החיסיון מפני הפללה עצמית: בחינה מחודשת בראי הטכנולוגיה

מאת

חיים ויסמונסקי* ועמוס איתן**

בשנים האחרונות מתמודדות רשויות אכיפת החוק ברחבי העולם עם קשיים הולכים וגוברים בכל הנוגע לצורך להתגבר על הגנות סיסמה והצפנה אשר מותקנות במחשבים, במכשירי טלפון סלולריים, ביישומים ספציפיים או בשירותים מקוונים. קשיים אלה צפו ועלו לתודעה הציבורית בעיקר לאחר פיגוע הטרור שבוצע בעיר סן־ברנרדינו שבארצות הברית בשנת 2015, אז פנה ה־FBI לחברת Apple בבקשה שזו תסייע לו להתגבר על הצפנה שהייתה במכשיר של אחד ממבצעי פיגוע הטרור, שכן לא הייתה אפשרות טכנית להתגבר על ההצפנה בפרק זמן סביר.

מקרים אלה ורבים אחרים מעידים על התנגשות בין צורכיהן של רשויות החקירה והביטחון בבואן לחדור, על פי סמכות כדין, למחשבים ולטלפונים סלולריים, לבין זכויותיהם של המשתמשים לפרטיות ולחיסיון מפני הפללה עצמית.

המאמר סוקר את הטכנולוגיות העיקריות המשמשות כיום לצורך הגנה מפני חדירה או עיון לא מורשים בחומרי מחשב האגורים במחשב או בטלפון סלולרי, ובהן זיהוי פנים, טביעת אצבע, זיהוי קולי ועוד. לאחר מכן המאמר סוקר את החיסיון מפני הפללה עצמית, בראייה היסטורית ובראי ההצדקות המוכרות לחיסיון זה. בהמשך מועלית הטענה כי החיסיון מפורש כבעל תחולה מוחלטת במקומות שבהם הוא מוחל, אולם ההצדקות לחיסיון יכולות להוביל אף לפירוש של החיסיון מפני הפללה עצמית כחיסיון יחסי, הניתן לאיזון אל מול אינטרסים אחרים.

המאמר מבקש להציג מודל משפטי להתמודדות עם סוגיית המתח בין רצונן של רשויות החקירה להתגבר על אמצעי האבטחה המגינים על מכשירי הטלפון הסלולריים ועל המחשבים של חשודים ונחקרים לבין זכויותיהם של בעלי המכשירים לחיסיון מפני הפללה עצמית ולפרטיות. המודל המשפטי המוצע מכיר בחיסיון מפני הפללה עצמית כחיסיון יחסי ומבקש לערוך איזון קונקרטי בין הזכויות לאינטרסים המתנגשים, לפי כמה קווים מנחים אשר יורכבו הן מכללים נוקשים, שהם בבחינת תנאי סף, והן מפרמטרים שייבחנו בכל מקרה ומקרה.

* דוקטור למשפטים, מנהל מחלקת הסייבר בפרקליטות המדינה, עמית מחקר במרכז הסייבר האוניברסיטאי של האוניברסיטה העברית בירושלים, מרצה מן החוץ באוניברסיטת תל אביב ובאוניברסיטת חיפה.

** לשעבר עורך דין במחלקת הסייבר בפרקליטות המדינה, בוגר תואר שני בפקולטה למשפטים באוניברסיטת תל אביב.

האמור במאמר מבטא את עמדתם האישית של הכותבים בלבד. נבקש להודות מקרב לב לחברי מערכת כתב העת **משפטים** ולעורכים, גל דפדי ויחיאל אורן, על הערותיהם הטובות שהעשירו ושיפרו את המאמר. נבקש להודות גם לגב׳ שרה גרין על הערותיה הטובות.

מבוא. א. טכנולוגיות של אבטחת מידע או משוכה לא עבירה בפני רשויות אכיפת החוק? ב. על החיסיון מפני הפללה עצמית ועל זכות השתיקה. ג. יישום החיסיון מפני הפללה עצמית באמצעי אבטחת מידע במחשבים, בטלפונים סלולריים ובשירותים מקוונים. 1. תחולה מלאה של החיסיון. 2. אי־תחולה של החיסיון. 3. מודל חיסיון השימוש. 4. עקיפת ההתנגשות החזיתית עם החיסיון מפני הפללה עצמית. **ד. המודל המוצע: חיסיון יחסי מפני הפללה עצמית.** 1. החיסיון מפני הפללה עצמית כיחסי ולא מוחלט. 2. המודל לבחינת סירובו של נחקר למסור מידע מפוענח ולא מוגן־סיסמה – כללים ותבחינים. 3. המודל המוצע בראי הצעת חוק החיפוש. **ה. סיכום.**

מבוא

> This has become, ladies and gentlemen, the wild west of technology. Apple and Google are the sheriffs and there are no rules.[1]

ב־2 בדצמבר 2015, במהלך אירוע שנערך לקראת חג המולד, התרחשה תקרית ירי בעיר סן ברנרדינו שבקליפורניה שבה נרצחו 14 בני אדם ונפצעו 22. מאוחר יותר הודיע נשיא ארצות הברית דאז ברק אובמה כי מדובר בפיגוע טרור שאחת משני מבצעיו נשבעה אמונים לארגון הטרור ״המדינה האסלאמית״. מייד לאחר הפיגוע החלה חקירה מאומצת של ה־FBI כדי לבחון אם שני מבצעי הפיגוע פעלו לבד או שמא היה גם אדם שלישי בזירת פיגוע הירי. לפי החשדות באותה העת, ראיות אפשריות לקיומו של יורה שלישי, כמו גם ראיות נוספות בעלות ערך רב לחקירה, היו אמורות להימצא בטלפון הסלולרי של אחד היורים, מכשיר מסוג iPhone 5C.[2] אולם סיסמת הכניסה למכשיר לא הייתה ידועה ל־FBI, והסוכנות חששה שניסיונות פריצה באמצעות ניחוש הסיסמה שוב ושוב יובילו אוטומטית למחיקת המידע מהמכשיר.[3] חרף השקעת מאמצים אדירים מצד ה־FBI לא הצליחה הסוכנות במשך תקופה ארוכה לחדור אל הטלפון הסלולרי ולעיין במידע האגור בו. התובע הכללי של ניו יורק אף

1 לדבריו של התובע הכללי של מחוז מנהטן בניו־יורק בדבר הקשיים של רשויות אכיפת החוק לחדור לטלפונים סלולריים ולעיין במידע האגור בהם ראו Alyssa Newcomb, *New York DA Says He Can't Access 175 iPhones from Criminal Cases Due to Encryption – Manhattan DA Cyrus Vance Slams Apple Over Encryption Stance*, ABC NEWS (Feb. 18, 2016), https://tinyurl.com/y3yqgrn4.

2 Lee Ferran & Jack Date, *San Bernardino DA: Clues to Unconfirmed 3rd Shooter, "Cyber Pathogen" Could Be on iPhone – Official Speculates Phone Could Be Used to Harm Infrastructure with Computer Bug*, ABC NEWS (Mar. 4, 2016), https://tinyurl.com/juwkfru.

3 מחיקת המידע האוטומטית מן המכשיר היא פונקצייה שניתנת להפעלה בחלק מהטלפונים הסלולריים מסוג iPhone. הפונקצייה ניתנת להפעלה בידי המשתמש באמצעות כמה פעולות פשוטות. ראו למשל Sidharth Rathore, *Auto Erase Your iPhone Data after 10 Failed Passcode Attempts*, TECHNOBUZZ (July 17, 2017), https://tinyurl.com/y3m6gwky. גם בטלפונים סלולריים שבהם הפונקצייה אינה כלולה כחלק מהגדרות המכשיר, יש יישומונים (אפליקציות) ייעודיים אשר מאפשרים למשתמש להגדיר שלאחר כמה ניסיונות כושלים לניחוש סיסמת הכניסה, המידע שעל המכשיר יימחק. ראו למשל Dallas Thomas, *Make Your Android Auto-Wipe Your Data When Stolen*, GADGETHACKS (Sep. 9, 2014), https://tinyurl.com/y57yaoab.

ציין בדבריו לתקשורת בעניין פרשה זו כי משטרת ניו יורק בלבד מחזיקה ב־175 טלפונים סלולריים מסוג iPhone שאינה מסוגלת לחדור אליהם ולעיין בתוכנם.[4]

פרשת סן־ברנרדינו זכתה להד תקשורתי רב בעיקר סביב דרישת ה־FBI מחברת Apple, שאף גובתה בצו שיפוטי, כי Apple תייצר גרסה חדשה של מערכת ההפעלה, ותספק העתק ממנה ל־FBI, כדי שהסוכנות תוכל לנחש את סיסמתו של היורה מבלי לחשוש שהמידע האגור במכשיר ימחק.

פרשת סן ברנרדינו והדרישה של ה־FBI כי חברת Apple תיצור "Backdoor" בתוכנת ההפעלה שלה פותחת צוהר לדיון בשאלות רחבות יותר שתעמודנה במוקד מאמר זה: כיצד מוחל החיסיון מפני הפללה עצמית בעידן הנוכחי בנוגע למערכות טכנולוגיות מוגנות סיסמה והצפנה, כגון מחשבים, טלפונים סלולריים או שירותים מקוונים; מהו המודל הראוי להחלת החיסיון מפני הפללה עצמית על כפיית פתיחתן של אותן מערכות טכנולוגיות; אם בנסיבות דומות לאלה שבפרשת סן ברנרדינו הייתה ה־FBI רשאית לכפות על בעל הטלפון הסלולרי למסור את הסיסמה לטלפון שלו או לחלופין לפתוח בעצמו את מכשיר הטלפון שלו ולמוסרו ללא הגנת סיסמה, או שמא היה קם לחשוד חיסיון מפני הפללה עצמית; מהן הסנקציות שהיה אפשר להטיל על החשוד כדי לאלצו למסור את הסיסמה, אם בכלל.

לפי הפרשנות הנוהגת כיום בקרב רשויות אכיפת החוק במדינות רבות, החיסיון מפני הפללה עצמית מאפשר לחשודים בעבירות פליליות להימנע ממסירת סיסמת הכניסה או את מפתח ההצפנה לטלפון הסלולרי או למחשב שבבעלותם, וכן להימנע מהנגשת המחשב או הטלפון הסלולרי שלהם או שירות מקוון ספציפי (כגון שירות "ענן", חשבון ברשת חברתית, חשבון דוא"ל או כדומה) כשהם במצב מפוענח וללא הגנת סיסמה. בעיה זו הולכת והופכת כיום לאחד האתגרים הגדולים של רשויות אכיפת החוק ברחבי העולם. למעשה, ניתן להניח כי הקשיים שהוצבו בפני ה־FBI בפרשת סן ברנרדינו ילכו ויגברו.[5]

גם בישראל התעכב פיצוחן של פרשות שונות בגלל אי־יכולתן של רשויות אכיפת החוק לחדור לטלפונים סלולריים, למחשבים או לשירותים מקוונים ולעיין במידע האגור בהם, ובשל הפרשנות הנוהגת לחיסיון מפני הפללה עצמית. כך אירע למשל בפרשה שזכתה לכינוי התקשורת "פרשת פישר". אחד מהנאשמים הראשיים בפרשת שחיתות זו, עו"ד רונאל פישר, טען בחקירתו במחלקה לחקירות שוטרים כי שכח את סיסמת הכניסה לטלפון הסלולרי שלו. לפי פרסומים בכלי התקשורת, עובדה זו עיכבה את החקירה הפלילית בפרשה זו לאורך תקופה ארוכה.[6]

סוגיה זו התעוררה פעמים נוספות בדיונים בערכאות הדיוניות בישראל, אך טרם הגיעה לפתחו של בית המשפט העליון או להסדרה בחקיקה. הקביעות השונות של הפסיקה הישראלית, הגם שלא דובר עד היום בקביעות מנומקות בהרחבה, יצרו עמימות מסוימת

4 Newcomb, לעיל ה"ש 1.

5 לפי דבריו של מנהל ה־FBI רק במהלך שנת 2017 נמנעה מהסוכנות היכולת לעיין בתוכנם של כ־7,775 טלפונים סלולריים ומחשבים שונים. ראו Ellen Nakashima, *FBI Chief Calls Encryption a "Major Public Safety Issue"*, WASH. POST (Jan. 9, 2018), https://tinyurl.com/y2q2qduy.

6 גלי גינת "החקירה נגד רונאל פישר תקועה – בגלל הקוד של האייפון" **וואלה!** (7.4.2015) https://bit.ly/3iFk4ah.

בדבר תחולתו של החיסיון מפני הפללה עצמית על מקרה שבו ידרשו רשויות אכיפת החוק מחשודים ומעדים למסור סיסמאות או מפתחות הצפנה למחשבים, לטלפונים סלולריים או ליישומונים מקוונים שבהם אגור המידע של אותם נחקרים, או להנגיש לחוקרים את חומר המחשב המצוי בהם כשהוא ללא הגנת הצפנה או סיסמה. למשל, בשני מקרים פסקו בתי המשפט כי בסמכותה של הרשות החוקרת להשתמש בכוח סביר כדי להצמיד את אצבעו של החשוד אל הטלפון הסלולרי שלו לשם התגברות על הגנת סיסמה או הצפנה. בשני מקרים אלה לא דנו בתי המשפט בהרחבה בתחולת החיסיון מפני הפללה עצמית של החשוד אשר יאפשר לו לסרב. במקרה אחד קבע בית המשפט בפשטות כי ״צורכי החקירה ואיסוף הראיות מצדיקים את קבלת הבקשה להפעלת כוח סביר כנגד החשוד בסחר בסמים לקבלת טביעת אצבע״,[7] ובמקרה אחר קבע בית המשפט כי פעולה של פתיחת הטלפון הסלולרי של החשוד באמצעות שימוש בכוח סביר ללקיחת טביעת אצבעו נופלת בהגדרה של ״חיפוש חיצוני״ לפי חוק סדר הדין הפלילי (סמכויות אכיפה – חיפוש בגוף ונטילת אמצעי זיהוי), התשנ״ו–1996 (להלן: חוק נטילת אמצעי זיהוי), ולכן מלכתחילה לא נדרשה הרשות החוקרת להרשאה שיפוטית כדי לעשות כן.[8] מנגד, במקרה אחר פסק בית המשפט 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 ו׳לפרוץ׳ למכשיר״.[9] כאמור, בתי המשפט לא נימקו בהרחבה את הכרעותיהם.

בצד ההתנגשות הפוטנציאלית שתוארה לעיל בין צורכי החקירה לבין החיסיון מפני הפללה עצמית, הסוגיה הנדונה רלוונטית לציר נוסף שנמתח בין צורכי החקירה מחד גיסא לבין הזכות לפרטיות מאידך גיסא. מחשבים, טלפונים סלולריים ושירותים מקוונים כדוא״ל, אחסון ב״ענן״ וכדומה, תופסים כיום חלק מרכזי בחקירות פליליות, משום שהם אוגרים בתוכם כמויות עצומות של מידע, הם משמשים את המעורבים (החשודים, נפגעי העבירה והעדים) בתכיפות, ולעיתים קרובות הם אף צמודים פיזית למעורבים. המחשבים, הטלפונים הסלולריים והשירותים המקוונים מוגנים באמצעי אבטחה מובנים (Built-in), כגון סיסמה, זיהוי פנים או טביעת אצבע.[10] משכך, בכוחו של המידע האצור בקרבם של המחשבים, הטלפונים הסלולריים והשירותים המקוונים לאשש או להפריך גרסאות של הנחקרים, להכיל אמרות נוספות שלהם, לכלול תיעוד של פעילותם, להעיד על מיקומם במועד הרלוונטי לחקירה ועוד. שפע זה של מידע מגביר את המתח שבין צורכי הרשות החוקרת לבין זכותו של המשתמש במחשב לפרטיות בנוגע לאותו מידע. מחד גיסא, כיוון שמחשבים, טלפונים סלולריים ושירותים מקוונים אוגרים או מתעדים כמויות עצומות של מידע אישי רגיש ממגוון סוגים, הן על המשתמש הקבוע במכשיר והן על צדדים שלישיים שמנהלים עימו

7 צ״ח 49644-06-18 **מדינת ישראל נ׳ פלוני** (21.6.2018).

8 ע״ח (מחוזי ת״א) 45208-01-19 **תחנת מרחב יפתח נ׳ רפאלי** (18.1.2019).

9 עמ״י (מחוזי י-ם) 65308-10-18 **דרוויש נ׳ מדינת ישראל** (נבו 26.10.2018).

