

# השימוש בכוח סביר לשם התגברות על הגנת סיסמה והצפנה: הצדקות וביקורות

חיים ויסמונסקי\* ועמוס איתן\*\*

## 1. הקדמה

על-ידי רשויות המדינה או, לחלופין, מצד גורמים עוינים. פיתוחים טכנולוגיים אלה מוטמעים במוצרים שמפתחות חברות אלה ואחרות כבר בשלב עיצוב המוצר, כחלק מקידום תפישה המכונה Privacy by Design<sup>2</sup>, כאשר המניע העיקרי לפעולות אלה הוא, מטבע הדברים, מניע כלכלי. יישומים מגבירי-פרטיות מקודמים ומשווקים פעמים רבות על-ידי חברות פרטיות מתוך ההנחה שקהל המשתמשים יתומרך בכך לרכוש את מוצריהן או להשתמש בשירותיהן.<sup>3</sup>

לטכנולוגיות מגבירות פרטיות המוטמעות במחשבים וטלפונים סלולריים "חכמים" יכולים להיות שימושים מסוגים שונים: חלקן מאפשר להצפין את התקשורת המקוונת של הפרט<sup>4</sup>, חלקן מאפשר לשמור על זהותו אנונימית<sup>5</sup> וחלקן מגביר את יכולתו של הפרט לבחור האם ועד כמה לשתף מידע אישי.<sup>6</sup> חלק אחר, בו נתמקד ברשימה זו, נועד למנוע גישה לתכנים האגורים במחשב, בטלפון הסלולרי, בהתקן האחסון הנייד או ביישומון ללא הרשאה מאת המחזיק כדין במכשיר או המשתמש ביישומון.

אין ספק שטכנולוגיות אלה משרתות מטרה ראויה ומאפשרות למשתמש לשלוט, ולו במידה מסוימת, במידע על אודותיו, ולבצר את בלעדיותו על הגישה למחשבו האישי, לטלפון הסלולרי שלו, להתקן האחסון הנייד שלו או לחשבונו האישי ביישומון בשימוש. אולם, בצד כל אלה, הגבלת הגישה של גורמים בלתי מורשים לתכנים האגורים במחשב

לאחרונה במסגרת גיליון מספר 267 של כתב עת זה פרסמו חברינו המלומדים מהסגוריה הציבורית, גיל שפירא, מנהל מחלקה וממונה ארצי על ייצוג אסירים, ויגאל בלפור, עוזר משפטי לסגור הציבורי הארצי, מאמר ובו ביקרו את הפרקטיקה של שימוש בכוח לצורך נטילת טביעת-אצבע הנדרשת לצורך חזירה למכשירי טלפון סלולריים.<sup>1</sup> במאמרם טענו בלפור ושפירא כי בהיעדר מקור סמכות מפורש בחקיקה ראשית, אין רשויות החקירה רשאיות ליטול בכוח טביעת אצבע מנחקר לצורך חזירה לטלפונים סלולריים. לנוכח חשיבות הנושא, התכבדנו לפרסם מאמר תגובה זה המבקש להציג את ההצדקות ולהתמודדות עם הביקורות על פרקטיקה זו. מסקנתנו בדבר המצב המשפטי הנוכחי – הפוכה משל חברינו המלומדים. כפי שנציג להלן, לגישתנו ניתן להשתמש בכוח סביר לצורך התגברות על הגנת סיסמה והצפנה, ככל שהדבר אפשרי מבחינה טכנית וככל שהשימוש בכוח מתגבר במישורן על הגנת הסיסמה ולא מוביל את החשוד למסור בעצמו את ה"מפתח" לצורך החזירה אל חומרי המחשב המוגנים שלו.

## 2. מבוא

ההגנה על מידע פרטי הפכה בשנים האחרונות לאחד מהמרכיבים החשובים ביותר בפיתוחים הטכנולוגיים שמקדמות ומייצרות חברות פרטיות. חברות פרטיות כמו Google או Apple מובילות מהלכים שנועדו להגן על פרטיותם של משתמשיהן מפני פגיעה בפרטיות

\* דוקטור למשפטים, מנהל מחלקת הסייבר בפרקליטות המדינה, עמית מחקר במרכז הסייבר האוניברסיטאי של האוניברסיטה העברית, מרצה מן החוג באוניברסיטת תל-אביב באוניברסיטת חיפה. תודה לדי"ר אלקנה לייסט, הסגור הציבורי המחוזי במחוז תל-אביב ועל"ד נועה זעירא מהסגוריה הציבורית הארצית על הערותיהם הטובות למאמר. האמור במאמר מבטא את עמדתם האישית של הכותבים בלבד.

\*\* עורך-דין במחלקת הסייבר בפרקליטות המדינה, סטודנט לתואר שני בפקולטה למשפטים באוניברסיטת תל-אביב ועוזר מחקר במרכז הסייבר האוניברסיטאי של האוניברסיטה העברית.

1 יגאל בלפור וגיל שפירא "ונשמרתם לאצבעותיכם: חובתו של חשוד לסייע לחיפוש במכשיר סלולרי ושימוש בכח לשם פתיחת מכשיר הנעול באמצעות טביעת אצבע" הסניגור 4 267 (2019) (להלן: בלפור ושפירא "ונשמרתם לאצבעותיכם").

2 תקנות האיחוד האירופי בנוגע הגנת מידע מתייחסות לרעיון של Privacy by Design וקובעות - "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation Article 25 (2))."

3 כדוגמה בלבד ראו: Heather Kelly *Everything Apple announced at WWDC, from Apple sign-in to dark mode*, CNN BUSINESS (3.6.2019), <http://edition.cnn.com/2019/06/03/tech/wwdc-2019-apple-keynote/index.html>. חברת Apple הודיעה כי תאפשר למשתמשיה להירשם ליישומים שונים ברשת האינטרנט באמצעות כתובת דואר-אלקטרוני פיקטיבית, זאת כדי לאפשר למשתמשיה שלא לחלוק מידע פרטי עם חברות אחרות כמו Google או Facebook.

4 כך הדבר, למשל, בכל הנוגע לתכתובות ביישומון להעברת המסרים המידיים WhatsApp, שבו מוצפנות באופן אוטומטי כל התכתובות בין משתמשי הקצה, ורק משתמשי הקצה המתקשרים ביניהם יכולים לעיין בהודעות המפוענחות, כאשר לחברת WhatsApp אין את מפתחות ההצפנה והיא לא מסוגלת לעיין בתוכן הודעות משתמשי הקצה. ראו: WhatsApp FAQ, "End-to-end encryption" (10.7.2019) <https://faq.whatsapp.com/en/android/28030015>.

5 כדוגמה לשירותים המאפשרים לשמור על אנונימיות בצורה מוגברת ניתן להזכיר שירותים כמו VPN או Tor. VPN (Virtual Private Network) הוא שירות המאפשר למשתמש לגלוש ממחשבו לשרת מסוים, וממנו "לצאת" אל האינטרנט, כך שההתחקות לאחור אחר פעולתו של המשתמש תוביל לכתובת ה-IP של אותו שרת, ולא אל כתובתו האמיתית של המשתמש. Tor (The Onion Router) הוא דפדפן המאפשר למשתמש לגלוש בצורה מוצפנת ואנונימית, כאשר תעבורת הרשת מתקום מושבו של המשתמש עוברת דרך מספר שרתים ממדינות שונות בדרך אל יעדה.

6 כדוגמה לשירותים שבהם המשתמש יכול לבחור האם ועד כמה לשתף במידע אישי, ראו למשל את האפשרות שניתנת למשתמשים ברשתות חברתיות כגון פייסבוק או אינסטגרם להחליט על מאפייני הפרטיות של חשבון המשתמש שלהם. בכלל זה, באפשרותו של המשתמש לבחור האם לחסום משתמשים ספציפיים מלקרוא את התוכן שהוא מפרסם, האם לשתף מידע באופן ציבורי, רק ל"חברים" של המשתמש או לאף אחד, וכיצא באלה אפשרויות לשליטה על מידת החשיפה אל המידע האישי של המשתמש.

