידע אישי, כתוצאה מכך שתהליך החדרת הרוגלה למכשיר היעד והסתרת פעילותה ממערכת ההפעלה או המשתמש כרוך לרוב בביטול חלק מתכונות האבטחה של מכשיר היעד. **(ב) אמינות הראיות וחשש ל"זיהום" של הנתונים המקוריים:** הצורך להסתיר את פעולת ההדבקה והעברת המידע באמצעותה מוביל לכך שכלים כדוגמת סייפן או Pegasus חייבים לשנות את התיעוד האוטומטי (log) במערכת ההפעלה או במערכת הקבצים של מכשיר היעד, מה שעשוי ליצור קושי ראייתי, עוד לפני החשש כי גורמי החקירה יכולים ליזום פעולות תקשורת בשם בעל המכשיר או לשנות את תוכנו באופן נסתר.

על רקע זה, ניתן להסיק כי השימוש העיקרי של כלים כדוגמאת "סייפן" על ידי משטרת ישראל, הוא כמקור למידע מודיעיני (שאינו כפוף לדיני הראיות בהיבטי קבילות או משקל), להבדיל מכלי Cellebrite שתוצריהם מוגשים לעיתים קרובות כראיה בהליכים פליליים.

70 Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective (21.4.2021) (link).

ג נתונים על חדירה וחיפוש בטלפונים חכמים וחשבונות ענן בישראל: תמונת מצב

ג.1 משטרת ישראל ורשויות נוספות משתמשות בכלים מתקדמים לפריצה ולחיפוש דיגיטליים

השימוש בכלים טכנולוגיים מתקדמים לפריצה ולחיפוש במכשירים חכמים, ובפרט בכלים מתוצרת חברת Cellebrite שנסקרו בהרחבה לעיל, אינו מוגבל רק למשטרת ישראל, אלא גם לשורה ארוכה של רשויות אכיפה אחרות הנדרשות לביצוע חקירות שאינן משטרתיות: הרשות להגנת הפרטיות, רשויות המס ומצ"ח.

גורמי החקירה השונים ברשות להגנת הפרטיות במשרד המשפטים (ובעבר, רמו"ט - הרשות למשפט, טכנולוגיה ומידע) משתמשים בשנים האחרונות באופן נרחב בטכנולוגיות החדירה והחיפוש של חברת Cellebrite, ובכלי Ufed Touch Ultimate Standard בפרט. למעשה, מסמך רשמי של החשב הכללי עבור משרד המשפטים מלמד כי עוד בראשית שנת 2015 הצהירה רמו"ט שהיא פונה למשטרת ישראל לקבלת שירותי חדירה וחיפוש כאמור.[71] ממסמך זה ניתן ללמוד על היכרות טובה של הרשות עם יכולות הכלים הטכנולוגיים, שאותם היא מתארת כמאפשרים "פריצת סיסמאות לטלפון; העתקה בינארית של המידע בהתאם למערכת ההפעלה והחומרה על הטלפון; הנגשת המידע לחוקר בטלפון ובתוכנות הנלוות".

בנוסף, מסמך רשמי של החשב הכללי עבור הרשות להגנת הפרטיות מיום 18.8.2020 מלמד כי היחידות החוקרות ברשות להגנת הפרטיות משתמשות מזה שנים מספר בכלים מתוצרת Cellebrite המאפשרים העתקה פיזית פורנזית של מוצרי Apple, ו"מיצוי מכספות של macOS".[72]

הממצא המעניין ביותר העולה ממסמכי הרשות להגנת הפרטיות הוא שהשימוש בכלי החדירה והחיפוש של חברת Cellebrite הוא חלק מסביבת העבודה של רשויות אכיפה נוספות מלבד משטרת ישראל, כגון רשויות המס, המכס ומצ"ח.

ג.2 טכנולוגיות פורנזיות לפריצה ולחיפוש בטלפונים חכמים מופעלות בהיקף עצום

> ״למעלה מ-20,000 צווי חיפוש במחשבים - ובכלל זה במכשירי טלפון ניידים חכמים - ניתנים מדי שנה. לרוב, הדבר נעשה לאחר דיון במעמד צד אחד, ובלי שתינתן לבעלי המכשירים הזדמנות נאותה לטעון באשר לנחיצות החיפוש והיקפו בטרם יבוצע״. כך פתח כ׳ השופט אלרון את פסק דינו בעניין שמעון, שניתן באמצע שנת 2021.[73]

71 משרד המשפטים (רמו"ט, מח"ש) **חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד / ספק חוץ** (27.1.2015) (קישור). ראו גם: הודעה מטעם משרד המשפטים: "התקשרות בפטור ספק יחיד עם חברת Cellebrite לרכישת ותחזוקה למערכת UFED עבור מח"ש ורמו"ט" (2021) (קישור).

72 FileVault הוא הכלי המובנה של מערכת ההפעלה Mac OS X 10.3 ואילך להצפנת קבצים או דיסקים במטרה למנוע גישה לא-מורשית אליהם (קישור).

73 בש"פ שמעון, לעיל ה"ש 4, בפסקה 1 לפסק הדין של השופט אלרון.

ואכן, חדירה וחיפוש בטלפונים ניידים הפכו לפרקטיקה נפוצה ביותר בקרב רשויות החקירה. כך למשל, בשנת 2019 התבקשו **וניתנו** כ-24,000 צווי חיפוש במכשירי טלפון נייד,[74] ובמהלכה נפתחו סך הכול כ-301,000 תיקי חקירה.[75] לצד זאת, במקרים רבים נוספים נתן הנחקר את הסכמתו לחיפוש ללא צו.

גם מנתוני המשטרה הצבאית נראה כי החדירה לטלפונים הפכה לתופעה נרחבת, כאשר רוב החיפושים נעשו בהסכמת הנחקר וללא כל צו, גם כאשר מדובר במכשירים אישיים-אזרחיים ולא צבאיים. כך למשל, בין החודשים פברואר 2014 למרץ 2015 נבדקו על ידי המשטרה הצבאית 2,499 טלפונים ניידים, כאשר רק 490 מתוכם נבדקו באמצעות צו שיפוטי, וב-2,009 המקרים הנותרים נעשו החיפושים בהסכמת החייל ללא צו. בשנה העוקבת נערכו חיפושים בטלפונים ניידים בהיקף דומה.[76]

בנוסף, צווים לפי חוק האזנת סתר זוכים לאישור נרחב יחסית מצד בתי המשפט. בעוד שבבחינת כלל תקופת הזמן בין השנים 2016–2002 עמד אחוז הבקשות שנדחו על 34%, בהתבוננות פרטנית על השנים 2016–2011 הצטמק שיעור הדחייה לאחוזים בודדים.[77] בשנת 2020 הפך המספר לזעום במיוחד – מתוך 3,692 בקשות שהוגשו ב-2020 נדחו 26 בלבד, שהן 0.7% מכלל הבקשות.[78] מגמה זו נמשכה בשנת 2021, בה הגישה המשטרה לבית המשפט 3,359 בקשות להאזנת סתר, מהן התקבלו 3,350, אשר מהוות יותר מ-99 אחוז.[79]

נתונים אלו מציגים על קצה המזלג את היקף התופעה ומחדדים את פוטנציאל הפגיעה העצום בפרטיותם של עשרות אלפי אנשים בשנה, ובהתחשב בפגיעה האינהרנטית שיש לחיפוש במכשירי טלפון חכם בפרטיותם של צדדים שלישיים, מדובר בהיקף עצום של אזרחים שמושפעים מהשימוש המשטרתי בטכנולוגיות מתקדמות לפריצה, חיפוש ומיצוי נתונים מטלפונים חכמים.

ג.3 אילו נתונים חשובים עדיין איננו יודעים

דיון אחראי וממצה בהבנה ובעיצוב של מסגרת הדין והנוהל להפעלה של כלים מתקדמים לפריצה, להעתקה ולחיפוש במחשבים ניידים ובטלפונים חכמים מחייב תשתית עובדתית מקיפה על ההיקף ועל האופן שבו מתבצעים בשנים האחרונות חיפושים בחומר מחשב, ובפרט בטלפונים ניידים,[80] ועל הערך החקירתי שלהם עבור האינטרס הציבורי באכיפת הדין, למשל כמה חיפושים בטלפונים חכמים נעשו מבלי שהחקירה הבשילה לכתב אישום.

מטבע הדברים, נתונים אלו זמינים לרשויות האכיפה בלבד ולא נחשפו מעולם באופן מלא ושיטתי.[81] על כן, לצורך דיון ציבורי וחקיקתי ממצה יש לבחון, בין היתר, את השאלות העובדתיות הבאות:

---

74 שם, בפסקה 24.

75 משטרת ישראל **השנתון הסטטיסטי** 2019 7 (2020).

76 עדי ריטיגשטיין־אייזנר "האם הסכמת הנחקר יכולה להוות מקור סמכות לחיפוש בטלפון הנייד שלו?" **מעשי משפט** ח 131, 132 (2016). הנתונים נמסרו לידי המחברת מדובר צה"ל על פי חוק חופש המידע.

77 עמיר כהנא ויובל שני "רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה" **מחקר מדיניות** 123, 34–42 (2019).

78 יהושע (ג'וש) בריינר "בכירים במשטרה: שופטים שמאשרים האזנה לא יודעים באיזה כלי המשטרה תשתמש" **הארץ** (19.1.2022).

79 צבי זרחיה ותומר גנון "היקף השימוש ברוגלות הוסתר גם בדיווחי האזנות הסתר לשנת 2021" **כלכליסט** (20.06.2022).

80 שם. משטרת ישראל טוענת כי השימוש בתוכנות ריגול אפשרי בזכות חוק האזנות הסתר. כחלק מחוק זה, המשטרה צריכה למסור לוועדת החוקה של הכנסת את הנתונים המדויקים בדבר מספר ההאזנות שבוצעו. עם זאת, משטרת ישראל אינה מספקת כחלק מנתונים אלה פירוט של הבקשות והאישורים להאזנות סתר מסוג תקשורת בין מחשבים.

81 לסקירה עכשווית, ראו: עמרי רחום-טוויג "חיפושים ממוחשבים" – על סמכויות חקירה בגישה מרחוק למחשבים ומידע דיגיטלי", **פורום עיוני משפט** מו (30.1.2022) (קישור).

איגוד האינטרנט הישראלי
ISOC-IL

שאלות לגבי הפעלת כלים טכנולוגיים למיצוי נתונים ממכשירים חכמים שנתפסו

מה היקף ההפעלה של כלים פורנזיים לחדירה ולחיפוש בטלפונים חכמים כדוגמת מוצרי Cellebrite על ידי רשויות החקירה והאכיפה השונות בישראל? כמה מתוך אלו נעשים בדרך המלך של צו שיפוטי וכמה על בסיס הסכמה? האם הפעלתם מוגבלת רק לעבירות בדרגת חומרה מסוימת? אם לא – כמה שכיח השימוש בכלים אלו בחלוקה לעבירות השונות שבמסגרתן הוא נעשה?

האם לכל אחד מגופי החקירה שמפעילים מערכות כדוגמת Cellebrite יש מדיניות ברורה בנוגע לאופן השימוש בהן, למשל בנוגע לסוג העבירות או מידת הנחיצות של האמצעי? אם אין נהלים, זה חמור במיוחד כי הם משתמשים בכלים הללו כבר שנים רבות. אם יש נהלים, האם אין הם מעורפלים להפליא, והאם הם מתייחסים למלוא החששות הקשורים לחיפושים דיגיטליים, כגון היקף החיפושים ומיקודם או שמירה ושימוש בנתונים שחולצו? בנוסף, יש לבחון האם קיימים כללים שונים לסוגי מידע רגישים יותר, וכמה גורמי חקירה מקבלים גישה למידע.

שאלות לגבי הפעלת כלים טכנולוגיים מסוג "הדבקה מרחוק" כלפי מכשירים חכמים

מה היקף ההפעלה של כלים לביצוע האזנת סתר לתקשורת בין מחשבים באמצעות "הדבקה" מרחוק, כדוגמת סייפן, על ידי רשויות האכיפה השונות בישראל?

מה האורך הממוצע של צווי האזנת סתר לתקשורת בין מחשבים, וכיצד מובטחת הסרת הגישה בסיום תקופת הצו?

האם יש טכנולוגיות נוספות של האזנת סתר לתקשורת מחשבים המיושמות על ידי גופי אכיפת חוק ואינן עוברות בחינה משפטית אובייקטיבית? זאת, למשל, על רקע פרסומים מהשנים האחרונות לפיהם משטרת ישראל מפעילה את ספקיות הגישה לאינטרנט על מנת לנטר תעבורת נתונים של אזרחי ישראל.[82]

מה פוטנציאל זיהום החקירה של מערכות אלו? בהינתן העובדה שהן משבשות את פעילותו התקינה של המכשיר, ובפרט את מערכות אבטחת המידע שלו.

שאלות נוספות על הפעלת טכנולוגיות לחדירה, לחיפוש או להאזנת סתר כלפי מכשירים חכמים

כמה מהחיפושים שבוצעו בטלפונים ניידים כללו גם מיצוי מידע מחשבונות ענן המקושרים למכשיר? אנו יודעים על מקרים לא מעטים שבהם כללה הפעלת כלים פורנזיים למיצוי מידע מטלפונים חכמים שימוש גם ביכולת זו,[83] אך היקף התופעה לוט בערפל.

כמה מהחיפושים שנעשים באמצעות טכנולוגיות פורנזיות במכשירים חכמים, וטלפונים ניידים בפרט, מניבים כתבי אישום והרשעות?

עד כמה בתי משפט נענים לבקשות חיפוש בטלפונים ניידים, תוך הבחנה בין קבלה מלאה, קבלה הכוללת קביעת תיחום נוסף לבקשה, ודחייה? הזכויות החוקתיות לפרטיות, לשמירה על כבוד האדם ולהליך הוגן מחייבות להגדיר באופן מפורט את המקומות שבהם יתקיים חיפוש ואת יעדיו. דרישה זו נועדה להגן מפני "צווים כלליים", ולמנוע מהרשויות לחטט ללא הבחנה ברכושו של אדם. כך גם בחוק סדר הדין הפלילי לגבי חיפוש בחומר מחשב. ואכן, קיימים מקרים בודדים שבהם

82 ראו למשל: עמי רוחקס דומבה "המשטרה מבקשת מספקי התקשורת אפשרות לרגל אחרי תעבורת גלישה של אזרחים" Israel Defense (13.12.2020) (קישור); "משטרת ישראל מרגלת אחר הגלישה שלנו באינטרנט" CyberCyber (12.12.2020) (קישור).

83 תפ"ח 42209-04-19 מדינת ישראל נ' סילבר (3.8.2022).

צמצם בית המשפט באופן אקטיבי את היקף צו החיפוש בחומר מחשב שהובא לאישורו, באמצעות תיחום הצו לשירותים ספציפיים בלבד (למשל, אפליקציות להעברת מסרים מיידיים בלבד, להבדיל משירותי מיקום); סוגי נתונים ספציפיים שרק אותם יורשה לחלץ מהטלפון הנייד (למשל איסור לכלול קובצי תמונה או סרטונים או היסטוריית גלישה);[84] או תיחום החיפוש לנתונים שהופקו בתקופה מוגדרת בלבד.[85] עם זאת, אין בפנינו נתונים שיאפשרו לבחון האם צמצום אקטיבי של צווי החיפוש על ידי בתי המשפט הוא פרקטיקה שגורה.

מה עולה בגורלם של הנתונים שהכלים הפורנזיים מחלצים מטלפונים ניידים ומחשבונות ענן לאחר החקירה? למשל, האם החומרים נשמרים כחומר מודיעיני שניתן להשתמש בו בחקירות אחרות? האם החומרים נמחקים במידה שתיק החקירה נסגר מחוסר אשמה? האם עקרון צמידות המטרה המוכר לנו מדיני הגנת הפרטיות חל גם על אופן השימוש בחומרים שנאספים במסגרת החקירה, חשאית או גלויה?

מה מידת הגישה של ספקיות הכלים הטכנולוגיים למידע שמתקבל מהם או למידע על הפעלתם ויעדיהם?

לצורך בדיקת הטענות שהועלו ושלשמה הוקמה הוועדה, דו"ח מררי מציג כיצד פנתה הוועדה לחברת NSO לצורך קבלת מידע האגור אצלה. לפי הדו"ח, החברה מחזיקה נתונים על אודות "כל הדבקה שבוצעה באמצעות המערכת לאורך כל שנות פעילותה במשטרה; המועד המדויק שבו בוצעה ההדבקה; והטלפון הנייד שנדבק באותו מועד".[86]

84 ראו למשל צ"א (שלום ב"ש) 30588-12-20 מדינת ישראל נ' אבקסיס (15.12.2020); צ"א (שלום ב"ש) 47580-12-20 מדינת ישראל נ' און (24.12.2020); צ"א 64974-12-20 מדינת ישראל נ' פלוני (30.12.2020); צ"א (שלום ב"ש) 68831-12-20 מדינת ישראל נ' פלוני (31.12.2020).

85 ראו למשל צ"א 5669-01-21 מדינת ישראל נ' פלוני (6.1.2021).

86 דו"ח מררי, לעיל ה"ש 39, בעמ' 29.

ד מסגרת הדין ונוהלי משטרת ישראל לפריצה ולחיפוש במכשירים חכמים

ד.1 מסגרת הדין בתהליך החקירה הסמויה: האזנת סתר לשיחות ותקשורת מחשבים

> ״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.״
>
> דו"ח ועדת מררי, 2022[87]

האזנת סתר מהווה כלי מרכזי במלחמה בפשיעה חמורה ולא אחת מהווה חוליה הכרחית ומרכזית בפעולות החקירה של רשויות האכיפה.[88] ביצועה מוסדר בחוק האזנות סתר, התשל"ט-1979. האזנת סתר מוגדרת בחוק כדליית נתונים מ"שיחה", ללא הסכמת וידיעת המשתתפים בה. נוכח הפוגענות הייחודית של פעולה זו, החוק מגביל את השימוש בה למקרים שבהם היא נחוצה לגילוי, לחקירה או למניעה של עבירות מסוג פשע. מהגדרות אלו ונוסחן ברור שכוונת המחוקק הייתה להסדיר מצב שבו מי שאינו "בעל שיחה" מאזין לשיחה המתבצעת בזמן אמת. בהתאם, בית המשפט העליון קבע את עקרון ה"בו-זמניות" כדי ללמוד האם מדובר בהאזנת סתר. כך, נקבע כי האזנת סתר משמעותה ציתות או הקלטה הנעשים בו בזמן עם קיומה של השיחה.[89]

המושג "שרשרת ההאזנה" מתאר את כלל השלבים השונים במסגרת ביצוע האזנת סתר, אשר מתחילים בשלב העלאת הצורך הראשוני על ידי הגוף המבקש לבצע האזנת סתר כלפי מטרה מסוימת ונגמרים בהפקת התוצרים שהתקבלו.[90] היחידה המזמינה פורסת בפני חטיבת הסייבר את הצורך המבצעי להאזנה מסוג תקשורת בין מחשבים. בהפקת התוצרים, בהתאם להנחיית העבודה של חטיבת הסייבר, אסור להפיק: אנשי קשר, פתקים, יומנים ורשימת אפליקציות. עם זאת, המפיקים חשופים לא רק למידע שמוגדר כתוצר של האזנת הסתר, אלא לכל המידע המגיע מהמכשיר.[91]

87 דו"ח מררי, שם, בעמ' 26.

