בבית המשפט העליון **רע"פ 9446/16**
ב י ר ו ש ל י ם **קבוע לדיון ביום 19.6.2017**

המבקשת להצטרף:

האגודה לזכויות האזרח בישראל
ע"י ב"כ עוה"ד אורי סבח ו/או דן יקיר ו/או אבנר פינצ'וק ו/או עודד פלר ו/או שרון אברהם-ויס ו/או גיל גן-מור ו/או נסרין עליאן ו/או משכית בנדל ו/או טל חסין ו/או שרונה אליהו חי ו/או אן סוצ'יו ו/או רגד ג'ראיסי ו/או רוני פלי ו/או סנא אבן ברי ו/או שדא עאמר

מהאגודה לזכויות האזרח בישראל
רחוב נחלת בנימין 75, תל אביב 65154
טלפון: 03-5608185, פקס: 03-5608165

המבקשת:

התובעת הצבאית הראשית
ע"י ב"כ עוה"ד רס"ן ענת ויינברג ורס"ן ניר שני
מחנה רבין ("הקריה"), תל אביב
טלפון: 03-5696716; פקס: 03-5694643

- נ ג ד -

המשיב:

רב"ט ב' ס'
ע"י ב"כ עוה"ד רס"ן (מיל') עדי ריטיגשטיין-אייזנר
וסרן עומר קנובלר
מטעם הסנגוריה הצבאית
מחנה רבין ("הקריה"), תל אביב
טלפון: 03-5691729; פקס: 03-5692193

ידידת בית המשפט

הסניגוריה הציבורית הארצית
ע"י ב"כ עוה"ד גיל שפירא ויגאל בלפור
רח' הנרייטה סולד 4, תל אביב
טלפון: 03-6932627, פקס: 03-6932617

מתייצב בהליך

היועץ המשפטי לממשלה
ע"י פרקליטות המדינה
משרד המשפטים, ירושלים

עמדת המבקשת להצטרף להליך במעמד של "ידיד בית המשפט"

בהתאם להחלטת בית המשפט הנכבד מיום 29.5.2017, מתכבדת האגודה לזכויות האזרח בישראל להגיש נייר עמדה מטעמה.

8 ביוני 2017

_____

אורי סבח, עו"ד

ב"כ המבקשת

בשים לב לקוצר היריעה ולאור העמדה המפורטת שהגישה בינתיים הסנגוריה הציבורית, נסתפק בציון מספר נקודות והערות. נבקש לתמוך בקריאה לבחינה מחודשת של הילכת **בן חיים**,[1] ולמצער – בקביעה שלפיה **הילכת בן חיים נסמכת על הנחות ועל הנמקות, שאינן מתקיימות בחיפוש בחומר מחשב** ועל כן אין אפשרות להחיל אותה גם על חיפוש כזה.

ויתור על פרטיות בנסיבות של פערי כוחות

1. החלטת בית הדין קמא לפסול את הראיות במקרה שלפנינו לא נסמכה רק על הקביעה העקרונית, שלפיה אין תוקף חוקי לחיפוש במעבדה שנסמך על "הסכמה", אלא גם בשל כך שהנחקר (המשיב דכאן) לא קיבל הסבר מפורט, שהיה עשוי לשוות להסכמה שנתן חזות של הסכמה "מדעת". ההכרעה בדינו של חיפוש "בהסכמה" בחומר מחשב אינה נדרשת אפוא בשל נסיבות המקרה הנדון, והיא גם לא תשפיע על התוצאה המעשית; היא נדרשת בשל השימוש הרב שעושות רשויות החקירה בפיקציה של חיפוש "בהסכמה" בחומר מחשב וזאת בין שהחיפוש מתבצע במעבדה, כפי שהיה בענייננו, ובין שהחיפוש הוא "ידני". הפגיעה השיטתית והנמשכת בזכויות יסוד של נחקרים היא זו שיוצרת את **האינטרס הציבורי לדון ולפסול את הפיקציה של חיפוש "בהסכמה" בחומר מחשב - מעבדתי וידני כאחד**.