10 ראו פירוט להלן בפרק א.

שיח,[11] קיים חשש לפגיעה עודפת לא מידתית בפרטיותם של המשתמש הקבוע במכשיר ושל הצדדים השלישיים בתהליך החיפוש בחומר המחשב ובעיבודו.[12] קיים חשש נוסף לפגיעה בפרטיות, מדלף המידע בשל אבטחה לא מספקת שלו.[13] מאידך גיסא, רשויות החקירה זקוקות פעמים רבות למידע האגור במחשבים, בטלפונים סלולריים ובשירותים מקוונים, הכולל ראיות חשובות שיסייעו בחקר האמת. התיעוד הרציף של חייו של אדם השמור במכשירים אלה, בייחוד בטלפון הסלולרי, עשוי פעמים רבות להכיל מידע רב ערך עבור רשויות החקירה.[14] למעשה, זכותם של חשודים לפרטיות והאינטרס החקירתי מצויים במעין מקבילית כוחות, שבה שינוי בצד אחד של המשוואה משפיע מייד על צידה האחר – הגברת פרטיותם של משתמשים בכל הנוגע להגנה על המידע האגור במחשבים, בטלפונים סלולריים ובשירותים מקוונים מעמידה חסמים בפני רשויות אכיפת החוק בבואן לחקור עבירות ולאכוף את הדין הפלילי. מתח זה בין פרטיותם של חשודים לבין האינטרס החקירתי ילווה את הדיון במאמר זה.

כפי שנראה לאורך המאמר, פעמים רבות רשויות אכיפת החוק אינן מסוגלות כיום להתגבר על אמצעי אבטחת מידע בכוחות עצמן. הפתרון לבעיה זו, מבחינתן של רשויות האכיפה, יכול להימצא באחד מחמשת המהלכים האלה: **האחד**, חיוב הנחקר (המשתמש או הבעלים של המחשב, הטלפון הסלולרי או החשבון ביישום המקוון) – על פי דין או על פי צו שיפוטי קונקרטי מכוח החוק – למסור את קוד ההצפנה או הסיסמה לעיון בחומר המחשב או להנגיש לידי החוקרים את חומר המחשב כשהוא בתצורה מפוענחת ונטולת סיסמה;[15] **השני**, קבלת מפתח ההצפנה או סיסמת הכניסה מידי המשתמש או הבעלים של

11 ראו, בהקשר אחר, את קביעותיו של בית המשפט העליון בבש״פ 6071/17 **מדינת ישראל נ׳ פישר**, פס׳ 10–12 לפסק דינו של השופט עמית (נבו 27.8.2017) (אשר דן בדרכים ליישומו של ס׳ 74 לחוק סדר הדין הפלילי [נוסח משולב], התשמ״ב–1982 (להלן: החסד״פ) בחומרי חקירה דיגיטליים האגורים במחשבים, בהתקני אחסון ניידים ובמכשירי טלפון סלולרי, והמובאות שם). בהקשר אחר ראו גם ע״פ 8627/14 **דביר נ׳ מדינת ישראל** (נבו 14.7.2015).

12 לדיון בשאלת החשש האמור לפגיעה בפרטיות ובכללים המשפטיים הנגזרים מן החשש האמור ראו לדוגמה בש״פ 7917/19 **אוריך נ׳ מדינת ישראל** (נבו 25.12.2019) (להלן: עניין **אוריך הראשון**); בש״פ 1758/20 **אוריך נ׳ מדינת ישראל** (נבו 26.1.2021).

13 ראו בהקשר זה צ״ח 42186-10-17 **מדינת ישראל נ׳ כהנא** (27.10.2017); ע״ח 57278-10-17 **כהנא נ׳ מצ״ח חיפה** (30.10.2017) (שם נחקר תא״ל כהנא במשטרה הצבאית החוקרת (מצ״ח) בחשד לעבירות של מרמה והפרת אמונים, עיכוב ציוד ואי־קיום הוראות מחייבות, עבירות בנשק והוצאת רכוש צבאי מרשות הצבא. כהנא התנגד לצו החדירה לחומרי המחשב שהוציאה מצ״ח בענייננו וטען בפני בית המשפט כי עצם ההחזקה של המידע הפרטי שאגור במכשיר הטלפון הסלולרי שלו בידי הרשות החוקרת עלולה להסב פגיעה בפרטיותו, בעיקר בשל החשש מפני ״דליפה״ של המידע הפרטי אל מחוץ ליחידה החוקרת).

14 בהקשר זה ראו רע״פ 8873/07 **היינץ ישראל בע״מ נ׳ מדינת ישראל**, פס׳ 17 לפסק דינה של הנשיאה ביניש (נבו 2.1.2011) (שם קבע בית המשפט העליון כי ״השימוש האינטנסיבי במחשבים הופך אותם גם לאוצר בלום של ראיות מפליליות ומידע רלוונטי אשר יכול וצריך לשמש את רשויות החקירה במאבקן במפרי חוק ועוברי עבירה״).

15 יוער כי ייתכנו מקרים שבהם גם לאחר שיחויב לעשות כן, ימסור החשוד סיסמה או מפתח הצפנה שגויים כדי להטעות את חוקריו. כך אירע למשל בת״פ (מחוזי ת״א) 40071/04 **מדינת ישראל נ׳ חברת בוריס פקר הנדסה בע״מ** (נבו 10.7.2005).

המחשב, הטלפון הסלולרי או השירות המקוון בדרך של תחבולה שתוביל אותו להסגיר את האמצעי שמאפשר את פתיחת הסיסמה או ההצפנה; **השלישי**, שימוש בכוח סביר, במקרים המתאימים, כדי לגשת אל המידע. למשל, כאשר הנחקר משתמש בטביעת אצבעו בתור מפתח הצפנה או סיסמה, ושימוש בכוח סביר יכול לאפשר לרשויות החקירה לגשת אל המידע המאוחסן במחשבו של החשוד או של העד;[16] **הרביעי**, זקיפת משקל ראייתי לחובתו של החשוד המסרב למסור את המידע המפוענח או את מפתח ההצפנה או הסיסמה, כתחליף למידע שנשלל מהרשות החוקרת בשל סירובו. ייאמר מייד כי ברוב המקרים סביר להניח כי מהלך זה לא יוביל לפתרון מלא לבעיה הניצבת בפני רשויות החקירה, שכן המשקל הראייתי החלופי שיינתן לעצם הסירוב לא ימלא את החלל הראייתי שנוצר מאי־פיענוחו של חומר המחשב המדובר; **החמישי**, קבלת ה״מפתח״ מידי היצרנית של המחשב או של הטלפון הסלולרי, מידי ספקית השירות המקוון או מידי צד ג אחר. ארבעת המהלכים הראשונים שמנינו מתייחסים לנחקר עצמו, ואילו המהלך החמישי מתייחס לצדדים שלישיים, שאינם נוגעים במישרין לחקירה. בכל הנוגע למהלך חמישי זה נדרש לדוגמה שליצרנית המחשב או הטלפון הסלולרי או לספקית השירות המקוון תהיה גישה לסיסמת הכניסה או למפתח ההצפנה. בפועל כיוון שעל פי רוב אין אסדרה מראש שדורשת מהיצרנית או מספקית השירות לשמור ברשותה סיסמת כניסה, מפתח הצפנה או לחלופין ״דלת אחורית״ שתאפשר לפתוח את המכשיר או את חשבון המשתמש — חברות רבות בוחרות לפתח את המערכות שלהן בדרך אשר אינה משמרת בידיהן את הכוח להשיג גישה כאמור.[17] כיוון שכך, גם אם תידרשנה על פי דין למסור לרשויות האכיפה את הסיסמה או את מפתח ההצפנה, הן לא תוכלנה, מבחינה מעשית, לספק את המידע הדרוש. הינה כי כן, המהלך המעשי המרכזי

16 במקום אחר דנו בהרחבה באפשרות של שימוש בכוח לצורך התגברות על הגנת סיסמה או הצפנה, בהצדקות להכרה בשימוש שכזה בכוח ובדרכים להתמודדות עם ביקורות על פרקטיקה זו. ראו חיים ויסמונסקי ועמוס איתן ״השימוש בכוח סביר לשם התגברות על הגנת סיסמה והצפנה: הצדקות וביקורות״ **הסניגור** 268, 4 (2019) (להלן: ויסמונסקי ואיתן ״השימוש בכוח סביר״). לגישה שונה ביחס להתמודדות עם קשיים טכנולוגיים אלה ולביקורת על התפיסה שהצגנו שם ראו יגאל בלפור וגיל שפירא ״ונשמרתם לאצבעותיכם: חובתו של חשוד לסייע לחיפוש במכשיר סלולארי ושימוש בכח לשם פתיחת מכשיר הנעול באמצעות טביעת אצבע״ **הסניגור** 267, 4 (2019).

17 רוב חברות הטכנולוגיות הגדולות, כמו Facebook, Apple או WhatsApp, פיתחו את מערכות המחשוב שלהן כך שסיסמאותיהם של המשתמשים או התוכן שאותו הם מעבירים מאחד לשני אינם נשמרים כלל בחברה. באשר ל־Facebook ראו Alex Hern, *Why Won't Facebook Give Access to Lucy McHugh Murder Suspect's Account?*, THE GUARDIAN (Sep. 5, 2018), https://tinyurl.com/yxjn8alj. באשר ל־WhatsApp, בפירוט המופיע באתר האינטרנט של החברה בכל הנוגע לשאלת אבטחת המידע נקבע כי: "WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp" (WHATSAPP, www.whatsapp.com/security/ (last visited Feb. 1, 2021)). באשר ל־Apple, במסמך ההנחיות שניסחה Apple לרשויות חקירה מחוץ לארצות־הברית, בבואן לבקש מידע מהחברה, נקבע כי: "Apple does not possess the encryption key" (ראו LEGAL PROCESS GUIDELINES – GOVERNMENT & LAW ENFORCEMENT OUTSIDE THE UNITED STATES הזמין באתר האינטרנט של החברה, *Apple's Guidelines for Law Enforcement Requests*, APPLE (last visited Oct. 6, 2021), https://apple.co/2ZZzjEh).

עשוי להיות בדרך של דרישת המידע המפוענח מידי הבעלים או המשתמש הקבוע במחשב, בטלפון הסלולרי או בשירות המקוון.

הדין הקיים בישראל אינו מתייחס במישרין לסוגיה דנן. עם זאת בשנת 2014 פורסמה הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע״ד–2014.[18] הצעת חוק זו קובעת הסדרים חדשים לכלל דיני החיפוש והתפיסה, ופרק ו׳ להצעה דן בפעולות בחומר מחשב. סעיף 95 להצעת החוק עניינו ב״צו למסירת סיסמה או מפתח הצפנה״, והוא קובע סמכות לדרוש מבעל גישה לחומר מחשב למסור את מפתח ההצפנה או הסיסמה לחומר מחשב הדרוש לחקירה, בתנאים שונים, כמפורט בסעיף. על פי הקבוע בסעיף 72 להצעת החוק, ״בעל גישה לחומר המחשב״ כולל גם את ספקית השירות.[19] סעיף 95(ג) להצעת חוק החיפוש קובע כי סירוב למסור מפתח הצפנה או סיסמה על פי צו מחייב משמעו חיזוק משקל הראיות של התביעה. במילים אחרות, סעיף 95 הנ״ל קובע סמכות לפעול על פי שלושה מהמהלכים שנמנו לעיל: דרישה מהמשתמש במחשב, בטלפון הסלולרי או בשירות המקוון למסור את הסיסמה או את מפתח ההצפנה; דרישה אפשרית גם מספקית השירות; הענקת משקל ראייתי במקרה של סירוב. הצעת חוק החיפוש אינה מתייחסת לשאלת האפשרות להשיג את הסיסמה או את מפתח ההצפנה מהנחקר בדרך של תחבולה, וכן אינה מתייחסת לאפשרות השימוש בכוח במקרה של סירוב לציית לצו המחייב מסירת סיסמה או מפתח הצפנה. בהמשך המאמר נשוב להידרש להוראת הסעיף הנ״ל, על רקע הניתוח הנורמטיבי של החיסיון מפני הפללה עצמית בראי ההתפתחויות הטכנולוגיות ועל רקע הצעתנו למודל ראוי באשר לתפיסתו של החיסיון האמור.

בדיון במאמר נציג בפירוט את המודלים השונים להתמודדות עם השאלה אם וכיצד ראוי לאפשר לנחקרים להשתמש בחיסיון מפני הפללה עצמית בנסיבות שבהן רשויות החקירה נעדרות יכולת עצמאית להתגבר על ״המנעול הטכנולוגי״ בדמותם של הסיסמה או מפתח ההצפנה. נבחן את המודלים הללו, נבקרם ונטען לבסוף כי החיסיון מפני הפללה עצמית לא נועד לאפשר לחשודים בעבירות פליליות חסינות מוחלטת מפני העמדה לדין. החיסיון מקדם מטרות חשובות וראויות להגנה, אולם כמרבית החסיונות בדין, עליו להתפרש כחיסיון יחסי, הניתן להגבלה מידתית בנסיבות מתאימות, שבעניינן נפרט בהמשך המאמר. כפי שנציג בהמשך, ניתן לאתר בחקיקה ובפסיקה ניצני הכרה בכך שהחיסיון מפני הפללה עצמית הוא יחסי, אך ניצני הכרה אלה טרם נדונו לעומק. עוד נטען כי ההתפתחויות

18 הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע״ד–2014, ה״ח 867 (להלן: הצעת חוק החיפוש) (הצעת חוק ממשלתית שעברה קריאה ראשונה, ובמהלך שנת 2018 החלה ועדת החוקה, חוק ומשפט של הכנסת בדיונים לצורך הכנת ההצעה לקריאה שנייה ושלישית).

19 יצוין כי הצעת חוק החיפוש הונחה על שולחן הכנסת ביום 19.5.2014, וכי תזכיר חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה), התשע״א–2011 הופץ להערות הציבור ביום 10.4.2011. מאז מועדים אלה חלו שינויים טכנולוגיים רבים, הן בכל הנוגע לסוגי הטכנולוגיה המשמשת לאבטחת המידע במחשבים, בטלפונים סלולריים ובשירותים מקוונים, ובעיקר בכל הנוגע לתפוצתם של אמצעי אבטחת מידע אלה. לשם ההמחשה נזכיר כי הטלפון הסלולרי הראשון, בתפוצה פופולרית רחבה, אשר השתמש בטביעת אצבע לצורך הגנה על המידע האגור במכשיר היה ה־iPhone 5c, של חברת Apple. המכשיר יצא לשוק בארצות הברית ב־20.9.2013 (כשנתיים וחצי לאחר פרסום תזכיר החוק וכשמונה חודשים בלבד לפני הנחת הצעת חוק החיפוש על שולחן הכנסת).

הטכנולוגיות בתחום הגנת המידע האישי במחשבים, בטלפונים סלולריים ובשירותים מקוונים אינן משנות את פניו של החיסיון מפני הפללה עצמית מן היסוד, אלא הן מאפשרות לדייק את ההתבוננות על החיסיון. הטכנולוגיה מאפשרת למעשה להשחיז ולמרק את הערכים שביסוד החיסיון מפני הפללה עצמית ולגזור מסקנות כלליות בעניינו שאינן נוגעות רק לסוגיה הקונקרטית של התגברות על מנגנוני ההגנה מפני חדירה למחשבים, לטלפונים סלולריים ולשירותים מקוונים.

מבנה המאמר יהיה כדלקמן: בפרק א להלן נסקור את עיקרי הטכנולוגיות הקיימות כיום שנועדו להגן על מחשבים, על טלפונים סלולריים ועל שירותים מקוונים מפני חדירה ללא הסכמת המשתמש. מטרתן של טכנולוגיות אלה להגביר את ההגנה על המידע האישי של המשתמשים. בעקבות זאת כאמור ניצבת משוכה, לעיתים לא עבירה, בפני רשויות אכיפת החוק. בפרק ב נציג בכלליות את החיסיון מפני הפללה עצמית, את ההצדקות העיוניות שבבסיסו וכיצד הוא מבוטא כיום בדין הישראלי. בפרק ג נתמקד בסוגיה שבמרכז המאמר ונציג שלושה מודלים שונים ליישום החיסיון מפני הפללה עצמית בהקשר של טכנולוגיות להגנה על מחשבים, על טלפונים סלולריים ועל שירותים מקוונים מפני חדירה ללא הסכמת המשתמש, אף אם את החדירה מבצעות רשויות החקירה על פי סמכותן כדין. בתוך כך נבקש להציג חמישה כלים פרקטיים אשר מאפשרים לפתור את הסוגיה שבמוקד מאמרנו ונבחן אם וכיצד ניתן ליישמם לפי כל אחד מן המודלים אשר מפורטים בפרק ג. לאחר מכן נציג בפרק ד את המודל המוצע להתבוננות על החיסיון מפני הפללה עצמית כיחסי במהותו. עוד נציג את עיקרי המודל המוצע ואת הממשקים שבינו לבין הקשרים דומים. עוד נטען כי ההתפתחויות הטכנולוגיות הנדונות במאמר מאפשרות לחשוף את מהותו האמיתית של החיסיון מפני הפללה עצמית, וכי למעשה אין מדובר בהצעה לשינוי טבעו של החיסיון בשל ההתפתחויות הטכנולוגיות אלא בגילוי טבעו האמיתי. בפרק ה נסכם את הדיון.