88 דו"ח מררי, שם, בעמ' 14 ("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").

89 ע"פ 92/1497 מדינת ישראל נ' צוברי, פ"ד מז(4)177, 195 (23.8.1993).

90 דו"ח מררי, לעיל ה"ש 39, בעמ' 49 ("שרשרת ההאזנה" הוגדרה ככלל השלבים השונים במסגרת ביצוע האזנת סתר, אשר ראשיתם בשלב העלאת הצורך הראשוני על ידי היחידה המזמינה לביצוע האזנת סתר כלפי יעד מסוים, ועד לשלב הפקת התוצרים שהתקבלו מהמערכת בעניין אותו יעד).

91 דו"ח מררי, שם, בעמ' 51 ("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").

חוק האזנת סתר נפתח באיסור פלילי על ביצוע של פעולות האזנת סתר שלא על פי היתר כדין.[92] לענייננו, המקרה הטיפוסי הוא הקבוע בסעיפים 6 ו-7 לחוק, העוסקים בהיתרים לביצוע האזנת סתר לצורך מניעת עבירות. באופן מסורתי, האזנות אלו נעשות דרך מרכזיות חברות התקשורת, על פי צו האזנת סתר שניתן על ידי שופט מחוזי (נשיא / ס' נשיא אשר הוסמך על ידי הנשיא לנושא זה) בבקשה חתומה על ידי קצין משטרה בדרגת ניצב משנה לכל הפחות, ולאחר שבקשה זו הוצגה בפני השופט על ידי קצין משטרה בדרגת סגן ניצב.[93]

האזנת סתר מחייבת ברגיל צו שיפוטי, לבקשת קצין משטרה מוסמך, לאחר שבית המשפט "שקל את מידת הפגיעה בפרטיות".[94] עם זאת, סעיף 7 מאפשר לאשר במקרים דחופים האזנה למשך 48 שעות גם ללא צו; וסעיף 8 מאפשר פעולת האזנת סתר ללא צו, לשיחות שנעשו ברשות הרבים – מקום שאדם סביר יכול לצפות ששיחותיו יישמעו ללא הסכמתו – כהגדרת הסעיף. בהיתר להאזנת סתר יש לתאר את זהות האדם אשר האזנה לשיחותיו הותרה, או זהות הקו או המִתקן המשמשים או המיועדים לשמש לקליטה, להעברה או לשידור של בזק ואשר האזנה אליהם הותרה ומקום השיחות או סוגן, הכול אם הם ידועים מראש. כמו כן, יש לפרט את דרכי ההאזנה שהותרו ואת תקופת תוקפו של ההיתר, אשר לא תעלה על 3 חודשים מיום מתן ההיתר.[95] אל הוראות אלו מתווספות תקנות האזנת סתר (בקשה להיתר האזנה), התשס"ז-2007, הקובעות את סדרי הדין בדיון בבקשה להאזנת סתר ואת הפרטים שיש לכלול בבקשה ובהיתר להאזנה (ראו הרחבה בהמשך).

ככלל, נדרש שצווי האזנת סתר ינקבו ביעד ההאזנה ובמספר הטלפון המפורש שאליו הותרה ההאזנה. ואולם, המחוקק הכיר בכך שלעיתים קיימות נסיבות שבהן חלק מהמידע אינו ידוע מראש בשלב הגשת הבקשה ומתן ההיתר השיפוטי.[96] 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 ההיתר כאמור, אשר אינו מוגבל רק למספר הטלפון המסוים שצוין בהיתר, צריך להינתן במפורש על ידי בית המשפט, על בסיס כלל המידע הרלוונטי לעניין זה.[97]

ראוי לציין כי צווי האזנת סתר ניתנים על עבירות מסוג פשע, אך תוצרי האזנת הסתר יכולים לשמש גם להוכחת עבירות מסוג עוון. סוגיה זו מעלה טענה כי לעיתים אישור זה בדיעבד מהווה פגיעה ניכרת בפרטיות, בניגוד לכוונת המחוקק שכיוון לאישור שימוש בצו זה רק בעבירות חמורות.[98]

האזנת סתר לתקשורת בין מחשבים

החל משנת 1995 הורחבה ההגדרה של שיחה בחוק האזנת סתר והחילה אותה גם על האזנה לשיחה בדרך של "תקשורת בין מחשבים", כאשר "האזנה" מתייחסת לשמיעה, קליטה או העתקה של "שיחה" כאמור באמצעות מכשיר.[99]

---

92 סעיף 2 לחוק האזנות סתר.

93 חוק האזנת סתר קובע גם מנגנון לצורך אישור האזנת סתר למטרת ביטחון המדינה (סעיף 4 לחוק), ובו רשאי שר לאשר האזנת סתר לאחר פנייה מאת רשות ביטחון.

94 שם.

95 סעיפים 6(ד) ו-6(ה) לחוק; ההיתר ניתן לחידוש מפעם לפעם. דו"ח מררי, לעיל ה"ש 39, בעמ' 16.

96 דו"ח מררי, שם, בעמ' 19.

97 שם.

98 ראו למשל דנ"פ 6143/10 סמהדאן נ' מדינת ישראל (28.10.2010); רע"פ 1089/21 מ"י נ' אטיאס (14.03.2022).

99 תיקון מס' 1 לחוק האזנות סתר, התשל"ט-1979 (1995), במסגרת חקיקת חוק המחשבים.

איגוד האינטרנט הישראלי ISOC-IL

ייחודו של חומר מחשב המועבר בתקשורת בין מחשבים עומד, בין היתר, על כך שהוא נתפש בחקיקה הישראלית באופנים שונים בנוגע למועד ולאופן שבו הוא נאסף על ידי גופי החקירה. כך, 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.

ההבחנה המקובלת בין הסמכויות השונות בדין הישראלי נשענת על ההבחנה בין מידע אגור (stored communication) – הכפוף לפקודת החיפוש,[100] לבין תקשורת בתעבורה (communications in transit) – הכפופה לחוק האזנת סתר. מקובל לראות בסמכות לבצע האזנת סתר כמזו 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.[101] חומר מחשב אשר אגור במכשיר הקצה, כגון טלפון נייד או מחשב אישי, גם אם הגיע אל מכשיר הקצה על ידי תקשורת בין מחשבים (למשל דוא"ל שהועבר בתקשורת בין מחשבים אך מבוקש לגשת אליו בדיעבד לאחר שנאגר במחשב), נתפש מהותית כ"חפץ".[102]

על כן, לפי עמדת פרקליטות המדינה, איסוף מידע אשר אינו מידע שמועבר בתקשורת בין מחשבים, וכן מידע אשר נתקבל קודם למועד התקנת הכלי, אינו מהווה פעולה של האזנת סתר המותרת לפי החוק, אלא חיפוש סמוי במחשב – שאינו בסמכות המשטרה.[103] עם זאת, העמדה המשפטית של פרקליטות המדינה היא שלא ניתן לשלול באופן גורף כל פעולה של האזנת סתר הכוללת חדירה למכשיר הקצה לצורך ביצוע האזנה.[104] עוד ראוי לציין בהקשר זה את הוראות סעיף 23א(ג) לפקודת החיפוש הקובע כי "קבלת מידע מתקשורת בין מחשבים אגב חיפוש" לא תיחשב כהאזנת סתר.

בנוסף, קיימת חשיבות לקיומו של פירוט נרחב במסגרת בקשה להאזנת סתר בכלל, ולהאזנה מסוג תקשורת בין מחשבים בפרט. כפי שציינה ועדת מררי, הבנת בית המשפט את היקף הפגיעה הפוטנציאלי בזכויות אזרח הנובע ממתן היתר להאזנה מסוג מסוים, הכרחית על מנת לאפשר לו לשקול באופן מלא את ההצדקה לשימוש באמצעי חקירה הפוגע באופן כה דרמטי בפרטיותו של אדם, ולערוך 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.[105]

אולם, כפי שעולה מהטופס האחיד לבקשות להאזנת סתר של תקשורת בין מחשבים הקבוע בהנחיית העבודה של חטיבת הסייבר במשטרת ישראל, ההנחיה עד היום הייתה כי בכל פעם שיש צורך בהאזנת סתר מסוג תקשורת בין מחשבים, יש לבקש מבית המשפט את כלל סוגי התקשורת.[106] פרקטיקה זו הייתה ידועה למשרד המשפטים. לגבי יכולת מסוימת הונחתה

---

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

101 דו"ח מררי, לעיל ה"ש 39, בעמ' 21.

102 ועל כן גישה אליו אפשרית על ידי המשטרה רק באמצעות צו חיפוש במחשב לפי סעיף 23א לפקודת החיפוש, תוך ביצוע החיפוש באופן גלוי; או על ידי מתן הוראה להציג את חומר המחשב. להרחבה ראו: חיים ויסמונסקי **חקירה פלילית במרחב הסייבר** פרק ד (2015); ובתת-הפרק הבא.

103 דו"ח מררי, לעיל ה"ש 39, בעמ' 41.

104 דו"ח מררי, שם, בעמ' 26 ("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 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").

105 דו"ח מררי, שם, בעמ' 45.

106 דו"ח מררי, שם, בעמ' 47.

איגוד האינטרנט הישראלי ISOC-IL

המשטרה לשקול את נחיצותה במקרים הקונקרטיים ולא לבקשה בכל צו, וכן לגבש נוהל שיתווה את שיקול הדעת בשימוש בה. עוד המליצה ועדת מררי לשנות את הפרקטיקה הנוהגת כיום ולהסביר לבית המשפט מדוע כל אחד מסוגי התקשורת נדרש לצורך החקירה הקונקרטית ולהבהיר את הנסיבות שבהן מבוקש להפעיל האזנת סתר לתקשורת בין מחשבים, על מנת שבית המשפט יתווה את התנאים לכך.[107]

יצוין כי כל השיטות המצוינות לעיל אינן יכולות לפגוע בחסיונות על פי פקודת הראיות, כגון חסיון עו"ד-לקוח, חסיון כוהן דת, חסיון רופא/פסיכולוג/עובד סוציאלי, ואף לא בחסיונות יצירי הפסיקה, כגון חסיון עיתונאי.[108] שיחות כאלו אינן אמורות להיות מתומללות, ככל שהן קשורות לשירות המקצועי שנתן אותו בעל מקצוע. כלומר, במקרים שבהם כוהן דת, לדוגמה, היה שותף לעבירה, ניתן לקבל צו בעניינו לאחר חשיפת הפרטים המלאים אל מול השופט הרלוונטי. כמובן, תוצרי השיטות לעיל, ככל ראיה, כפופים לכללי הפסילה החקיקתיים והפסיקתיים בנוגע לראיות שהושגו שלא כדין או תוך כדי פגיעה אסורה בפרטיות.

ד.2 תהליך החקירה הגלויה: תפיסה, חיפוש וחדירה למכשירים וחומר מחשב

שלב החקירה הגלויה מתחיל עם יום ה"פרוץ", שהוא בעגה המשטרתית הרגע שבו החקירה הופכת מסמויה לגלויה, עם עיכובם לחקירה/מעצרם של מושא החקירה או אנשים מסביבתו. תהליך החקירה בנוי משלבים שונים, והפעולות המבוצעות בכל שלב אחרות ודורשות הפעלת סמכות שונה. על מנת להבין את המסגרת המשפטית הכללית ואת המשמעות השונה של אותם הצווים בשלבים השונים, חילקנו חלק זה לפי אותם שלבים בחקירה. במילים אחרות, צווי החיפוש אשר ניתנים טרם המעצר ואלה שלאחר המעצר כפופים למסגרות משפטיות שונות.

המסגרת המשפטית העיקרית לתהליך החקירה הגלויה היא פקודת החיפוש שמסדירה את השלבים השונים של התהליך, כמתואר להלן:

צו להמצאת מסמכים/חפצים

סעיף 43 לפקודת החיפוש קובע את המסגרת ואת התנאים להמצאה או לתפיסה של חפצים:

> ראה שופט שהצגת חפץ נחוצה או רצויה לצרכי חקירה או משפט, רשאי הוא להזמין כל אדם, שלפי ההנחה החפץ נמצא בהחזקתו או ברשותו, להתייצב ולהציג את החפץ, או להמציאו, בשעה ובמקום הנקובים בהזמנה.

107 דו"ח מררי, שם.

108 סעיפים 48–52 לפקודת הראיות [נוסח חדש], תשל"א-1971, סעיף 22 לתקנון האתיקה המקצועית של מועצת העיתונות בישראל. ראו גם: ב"ש 298/86 ציטרין נ' בית הדין המשמעתי של לשכת עוה"ד במחוז ת"א (1987).

צו זה ניתן על ידי שופטי שלום, לרוב לפני יום של דיוני מעצרים שבו הם תורנים, ולאחר שהשוטר מוכיח לשופט קיומו של חשד סביר המצדיק מתן צו כאמור (להבדיל מהדרישה להוכיח את הנחיצות או הרלוונטיות של המצאת המסמך או החפץ לחקירה).

צווים אלו מכילים כמעט כל מידע שאפשר לקבל, או כל חפץ שאפשר לקבלו, ואשר נשוא הצו הוא זה שמעבירו/מוסרו לידי המשטרה. כלומר צווים אלו הינם צווים המחייבים פעולה פרואקטיבית ושיתוף פעולה של מקבל הצו. בדרך זו המשטרה מקבלת מידע פיננסי רב, מקבלת רשומות מחשב קיימות מגופים ורשויות שונות, ואף שמה ידה על חפצים וראיות שונים הנדרשים לחקירה או להיות מוצגים בבית המשפט.

יודגש כי גם צווים אלו מוגבלים על ידי השופט לנושאי החקירה בלבד, ולעיתים אף לפרטים/אנשים מסוימים בתוך החקירה ולא לכולם. צווים אלו מאפשרים תפיסת החפצים/מסמכים לתקופה של עד 180 יום, ואמורים להיות מחודשים בכל פעם שתקופה זו מסתיימת.[109]

צווי חיפוש[110]

סעיף 23 לפקודת החיפוש מונה את הנסיבות ששופט רשאי ליתן בהן צו לעריכת חיפוש בכל בית או מקום: (1) החיפוש בו נחוץ כדי להבטיח הצגת חפץ לצורך כל חקירה, משפט או הליך אחר; (2) יש לשופט יסוד להניח שהוא משמש להחסנתו או למכירתו של חפץ גנוב, או שנשמר בו או מאוחסן בו חפץ שנעברה בו או לגביו עבירה, או ששימש, או מתכוונים להשתמש בו, למטרה לא-חוקית; (3) יש לשופט יסוד להניח שנעברה עבירה או שמתכוונים לעבור עבירה נגד אדם הנמצא בו.

צו החיפוש מוצא אף הוא בבית משפט השלום, במעמד צד אחד. צו החיפוש יכול שיינתן לביצוע בנוכחות שני עדים שאינם שוטרים, עד אחד או ללא עדים כלל, אך בכל מקרה מחזיק המקום אמור להיות נוכח בעת הביצוע. צו החיפוש תקף ל-30 יום מיום הוצאתו, ויכול להינתן לכתובות אחדות ואף לכל מקום שבחזקתו/בעלותו של פלוני, ובכל מקרה יוגבל לנושאי החקירה. ראוי לציין כי מגבלה זו איננה אפקטיבית במיוחד, באשר נמען הצו מקבל את הצו בלבד, ללא הבקשה, ובו רשום בדרך כלל "חקירה" ללא הסברים וללא פירוט. מנגד, השופטים מגבילים לא אחת את הצווים בפירוט החומרים הנדרשים.[111]

פקודת החיפוש אינה קובעת הגבלות בנוגע למיקום המותר לחיפוש או לסוג העבירה שבגינה מותר להמציא צו חיפוש;[112] או הוראה לגבי פסלות ראיות שהושגו שלא כדין (כך שפסילת ראיות נתונה לשיקול דעתו של בית המשפט).[113] בהתאם, רשויות החקירה נהגו לבקש (ולקבל) צווי חיפוש גורפים כלפי כל המידע שעל הטלפון הנייד, לעיתים קרובות מבלי להצביע על עילה לביצוע החיפוש.

עם עדכון פקודת החיפוש בשנת 1995 נוספה לה סמכות ייעודית להורות על חדירה לחומר מחשב, כמפורט להלן.

---

109 צווים אלו משמשים כיום גם לתפיסת נכסים – "תפיסה פסד"פית" – לצורכי חילוט עד לסיום ההליכים, ובכך "עוקפים" את המגבלה החקיקתית על תפיסת נכסים לחילוט לפי חוק איסור הלבנת הון.

110 צווי החיפוש משמשים גם כבסיס לחדירות סמויות למקומות לצורכי תיעוד והאזנה. מטיבם וטבעם צווים אלו אינם ניתנים לביצוע במעמד מחזיק המקום. כאמור, חדירות שכאלו תגובינה גם בצווי האזנת סתר, ככל שתהיה האזנת נפח אודיו במקום. משמעות הדבר, שהיחידה החוקרת מקבלת אישור מיוחד מבית המשפט לבצע חדירה למקום, להתקין אמצעי האזנה ולעיתים גם אישור לצילום מבלי ידיעת החשוד.

111 קיימים פערי חקיקה ניכרים בין המסגרת המוגדרת בחוק לשימוש בפועל בצווים אלה, כגון חיפוש מתמשך לחומרי מחשב ועוד. בסוגיות אלה נדון בחלקו השני של מסמך זה.

112 אסף הרדוף "להכשיר את הפרץ: בקשת צו חדירה לחומר מחשב לאחר חדירה שלא כדין – צו ניקוי או צו הלבנה?" **משפטים על אתר** טו 60 64–69 (תש"ף).

113 עם זאת, תוצרי החיפוש כפופים לחקיקה ולפסיקה הקובעות כללי פסילה ראייתיים. ראו למשל סעיף 139 לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב-1982; סעיף 32 לחוק הגנת הפרטיות; ע"פ 98/5121 יששכרוב נ' התובע הצבאי, פ"ד סא (1) 461 (2006); רע"פ 10141/09 בן חיים נ' מדינת ישראל (6.3.2012); תיקון מס' 19 לפקודת הראיות משנת 2022 המעגן את סמכותו של בית המשפט הדין בעניין פלילי לפסול ראיה שהושגה שלא כדין (קישור).