או במכשיר טלפון "חכם" טומנת בחובה אתגר ניכר לרשויות אכיפת החוק. למעשה, ישנם מקרים שבהם רשויות אכיפת החוק לא יכולות ברמה הטכנית, בוודאי לא בפרק זמן סביר, להתגבר על הגנת סיסמה או על הצפנה שמונעות גישה למידע האגור במכשיר. כך אירע למשל בעת חקירת פיגוע הירי שאירע בסן-ברנרדינו (קליפורניה) בשנת 2015, שבו נרצחו 14 בני-אדם ונפצעו 22. באותו מקרה, החזיקה ה-FBI במידע אשר הביא אותה לחשוד כי בפיגוע היו מעורבים שלושה מפגעים (ולא שניים, כפי שהחקירה העלתה בראשיתה). ה-FBI סברה כי ראיות לקיומו של יורה שלישי אגורות בטלפון הסלולרי של אחד היורים, מכשיר מסוג iPhone 5C.<sup>7</sup> חרף השקעת מאמצים אדירים מצד ה-FBI, הוסכנות לא הצליחה במשך תקופה ארוכה לחדור אל הטלפון הסלולרי ולעיין במידע האגור בו.<sup>8</sup> בישראל מוכרת בציבור הפרשה בה היה מעורב גם עורך-הדין רונאל פישר, שעניינה בעבירות שוחד, מרמה והפרת אמונים שיוחסו למעורבים בפרשה. חקירת הפרשה התעכבה במשך חודשים ארוכים בשל טענתו של פישר כי אינו זוכר את סיסמת הכניסה לטלפון הנייד שלו.<sup>9</sup> אומנם בשתי פרשות אלה עלה בידי החוקרים לפצח את סיסמת הכניסה לטלפונים הסלולריים של החשודים, אולם במקרים מסוימים לא מצליחות רשויות אכיפת החוק לחדור אל המחשב, הטלפון הסלולרי, התקן האחסון הנייד או היישומון המוגנים בסיסמת כניסה. זאת אף אם השקיעו משאבים בלתי מוגבלים לשם כך.<sup>10</sup> האתגר המוצב לפתחן של רשויות החקירה איננו אתגר מקומי-ישראלי, אלא אתגר לו שותפות רשויות אכיפת החוק במדינות רבות בעולם. רק לאחרונה, פרסמו ממשלותיהן של ארצות-הברית, בריטניה, קנדה, אוסטרליה וניו-זילנד הצהרה משותפת, המעידה על היקפו וחומרתו של האתגר שמוצב בפני רשויות החקירה במדינותיהן.<sup>11</sup> יש הטוענים כי הדרך להתגבר על האתגר האמור טמונה בהקצאת משאבים רבים יותר לרשויות החקירה,<sup>12</sup> אולם המציאות, כך נראה, מלמדת כי לא תמיד ניתן לייצר "פותר מנעולים" טכנולוגי זמין לכל מחשב, טלפון סלולרי, התואם כל מערכת הפעלה וכל יישומון המותקן עליהם.

המתח בין צרכי החקירה מחד גיסא, לבין זכויותיהם של המשתמשים בחומרי המחשב המוגנים בסיסמה מאידך גיסא, מעורר שאלות מכבידות. נמנה כמה מהן: (א) האם ניתן לחייב נחקר למסור את "מפתח" הכניסה למחשבו, לטלפון הסלולרי שלו, להתקן האחסון הנייד שלו או ליישומון שבשימוש, לחשל באמצעות צו להמצאת מסמכים לפי סעיף 43 לפקודת סדר הדין הפלילי (מעצר וחפוש) [נוסח חדש], התשכ"ט-1969 (להלן: "הפסד"פ")?<sup>13</sup> (ב) האם, במקרה שהנחקר יחויב למסור את אותו "מפתח", המידע שיימצא בחומרי המחשב שלו יוכל לשמש גם לחובתו של הנחקר, או שמא רק לחובתם של אחרים? (ג) האם, במקרה שהנחקר יחויב למסור את אותו "מפתח", ישמש הסירויב כראיה לחובתו של הנחקר? האם ניתן יהיה לנקוט נגד הנחקר הליכי ביזיון בית-המשפט (במקרה של אי ציות לצו שיפוטי מחייב)? האם ניתן יהיה לפתוח נגד הנחקר בחקירה פלילית בגין עבירה של הפרת הוראה חוקית, לפי סעיף 287(א) לחוק העונשין, התשל"ז - 1977 (להלן: "חוק העונשין")?

אין ספק ששאלות אלה מחייבות דיון מעמיק, אולם בגדרה של רשימה זו נתמקד בשאלה אחת נוספת ממשפחת השאלות הנוגעות בדבר, והיא שאלת הסמכות להשתמש בכוח סביר, במסגרת הדין הקיים, על מנת להתגבר על הגנת הסיסמה או ההצפנה בכניסה למחשב של נחקר, לטלפון הסלולרי שלו, להתקן האחסון הנייד שלו או ליישומון שבשימוש. כפי שנסקור להלן, ההכרה בסמכות השימוש בכוח מספקת פתרון חלקי בלבד לאתגר ההתגברות על מנגנוני אבטחת המידע המצוי במחשבים, בטלפונים הסלולריים (או כדומה), אך פתרון זה עשוי לסייע לעיתים קרובות לרשויות אכיפת החוק בבואן לבצע את תפקידן על-פי דין. עוד כפי שנראה בהמשך, ניתן להעלות מספר ביקורות כלפי פרקטיקה זו, ואנו נבקש להתמודד עמן ולטעון כי חרף הביקורות, ראוי וניתן במסגרת הדין הקיים להכיר בסמכות השימוש בכוח לצורך התגברות על מנגנוני אבטחת המידע.

7 Lee Ferran and Jack Date *San Bernardino DA: Clues to Unconfirmed 3rd Shooter, 'Cyber Pathogen' Could Be on iPhone*, ABC News (4.3.2016), <http://abcnews.go.com/US/san-bernardino-da-clues-unconfirmed-3rd-shooter-cyber/story?id=37399545>.  
8 התובע הכללי של ניו-יורק אף ציין בדבריו לתקשורת סביב פרשה זו, כי משטרת ניו-יורק בלבד מחזיקה ב-175 טלפונים סלולריים מסוג iPhone שאינה מסוגלת לחדור אליהם ולעיין בתוכנם. ראו: Alyssa Newcomb *New York DA Says He Can't Access 175 iPhones From Criminal Cases Due to Encryption*, ABC News (18.2.2016), <https://abcnews.go.com/Technology/york-da-access-175-iphones-criminal-cases-due/story?id=37029693>.  
9 גלי גינת "החקירה נגד רונאל פישר תקועה - בגלל הקוד של האיפון" **ynet** 7.4.2015 [news.walla.co.il/item/2844181](http://news.walla.co.il/item/2844181).  
10 John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VANDERBILT J. ENT. & TECH. L. 253, 257 (2012), וכן ראו: Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISC. 298, 302-03 (2014).  
11 Five Country Ministerial, *STATEMENT OF PRINCIPLES ON ACCESS TO EVIDENCE AND ENCRYPTION* 11 <https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf>.  
12 כך טוענים לחשל בלפור ושפירא **ונשמרתם לאצבעותיכם**, בעמ' 4.  
13 נזכיר בהקשר זה את רע"פ 8600/03 **מדינת ישראל נ' גלעד שרון**, פ"ד (1) 748 (2003), שם קבע בית-המשפט העליון כי בכל הנוגע להמצאת מסמכים לפי סעיף 43 לפס"פ, קם לחשוד החיסיון מפני הפללה עצמית, אך לא זכות השתיקה, ולכן אין הוא רשאי להתעלם מצו ההמצאה, ועליו לפנות לבית-המשפט בבקשה שיפטור אותו מהמצאת המסמכים ככל שיש בהם כדי להפילול.  
14 להרחבה בהקשר זה ראו: Paul Horowitz et al., *The Law of Prime Numbers*, 68 N.Y.U. L. REV. 185, 188-89 (1993).  
15 בכל הנוגע למחשבים, מפתח הצפנה הוא לרוב פונקציה מתמטית ארוכה, שיכולה לכלול גם מאות מספרים שונים. עם זאת, למתן נוחות השימוש, נוצר לרוב מפתח הצפנה נגיש יחסית (כמו מילת קוד או רצף מספרים אותו ניתן לזכור בקלות יחסית), אשר בעת הקשתם מומרים למפתח ההצפנה האמיתי - הפונקציה המתמטית. להרחבה בעניין זה ראו: Andrew J. Ungberg, *Protecting Privacy through Responsible Decryption Policy*, 22 HARV. J. OF L. AND TECH. 537, 540-41 (2009).  
16 Shari Trewin et al., *Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption*, IBM (2012), 6-7, 16 <https://researcher.watson.ibm.com/researcher/files/us-kapil/ACSAC12.pdf>.



### 3. השימוש בכוח סביר - באילו מצבים הוא רלוונטי?

בענייננו, מדובר בהגנת סיסמה או הצפנת המידע, שנועדה למנוע גישה אל התכנים האגורים במחשבים, בטלפונים הסלולריים, בהתקני האחסון הניידים וביישומים מקוונים. הגנה באמצעות סיסמת כניסה נועדה לנעול את "שער הכניסה" הרגיל אל המכשיר כולו, אל יישום ספציפי בתוך המכשיר, או אל קובץ ספציפי במכשיר. הצפנה, לעומת זאת, מתבצעת באמצעות ערבול התוכנה או המידע המיוצגים בביטים, על בסיס מניפולציה מתמטית מסוימת,<sup>14</sup> ובכך הופך רצף הביטים לבלתי-ניתן לפיענוח. הפיכת מידע מוצפן למידע ניתן לפיענוח נעשית באמצעות "מפתח הצפנה", הידוע למורשי הגישה אל המידע.<sup>15</sup> מפתח ההצפנה מאפשר לבצע במהופך את המניפולציה המתמטית ולהשיב את מבנה התוכנה או המידע הדיגיטלי על כנו.

