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 <u>נתונים ועובדות</u> 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:

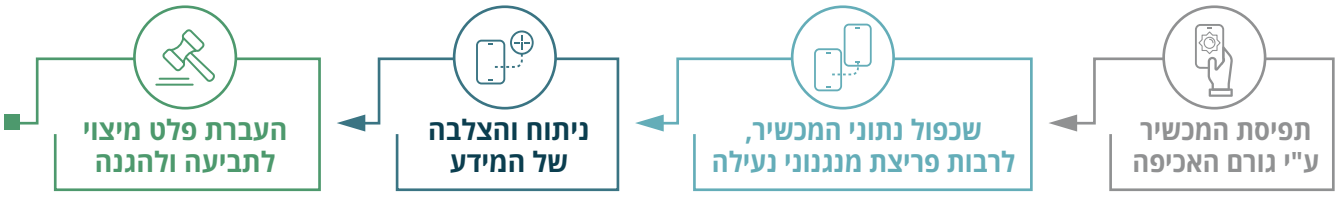
נתונים מתוכנות ייעודיות ויישומונים (אפליקציות): מרבית התוכנות הייעודיות והאפליקציות בטלפונים חכמים יוצרות ושומרות נתוני משתמשים – היסטוריית גלישה, נתונים ומדדים רפואיים, מידע פיננסי והיסטוריית תשלומים, תכתובות, שיחות צ'ט ועוד. הטכנולוגיות הפורנזיות שמפעילות הרשויות יכולות להעתיק נתונים מתוכנות ואפליקציות 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 לדלייית מידע מכל שירות שאליו הן מקושרות.

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:

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

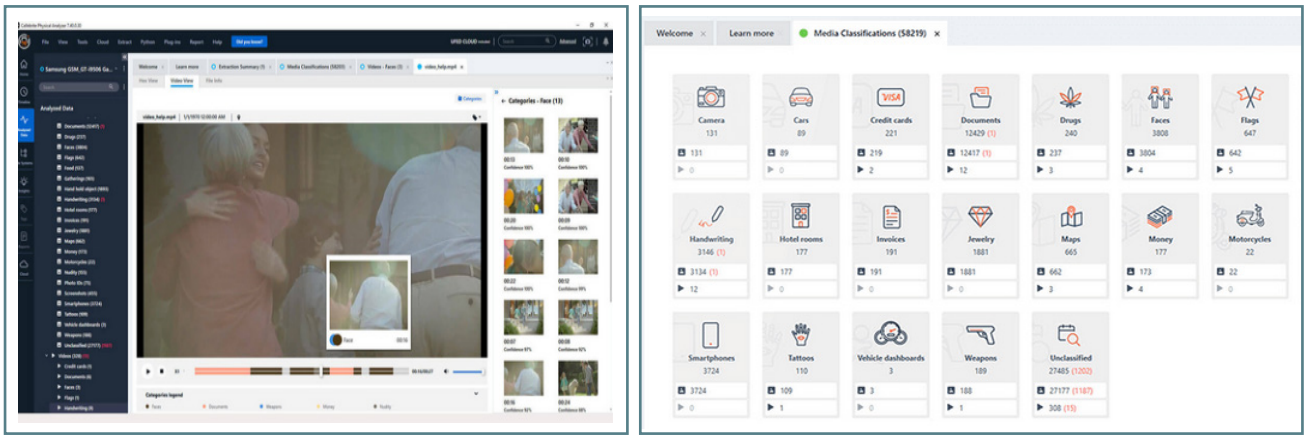
משטרת ישראל מבצעת חדירה, פריצה, חיפוש, האזנה והעתקה של חומר לא רק באמצעות תפיסה פיזית, אלא גם באמצעות רוגלות המותקנות מרחוק ובסתר במערכות מחשוב ובמכשירים חכמים. רוגלה שהותקנה בהצלחה מאפשרת גישה מלאה לתוכן שנאגר במכשיר לאורך זמן (בדומה לחיפוש במכשירים שנתפסו), וכן מעקב אחר השימוש הרציף בו, ביצוע פעולות 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

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 (הוספת או הסרת טקסט, דוא"ל, תמונות, אנשי קשר ועוד), לרבות מכשירים עתידיים.

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:

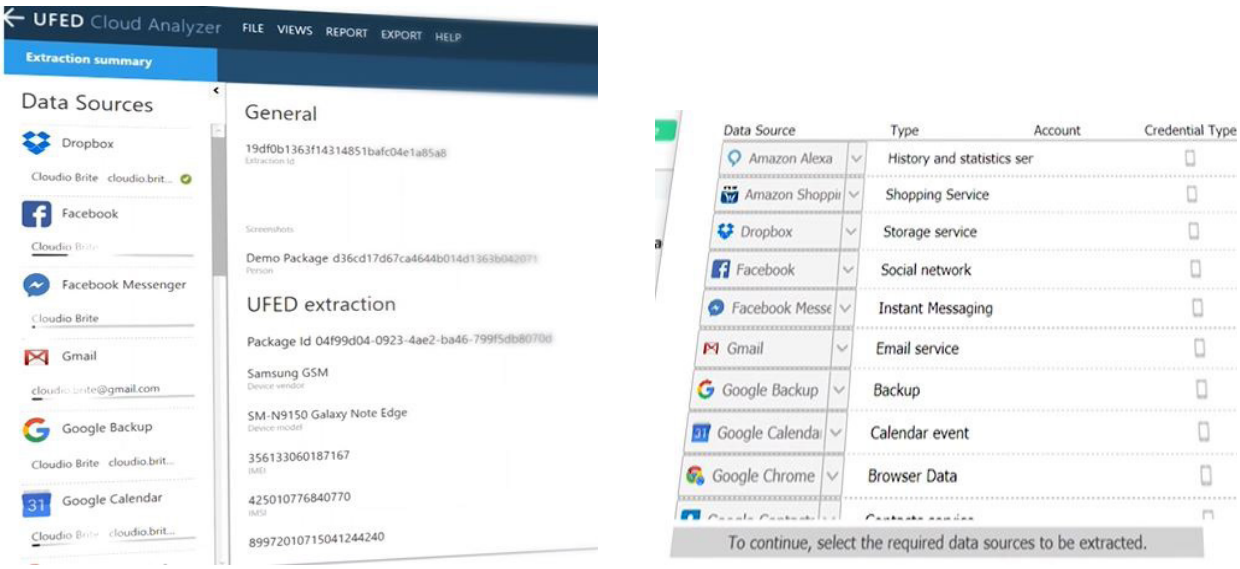
להבדיל מחיפוש במרחב הפיזי, שמוגבל לתפיסה של חומרים רלוונטיים לחקירה, טכנולוגיות לחיפוש במכשירים חכמים ומשאבי ענן המקושרים אליהם מבוססות על חילוץ המידע כולו, ללא סינון מראש לתקופה מסוימת או לסוג חומר רלוונטי בלבד.

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 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 כלים טכנולוגים אלו על בסיס הסכמה בלבד.