ד.2.א שלב ההרשאה: הנפקת צו חדירה למחשב או קבלת הסכמה

בשנת 1995, עם חקיקתו של חוק המחשבים, נחקק סעיף 23א לפקודת החיפוש אשר ייחד לראשונה את סוגיית החדירה לחומר מחשב, במקביל לכך שחוק המחשבים קבע כי הפעולות הכרוכות בכך, כגון שיבוש או הפרעה לחומר מחשב, חדירה לחומר מחשב או חדירה לחומר מחשב שלא כדין, מהוות עבירות פליליות. סעיף 23א(א) לפקודת החיפוש קובע כי הפעולה של "חדירה לחומר מחשב" (שהיא עבירה לפי סעיף 4 לחוק המחשבים) יכולה להיעשות על ידי רשויות החקירה על פי התנאים של סמכות החיפוש בכל בית או מקום, ועליה להיעשות בידי בעל תפקיד המיומן לביצוע פעולות אלו.[114] סעיף 23א(ב) לפקודת החיפוש מוסיף וקובע כי למרות התנאים הכלליים שקובעת הפקודה לביצוע חיפוש, חדירה לחומר מחשב לא תיערך אלא על פי צו שיפוטי, תוך פירוט "מטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש".

החוק מוסיף ומציין בסעיף זה כי תקשורת מחשבים שהגיעה ליחידת הקצה הנחקרת, אגב החיפוש, לא תיחשב להאזנת סתר, ובכך המחוקק קובע פרדיגמה שהשתרשה גם לאחר מכן של הבחנה בין נתונים ותקשורת במעבר בין מחשבים/יחידות קצה לבין נתונים האגורים ביחידת הקצה.[115] כך, דרך המלך לחדירה ולחיפוש בחומרי מחשב היא הגשת בקשה לצו חדירה לחומרי מחשב לפי הוראות פקודת החיפוש. צווים אלו ניתנים על ידי בית משפט לבקשת גופי החקירה, וכוללים היתר מפורש לתפיסת מחשב והיתר מפורש לחדירה אליו.

על רקע דרישת החקיקה לפרט את מטרת החדירה לחומר מחשב ולתחום את החיפוש כך שלא יפגעו בפרטיות של אדם מעבר לנדרש,[116] **נוהלי חטיבת החקירות במשטרת ישראל קובעים כי הגורם האחראי על החקירה נדרש לתחום את בקשת החדירה לחומר המחשב** הן מטעמי הגנה על פרטיות בעל ההרשאה במכשיר והן מטעמי יעילות החקירה, על פי השיקולים הבאים:[117] מעמדו של בעל הרשאת הגישה (יש לתחום את החיפוש באופן הדוק יותר כשמדובר בנפגע עבירה או עד, לעומת חשוד) וטיב החשד הנחקר (בתיקים שאינם מורכבים עם מיעוט מעורבים, וככל שזירת המחלוקת מצומצמת וברורה, הנטייה לצמצם את גדרי העיון תהיה גדולה יותר).

בדומה להאזנת סתר, בקשה למתן צו חיפוש נערכת במעמד צד אחד, באופן סמוי, מבלי שהאדם או מחזיק המקום שלגביו הוצא הצו יכול לדעת על כך מראש. עם זאת, בשנים האחרונות בתי המשפט מתייחסים באופן ספציפי לצורך בבסיס ראייתי מבוסס במיוחד כדי לאשר צו לחיפוש בחומר מחשב, לאור הפגיעה הניכרת שלו בזכויות אזרח. על פי נוהל נשיאת בית המשפט העליון מיום 13.4.2022, שופט המקבל לידיו בקשה לצו חיפוש בחומר מחשב נדרש לבחון, בין היתר, האם הבקשה כוללת את עילת החיפוש; מטרות החיפוש והטעמים העומדים בבסיס סברת החוקרים שימצאו מידע רלוונטי במכשיר; העבירות הנחקרות; הצהרה האם לבקשת החיפוש קדם חיפוש בלתי חוקי שבוצע במכשיר או אם נפל פגם משמעותי אחר בהתנהלות הרשות החוקרת; היקף החומר שמבוקש לחפש בו ותחימת החיפוש ככל הניתן (למשל לפי סוגי

114 החקיקה אינה מגדירה את המונח "בעל תפקיד מיומן", ובפועל דרישה זו מתקיימת עבור מי שעבר קורס משטרתי של "חוקר מחשב מיומן" בדרגת בסיסי או מתקדם. הנוסח שמובא פה הוא הנוסח המתוקן של הסעיף. תיקון הסעיף ב-2005: חוק לתיקון פקודת סדר הדין הפלילי (מעצר וחיפוש) (תיקון מס' 12) (חיפוש ותפיסת מחשב), התשס"ה-2005 (קישור).

115 ראו למשל: ת"פ 40206/05 מדינת ישראל נ' פילוסוף (05.02.2007) (פרשת "הסוס הטרויאני"), שם הורשעו בני זוג וכן כמה חוקרים פרטיים בהתקנת תוכנת רוגלה במחשביהן של חברות מרכזיות במשק הישראלי במטרה לאסוף מודיעין עסקי. ראיות אלה נתגלו אגב חקירה אחרת, ב"ש 90868/00 נטוויזן בע"מ נ' צבא הגנה לישראל (22.06.2000), שם נקבע כי תפיסת דואר אלקטרוני שטרם הגיע למחשבו של החשוד ומוחזק בידי ספק האינטרנט הינו בגדר חומר עתידי ולכן לא חל עליו צו החיפוש, וכי פעולה כזו יכולה להתבצע רק מכוח חוק האזנת סתר.

116 סעיף 23א(ב) לפקודת החיפוש.

117 חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124, בעמ' 6.

איגוד האינטרנט הישראלי ISOC-IL

קבצים, טווח תאריכים, מילות חיפוש והתקשרויות עם גורמים ספציפיים), והסבר בדבר הבחירה לתחום כך את החיפוש; ועוד.[118]

כמו כן, בית המשפט הכיר בכך שבנסיבות מיוחדות שבהן יש צורך לשמוע את בעל המכשיר לצורך ההכרעה השיפוטית בנוגע למתן צו אזי ניתן לקיים את הדיון במעמד שני הצדדים,[119] ומקרי עבר הראו כי כאשר הדיון מתקיים בנוכחות כל הצדדים הרלוונטיים בדיון על בקשת צו חיפוש, קיים סיכוי גבוה יותר כי הבקשה תידחה.[120]

עם כל אלו, רק לעיתים נדירות בקשות לצו חיפוש נדחות בפרקטיקה ורובם המוחלט של הצווים ניתן באופן שגרתי על סמך הצהרת המבקש ומידע מודיעיני בלבד.[121]

חרף האמור בסעיף 23א(ב) לפקודת החיפוש, אשר קובע שחיפוש יכול להיערך רק על פי צו שיפוטי, התפתח בפרקטיקה אפיק נוסף לביצוע חיפוש אף בהיעדר צו שיפוטי, על בסיס קבלת הסכמה מדעת של מושא החיפוש. בפסק הדין שניתן בעניין בן חיים[122] נקבע כי בהתקיים אחת העילות הקבועות בחוק, בסמכותו של שוטר לבצע חיפוש על גופו של אדם גם ללא צו, סמכות שיושמה בהמשך גם במקרים של חיפוש בחומרי מחשב. מאז הפך כאמור אפיק החיפוש בחומרי מחשב על בסיס הסכמת הנחקר לפרקטיקה מקובלת ונפוצה, חרף היותה שנויה במחלוקת.[123]

על פי נוהלי האגף לחקירות ולמודיעין במשטרת ישראל, ככלל יש להעדיף חיפוש בחומר מחשב על סמך צו שיפוטי, כאשר הסתמכות על הסכמה מדעת כתחליף לצו תיעשה רק כאשר יש דחיפות מיידית בביצוע החיפוש או כשלא נדרש חיפוש מעמיק או בנסיבות מיוחדות אחרות.[124] במקרים של דחיפות מיידית כאמור, החיפוש צפוי להתבצע במתכונת של "חיפוש חי" או "ידני", המתאפיינת בתיעוד מופחת וחשש מוגבר לזיהום ראייתי.

לפי הנוהל הרשמי של משטרת ישראל, הסכמה מדעת תתאפשר רק לאחר שניתן לבעל ההרשאה כל המידע הרלוונטי לגבש את הסכמתו: מהי העילה לחיפוש, מהן הסמכויות הנלוות לחיפוש ומהן זכויותיו במהלך החיפוש, למשל הזכות לנוכחות של עדים בחיפוש.[125] כמו כן, הסכמה תיתפס כהסכמה מדעת רק אם החוקר הבהיר לבעל המכשיר כי הוא זכאי שלא להסכים לחיפוש ללא צו שיפוטי וסירוב זה לא ייזקף לחובתו, וכי הוא זכאי הן להתנות את הסכמתו בתנאים שונים והן לחזור בו מהסכמתו

---

118 נוהל נשיאת בית המשפט העליון 1-18 בנושא "ממשק העבודה בין שופטים ובין גורמי תביעה וחקירה בבקשות לפני הגשת כתב אישום", פסקה 24 (קישור). עוד נקבע בפסיקה כי יש לתעד ברפרוטוקול את דיון בקשת צו החיפוש, ושעל השופטים לקבל החלטה לפי אמות המידה שנקבעו בפסקי הדין בעניין אוריך ושמעון (אוריך, פסקאות 66–77 לחוות דעתה של הנשיאה חיות; שמעון, פסקה 27 לחוות דעת השופט אלרון).

119 דנ"פ אוריך, לעיל ה"ש 1. ראו גם: במ"י 60382-05-22 תחנת משטרה לב תל אביב נ' פלונית (9.6.2022). בית המשפט סירב לקיים דיון במעמד צד אחד בבקשה לבצע חיפוש בחומרי מחשב שנתפסו, ללא מגבלות כלשהן, כאשר בחומרי המחשב עשוי להימצא חומר המצוי תחת חיסיון עורך דין - לקוח. בית המשפט קבע כי במקרה זה יש לקיים דיון במעמד שני הצדדים, ולבסוף הוציא צו חיפוש "כירורגי" המוגבל לתקופה שבה החלו העבירות לכאורה ולמילות חיפוש ספציפיות הנוגעות לפרטי המתלוננים.

120 ראו למשל, צ"ח (שלום ב"ש) 8163-01-21 מדינת ישראל נ' פלוני (6.1.2021).

121 לנתונים על אודות שיעורי הקבלה הגבוהים של בקשות לצווים מסוג זה, ראו לעיל בפרק ג.2.

122 רע"פ 10141/09 בן חיים נ' מדינת ישראל (נבו 6.3.2012).

123 ראו למשל רע"פ 9446/16 התובעת הצבאית הראשית נ' סיגאוי (19.6.2017) (בקשת רשות ערעור על פסק דינו של בית הדין הצבאי לערעורים שבו נקבע כי לצורך עריכת חיפוש נרחב בטלפון נייד, המבוצע במעבדה ובלא נוכחות הנחקר, יש צורך בהוצאת צו בית משפט המאפשר את עריכת החיפוש, וכי הסכמה של הנחקר אינה יכולה לשמש מקור סמכות לצורך כך. בית המשפט העליון דחה את בקשת רשות הערעור, בשים לב לכך שבאותו מקרה ממילא לא ניתנה הסכמה מדעת של המשיב לכך שייערך חיפוש במכשיר הטלפון הנייד שלו).

124 האגף לחקירות ולמודיעין, חטיבת החקירות נוהל 035.300.03 "נוהל תפיסה וחיפוש במחשב" (פברואר 2021), בעמ' 14 (להלן: חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב").

125 יש להבהיר לבעל ההרשאה כי זכותו שהחיפוש יתבצע בפני שני עדים שאינם שוטרים ובנוכחותו. על החוקר לקבל הסכמה מפורשת ובכתב מבעל ההרשאה לחיפוש שלא בנוכחותו או בנוכחות עדים, אלא אם לא ניתן בנסיבות העניין ובגלל דחיפותו לערוך את החיפוש בחומר המחשב בפני עדים.

בכל עת.[126] אדם עם מוגבלות נפשית או שכלית[127] לא יכול לתת את הסכמתו מדעת על פי חוק. גם במקרה של קטין לא ניתן לבצע חיפוש במחשב שבחזקתו על בסיס הסכמתו בלבד ונדרשת בנוסף הסכמתו של אפוטרופוס או אחד מהוריו, כל עוד ההורה האחר לא הביע התנגדות לחיפוש. ככל שנעשה חיפוש במכשירים חכמים או חומרי מחשב על בסיס הסכמה מדעת, יש לתעד את הסכמת "בעל הרשאת הגישה והשימוש בחומר המחשב"[128] על גבי טופס "הסכמה מדעת לחדירה".

עם חתימה של חלק זה בסקירה, חשוב להדגיש כי הסכמה לחיפוש בחומרי מחשב יכולה להיות מתוחמת לסוג נתונים או פעילות מסוימים. עם זאת, חשוב לציין כי גם כאשר בעל ההרשאה נותן את אישורו לחיפוש חלקי, לרוב כלל חומרי המחשב יועתקו, גם אלה שלא הרשה את העיון בהם, וייתכן ששמורה לצוות החקירה הזכות לפנות לבית המשפט בעתיד להתיר את העיון בקבצים נוספים, ובהתאם להתקדמות החקירה.

בנוסף, ראוי כבר בשלב זה להזכיר את כללי פסלות הראיות שהוגשו שלא כדין,[129] המשפיעים באופן ישיר על התנהלות המשטרה כבר בשלב הראשוני של קבלת ההיתר.

שאלת הסמכות לביצוע חיפוש משטרתי בחשבונות ענן המקושרים למכשיר הנתפס

בשנים האחרונות ניתן להבחין במגמה של הרחבת סמכויות החיפוש והחדירה לחומר מחשב, גם בנוגע למידע ונתונים שאינם מאוחסנים במכשיר הנחפש אלא אגורים בענן ובשרתים מרוחקים. הפסיקה הכירה באפשרות להוצאת צווי המצאת מסמכים, לרבות חומר מחשב, האגורים מחוץ לטריטוריה הישראלית מכוח סעיף 43 לפקודת החיפוש (העוסק בהמצאת חפצים, כמפורט לעיל). מהלך זה של ניתוק הזיקה בין החזקה הפיזית לחזקה דיגיטלית מודגם בפסיקת בית המשפט העליון עוד משנת 2004:

> בחיים המודרניים של זמננו הנגישות אל חפץ מסוים, אינה כרוכה בהכרח בהחזקתו הפיזית. לעיתים, יכול אדם להגיע 'בלחיצת כפתור', אל מידע המצוי בשליטתו, אך לא בהחזקתו הפיזית... דרך האינטרנט ובאמצעות שימוש בסיסמא מזהה שמאפשרת להם ולהם בלבד, נגישות מיידית אל המידע וכן את הנפקתו המיידית בצורה של מסמך. התפתחויות אלה מחלישות במידה רבה את הקשר בין הנגישות או הזמינות של חפץ לבין החזקתו הפיזית. הן מלמדות כי מהעדר החזקתו הפיזית של החפץ, אין לגזור בהכרח את היעדר הנגישות אל אותו חפץ.[130]

126 אין בחזרה מהסכמה כדי לפגוע בחוקיות הפעולות שנעשו עד לחזרה מההסכמה. אם הבעלים חזר בו במהלך החיפוש ניתן להשלים את פעולת החדירה/העתקה, אך אין לעיין בחומר שהועתק ללא הסכמה מחודשת/צו.

127 לפי חוק הליכי חקירה והעדה (התאמה לאנשים עם מגבלות שכלית או נפשית) התשס"ו-2005.

128 בגיר שיש לו הרשאת גישה ושימוש תקפה בחומר מחשב, בין שחומר המחשב מצוי בישראל ובין אם מצוי מחוץ לישראל. לא ניתן לקבל הסכמה מטעם בעל גישה **שאינו מורשה שימוש** (ספק שירות למשל). באופן דומה, במחשב מוסדי ובו חומר שסומן בידי עובד כחומר פרטי, לא ניתן להסתפק בהסכמת בעל העסק או המעביד לביצוע חדירה לחומר שסומן כפרטי. במקרה של כמה בעלי הרשאות המשתמשים במשותף במכשיר אחד, יכול כל אחד מהם להסכים לחדירה לחומר המחשב, במידה שלא התעוררה התנגדות מצד אחד השותפים, ובלבד שהוא בעל הרשאה לחלק במחשב שלגביו ניתנה ההסכמה. במידה שקיימת הפרדה בין המשתמשים במחשב, למשל על ידי פרופילים שונים של משתמשים, הסכמתו של האחד אינה מאפשרת חדירה לחומר המחשב תחת פרופיל המשתמש של האחר.

129 ראו המקורות לעיל בה"ש 113.

130 ע"פ 1761/04 שרון נ' מדינת ישראל, פ"ד נח(4) 9, 18 (2004). ראו גם: חקירה פלילית במרחב הסייבר, לעיל ה"ש 102, פרק ג: התפישה הטריטוריאלית באשר לאיסוף ראיות בחקירה פלילית במרחב הסייבר.

על רקע זה, בשנים האחרונות משטרת ישראל מבצעת חדירה לחשבונות ענן ומידע מרוחק אשר למכשיר הנתפס יש הרשאות גישה אליהם (באמצעות "התחזות" לבעל החשבון), ללא הסמכה מפורשת בחקיקה ראשית אלא באמצעות הסתמכות על המסגרת המשפטית של סעיף 23א לפקודת החיפוש ועל "היתר" מטעם מְנַהֵל מחלקת הסייבר בפרקליטות המדינה לבקש ולבצע "צווי חדירה לחומר מחשב שיכללו גישה לחומרי מחשב מרוחקים המקושרים אל מחשבים התפוסים כדין בישראל", במקרים מוגדרים כמו:

- חדירה לארנקים וירטואליים וארנקים דיגיטליים שבחזקת החשודים.
- תכתובות או שיחות של חשודים באמצעות אפליקציות מסרים מיידיות.
- חדירה לחומרי מחשב בשרתים מרוחקים המשמשים על פי החשד לניהול בסיסי נתונים של המיזם העברייני הנחקר.

דוגמה להיתר כזה שניתן עוד בשנת 2019 ממחלקת הסייבר בפרקליטות המדינה לראש יחידת הסייבר וראש חטיבת סיגינט-סייבר, שעליו חתום שופט בית משפט שלום, מצורפת כנספח ב. ההיתר מטעם הפרקליטות מדגיש כי על צו החקירה במקרים אלו לכלול התייחסות מפורשת לכך שהוא כולל חדירה לחומרי מחשב המקושרים למכשיר התפוס בישראל "בכל מקום בהם נמצאים אותם חומרי המחשב"; יש לאשר נוסח הבקשה לצווי חדירה כאמור עם מנהל מחלקת הסייבר בפרקליטות; ועל החדירה להתבצע בנוכחות המחזיקים של המחשבים או הטלפונים הניידים התפוסים, אלא אם כן יוותרו מרצונם הטוב והחופשי על נוכחותם.

לאחר שניתן צו חדירה או מתקבלת הסכמה, מתחיל תהליך החדירה והחיפוש בתפיסה של מכשיר היעד.