א. טכנולוגיות של אבטחת מידע או משוכה לא עבירה בפני רשויות אכיפת החוק?

לורנס לסיג (Lessig), מאבות האסכולה של משפט וטכנולוגיה, סרטט לפני קרוב ל־20 שנה את הקשר ההדוק שבין המשפט לבין הטכנולוגיה. לפי המודל שזכה לכינוי ״מקבילית הכוחות הלסגיאנית״, יש ארבעה גורמים המסדירים את התנהגותו של הפרט במרחב – המשפט, הנורמות החברתיות, כוחות השוק והארכיטקטורה, כאשר במרחב המקוון הארכיטקטורה נוצרת באמצעות הטכנולוגיה, בידי עורכי התוכנות או היישומים. ארבעת המסדירים הללו מנהלים מערכת של יחסי גומלין אלה עם אלה ומשפיעים זה על זה.[20] בתוך כך בעניינו הנדון כאן נתמקד בציר שבין המשפט, המכונן בין היתר את סמכויות החקירה, את דיני החסיונות ואת הזכות פרטיות, לבין הטכנולוגיות שיפורטו להלן, שהמשותף להן הוא

20 Lawrence Lessig, *The Law of the Horse: What Cyber Law Might Teach*, 113 HARV. L. REV. 501 (1999).

ההגנה על המידע האישי של המשתמש במחשב, בטלפון הסלולרי או בשירותים מקוונים, ומטרתן להגביר את פרטיות המשתמשים (להלן: טכנולוגיות מגבירות־פרטיות).[21]

טכנולוגיות מגבירות־פרטיות הן שם כולל למגוון רחב של טכנולוגיות, ובהן תוכנות שבאמצעותן יכול המשתמש להצפין את שיחותיו ואת תכתובותיו, מנעולים שבאמצעותם הוא יכול להגן על חומרי המחשב שלו מפני חשיפה לא מורשית לאחר או אמצעים אחרים לטשטש או למנוע גישה אל עקבותיו הדיגיטליים.[22] טכנולוגיות מגבירות־פרטיות מאפשרות להצפין את התקשורת המקוונת, לרבות התקשורת האגורה,[23] של הפרט, לשמור על זהותו אנונימית או להגביר את יכולתו לבחור אם ועד כמה לשתף במידע אישי.[24] חלק מהטכנולוגיות מגבירות־הפרטיות מעוצבות מראש, בשלב התכנון של המוצר, וחלקן מוטמעות במוצר לאחר יציאתו לשוק. עיצובן ויישומן של טכנולוגיות מגבירות־פרטיות בשלב התכנון המוקדם של המוצר מגלמים תפיסת פרטיות המכונה Privacy by Design.[25] לטכנולוגיות מגבירות־פרטיות יתרונות רבים מבחינתו של משתמש הקצה: מלבד החשיבות שכל אדם מייחס, אם הוא מייחס, לפרטיותו כשלעצמה, טכנולוגיות מגבירות־פרטיות מסוככות על המשתמש מפני פעילויות לא חוקיות כמו הונאה או גנבת זהות,[26] וגם מפני פעילויות העשויות להיות חוקיות אך המשתמש יעדיף להימנע מהן, כמו פרסום ממוקד או מחירים מותאמים אישית בפלטפורמות מקוונות.[27] טכנולוגיות מגבירות־פרטיות אף עשויות להקנות אנונימיות לאנשים המבקשים להתבטא בחופשיות וחוששים מפני עינה הפקוחה של המדינה או של הקהילה שבה הם חיים.[28] יתרונות אלה, מבחינתו של משתמש הקצה, יכולים להיתרגם לתמריץ עבור יצרניות מכשירי הקצה לייצר מכשירים הכוללים

21 לסקירה מעמיקה על הקשר שבין הזכות לפרטיות לבין ארכיטקטורה, ראו מיכאל בירנהק **מרחב פרטי – הזכות לפרטיות בין משפט לטכנולוגיה** 45–48 (התשע״א).

22 חיים ויסמונסקי **חקירה פלילית במרחב הסייבר** 38–39 (2015) (להלן: ויסמונסקי **חקירה פלילית**).

23 הכוונה ב״תקשורת אגורה״ (stored communication) היא לתקשורת שהגיעה ליעדה הסופי (כגון מכשיר הקצה של הנמען) או ליעד ביניים (כגון שרת מקשר), ובשלב זה היא נאגרת. להרחבה ראו שם, בעמ׳ 186–196.

24 Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1414–1415 (2011).

25 תקנות האיחוד האירופי בנוגע להגנת מידע (GDPR) מתייחסות במפורש לרעיון של Privacy by Design ראו 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), art. 25(2), 2016 O.J. (L 119) 1, 48 (“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 are processed”).

26 לפי הערכות שונות, בשנת 2016 לבדה ״נגנבה זהותם״ של יותר מ־15 מיליון אמריקנים. ראו Herb Weisbaum, *Identity Fraud Hits Record Number of Americans in 2016*, NBC NEWS (Feb. 2, 2017), https://tinyurl.com/y5jl2sdc.

27 לסקירה בכל הנוגע לאפשרות להתאים את מחיריהם של מוצרים באופן אישי ללקוח, על בסיס מעקב אחר הרגלי הצריכה שלו, ראו Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1015–1018 (2014).

28 בירנהק, לעיל ה״ש 21, בעמ׳ 402.

אמצעים להגנת המידע האישי. תמריץ נוסף להטמעה של טכנולוגיות מגבירות־פרטיות במכשיר הקצה נעוץ בעובדה שלעיתים מוצר שאינו מאובטח כראוי לא יוכל ״לתקשר״ עם מוצר אחר, כיוון שלא יעמוד בדרישות סף של אותו מוצר אחר לאבטחת מידע. בנסיבות אלה אפשר שהמשתמש במוצר הלא מאובטח יידרש להטמיע מערכות מגבירות־פרטיות על מנת לחצות את אותו סף.

עם זאת ייתכן שמחיר מכירה נמוך יותר של מוצר הנעדר טכנולוגיות מגבירות־פרטיות ישפיע על חלק ממשתמשי הקצה יותר מאבטחה מוגברת. ״מחיר״ נוסף של השימוש בטכנולוגיות מגבירות־הפרטיות יכול לבוא לידי ביטוי בחוויית המשתמש. כך הוא למשל במקרים שבהם אתר אינטרנט מסוים אינו מאפשר שמירה אוטומטית של שם המשתמש והסיסמה, מה שמכביד על המשתמש שנאלץ לזכור ולהקליד כל פעם מחדש את שם המשתמש והסיסמה. דוגמה נוספת נעוצה במורכבותה של סיסמת הכניסה למחשבים, לטלפונים סלולריים או לשירותים מקוונים. למשל, משתמשים רבים יבחרו להתקין במכשיר הטלפון הסלולרי שבבעלותם סיסמת כניסה (אם בדמות דפוס סרטוט ואם בקוד מספרי). עם זאת אילו היה אפשר להתקין במכשיר הטלפון הסלולרי רק סיסמת כניסה בעלת עשרה תווים ולהוסיף דרישה שלפחות תו אחד יכלול אות גדולה, אות קטנה, מספרים וסימנים, סביר להניח שחלק מבעלי הטלפונים הסלולריים היו מעדיפים שלא להתקין סיסמה כאמור, בשל הסרבול שבחוויית המשתמש.[29]

בהנחה שמדובר בשוק משוכלל וחופשי, משתמש הקצה רשאי לבחור בכל עת מהו ״מחיר הפרטיות״ שאותו הוא מוכן לשלם כדי להשתמש במחשבים, בטלפונים סלולריים ובשירותים מקוונים. מובן שהנחת המוצא בדבר שוק משוכלל וחופשי היא במישור העיוני בלבד, שכן בפועל השוק הנדון סובל מפוטנציאל קרטליזציה או מונופוליזה; משתמש הקצה סובל לעיתים מפערי מידע; מאסדרים מדינתיים ובין־לאומיים שונים כופים הסדרים מסוימים המשפיעים על השוק.

עם זאת הבחירה של משתמש הקצה מציבה אתגר לפתחן של רשויות אכיפת החוק.[30] העובדה שמשתמש הקצה הוא שמחליט למעשה בדבר גובה המשוכה שתוצב בפני הרשות החוקרת היא ייחודית ומאפשרת למבצעי עבירות, בצד כל הברכה שבשימוש בטכנולוגיות מגבירות־פרטיות, לנצל לתועלתם את השימוש בהן.

נציג להלן את הטכנולוגיות מגבירות־הפרטיות הרלוונטיות לדיוננו. בהקשרנו ניתן לחלק את הטכנולוגיות מגבירות־הפרטיות לשתי קטגוריות: הגנת סיסמה והצפנה. נעמוד תחילה על ההבדל בין השתיים. סיסמת כניסה נועדה לנעול את שער הכניסה אל המכשיר או אל יישום או קובץ ספציפי. לעומת זאת הצפנה היא דרך מורכבת יותר להגן על פרטיותם של משתמשים, בדרך של ערבול התוכנה או המידע המיוצגים בביטים, על בסיס מניפולציה

29 לסקירה על הקושי שבשינוי הרגלי היום־יום כדי להגן על הפרטיות ראו Calo, לעיל ה״ש 27, בעמ׳ 1027–1031.

30 ראו למשל John E.D. Larkin, *Compelled Production of Encrypted Data,* 14 VAND. J. ENT. & TECH. L. 253, 257 (2012); Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISC. 298, 302–303 (2014).

מתמטית מסוימת,[31] ובכך הופך רצף הביטים לבלתי ניתן לפיענוח, לג׳יבריש.[32] הפיכת מידע מוצפן למידע ניתן לפיענוח נעשית באמצעות ״מפתח הצפנה״, הידוע למורשי הגישה אל התוכנה או המידע.[33] מפתח ההצפנה מאפשר לבצע במהופך את המניפולציה המתמטית ולהשיב את מבנה התוכנה או המידע הדיגיטלי על כנו. בהקשר זה יוער כי לעיתים מי שמבצע את פעולת ההצפנה אינו מורשה־גישה למידע ולעיתים אף אינו מחזיק במפתח ההצפנה. כך הוא למשל בכל הנוגע לתכתובות ביישומון להעברת המסרים המיידיים WhatsApp, שבו מוצפנות אוטומטית כל התכתובות בין משתמשי הקצה, ורק משתמשי הקצה המתקשרים ביניהם יכולים לעיין בהודעות המפוענחות. לחברה המספקת את השירות אין מפתחות ההצפנה.[34]

טכניקות ההצפנה הולכות ומשתכללות עם השנים, וככל שמפתח ההצפנה ארוך יותר ומשתמש בפונקצייה מתמטית מורכבת יותר, כך יהיה קשה יותר למי שאינו מורשה־גישה לתוכן המוצפן לפענח את מפתח ההצפנה. מכאן שלרשויות החקירה הנדרשות לפענח טקסט מוצפן עומדות לכאורה ארבע אפשרויות: **הראשונה**, שימוש בטכניקה של ניחוש אוטומטי של מפתח ההצפנה. טכניקה זו עשויה להימשך לעיתים שנים רבות (ולעיתים – תלוי במורכבות ההצפנה – אף אלפי שנים) עד למציאת מפתח ההצפנה הנכון.[35] יתרה מזאת, לעיתים התוכן המוגן בהצפנה יינעל זמנית או סופית בעקבות שגיאה חוזרת בניחוש מפתח ההצפנה. האפשרות **השנייה** היא פיצוח של הקוד המתמטי שבאמצעותו מוצפן התוכן, משמע למידה של המניפולציה המתמטית שבאמצעותה בוצעה ההצפנה, איתור דפוסיה והגעה אל המספר המייצג את מפתח ההצפנה בדרך מושכלת.[36] האפשרות **השלישית** היא דרישה מבעל המכשיר למסור את המידע כאשר הוא מפוענח ולא מוצפן כתלות במכשיר המשפטי הרלוונטי המאפשר להציב דרישה משפטית שכזאת. האפשרות

31 להרחבה בהקשר זה ראו Paul Horowitz et al., *The Law of Prime Numbers*, 68 N.Y.U. L. REV. 185, 188–189 (1993).

32 בהקשר זה יש להבחין בין קריפטוגרפיה (Cryptography) לבין סטגנוגרפיה (Steganography). סטגנוגרפיה היא פעולה אשר הופכת טקסט מקורי ומובן לבלתי נראה, משמע עצם הימצאותו של הטקסט אינה ידועה לאנשים שאינם מחזיקים במפתח ההצפנה. הדוגמה הקלאסית לטקסט שעבר הליך של סטגנוגרפיה היא השימוש בדיו נעלמת. לעומת זאת קריפטוגרפיה היא הפעולה של כתיבת הטקסט המקורי באמצעות סימנים שונים שנועדו להסוות את משמעותו של הטקסט המקורי. בהקשר הטכנולוגי נפוץ השימוש בקריפטוגרפיה, אך לא שכיח השימוש בסטגנוגרפיה. משמע, לרוב ידע מי שמבקש לפענח את הטקסט המוצפן כי אכן יש טקסט מוצפן, אך הוא לא יהיה מסוגל לקרוא את הטקסט מבלי להשיג ראשית את מפתח ההצפנה. להרחבה בעניין זה ראו DAVID KAHN, THE CODEBREAKERS 4–6 (1973).

33 בכל הנוגע למחשבים, מפתח הצפנה הוא לרוב פונקצייה מתמטית ארוכה, שיכולה לכלול גם מאות מספרים שונים. עם זאת למען נוחות השימוש, נוצר לרוב מפתח הצפנה נגיש יחסית (כמו מילת קוד או רצף מספרים שניתן לזוכרו בקלות יחסית), אשר בעת הקשתם מומרים למפתח ההצפנה האמיתי – הפונקצייה המתמטית. להרחבה בעניין זה ראו Andrew J. Ungberg, *Protecting Privacy through Responsible Decryption Policy*, 22 HARV. J. L. & TECH. 537, 540–541 (2009).

34 *About End-To-End Encryption*, WHATSAPP (2021), https://bit.ly/3mxqp8H.

35 Ungberg, לעיל ה״ש 33, בעמ׳ 541.

36 שם.

הרביעית, כמובן, היא ידיעת הקוד.[37] לשם כך נדרשות רשויות החקירה לקבל את מפתח ההצפנה מאת משתמש הקצה או מאת ספקית השירות. לחלופין, עשוי המפתח להתגלות במהלך ביצוע פעולות חקירה אחרות, כגון מציאת המפתח במהלך חיפוש או קליטתו במהלך האזנת סתר שבה חשף המשתמש במכשיר את מפתח ההצפנה.

השימוש בהצפנות, כחלק אינטגרלי מהשימוש בשירותים מקוונים, הולך ונפוץ בעולם. ההצפנה הפכה בשנים האחרונות לחלק בלתי נפרד משירותי העברת מסרים מיידיים כגון WhatsApp, Telegram, Facebook Messenger, Viber ועוד. הערכות שונות גורסות כי יותר מ־1.5 מיליארד איש ברחבי העולם משתמשים ביישומונים להעברת מסרים מיידיים אשר משתמשים שימוש מובנה (Built-in) בהצפנה.[38] כמו כן במהלך שנת 2017 הוערך כי בכ־21% ממכשירי הטלפון הסלולריים בעולם המידע מוצפן אוטומטית, ללא החלטה מודעת או בחירה אקטיבית של משתמש הקצה.[39] הנה כי כן, נראה כי הצפנה של מידע ממוחשב הפכה בימינו לחיזיון נפוץ, וכפועל יוצא מכך אותו מידע העשוי להיות בעל פוטנציאל ראייתי עלול להפוך ללא נגיש לרשויות החקירה.[40]

להלן נמנה חמש דרכים להנגשת הסיסמה או מפתח ההצפנה למשתמשי הקצה במחשב, בטלפון סלולרי או בשירות מקוון, ואלה הן: קוד תווי, טביעת אצבע, זיהוי פנים, דגימת קול וזיהוי דפוס השימוש במכשיר.