2. מטבע הדברים, כתבי הטענות בתיק זה מתמקדים במשפט הפלילי ובהשלכות האפשרויות של הכרעה בתיק זה על הדין והפרקטיקה בתחום זה. אבל הכרעה בתוקפה של הסכמה בנסיבות המקרה שלפנינו עלולה גם להשליך על גורלה של הזכות לפרטיות במישורים רבים אחרים.

3. "הפרטיות נתונה תחת מתקפה קשה שמאיימת להכריעה"[2] המרווח ההולך ונפער בין הטכנולוגיה לבין המשפט מאפשר, בין היתר, לאיין את הזכות לפרטיות באמצעות קביעת עובדות בשטח וניצול של פערי כוח לצורך חילוץ "הסכמה" או "ויתור" על הפרטיות.

4. חלק ניכר מהפגיעות בפרטיות מתרחש במסגרת יחסים בלתי שוויוניים, כאשר הפוגע מתיימר להצדיק את הפגיעה על סמך "הסכמה" שניתנה לו כביכול על ידי הנפגע. הסכמה של נחקר לחיפוש בטלפון הנייד שלו היא רק דוגמא אחת להסכמות "שהן 'חשודות' מטבען", כהגדרתו של פרופ' בירנהק, כיוון שהצדדים "אינם שווי כוח, למשל, המדינה מול האזרח, תאגיד גדול מול צרכן בודד, מעסיק מול עובד...."[3] כך, למשל, בנוגע לאפשרות של מעסיק לעיין בתוכן של תיבת דואר אלקטרונית פרטית של העובד, פסק בית הדין הארצי לעבודה כי "חזקה, כי העובד לא ייתן הסכמה לחדירת המעסיק לתיבה הפרטית שלו ולחשיפת מלוא עולמו האישי, לרבות תקשורת עם צדדים שלישיים... גם אם ניתנה הסכמת העובד מדעת, חזקה היא כי הסכמה זו לא ניתנה מרצון חופשי אלא מכורח, ולכן אינה תקפה".[4] קביעה זו והשיקולים שהנחו את בית הדין הארצי לעבודה רלבנטיים גם לחיפוש במכשיר טלפון חכם, המכיל מידע אישי רב לאין ערוך מהמידע שבתיבת הדואר האלקטרוני.

---

[1] רע"פ 10141/09 **בן חיים נ' מדינת ישראל** (6.3.2012) (להלן: פס"ד **בן חיים**).

[2] מיכאל בירנהק "**שליטה במידע והסכמה מדעת: הבסיס העיוני של הזכות לפרטיות**" **משפט וממשל** יא 9 2007 עמ' 10, 14.

[3] מיכאל בירנהק, **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה**, ע' 253 (2011).

[4] ע"ע (ארצי) 90/08 **איסקוב - הממונה על חוק עבודת נשים**, בפסקאות 49-52 (8.2.2011); ר' עוד: בר"ע (ארצי) 44667-05-13 **בת-חן שחר – עיריית שדרות** (21.6.2013) (שעון נוכחות ביומטרי); עס"ק (ארצי) 7541-04-14 **הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי נ' עיריית קלנסווה** (15.3.2017).

5. בחינה של "ההסכמה" לפגיעה בפרטיות בעידן הנוכחי, צריכה גם להביא בחשבון את המגבלות והכשלים המובנים שמגבילים את היכולת לתת הסכמה מדעת ומרצון חופשי, בעיקר בכל הקשור למידע אישי הנשמר במדיה דיגיטלית.[5]

6. מנגד הכרה בתוקפה של "הסכמה" שנגבית מנחקר – אדם המצוי בנסיבות קיצוניות של נחיתות בידע, עייפות פיזי ונפשית, ותחושה של מצוקה וחוסר אונים – עלולה להכשיר ואף לתמרץ את הפרקטיקה של חילוץ הסכמות כפויות לפגיעה בפרטיות בכל המישורים האחרים – יחסי העבודה, צרכנות, יחסינו עם תאגידי הענק באינטרנט ועוד.