ד.2.1 שלב התפיסה הפיזית של המכשיר הנחפש

שלב זה עוסק בתפיסה הפיזית של מכשיר המחשב, הטלפון או התקן האחסון הדיגיטלי, טרם ביצוע פעולות העתקה וחדירה לחומרי המחשב. לפי הנחיית פרקליט המדינה מספר 7.14 משנת 2020,[131] יש קושי בהגבלת פעילויות רשויות החקירה בשלביהן הראשונים, ולכן ההגבלה המשמעותית יותר תבוצע בשלב העיון והניתוח וכן בשלב ההפקה של תוצרי החיפוש. **על כן, ניתן ללמוד מהנחיה זו כי הנטייה להגביל את פעולות החקירה בשלב התפיסה מצומצמת יותר.**

סעיף 32 לפקודת החיפוש קובע כי רשויות החקירה מוסמכות לתפוס "חפץ" (לרבות מחשבים וחומר מחשב), כאשר עיון בו מחייב צו לפי סעיף 23א לפקודה.[132] בנוסף, סעיף 43 לפקודת החיפוש קובע כי בית המשפט יכול להורות לאדם להמציא חפץ הנחוץ לצורכי חקירה או משפט. עם זאת, במקרה כזה החפץ אינו מגיע לרשויות החקירה אלא לבית המשפט.[133]

---

131 הנחיית פרקליט המדינה 7.14 עקרונות הפעולה בנוגע לאופן התפיסה, החיפוש, ההעתקה והעיון במחשבים ובחומרי מחשב, תיעודם והעמדת התוצרים המהווים 'חומר חקירה' לעיון ההגנה בסעיף 6 (להלן: "הנחיית פרקליט המדינה 7.14").

132 עוד ראו סעיף 32(ב) לפקודת סדר הדין הפלילי בכל הנוגע לתפיסת חומר מחשב מוסדי; דו"ח מררי, לעיל ה"ש 39, בעמ' 22.

133 דו"ח מררי, שם ("סעיף 43 לפקודת סדר הדין הפלילי קובע את הסמכות של בית המשפט להורות לאדם על הצגת חפץ הנחוץ לצורכי 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").

על כן, תפיסה של "מחשב" (לרבות טלפונים ניידים ומכשירים חכמים) על ידי רשויות החקירה יכולה להיעשות גם ללא צו חיפוש וללא הסכמה, ככל שלא מדובר במכשיר המשמש עסק (מחשב מוסדי).[134] עם זאת, פעולת החדירה לחומר מחשב מחייבת צו או הסכמה מדעת, כפי שתואר בתת-הפרק הקודם.

טרם החדירה/העתקת החומרים, צוות החקירה נדרש למלא **"טופס לוואי" – טופס הזמנת מיצוי ראיות ממחשב**, שמפרט **מראש** את הפעולות הדרושות לביצוע ואת סוגי הסינונים הנדרשים בהתאם לצורכי החקירה. לטופס תצורף ההרשאה לביצוע – צו חיפוש בתוקף / טופס חיפוש בהסכמה מדעת.[135]

נוהלי משטרת ישראל לשלב תפיסת המכשירים מכתיבים את סדר הפעולות הבא במטרה להבטיח את תקינות ומהימנות הפעולה ותוצריה:[136] אבטוח הזירה; תפיסת המטענים הקיימים; כיבוי המכשירים הרלוונטיים וניתוקם מהחשמל במידת הצורך; הצמדת תוויות למכשירים; תיעוד בצילום לצורך שחזור ההתקנה של הכבלים (בנוסף, כלל החיפוש יתועד על ידי צוות החיפוש ויתועד בדו"ח פעולה שיימסר לצוות החקירה); אריזה, שינוע ואחסון.

במידה שלא ניתן לתפוס את המכשיר או שקיים צורך מיוחד לבצע עיון ראשוני בחומרי מחשב כבר בזירה, ניתן לבצע מנעד של פעולות על ידי בעל תפקיד מיומן בלבד: העתקה בלבד; דפדוף בטלפון סלולרי בזמן אמת (בכפוף לקיומם של צו / הסכמה מדעת); וחדירה בזמן אמת (Live Forensic) – שעשויה לחייב תיעוד מוגבר.

פעולות אלה תבוצענה במקרים הבאים: קיים צורך דחוף לבצע עיון ראשוני כבר בזירה לאיתור קבצים הנחוצים באופן מיידי לצוות החקירה; לצורך איזון בין צורכי החקירה לפגיעה בעסק כתוצאה מהתפיסה, ניתן להסתפק בחדירה למחשב בזירה הממוחשבת; כאשר מדובר ברשת או בשרת; או כאשר ניתן לתפוס את המחשב או קיים קושי טכנולוגי לבצע העתק פורנזי ולכן יש לעבוד על המקור.

תפיסה בכוח (במקרים שבהם חומר המחשב מוגן באמצעות אמצעי אבטחה ביומטריים):[137]

ככלל, השימוש בכוח הוא בגדר סמכות נלווית לחיפוש בחומר המחשב ועל כן כוחות השיטור רשאים להפעיל כוח לצורך מימוש מטרת החיפוש במידה שבעל המכשיר מסרב לסייע בפתיחתו, בהתקיים התנאים הבאים:

(א) קיים צו מטעם בית משפט המאשר את פעולות החיפוש והחדירה; (ב) הקצין הממונה אישר את הפעלת הכוח; (ג) בעל המכשיר הוזהר שאם יתמיד בסירובו עורך החיפוש רשאי להשתמש בכוח כדי להתגבר על אמצעי האבטחה; ו-(ד) השימוש בכוח הוגבל לכוח סביר, ובוצע במידה המינימלית הנדרשת לשם חדירה לחומר מחשב. בנוסף, חל איסור על הפעלת כוח שיש בו כדי לגרום לפגיעה בגוף.

134 סעיף 23(ב) לפקודת החיפוש ("על אף הוראות פרק זה, לא ייתפס מחשב או דבר המגלם חומר מחשב, אם הוא נמצא בשימושו של מוסד כהגדרתו בסעיף 35 לפקודת הראיות... אלא על-פי צו של בית משפט"). על פי נוהלי חטיבת החקירות של משטרת ישראל, מחשב שאינו מוסדי ניתן לתפוס גם ללא צו או הסכמה מדעת אם מתקיימת עילת תפיסה (למשל מחשב גלוי וקיים יסוד להניח שמכיל ראיות רלוונטיות). ברם, על מנת לחדור אליו יש צורך בצו/הסכמה מדעת (כפי שיפורט בהמשך). יש להשיב את המחשב תוך 30 יום (בייחוד אם החומר הרלוונטי ניתן להפרדה מהמכשיר עצמו, כגון כונן קשיח), אך תקופת החזקה זו ניתנת להארכה ללא הגבלה. מחשב מוסדי (בשימוש של מוסד) ניתן לתפוס רק אם ניתן צו בית משפט המתיר את התפיסה, למשך 48 שעות שלא במעמד המחזיק (ניתן להארכה לפני תום המועד, בכפוף לדיון). אם לא ניתן להפריד את חומר המחשב, ניתן להחזיקו לתקופה של 180 יום מהתפיסה. ראו: חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124, בעמ' 8. הפסיקה נוטה לראות טלפונים ניידים כמחשב מוסדי נוכח תפקידם המרכזי בשגרת הפעילות העסקית, אף אם הם משמשים גם את בעליהם לשימושים אישיים. ראו למשל צ"א שלום (ת"א) 16162-10-14 משטרת ישראל נ' קוריס (2014); ה"ת (שלום נצרת) 70495-02-21 מדינת ישראל נ' ד.ה (2021) **("היה על היחידה החוקרת להצטייד מבעוד מועד בצו שופט לתפיסת המחשב או חומר המחשב בטרם נתפס מכשיר הטלפון הנייד... לא היה זה בסמכותו של השוטר לתפוס את מכשיר הטלפון הנייד מרגע שעורך הדין ציין בפניו כי מדובר במחשב מוסדי").**

135 דו"ח מררי, לעיל ה"ש 39, בעמ' 8.

136 דו"ח מררי, שם, בעמ' 18–20.

137 דו"ח מררי, שם, בעמ' 16.

השאלה האם חשוד אשר רשויות האכיפה לא הצליחו לפרוץ למכשיר הנייד שלו יכול להיות מחויב "לפתוח" את נעילת המכשיר על אף החיסיון מפני הפללה עצמית התעוררה לאחרונה בעניין **זינו**, אך לא נקבעה בה הלכה מנחה.[138] עם זאת, בפסק הדין הסתמך השופט עמית על ספרו "חסיונות ואינטרסים",[139] שם כתב שלדעתו **חשוד רשאי לסרב לשתף פעולה בפתיחת הטלפון הנייד שלו גם כאשר מדובר בשימוש בטביעת אצבע, או בזיהוי פנים.** בתי המשפט גם דנו בשאלה האם חוקרים יכולים להפעיל כוח על מנת שחשוד יפתח את מכשיר הטלפון הנייד הנעול שלו. **במקרים מספר הוכרע כי אף על פי שהחוקרים קיבלו צו לצורך חיפוש במכשיר הנייד, אין הם רשאים להפעיל כוח לצורך פתיחת המכשיר כאשר הכלים הטכנולוגיים העומדים לרשותם אינם מספקים.**[140] מנגד, ישנה עמדה שטוענת שחיסיון מפני הפללה עצמית קיים רק כאשר הסיסמה למכשיר הינה קוד, וכי רשויות החקירה יכולות להפעיל כוח במקרים שהמכשיר המבוקש נעול בעזרת טביעת אצבע או כלי ביומטרי אחר.[141]

השבת התפוס טרם ההליך הפלילי העיקרי

חפץ או מכשיר תפוס שנמצא בו חומר חקירה רלוונטי או שטרם נבדק יוחזר תוך 6 חודשים מיום התפיסה, אלא אם הוארכה תקופת ההחזקה. אם נמצא חומר רלוונטי, התפוס המקורי יוחזר בתנאי שכל החשודים בתיק חתמו על התחייבות שלא לדרוש לפסול את הראיות שנמצאו בתעתיק שבידי המשטרה בהתאם לכלל הראיה הטובה ביותר. בפועל, המחשב לא יוחזר במידה שטרם בוצעה העתקה, במידה שהמחשב מכיל חומר אסור להחזקה או במקרה שהמחשב שימש לביצוע עבירה ומיועד לחילוט.

> ”תפיסת חפצים אינה פעולה של מה בכך - קל וחומר מקום שבו מדובר בתפיסת מכשירי טלפון ניידים, אשר מדור לדור הולכים ומשתכללים, ומכילים מידע אישי רב על האדם, על זהותו, על מחשבותיו, הגיגיו ורעיונותיו; כפועל יוצא, נוכח עוצמת הפגיעה הגלומה בה, תפיסת מכשירי טלפון ניידים לא תֵעשה אלא במידה ובמשוּרה, כאשר נמצא כי קיים צורך ממשי בכך, ולאחר מחשבה קפדנית. בהתאם, שומה על ביהמ"ש לשקול בקשה להחזרת תפוס שכזה בזהירות רבה, בדקדקנות, מתוך התחשבות בפגיעה הקשה הנובעת הימנה.”
>
> **בש"פ 5974/21, קובי נ' מדינת ישראל (2022)**

כלומר, בדין הקיים בישראל אין הבדל בין השבת טלפון חכם או מחשב שנתפסו לבין השבת חפצים פשוטים, מעבר להגבלה על תפיסת מחשב מוסדי.[142] עם זאת, פסיקת בית המשפט העליון מהעת האחרונה מדגישה כי נוכח היקפי המידע האישי הטמון בטלפונים ניידים, רשויות החקירה ובתי המשפט נדרשים להתייחס באופן קפדני יותר לתפיסה או להחזרה שלהם:[143]

138 בש"פ 6155/21 זינו נ' מדינת ישראל (10.10.2021).
139 יצחק עמית **חסיונות ואינטרסים מוגנים – הליכי גילוי ועיון במשפט האזרחי והפלילי** 889 (2021).
140 ראו במ"י (שלום ת"א) 40333-12-20 משטרת ישראל נ' בר ציון (18.12.2020); מ"י (שלום ראשון לציון) 55518-04-21 מדינת ישראל נ' אבו גאמע (26.4.2021).
141 ראו חיים ויסמונסקי ועמוס איתן "השימוש בכוח סביר לשם התגברות על הגנת סיסמה והצפנה: הצדקות וביקורת" **הסניגור** 268 (2019).
142 להגדרת המונח מחשב מוסדי ומשמעויותיו, ראו לעיל ה"ש 134.
143 בש"פ 5974/21 קובי נ' מדינת ישראל, פס' 12 (10.1.2022).

איגוד האינטרנט הישראלי ISOC-IL

ד.2.ג שלב הפריצה והעתקת נתונים מהמכשיר התפוס

על פי הנחיית פרקליט המדינה, ההגבלות שניתן להחיל גם על שלב זה מצומצמות.[144] למעשה, מאחר שצו החדירה מגביל את שלב העיון בחומרי המחשב ואינו חל על תהליך ההעתקה עצמו, **כל חומרי המחשב האגורים במחשב יועתקו בהעתקה פורנזית**, גם מעבר לגדרי צו החדירה.[145] שלב זה יתועד בדו"ח בדבר ביצוע העתקה של חומרי המחשב התפוסים.

ההעתקה תתבצע רק בידי בעל תפקיד מיומן, לאחר שווידא את רישום הפריטים בטופס הלוואי ואת קיומו של צו שיפוטי/טופס הסכמה מדעת לחיפוש.[146] ייתכן שההעתקה תבוצע בעזרת מוצר או שירות של גורם אזרחי.[147]

שלב זה יתבצע בנוכחות שני עדים או בנוכחות בעל הרשאת הגישה עצמו לבקשת בעל הרשאת הגישה. ברם, בנסיבות המתאימות לא ינכחו עדים,[148] ובמקרים אלו חלה חובת תיעוד מוגברת מטעם הצוות החוקר.

זכות החשוד לקבלת העתק: כבר בשלב זה עומדת לבעל ההרשאה במכשיר שנתפס זכות לקבלת העתק מחומר המחשב, מתוקף זכותו הקניינית על החומרים[149] ומתוקף סעיף 32א לפקודת החיפוש. עם זאת, הרשות החוקרת יכולה לדחות את מימושה של הזכות אם מתקיים אחד מהמצבים הבאים (ניתן לערעור): החזקת החומרים המבוקשים אסורה; יש חשש שיובילו לשיבוש החקירה; קיים חשש סביר שההעתקה תשמש לביצוע עבירה.[150]

בנוסף, הרשות החוקרת בוחרת את סוג פלט ההעתק שמקבל בעל המכשיר, לעיתים באופן המגביל משמעותית את גישתו למידע האגור במכשיר או למידע לאחר מיצוי, כאמור.

ד.2.ד שלב הניתוח והעיון באמצעות טכנולוגיה פורנזית

כפי שפירטנו בפרקים הקודמים, רשויות אכיפת החוק בישראל משתמשות בטכנולוגיות המתקדמות של חברת Cellebrite ואחרות על מנת לנתח ביעילות את הנתונים מהמכשירים הנחפשים וחשבונות הענן המקושרים אליהם. בסופו של דבר, היכולת להעתיק כמות עצומה של נתונים מטלפון סלולרי אינה מועילה אם אי אפשר לחפש בהם ביעילות.

בדין הישראלי, שלב זה מותנה בקיומו של צו לחיפוש בחומרי מחשב או בהסכמתו של בעל ההרשאה. העיון אינו כרוך בחדירה או בפריצה מחדש למכשיר, מכיוון שכל המידע הזמין על המכשיר מועתק לאחר החדירה הראשונית (ראו לעיל בתת-הפרק הקודם). לכן, לשיטת פרקליטות המדינה, נראה ששלב העיון אינו מוגבל בזמן ויכול להיעשות על ידי כל בעל תפקיד רלוונטי לחקירה.[151] **לפי הנחיות פרקליט המדינה בנושא זה**, מטעמים חוקתיים ומעשיים, על רשויות האכיפה לשקול לבקש צווי חדירה אשר יהיו מצומצמים יותר מאשר כלל הקבצים התפוסים, שיאפשרו פחות גישה למידע במקרים שבהם צמצום זה אינו פוגע באפקטיביות החקירה. לפי ההנחיות, הגבלת היקף המידע הנגיש תמנע פגיעה עודפת בפרטיות של

144 "הנחיית פרקליט המדינה 7.14", לעיל ה"ש 131, בסעיף 6.
145 חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124, בעמ' 7.
146 שם, בעמ' 10; סעיף 23א(א) לפקודת החיפוש.
147 חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124 , בעמ' 21.
148 כאשר נסיבות העניין ודחיפותו אינן מאפשרות את נוכחות העדים; כאשר שופט התיר בצו את קיומה של החדירה ללא נוכחות העדים לבקשת הצוות החוקר, מחשש לפגיעה במטרות החיפוש והחקירה או בשיטות ואמצעי החקירה; כאשר בעל ההרשאה התיר בכתב כי החדירה תבוצע ללא נוכחות עדים (שם, בעמ' 10).
149 "הנחיית פרקליט המדינה 7.14", לעיל ה"ש 131, בסעיף 17.
150 שם, בסעיף 16.
151 חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124, בעמ' 11.

איגוד האינטרנט הישראלי ISOC-IL

מחזיק המידע וצדדי ג' ותגביר את היעילות של הרשויות בכך שלא תצטרכנה לסווג חומר מיותר.[152] עם זאת, בשל המגבלה הטכנולוגית לתחם את חילוץ הנתונים ממכשיר היעד, ברוב המקרים תיחום עשוי להיחשב כפגיעה באפקטיביות החקירה.

ההנחיות מבחינות בין שלושה שלבים שונים בחקירה (תפיסת החומר, העתקת החומר ועיון וניתוח החומר), ומבהירות שבעוד שבשניים הראשונים ייתכן שאיסוף כלל החומר דרוש לצורך ניהול החקירה והכרחי עקב מגבלות טכניות, בשלב השלישי ניתן ואף נדרש לעיתים להגביל את יכולת העיון והפקת החומר שנאסף. כיוצא מכך, ההנחיות מבהירות שבמקרים המתאימים יש להטיל מגבלות אלו מראש, כבר בשלב בקשת הצו לחדירה.[153]

סדר הפעולות הקבוע בנוהלי משטרת ישראל:

א. **העברת החומר המועתק לחוקר:** בעל התפקיד המיומן ימסור, ככל הניתן, לחוקר המטפל בתיק **העתק מסונן ומצומצם** אשר יכלול רק את חומר המחשב שהותר לעיון על פי הצו. ככל שקיימת מגבלה טכנולוגית על ביצוע סינון וצמצום בהתאם להוראות הצו, ויימסר העתק רחב יותר מהיקפו של הצו, **החוקר המטפל לא יעיין ויפיק חומרי מחשב מעבר למה שהותר בצו.** תוצרים חזותיים (למשל תמונות) מועברים ישירות לתיק החקירה.[154] ככל שהצו אינו מתוחם ולא מדובר בכמויות גדולות של חומר, **תבוצע בחינה אנושית של כלל חומרי המחשב.**[155]

ב. **חיפוש מושכל:** במידה שקיימות כמויות גדולות של חומר המקשות על עיון אנושי בכל היקף החומר המותר לעיון, החוקר יבצע פעולות של חיפוש מושכל על פי מילות חיפוש / סוגי קבצים / פרק זמן / מעורבים.[156]

אפשרות לבחינה מדגמית:[157] במידה שגם לאחר תוצאות הסינון החוקר נותר עם כמויות גדולות של מידע, הוא רשאי לערוך **בחינה מדגמית** של המידע שהתקבל על מנת לאפשר עיון אנושי מבלי להכביד על גוף החקירה באופן בלתי סביר.