הדרך **הראשונה** היא הקוד התווי. זוהי ככל הנראה טכנולוגיית האבטחה הנפוצה ביותר,[41] ולעיתים גם נתפסת כשיטה הידידותית ביותר למשתמש הקצה.[42] מדובר ברצף של תווים שהמשתמש מקיש במחשב, בטלפון הסלולרי או בשירות המקוון כדי לגשת אל המידע האגור בו. הקוד התווי יכול להתבטא בכמה אופנים: רצף של ספרות, סרטוט ״קו נעילה״[43] או קוד מילולי (המתורגם לתווים). אין לבלבל בין קוד תווי לבין סיסמה. הקוד התווי יכול לשמש לצורך התגברות על הגנת סיסמה, במובן של שמירה מפני גישה לא

37 שם.

38 JAMES A. LEWIS, DENISE E. ZHENG & WILLIAM A. CARTER, THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA 6 (CSIS Tech. Pol'y Program, 2017), https://bit.ly/3iHWdXc.

39 שם, בעמ׳ 9.

40 להרחבה בדבר הקושי של רשויות אכיפת החוק להתמודד עם הצפנה ראו J. Riley Atwood, *The Encryption Problem: Why the Courts and Technology are Creating a Mess for Law Enforcement*, 34 ST. LOUIS PUB. L. REV. 407, 424–427 (2015).

41 קיים קושי לאתר נתונים מדויקים בהקשר זה. סקר שנערך בקרב הציבור האמריקני בשנת 2014 מצא שכ־47% מהנשאלים השתמשו בסיסמת כניסה כדי להגן על המידע האגור במכשיר הטלפון הסלולרי שברשותם. כשליש מהנשאלים לא נקטו כלל טכניקות אבטחת מידע, והשאר (כ־20%) השתמשו בשיטות אחרות לאבטחת מידע, אשר חלקן לא רלוונטיות למאמר זה (כמו גיבוי תוכן המכשיר הסלולרי או התקנת תוכנת אנטי־וירוס). ראו *Smart Phone Thefts Rose to 3.1 Million in 2013 – Industry Solution Falls Short, While Legislative Efforts to Curb Theft Continue*, CONSUMER REP. (May 28, 2014), https://tinyurl.com/ybjfxc29.

42 SHARI TREWIN ET AL., BIOMETRIC AUTHENTICATION ON A MOBILE DEVICE: A STUDY OF USER EFFORT, ERROR AND TASK DISRUPTION (IBM) 6–7 (2012), https://ibm.co/2YtHTKV.

43 שיטה זו נפוצה יחסית בקרב מכשירי טלפון סלולרי המשתמשים במערכת הפעלה של אנדרואיד. הכוונה לסרטוט של קו מסוים על פני ״משטח״ של תשע נקודות.

מורשית למידע, וכן הוא יכול לשמש מפתח הצפנה המפענח את המידע המוצפן והופך אותו מלא קריא למחשב או לאדם – לקריא ולניתן לפיענוח ולעיבוד.

הדרך **השנייה** היא טביעת אצבע. טביעת אצבע נחשבת לרוב אמצעי חד־ערכי לזיהויו של אדם, שכמעט אינו ניתן לזיוף.[44] בטלפונים סלולריים רבים ובחלק מהמחשבים יכול המשתמש לבחור בטביעת האצבע שלו בתור מפתח להתגברות על נעילת המכשיר או הצפנתו. משמע, טביעת האצבע יכולה להיות הן סיסמת הכניסה והן מפתח ההצפנה. בטלפונים סלולריים משמשת טביעת אצבע אמצעי אבטחה נפוץ למן השימוש שעשתה בו חברת Apple במכשיר ה־iPhone 5s ואילך. טביעת אצבע נחשבת אמצעי אבטחה מצוין, שכן קשה להתגבר עליו בדרך של זיוף. עם זאת ניתן ליטול טביעת אצבע בכוח, שלא כסיסמה, שאותה לא ניתן ליטול מאדם, ועליו למסור אותה. הדין הישראלי מכיר במפורש בשימוש בכוח כדי ליטול מחשוד טביעת אצבע, הן בהקשרים של חיפוש חיצוני בגוף החשוד והן בהקשרים של טביעת אצבע כאמצעי זיהוי.[45] בית המשפט העליון התייחס בעבר לשימוש בכוח כדי ליטול מחשוד את טביעת האצבע שלו וסבר כי העניין אינו מעורר שאלות בהקשר של החיסיון מפני הפללה עצמית.[46] עם זאת הבחינה האמורה לא נעשתה בהקשר של שימוש בטביעת אצבע כדי לפצח הגנת סיסמה או הצפנה של מחשב, טלפון סלולרי או שירות מקוון.

הדרך **השלישית** להנגשת הסיסמה או מפתח ההצפנה למשתמשי הקצה במחשב, בטלפון סלולרי או בשירותים מקוונים היא זיהוי פנים. פניו של אדם הן אמצעי שלא ניתן לזיוף בידי אדם אחר.[47] העובדה שאדם אינו יכול לשנות בקלות את פניו היא הזדמנות של

44 עם זאת נשמעות 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. STAT. REV. 521 (2003).

45 הוראות חוק נטילת אמצעי זיהוי עוסקות בשתי דרכים אלה של משטרת ישראל לדלות את טביעות אצבעותיהם של חשודים בפלילים. סעיף 1 לחוק נטילת אמצעי זיהוי מגדיר נטילת טביעת אצבע כ״חיפוש חיצוני״, וסעיף 3(ב) לחוק זה מאפשר את ביצועו של חיפוש חיצוני כאמור בשימוש בכוח סביר. כמו כן, קריאה משותפת של סעיפים 11ז ו־11טז לחוק נטילת אמצעי זיהוי מאפשרת לטעון כי משטרת ישראל רשאית ליטול בכוח טביעת אצבע לשם הכנסתה למאגר טביעות האצבע המשטרתי, ולאחר מכן להשתמש במידע האגור במאגר לצורך חקירות פליליות.

46 בע״פ 663/81 **חורי נ׳ מדינת ישראל**, פ״ד לו(2) 85, פס׳ 4 לפסק דינו של השופט שמגר (1982) קבע בית המשפט העליון כי כאשר מבוצע חיפוש בגופו או על גופו של חשוד, אין בכך כדי לעורר שאלות של חיסיון מפני הפללה עצמית אלא שאלות של זכותו של הפרט לשלמות גופנית ולשמירת כבוד האדם (ובלשון בית המשפט: ״חיפוש – בין על גופו של אדם ובין על־ידי בדיקה אחרת בנסיבות שבהן מותר הדבר, בין חיצוני בעזרת העין הבלתי מזוינת בלבד ובין חיצוני בעזר אמצעי עזר טכנולוגיים לגילוי סימנים הסמויים מן העין, אינו פוגע, כמבואר לעיל, בזכות לאי־הפללה עצמית. האבחנה המקובלת אצלנו – ואשר, כאמור, איננה מעוגנת בזכות אי ההפללה העצמית אלא בזכותו של הפרט לשלמותו הגופנית ולשמירת כבודו כאדם״).

47 בסרט הפופולרי ״עימות חזיתי״ ((FACE/OFF (Paramount Pictures 1997), מוחלפות פניהם של ניקולס קייג׳, המגלם פושע מטורף, וג׳ון טרבולטה, המגלם סוכן FBI אשר מבקש ללכוד אותו, וסביבתם הקרובה של השניים סבורה כי כל אחד מהם הוא האחר. נכון להיום, מדובר בטכנולוגיה שהיא לא יותר ממדע בדיוני, אשר לא נראה שעתידה להתקיים בעתיד הנראה לעין. ניתוחים להשתלת פנים הם עדיין בתחילת דרכם, הם יקרים במיוחד ואינם מאפשרים ״החלפה״ של פנים עם אדם אחר, אלא לרוב השתלה

ממש במובני אבטחת מידע. טכניקה של זיהוי פנים מאפשרת לנעול את המכשיר באופן שרק לאחר התאמה בין פניו של האדם המתבונן במכשיר לבין פניו של בעל המכשיר כפי שהן אגורות במכשיר עצמו תהיה אפשרות גישה אל תכניו או אפשרות לפענח את ההצפנה.[48] מכשיר ה־iPhone X של חברת Apple הוא המכשיר הראשון בייצור המוני שהשתמש, כברירת מחדל, בטכניקת אבטחת מידע מסוג של זיהוי פנים. לטענת Apple, הסיכוי שאדם רנדומלי יצליח להתגבר על טכניקת אבטחה של זיהוי פנים רק בדרך של הסתכלות אל המכשיר היא אחד למיליון, שלא כסיכוי בכל הנוגע להתגברות אקראית על טביעת אצבע, שהוא אחד ל־50,000.[49] מבחינה טכנית, זיהוי הפנים נעשה בדרך של מדידת 30,000 נקודות בפניו של המתבונן במכשיר, הפיכת הנקודות הללו והמרחק ביניהן לפונקצייה מתמטית והשוואת התוצאה של הפונקצייה המתמטית לתוצאה האגורה במכשיר זה מכבר.[50] לשמירת המידע הביומטרי הזה של בעל המכשיר עשויות להיות, מטבע הדברים, השלכות על פרטיותו של המשתמש,[51] והן מחוץ לגדרי מאמר זה. עם זאת ברור שמדובר בטכניקה המקילה במידה ניכרת על בעל המכשיר ואינה מצריכה ממנו לזכור סיסמאות, שכן אין הוא נדרש אלא להביט אל המכשיר.

הדרך **הרביעית** היא דגימת קול. נכון להיום מעטים המכשירים שנעשה בהם שימוש בדגימת קול כאמצעי לאבטחת מידע, ונפוץ יותר השימוש בקול כדי להקל את חוויית המשתמש כאשר הוא אינו מסוגל או אינו מעוניין להשתמש בידיו בעת מתן פקודות למכשיר (למשל בשעת נהיגה). עם זאת חברות טכנולוגיה שונות החלו לבחון בשנים האחרונות אם ניתן להשתמש בדגימת קולו של בעל המכשיר כאמצעי לאבטחת המידע האגור במכשיר. על פי טכניקה זו, גלי הקול של אדם האומר מילת קוד מסוימת מתורגמים למעין תמונה ויזואלית הנשמרת על גבי המכשיר. בבואו של בעל המכשיר לנסות ולגשת אל המידע האגור במכשיר באמצעות אותה מילת קוד, תיווצר במכשיר ״תמונה ויזואלית״ חדשה של קולו, והיא תושווה לתמונה השמורה זה מכבר במכשיר. ״התמונה הוויזואלית״ מורכבת ממספר רב של מאפיינים כמו מבטא, קצב הדיבור, גובה הצליל וחיתוך הדיבור –

של תאי עור לאחר פציעות שרפה וכדומה. ראו למשל Ariana Eunjung Cha, *Groundbreaking Face Transplant: After a Firefighter was Injured on Duty, a Deceased 26-Year-Old Cyclist Gave Him His Life Back*, WASH. POST (Nov. 17, 2015), https://tinyurl.com/y3fjsvy3.

48 טכניקה זו קרויה, ביתר דיוק, ״השוואת פנים״ ולא ״זיהוי פנים״. השוואת פנים (Face Verification) היא טכניקה שבה מבוצעת השוואה בין פנים מסוימות המוצגות מול המכשיר לבין אותן פנים ספציפיות אשר אגורות במכשיר (השוואה מסוג של 1:1). לעומת זאת זיהוי פנים (Face Identification) היא טכניקה שבה מבוצעת השוואה בין פנים מסוימות לבין מאגר שלם של פנים שאגורות במכשיר, כדי לזהות למי שייכות הפנים המסוימות מתוך כלל הפנים אשר אגורות במכשיר (השוואה מסוג של 1:N). להרחבה בעניין זה ראו Andrea F. Abate et al., *2D and 3D Face Recognition: A Survey*, 28 PATTERN RECOGNITION LETTERS 1885 (2007). לשם הנוחות, נשתמש בביטוי ״זיהוי פנים״ כשם כולל לשתי טכניקות אלה.

49 APPLE, FACE ID SECURITY (2017), https://apple.co/3iHShWx.

50 שם. לפי חברת Apple, טכניקה זו מאפשרת לזהות גם ניסיונות להתגבר על אבטחת המכשיר באמצעות תמונה של בעל המכשיר והיא פועלת גם בחשכה מוחלטת.

51 לעניין זה ראו Yana Welinder, *A Face Tells More Than A Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J. L. & TECH. 165 (2012).

כל אלה יחדיו מרכיבים תמונה ויזואלית ייחודית שאינה ניתנת להתגברות באמצעות חיקוי קולו של בעל המכשיר.[52] המפתח הייחודי שנוצר בעת ההתאמה בין הדגימה השמורה במכשיר לבין הדגימה החדשה יכול להיות הן מפתח הצפנה והן סיסמה הדרושה לשם גישה אל התכנים האגורים במכשיר.

הדרך **החמישית** והאחרונה היא זיהוי דפוס השימוש במכשיר. לפי מיטב בדיקתנו, אין כיום מכשיר שמוטמעת בו טכניקה זו בפועל, ונכון לעת הזאת מדובר ברעיון תאורטי. טכניקה זו משתמשת בביומטריקה התנהגותית (Behavioral Biometrics) שמורכבת מדפוסי התנהגות מסוימים המאפיינים את האינטראקצייה שבין בעל המכשיר למכשיר, משמע המכשיר לומד את דפוסי השימוש של המשתמש ללא הרף, ולכן אדם שאינו המשתמש המוגדר לא יוכל להתגבר על אבטחת המכשיר. הדפוסים שאותם לומד המכשיר כוללים פרמטרים כמו עובי האצבע של המשתמש, עוצמת הלחיצה או זווית האחיזה של המכשיר ומאפיינים התנהגותיים ופיזיולוגיים נוספים שכמעט שאין אפשרות לצפות אותם מראש או לחקותם.[53] מנקודת מבט של חוויית השימוש במכשיר, אין ספק כי מדובר באמצעי המכביד פחות על המשתמש, שכן הוא אינו דורש ממנו להתאמץ ולזכור סיסמה או מפתח הצפנה או להתגבר על נעילה שהתרחשה בגלל הקשה שגויה של קוד תווי. נוסף על זה, ייתכן לומר שמדובר באמצעי הבטוח ביותר מכל החמישה משום שקשה לתאר דרך שבה אדם לא מורשה יהיה מסוגל לחקות או לזייף את דפוס ההתנהגות הספציפי של בעל המכשיר עם המכשיר.[54]

להלן נציג כמה מאפיינים המשותפים לחלק מהטכניקות שפירטנו לעיל או לכולן. למאפיינים אלה תהיה השפעה על בחינת השאלה של החלת החיסיון מפני הפללה עצמית כשמדובר בדרישה מהמשתמש, חשוד או עד, לנקוט פעולות על מנת להתגבר על סיסמה או על הצפנה של מחשב, טלפון סלולרי או שירות מקוון. **ראשית**, מדובר בטכניקות קלות לשימוש וידידותיות למשתמש הקצה. הסיבה לכך ברורה מאליה: אבטחת המידע במוצרים אלה נועדה להיות פשוטה להפעלה, שאם לא כן יהפכו מנגנוני ההגנה לעול לא סביר על משתמשי הקצה ולא יהיו בשימוש; **שנית**, מדובר בטכניקות שנועדו להיות זמינות, ולעיתים אף חינמיות. חלק מטכניקות האבטחה הנקוטות כיום, כמו קוד תווי, הצפנה (בחלק מהמקרים) וטביעת אצבע טבועות במכשיר הקצה ללא בחירה אקטיבית של המשתמש (Built-in).[55] גם כאשר הטכניקה אינה Built-in, מדובר לעיתים קרובות ביישומונים חינמיים (או בעלות זניחה) שניתנים להורדה מהאינטרנט; **שלישית**, וכפועל יוצא של שני המאפיינים הקודמים, השימוש בטכניקות הללו נפוץ מאוד. המשמעות הנורמטיבית של זמינותן של הטכניקות הללו היא שלא ניתן בהכרח להסיק מסקנות על ״פליליותו״ של המידע האגור

52 Julia Kollewe, *HSBC Rolls Out Voice and Touch ID Security for Bank Customers*, THE GUARDIAN (Feb. 19, 2016), https://tinyurl.com/hpvj6p8.