חיפוש בטלפון סלולרי – הלכה למעשה

7. נבקש לשפוך אור על האופן שבו מתבצע חיפוש בטלפון חכם, ועל הדרכים הבלתי נדלות שהוא מאפשר לחשיפת מידע אישי עצום בהיקפו ורגיש במהותו. בכך נבקש להמחיש עד כמה חמורה היא הפגיעה בפרטיות כתוצאה מחיפוש בחומר מחשב שבטלפון הנייד – בשונה מהפגיעה הקלה יחסית ששימשה טעם מרכזי בהלכת בן חיים להכרה באפשרות שהסכמה תינתן **מרצון חופשי**. בדרך זו גם נוכל להיווכח עד כמה בלתי סביר הוא שאדם, שמתבקש להסכים לחיפוש בטלפון הנייד שלו, יוכל לעמוד על היקף המידע האישי שהוא חושף ועל טיבו – דהיינו שיתקיים יסוד "**ההסכמה <u>מדעת</u>**".

8. החיפוש שנערך במכשיר הטלפון החכם של המשיב נעשה באמצעות ערכת UFED Cellebrite.[6] פרטים על ערכה זו ניתן למצוא בפסיקת בתי הדין הצבאיים: ניתן להפיק באמצעותה את המידע הנמצא על מכשיר הטלפון, ולאחר "העתקת החומר המצוי על גבי המכשיר, נעשה שימוש בתוכנה של חברת 'סלברייט' על מנת לנתח את כלל המידע שהופק".[7] חוקרי מצ"ח מפיקים בעזרת הערכה, בין היתר, מידע על רשימות אנשי קשר; מסרוני טקסט שנשלחו והתקבלו, כולל מסרונים שנמחקו; הודעות שנשלחו באמצעות יישום whatsapp ומידע על אנשי הקשר החברים בקבוצות whatsapp ותמונות.[8]

9. פירוט נוסף על מערכת UFED (Universal Forensic Extraction Device) ניתן למצוא בפרסומים רשמיים של חברת סלברייט. המערכת מסוגלת להפיק מידע גם על יישומי תקשורת, רשתות חברתיות ושירותי מידע כמו פייסבוק, סקייפ, טוויטר ועוד.[9] החברה מתהדרת בכך שהמערכת מסוגלת להפיק מידע שהמשתמש ביקש למחוק, ומידע שמכשיר הטלפון אוגר ללא מעורבת המשתמש ולעתים **אף ללא ידיעתו**, כמו מידע על מיקום, רשתות אינטרנט אלחוטי אליהן התחבר המכשיר, כותרות של הודעות דוא"ל, היסטוריית גלישה באינטרנט.[10]

---

[5] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1885 (2013).

[6] פס' 10 לפסק הדין נשוא בקשת הערעור, ע 24/15 (ערעורים צה"ל) **<u>ב.ס. נ' התובעת הצבאית הראשית</u>** (6.11.2016).

[7] ראו 407/15 (צבאי דרום) **<u>התובע הצבאי נ' ר. ש.</u>**, פס' 12-13 (19.6.2016); 313/15 (צבאי צפון) **<u>התובע הצבאי נ' ז. א. נ.</u>**, עמ' 2, 4 (3.2.2016); מר/112/13 (צבאי מרכז) **<u>התובע הצבאי נ' ל. ל.</u>**, פס' 27 (30.12.2014).

[8] 313/15 (צבאי צפון) **<u>התובע הצבאי נ' ז. א. נ.</u>**, עמ' 4-5, 9 (3.2.2016); מר/112/13 (צבאי מרכז) **<u>התובע הצבאי נ' ל. ל.</u>**, פס' 27, 70 (30.12.2014); ע 16/14 (ערעורים צה"ל) **<u>ל. כ. נ' התובע הצבאי הראשי</u>**, פס' 4, 80 (18.4.2016).

[9] Cellebrite, *<u>What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes</u>*, pp. 4, 8. כל אתרי האינטרנט נבדקו ב-7.6.2017.