הסיסמה ומפתח ההצפנה יכולים להופיע בתצורות שונות. הן הסיסמה והן מפתח ההצפנה יכולים להיות שמורים בתוך קוד תווי (רצף של מספרים או אותיות), אשר נחשב כדרך ייחודית מאוד למשתמש הקצה;<sup>16</sup> ניתן להציג סיסמה ומפתח הצפנה גם בתוך טביעת אצבע, אשר נחשבת לרוב כאמצעי זיהוי טוב וכמעט בלתי ניתן לזיוף;<sup>17</sup> זיהוי פנים משמש גם הוא לעיתים, בעיקר במכשירי טלפון "חכם" מהשנים האחרונות, כסיסמה או מפתח הצפנה, בדרך של השוואת הפנים המוצגות מול המכשיר לבין דפוס הפנים האגור במכשיר כסיסמה או מפתח הצפנה;<sup>18</sup> דרך נוספת לתצורה של סיסמה או מפתח הצפנה היא דגימת קול, שבה מילת "קוד" שאגורה במכשיר מושווית על-ידי המכשיר למילת הקוד שנאמרה על-ידי אדם המבקש לעיין בתכנים האגורים במכשיר, ורק במקרה של התאמה יתאפשר עיון בתכנים האגורים במכשיר.<sup>19</sup> הדרך החדשה ביותר לשמירת תצורה של סיסמה או מפתח הצפנה היא דפוס התנהגות עם המכשיר. לפי מיטב בדיקתנו, אין כיום מכשיר שמוטמעת בו טכניקה זו בפועל, ונכון לעת הזאת מדובר ברעיון תיאורטי. טכניקה זו מושתתת על למידה מתמדת של המכשיר את דפוסי השימוש של המשתמש ושל מאפיינים ביומטריים שונים (כמו עובי האצבע של המשתמש, עוצמת הלחיצה או זווית האחיזה של המכשיר) וכך מתאפשר עיון בתכנים האגורים במכשיר רק לאדם שמאפייניו תואמים לאלה שהוטמעו במכשיר לאורך השימוש הראשוני בו.<sup>20</sup>

ההתגברות על סיסמה או על הצפנה באמצעות "כלי פריצה" טכנולוגיים, אשר יעקפו את הסיסמה או יגלו את מפתח ההצפנה, מעסיקה רבות את גורמי החקירה והביטחון. "ניחוש" סיסמה או מפתח הצפנה בשיטה "טיפשה", כלומר בדרך של מעבר על כל הצירופים האפשריים עד לזיהוי ה"מפתח", עלול להימשך מאות שנים של הפעלת כוח המחשוב לכל סיסמה או הצפנה בודדת.<sup>21</sup>

כיוון שהאפיק של פיצוח הסיסמה או ההצפנה באמצעים טכנולוגיים אינו אפיק צליה לפחות בחלק מהמקרים, עולה שאלת השימוש בכוח על מנת להתגבר על הגנת הסיסמה או ההצפנה. רק בשתי תצורות מתוך החמש שנסקרו לעיל יכולות רשויות אכיפת החוק, ברמה המעשית, להשתמש בכוח סביר על מנת לחדור את המחשב, הטלפון הסלולרי, התקן האחסון הנייד או היישומון המוגן, זאת במקרה של טביעת אצבע זיהוי פנים. מבחינה מעשית, יכולה רשות אכיפת החוק להצמיד את אצבעו של בעל המכשיר אל המקום המתאים על-גבי המכשיר כדי לאפשר לה גישה לתכנים, והיא יכולה גם להחזיק בכוח את פניו של בעל המכשיר ולהציב מולם את המכשיר, כדי שיופעל זיהוי הפנים. עם זאת, שימוש בכוח לא יכול להוביל כשלעצמו, להקלדת קוד תווי, לאמירת מלים מסוימות שיאפשרו זיהוי קולי ולזיהוי על פי דפוס פעילות עם המכשיר.

### 4. השימוש בכוח סביר - כיצד הוא מתאפשר, מבחינה לשונית, במסגרת הדין הקיים?

דיני החיפוש הקיימים אינם מתייחסים במפורש לסיטואציה של הפעלת כוח סביר על מנת לחדור אל חומרי המחשב המוצפנים או המוגנים בסיסמה. כידוע, דיני החיפוש המתייחסים לחדירה אל חומר מחשב נוסחו באופן תוספתי, כך שנקודת המוצא לדיני החיפוש במחשב נעוצה בדיני החיפוש בחצרים.<sup>22</sup> הוראות החיפוש בחצרים מוחלות בשינויים המחויבים אל החדירה לחומר המחשב, בתוספת כמה הוראות ייחודיות לחדירה אל חומרי המחשב.<sup>23</sup>

סעיף 45 לפסד"פ המתייחס לדיני החיפוש הכלליים (ועל כן עשוי גם לחול בענייננו) קובע כדלקמן:

"אדם הגר בבית או במקום שמותר להיכנס אליו מכוח רשות לעצור או לחפש, או הממונה על בית או מקום כאמור, ירשה,

17 עם זאת, קיימות גם ביקורות, מכיוון סטטיסטי, על הסתמכותם של בתי-המשפט על טביעות אצבע. ראו: David H. Kaye, *Questioning a Courtroom Proof of the Uniqueness of Fingerprints*, 71 INTER. STATISTICAL REV. 521 (2003).  
18 להרחבה בדבר הניתוח המתמטי של השוואת פנים כאמור ראו: Andrea F. Abate et al., *2D and 3D Face Recognition: A Survey*, 28 PATTERN RECOGNITION LETTERS 1885 (2007).  
19 Julia Kollwe *HSBC rolls out voice and touch ID security for bank customers*, THE GUARDIAN (19.2.2016), <https://www.theguardian.com/business/2016/feb/19/hsbc-rolls-out-voice-touch-id-security-bank-customers>.  
20 חברה ישראלית בשם Secured Touch פועלת בימים אלה כדי להמשיך את פיתוח המוצר הראשוני הזה. ראו באתר האינטרנט של החברה - <https://securedtouch.com/about>.  
21 להרחבה בעניין זה ראו: Andrew J. Ungberg, *Protecting Privacy through Responsible Decryption Policy*, 22 HARV. J. OF L. AND TECH. 537, 541 (2009). חברות היי-טק פרטיות מציעות כלים ושירותים להתגברות על ססמאות כניסה או הצפנות של תכנים. ראו, לדוגמה, את שירותיה של חברת Cellebrite, המציעה לרשויות אכיפת החוק ברחבי העולם סיוע בהתגברות על הגנות סיסמה והצפנה, באתר האינטרנט של החברה: <https://www.cellebrite.com/en/advanced-services>.  
22 להרחבה בדבר הטכניקה התוספתית שבה נקט המחוקק בכל הנוגע לדיני איסוף הראיות בחקירה פלילית במרחב הסייבר 178-175 (2015).  
23 ראו סעיף 23 לפסד"פ.

24 בלפור ושפירא *ונשמרתם לאצבעותיכם*, בעמ' 7.

25 עמ"מ 3782/12 *מפקד מחוז תל אביב-יפו במשטרת ישראל נ' איגוד האינטרנט הישראלי*, פסקה 35 לפסק-דינו של השופט סולברג (פורסם בנוב, 24.3.2013).  
(להלן עניין *מפקד מחוז תל אביב-יפו* או *פרשת איגוד האינטרנט*). לביקורת על המטאפורה של "אתר אינטרנט" כ"מקום" ראו אברהם נ. טננבוים "על המטאפורות

לפי הדרישה, כניסה חפשית ויתן כל הקלה סבירה; נדרש וסירב להרשות כניסה כאמור, מי שזכאי להיכנס ראשי לבצע את הכניסה בכוח.

נראה אם כן, כי סעיף 45 מורכב משני חלקים - הרישא מטילה חובה פוזיטיבית על האזרח לתת כל הקלה סבירה לאיש רשות אכיפת החוק אשר מבקש להיכנס אל המקום עליו ממונה הפרט; הסיפא מעניקה סמכות לאיש רשות אכיפת החוק להשתמש בכוח כדי להיכנס לאותו מקום. האם ניתן - מבחינת לשונו של הסעיף - להחיל אותו גם על ענייננו?