ג. **הרחבת החיפוש למעגל ההקשרי של חומר שנמצא רלוונטי:**[158] כאשר במהלך החיפוש בחומרי המחשב נמצא ממצא מסוים אשר עשוי להיות קשור לנושא החקירה, על רשות החקירה לבדוק האם ניתן לתור אחר ה"מעגל ההקשרי" של התוצר הרלוונטי: היינו כל חומר נוסף שיכול לנבוע ממנו ולהיות רלוונטי לחקירה, וזאת על מנת לבחון את היתכנותן של ראיות נוספות, בעלות משקל מזכה או מפליל. הכוונה היא להרחיב את החיפוש למשל לתכתובות נוספות בין הצדדים, קבצים רלוונטיים שנוצרו בסמוך למועד יצירת הקובץ הרלוונטי וכדומה. קביעת "המעגל ההקשרי" תיקבע לפי נסיבות המקרה מתוך התחשבות מיוחדת **בשיקולי הגנה על פרטיותם של הצדדים המעורבים וצדדים שלישיים.** אם צו החדירה לחומר המחשב כלל מגבלות בדבר היקף החומרים המותרים בעיון ובהפקה, הדבר ישליך על האפשרות לתור אחר המעגל ההקשרי, ועל כן תיתכן בשלב זה בקשה להרחבת הצו.

152 "הנחיית פרקליט המדינה 7.14", לעיל ה"ש 131, בסעיף 6.

153 שם, בסעיף 7.

154 חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124, בעמ' 11.

155 בכך, אופן היישום של הוראות סעיף 74 לחסד"פ בנוגע לחיפוש בחומרי מחשב שונה מאופן יישומו של הסעיף בנוגע להאזנת סתר – בעוד שבכל הנוגע להאזנת סתר המפיק מקשיב ומסווג את כל השיחות הנקלטות במסגרת היתר ההאזנה, בחומרי מחשב ניתן לערוך "חיפוש מושכל" שבמהלכו יסונן החומר מבלי שהחוקר יעיין בו בפועל.

156 הנחיה זו מתבססת בחלקה על פסק דינו של השופט עמית בפסק הדין בעניין פישר, לעיל ה"ש 17.

157 חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124, בעמ' 12; "הנחיית פרקליט המדינה 7.14", לעיל ה"ש 131, בסעיף 13.

158 שם.

איגוד האינטרנט הישראלי ISOC-IL

ד. השמטת החומר שנמצא בלתי רלוונטי:[159] כל תוצרי הביניים של פעולות הסינון של חומרי המחשב שנתפסו ושנמצאו בלתי רלוונטיים לחקירה – אינם בבחינת "חומר חקירה", ולכן אין לאפשר לתביעה ולהגנה לעיין בהם. יחד עם זאת, להגנה שמורה זכות עיון מלאה, בכלל החומרים שנתפסו, לאחר הגשת כתב האישום. התפוס יוחזר לאדם שממנו נתפס, לצד דו"ח המתעד את פעולות העיון שנערכו בו והובילו למסקנה בדבר אפיונו כבלתי קשור לנושא החקירה. לפי הנחיית פרקליט המדינה, אין הצדקה לשמור עותק פורנזי של חומרים אלו.

ה. תיעוד:[160] על רשויות החקירה לתעד את הפעולות שבוצעו על ידן בעת חיפוש בחומרי מחשב באופן שיאפשר לתביעה, להגנה ולבית המשפט להתחקות אחר מהלכי החיפוש ולאפשר בחינה בדיעבד האם לא נשמטו חומרים העשויים לסייע להגנה. **עם זאת, התיעוד לא יכלול את השיקולים** שעמדו בבסיס ההחלטות לערוך את פעולות הסינון השונות. התיעוד יכלול בין היתר את הנושאים הבאים: תהליך ההעתקה של חומר המחשב המקורי שנתפס והיקפו, מילות החיפוש שנעשה בהן שימוש ופעולות סינון ותיחום נוספות. על חלק מפעולות התיעוד ייתכן שיחול לשיקול דעתה של הרשות החוקרת חיסיון מחשש לחשיפת שיטה ואמצעים או חשיפת זהותם של מקורות מודיעיניים.

ו. מיפוי:[161] בנוסף, מיפוי של חומרי המחשב שנתפסו בתיק ומותרים לעיון בהתאם לגדרי צו החיפוש יועבר **לידי התביעה, ולעיון ההגנה** לביקורת על פעולות החקירה והצעת פעולות נוספות. ככל שניתן מבחינה טכנולוגית ואפשרי במאמץ סביר, המיפוי יכלול: שמות משתמשים, נפח אחסון הזיכרון שבשימוש לעומת הנפח הכולל, פירוט הכוננים ומספר הקבצים הקיימים. בנוסף, ניתן לכלול רשימה של האפליקציות שנמצאו מותקנות על המחשב ורשימת אנשי קשר פעילים, **אך לא תופק רשימה של כלל הקבצים במחשב.**

ד.3 שלב ההליך הפלילי: חסיונות והעברת חומרי חקירה וראיות לתביעה ולהגנה

בשלב זה יועברו תוצרי החיפוש של היחידה החוקרת, לצד דו"חות התיעוד והמיפוי השונים, לידי רשויות התביעה. למעשה, התביעה אינה מקבלת את תיק חקירה הכולל העתק מלא של חומר המחשב האגור במכשירים התפוסים, אלא את פלט תוצרי החיפוש ("מיצוי") שנערך בחומרים הרלוונטיים לעבירות שעליהן הוזהר החשוד.

לפי הנחיות פרקליט המדינה, לצד תוצרי החיפוש במחשב לתיק החקירה ייכנסו גם החומרים הבאים:

1. צו החדירה לחומר המחשב, לרבות הבקשה להוצאת הצו, או טופס הסכמה מדעת לחדירה לחומרי המחשב, החתום בידי מחזיק המחשב.
2. דו"ח בדבר ביצוע העתקה של חומרי המחשב התפוסים.
3. דו"ח החיפוש בחומרי המחשב, המתעד את ביצוע החיפוש, בהתאם לקבוע בסעיפים 14–16 להנחיית פרקליט המדינה בנוגע לשלב החקירה.
4. דו"ח בדבר מיפוי של חומרי המחשב התפוסים: "רשימת כל החומר" בנוגע לחומרי המחשב שנמצאו.

---

159 שם;

160 "הנחיית פרקליט המדינה 7.14", לעיל ה"ש 131, בסעיפים 7, 9.

161 חטיבת החקירות, "נוהל תפיסה וחיפוש במחשב", לעיל ה"ש 124, בעמ' 13; "הנחיית פרקליט המדינה 7.14", לעיל ה"ש 131, בסעיף 24; הנחיית פרקליט המדינה 15.7 "יישום הוראות סעיף 74 לחוק סדר הדין הפלילי [נוסח משולב] התשמ"ב-1982 על תוצרי חיפוש בחומרי מחשב – עבודת התובע" (להלן: "הנחיית פרקליט המדינה 15.7"), בסעיף 5.

בשלב זה, התביעה רשאית לבצע שתי פעולות:

סינון חומר החקירה:[162] ככל שנמצא כי חומרי מחשב מסוימים שהופקו בידי היחידה החוקרת אינם רלוונטיים, התובע רשאי להוציאם מתיק החקירה. ברם, עם העברת רשימת חומרי החקירה לעיון ההגנה, יש להותיר חומרים אלה ב"רשימת כל החומר" המועברת לעיון ההגנה (בכפוף לחריגים שבדין).

השלמות חקירה:[163] ככלל, תובע אינו רשאי לערוך חיפושים עצמאיים בחומרי מחשב שלא הוגדרו כחומרים העשויים להיות קשורים לחקירה. לכן, לאחר שהתובע קורא את חומרי החקירה, הוא רשאי לבקש מהיחידה החוקרת לבצע השלמות חקירה: לבצע חיפושים נוספים, להציע חיתוכים מסוימים, להרחיב את המעגל ההקשרי של פרט מידע מסוים (בכפוף לשיקולי פרטיות של מעורבים נוספים שמנחים את פעולות המעגל ההקשרי כאמור) או להרחיב את היקפי הבדיקה המדגמית. לשם ביצוע השלמות החקירה נדרש צו חיפוש ועיון מעודכן לגדרי החומר המבוקש.[164] דבר קיומה של בקשת השלמה יופיע במסגרת "רשימת כל החומר" בתיק החקירה אף על פי שאינה בגדר "חומר חקירה".

שלב ביניים: שקילת חיסיון שיטה ואמצעים טרם העמדת חומרי החקירה לעיון ההגנה

בשלב זה נערכת ישיבת חסיונות לצורך הגשת בקשות לתעודת חיסיון על חומר שהוא חלק מחומר חקירה או על חומר אחר שיש חובה לגלותו, אם התקיימו כל התנאים האלה: יש חשש ממשי שפרסום החומר עלול לפגוע בעניין ציבורי חשוב ואין דרך אחרת למנוע את הפגיעה בעניין הציבורי החשוב. כלומר, דיון בדלתיים סגורות, העדת עד בתחפושת או כל דרך או אמצעי אחרים לא ימנעו את הפגיעה; אין החומר מרכזי וחיוני להגנת הנאשם והעניין הציבורי שבאי-גילוי החומר עולה על הצורך לגלותו לשם עשיית צדק. **ראוי לציין כי פקודת המשטרה דורשת לצמצם, ככל שניתן, את תחולת הבקשה לאי גילויו של חומר, ויש לייחד את הבקשה לחומר המינימלי שגילויו יגרום את הפגיעה.**[165]

בשלב זה, חומרי המחשב שנתפסו בתיק יועברו לעיון ההגנה בהתאם לשני מצבים:[166]

חומרי המחשב שנתפסו בתיק הם בבעלות הנאשם בלבד: במצב זה יקבל הנאשם העתק מלא של חומרי המחשב שנתפסו מרשותו מתוקף זכותו הקניינית על החומר,[167] למעט החומרים הבאים:

- חומרים האסורים בהחזקה (למשל פרסומי תועבה) **– בהם תתאפשר להגנה זכות עיון בלבד.**
- חומרים הנהנים מחסינות על פי דין, לרבות הלכה פסוקה כגון חיסיון רופא-מטופל או חיסיון מטעם אינטרס הציבור. **בחומרים אלה לא תתאפשר להגנה אף לא זכות עיון.**

162 שם, בסעיף 12.

163 שם, בסעיפים 13–15.

164 כאשר החומרים המבוקשים הם מעבר לגדרי המותר לעיון בצו החדירה המקורי או כאשר היחידה החוקרת לא שמרה העתק פורנזי מלא של חומר המחשב וחיפוש משלים יצריך חדירה מחדש, הרשות החוקרת תצטרך להגיש בקשה להרחבת צו החיפוש או להנפקת צו חיפוש חדש מבית משפט על מנת לבצע את החיפושים.

165 למשל, אם החומר שגילויו עלול לפגוע בעניין ציבורי חשוב נמצא בחלק אחד של מסמך, יש לייחד את הבקשה לחיסיון לחלק אחד זה, שגילויו עלול לפגוע, כאמור, ולו בלבד. ראו: פקודת מטא"ר 04.01.1: תעודת חיסיון – הכללים וההנחיות להגשת הבקשה.

166 "הנחיית פרקליט המדינה 7.14", לעיל ה"ש 131, בסעיפים 20–23.

167 למעשה, עשוי להיווצר מצב שבו זכות העיון של בעל המכשיר, מכוח זכותו הקניינית בחומר, תהיה רחבה מזכות העיון של התובע כך שתכלול העתק של **כל חומרי המחשב שנתפסו ברשותו**, כבר בשלב החקירה כחלק מזכויותיו כחשוד לפי סעיף 32א לפקודת החיפוש. זאת, למעט מקרים שיש בהם חשש לשיבוש חקירה (שמתאיין בשלב הגשת כתב האישום). **כלומר זכות העיון שלו רחבה משל התובע**, אשר רשאי לעיין רק בחומרים שיימצאו כרלוונטיים לחקירה, ובחומרים שיימצאו לאחר ביצוען של השלמות חקירה בהוראתו. "הנחיית פרקליט המדינה 15.7", לעיל ה"ש 161, בסעיפים 17–18.

- חומרים הנוגעים לצנעת הפרט של נאשם אחד בלבד, שאינם רלוונטיים במישרין להגנתם של הנאשמים האחרים – ייחשפו בפני הנאשם (המבקש) בלבד ולא בפני הנאשמים האחרים בתיק.

לצד חומרי המחשב תקבל ההגנה את דו"ח תיעוד החיפוש בחומרי המחשב המפרט את פעולות החיפוש והסינון שבוצעו על ידי גורמי החקירה. יצוין כי מאחר שכלל החומר ניתן לעיון מצד ההגנה, אין חובה להעביר לידיה את מיפוי החומרים ברשימת כלל החומר.

חומרי המחשב שנתפסו בתיק אינם בבעלות הנאשם או אינם בבעלותו בלבד: למשל, אם חומרי המחשב בבעלותם של נאשמים אחרים, עדים בתיק או נפגעי העבירה. במצב זה הנאשם מקבל לידיו העתק אך ורק של חומרי המחשב שנמצאו כרלוונטיים לעניינו, יחד עם התיעוד כיצד הגיעו החוקרים לחומרים אלה דווקא. בניגוד לתרחיש הקודם, לצד דו"חות הפעולה, כאן עולה הצורך לערוך ולמסור להגנה מיפוי של כלל חומרי המחשב התפוסים ("רשימת כל החומר"),[168] המעניקה לה כלי נוסף בביקורתה על אופן המיון והסיווג של חומרי המחשב בחקירה.

פעולות המשך שההגנה רשאית לבצע:[169]

1. **השלמת חומרים שנתפסו מידי אחרים:** כל נאשם זכאי לבקש בכתב לעיין בחומרי מחשב נוספים אשר לא הועמדו לרשותו הגם שנתפסו בתיק, אם בקשתו תהיה ממוקדת ותימצא "סבירה ועומדות במבחן ההיגיון וסבירות המשאבים".[170] **בכפוף להסכמתו של האדם שחומרי המחשב המבוקשים נתפסו מרשותו, ניתן להעביר את החומר המבוקש לכל הצדדים בהליך.**
2. **העברת הצעות להשלמות חקירה:** ההגנה רשאית להעביר הצעות לחיתוכים, סינונים וחיפושים נוספים שניתן לערוך בחומרי המחשב במידה שבקשתם תימצא סבירה ואפשרית. למשל, בקשה לבצע חילוץ נתונים נוספים מהמכשיר על ידי מומחה מטעם ההגנה לצורך הפקת ראיות הזמה לראיות התביעה המבוססות על חומר שלא הופק מהפריקה הראשונה.[171]

168 בהתאם לסעיף 74(א)(1) לחוק סדר הדין הפלילי [נוסח משולב], תשמ"ב-1982.

169 שם, בסעיפים 19–26.

170 עניין פישר, לעיל ה"ש 17.

171 ראו למשל בש"פ 46/21 אמסלם נ' מדינת ישראל (7.1.2021) (הסכמת הפרקליטות לבקשת נאשם לבצע פריקה נוספת של הטלפון הנייד שממנו הופקו ראיות התביעה, על ידי מומחה מטעם ההגנה, שתתבצע במשרדי היחידה החוקרת ובנוכחות חוקר מיומן אשר יפקח על תהליך הפריקה); ה"ת (מחוזי מרכז) 21933-04-22 טחלוב נ' מדינת ישראל (4.5.2022) (החלטת בית המשפט לקבל בקשה של נאשמת לבצע פריקה מטעמה של נתונים ממכשיר הטלפון הנייד שלה, בנסיבות שבהן התברר כי מלוא החומר שהופק בפריקה לא גובה על ידי המשטרה, כך שבידיה נותרו רק חלק מתוצרי הפריקה. בדיון שהתקיים הסכימו הצדדים כי תוכן הטלפון יועתק על ידי המדינה, אך ייאסר עליה לצפות בו, אלא לפי צו חיפוש חדש של בית המשפט – וכי לאחר השלמת הפריקה על ידי המדינה יושב המכשיר הנייד לידי הנאשמת).

איגוד האינטרנט הישראלי ISOC-IL

ד.4 שמירת ראיות וחומרי חקירה על ידי רשויות החקירה ושימוש עתידי בהם

כאשר נעשה שימוש בטכנולוגיות פורנזיות לצורך חדירה או מיצוי נתונים דיגיטליים, מיצוי החומרים הרלוונטיים לחקירה נשמרים בתיק ככל חומר חקירה אחר, עד לביעורו של התיק.

עם זאת, נזכיר כי הכלים הטכנולוגיים כדוגמת UEFD שמפעילות רשויות החקירה בישראל מבוססים לרוב על יצירת העתק דיגיטלי מלא של המכשיר נחפש (לרבות חומרים שאינם רלוונטיים לחקירה או לא בגדרו של צו החדירה), אשר מגיע לידי היחידות הטכנולוגיות של הגוף החוקר, לפני שמסוננים ממנו נתונים לא-רלוונטיים מתוך ההעתק המלא. **ההעתק הדיגיטלי המלא של הטלפון החכם, שנוצר לצורך הפעלת כלי החדירה והחיפוש, מכיל את כל עולמו של בעל המכשיר ובמקרים רבים גם מידע אישי על צדדים שלישיים שאינם חשודים, אך איננו יודעים מה עולה בגורל נתונים אלו לאחר סיום ההליך המשפטי או סגירת תיק החקירה.** אדרבא, קיים יסוד סביר להאמין כי ההעתק הדיגיטלי שיצרה המשטרה עבור טלפון חכם בזמן החקירה, או חלקים ממנו, נשמרים על ידי רשויות האכיפה כ-"חומר מודיעיני" עבור תיקים אחרים וחקירות עתידיות.

בהיעדר אסדרה חקיקתית ייעודית של שמירת החומרים הדיגיטליים שחולצו ממכשירי טלפון וחשבונות ענן לאחר סיום החקירה במסגרתה נאספו החומרים – חולשת על מישור זה ההלכה הכללית כי שמירת מוצגים או חומרים תיעשה לפי שיקול דעתו של בית המשפט.[172]

172 כמובן בכפוף לכל דין, ובעיקר חוק הגנת הפרטיות, חוק הארכיונים ותקנותיהם. ראו גם: רע"פ 5295/18 מאור נ' מדינת ישראל (15.8.2018).