[10] "Content that the phone collects without any user action (and sometimes without user knowledge)", Cellebrite, *What Happens When You Press that Button?* p. 9-10

10. המערכת מסוגלת גם לעקוף כל סוג של נעילה, הצפנה או הגנה במרבית המכשירים הסלולריים הפועלים על מערכת ההפעלה אנדרואיד[11] ובחלק גדול מהמכשירים מסוג אייפון.[12] משמעות הדבר היא שלמרות שמשתמש המכשיר התכוון במפורש למנוע גישה למכשיר למי שאינו מחזיק בסיסמה או בקוד הגישה, **ניתן בכל זאת להפיק את המידע במכשיר, גם ללא הסכמתו של המשתמש**, מבלי לקבל את הרשאתו ומבלי ליידע אותו.

11. מערכות של החברה מסוגלות לחשוף סיסמאות של המשתמש שנועדו להפעיל יישומים שונים המותקנים במכשיר, כמו שם המשתמש וסיסמת המשתמש בחשבון הדואר האלקטרוני, חשבונות ברשתות חברתיות או שירותי אינטרנט אחרים.[13] זאת, גם ללא קבלת רשותו או הסכמתו של מחזיק המכשיר לחשיפת סיסמאות אלה.

12. למעשה, מערכת UFED של סלברייט, כמו מוצרים דומים של חברות אחרות,[14] מיועדת להפיק מידע ממכשיר סלולרי גם **ללא מודעותו ובניגוד לרצונו ולכוונתו המקורית של מחזיק המכשיר**: מידע שנמחק על ידי משתמש המכשיר; מידע ממכשיר שהותקנה עליו סיסמת נעילה, או חשיפה של סיסמאות המאוחסנות על גבי המכשיר.

13. חומרת הפגיעה בזכות לפרטיות גדולה הרבה יותר, שעה שהמידע הנאסף הוא מידע שמחזיק המכשיר לא היה מודע לקיומו, או היה סבור שהוא מוצפן או נעול בעזרת סיסמה. לא דומה חיפוש בארון מסמכים לחיפוש בארון מסמכים **נעול**, במיוחד כאשר החיפוש מסתמך על "הסכמה" ראשונית של המחזיק במכשיר, אך לא מתבקשת הסכמה מפורשת לפתיחת כל אחת מהנעילות והסיסמאות. לא ניתן לדבר על הסכמה **מודעת**, שעה שמהות החיפוש ומהות המידע שעשוי להתגלות אינם מוסברים היטב לנחקרים. אדם יכול להבין מהו חיפוש בכליו ובכיסיו, אך רובם המכריע של המשתמשים בטלפון חכם יכולים רק לנחש מה תהיה התוצאה של "שימוש בכל אמצעי טכנולוגי שברשותה" של מצ"ח, כפי שהדבר מנוסח בטופס ההסכמה של מצ"ח, שצורף לבקשת רשות הערעור. בוודאי שלא ניתן לדבר על הסכמה מודעת כאשר חלק מהמידע המופק הוא מידע שמשתמש הטלפון לא היה מודע לקיומו.

14. חשוב לציין, כי ההבחנה בין חיפוש במעבדה לחיפוש שנערך בנוכחות הנחקר הולכת ומיטשטשת. סלברייט משווקת ערכות מסדרת UFED Field Series, המאפשרות לכל שוטר להתחבר למכשירים סלולריים ולקבל גישה מיידית למידע שבהם.[15] לפיכך, ההבחנה שביקש לעשות בית הדין הצבאי בפסק הדין נשוא הערעור, בין חיפוש "ידני" לבין "חיפוש במעבדה" הינה הבחנה בעייתית, והיא עשויה להיות לא רלבנטית בעתיד הקרוב. כבר כיום ניתן לבצע חיפוש באמצעות מסוף נייד בנוכחות הנחקר, מבלי לשלוח את המכשיר למעבדה ולקבל תוצאות זהות. לפיכך, כפי שציינה הסנגוריה הציבורית בפס' 161

---

[11] "bypassing any type of lock (Pattern/PIN/Password)", Cellebrite, *Android Forensics - Physical Extraction and Decoding from Android Devices*

[12] Cellebrite, *iOS Forensics - Physical Extraction, Decoding and Analysis from iOS Devices*.

[13] "Extract and analyze real-time mobile data, including call logs, contacts, calendar, SMS, MMS, media files, apps data, chats, **passwords**". Cellebrite, *Extend Immediate Access to Mobile Forensic Data in the Field*.