לשם כך, נדרש לבחון האם החדירה אל המחשב, הטלפון הנייד, התקן האחסון או היישומון יכולים להתפרש כ"מקום" ש"נכנסים" אליו. בלפור ושפירא סבורים כי מחשב או טלפון נייד לא יכולים להיות מוגדרים כ"מקום".<sup>24</sup> לגישתם, מחשב איננו מקום שבו ניתן "לגור" ולכן לא ניתן להחיל את סעיף 45 על מחשב או טלפון סלולרי. בניגוד לגישתם זו, אנו סבורים כי ניתן בהחלט לטעון כי אדם יכול להיות "ממונה" על "מקום" שהוא מחשב או טלפון סלולרי. עוד טוענים בלפור ושפירא כי פרשנות "חומר מחשב" כ"מקום" תוביל לסתירה, משום שמסעיפי ההגדרות בפסד"פ ובחוק המחשבים, התשנ"ה-1995 עולה כי "חומר מחשב" הוא "חפץ". לשיטתנו, אין לראות בהגדרת חומר המחשב כ"חפץ" משום הגדרה המוציאה מתחולה כל אפשרות לראות את המחשב גם כ"מקום" לעניין סמכות השימוש בכוח. זאת, בפרט כאשר ה"חפץ" מיוצג במקום פיזי-מוחשי. יתרה מכך, כפי שציינו לעיל, דיני החדירה לחומר מחשב נובעים מדיני החיפוש. דיני החיפוש מוחלים על דיני החדירה לחומר המחשב, בשינויים המחויבים. סעיף 23 לפסד"פ קובע כי שופט ראשי להורות בצו על חיפוש "בכל בית או מקום", ואילו סעיף 23א לפסד"פ קובע כי "חדירה לחומר מחשב וכן הפקת פלט תוך חדירה כאמור, יראו אותן כחיפוש...". מכאן נובע כי המחוקק ביקש להחיל את הוראות החיפוש הכלליות המוחלות על המרחב הפיזי, ובכללן הוראות של סעיף 45 לפסד"פ, גם על דיני חדירה לחומר מחשב, בשינויים המחויבים. השינוי המחויב הוא כי במקום "אדם הגר בבית או מקום" ייקרא "אדם המחזיק או המשתמש

בחומר המחשב", ובמקום "כניסה" ייקרא "חדירה". לכאורה, כשמדובר בהענקת סמכויות לרשויות אכיפת החוק, ראוי לפרשן בצמצום, כך שהסמכה שלא נאמרה במפורש בלשון החוק לא תחול על הרשות, אולם בענייננו שונה הדבר, בשל ההוראה הברורה שדיני החיפוש יחולו, בשינויים המחויבים, על דיני החדירה אל חומר המחשב.

מן הראוי לציין כי אף במקרה שבו המחוקק לא קבע הוראת החלה מהמרחב הפיזי למרחב המקוון, כבענייננו, בית-המשפט העליון הכיר בחומר מחשב כמיוצג ב"מקום". בעניין **מפקד מחוז תל אביב-יפו במשטרת ישראל** דן בית-המשפט העליון בשאלה האם סעיף 229 בחוק העונשין (בנוסחו דאז) - אשר הקנה לשוטרי משטרת-ישראל את הסמכות לסגור בצו "מקום" המשמש לעריכת משחקים אסורים, הגרלות או הימורים - מקנה למשטרת-ישראל את הסמכות להורות לספקיות הגישה לאינטרנט להגביל את הגישה של משתמשיהן אל אתרי אינטרנט המשמשים לעריכת הימורים באינטרנט. באותו עניין קבע בית-המשפט העליון כי "לא תהא זו סטיה מ'עקרון החוקיות', ולא מכללי הפרשנות, אם נקבע כי 'מקום' מכיל בקרבו גם את המרחב הוירטואלי, ואוצר במשמעו גם אתר אינטרנט".<sup>25</sup> למחן הדיוק, נציין כי קביעה זו היא מבחינת אוביטר בפסק-הדין, שכן היא לא הייתה מחויבת המציאות לצורך ההכרעה כפי שנתקבלה. באותו עניין העיר עוד השופט סולברג כי לטעמו גם הביטוי "חצרים" כולל "חצרים וירטואליים", אך הותיר את ההכרעה בשאלה זו בצריך עיון.<sup>26</sup>

בעניין **מפקד מחוז תל אביב-יפו במשטרת ישראל** אימץ בית-המשפט העליון את עמדת איגוד האינטרנט הישראלי לפיה אתר אינטרנט הוא "אוסף של מידע ויישומים, המותקנים על גבי מחשב, המתקשר עם מחשבים רבים ברשת האינטרנט". לדעתנו, אם בכל הנוגע להגדרה אמורפית-יחסית זו של "אתר אינטרנט" הכיר בית-המשפט העליון כי ניתן לראות בו משום "מקום", הרי שמקל וחומר שניתן לראות במחשב, בטלפון סלולרי, בהתקן אחסון נייד ואף ביישומון המותקן על גבי מחשב או טלפון סלולרי - משום "מקום". הלא כל אחד מאלה מיוצג במכשיר פיזי, חפצי, שתפוס בידי הרשות החוקרת.<sup>27</sup>

בדיני המחשבים והאינטרנט "שערי משפט ד" (2) 359, 369-375 (התשס"ו).

26 ראו לעיל, עניין **מפקד מחוז תל אביב-יפו**, בפסקה 20 לפסק-דינו של השופט סולברג. להשלמת התמונה, יצוין כי באותו מקרה קבע בית-המשפט העליון ברוב דעות, כי חרף העובדה שאתר אינטרנט הוא "מקום", הרי שמשטרת-ישראל אינה רשאית להסתמך על סעיף 229 לחוק העונשין כדי להורות לספקיות הגישה לאינטרנט להגביל את הגישה של משתמשיהן לאתרי אינטרנט המשמשים להימורים. זאת כיוון שמתן הוראה לחסימת הגישה בידי צד ג' תם-לב (ספקיות הגישה לאינטרנט) אינה יכולה להילמד מסמכות ה"סגירה" של המקום בידי המשטרה, שהיא בלבד מנויה בסעיף 229 לחוק העונשין.

27 ראו גם את עניין **אבו סלים**, בו קבע בית-המשפט השלום בצורת קביעה דומה, ולפיה תחת ההגדרה של "מקום ציבורי" נכנס גם "אתר אינטרנט". באותו עניין דן בית-המשפט השלום בעניינו של אימאם אשר הואשם בעבירה של תמיכה בארגון טרור (כנוסחה דאז), זאת בשל תכנים שפרסם באינטרנט. בית-המשפט קבע כי הגדרת ה"פרסום" של דברי התמיכה בארגון הטרור מחייבת כי הדברים יופצו ב"מקום ציבורי", וכי אתרי האינטרנט שבהם הופצו הדברים נחשבים כ"מקום ציבורי" לעניין עבירה זו. ראו ת"פ (שלום נצ') 10-11-12629-11 **מדינת ישראל נ' אבו סלים** (פורסם בנבו, 1.4.2012).

חזוק נוסף למגמה של הכרה באתר אינטרנט כ"מקום" באה לידי ביטוי גם לאחרונה, בהחלטתו של יושב-ראש ועדת הבחירות המרכזית לכנסת ה-21, המשנה לנשיאת בית-המשפט העליון, השופט חנן מלצר. השופט מלצר קבע כי מודעות פוליטיות ברשתות החברתיות באינטרנט תשאנה את זיהוי הגוף המפלגתי המפרסם אותן. ראו תב"כ 8/21 **בן מאיר נ' מפלגת הליכוד ואח'** (פורסם בנבו, 27.2.2019). באותו עניין נדרש יו"ר ועדת הבחירות המרכזית לפרשנות סעיף 10(ב)(5) לחוק הבחירות (דרכי תעמולה), התש"ט-1959, אשר קובע כי גוף מפלגתי חייב לציין על גבי "מודעות מודפסות המתפרסמות בעיתונים יומיים, בשבועונים או בירחונים" כי הן מודפסות מטעמו. לטענת העותרים באותו עניין, יש להחיל הוראה זו גם על מודעות המתפרסמות באינטרנט. יו"ר ועדת הבחירות קבע בהחלטתו, כי יש להחיל את החובה האמורה גם על מודעות באינטרנט, תוך שפסק כי "בדמיון-מה לפרשנות שניתנה בפרשת **איגוד האינטרנט**, סבורני כי גם השאלה הטעונה הכרעה בעתירה שלפניי, תיפתר על דרך של פרשנות תכליתית, המרחיבה את המונח: 'מודעה' אף לגבי פרסומים ברשת האינטרנט". ראו שם, בפסקה 66 להחלטה.

28 ראו סעיף 11(ג) לחוק החיפוש בגוף.



אכיפת החוק בבואן להיכנס, קרי "לחדור" אל ה"מקום" ומכאן גם שבסמכותן של רשויות אכיפת החוק להשתמש בכוח סביר כדי לאפשר את החדירה אל המקום.