53 חברה ישראלית בשם Secured Touch פועלת בימים אלה לגייס משקיעים והון כדי להמשיך את פיתוח המוצר הראשוני הזה. ראו *About*, SECUREDTOUCH (last visited Oct. 6, 2021), www.securedtouch.com.

54 הילה חיימוביץ׳ ״הסטארטאפ הישראלי שרוצה לשים סוף לסיסמאות גייס 8 מיליון דולר״ **Geektime** (23.4.2018) https://tinyurl.com/bx94y54a.

55 ויסמונסקי **חקירה פלילית**, לעיל ה״ש 22, בעמ׳ 215.

במכשיר רק על בסיס השימוש עצמו בטכניקת אבטחת המידע. כאמור, טכניקות אלה נועדו לעיתים קרובות ליצור הגנה רצויה על פרטיותו של משתמש הקצה, ולכן לרוב לא יהיה אפשר להסיק מסקנות מרחיקות לכת מעצם השימוש בטכניקות אלה;[56] **רביעית**, אי־פיצוח של חלק מטכניקות אבטחת המידע עלול להוביל למחיקת המידע. כזכור, זה היה החשש שהיה בבסיס פעולותיו של ה־FBI בפרשת סן ברנרדינו. המחיקה האוטומטית עשויה להתרחש בתוך פרק זמן מסוים שבעל המכשיר הגדירו מראש או שעשויה להתרחש אוטומטית לאחר כמה ניסיונות כושלים להתגבר על אמצעי האבטחה שהותקן במכשיר. מאפיין זה, מטבע הדברים, תוחם בסד זמנים קשיח את רשויות אכיפת החוק בבואן לנסות ולהתגבר על אמצעי האבטחה; **חמישית**, לעיתים נדרשים משאבים אדירים, הן מבחינה כספית והן מבחינת משאבי זמן, כדי להתגבר על אמצעי האבטחה.[57] שילוב המאפיין הזה עם המאפיין הקודם מוביל למסקנה הבלתי נמנעת שלעיתים רשויות החקירה אינן מסוגלות להתגבר על אמצעי אבטחת מידע בפרק זמן סביר ובהקצאת משאבים סבירה; **שישית**, קצב התפתחותן של טכניקות אבטחת מידע חדשות הוא מהיר במיוחד. משמעותה של ההתפתחות הטכנולוגית המואצת הזאת היא שלא ניתן לייצר הסדרה משפטית תלוית־טכנולוגיה לטכניקות הללו, אלא יש לנקוט הסדרה משפטית הוליסטית וכוללת שתספק מענה הולם וראוי לכל הטכניקות הקיימות – ובעיקר לאלה שעדיין אינן קיימות.

ב. על החיסיון מפני הפללה עצמית ועל זכות השתיקה

עד כה הצגנו את הטכנולוגיות השונות המשמשות להגנת סיסמה או להצפנת מידע האגור בטלפון סלולרי, במחשב או בשירות מקוון. הראינו כי מחד גיסא מדובר בטכניקות נפוצות מאוד, ומאידך גיסא מדובר בטכנולוגיות מורכבות מאוד לפריצה, ולעיתים מדובר בטכנולוגיה שלא ניתן כלל להתגבר עליהן ללא שיתוף הפעולה של בעל המכשיר. בפרק זה נציג את הרקע התאורטי לחיסיון מפני הפללה עצמית, הן במישור העיוני והן בפירושו עד היום בבתי המשפט בישראל, כבסיס להמשך הדיון בדבר החלתו על המקרים של הגנת סיסמה או הצפנה במחשב, בטלפון סלולרי או בשירות מקוון. כמו כן נבקש לעמוד בפרק זה בקצרה על ההבחנה שבין החיסיון מפני הפללה עצמית לבין זכות השתיקה.

סעיף 47(א) ו־52 לפקודת הראיות [נוסח חדש], התשל״א–1971 קובעים יחד את העיקרון של חיסיון מפני הפללה עצמית בדין הישראלי, וזו לשונם:

> 47. (א) אין אדם חייב למסור ראיה אם יש בה הודיה בעובדה שהיא יסוד מיסודותיה של עבירה שהוא מואשם בה או עשוי להיות מואשם בה.

56 למעשה, יש שטענו כי שימוש יזום בטכניקות של הגנת סיסמה או הצפנה משפיע גם על דרך בחינת הציפייה הסבירה לפרטיות ומחייב את המסקנה שהמידע המוצפן / מוגן־סיסמה הוא מידע פרטי יותר מאשר מידע שלא מוגן בצורה דומה, ולכך השפעה דרמטית על שיקול הדעת השיפוטי בעת הוצאת צווי חיפוש בחומרי מחשב מוצפנים או מוגני־סיסמה. להרחבה בעניין זה ראו שם, בעמ׳ 257–258.

57 בהקשר זה ראו דברי ההסבר להצעת חוק החיפוש, בעמ׳ 633 (שם ההתייחסות למנגנוני אבטחת מידע כאלה ואחרים היא כאל מנגנונים ש״אינם ניתנים לפריצה״).

> 52. הוראות פרק זה יחולו הן על מסירת ראיות בפני בית משפט ובית דין והן על מסירתן בפני רשות, גוף או אדם המוסמכים על פי הדין לגבות ראיות;

החיסיון מפני הפללה עצמית חל כבר בשלב החקירה גם על בסיס סעיף 2(2) לפקודת הפרוצדורה הפלילית (עדות) (להלן: פקודת העדות), וזו לשונו:

> אדם, הנחקר כך, יהיה חייב להשיב נכונה על כל השאלות, שיציג לו בשעת החקירה אותו קצין משטרה, או קצין מורשה אחר כנ״ל, חוץ משאלות שהתשובות עליהן יהיה בהן כדי להעמידו בסכנת אשמה פלילית.

כפי שניתן לראות, סעיף 2(2) לפקודת העדות עוסק בשאלות המוצגות לנחקר במהלך החקירה, ואילו סעיפים 47 ו־52 לפקודת הראיות נוגעים גם למסמכים שהוא נדרש למסור.

העיקרון של אי־הפללה עצמית נקבע בשיטותיהן המשפטיות של מדינות רבות[58] ובמשפט הבין־לאומי.[59]

החיסיון מפני הפללה עצמית פורש כזכות יסוד של הפרט. עם זאת אין מדובר בזכות שההכרה בה היא טבעית ומובנת מאליה. אמרה המיוחסת לג׳רמי בנת׳האם, שידוע כמי שהתנגד לחיסיון מפני הפללה עצמית, גורסת כי החיסיון מסייע בראש ובראשונה לאשמים ולא לחפים מפשע.[60] סקירה היסטורית של התפתחות החיסיון מצביעה על התפתחות כמעט

58 בדין האנגלי הפך החיסיון מפני הפללה עצמית לנפוץ החל מאמצע המאה השבע־עשרה, והשתרש כחלק בלתי נפרד מהמשפט המקובל בשנים שלאחר מכן. להרחבה ראו John H. Langbei, *The Historical Origins of the Privilege against Self-Incrimination at Common Law*, 92 MICHIGAN L. REV. 1047 (1994). בדין האמריקני בוסס החיסיון מפני הפללה עצמית בתיקון החמישי לחוקה האמריקנית. שם נקבע כך: ראו U.S. CONST. amend. V, "No person shall [...] be compelled in any criminal case to be a witness against himself". בדין הקנדי ראו Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c 11, § 11 (U.K.). בדין הניו זילנדי ראו Evidence Act 2006, s 60 (N.Z.). בדין הגרמני, להסדרה של זכות השתיקה בקוד הפרוצדורה הפלילית, ראו STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE] §136, https://tinyurl.com/3tzzuvew (Ger.).

59 ראו ס׳ 14(3)(ז) לאמנה בינלאומית בדבר זכויות אזרחיות ומדיניות, כ״א 31, 169 (נפתחה לחתימה ב־1966) הקובע כך: ״כל אדם שהואשם בעבירה פלילית זכאי, תוך שוויון גמור, לערבויות מינימום אלו: [...] כי לא יכפו עליו להעיד נגד עצמו או להודות באשמה״. בדין האירופי ראו European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 6, Nov. 4, 1950, 213 U.N.T.S. 222, *entered into force* Sep. 3, 1953. אומנם הסעיף שכותרתו "Fair Trial" אינו מונה את הזכות לאי־הפללה עצמית ישירות, אך בעניין *Murray* קבע בית הדין האירופי לזכויות אדם במפורש כי: "There can be no doubt that the right to remain silent under police questioning and the privilege against self-incrimination are generally recognized international standards which lie at the heart of the notion of a fair procedure under Article 6" (ראו Murray v. United Kingdom, App. No. 18731/91, Eur. (Ct. H.R., §45 (1996)).

60 לציטוט של הדברים ראו Ian Dennis, *Instrumental Protection, Human Rights or Functional Necessity? Reassessing the Privilege against Self-Incrimination*, 54 CAMBRIDGE L.J. 342, 342 (1995) ("If all the criminals of every class had assembled and framed a system after their own wishes, is not this rule the very first they would have established for their security? Innocence

קזואיסטית, שמקורה בפרקטיקה של בתי המשפט הכנסייתיים באנגלייה לחקור אדם בשבועה על מעשים שלא ידוע כלל אם בוצעו, ואין כל חשד שבוצעו בידי האדם הנחקר.[61]

נעבור עתה להתבונן על זהות השתיקה. נהוג לתפוס את זכות השתיקה ככזו אשר פותחה כדי להגן הגנה רחבה ככל הניתן על החיסיון מפני הפללה עצמית של חשודים ונאשמים. עם זאת כפי שנראה להלן, זכות השתיקה מצומצמת בהיקפה מבחינת סוג התכנים שעליהם היא חלה (אמרה או יצירת מסמך) ומבחינת זהות הנחקרים שעליהם היא חלה (חשודים או נאשמים בלבד).

בחקיקה הישראלית הוענקה זכות השתיקה במפורש לנאשם במשפטו בלבד,[62] אך הפסיקה הרחיבה את זכות השתיקה שתחול אף לפני כן – בשלב חקירת רשויות החקירה את החשוד.[63] בית המשפט העליון קבע כי הטעמים העיקריים להרחבה זו של זכות השתיקה גם לשלב החקירה הם להגן על החשוד מפני התנהגות לא ראויה של חוקריו, למנוע גביית הודאות שווא, להימנע מהטלת חובות עשה על הפרט ושהחשוד לא יסתכן באמירת דברים אשר בשלב החקירה לא נראו לו מפלילים, אך בדיעבד הפלילו אותו.[64] זכות השתיקה אפוא נועדה לאפשר לחשוד ולנאשם להימנע מלטעות ולהשיב בשגגה על שאלות העשויות להפליל אותו בהמשך אף מבלי שידוע לו כיצד תפללנה אותו התשובות. במובן זה היא רחבה מהחיסיון מפני הפללה עצמית, אשר מאפשר לנחקר שלא להשיב רק על שאלות שהוא יודע כי הן עשויות להפלילו.

כמו כן, שלא כחשוד, על נחקר שאינו חשוד חלה החובה לשתף פעולה עם רשויות החקירה. למשל, ראינו כי סעיף 2(2) רישה לפקודת העדות מטיל חובה פוזיטיבית על אדם הנחקר במשטרה להשיב דברי אמת על שאלות החוקר. נוסף על זה, סעיף 5 לפקודת בזיון בית משפט קובע כי ניתן להטיל על עד המסרב להעיד, ללא טעם צודק לסירובו, עונש מאסר, עד שישוב וישתף פעולה. סירוב לציית לצו שיפוטי המחייב למשל המצאה של מידע מסוים – עשוי לגרור עונש מאסר או קנס, לפי סעיף 6(1) לפקודת בזיון בית המשפט.[65]

חובה זו של שיתוף פעולה עם רשויות החקירה מגולמת בהוראות חוק נוספות בדין הישראלי. למשל סעיף 45 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש],

never takes advantage of it. Innocence claims the right of speaking as guilt invokes the privilege of silence").

61 לסקירה על התפתחותו ההיסטורית של החיסיון מפני הפללה עצמית ראו עמנואל גרוס ״החסיון מפני הפללה עצמית – האמנם ציון דרך במאבקו של האדם הנאור לקידמה?״ **מחקרי משפט** ז 167, 168–172 (התשמ״ט). לפי גרוס, במהלך משפטו של אדם בשם Lilburn בשנת 1637, העלה הנאשם לראשונה את הטענה שאין הוא מחויב להשיב על שאלות שהטיחו בו השופטים, כאשר כל מטרתן ״לסחוט״ ממנו הודאה על מעשים כאלה ואחרים, שלא בגינם נעצר ונחשד מלכתחילה.

62 ס׳ 161(א)(2) לחסד״פ.

63 רע״א 5381/91 **חוגלה שיווק (1982) בע״מ נ׳ אריאל**, פ״ד מו(3) 378, פס׳ 4 לפסק דינו של השופט (כתוארו אז) מצא (1992).

64 ע״פ 196/85 **זילברברג נ׳ מדינת ישראל**, פ״ד מד(4) 485, פס׳ 4 לפסק דינו של השופט לוין (1990).

65 לפי סעיף 6(2) לפקודת בזיון בית משפט, אם האדם הממרה את הצו השיפוטי יספק טעם סביר לסירובו, בית המשפט עשוי להימנע מנקיטת סנקצייה של מאסר או קנס נגדו. מובן כי הכרה של בית המשפט בקיומו של חיסיון מפני הפללה עצמית (ככל חיסיון אחר) תשמש טעם סביר ולגיטימי לסירוב לציית לצו.

התשכ״ט–1969 (להלן: פסד״פ) קובע כי אדם הגר במקום שמותר לרשות חוקרת להיכנס אליו חייב לאפשר כניסה חופשית ולהעניק לרשות החוקרת ״כל הקלה סבירה״; סעיף 241 לחוק העונשין, התשל״ז–1977 קובע עונש מאסר של שנתיים על מי שחלה עליו החובה להעיד או למסור ראיה והוא מסרב לעשות זאת; סעיף 244 לחוק העונשין קובע עונש מאסר של שלוש שנים לאדם העושה כל פעולה שמטרתה למנוע או להכשיל הליך חקירתי או שיפוטי.

עינינו הרואות כי על כל אדם שאינו חשוד מוטלות חובות עשה של שיתוף פעולה עם רשויות החקירה ואכיפת הדין הפלילי, ואילו חשוד בפלילים ונאשם פטורים מחובה זו בשל החיסיון מפני הפללה עצמית ובשל זכות השתיקה.

מהן אפוא ההצדקות להכרה בזכות השתיקה ובחיסיון מפני הפללה עצמית? נמנה להלן את ההצדקות העיקריות שבבסיס שני מושגים אלה. עמנואל גרוס מנה שבעה טעמים לחיסיון מפני הפללה עצמית אגב מתיחת ביקורת על הטעמים הללו:[66] **ראשית**, הימנעות מהעמדת הנחקר בפני טרילמה מוסרית (שתפורט בהמשך); **שנית**, העדפת השיטה האדוורסרית על פני השיטה האינקוויזיטורית; **שלישית**, החשש כי הודאות מפלילות יושגו באמצעים לא אנושיים; **רביעית**, תחושה פנימית שלפיה לא הגון שאדם יפליל את עצמו; **חמישית**, זכותו של החשוד לפרטיות; **שישית**, חוסר אמון מובנה בהודאות מפלילות; **שביעית**, הכרה בכך שהחיסיון אומנם מגן על האשמים, אך בכך מגן לעיתים גם על החפים מפשע. גם רונלד אלן (Allen) מנה כמה טעמים לחיסיון מפני הפללה עצמית, במותחו ביקורת על האופן שבו הם משמשים לשם הצדקת קיומו של החיסיון:[67] **ראשית**, החיסיון מגן על הפרט מפני הטרילמה המוסרית (כאמור, נפרט על אודותיה בהמשך); **שנית**, שמירה על יחסי כוחות הוגנים בין רשויות החקירה לבין הפרט; **שלישית**, החיסיון יפחית את הסיכוי להודאות שווא; **רביעית**, החיסיון מונע שימוש בנחקר ככלי להפללתו.