הצורך בעדכון הדין ומסגרת הפיקוח על חדירה למכשירים חכמים ומשאבי ענן שמבצעות רשויות האכיפה בישראל

ה

ה.1 התפתחויות טכנולוגיות המעצימות את היקף ורגישות המידע שניתן לחלץ מטלפונים חכמים ומכשירים דיגיטליים

> 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.
>
> ועדת מררי, אוגוסט 2022[173]

כפי שהראינו עד כה, עידנים שלמים בתחום המחשוב והאינטרנט חלפו מאז שנחקק חוק המחשבים והתיקון לפקודת החיפוש בעניין חדירה וחיפוש בחומרי מחשב. בשנים שחלפו, יכולות האחסון והעיבוד של טלפונים חכמים התרחבה לאין שיעור, וכך גם היקף השימושים האישיים בטלפון נייד ובחשבונות ענן. הגידול בהיקף השימוש נבע גם מהתקדמות טכנולוגית אשר הביאה לירידה במחיר המכשירים, שבתורה עזרה להגדיל את כמות המשתמשים במכשירי טלפון חכמים. מרכזיותו הטלפון החכם כמחשב העיקרי בחיינו, יחד עם התפתחויות טכנולוגיות של אינטימיות והיקף הנתונים שהוא אוצר, הופכת את הפריצה והחיפוש בו לפגיעה כבדה במיוחד בזכויות החוקתיות להליך הוגן, כבוד האדם והזכות לפרטיות. בנוסף, חיפושים בטלפון שונים מהחרמה מסורתית של חפצים מכיוון שרשויות האכיפה לרוב ממצות את כל הנתונים מהמכשיר ורק בשלב ניתוח המידע מתחתמות את הבדיקה לפי תנאי הצו או הרלוונטיות לחקירה. במובן זה, שמירת מידע שאינו מוגדר בצו חיפוש דומה לשמירת זכותה של רשות אכיפת החוק לבצע חיפוש בביתו של אדם, ללא כל הגבלת זמן.

כפי שהוזכר לא מעט במסמך זה, הטלפון החכם הפך לכלי ביטוי מרכזי בחיי היום-יום של מרבית האוכלוסייה. אצל אנשים רבים, כלל חייהם המקצועיים והאישיים תלויים במידע וביישומים אשר נמצאים על הטלפון החכם. ניתן לראות ביטוי למרכזיותו של הטלפון החכם ביכולת לבצע תשלומים בעזרתו ללא ארנק ובשיפור ביכולת הצילום של המכשירים אשר יכולה להחליף מצלמה מקצועית. בכלל זה, גם תקופת הקורונה חשפה ועודדה את התפתחותם של יישומים ומכשירים חכמים רפואיים אשר מקילים על חולים לתקשר ולקבל מידע רפואי נחוץ. מעבר לסכנה שיכולה להיווצר מאגירה של מידע זה, השימוש בתוכנות שהוזכרו במסמך זה עלול ליצור אפקט מצנן אשר ימנע מאזרחים להשתמש ביישומים רפואיים מחשש שמידע זה ייחשף וייאגר.

גם בתי המשפט בישראל הכירו זה מכבר בכך שפריצה וחקירה של טלפונים חכמים ומכשירים אישיים נוספים מאפשרת לרשויות החקירה גישה להיקף חסר תקדים של מידע אישי ורגיש; וכי המסגרת החקיקתית המיושנת של דיני החיפוש בישראל אינה מספקת פיקוח וביקורת מספקים כנגד שימוש מופרז, לא-מידתי או לא-מפוקח דיו בכלים טכנולוגיים רבי עוצמה לפריצה ולחיפוש במכשירים חכמים וחשבונות הענן המקושרים אליהם.[174]

---

173 דו"ח מררי, לעיל ה"ש 39, פרק ההמלצות, עמ' 69.

174 ראו לעיל פרק ב.

איגוד האינטרנט הישראלי ISOC-IL

זה המקום להזכיר את עיקרי הצעת החוק הממשלתית שהונחה על שולחן הכנסת ה-19 וה-20 – חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, תפישה וחיפוש), התשע"ד-2014 ("הצעת חוק החיפוש") – שנועדה להחליף את ההסדרים הקבועים כיום בפקודת החיפוש. הצעת חוק החיפוש מסדירה באופן מקיף וכולל את הפעולות הנוגעות לחומר מחשב אשר כיום מוסדרות בפקודת החיפושים, תוך הדגשת הבעייתיות במצב החוקי הקיים לעניין חיפוש במחשבים, שאינו נותן מענה מספק בכל הקשור לחדירה לחומר מחשב.

פרק ו להצעת חוק החיפוש מבטא את ההכרה כי מתחייבת התייחסות מיוחדת למחשב ולחומר מחשב בדיני החיפוש, התפיסה וההמצאה, שמתחייבת 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.[175] בהצעת החוק הוצע לקבוע איזון קפדני נוכח מאפייניו הייחודיים של חומר המחשב, בין צורכי 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.[176]

הצורך בעדכון מסגרת הדין והנוהל להפעלת אמצעים טכנולוגיים לחדירה ולחיפוש בטלפונים ניידים בוער במיוחד בעידן מחשוב הענן של השנים האחרונות ויכולת גופי האכיפה לחדור ולחפש בחשבונות ענן הנגישים מהמכשיר – המהווה הרחבה עצומה של סמכויות החקירה וחודרנותה. כפי שפירטנו לעיל בפרק ב, כלים אלו מעניקים לרשויות החקירה גישה למידע אישי בהיקף אינסופי, ואף מאפשרים לרשויות להתחזות לאדם ברשתות החברתיות או חשבונות מקוונים אחרים. בנוסף, היכולות החדשות של גופי החקירה לחלץ נתונים ממשאבי ענן וחשבונות מחייבות עדכון של הדין והנוהל הקיימים, נוכח טשטוש הגבול בין חיפוש (המאפשר לקבל נתונים במועד קבלת הצו) לבין האזנת סתר (המאפשרת לקבל נתונים עתידיים).

ה.2 שאלת אמינות ומהימנות ראיות שהופקו באמצעים בעלי מעמד פורנזי

בחינה מחדש של מסגרת הדין לחדירה וחיפוש במכשירים חכמים וטלפוניים ניידים בפרט נדרשת לא רק מטעמי הגנה על פרטיות וכבוד האדם, אלא בראש ובראשונה מטעמי הליך הוגן ואמינות של הראיות המופקות באמצעות הכלים הטכנולוגיים המופעלים בישראל בעת הליכי חקירה.

בראיות דיגיטליות, ההבדל בין מקור לבין העתק מיטשטש עד שלעיתים אין הוא קיים כלל, כך שהדיון הראייתי אינו מתמקד בראיה גופה אלא בדרכי הפקתה. על כן, הראיות אמורות להיות Forensically Sound, כלומר נאמנות למקור, ומופקות בדרכים ספציפיות שאינן משנות את ה"מטה דאטה" של הנתונים, כגון מידע המתאר את הקבצים, מועדי יצירתם וכו'.

175 תיאור זה מבוסס על דו"ח מררי, לעיל ה"ש 39, בעמ' 23.

176 דו"ח מררי, שם ("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").

למרות זאת, כפי שתיארנו בהרחבה בפרק ב.4, כלים טכנולוגיים בעלי מעמד פורנזי, כגון מוצרי Cellebrite או NSO שרשויות אכיפת החוק בישראל משתמשות בהם, מעוררים אתגרים ראייתיים-הליכיים ייחודיים בכל הנוגע לאמינות הראיות, חשש ל"זיהום" הממצאים ושאלת השרשרת הראייתית של חיפושים דיגיטליים.[177] זאת, במיוחד בנוגע לביצוע חדירה נסתרת מרחוק, הכרוכה בהכרח בשינוי הנתונים ומערכות האבטחה של מכשיר היעד.[178]

על רקע זה, עדכון מסגרת הדין והנוהל לחדירה וחיפוש במכשירים חכמים של אזרחים נדרש כדי להבטיח את זכות האזרח להליך הוגן במסגרת פעולה רגישה זו, יחד עם האינטרס הציבורי להבטחת האמינות והמהימנות של הראיות המובאות בפני בתי המשפט. זאת, הן ביחס לאמינות הכלים הטכנולוגיים והן ביחס לשרשרת הראייתית והגנה מפני זיהום.

ה.3 חיפוש בחומרי ענן באמצעות תפיסה של מחשבים או מכשירים חכמים מהווה פעולה חוץ-טריטוריאלית

התרחבות הזמינות והשימוש של טלפונים ניידים ומכשירים חכמים באחסון מבוסס-ענן מעוררת קושי משפטי בכל הנוגע לסמכותן של רשויות האכיפה לבצע פעולות חדירה או חיפוש במידע המאוחסן מחוץ לשטחה הריבוני של מדינת ישראל.

בשני העשורים האחרונים רווחת במדינות דמוקרטיות התפיסה כי רשויות האכיפה אינן רשאיות לבצע חיפוש בנתונים או במאגרי מידע שלא בשטחן הטריטוריאלי.[179] אמנת בודפשט (2016), שחתומות עליה כ-60 מדינות, קובעת כי לא ניתן לאסוף, לעיין ולהשתמש במידע הנמצא מחוץ לגבולותיה הטריטוריאליים של המדינה אלא אם הגורמים הרלוונטיים במדינה שבה נמצא המידע אישרו זאת (בדרך כלל על ידי MLA – Mutual Legal Assistance). במקביל, השינויים היסודיים באופן שבו מופק ומאוחסן מידע אישי בעידן הרשת הניעו את חקיקת ה-GDPR באיחוד האירופי, אשר בין היתר כוללת איסורים ומגבלות על העברת מידע אל מחוץ לטריטוריית האיחוד (לרבות על גורמים אשר אינם בטריטוריה של האיחוד האירופי, אך מעבדים נתונים של נושאי מידע באיחוד), ובפרט סעיף 48 הקובע כי צו בית משפט זר או החלטה של רשות מנהלית לא יוכרו וייאכפו באופן אוטומטי באיחוד האירופי, אלא אם ייננתו במסגרת MLA.[180]

דוגמה ממחישה למעמדה של המוסכמה הבין-לאומית שחדירה של רשויות אכיפה מדינתיות לנתונים המאוחסנים מחוץ לגבולות המדינה מחייבת הסדרה חקיקתית ספציפית היא ה-CLOUD ACT שחוקקה ארצות הברית בשנת 2018.[181]חוק זה תיקן חקיקה קיימת שאפשרה להוציא צו המחייב חברות טכנולוגיה להעביר לרשויות האכיפה את כל הנתונים המאוחסנים לגבי משתמש מסוים אשר יש עדויות לכך שביצע פשע, וקבע כי ניתן לחייב, בעזרת צו, חברות לספק מידע הנמצא ברשותן או בשליטתן גם אם הנתונים אינם נמצאים בארה"ב, ובמקרים מסוימים גם אם הבקשה נוגדת חוק במדינה

177 לפירוט חולשות אבטחה בכלים אלו שאפשרו לשבש את פלט מערכת UFED, ראו לעיל פרק ב.4.

178 כמתואר בחלקים הקודמים, הכלים הפורנזיים לחילוץ ולעיבוד מידע ממכשירים חכמים כגון אלו של Cellebrite ו-NSO מנצלים חולשות אבטחה בתוכנה או בקוד של מערכות הטלפונים הניידים כדי לשבש או לעקוף את מנגנוני הנעילה והאבטחה המובנים שלהם.

179 Robert J. Currie, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, The Canadian Yearbook of International Law 54 (2017). לעיגון תפיסה זו בדין הישראלי ראו למשל ע"פ 7230-96 פלוני נ' מדינת ישראל (1997) ("עקרון הפתיחה הכללי הוא, כידוע, שדיני העונשין תופשים בתחומיה הטריטוריאליים של המדינה"); חוק עזרה משפטית בין מדינות, התשנ"ח-1998 (קובע מסלול ייעודי לחיקור דין או איסוף ראיות מחוץ למדינת ישראל).

180 ה-GDPR מחריג מתחולתו את רוב המקרים של העברת מידע מטעם גופי אכיפה, להבדיל מהעברת מידע לגופי אכיפה מחברות התקשורת.

181 Clarifying Lawful Overseas Use of Data Act (2018).

אחרת. משרד המשפטים האמריקני דאג להדגיש כי החוק אינו נותן לרשויות האכיפה ולרשויות החוק סמכות חדשה על חברות זרות, אלא נותן מענה למגבלה הטריטוריאלית של פעילות אכיפה מדינתית בנוגע למידע המאוחסן מחוץ לגבולות המדינה.

נדבך נוסף של ה-CLOUD Act מתמודד עם המגבלות היישומיות לבצע הליך MLA עבור כל מקרה שבו רשות חקירה ניגשת למידע המאוחסן בשרתים מרוחקים אגב חיפוש במחשב או בטלפון חכם שנתפסו בטריטוריה. זאת, באמצעות הסמכה ייעודית של הרשות המבצעת לחתום על הסכמים בין-מדינתיים לדרישת נתוני משתמשים משירותי הטכנולוגיה והענן, שיאפשרו למדינה זרה לפנות ישירות לחברה ללא אישור ובדיקה פרטנית של הבקשה כפי שנדרש בהליך MLA. נדבך זה למעשה נשען על הנדבך הראשון, ודורש כי במדינה השנייה יהיה חוק דומה. כלומר, הסכם יכול להיחתם בין המדינות רק אם החוק המקומי קובע כי רשויות האכיפה יכולות לגשת למידע הנמצא מחוץ למדינה (כפי שעושה הנדבך הראשון לגבי ארה"ב).

גם האיחוד האירופי פרסם בשנת 2018 הצעת חקיקה דומה במאפייניה, מתוך הכרה בצורך לעדכן את האסדרה המסורתית של גישה לראיות אלקטרוניות בעניינים פליליים.[182] ההצעה עדיין לא התקבלה, אך היא מציעה חוקים להסדרת היכולת של מדינה לדרוש מידע מתאגיד אשר פועל באיחוד באופן ישיר, ללא קשר למיקום הפיזי של המידע. הצעת החוק מקווה לשפר את ההעברה הבטוחה של ראיות אלקטרוניות אשר מוחזקות אצל ספקי שירות שנמצאים במדינה אחרת, לצורך חקירות פליליות. הרגולציה קובעת מסגרת של צווי בקשות מידע אשר תאפשר לבתי משפט ולרשויות אכיפת חוק לקבל גישה לראיות אלקטרוניות ישירות מספקיות שירות במדינות אחרות באיחוד האירופי. הרגולציה קובעת גם מסגרת של צווי שימור אשר תאפשר לרשויות שיפוטיות לבקש מספקיות שירות במדינות אחרות לשמר מידע מסוים.

על רקע זה, הפרקטיקה הקיימת בישראל שלפיה חדירה לחומר מחשב האגור מחוץ לישראל יכולה להיעשות ללא הסמכה מפורשת בחקיקה, אלא על בסיס היתר של פרקליטות המדינה,[183] אינה עולה בקנה אחד עם עקרון הטריטוריאליות ועם ההכרה של מדינות דמוקרטיות בצורך לעדכון החקיקה הראשית של דיני החיפושים לעידן מחשוב הענן הנוכחי, שבו כמעט כל חיפוש במחשב או במכשיר חכם שנתפס בישראל כרוך בגישה לנתונים שמאוחסנים מחוץ לגבולות המדינה.[184]

עם חתימה, נציין סוגיית הסמכות לעריכת חיפוש בחומר מחשב בדרך של חדירה לשרתים מרוחקים התעוררה בהליך הפלילי כנגד הנאשמים בפרשת טלגרס, אשר נכון לפרסום סקירה זו עדיין תלוי ועומד בפני בית המשפט.[185]

182 European Production and Preservation Orders for electronic evidence in criminal matters (link).

183 ראו להלן הפרק ד.2.א ונספח ב. למסגרת הנורמטיבית הבינלאומית העוסקת בפשעי מחשב וחדירה לשרתים מרוחקים, ראו האמנה הבינלאומית על פשעי מחשב (Convention on Cybercrime), שאליה הצטרפה מדינת ישראל בשנת 2016.

184 בארה"ב ובאיחוד האירופי, ראו פסקאות לעיל. באנגליה, ועדת החוק (Law Com No 396- search warrants) קבעה שהמסגרת הנוכחית של צווי חיפוש לא יועדה ואינה מותאמת למאפייניו הייחודיים של מידע אלקטרוני. הוועדה ממליצה לשנות את הוראות צו החיפוש כך שכאשר מחפשים מידע אלקטרוני, מכשירים אלקטרוניים יוכלו להיות היעד של הצו רק כל עוד הנתונים עומדים בתנאים שבחוק הנוגעים לחומר היעד. בנוסף, הוועדה מציעה להוסיף צו נוסף (מעבר לצו החיפוש למכשיר) אשר יציין מהו המידע הספציפי אשר מבוקש על המכשיר. לשם איזון ראוי בין צרכי חקירה לבין הבטחת הליך הוגן וזכויות אזרח נוספות, הוועדה מדגישה כי נדרשת רפורמה משפטית לעדכון החקיקה הקיימת.

185 תפ"ח (מחוזי מרכז) 42209-04-19 מדינת ישראל נ' סילבר. לטענות ההגנה בעניין זה ותגובת הפרקליטות ראו: דניאל דולב "המסלול העוקף שמאפשר למשטרה לחטט לחשודים בענן" N12 (4.10.2022) (קישור).

ה.4 הגידול בהיקף החיפושים בטלפונים חכמים פוגעני במיוחד בקרב אוכלוסיות מוחלשות

כאשר מדובר בהשלכות השימוש הנרחב בכלי חקירה פוגעני, חשוב לספק מענה לעובדה כי מי שיושפעו מכך במיוחד ובצורה חריפה הם אוכלוסיות מוחלשות או מיעוטים, אשר באופן שיטתי סובלים מאכיפה מוגברת. הדוגמאות המוכרות לאכיפת יתר שכזו בישראל הן פערי האכיפה כלפי לא-יהודים[186] וכלפי יוצאי אתיופיה (ובייחוד קטינים),[187] ששיעור פעולות האכיפה הננקטות נגדם גדול בהרבה משיעורם באוכלוסייה.