מהפרשנות הלשונית - אל הבחינה הנורמטיבית. לדעתנו, התכלית שנועד להגשים סעיף 45 לפסד"פ היא לאפשר כניסה אל מקום. אומנם המצב הנפוץ יותר שאליו מתייחס הסעיף הוא מצב שבו המשטרה מפעילה כוח כלפי חפץ, ולא כלפי אדם, על מנת להיכנס אל המקום (למשל תשבור חלון, מנעול או כדומה), אולם בהחלט ייתכן שיופעל גם כוח כלפי המשתמש הקבוע ב"מקום" החיפוש. כך, למשל, ייתכן שאם אדם, לרבות החשוד, חוסם את הכניסה לביתו, הרי שניתן יהיה, מכוח סעיף 45 לפסד"פ, להזיזו בכוח סביר, למנוע את החסימה ולאפשר בכך את ביצוע החיפוש. ריבוי המצבים שבהם נחסמת ה"כניסה" אל חומרי מחשב הנחוצים לחקירה, שהותר העיון בהם במסגרת צו חדירה לחומר מחשב, מקים צורך להכיר בסמכות השימוש בכוח סביר למטרת "כניסה" זו. אומנם ניתן לטעון כי חומרי המחשב שבשימוש של אדם נוגעים לזכותו הפרטית ולהגנת המידע האישי שלו באופן מוגבר לעומת כניסה לביתו של אדם ועיון בחפציו הפיזיים, אולם איננו רואים טעם לקבוע כי בשל כך תישלל עצם הסמכות להשתמש בכוח. ההבחנה בין עוצמת הפגיעה בפרטיות בעת כניסה לחומר מחשב לעומת עוצמת הפגיעה בפרטיות בעת כניסה לחצרים רלוונטית, אם כבר, לשלב מתן ההיתר השיפוטי לבצע את החדירה. בשלב זה, עשוי בית-המשפט לקבוע, כי באיזון הקונקרטי בין צרכי החקירה לבין הפגיעה האפשרית בפרטיות כתוצאה מהחדירה - הוא אינו מאשר את הבקשה לצו החדירה או שהוא מאשר בתנאים ובסייגים שימנעו פגיעה עודפת בפרטיות הנחפש ובפרטיותם של צדדים שלישיים.<sup>31</sup> אולם, בין זה לבין השימוש בסמכות הנלווית לצורך הוצאתה אל הפועל של החדירה - אין קשר רציונלי.

נציג להלן שלושה טיעונים אפשריים כנגד ההכרה בסמכות השימוש בכוח סביר על מנת להתגבר על הגנת סיסמה או הצפנה, המגולמת באמצעות טביעת אצבע או זיהוי פנים. כפי שנראה, חרף טענות אלה, המופיעות בעיקרן גם במאמרם של בלפור ושפירא,<sup>32</sup> עמדתנו היא כי ההכרה בסמכות הנדונה מוצדקת וראויה.

### 5.1. החיסיון מפני הפללה עצמית

לפי הטיעון הראשון, אין מקום להשתמש בסעיף 45 לפסד"פ כדי

בצד האמור נציין אפיק פרשני נוסף על-בסיסו ניתן היה לטעון כי לרשויות אכיפת החוק הסמכות להפעיל כוח סביר כדי לעיין בחומרי מחשב, זאת האפיק של חוק סדר הדין הפלילי (סמכויות אכיפה - חיפוש בגוף ונטילת אמצעי זיהוי), התשנ"ו-1996 (להלן: "**חוק החיפוש בגוף**"). סעיף 3(ב) לחוק החיפוש בגוף קובע כי רשאי שוטר לערוך חלק מהחיפוש החיצוניים בגופו של חשוד תוך שימוש בכוח סביר, כאשר החשוד לא נתן את הסכמתו. המונח "חיפוש חיצוני" מוגדר בחוק החיפוש בגוף, בין היתר, כ"נטילת טביעה של כל חלק מהגוף". מכאן נובע כי שוטר רשאי לערוך חיפוש חיצוני שכולל גם לקיחת טביעת אצבע מידו של חשוד. עוד נקבע בחוק החיפוש בגוף כי שוטר רשאי להשתמש בכוח כדי ליטול טביעת אצבע מאדם כאשר הדבר משמש לצורך זיהויו של האדם.<sup>28</sup> לפי מהלך פרשני זה, רשאי השוטר ליטול טביעת אצבע בכוח כדי לזהות את האדם או כאשר הדבר מהווה חיפוש חיצוני, ומכאן ששוטר יכול גם לעשות כן לשם התגברות על הגנת סיסמה או הצפנה, כדי לערוך חיפוש במחשב או טלפון סלולרי. במקרה אחד הידוע לנו ננקטה דרך פרשנות זו על-ידי בית-המשפט המחוזי בתל-אביב.<sup>29</sup> בכל הנוגע לאמצעי אבטחה של זיהוי פנים, הרי שבהתאם לאותו היגיון, ניתן לפרש את אופן החיפוש החיצוני של "בחינה חזותית של גופו העירום של אדם, לרבות צילומו" ככזה אשר מאפשר כביכול, מקל וחומר, לבחון גם את פניו של האדם, ולבוחנם באמצעות הטלפון הנייד שלו - במטרה לתגבר על אמצעי האבטחה.

כשלעצמנו, אנו סבורים כי אפיק פרשני המבוסס על חוק החיפוש בגוף מעורר קשיים רבים ואין לקבלו. בקצרה נציין, כי אפיק זה מחייב "דילוג" פרשני בעייתית בין החיפוש החיצוני בגוף עצמו, שהסמכות לו מוקנית במפורש, לבין שימוש באותו חלק בגוף לצורך עריכת חיפוש בתפוס אחר - המחשב, הטלפון הסלולרי של הנחפש או כדומה. בכך אנו מסכימים עם הטיעון של בלפור ושפירא בהקשר זה.<sup>30</sup> לפיכך, נמקד את המשך דיוננו בניתוח הסמכות מכוח סעיף 45 לפסד"פ.

### 5. השימוש בכוח סביר לשם התגברות על סיסמה או הצפנה - האומנם הוא ראוי?

עד כאן הראנו כי מבחינה לשונית ניתן לבסס את הקביעה לפיה מחשב או טלפון סלולרי הם "מקום", ומכאן שניתן לטעון כי סעיף 45 לפסד"פ חל בענייננו. משמע, ניתן לראות במחזיק או במשתמש בחומר המחשב כמי שממונה על ה"מקום", ומכאן שעליו לתת כל הקלה סבירה לרשויות

29 ראו ע"ח (מחוזי ת"א) 19-01-45208 תחנת מרחב יפתח נ' רפאלי (לא פורסם, 18.1.2019). בית-המשפט המחוזי קבע באותו עניין כי פעולה של פתיחת הטלפון הסלולרי של החשוד באמצעות שימוש בכוח סביר ללקיחת טביעת אצבעו, נכנסת תחת ההגדרה של "חיפוש חיצוני" לפי חוק החיפוש בגוף, ולכן מלכתחילה לא נדרשה הרשות החוקרת להרשאה שיפוטית כדי לעשות כן.

30 בלפור ושפירא ונשמרתם לאצבעותיכם, בעמ' 6-7.

31 יצוין כי סעיף 23א(ב) לפסד"פ קובע כי לשם עריכת חיפוש בחומרי מחשב, על הרשות החוקרת להצטייד בצו חדירה כדין. עוד קובע סעיף זה, כי על בית-המשפט לקבוע בצו "את מטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש".

32 בלפור ושפירא ונשמרתם לאצבעותיכם.

33 במקרה אחד המוכר לנו קבע בית-המשפט המחוזי בירושלים, במסגרת שלב "מעצר ימים" של חשוד, כי - "לא ניתן - מבחינה משפטית - לכוף על אדם למסור את סיסמת המכשיר האלקטרוני שברשותו לגורמי החקירה, בין אם מדובר בשב"כ ובין אם מדובר במשטרה. המכשיר נמצא בידי המשטרה/השב"כ, והם רשאים לפנות למומחים מכל סוג ומין שהוא, כדי לנסות ולפרוץ למכשיר". ראו עמ"י (מחוזי-י-ם) 18-10-65308 דרויש נ' מדינת ישראל (פורסם בנבו, 26.10.2018). כאמור, עניינו של מאמר זה אינו בשאלת הסמכות לדרוש מהנחקר למסור את סיסמת הכניסה לחומר המחשב שבהחזקתו או בשימוש, אולם נציין - מבלי להרחיב בעניין זה - כי ניתן להעמיד טיעוני נגד לפיהם ניתן להכיר בסמכות הדרישה מחשוד אף למסור את סיסמת הכניסה בעצמו, בבחינת מסירת המפתח לתכנים ולא מסירת התכנים המפלילים עצמם (בהנחה מובן שתכנים אלה נתפסו כדין בידי הרשות החוקרת).