בכל הנוגע לזכות השתיקה, הרנון מנה שני טעמים עיקריים המצדיקים אותה: **ראשית**, היא מאפשרת להימנע מהפעלת אמצעים לא הוגנים ולא חוקיים כלפי הנחקר; **שנית**, הזכות מגינה על פרטיותם של הנחקרים, אשר אינם מחויבים לחלוק עם הרשות החוקרת פרטים על חייהם האישיים.[68]

לטעמנו, ניתן להכליל את ההצדקות שנמנו לעיל בשלוש הצדקות עיקריות: **האחת**, תמרוץ רשויות החקירה לפעול באורח מסוים (הצדקה בעלת היגיון כלכלי); **השנייה**, מתן ביטוי לזכותו של החשוד לפרטיות ולאוטונומיה (הצדקה הנובעת מטעמים אינטרינזיים); **השלישית**, פתרון לטרילמה המוסרית (טעם לוגי במהותו). נרחיב להלן על הצדקות אלה.

לפי ההצדקה **הראשונה**, בעלת הרציונל הכלכלי, זכות השתיקה והחיסיון מפני הפללה עצמית נועדו ליצור תמריץ בקרב רשויות החקירה לפעול להשגת ראיות שהן חיצוניות לחשוד עצמו. רבות נכתב על חתירתן של רשויות החקירה להשגת הודאה מפיו של החשוד,

66 גרוס, לעיל ה״ש 61, בעמ׳ 173–181.

67 Ronald J. Allen, *Theorizing about Self-incrimination*, 30 CARDOZO L. REV. 729, 731 (2008).

68 אליהו הרנון ״על זכות השתיקה״ **משפטים** א 95, 105–111 (1967).

שהוגדרה לא פעם – "מלכת הראיות".[69] בלשונו של השופט דנציגר: "בהודאה טמון כוח שכנוע כה רב עד כי קשה שלא לקבלה. הנטייה האינטואיטיבית היא להאמין לאדם המעיד נגד עצמו, שהרי מדוע ייטול על עצמו אחריות למעשה שלא ביצע, בניגוד לאינטרס שלו עצמו".[70] בכוחה הרב של ההודאה טמונה גם חולשתה הגדולה, ולא פעם מוזכר החשש מפני הודאות שווא, ובעקבותיהן הרשעות שווא, במערכת המשפט הישראלית.[71] בשל החשש מהודאות שווא – וכפועל יוצא שלהן מהרשעות שווא – מבקשת מערכת המשפט ליצור תמריץ בקרב רשויות החקירה לפעול לחיפוש ראיות שהן חיצוניות לחשוד עצמו.[72] התמריצים שנועדו למנוע את הודאות השווא כוללים הן את הדרישה הראייתית ל"דבר מה נוסף" כדי להרשיע אדם על בסיס הודאת חוץ שלו,[73] והן את זכות השתיקה והחיסיון מפני הפללה עצמית. לפי הצדקה זו, לולא הזכות והחיסיון היו רשויות החקירה מתמקדות אך ורק בהשגת הודאה מפיו של הנאשם. זכות השתיקה והחיסיון מפני הפללה עצמית מונעים מהרשויות את הסמכות לדרוש מהחשוד להודות במעשיו, ובכך יוצרים לרשויות החקירה תמריץ להשיג ראיות נוספות, החיצוניות לחשוד עצמו.

לפי ההצדקה **השנייה**, זכות השתיקה והחיסיון מפני הפללה עצמית נובעים מזכותו של הנחקר לפרטיות. הזכות לפרטיות, שהיא כידוע בעלת מעמד חוקתי,[74] היא חלק מיסודות אישיותו של האדם. ניתן להתבונן על הזכות לפרטיות כזכות המגדירה את יכולתו של אדם לשלוט ב"זרימת המידע" (flow of information) על אודותיו.[75] לפי גישה זו, ידיעותיו של אדם זר על כל מחשבה ומחשבה של הפרט עלולה להסב פגיעה ממשית לאישיותו. מסיבה זו ראוי לשלול מגורם זר את האפשרות לגשת בחופשיות לכל פרט מידע על אדם אחר. זכות השתיקה והחיסיון מפני הפללה עצמית יוצרים חסם מפני גישה של גורם זר אל המידע

69 דנ"פ 4342/97 **מדינת ישראל נ' אל עביד**, פ"ד נא(1) 736, פס' 10 לפסק דינו של השופט (כתוארו אז) חשין (1998).

70 ע"פ 7939/10 **זדורוב נ' מדינת ישראל**, פס' 127 לפסק דינו של השופט דנציגר (נבו 23.12.2015).

71 ראו למשל דליה דורנר "מלכת הראיות נ' טארק נוג'ידאת – על הסכנה שבהודאת שווא ועל הדרך להתמודד עמה" **הפרקליט** מט 7 (2006); חגית לרנאו "הודאות שווא והרשעות שווא" **עלי משפט** יא 351 (2014); בועז סנג'רו "ההודאה כבסיס להרשעה – האומנם 'מלכת הראיות' או שמא קיסרית הרשעות השווא" **עלי משפט** ד 245 (2005).

72 בני שטיינברג "מה נותר מן האזהרה על זכות השתיקה?" **הפרקליט** מח 163, 168–169 (2004).

73 הדרישה הראייתית ל"דבר מה נוסף" נקבעה לראשונה במשפט הישראלי בע"פ 3/49 **אנדלרסקי נ' היועץ המשפטי לממשלה**, פ"ד ב 589 (1949). להרחבה ראו אהוד קמר "דבר־מה נוסף מפי הנאשם" **פלילים** ה 277 (1996). כן ראו הועדה לענין הרשעה על סמך הודאה בלבד ולענין העילות למשפט חוזר **דין וחשבון** (1994) (המכונה גם "ועדת גולדברג"). ועדת גולדברג הציעה כי תידרש תוספת ראייתית להודאת חוץ של נאשם, וטיבה של התוספת – בין סיוע, בין דבר לחיזוק ובין דבר־מה נוסף – ייקבע לפי נסיבותיו הקונקרטיות של המקרה הנתון, ובלבד שיש בה כדי להסיר ספק סביר בדבר אמינותה של האמרה בכל הנוגע לביצוע העבירה (שם, בעמ' 20–22). יוער כי פרופ' מרדכי קרמניצר הביע דעת מיעוט בעניין זה, וסבר כי יש לקבוע תוספת ראייתית מסוג סיוע בכל מקרה של הודאת חוץ של נאשם (שם, בעמ' 64–66).

74 ראו ס' 7(א) לחוק־יסוד: כבוד האדם וחירותו (הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"). הזכות לפרטיות מוכרת כזכות יסוד גם בדברי חקיקה שנחקקו לפני חוק היסוד. ראו בג"ץ 8070/98 **האגודה לזכויות האזרח בישראל נ' משרד הפנים**, פ"ד נח(4) 842 (2004).

75 בירנהק, לעיל ה"ש 21, בעמ' 89–108.

האישי של האדם, במקרה זה הנחקר.[76] בעולם ללא הזכות והחיסיון יהיה אפשר לכפות בכל מקרה על האדם למסור מידע על עצמו ובכך לאבד את שליטתו במידע.[77] עוד ניתן לטעון כי ההפללה העצמית טומנת בחובה גם את ההכרה ברע ולעיתים אף את ההכאה על חטא מצד החשוד. כל אלה הם מידע פרטי במיוחד השמור ליחסים שבין אדם למצפונו.[78]

עוד ברוח הצדקה זו, אם כי מכיוון מעט שונה, ניתן להתבונן על זכות השתיקה והחיסיון מפני הפללה עצמית מכיוון של תפיסה פוליטית־ליברלית המדגישה את היחידה האוטונומית של הפרט אל מול הממשל. לפי תפיסה זו, בבוא הממשל להאשים אדם בעבירה פלילית, עליו להשתמש בכוחו ובמשאביו כדי להוכיח את החשדות, ללא עזרת הנחקר. לא ראוי שהפרט יידרש לשתף פעולה עם הכוח שמופעל נגדו. לפיכך הזכות והחיסיון מבטיחים יחסים פוליטיים תקינים בין הפרט לבין ממשלו.[79]

ההצדקה **השלישית** לזכות השתיקה והחיסיון מפני הפללה עצמית – ההצדקה ה״לוגית״ – היא ההגנה על החשוד מפני ״הטרילמה המוסרית״. בעולם ללא זכות השתיקה והחיסיון מפני הפללה עצמית יעמוד החשוד־האשם בעת חקירתו בפני שלוש אפשרויות, כל אחת מהן גרועה מרעותיה: האפשרות **הראשונה** היא לשקר לחוקריו. יש הגורסים כי נטייתו הטבעית של האדם לנסות ולחמוק מענישה תוביל אותו מדרך הטבע לממש אפשרות זו ובכך להטעות פוזיטיבית את חוקריו; האפשרות **השנייה** היא לומר אמת לחוקריו, ובכך להביא על עצמו ענישה, לעיתים מחמירה; האפשרות **השלישית** היא לשתוק, ובכך להוביל את חוקריו למסקנה שהוא האשם בביצוע העבירה.[80] ביקורתו של בנת׳האם שהוזכרה לעיל[81] מתחדדת בכל הנוגע להצדקה זו, שכן אדם חף מפשע לא יחשוש כלל ממענה לשאלות חוקריו, ואילו אדם אשם יעמוד בפני ״הטרילמה האכזרית״, כלשונו של בנת׳האם.[82] ניתן לטעון כי אין כל הצדקה מוסרית של ממש התומכת בדרישתו של חשוד־אשם כי החברה תימנע מלהעמידו בפני הטרילמה המוסרית האמורה.[83] מנגד, ניתן לטעון כי ההגנה על החשודים־האשמים מפני הטרילמה המוסרית מביאה להחצנות חיוביות גם על אותם חשודים־חפים מפשע. לפי טיעון זה, במקרים שבהם הראיות שמחזיקה המדינה הן בעוצמה בינונית (לעומת עוצמה חלשה או עוצמה חזקה), יבחר החשוד־האשם לשמור על זכות השתיקה, ואילו החשודים־החפים מפשע יבחרו למסור את גרסתם

76 לטיעון ברוח הצדקה זו ראו D.J. Galligan, *The Right to Silence Reconsidered*, 41 CURRENT LEGAL PROBLEMS 69, 88–89 (1988).

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

78 שם, בעמ׳ 90.

79 Dennis, לעיל ה״ש 60, בעמ׳ 353–354. הטלת חובות מוגברות על המדינה־התביעה ביחסיה עם הפרט־החשוד מתיישבת גם עם ההימנעות, ככלל, מהטלת חובות עשה על הפרט במסגרת ההליך הפלילי. הדבר נכון במיוחד כאשר חובות העשה המוטלות על הפרט דורשות ממנו לוותר על האוטונומיה שלו, ובתוך כך לגזור על עצמו ענישה. לטיעון זה ראו דוד ליבאי ״חקירת חשוד והחיסיון מהפללה עצמית״ **הפרקליט** כט 92, 98–99 (1973).

80 Dennis, לעיל ה״ש 60, בעמ׳ 358–359.

81 שם.

82 שם.

83 Allen, לעיל ה״ש 67.

לחוקריהם.[84] טיעון זה מתבסס על הנחה שהתמונה הראייתית נהירה בשלב זה לחשוד, אולם פערי המידע בין החוקר לחשוד הנחקר הם חלק אינטגרלי משלב החקירה, ועל כן יכולתו של החשוד להבין את עוצמת החשדות נגדו בשלב זה היא מוגבלת.

קיומן של הצדקות אלה לחיסיון מפני הפללה עצמית ואף לזכות השתיקה אינו מחייב פרשנות שלפיה הזכות והחיסיון הם מוחלטים. על פני הדברים נראה כי מתוך הצדקות אלה ממש יכולה לקום גם תפיסה המכירה בזכות השתיקה ובחיסיון מפני הפללה עצמית, אך בסיוגן אל מול אינטרסים אחרים. לפי ההצדקה **הראשונה**, אכן אפשר ליצור תמריץ לרשויות אכיפת החוק לפעול להשגת ראיות שהן חיצוניות לחשוד עצמו גם כאשר זכות השתיקה והחיסיון מפני הפללה עצמית יפורשו כזכות וכחיסיון יחסיים. אומנם תמריץ זה יהיה חלש במעט מן התמריץ הקיים במקום שבו הזכות והחיסיון מפורשים כמוחלטים, אולם אין ספק כי גם זכות וחיסיון יחסיים מחייבים את רשויות אכיפת החוק להתחשב בקיומם, לגבש טיעון מבוסס בדבר המקרים שבהם ראוי להסירם ולנסות לשכנע את בית המשפט בצדקת הטיעון של הרשות החוקרת. לפי ההצדקה **השנייה**, המבוססת על זכותו של הנחקר לפרטיות – אף היא אינה מחייבת פרשנות שלפיה זכות השתיקה והחיסיון מפני הפללה עצמית הם מוחלטים. כידוע, הזכות לפרטיות אינה זכות מוחלטת,[85] ולפיכך הטלת חובה על אדם לוותר על השליטה במידע עליו יכולה לעיתים להיות מוצדקת, כאשר יעמוד אינטרס לגיטימי מנגד.[86] לפי ההצדקה **השלישית**, אכן אי־הכרה בזכות השתיקה או בחיסיון מפני הפללה עצמית (או הכרה חלקית בהם) עלולה להעמיד בפני הנחקר ״טרילמה מוסרית״ קשה. עם זאת עצם קיומה של הטרילמה אינו מחייב בהכרח שבכל מצב אפשרי יהיה לא ראוי או לא צודק להעמידה בפני הנחקר. ניתן אפוא, על סמך ההצדקות שמנינו לעיל, לבסס טיעון כי זכות השתיקה והחיסיון מפני הפללה עצמית הם יחסיים. ואכן, כפי שנראה בהמשך המאמר, בחקיקה ובפסיקה הישראלית ניתן לאתר ״ניצני הכרה״ בכך שהחיסיון מפני הפללה עצמית הוא יחסי. ההקשר הטכנולוגי שבבסיס דיוננו במאמר זה מחדד את המסקנה האמורה. לעומת החיסיון מפני הפללה עצמית, זכות השתיקה פורשה עד היום בפסיקת בתי המשפט בישראל כזכות מוחלטת, אשר אין לסייגה למול אינטרסים וזכויות אחרים.[87] נפרט

84 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, 467–470 (2000).

85 לעניין יחסיותה של הזכות לפרטיות, ראו למשל את בג״ץ 3809/08 **האגודה לזכויות האזרח בישראל נ׳ משטרת ישראל** (נבו 28.5.2012). באותו עניין קבע בית המשפט העליון כי חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס״ח–2007 הוא חוקתי חרף פגיעתו בזכות לפרטיות, בשל צורכי החקירה המצדיקים את הפגיעה המגולמת בו, לפי המגבלות והתנאים שנקבעו בחוק.

86 בהקשר זה יצוין כי עמנואל גרוס (לעיל ה״ש 61, בעמ׳ 178–179) טען שיש להימנע מהעלאת טענות ברוח הזכות לפרטיות שמשמעותן המעשית תהיה הענקת זכות של אדם ״לפינה משלו שם יוכל, באין מפריע, לעבור עברות״.

87 עניין **חוגלה**, לעיל ה״ש 63, פס׳ 4 לפסק דינו של השופט (כתוארו אז) מצא. באותו עניין נקבע כי ״זכות השתיקה הינה הביטוי המובהק ביותר לחיסיון מפני הפללה עצמית. בצורתה ה׳מוחלטת׳ – שלא לפצות פה ולא לומר דבר – הוענקה זכות השתיקה על־ידי המחוקק, במפורש, רק לנאשם במסגרת משפטו [...] החיסיון מפני הפללה עצמית, במסגרתה של חקירה, מקנה אך זכות שתיקה ״יחסית׳, דהיינו זכות שלא להשיב על שאלות מפלילות. אך כשהמדובר בחשוד בביצוע עבירה, הנחקר בידי איש מרות, מתפרש גם חיסיון זה, על דרך ההרחבה, כזכות שתיקה מוחלטת״.

על כך עוד להלן בפרק ד כשנציג את המודל המוצע להתמודדות עם סיסמאות ומפתחות הצפנה למחשבים, לטלפונים סלולריים ולשירותים מקוונים.