בהתחשב בכך שהפערים בשיעורי המעצר מאפיינים את מערכת המשפט הפלילי, סביר להניח שחילוץ נתונים מטלפונים סלולריים כבר משקף אותם. כלומר, בני מיעוטים ואוכלוסיות חלשות חשופים יותר לסכנת הפגיעה של חדירה משטרתית לנתונים ומידע אישי, **והעובדה כי אוכלוסיות מוחלשות בישראל מסתמכות לרוב על טלפון נייד עבור מרבית הפעילות המקוונת שלהן מעצימה עוד יותר את הפוגענות של התפיסה והחיפוש במכשיריהן.**[188]

בנוסף, **חיוני להכיר במגבלות ההסכמה הניתנת מצד מיעוטים הסובלים מאכיפת יתר כתוצאה של חוסר סימטריה קיצוני בסמכויות ובמעמד.** אף על פי שבית המשפט העליון קבע שאי אפשר לכפות הסכמה, באמצעים מפורשים או לא מפורשים, ניסיון החיים מלמד כי אינטרקאקציה של מיעוטים תרבותיים הנתונים לאכיפת יתר מצד גורמי האכיפה מתאפיינת בתחושת איום או אסימטריה קיצונית בסמכויות, וזו עשויה לגרום לאנשים להרגיש שאין באפשרותם או בטובתם לסרב לבקשת חיפוש מצד שוטרים.[189] המלצה זו עולה בקנה אחד עם ההכרה של בית המשפט העליון בסכנה הפוטנציאלית של "שיטור יתר" כלפי קבוצות אתניות או תרבותיות מוחלשות.[190]

186 בשנת 2019, ב-41% מהמקרים נרשם חשוד שאינו יהודי, ומתוך כלל כתבי האישום שהוגשו, 43% מהם היו כנגד נאשם שאינו יהודי; מכלל המעצרים הפליליים שבוצעו באותה שנה, 57% מהעצורים היו לא יהודיים. כמו כן, בסוף חודש מרץ 2020, 55% מכלל העצורים תושבי ישראל במתקני הכליאה השונים ברחבי המדינה היו לא יהודים. זאת בעוד ששיעור הלא יהודים באוכלוסייה עומד על 25.7% בלבד. מקור: ד"ר נורית יכימוביץ כהן "נתונים על פשיעה בחברה הערבית – עדכון" 1 **(הכנסת – מרכז המחקר והמידע, 2020)**. הנתונים מתייחסים ל"לא יהודים", אך רובה המוחלט של קבוצה זו הוא של בני המגזר הערבי: מבין 2.27 מיליון לא יהודים שחיו בישראל בשנת 2018, 1.86 מיליון היו ערבים.

187 בשנת 2019, למשל, שיעור תיקי החקירה של בגירים יוצאי אתיופיה עמד על 3.2% מכלל תיקי החקירה לבגירים באותה שנה, כמעט פי 2 משיעורם באוכלוסייה הכללית. בקרב קטינים, שיעור המעצרים של קטינים יוצאי אתיופיה עמד על 5.6% מכלל המעצרים של קטינים באותה שנה, יותר מפי 3 משיעורם באוכלוסייה. ראו: מבקר המדינה **דו"ח שנתי 72א – התנהלות גורמי האכיפה אל מול יוצאי אתיופיה** 292 (התשפ"א-2021).

188 על פי נתוני הלמ"ס ואיגוד האינטרנט הישראלי משנת 2018, אין הבדלים בין הציבור הערבי ליהודי בבעלות על טלפון חכם; אולם 28% מהציבור הערבי העידו על גלישה באינטרנט מהטלפון הנייד בלבד, לעומת 10% מהציבור היהודי. כמו כן, כ-66% מהחברה הערבית דיווחו כי עיקר השימוש שלהם באינטרנט נעשה באמצעות הטלפון הנייד (קישור). נתונים משנת 2020 מלמדים שקרוב ל-20% מהחברה הערבית והדרוזית משתמשים באינטרנט רק באמצעות מכשירים ניידים, לעומת כ-7% מהאוכלוסייה היהודית (קישור).

189 לתיאור תופעה זו בנוגע למיעוטים לא-לבנים מול רשויות האכיפה בארצות הברית, ראו: Upturn Report, לעיל ה"ש 10, בעמ' 59; Tracey Maclin, “Black and Blue Encounters” Some Preliminary Thoughts About Fourth Amendment Seizures: Should Race Matter?, 26 Val. U. L. Rev. 243, 248 (1991); Marcy Strauss, Reconstructing Consent, 92 J. Crim. L. & Criminology 211, 242–243 (2001); George C. Thomas III, Terrorism, Race and a New Approach to Consent Searches, 73 Miss L. J. 525, 542 (2003).

190 בג"ץ 4455-19 עמותת טבקה – צדק ושוויון ליוצאי אתיופיה נ' משטרת ישראל (25.01.2021).

1 במקום סיכום: מתווה לפיתוח האסדרה של חיפוש במכשירים חכמים אישיים

כפי שציינו בפתח מסמך זה, מטרתו העיקרית היא לספק נתונים ועובדות על יכולותיהן חסרות התקדים של טכנולוגיות פורנזיות לחדירה ולחיפוש בטלפונים חכמים ובחשבונות הענן המקושרים אליהם ועל מסגרת הדין והנוהל להפעלתם. בחלק מסכם זה נבקש להציע תשתית רעיונית באשר לעקרונות שאנו סבורים כי ראוי ונדרש לאמץ על מנת להבטיח איזון ראוי בין האינטרס הציבורי בחקר האמת ואכיפת הדין לבין זכויות היסוד לפרטיות, להליך הוגן ולכבוד האדם של תושבי ישראל.

נדגיש כי המלצות אלו ממוקדות למקרים של חדירה וחיפוש בחומר מחשב לאחר תפיסתו (מכוח פקודת החיפוש), ולא למקרים של "חיפוש מרחוק" או שימוש ברוגלות. עם זאת, גם בתחום זה יפה המלצתה המרכזית של ועדת מררי.

הגבלת האפשרות לחיפוש בטלפונים ניידים ובמשאבי ענן על בסיס הסכמה וללא צו שיפוטי

כפי שהסברנו בתיאור שלבי החקירה, ככלל, הליך החיפוש דורש צו שיפוטי. עם זאת, בשנים האחרונות קיימת גם פרקטיקה של חיפוש בהסכמת החשוד. "הסכמה" זו, שניתנת לא אחת במפגש לא סימטרי בין בעל סמכות חוקרית לבין נחקר/חשוד שמנסה לרצות את בעל הסמכות שמולו, מעלה סוגיות משפטיות ואתיות רבות. חיפושים בהסכמה על ידי שוטרים הם מדאיגים בכל הקשר,[191] אבל האסימטריה בסמכויות ובמידע במקרה של חיפושים בהסכמה בטלפון סלולרי היא עצומה במיוחד, בייחוד כאשר מדובר בחיפוש הנעשה באמצעות כלים טכנולוגיים.

סביר להניח שלאדם שמסכים לחיפוש בטלפון שלו אין מושג מה באמת המידע שניתן לחלץ מהמכשיר שלו, ומה יקרה למכשיר. עקב היעדר דיון ציבורי על הכלים הפורנזיים שמפעילות רשויות האכיפה, סביר להניח שרוב האנשים יופתעו מהעוצמה של הכלים שרשויות אכיפת החוק יכולות להשתמש בהם כדי למצות ולנתח נתונים מהמכשיר. יתרה מזו, מרבית הטפסים לחיפוש בהסכמה של טלפון אינם מפרטים כיצד הן תבצענה חיפוש בטלפון, באילו כלים ובאיזה היקף יהיה החיפוש. בנוסף, הניתוח שהצענו לעיל מלמד כי בפועל אין כמעט מגבלות על השימוש שרשויות אכיפת החוק יכולות לעשות עם נתונים שמוצו מטלפון סלולרי לאחר שמישהו הסכים לחיפוש. אם טופס ההסכמה נוסח באופן רחב מספיק, אין הגבלת זמן על התקופה שבה רשות אכיפת חוק יכולה לבדוק מחדש נתונים שמוצו מטלפון סלולרי.

בעיה נוספת בפנייה הרחבה של הרשות החוקרת לאפיק ההסכמה על פני צו שיפוטי היא כי חיפוש בהסכמה אינו מתייחס לשיקול הפגיעה בצדדים שלישיים, שהוא אחד משלושת השיקולים המרכזיים באפיק הצו השיפוטי, לאישור הצו ולקביעת היקפו. כלומר, גם אם אפשר להכשיר את השרץ על ידי טיוב ההסכמה מדעת שניתנת על ידי בעל המכשיר, אין הסכמתו

191 מחקר שבוצע לאחרונה ותוכנן "במיוחד כדי לבחון את הפסיכולוגיה של חיפושים בהסכמה" מדגיש את הבעיות בהסתמכות על כך ש"אדם סביר" יחליט מה לעשות בקשר לחיפוש בהסכמה. המשתתפים במחקר הובאו למעבדה והוצגה להם "בקשה מאוד פולשנית: לאפשר לחוקר גישה ללא פיקוח לטלפון החכם הלא נעול שלהם". יותר מ-97% מהמשתתפים מסרו את הטלפון שלהם לחיפוש כאשר התבקשו, למרות שרק 14.1% מהאנשים בקבוצה נפרדת של צופים אמרו שאדם סביר יסכים למסור את הטלפון שלו. המחקר מגלה שקיימת "הטיה שיטתית שגורמת לצופים ניטרליים מהצד לראות בהסכמה משהו יותר רצוני, ולראות בסירוב משהו יותר קל, מאשר האנשים שעוברים את החוויה". בעוד שקיימות טענות סבירות על כך שמחקרים במעבדה מגזימים בהערכת שיעורי ההיענות לבקשות חיפוש מצד שוטרים, קיימות ראיות חזקות לכך ששיעורי ההיענות במחקרים נמוכים משיעורי ההיענות האמיתיים. ראו: Roseanna Sommers, Vanessa K. Bohns, The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance, 128 Yale L. J (2019).

מכשירה פגיעה בפרטיותם של צדדים שלישיים אשר מושפעת גם היא מתוכן המחשב.

הגבלת האפשרות להפעיל כלים פורנזיים למיצוי מידע מטלפונים חכמים על בסיס הסכמה אינה הצעה חדשה,[192] והיא גם לא פתרון אידיאלי, מכיוון שלרשויות אכיפת החוק לא קשה להשיג צו חיפוש. עם זאת, הגבלת חיפוש בהסכמה בטלפון סלולרי יכולה לעזור להגביל את שיקול הדעת של גורמי החקירה, להגביל את יכולת הכפייה שלהם, ולמזער את כמות המידע שאפשר לאסוף מאנשים שנמצאים תחת חקירה.

בנוסף, ראוי לבחון מחדש את האבחנות ההיסטוריות בין "חיפוש" ל-"האזנת סתר" ובין ועבירות מסוג פשע לעבירות עוון, לצורך בקשה או מתן צווים בעניינים אלו על מנת ליצור מדרג עשיר יותר של שיקולים לפיו יאשרו בתי המשפט ביצוע חיפושים במחשב, לרבות חדירה בלי הסכמה של בעל המחשב. קל וחומר לגבי חדירה או חיפוש מרחוק.

חובת תיעוד (audit logs) של פעילות הכלים הפורנזיים לחדירה ולחיפוש במכשירים חכמים

הסכנה הטמונה בחיפושים רחבים מדאיגה במיוחד בהתחשב בעובדה שמי שאינם נמנים עם רשויות אכיפת החוק – כמו סניגורים – יתקשו מאוד לשחזר את הצעדים שנקט החוקר הפלילי בניסיונם לפקח על היקף החיפוש או לחלוק על אמינותו.

קומץ מסמכי מדיניות אומנם מחייב את החוקרים לתעד כיצד נערך החיפוש, אבל לא סביר שרמת התיעוד הנדרשת תאפשר לסניגור לבצע ביקורת יעילה של פעולות החדירה, החילוץ והניתוח שביצעו רשויות החקירה באמצעות הכלים הטכנולוגיים שברשותם. באופן כללי יותר, יש להכיר בפערי המומחיות והמשאבים שבין רשויות אכיפת החוק לבין סנגורים (וסנגורים ציבוריים במיוחד), כאשר לאחרונים לרוב אין גישה לכלים הפורנזיים הרלוונטיים. במקום זאת, לעיתים קרובות סנגורים נאלצים לבחון דו"חות פורנזיים שמכילים אלפי עמודים וניתנים לניווט מעשי רק באמצעות תוכנה קניינית של חברה פורנזית, או על-ידי תשלום שכר טרחה בהיקף גבוה למומחים מקצועיים בתחום הפורנזיקה הדיגיטלית.

על רקע זה, ראוי לקבוע בחקיקה כי לכלים שרשויות אכיפת החוק מפעילות על מכשירי טלפון ניידים יהיו פונקציות לניהול רשומות ברורות, ובאופן מיוחד יומני ביקורת (audit logs) מפורטים והקלטות מסך אוטומטיות. יומני ביקורת והקלטות מסך יספקו תיעוד כרונולוגי של כל האינטראקציות של רשויות אכיפת החוק עם התוכנה, כגון איך הן דפדפו בנתונים, באילו שאילתות חיפוש הן השתמשו, ואילו נתונים הן היו יכולות לראות. על בסיס יומנים כאלה, שופטים ואנשים אחרים יוכלו להבין טוב יותר את הצעדים המדויקים שרשויות אכיפת החוק נקטו במהלך מיצוי נתונים ובדיקה של טלפון, ולסנגורים ציבוריים יהיו כלים טובים יותר כדי לקרוא תיגר על הצעדים האלה במקרים המתאימים, ובפרט כאשר רשויות אכיפת החוק חרגו מהמגבלות של צו החיפוש בטלפון.

192 רע"פ סיגאוי, לעיל ה"ש 123 ("השאלה העקרונית שהונחה בפנינו היא האם הסכמתו של חשוד מספקת על מנת להסמיך חוקרים לערוך חיפוש בטלפון הנייד – שאלה זו תישאר תיאורטית ולא תשפיע על תוצאות ההליך... לא מן המותר להרהר גם בשאלה האם אין זה ראוי להסדיר את הנושא הספציפי בחקיקה").

איגוד האינטרנט הישראלי ISOC-IL

המלצה זו עולה בקנה אחד עם עקרונות שנוסחו על ידי ארגוני עובדים בתחום אכיפת החוק, כגון איגוד מפקדי משטרה בארצות הברית, שקבע כי "יש ליצור ולשמר נתיב ביקורת... על כל התהליכים שיושמו על ראיות דיגיטליות. גוף שלישי בלתי תלוי צריך להיות מסוגל לבחון את התהליכים האלה ולהגיע לאותה תוצאה".[193]

הסדרת היכולת של חוקרים להשתמש במידע מחוץ למטרת החיפוש הספציפי: צמידות מטרה?

מסמכי מדיניות מעטים מספקים הנחיות לגבי הצעדים שחוקרים צריכים לנקוט אם נתקלו בראיות פוטנציאליות לפשע אחר שאינו מפורט בצו החיפוש הראשוני. שימוש בצו כדי לחפש ראיות דיגיטליות לפשע פוטנציאלי אחד רק כדי לחפש ראיות דיגיטליות לפשע אחר לגמרי מעלה שאלות חוקתיות חמורות. ללא הגבלת היכולת של חוקרים לגשת למידע החורג ממטרת החקירה הספציפית, יכולות רשויות אכיפת החוק לצאת ל"מסע דיג" בחיפוש אחר ראיות לפשע כלשהו – הרבה מעבר לצידוק המקורי לחיפוש.

על כן, האסדרה העתידית של אמצעים טכנולוגיים למיצוי מידע מטלפונים חכמים נדרשת לקבוע עקרונות ברורים באשר לסוגיות אלו אשר טרם זכו לליבון בפסיקה. אלו צריכים להיות מחמירים במיוחד לגבי נתונים שמקורם בהפעלת הטכנולוגיות הפורנזיות על בסיס הסכמה.

חובות לגבי טיפול במידע שנאסף ממכשירים חכמים: חתימה ומחיקה

בהיעדר חוק או מדיניות ברורים, רשויות אכיפת החוק עשויות להשתמש במידע אישי כגון רשימות אנשי קשר, תמונות ונתוני מיקום כדי להזין מערכות מעקב משטרתיות. זה נכון לא רק לגבי הנתונים של האדם שהטלפון שלו עבר חיפוש, אלא גם לגבי כל האנשים שאיתם היה לו קשר באמצעות הטלפון שלו. במובן זה, חיפושים בטלפון שונים מהחרמה מסורתית של חפצים מכיוון שרשויות אכיפת החוק ממצות את כל הנתונים מהמכשיר ורק אחר כך מחפשות מידע שקשור לתיק.

מכיוון ששמירת מידע שאינו מוגדר בצו חיפוש דומה לשמירת זכותה של רשות אכיפת החוק לבצע חיפוש בבית ללא כל הגבלת זמן, ראוי לחייב את רשויות אכיפת החוק למחוק כל נתון שמוצה מטלפון סלולרי שאינו קשור למטרה של צו החיפוש – תוך חודשים ספורים מיום קבלת המידע. בתיקים שהסתיימו בהגשת כתב אישום – נתונים שנחשבו רלוונטיים צריכים להיגנז עם סגירת התיק. בתיקים אחרים, שבהם ההאשמות מבוטלות או אינן מסתיימות בהרשעה, כל הנתונים צריכים להימחק, בין אם הם רלוונטיים ובין אם לאו. נתונים שנחשבו רלוונטיים בתיק אחד אינם צריכים לעולם לשמש למטרות מודיעיניות כלליות או לשמש בתיקים שאינם קשורים לאותו תיק.[194] **בנוסף, ראוי לקבוע כי אם רשויות החקירה מפעילות כלים טכנולוגיים למיצוי נתונים ממכשירים חכמים ו/או מחשבונות הענן המקושרים אליהם, על המידע המוזן למערכת ונשמר בתיק החקירה להיות רק זה שכבר סונן ונמצא רלוונטי על ידי גורמי החקירה, ולא כלל המידע שנשאב מהמכשיר.**

193 Association of Chief Police Officers, ACPO Good Practice Guide for Computer based Electronic Evidence, March 2012.

194 במדינות ניו מקסיקו, יוטה וקליפורניה שבארצות הברית כבר קיימת מדיניות שמחייבת מחיקה או גניזה של נתונים. New Mexico's Electronic Communications Privacy Act, Section 3.D.2; Utah's Electronic Information or Data Privacy Act, Section 1.B, 1.D; California's Electronic Communications Privacy Act, 1546.1(d)(2); בנוסף, מדינת ניו יורק מחייבת גניזה של כל רשומות המעצר של אדם שלא הורשע בפשע. New York Consolidated Laws, Criminal Procedure Law – CPL § 160.50 Order upon termination of criminal action in favor of the accused.

בהקשר זה ראוי לציין כי חוק האזנות סתר (שמהווה כעת לטענת משטרת ישראל את האכסניה המשפטית להפעלת רוגלות כגון "סייפן") מורה על מחיקת החומר רק לאחר תום ההליכים המשפטיים, באישור התובע, ורק כאשר ניתן למחוק את החומר במלואו (אחרת יש לנקוט מניעת גישה באמצעות תוכנה ייעודית). לגבי חומר האזנה ששמירתו נדרשת מטעמי ביטחון לא הותוו בחוק כללים ברורים למחיקה, והסמכות לקביעתם נתונה בידי ראש הממשלה.