להתגבר על הגנת הסיסמה או ההצפנה, שכן הדבר מגלם פגיעה בחיסיון מפני הפללה עצמית, העומד לזכותו של המחזיק או המשתמש בחומר המחשב הדרוש לחקירה. סעיף 47(א) לפקודת הראיות [נוסח חדש], התשל"א-1971 (להלן: "פקודת הראיות") קובע כי - "אין אדם חייב למסור ראייה אם יש בה הודיה בעובדה שהיא יסוד מיסודותיה של עבירה שהוא מואשם בה או עשוי להיות מואשם בה". סעיף 2(2) לפקודת הפרוצדורה הפלילית (עדות) קובע בנוסף - "אדם, הנחקר כך, יהיה חייב להשיב נכונה על כל השאלות, ששיגי לו בשעת החקירה אותו קצין משטרה, או קצין מורשה אחר כנ"ל, חוץ משאלות שהתשובות עליהן יהיה בהן כדי להעמידו בסכנת אשמה פלילית". כבר בראשית הדברים יוער, כי שאלת החיסיון מפני הפללה עצמית עשויה להתעורר ביתר שאת בכל הנוגע לרישא של סעיף 45 לפסד"פ, היינו להטלת החובה לשותף פעולה עם רשויות החקירה.<sup>33</sup> כאמור לעיל, בגדרי מאמר זה נבקש להתמקד רק בפרקטיקה של השימוש בכוח סביר, ולכן נמקד את טענתנו לגבי הסיפא של סעיף 45 לפסד"פ, אשר מעניקה סמכות לעשות שימוש בכוח סביר.

ניתן למנות שלוש הצדקות עיקריות לקיומו של החיסיון מפני הפללה עצמית. לפי ההצדקה הראשונה, החיסיון מפני הפללה עצמית נועד ליצור תמריץ בקרב רשויות החקירה לפעול להשגת ראיות שהן חיצוניות לחשוד עצמו. בשל החשש מהודאות שווא, וכתוצאה מהן - הרשעות שווא,<sup>34</sup> מבקשת מערכת המשפט ליצור תמריץ בקרב רשויות החקירה לחפש ראיות שהן חיצוניות לחשוד עצמו, ולא להיתלות בהודאתו בלבד.

לפי ההצדקה השנייה, החיסיון מפני הפללה עצמית נובע מזכותו של הנחקר לפרטיות. פרשנות מקובלת לזכות לפרטיות גורסת כי זכות זו מגדירה את יכולתו של אדם לשלוט ב"זרימת המידע" (flow of information) על אודותיו.<sup>35</sup> מסיבה זו ראוי, כך לפי הצדקה זו, לשלול מגורם זר את האפשרות לגשת בצורה חופשית לכל פרט מידע על אודות אדם אחר. החיסיון מפני הפללה עצמית יוצר חסם מפני גישה של גורם זר אל המידע האישי של האדם, במקרה זה החשוד.<sup>36</sup> בעולם ללא החיסיון מפני הפללה עצמית, ניתן יהיה לכפות על האדם למסור מידע על עצמו ובכך תאבד לו שליטתו במידע.<sup>37</sup>

לפי ההצדקה השלישית, החיסיון מפני הפללה עצמית מבקש להגן על החשוד מפני הטריילמה המוסרית, שעצם העמדת החשוד בפניה היא

לא-מוסרית. לפי הצדקה זו, בעולם ללא החיסיון מפני הפללה עצמית, יעמוד החשוד-האשם (קרי החשוד שביצע את העבירה המיוחסת לו) בעת חקירתו במשטרה בפני שלוש אפשרויות: לשקר לחוקריו; לומר אמת לחוקריו ובכך להביא על עצמו ענישה; לשתוק ובכך להוביל את חוקריו למסקנה לפיה הוא זה שאשם בביצוע העבירה.<sup>38</sup> הצדקה זו מניחה כי נחקרים-אשמים רבים יעדיפו לשקר, ובכך יטעו בצורה פוזיטיבית את המשטרה. על כן, עדיף לאפשר להם לשתוק מאשר להעמידם בפני הטריילמה שתתמרץ אותם להטעות את המשטרה.<sup>39</sup> לפי הצדקה זו, הזכות לאי הפללה עצמית (ואף זכות השתיקה לחשודים) מונעת כניסה לטריילמה מוסרית זו, שכן היא מאפשרת לשתוק בלא שיהיו לכך השלכות שליליות ניכרות על החשוד.<sup>40</sup>

במענה לטיעון זה, נציין כי השימוש בכוח על מנת ליטול טביעת אצבע או על מנת להחזיק את פניו של הנחקר כך שיזוהו פניו במחשב או בטלפון הסלולרי - אומנם מוביל לכניסה לחומרי המחשב, אולם אין מדובר בהפללה "עצמית" או באמרה או אף במעשה של החשוד עצמו.<sup>41</sup> השימוש בכוח בידי איש הרשות החוקרת מפקיע את יסוד הפעולה ה"עצמית", ועל כן אין בענייננו התנגשות, אף לא התחככות של ממש, עם החיסיון מפני הפללה עצמית. יצוין בהקשר זה, כי גם בלפור ושפירא מיקדו את טיעוניהם בנוגע לחיסיון מפני הפללה עצמית בשאלת שיתוף הפעולה של הנחקר עם הרשות החוקרת, למשל שיתוף הפעולה של הנחקר בהתבוננות אל הטלפון הנייד התפוס.<sup>42</sup> שאלה זו נוגעת לרישא של סעיף 45 לפסד"פ, ולא לסיפא של סעיף זה, העוסקת בסמכות הפעלת הכוח הסביר על-ידי הרשות החוקרת חרף אי שיתוף הפעולה מצד הנחקר.

## 5.2. אפליה אסורה בין חשודים

לפי הטיעון השני, השימוש בכוח כדי להתגבר על הגנת סיסמה או על הצפנה המותקנים במחשב, בטלפון סלולרי, בהתקן אחסון נייד או ביישומון של החשוד עלול להביא לאפליה אסורה בין חשודים. זאת מכיוון שהכרה בסמכותן של רשויות אכיפת החוק להשתמש בכוח כאמור תביא לכך שחשודים שהשתמשו, למשל, בקוד תווי כאמצעי אבטחה יהיו חסינים מפני החדירה אל מכשיריהם (שכן השימוש בכוח לא יוכל להביא, בפועל, להקלת הקוד התווי), בעוד שחשודים שהשתמשו, למשל, בטביעת אצבע כאמצעי אבטחה לא יהיו חסינים כאמור. יתרה

34 ראו למשל דליה דורנר "מלכת הראיות נ' טארק נוג'ידאת - על הסכנה שבהודאת שווא ועל הדרך להתמודד עמה", הפרקליט מט 7 (2006); חנית לרנאו "הודאות שווא והרשעות שווא" עלי משפט יא 351 (התשע"ד); בועז סגל "ההודאה כבסיס להרשעה - האמנת 'מלכת הראיות' או שמא קיסרית הרשעות השווא" עלי משפט ד 245 (התשס"ה).

35 מיכאל בירנהק [מרחב פרטי] הזכות לפרטיות בין משפט לטכנולוגיה 89-108 (התשע"א).

36 לטיעון ברוח הצדקה זו ראו: D. J. Galligan, *The Right to Silence Reconsidered*, 41(1) CURRENT LEGAL PROBS 69, 88-89 (1988).

37 Robert S. Gerstein, *Privacy and Self-Incrimination*, 80(2) ETHICS, 87, 89 (1970).

38 Ian Dennis, *Instrumental Protection, Human Rights or Functional Necessity? Reassessing the Privilege against Self-Incrimination*, 54(2) 38 (1995) CAMBRIDGE L. J. 342, 358-59.

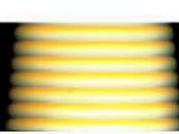
39 שם.

40 דניאל זידמן ואלכס שטיין טענו כי ההגנה שניתנת לחשודים-אשמים מפני הטריילמה המוסרית מביאה להחצנת חוביות על חשודים-חפים מפשע. לפי טיעון זה, במקרים שבהם ראיות התביעה הן בעוצמה בינונית (לעומת עוצמה חלשה או עוצמה חזקה), יבחר החשוד-האשם לשמור על זכות השתיקה, בעוד שהחשודים-החפים מפשע יבחרו למסור את גרסתם לחוקריהם. ראו: Daniel J. Seidmann & Alex Stein, *The Right to Silence Helps the Innocent: A Game-Theoretic Analysis of the Fifth Amendment Privilege*, 114 HARV. L. REV., 431, 467-70 (2000).

41 לטיעון דומה ראו עמנואל גרוס "החיסיון מפני הפללה עצמית - האמנם ציון דרך במאבקו של האדם הנאור לקידמה?" מחקרי משפט ז 167, 183 (התשמ"ט).

42 בלפור ושפירא ונשמרתם לאצבעותיכם, בעמ' 9.

43 בג"ץ 6396/96 זקין נ' ראש עיריית באר-שבע, פ"ד נג(3) 289, 305 (1999).