[14] Eoghan Casey and Benjamin Turnbull, *Digital Evidence on Mobile Devices*, *in*: DIGITAL EVIDENCE AND COMPUTER CRIME (2011), 23-28.

[15] Cellebrite, *Extend Immediate Access to Mobile Forensic Data in the Field*.

בעמדתה, הנימוקים לכך שלא ניתן להסתפק בהסכמת הנחקר לביצוע חיפוש בטלפון סלולרי תקפים הן לחיפוש שנערך במעבדה, והן לחיפוש שנערך בנוכחות הנחקר.

היקף המידע הנאגר במכשירי טלפון חכמים, ביישומים השונים, ובשירותי ענן מקושרים

15. מחקר עדכני מצא כי על גבי טלפון חכם מותקנים בממוצע 70-100 יישומים שונים,[16] המשמשים למגוון רב של מטרות. המידע שנאסף על ידי היישומים כולל מידע אישי רב, הקשור לעצם השימוש ביישום (כמו, מסרונים שהועברו באמצעות whatsapp) אך גם מידע שנאסף באופן "אגבי". כך, למשל, יישום סטנדרטי של חברת גוגל עשוי לאסוף מידע מדויק על מיקומו של המכשיר על פני ציר הזמן, לאסוף מידע על חיפושי אינטרנט והיסטוריית הגלישה.[17] מידע זה מאוחסן הן במכשיר הטלפון החכם עצמו, והן בשרתים של ספקי השירות.

16. המידע, כמו גם עצם הרשאת השימוש בשירות או ביישום, מוגנים לרוב באמצעות שם משתמש ייחודי וסיסמה, המאוחסנים גם הם על המכשיר, כך שהמשתמש במכשיר יוכל לעשות שימוש בשירותי האינטרנט השונים.

17. ההסדר החקיקתי לחיפוש בחומר מחשב, קובע שקבלת מידע מתקשורת בין מחשבים אגב חיפוש לא תיחשב כהאזנת סתר.[18] מכאן, שמתן היתר לחיפוש בחומר מחשב ובמכשירי טלפון חכם יאפשר קבלת מידע מתקשורת שהתנהלה ותתנהל בין המחשב שבו נערך החיפוש לבין מחשבים אחרים, ולעקוף בכך את הדרישות החוקיות המחמירות לקבלת צו להאזנת סתר. בפרט, **תתאפשר גישה למידע שנאגר באמצעות יישומים המותקנים במכשיר ואשר מאוחסן גם בשרתים מרוחקים**.[19] זאת, במיוחד, שעה שההסכמה מנוסחת כך שהיא הסכמה "לחדירה **נמשכת** לחומר מחשב", כפי שהיא מנוסחת כיום בטופס ההסכמה של מצ"ח, שצורף בנספח ט' לבקשת רשות הערעור.

18. אם יתאפשר חיפוש על בסיס הסכמתו של מחזיק המכשיר, יתאפשר גם חיפוש בכל עשרות היישומים שהותקנו על המכשיר. הסכמה זו עשויה אף לאפשר חיפוש במידע המוצפן או מוגן באמצעות סיסמה. את הסיסמה הקליד המשתמש כאשר התקין את היישום, אך כעת התביעה משתמשת בהסכמתו לחיפוש במכשיר גם בתור הרשאת גישה והרשאת חיפוש בכל שירותי המידע שהותקנו על המכשיר, כולל שמות המשתמש והסיסמאות השונות. בניגוד לטענת התביעה, משתמש הטלפון החכם אינו יכול לזכור את כל היישומים המותקנים במכשיר, את כל ההרשאות שהעניק ליישומים, מה היה היקף השימוש שלו בכל אחד מהיישומים ואיזה מידע נאגר אודותיו בשרתי הענן של כל אחד משירותי האינטרנט הללו. רק אדם שאינו משתמש בטלפון יכול לטעון, כפי שטענה התביעה, כי "אין כל יסוד להניח שהנחקר אינו מודע

---

[16] המחקר בדק משתמשים מכמה ארצות, בהן הודו, ברזיל, סין, גרמניה, ארצות הברית, צרפת, בריטניה יפן, מקסיקו. App Annie, *Spotlight on Consumer App Usage*, May 2017.