דרישות ברורות לשמירת רשומות יכולות לעזור לא רק לוודא שרשויות אכיפת החוק נותנות דין וחשבון על חריגה מההיקף של צו חיפוש, אלא גם להגביל באופן משמעותי את הנתונים שרשויות אכיפת החוק יוכלו לשמור במערכות פנימיות כגון מסדי נתונים מודיעיניים, מסדי נתונים על כנופיות וכלי מניעה משטרתיים; וכן להגביל את הנתונים האישיים שייחשפו כתוצאה משימוש לא מורשה על ידי אנשים בגופי האכיפה.[195]

חובות שקיפות על רשויות החקירה

קובעי מדיניות מדינתיים ומקומיים צריכים לחייב דיווח ורישום ציבורי על האופן שבו רשויות אכיפת החוק משתמשות בכלים פורנזיים למכשירים ניידים. יש צורך להפיץ את הרשומות הללו לפחות אחת לחודש, על מנת לאפשר גישה מיידית יותר למידע על ידי עורכי דין, קובעי מדיניות וגורמים בציבור שרוצים להבין את היכולות של רשויות אכיפת החוק שאמונות על ביטחונם. בנוסף לכך, הרשויות צריכות להפיץ דו"חות שנתיים על השימוש הכולל שלהן בכלים אלה, לרבות קביעת חובת דיווח לכנסת ולוועדותיה הרלוונטיות.

הרשומות האלה צריכות לכלול מידע מצרפי על האופן שבו רשויות אכיפת החוק משתמשות בכלים פורנזיים למכשירים ניידים, לרבות:

- בכמה מכשירי טלפון נעשה חיפוש בתקופה נתונה;
- האם החיפושים האלה נעשו בהסכמה (אם כי חיפושים בהסכמה צריכים להיות אסורים), או באמצעות צו חיפוש;
- מספרי הצווים שקשורים בחיפוש, אם זה ישים;
- סוג(י) העבירות שנחקרות;
- באיזו תכיפות הובילו הכלים למיצוי נתונים מוצלח;
- הסברים על מיצוי נתונים שנכשלו;
- אילו כלים (וגרסאות) שימשו למיצוי וניתוח נתונים, ומספרי הגרסאות שלהם.

דוגמה מרכזית ליישום של חובות שקיפות מלאות כלפי המחוקק והציבור היא ארה"ב, שבה החוק מחייב את בתי המשפט לדווח את מספר הבקשות המדינתיות לצווים אשר מבקשים ליירט תקשורת קווית, אוראלית או אלקטרונית, ואת מספר הבקשות אשר התקבלו או נדחו.[196] בנוסף, הדיווחים כוללים בין היתר מידע מפורט ומנותח לגבי סוג העבירות שבו עסקו התיקים שבהם התבקש הצו, סוג המעקב, ומספר המעצרים וכתבי האישום שנבעו מהמידע שהושג באמצעות הצו.

---

195 בשנים האחרונות ניכרת בישראל תופעה בלתי מבוטלת של גישה לא מפוקחת מצד עובדים ברשויות החקירה למאגרי מידע רגישים. ראו: דניאל דולב **מי שומר על השומרים? החיפושים הפיראטיים של שוטרים במאגרי המידע של כולנו** (שומרים, 10.8.2021) (קישור). לדוגמה של שימוש לרעה ביכולות אלה על ידי שוטרים ראו קישור.

196 United States Courts – Wiretapes Reports (link).

הבנת האופן, המועד והסמכות החוקית שמאשרת לרשויות אכיפת החוק להשתמש בטכנולוגיות העוצמתיות האלה יכולה להגדיל שקיפות ומתן דין וחשבון. מעבר לשקיפות כשלעצמה, רשומות כאלה הן חשובות מכיוון שהן יכולות לסייע לעורכי דין, לחוקרים, לקובעי מדיניות ולציבור. באופן כללי יותר, רשומות כאלה יכולות לעזור לקרוא תיגר על הנרטיב של רשויות אכיפת החוק בנוגע לשאלות איך, מתי ומדוע הן משתמשות בכלים האלה.

אסדרת מערכת היחסים והגישה לנתונים בין רשויות החקירה לספקי טכנולוגיות פורנזיות דיגיטליות

העובדה כי הכלים הפורנזיים שמפעילות רשויות האכיפה לפריצה ולחיפוש בטלפונים חכמים או להאזנת סתר לתקשורת בין מחשבים מסופקים לה על ידי חברות פרטיות מעוררת שאלות בנוגע לגישה של אותם גורמים פרטיים לנתונים על הפעלת הכלים הללו או מטרותיה. כפי שנוכחנו לדעת מדו"ח ועדת מררי, לחברת NSO למשל יש יכולת להפיק מידע על הפעלות הכלים שסיפקה למשטרת ישראל, ניסיונות להפעלה ואולי אף מידע על יעדיהם. על כן, אסדרה עתידית של תחום זה נדרשת להתייחס לכמה היבטים יסודיים.

ראשית, אסדרה עתידית חייבת לכלול כללי סף להתקשרות גורמי האכיפה המדינתיים עם חברות פרטיות המספקות שירותי פריצה לטלפונים ניידים או "האזנה לתקשורת בין מחשבים", שייקבעו בחקיקה לגבי פעולות עתידיות של כלל גופי האכיפה הרלוונטיים. מגבלות אלו צריכות להתחיל ולהיות מבוססות על קביעת איסור גורף על נגישות של הגורם הפרטי למידע הנאסף בעזרת המכשירים אשר סיפק, והעיקרון שלפיו המידע המופק והכלים והמידע המתעד את הפעלתם ייאגר רק במאגרים מדינתיים.

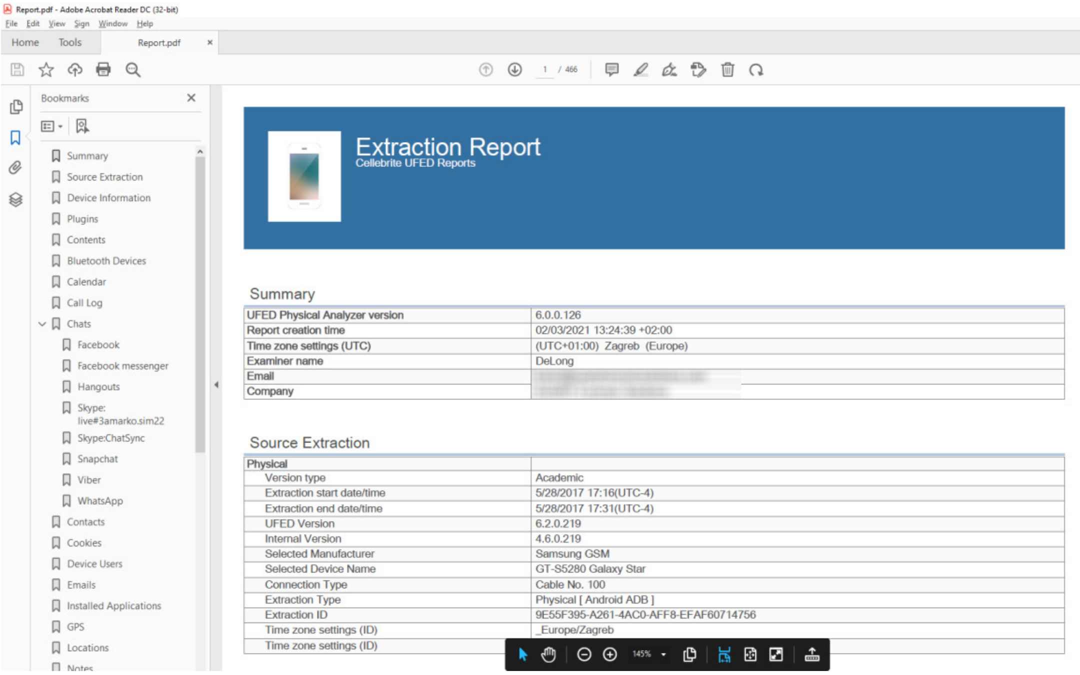
הדרכות והשתלמויות לשופטים על טכנולוגיות פורנזיות ויכולותיהן

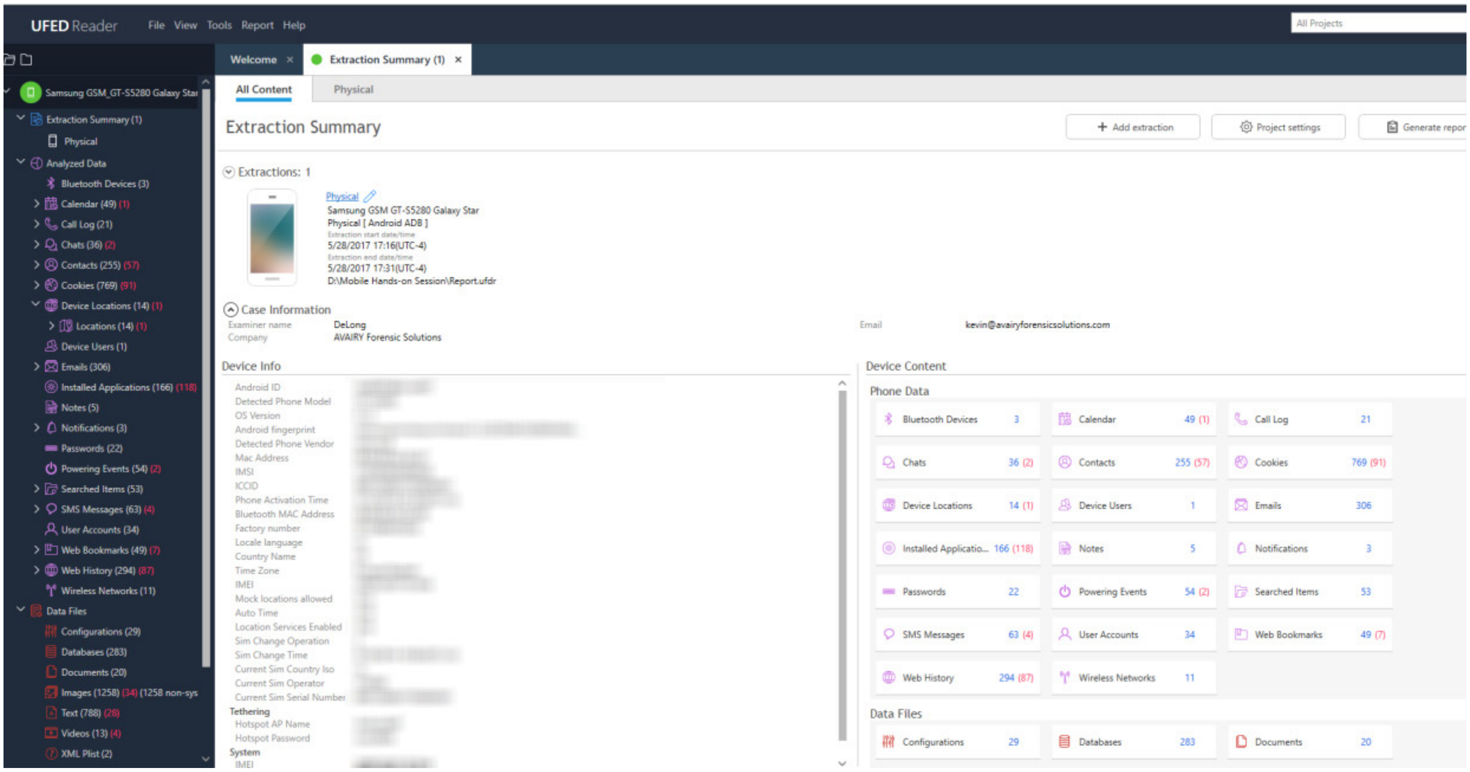
בדומה להמלצת דו"ח ועדת מררי כי יש לקיים השתלמויות עיתיות שבהן יוצגו לשופטים כלל הכלים הטכנולוגיים שבאמצעותם ניתן לבצע האזנות סתר ויכולותיהם,[197] יש לעשות כן גם בנוגע למכלול הכלים הטכנולוגיים שמפעילות רשויות האכיפה לחדירה ולחיפוש בחומר מחשב, ובטלפונים ניידים בפרט, לרבות סוג והיקף המידע המתקבל באמצעותם. יידוע כאמור של כלל שופטי הערכאות הרלוונטיות יחזק בדרך נוספת את האפשרות של בתי המשפט במקרים הקונקרטיים לבצע איזון בין הצורך החקירתי למידת הפגיעה בפרטיות, ואף לבחון האם קיים אמצעי שפגיעתו פחותה.

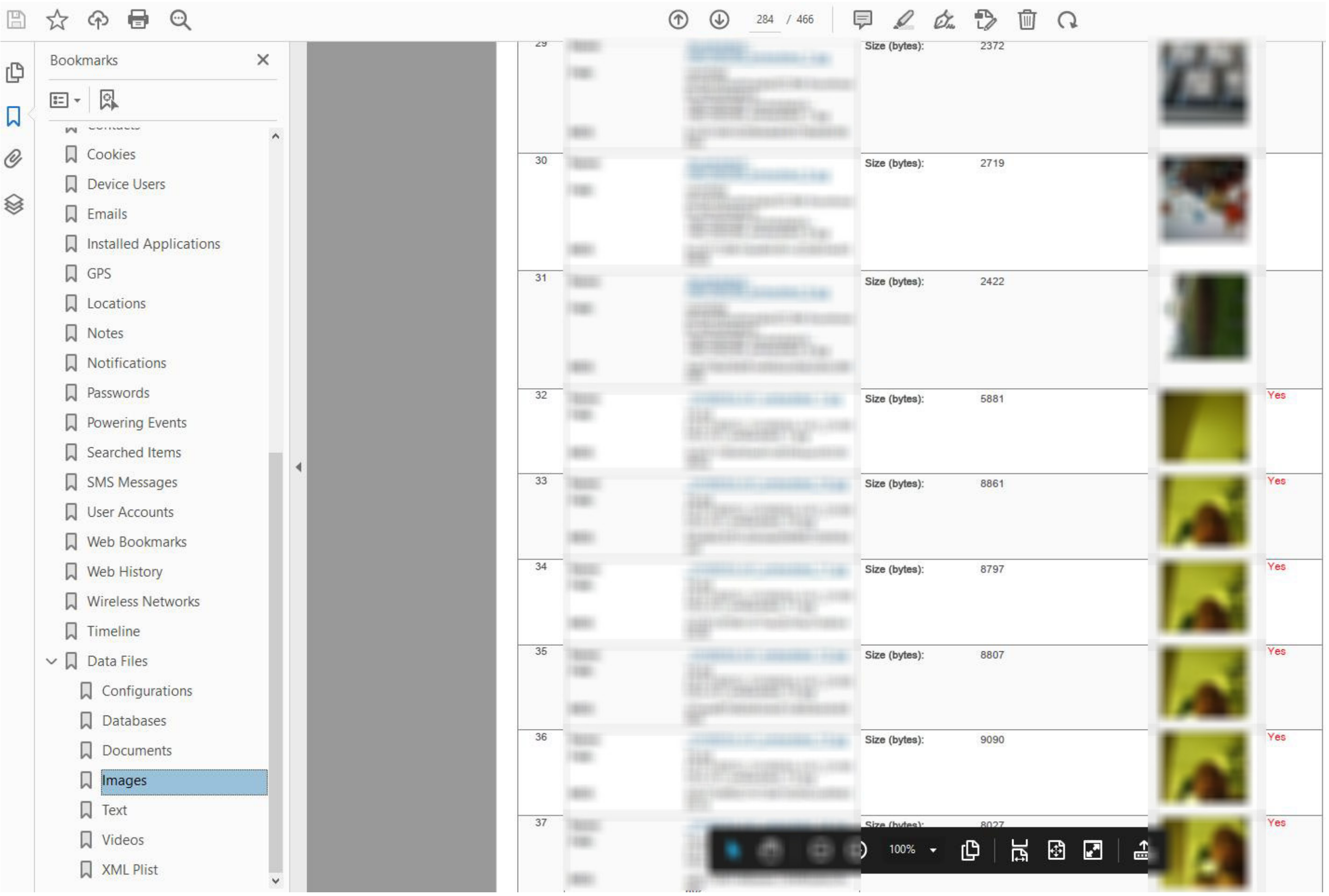
---

197 דו"ח מררי, לעיל ה"ש 39, בעמ' 47 ("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").

נספח א - פלטים המופקים ממערכות Cellebrite






284 / 466
Bookmarks
Cookies
Device Users
Emails
Installed Applications
GPS
Locations
Notes
Notifications
Passwords
Powering Events
Searched Items
SMS Messages
User Accounts
Web Bookmarks
Web History
Wireless Networks
Timeline
Data Files
Configurations
Databases
Documents
Images
Text
Videos
XML Plist
30 Size (bytes): 2719
31 Size (bytes): 2422
32 Size (bytes): 5881 Yes
33 Size (bytes): 8861 Yes
34 Size (bytes): 8797 Yes
35 Size (bytes): 8807 Yes
36 Size (bytes): 9090 Yes
37 Yes
100%

איגוד האינטרנט הישראלי ISOC-IL

נספח ב

משרד המשפטים
פרקליטות המדינה
מחלקת הסייבר

כ"ח באדר א' תשע"ט
5 במרץ 2019

גיא אבנון, שופט
06-03-2019
בית משפט השלום
ראשון לציון (1)

לכבוד
ר' יחידת הסייבר בלהב 433
רח"ט סיגינט-סייבר

שלום רב,

הנדון: ***היתר פנייה לבית-המשפט לצורך בקשה לצו חדירה לחומר מחשב האגור מחוץ לישראל***

הריני להודיעכם כי לאחר שהבאתי את הדברים בפני היועץ המשפטי לממשלה ופרקליט המדינה, ועל דעתם, ניתן בזאת היתר לפנייה לבית משפט השלום בבקשה להוצאת צווי חדירה לחומר מחשב, שיכללו גישה לחומרי מחשב מרוחקים המקושרים אל מחשבים התפוסים כדין בישראל, זאת במסגרת חקירתכם בתיק פלא 118705/18.

ההיתר כפוף לתנאים הבאים:

א. תותר חדירה לחומרי המחשב הנמצאים במחשבים או שרתים מרוחקים כמפורט להלן:
   1) ארנקים וירטואליים וארנקים דיגיטליים שבחזקת החשודים.
   2) תכתובות או שיחות של החשודים באמצעות פלטפורמת טלגרם.
   3) חומרי המחשב שבשרתי המחשב המשמשים, על פי החשד, לניהול בסיסי הנתונים של המיזם העברייני הנחקר.

ב. על צו החדירה לחומר המחשב לכלול התייחסות מפורשת לכך שהוא כולל חדירה לחומרי המחשב המקושרים למחשב או לטלפון סלולרי התפוס בישראל, וזאת בכל מקום בהם נמצאים אותם חומרי המחשב. יש לאשר את נוסח הבקשות לצווי החדירה כאמור עמי מראש.

ג. על החדירה להתבצע בנוכחות המחזיקים של המחשבים או הטלפונים הניידים התפוסים, אלא אם כן יוותרו מרצונם הטוב והחופשי על נוכחותם.

בכבוד רב,

ד"ר חיים ויסמונסקי, עו"ד
מנהל מחלקת הסייבר בפרקליטות המדינה

רח' הנרייטה סולד 1, ת"ד 33475, תל אביב 64924, טלפון: 03-6949380 פקס: 02-6468009
דוא"ל: Cyber-unit@justice.gov.il