מזאת, לפי טיעון זה, סמכות השימוש בכוח עלולה להוביל מלכתחילה לאכיפה מוגברת כלפי חשודים שהשתמשו באמצעי אבטחה, שניתן להשתמש בכוח כדי להתגבר עליהם (טביעת אצבע זיהוי פנים), ומנגד להפחתת האכיפה מול חשודים שהשתמשו באמצעי אבטחה אחרים, שלא ניתן להשתמש בכוח כדי להתגבר עליהם (קוד תווי, זיהוי קולי או דפוס התנהגות עם המכשיר), באופן שיפלה בין חשודים.

טיעון זה יונק את חיותו מהדוקטרינה של אכיפה בדרנית. כידוע, דוקטרינת האכיפה הדרנית מתייחסת לאכיפה הפוגעת בשוויון במובן זה שהיא מבדילה לצורך אכיפה בין בני אדם דומים או בין מצבים דומים לשם השגת מטרה פסולה, או על יסוד שיקול זר או על יסוד שרירותיות גרידא.<sup>43</sup> על פי ההלכה הפסוקה, ההכרעה בשאלה אם המדובר, במקרה נתון, באכיפה חלקית מותרת או באכיפה בדרנית פסולה, עשויה בדרך-כלל להיגדר מבחינה של מניעה של התביעה.<sup>44</sup> עם זאת, נפסק כי במקרים נדירים תיתכן קבלתה של טענת אכיפה בדרנית גם כאשר נוצרו תוצאות מפלות בפועל, ללא מניע זדוני או שקילת שיקולים פסולים על-ידי הרשויות.<sup>45</sup>

בענייננו, התוצאה המבחינה בפועל בין אמצעי האבטחה השונים למחשבים, טלפונים סלולריים, התקני אחסון ניידים או יישומונים אינה מעוררת כל קושי בדמות מניע פסול לאכיפה. ראשית, השימוש בכוח יכול להוביל להתגברות ישירה על חלק מאמצעי האבטחה בעוד שלגבי חלק אחר מאמצעי האבטחה - הוא אינו יכול להוביל להתגברות שכזו באופן ישיר. כך, כאשר מדובר באמצעי אבטחה של כניסה באמצעות זיהוי טביעת אצבע, הרי שהשימוש בכוח, על דרך של נטילת אצבעו של החשוד והשמתה על גבי המכשיר, יכולה להוביל במישור לכניסה אל המכשיר. לעומת זאת, כאשר מדובר בהקלדת קוד תווי, השימוש בכוח לא יכול להוביל ל"ניחוש" הקוד, ועל כן, אם יוביל להקשת הקוד התווי, יהיה זה באופן עקיף בלבד, כך שהשימוש בכוח יוביל את החשוד להקליד בעצמו את הקוד התווי. בכך יש משום פגיעה ישירה בחיסיון מפני הפללה עצמית. נוסף על כך, השימוש בכוח אינו ממוקד לפעולה הנדרשת אלא להוצאת המידע מהחשוד. מכאן נובע, שההבחנה בין אמצעי האבטחה השונים משליכה מהותית על אפשרות השימוש בכוח ועל ההצדקה המשפטית להשתמש בכוח. על כן, העובדה שהשימוש בכוח רלוונטי רק לחלק מאמצעי האבטחה אינה עובדה שרירותית, אלא הבחנה מהותית ומוצדקת. שנית, לא ניתן להבחין כיום בפלחי אוכלוסייה מסוימים המשתמשים באמצעי אבטחה מסוג מסוים, שניתן להתגבר עליו באמצעות שימוש בכוח, בעוד שפלחי אוכלוסייה אחרים מתאפיינים דווקא בשימוש באמצעי אבטחה מסוג אחר, שלא ניתן

להתגבר עליו באמצעות שימוש בכוח. משכך, לא ניתן להצביע על תוצאה חפלה בין קבוצות שונות באוכלוסייה בשים לב לאמצעי האבטחה שבהם הן נוהגות להשתמש בנוגע למחשבים, הטלפונים הסלולריים, התקני האחסון הנייד או היישומונים שבהם הן משתמשות. **שלישית**, לטעמנו אין חשש של ממש לפיו רשויות אכיפת החוק תפעלנה מלכתחילה לחקור עבירות רק במקרים שבהם החשוד משתמש באמצעי אבטחה של טביעת אצבע או זיהוי פנים. לרשויות החקירה לא בהכרח יהיה את המידע איזה אמצעי אבטחה נוקט בו החשוד, ואף אם היה לה מידע זה, ברי כי חובותיהן ותפקידן הציבורי היה מביא אותן לחקור עבירות גם במקרים אלה.

### 5.3. פגיעה בזכות לשלמות הגוף

לפי הטיעון השלישי, השימוש בכוח כדי להתגבר על אמצעי אבטחה כמו טביעת אצבע וזיהוי פנים עלול להסב פגיעה בזכותו של החשוד לשלמות הגוף. עוד על פי טיעון זה, פגיעה בזכות זו מצריכה הסמכה מפורשת בחקיקה, ואין מקום להכיר בסמכות לפגיעה כאמור על דרך של פרשנות לסעיף 45 לפסד"פ. עוד בהקשר זה ניתן לטעון כי סעיף 45 לפסד"פ מקנה סמכות להפעיל כוח רק כלפי חפץ, ולא כלפי אדם.

במענה לטיעון זה, נשיב כי לגישתנו, סעיף 45 לפסד"פ נוקט בלשון הסמכה העונה על דרישת ההסמכה המפורשת. זאת, בוודאי אם ניקח בחשבון את קביעתו של בית-המשפט העליון בעניין **המפקד הלאומי**, שם קבעה השופטת (כתוארה דאז) ביניש כי "ככל שהטעמים שבבסיס הזכות המוגנת הינם בעלי חשיבות חברתית נמוכה יחסית, וככל עוצמת הפגיעה בזכות חלשה בהתחשב בהקשר ובמכלול נסיבות העניין, כך ניתן לפרש את דרישת 'ההסמכה המפורשת' באופן גמיש ומרוכך יותר".<sup>46</sup> בהקשר זה ניתן לומר כי אומנם ברור לכל שפגיעה בזכות לשלמות הגוף היא פגיעה בזכות חשובה ומרכזית, אולם עוצמת הפגיעה בזכות בהקשרו הנדון היא חלשה יחסית, שכן מדובר בהחזקת ראשו או אצבעו של הנחפש, ולא בפגיעה בליבת הזכות לשלמות הגוף.<sup>47</sup> מכאן שגם אם ברי כי המחוקק בסעיף 45 לפסד"פ לא התכוון במפורש, מטבע הדברים, לשימוש בכוח לצורך כניסה למחשבים, טלפונים סלולריים, התקני אחסון ניידים או יישומונים, אשר כולם כאחד לא היו בשימוש בשנת 1969, עת נוסח מחדש, הרי שניתן לראות בסעיף 45 משום הסמכה ברורה במידה מספקת לפגיעה בזכות לשלמות הגוף, במקרה של שימוש בכוח לצורך התגברות על הצפנה או סיסמה המוגנים בזיהוי פנים או בטביעת אצבע.

44 ע"פ 4855/02 **מדינת ישראל נ' בורוביץ**, פ"ד נט(6) 776, פסקאות 26-27 לפסק הדין (2005).

45 רע"פ 1611/16 **מדינת ישראל נ' ורדי**, פסקאות 65-80 לפסק-דינו של השופט מצ'ר (פורסם בנבו, 31.10.2018). כן ראו ע"פ 6328/12 **מדינת ישראל נ' פרץ**, פסקה 29 לפסק-דינו של השופט פוגלמן (פורסם בנבו, 10.9.2013). לביקורת ראו מיכל טמיר **אכיפה סלקטיבית** 168-153 (2008). טמיר גורסת כי בית-המשפט העליון צמצם את דוקטרינת האכיפה הדרנית יתר על המידה, בכך ששם את הדגש על מניעי התביעה ולא על מבחן התוצאה של אפליה בין חשודים.

46 בג"ץ 10203/03 **"המפקד הלאומי" נ' היועץ המשפטי לממשלה**, פ"ד סב(4) 715, פסקה 12 לפסק-דינה של השופטת ביניש (פורסם בנבו, 20.8.2008).

47 כדוגמה הפוכה לפגיעה בליבת הזכות לשלמות הגוף, ראו למשל את בג"ץ 5100/94 **הוועד הציבורי נגד עינויים בישראל נ' ממשלת ישראל**, פ"ד נג(4) 817 (1999), שם קבע בית-המשפט העליון כי נדרשת הסמכה מפורשת לשם הפעלתם של אמצעים פיזיים נגד נחקרים בחשד לביצוע של עבירות ביטחון לצורך קבלת אמרתם.

48 ראו ת"א (שלום י-ם) 32099-04-10 **בול נ' מדינת ישראל** (פורסם בנבו, 24.6.2012). באותו מקרה פסק בית-המשפט השלום בירושלים כי סעיף 45 לפסד"פ חל גם במקרה שבו דחפו שוטרים את בעלת הבית אשר חסמה בגופה את הכניסה לבית שבו היו רשאים השוטרים לערוך חיפוש.