[17] Becca Caddy, *Google Tracks Everything You Do: Here's How to Delete it*, WIRED UK, 20.3.2017.

[18] סעיף 23א(ג) לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969.

[19] ראו למשל ערכה מיוחדת של חברת סלברייט, שנועדה לאסוף מידע משירותי ענן, באמצעות שמות משתמש וסיסמאות המופקות ממכשירי טלפון סלולריים. Cellebrite, *Extracting Legally Defensible Evidence from the Cloud*.

לקיומן של אותן ראיות מפלילות במכשירו הסלולארי, או לכל הפחות נותן דעתו ומעיינו להן" (ס' 89 לבקשת רשות הערעור).

19. התביעה מבקשת לראות בהסכמת הנחקר לבצע חיפוש בטלפון סלולרי **הסכמה מלאה מדעת** לבצע חיפוש בכל המידע האגור ביישומים השונים המותקנים במכשיר. היא מבקשת להשתמש במפתח אחד – בהסכמה שנתן המשתמש לגישה למכשיר עצמו – כמעין מפתח "מאסטר" שיאפשר גישה לכל היישומים השונים המותקנים על המכשיר, המוצפנים כל אחד בסיסמה ובמנעול נפרד משלו. הדבר דומה לחיפוש בהסכמה בבית, אשר במסגרתו נתקלים החוקרים בחדר נעול. אם יפרצו החוקרים את הדלת הנעולה ללא רשותו וללא ידיעתו של האדם אשר הסכמתו אפשר את החיפוש מלכתחילה, ברור שייפגע רכיב ההסכמה המלאה בחיפוש. כך גם בנוגע לחיפושים הנערכים ביישומים השונים המותקנים על מכשיר טלפון חכם.[20]

התפתחויות טכנולוגיות צפויות

20. מתן היתר לביצוע חיפוש בהעדר צו במכשיר טלפון חכם, עשוי להיות מיושם בעתיד הקרוב גם למקרים אחרים של חיפוש בחומר מחשב. כבר היום, מצוידים בתים רבים במכשירים המקליטים ומצלמים את הנעשה בקרבתם (קונסולות משחק, טלוויזיות "חכמות", מצלמות אבטחה, או מכשירים כדוגמת Amazon Alexa).[21] מכשירים אלה מחוברים לרשת האינטרנט, והמידע שהם אוגרים מאוחסן בשרתים ומחשבים העשויים להיות מושא לחיפוש. לעתים קרובות ניתן לגשת למידע זה גם ממכשירים סלולריים. עולם המכשירים החכמים והמקושרים, the Internet of Things, הולך ומתפתח, ועמו גם כמויות המידע הנאגר, והאתגרים הנוגעים לזכות לפרטיות.[22] יש לתת את הדעת להתפתחויות אלה כאשר דנים בסוגיה העקרונית של חיפוש בחומר מחשב. מתן גישה להודעות וואטסאפ או למסרונים שהועברו באמצעות פייסבוק, באמצעות חיפוש שנעשה בהעדר צו, עשוי לאפשר גישה לכמויות אדירות של מידע אישי, פרטי, אינטימי, הנאגר ונאסף באופן אוטומטי, ועשוי להכיל מידע רב גם על צדדים שלישיים.

---

[20] ראו מר/112/13 (צבאי מרכז) **התובע הצבאי נ' ל. ל.**, פס' 85-86: "היכולת הטכנולוגית המאפשרת לשמור את המידע בתוך שרתים ו"עננים" כאלה ואחרים, בעלי היקף אכסון בלתי מוגבל, מביאה לכך שבחיפוש במכשיר עשויים להימצא חומרים רבים מאוד, אף מעבר להיקף הזכרון של המכשיר עצמו... הקושי העיקרי במתן הסכמה כתחליף לצו שיפוטי, הוא בכך שהסכמה כזו נתפסת כבלתי מסוייגת וכזו הכוללת את כלל המידע האצור על גבי המכשיר".

[21] Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices*, April 2016.

[22] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment Effects*, 104 CAL. L. REV. 805 (2016).