מן הרמה העיונית אל הרמה המעשית. נציג כעת כיצד מוחלים זכות השתיקה והחיסיון מפני הפללה עצמית במשפט הישראלי. בית המשפט העליון עסק כמה פעמים בשאלה אם החיסיון מפני הפללה עצמית חל רק על שאלות שנשאל הנחקר במהלך חקירותיו באזהרה, או שמא החיסיון חל גם על חובתו של הנחקר למסור מסמכים בכתב או ראיות פיזיות אחרות. בעניין **חורי** קבע בית המשפט העליון כך בעניין החיסיון מפני הפללה עצמית:

> הזכות לאי־הפללה עצמית משמעותה [...] כי אין כופין על אדם להעיד נגד עצמו או לספק לרשויות המדינה נגד רצונו ראיה **בדרך הדומה למסירתה או להעברתה של עדות** [...] הזכות לאי־הפללה עצמית איננה אלא תמציתו של הכלל [...] ואשר לפיו **איש אינו חייב להשיב על שאלה**, אם התשובה לשאלה עלול להיות בה, לדעת בית המשפט, כדי להניח את היסוד להבאתו לדין פלילי של מי שמשיב את התשובה. זכות זו מתייחסת גם לדרישה להצגתם של מסמכים ומטלטלים אחרים.[88]

בעניין **שרון**, אשר יפורט עליו בהרחבה בהמשך המאמר, עסק בית המשפט העליון בשאלת תחולתו של החיסיון מפני הפללה עצמית או זכות השתיקה על חובת החשוד להמציא מסמכים מכוח צו שיפוטי.[89] באותו עניין עמד השופט אור על הטעמים להקנייתה של זכות שתיקה מוחלטת לחשוד, ואלה הם: הזכות מגינה על החשוד מפני התנהגות לא הולמת של חוקריו; הזכות מגינה על מערכת המשפט מפני הודאות שווא; הזכות מונעת הטלת חובת עשה על החשוד; הזכות מתיישבת עם ההליך האדוורסרי שבו על התביעה לגייס את הראיות, ולא על הנאשם לספקן.[90]

בהמשך בחן השופט אור אם טעמים אלה מתקיימים בכל הנוגע להטלת חובה להמצאת מסמכים על החשוד וקבע כי הם אינם מתקיימים. החשש מפני התנהגות לא הולמת של רשויות החקירה אינו קיים משום שבעת קבלת צו להמצאת מסמכים יש לחשוד פנאי להתייעץ עם עורך דינו ולנסות לפעול לביטול הצו. כמו כן מדובר בראיות ״אובייקטיביות, בנות־קיימא, ולא בראיות באופי של עדות״, ולכן קיים חשש מופחת כי חוקרי המשטרה (ושאר רשויות החקירה) ינקטו אמצעים פסולים כדי להגיע אל הראיות.[91] בכל הנוגע לחשש מפני הודאת שווא קבע השופט אור כי ״החשוד אינו נדרש ליצור את הראיה בעצמו, אלא להמציא מסמכים שנוצרו בעבר ואשר קיימים ברשותו. לגבי מסמכים כאלה יכולתו למסור ראיות שקריות קטנה בהרבה במסמכים לעומת עדות בעל־פה״.[92] הנמקה דומה הושמעה מפיו של השופט אור גם בכל הנוגע לחשש מפני הטלת חובות עשה על החשוד, שכן ״שלא כמו העדות, מסירת המסמכים אינה דורשת מן הנחקר ליצור, באופן אקטיבי, את הראיות

88 עניין **חורי**, לעיל ה״ש 46, פס׳ 4 לפסק דינו של השופט שמגר (ההדגשות הוספו).
89 רע״פ 8600/03 **מדינת ישראל נ׳ שרון**, פ״ד נח(1) 748 (2003).
90 שם, פס׳ 9 לפסק דינו של השופט אור.
91 שם, פס׳ 10.
92 שם, פס׳ 11.

המבוקשות לדרישת חוקריו, אלא אך להמציא לידיהם ראיות שנוצרו בעבר ואשר קיימות ברשותו״ והוסיף כי ״למעשה, המצאת מסמכים בהתאם לצו דומה לחיפוש המתבצע בחצריו של אדם יותר מלמסירת עדות בעל־פה״.[93]

על בסיס האמור קבע בית המשפט העליון בעניין **שרון** כי זכות השתיקה לא חלה על המצאת מסמכים **קיימים** מידי החשוד לידי הרשות החוקרת, בניגוד לייצור מסמכים **חדשים** לפי דרישת הרשות החוקרת, שאז תקום לחשוד זכות השתיקה. לצד זאת נפסק כי על מסמכים חל החיסיון מפני הפללה עצמית, וכי במקרים שבהם נשמעת טענה לחיסיון כאמור, יבחן בית המשפט את המסמכים ויחליט אם אין חשש להפללת החשוד – ואז יחויב החשוד למוסרם – או שיש חשש להפללת החשוד – ואז ישקול בית המשפט להעניק לחשוד ״חיסיון שימוש״.[94] חיסיון שימוש, אשר מבוסס על פרשנות בית המשפט העליון לסעיף 47(ב) לפקודת הראיות,[95] משמעו כי יוסר מהמסמכים החיסיון מפני הפללה עצמית, ״אך יובטח לחשוד כי מסמכים אלה לא ישמשו כראיה נגדו בהליכים משפטיים בעתיד״.[96]

לעומת המצאת מסמכים בידי החשוד שבעניינם לא קמה לחשוד זכות השתיקה קבעו בתי המשפט כי ניתן לדרוש מחשוד להשתתף במסדר זיהוי, וכי הימנעותו מהשתתפות תשמש חיזוק לראיות התביעה. בית המשפט העליון קבע כי דרישה מחשוד להשתתף במסדר זיהוי כאמור והסנקצייה הראייתית בצד סירובו להשתתף אינן בבחינת הפרה של זכותו לאי־הפללה עצמית.[97] מדוע חיובו של אדם להשתתף במסדר זיהוי אינו פוגע בזכות השתיקה ובחיסיון מפני הפללה עצמית, ואילו מסירת עדות או מסמכים עולה כדי פגיעה שכזו? הסבר אפשרי לכך הוא ההבדל שבין ״פעולה אקטיבית״ של החשוד לבין הצורך בעדותו של אדם נוסף לשם הפללת החשוד בעזרת הראיה שנמסרה.[98] זו גם הסיבה לכך שחיפוש בביתו של אדם או בכליו אינו מעורר את השאלה של זכות השתיקה והחיסיון מפני הפללה עצמית – הפללה זו איננה ״עצמית״. לעומת זאת ההשתתפות במסדר זיהוי, בדומה למסירה של דוגמת כתב יד,[99] הן כולן פעולות ניטרליות שאינן מעידות כשלעצמן על הקשר שבין החשוד לבין העבירה. לכן נקבע כי דרישה מהחשוד להשתתף בהן והמחיר הראייתי של חיזוק לראיות התביעה במקרה של סירובו לכך – אינם פוגעים בזכות השתיקה ובחיסיון מפני הפללה עצמית. לשם הוכחת קשר בין החשוד לבין הפעולה הניטרלית שבה הוא

93 שם, פס׳ 12.

94 שם, פס׳ 17–18.

95 בג״ץ 6319/95 **חכמי נ׳ שופטת בית־משפט השלום בתל־אביב־יפו**, פ״ד נא(3) 750, פס׳ 12 לפסק דינה של השופטת שטרסברג־כהן (1997).

96 עניין **שרון**, לעיל ה״ש 89, פס׳ 18 לפסק דינו של השופט אור.

97 ע״פ 648/77 **קריב נ׳ מדינת ישראל**, פ״ד לב(2) 729, פס׳ 5 לפסק דינו של השופט שמגר (1978). באותו העניין אף צוטטה פסיקתו של בית המשפט העליון בארצות הברית בעניין United States v. Wade, 388 U.S. 218, 221 (1967): “Neither the lineup itself nor anything shown by this record that Wade was required to do in the lineup violated his privilege against self-incrimination. We have only recently reaffirmed that the privilege ‘protects an accused only from being compelled to testify against himself or otherwise provide the State with evidence of a testimonial or communicative nature’”.

98 עמנואל גרוס (לעיל ה״ש 61, בעמ׳ 183) תמך בהבחנה זו.

99 ע״פ (מחוזי ת״א) 70996/05 **עם דוד נ׳ מדינת ישראל**, פס׳ 44 (נבו 8.3.2006).

נדרשת להשתתף יש צורך בעדותו של אדם נוסף – עד ראייה או עד מומחה – אשר יעיד על הקשר שבין המידע שנמסר באמצעות החשוד (מראהו, קולו או כתב ידו) לבין הראיה הקושרת את החשוד לעבירה.[100]

בדרך זו ניתן להסביר גם את ההוראה המופיעה בחוק נטילת אמצעי זיהוי, אשר קובעת כי סירובו של החשוד שיבוצע חיפוש בגופו ובכך נמנע ביצוע החיפוש, עשוי לשמש חיזוק לראיות התביעה.[101] חוק נטילת אמצעי זיהוי אף מתיר, בנסיבות מסוימות, שימוש בכוח לשם נטילת ראיה מגופו של אדם.[102] על מנת להפליל אדם בנסיבות של חיפוש בגופו או נטילת אמצעי זיהוי מגופו, עשויה להידרש עדותו של אדם נוסף – מבצע החיפוש או עד מומחה – כדי לקבוע שיש קשר בין הראיה שנלקחה מהחשוד לבין העבירה.

מכל האמור לעיל ניתן להסיק את המסקנות האלה בכל הנוגע ליחס שבין זכות השתיקה לבין החיסיון מפני הפללה עצמית: מחד גיסא זכות השתיקה היא זכות מוחלטת, ואילו אשר לחיסיון מפני הפללה עצמית יש ניצני הכרה באפשרות שהוא אינו מוחלט, ומאידך גיסא פריסתה של זכות השתיקה מצומצמת מפריסתו של החיסיון מפני הפללה עצמית: החיסיון מפני הפללה עצמית חל הן על עדים והן על חשודים ונאשמים, ואילו זכות השתיקה קמה רק לחשודים ולנאשמים. כמו כן זכות השתיקה נפרסת רק על אמרות ועדויות של החשודים והנאשמים ואינה חלה על הפעולה של המצאת מסמכים קיימים מידי החשוד והנאשם לידי המדינה, ואילו החיסיון מפני הפללה עצמית חל גם בכל הנוגע לפעולה של המצאת מסמכים קיימים מידי החשוד והנאשם לידי המדינה.[103] אכן ניתן לטעון כי הסיבה לפריסתה המצומצמת יחסית של זכות השתיקה טמונה בעובדה שהיא זכות מוחלטת – לא ניתן לסייגה מפני אינטרסים וזכויות אחרים, ומכאן שיש להחילה במספר מצומצם של מקרים: אמרות ועדויות של חשודים ונאשמים בלבד.

איננו מבקשים לחלוק במאמר זה על הפרשנות של זכות השתיקה כזכות מוחלטת, והתמקדותנו במאמר היא דווקא בחיסיון מפני הפללה עצמית. כפי שיוצג בהמשך, נבקש לטעון כי יש לפרש את החיסיון מפני הפללה עצמית כחיסיון יחסי, מה שיאפשר לבית המשפט, בנסיבות המתאימות, לתת הוראות לחשוד אשר תגברנה על החיסיון. לעומת זאת בשל העובדה שזכות השתיקה עוסקת בסיטואציה העובדתית של **אמרות שמוסר החשוד או**

100 גרוס, לעיל ה״ש 61, בעמ׳ 184. גם בארצות הברית נהוגה הבחנה זו שבין ״עדות בדרך של תקשורת״ (Testimonial Communication) לבין ראיה חפצית. לא ניתן לחייב חשוד למסור עדות שתפליל אותו, אולם ניתן לחייב אותו למסור ראיה חפצית העלולה להפליל אותו. ראו למשל Schmerber v. California, 384 U.S. 757 (1966). יוער כי בעבר נמתחה ביקורת על ההשוואה בין הדין הישראלי לדין האמריקני בהקשר זה, שכן בדין הישראלי החיסיון מפני הפללה עצמית חל בנוגע לכל ״ראיה״, ואילו בדין האמריקני מדובר בחיסיון מפני מסירתה של ״עדות״ מפלילה. ראו אמנון סטרשנוב ״צמצום החסיון בפני הפללה עצמית״ **הפרקליט** לה 243, 244–245 (1983). בפרק הבא נרחיב בדבר ההסדרים החלים בארצות הברית בהקשר זה.

101 ס׳ 11 לחוק נטילת אמצעי זיהוי.

102 סעיף 3(ב) לחוק נטילת אמצעי זיהוי מאפשר לשוטר להשתמש בכוח סביר כדי לערוך ״חיפוש חיצוני״ בגופו של אדם, כקבוע בפסקאות (1)–(3) ו־(6)–(8) להגדרת ״חיפוש חיצוני״, משמע: בחינה חזותית של גופו העירום של אדם, לרבות צילומו; נטילת טביעה של כל חלק מהגוף; לקיחת חומר שמתחת לציפורניים; לקיחת שיער לרבות שורשיו; לקיחת חומר מעל הגוף ובדיקה על הגוף.

103 עניין **שרון**, לעיל ה״ש 89, פס׳ 17–18 לפסק דינו של השופט אור.

מסמכים שמייצר החשוד לפי דרישתה של הרשות החוקרת, טענתנו היא שזכות השתיקה אינה רלוונטית לשאלה שבמוקד מאמרנו, מכיוון שהמודל המוצע במאמר זה מתמקד בסיטואציה העובדתית שלפיה המחשב, הטלפון הסלולרי או היישום המקוון תפוסים כדין אצל הרשות החוקרת, והתפיסה אינה מכוח הוראה שניתנה לנחקר עצמו כי אם מכוח הפעלת סמכויות חיפוש ותפיסה ממקורות אחרים. כאשר המחשב, הטלפון הסלולרי או היישום המקוון כבר מצויים אצל הרשות החוקרת, נדרש הנחקר אך ורק להנגיש את המידע הקיים, ולא למסור אמרה אשר היא כשלעצמה אמורה להפלילו ולא לייצר מסמך עבור הרשות החוקרת.

דרכי הנגשת המידע הקיים יכולות להיעשות באחת מכמה דרכים: **האחת**, בדרך של מסירת הסיסמה או מפתח ההצפנה המגולמים בקוד תווי; **השנייה**, הקשת הנחקר את הקוד התווי בלא נוכחות החוקר, מבלי למסור לידיו את הקוד התווי, והעברת המחשב, הטלפון הסלולרי או היישום המקוון להמשך עיון בידי החוקר; **השלישית**, העמדת הפנים מול מערכת זיהוי הפנים, הנחת האצבע על גבי מערכת זיהוי טביעת האצבע במחשב או בטלפון הסלולרי, דיבור מול מערכת הזיהוי הקולי או נשיאת המחשב באופן שמערכת הזיהוי של דפוס השימוש במכשיר תזהה את המשתמש. הדרך הראשונה אומנם קרובה יותר, מבחינה טכנית, למסירת אמרה, ומשכך לכאורה יש קרבה לסיטואציה שמקימה לחשוד או לנאשם את זכות השתיקה, אולם מבחינה מהותית אין הבדל בין ה״אמרה״ הטכנית האמורה לבין פתיחת המכשיר בדרך של מסירת טביעת אצבע או העמדת הפנים אל מול המכשיר או כדומה. על כן יש לראות ב״אמרה״ כאן משום אמרה במובן הטכני אך לא במובן המהותי, בחריג אחד שבו מסירת הקוד התווי יש בכוחה להוכיח את זיקתו של החשוד או הנאשם למחשב, לטלפון הסלולרי או ליישום המקוון, ושאלת הזיקה היא השאלה שבמחלוקת אשר טעונה הוכחה. במקרה זה לא זו בלבד שתיווצר אמרה במובנה הטכני, אלא תיווצר גם אמרה בעלת כוח הוכחתי מהותי, ומכאן שההתנגשות עם זכות השתיקה של החשוד או של הנאשם — תהיה התנגשות חזיתית ומהותית.[104]

לעומת האמור על זכות השתיקה בכל הנוגע לפגיעה האפשרית בחיסיון מפני הפללה עצמית — כאן ודאי שנוצר חיכוך רחב יותר בין הפעולה שיידרש הנחקר לבצע לבין העובדה שיהיה בכוחה לתרום להפללתו. במילים אחרות, עניין לנו במצבים שבהם, ככלל, אין התחככות עם זכות השתיקה, אולם יש התנגשות פוטנציאלית עם החיסיון מפני הפללה עצמית. לכן אפוא התמקדותנו במאמר היא בחיסיון מפני הפללה עצמית ותחולתו על הגנת סיסמה או הצפנה של חומרי מחשב, ולא בזכות השתיקה.