49 סעיף 45 לפסד"פ קובע כי אם נדרש הנחפש וסירב להרשות כניסה ל"מקום", אזי "מי שזכאי להיכנס רשאי לבצע את הכניסה בכוח". בניגוד לחקיקה מודרנית יותר, לא מדובר בשימוש ב"כוח סביר", אלא ב"כוח" בלבד. השו, מנגד, עם סעיפים 10(א), 72(ב) ו-75(ג) לחוק סדר הדין הפלילי (סמכויות אכיפה - מעצרים), התשנ"ו-1996, ועם סעיפים 3(ב), 11(ג), 11(ג) ו-11(ד) לחוק החיפוש בגוף. אולם, אין ספק בעינינו כי ראוי לקרוא את דרישת הסבירות בהחלטה בדבר הפעלת הכוח והמידתיות בעוצמה ובאופן הפעלתה לתוך סעיף זה.

יובהר עוד כי מלשונן הרחבה של סעיף 45 לפסד"פ עולה כי במקרה של סירוב לאפשר "כניסה למקום", ראשי השוטר להפעיל כוח כלפי אדם והן כלפי רכוש.<sup>48</sup> בענייננו, מדובר בשימוש בכוח כלפי אדם, לצורך כניסה ל"מקום" שבו מצוי חומר מחשב הדרוש לחקירה, ומכאן שהסיטואציה דן חוסה בצלו של סעיף 45 לפסד"פ. עם זאת, ראוי להדגיש כי אומנם לשונן הרחבה של סעיף 45 לפסד"פ מאפשרת את ההכרה בעצם סמכות השימוש בכוח לשם התגברות על אמצעי האבטחה בכניסה לחומרי המחשב האגורים במחשבים, טלפונים סלולריים, התקני אחסון דיגיטליים ויישומונים. אולם, אופן הפעלת הסמכות צריך להיות מפורש ברוח עקרונות של מידתיות הפעלת הכוח. להלן נציע כמה מגבלות בנוגע לאופן הפעלת הכוח בסיטואציה דנן: **ראשית**, יש להפעיל את הכוח כלפי הנחפש רק כאשר אין בנמצא חלופה סבירה אחרת, כגון התגברות על אמצעי האבטחה באמצעות כלים טכנולוגיים מתאימים, ניחוש הסיסמה או מציאתה במסמכים או חומרי מחשב אחרים הנגישים לרשות החוקרת מכוח צו חיפוש. **שנית**, ברי כי הפעלת הכוח צריכה להיעשות באופן סביר, מוגבל, מרוסן, במינימום הדרוש, ולאחר אזהרה מקדימה לחשוד כי בכוונת הרשות החוקרת להשתמש בכוח סביר כדי לממש את הפעולה שבסמכותה לבצע.<sup>49</sup> **שלישית**, יש לתעד את סירובו של הנחפש למסור את טביעת האצבע או להעמיד את פניו מול המכשיר הדורש זיהוי פנים, וכן יש לתעד את אופן השימוש בכוח. זאת על מנת לאפשר בקרה בדיעבד לגבי השימוש בכוח, הן מצד התביעה, הן מצד ההגנה לאחר מכן, והן מצד בית-המשפט במקרה של הגשת כתב-אישום.

## 6. סיכום

המחירה בדבר היחס בין הטכנולוגיה המתקדמת במהירות מסחררת לבין המשפט אשר משתרך אחריה בעצלתיים הפכה בשנים האחרונות כמעט לקלישאה. בעוד שהטכנולוגיה משתכללת ומתקדמת, בעיקר על-בסיס תמריצים כלכליים של חברות פרטיות, המשפט מנסה להתמודד בעזרתה של חקיקה ישנה עם הסיטואציות החדשות. בהקשרנו הנדון כאן, אין מנוס מלשוב ולחזור על הקלישאה השחוקה.

בשנים האחרונות חלה קפיצה נחשנית בפיתוחם של אמצעי אבטחת מידע המבקשים להגן על פרטיותם של המשתמשים במחשבים, בטלפונים סלולריים, בהתקני אחסון ניידים וביישומים מקוונים מפני עיון של גורמים בלתי מורשים בתכנים האגורים במכשירים אלה. קפיצה מקבילה לא אירעה בכל הנוגע לסמכויות החיפוש והחקירה

של רשויות אכיפת החוק. מזה למעלה מ-23 שנה מתקיים דיון בדבר הצורך בחידושם של דיני החיפוש, התפיסה וההמצאה,<sup>50</sup> והצעת חוק ממשלתית הונחה על שולחן הכנסת עוד בשנת 2014.<sup>51</sup> בהצעת חוק זו, המכונה "הצעת חוק החיפוש", התייחסות מפורשת לסמכות לדרוש מנחקר, לרבות חשוד, למסור את מפתח ה"כניסה" אל חומרי המחשב שבשימוש המצויים במחשב, טלפון סלולרי, התקן אחסון נייד או יישומון,<sup>52</sup> אולם גם הצעת חוק זו לא התייחסה לטכנולוגיות של טביעת אצבע או זיהוי פנים, שלא היו מוכרות אז, ומכאן שגם הצעת חוק זו החלה לצבור פיגור אחר ההתפתחויות הטכנולוגיות של השנים האחרונות.

הפיגור האינהרנטי של הדין הקיים אחר ההתפתחויות הטכנולוגיות אינו מכתוב בהכרח תוצאה של אין אונים מצד "עושי המשפט" ובכללן רשויות אכיפת החוק. כיוון שרקמתו של החוק לעולם אינה סגורה לחלוטין, בוודאי כאשר המחוקק השתמש במושגי שסתום פתוחים, ובוודאי בכל הנוגע להוראת סעיף 45 לפסד"פ בה עסקינן כאן, הרי שניתן לפרוש את הוראת הסעיף גם על הסיטואציה החדשה של אמצעי אבטחה חזקים הכוללים זיהוי פנים או שימוש בטביעת אצבע. פרשנות אחרת תוביל, לדעתנו, ליצירת "מרחב חסינות" דה-פקטו לכל מי שמשתמש במחשב, טלפון סלולרי, התקן אחסון נייד או יישומון המוגנים בסיסמה חזקה או במפתח הצפנה שאינה פציחה באמצעים הטכנולוגיים הקיימים כיום בשימושן של רשויות אכיפת החוק. כיוון שבפועל, הטכנולוגיות שבשימושן של רשויות האכיפה אינן מאפשרות להן להתגבר על חלק מהגנות הסיסמה או ההצפנות, הרי שאין לראות בפנייה לשימוש בכוח משום "קיצור דרך" אלא משום בחירה במסלול זה בלית-בררה.

הראינו אפוא כי השימוש בכוח סביר, בהתאם לקבוע בסעיף 45 לפסד"פ, כדי להתגבר על אמצעי אבטחת מידע כמו טביעת אצבע או זיהוי פנים, איננו רק כורח המציאות, אלא הוא אף מתיישב עם פרשנות לשונית ותכליתית של סעיף 45 האמור. יתרה מכך, ביקשנו להראות כי הביקורות המרכזיות שעשויות לקום לפרשנות האמורה - בשל פגיעה בחיסיון מפני הפללה עצמית, אפליה אסורה בין חשודים והפגיעה בזכות לשלמות הגוף - אינן שומטות את הקרקע מתחת לעצם ההצדקה להשתמש בסעיף 45 לפסד"פ בענייננו. עם זאת, ביקורות אלה בהחלט מחדדות את הצורך לפנות לאמצעי זה, של שימוש בכוח, כמפלט אחרון; להשתמש בכוח במידה הפחותה ביותר האפשרית; ולתעד את השימוש בכוח לצורך בקרה בדיעבד בידי ההגנה ובית-המשפט.

50 בשנת 1996 הוגש דין וחשבון של ועדה ציבורית בראשות השופט דב לוין, שנועדה להציע רפורמה בדיני החיפוש, התפיסה וההמצאה שמעוגנים בפסד"פ המיושן. ראו משרד המשפטים **דין וחשבון הוועדה לסדר דין פלילי (אמצעים משטריים) (חיפוש, הצגה, תפיסה וחילוט)** (1996). לאחר הגשת דו"ח ועדת לוין, הוחל בדיונים במחלקת ייעוץ וחקיקה במשרד המשפטים לקראת ניבוש הצעת חוק שתתבסס על מסקנות הוועדה.

51 הצעת חוק סדר הדין הפלילי (סמכויות אכיפה - המצאה, חיפוש ותפיסה), התשע"ד-2014, ה"ח 867. לנוסח הצעת החוק בקריאה ראשונה ראו [fs.knesset.gov.il/19/](http://fs.knesset.gov.il/19/) [law/19\\_Is1\\_278957.pdf](http://law/19_Is1_278957.pdf).

52 שם, בסעיף 95 להצעת החוק.