נסכם עד כאן. הצגנו בפרק זה הצדקות מכיוונים שונים לזכות השתיקה ולחיסיון מפני הפללה עצמית — הן הצדקות במישור של תמרוץ הרשות החוקרת לאסוף ראיות ממקורות עצמאיים, הן הצדקות במישור של זכויות הנחקר לפרטיות ולאוטונומיה והן הצדקות במישור הלוגי של הימנעות מהעמדתו של הנחקר בפני טרילמה מוסרית. זכות השתיקה פורשה כזכות המוענקת לחשוד או לנאשם בנוגע לאמרה או ליצירת מסמך, ואילו החיסיון מפני הפללה עצמית רחב יותר, הן בנוגע לזהות ״בעליו״ (כל נחקר) והן בנוגע לסוגי

104 להרחבה נוספת ראו להלן תת־פרק ד.2.

הפעולות בחקירה (כל פעולה, אף אם אינה בגדר מסירת אמרה או יצירת מסמך אלא גם המצאת מסמך קיים, הנגשתו וביצוע כל פעולה אחרת). עוד כפי שהראינו, זכות השתיקה פורשה כזכות מוחלטת, וכפי שנראה להלן, החיסיון מפני הפללה עצמית יכול להתפרש כיחסי, ראוי שיתפרש ככזה, ואף ניתן לאתר ניצני הכרה בו כחיסיון בעל מובנים יחסיים. מכאן תיסלל הדרך, מבחינה נורמטיבית ומעשית, להכיר באפשרות להתגבר במקרים המתאימים על הגנת הסיסמה או ההצפנה המגינה על חומרי מחשב.

ג. יישום החיסיון מפני הפללה עצמית באמצעי אבטחת מידע במחשבים, בטלפונים סלולריים ובשירותים מקוונים

בפרק זה נבקש להציג שלושה מודלים שניתן, מבחינה רעיונית, להחילם במענה לשאלה בדבר אופן התמודדותה של הרשות החוקרת עם אמצעי אבטחת מידע במחשבים, בטלפונים סלולריים ובשירותים מקוונים. כפי שנראה, כל אחד מהמודלים האלה אינו חף מחסרונות ומביקורות. עוד נבקש להציג בפרק זה כמה דרכי פעולה אפשריות למניעת ההתנגשות בין החיסיון מפני הפללה עצמית לבין האינטרס החקירתי.

1. תחולה מלאה של החיסיון

בתמצית, מודל זה מכיר בכך שקם לעד ולחשוד החיסיון מפי הפללה עצמית, מפני דרישת הרשות החוקרת כי הנחקר ימסור להם את מפתח ההצפנה או הסיסמה שלו, או לחלופין – כי ינגיש את חומר המחשב לרשות החוקרת במצב מפוענח ולא מוגן־סיסמה. מודל זה זכה להכרה עד כה בעיקר בכמה ערכאות בארצות הברית. בדין האמריקני מעוגן החיסיון מפני הפללה עצמית בתיקון החמישי לחוקה האמריקנית, אשר קובע כי לא ניתן לכפות על אדם ״להעיד נגד עצמו״, ובלשון החוקה האמריקנית: "No person shall […] be compelled in any criminal case to be a witness against himself".[105]

המונח ״להעיד נגד עצמו״ פורש בעבר בבית המשפט העליון הפדרלי של ארצות הברית כך: "the privilege protects a person only against being incriminated by his own compelled testimonial communications",[106] משמע שהמונח ״להעיד נגד עצמו״ פורש כמגן על הפרט מפני הפללה על בסיס ״תקשורת בדרך של עדות״ (testimonial communications) אשר נכפתה עליו. בהמשך פירש בית המשפט העליון הפדרלי האמריקני את המונח "testimonial communications" כנוגע לפעולה אשר "relate a factual assertion or disclose information",[107] דהיינו כי לא ניתן לחייב את החשוד ״להסגיר״ מידע המצוי ברשותו והידוע רק לו, שכן מידע שכזה עולה כדי "testimonial communications" ומכאן שנחשב ל״עדות״ (ובהקשרנו – עדות נגד עצמו). נוסף על כך, בית המשפט העליון הפדרלי האמריקני קבע כי כאשר לעצם המצאת המידע מטעם החשוד לידי הרשות החוקרת יש

105 U.S. CONST. amend. V.

106 Fisher v. United States, 425 U.S. 391, 409 (1976).

107 Doe v. United States, 487 U.S. 201, 210 (1988).

משמעות תקשורתית (שאינה נובעת מנבכי מחשבתו של החשוד), גם אז יקום לחשוד החיסיון מפני הפללה עצמית.[108] מכאן שבבואם של בתי המשפט האמריקניים לבחון אם יש מקום להיעתר לבקשת הרשות החוקרת כי החשוד יחויב למסור את הסיסמה, את מפתח ההצפנה או את המידע המפוענח, נבחנת השאלה אם מסירת מידע כזה היא "contents of his own mind" (של החשוד), ומכאן שהיא עדות נגד עצמו.

בכל הנוגע לשאלה שבבסיס דיוננו במאמר, זו טרם הגיעה לפתחו של בית המשפט העליון האמריקני. כמה פסקי דין של ערכאות נמוכות יותר, הן במישור המדינתי והן במישור הפדרלי, הכירו בזכותו הלא מסויגת של החשוד לאי־הפללה עצמית בהקשרים טכנולוגיים אלה. לפיכך קבעו כי לא ניתן לחייב את החשוד למסור את סיסמת הכניסה או את מפתח ההצפנה, וכן לא ניתן לחייב את החשוד למסור לרשות החוקרת את חומר המחשב כשהוא מפוענח ולא מוגן־סיסמה.

בשנת 2009 זכתה השאלה להתייחסות ראשונה בעניין *Boucher*, שם הכיר בית המשפט המחוזי במדינת ורמונט בתחולת החיסיון מפני הפללה עצמית בעניינו של חשוד שנדרש למסור את סיסמת הכניסה לחומר המחשב שלו, ובלשונו של בית המשפט: "Compelling Boucher to produce the password compels him to display the contents of his mind to incriminate himself".[109] ייאמר מייד כי באותו עניין הפכה ערכאת הערעור את פסיקת בית המשפט המחוזי,[110] ועל כן בעניינו של Boucher הוכרה לבסוף גישה של אי־תחולת החיסיון מפני הפללה עצמית, שעליה יפורט בהמשך. בשנת 2010 קבע בית המשפט המחוזי בדרום מישיגן כי גם אם יובטח לחשוד כי לא ייעשה שימוש בפעולה של מסירת הסיסמה או מפתח ההצפנה נגדו (למשל, כדי להוכיח בכך כי מכשיר הטלפון הסלולרי הוא בבעלותו של החשוד), עדיין לא יהיה אפשר לחייב את החשוד למסור את הסיסמה או את מפתח ההצפנה שלו.[111] בשנת 2013 המשיך בית המשפט המחוזי במחוז המזרחי של מדינת ויסקונסין

108 כדוגמאות למידע שאינו ״נבכי מחשבתו״ של החשוד, אך עדיין יש לו משמעות תקשורתית, ניתן לציין את הדברים האלה: עצם קיומו של המסמך שממציא החשוד, העובדה שהחשוד שולט במסמך המומצא והעובדה שהחשוד מאמין שהמסמך שהוא ממציא הוא אותנטי. להרחבה בעניין זה ראו United States v. Hubbell, 530 U.S. 27 (2000). בהצעת חוק החיפוש נקבע הסדר דומה בכל הנוגע לחיסיון מפני הפללה עצמית ובלשונה של הצעת החוק: ״עצם מסירת הסמה אינו פוגע בחיסיון מפני הפללה עצמית, ככל שהטענה היא כי החומר המוצפן הוא מפליל, שהרי מדובר בחומר שהמשטרה היתה יכולה לתפוס, לולא היה מוצפן, ועצם ההצפנה אינו משנה את טיב סמכות המשטרה, או את טיבו של החומר. עם זאת, אין במתן הצו כדי למנוע טענות בנוגע לחיסיון מפני הפללה עצמית, ככל שנטען כי עצם מסירת הסמה הוא המפליל (למשל, מסירת הסמה תקשור את האדם לביצוע העבירה, בגלל הכינוי שנעשה בו שימוש כסמה)״ (שם, בעמ׳ 633). להלן בתת־פרק ד.3 נעסוק בהרחבה בהצעת חוק החיפוש, ובשאלה זו באופן ספציפי.

109 *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951 (D. Vt. Nov. 29, 2007).

110 *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009).

111 United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010). בלשונו של בית המשפט: "even if the government provides defendant with immunity with regard to the act of producing the password to the grand jury, that does not suffice to protect Defendant's

באותו קו ופסק כי לא ניתן לחייב חשוד לפתוח את ההצפנה של מערכות גיבוי המידע שלו, שכן יהיה זה מנוגד לתיקון החמישי לחוקה האמריקנית.[112] בשנת 2017 פסק בית המשפט במחוז הצפוני של מדינת אילינוי פסיקה דומה בכל הנוגע לטביעות אצבע. באותו מקרה ביקשה הרשות החוקרת כי בית המשפט יאפשר לה לקחת את טביעות האצבע של כל השוהים במקום כדי לראות אם אחד מהאנשים הללו היה מעורב בעבירות הנחקרות. בית המשפט דחה את בקשת הרשות החוקרת וקבע כי מסירת טביעת אצבע תעלה כדי מסירת ״מידע״ לרשות החוקרת – העובדה שמוסר הטביעה הוא בעליו של מכשיר הטלפון הסלולרי. מכאן שמדובר ב־"testimonial communications", ולכן קם ליושבי הבניין החיסיון מפני הפללה עצמית.[113] במישור הפדרלי ניתן לציין את החלטתו של בית המשפט הפדרלי לערעורים ב־11th Circuit, אשר קבע מפורשות כי "We hold that Doe's decryption and production of the hard drives' contents would trigger Fifth Amendment protection".[114] בעקבות זאת ביטל בית המשפט הפדרלי לערעורים את החלטת בית המשפט קמא שלפיה סירובו של החשוד למסור את מפתח ההצפנה לאחר שנמסר לו צו מתאים עולה כדי ביזיון בית המשפט. להשלמת התמונה נציין כי נוסף על פסקי דין אלה, כמה ערכאות בארצות הברית פסקו דווקא לפי מודל של אי־תחולת החיסיון מפני הפללה עצמית, ועל כך נרחיב בתת־הפרק הבא.

לסיכום עד כאן, לפי מודל התחולה המלאה של החיסיון מפני הפללה עצמית לא ניתן לחייב אדם למסור את סיסמתו או את מפתח ההצפנה שלו משום שהדבר חוסה בצילו של החיסיון, או במונחי המשפט האמריקני – מדובר ב־"testimonial communications". בדומה לזה, לפי גישה זו, לא ניתן לחייב את האדם למסור לרשות החוקרת את המידע כשהוא מפוענח או לאחר שהוסרה ממנו הגנת הסיסמה (ומבלי שימסור לרשות החוקרת את הסיסמה או את מפתח ההצפנה עצמם), שכן אף בכך יהיה כדי להפר את החיסיון מפני הפללה עצמית. אי לכך, על פי מודל זה, על מנת להגיע למידע הממוחשב, יהא על רשויות החקירה להגיע לסיסמה או למפתח ההצפנה דרך מקור חיצוני לחשוד או לעד עצמם (למשל, בדרך של חיפוש בכליו של החשוד ותפיסת פתק שבו נרשמה הסיסמה; קבלת הסיסמה מאשת הנחקר במסגרת עדות או כדומה). אומנם מודל זה מונע כל חיכוך עם החיסיון מפני הפללה עצמית, אולם לגישתנו מודל זה מקים קשיים ממשיים ולא סבירים בפני רשויות החקירה. ההטמעה האינהרנטית של אמצעי אבטחת מידע כסיסמאות והצפנות בקרב המחשבים האישיים, הטלפונים הסלולריים, התוכנות והיישומים השונים, הופכת למעשה את מלאכת החיפוש והעיון במידע מטעם הרשות החוקרת לכמעט בלתי אפשרית, כל עוד לא תימצא הדרך להתגבר, במקרים המתאימים, על ההגנות האלה. כיוון שלא אחת

invocation of his Fifth Amendment privilege in response to questioning that would require him to reveal his password".

112 *In re* Decryption of a Seized Data Storage Sys., No. 13-M-449, 2013 U.S. Dist. LEXIS 202353 (E.D. Wis. Apr. 19, 2013).

113 *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066 (N.D. Ill. 2017). לפסיקה ברוח דומה ראו גם G.A.Q.L v. State, 257 So. 3d 1058 (Fla. Dist. Ct. App. 2018).

114 United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335 (11th Cir. 2012).

אין מנוס מלקבל את הסיסמה או את מפתח ההצפנה מהחשוד או מהעד, הרי שההכרה במודל התחולה המלאה של החיסיון עלולה להוביל לתוצאה לא רצויה של פגיעה אסטרטגית ביכולת הרשות החוקרת לאסוף את הראיות, אשר תיאלץ להסתפק בכלים פרקטיים המגלמים פתרון חלקי בלבד (ועל כך יפורט עוד בהמשך, בתת־פרק 4 שבפרק זה).[115] יש לציין כי הצורך בפיענוח ראיות דיגיטליות אינו רלוונטי לחקירת עבירות פליליות במרחב הסייבר בלבד. גם בחקירות פליליות בגין עבירות במרחב הפיזי הראיות הרלוונטיות להוכחת אשמתו או חפותו של החשוד עשויות להימצא במחשבים, בטלפונים סלולריים או בשירותים מקוונים. למשל, במסגרת חקירת עבירה של אינוס עשוי לקום הצורך לבחון תכתובות של החשוד עם המתלוננת במסגרת יישומונים להעברת מסרים מיידיים כגון WhatsApp או Telegram. לכן יישומו של מודל התחולה המלאה של החיסיון מפני הפללה עצמית במצבים של דרישה למסירת סיסמה או מפתח הצפנה למחשבים, לטלפונים סלולריים או לשירותים מקוונים – משמעו יצירת חסינות דיונית דה פקטו, ברובן של החקירות הפליליות, מפני חיפוש בחומרי המחשב הרלוונטיים לחקירת עבירות פליליות.[116]

2. אי־תחולה של החיסיון

מודל זה מנוגד לקודמו, ועל פיו, החיסיון מפני הפללה עצמית אינו חל על הסיטואציה דנן, שבה המחשב או הטלפון הסלולרי תפוסים כדין אצל הרשות החוקרת, או שיש לה גישה כדין לשירות המקוון, וקיים ברשותה היתר כדין לעיין בחומרי המחשב (כולם או חלקם), ואין בידיה לגשת אל אותם חומרים בשל הגנת סיסמה או הצפנה. על פי מודל זה, במצב הדברים המתואר לא יקום לחשוד ולעד החיסיון מפני הפללה עצמית.

יעילותו של מודל זה, מבחינתן של רשויות החקירה, מובנת מאליה. אולם ניתן למנות הצדקה נוספת, סמויה יותר מן העין, והיא כי הסמכות לכפות על הנחקר את מסירת הסיסמה או מפתח ההצפנה או להמציא לרשות החוקרת את המידע במצב לא מוצפן ולא מוגן־סיסמה היא פוגענית פחות מהאלטרנטיבה של פיתוח מערך רוחבי של מעקב וניטור של פעילות כלל המשתמשים, על מנת שיתאפשר לרשות החוקרת לזכות בגישה אל המידע

115 קיימת זיקה הדוקה בין יכולתן של רשויות אכיפת החוק לאסוף ראיות דיגיטליות לבין עצם יכולתן לאכוף את הדין הפלילי. להרחבה בעניין זה ראו U.N. Office on Drugs & Crime, Comprehensive Study on Cybercrime 157–161 (2013), https://bit.ly/3DpRv8B (טיוטת המחקר של ה־UNODC בנוגע לפשיעת סייבר).

116 לעניין זה השוו עם ס׳ 2(א), 2(ב) לחוק חסינות חברי הכנסת, זכויותיהם וחובותיהם, התשי״א–1951 (להלן: חוק חסינות חברי הכנסת). סעיפים אלה קובעים כי ככלל, להוציא חריגים נדירים המנויים בחוק, חבר הכנסת יהיה חסין מפני חיפוש בדירתו, בגופו, בחפציו או בניירותיו. אומנם החוק נוקט לשון ״חפצית״ ואינו מתייחס לחומרי מחשב, אולם ניתן להניח שהמונח ״ניירותיו״ של חבר הכנסת מוחל על מסמכים אלקטרוניים, תכתובות דוא״ל וכדומה. הסדר ייחודי זה של חסינות מפני חיפוש מלמד על הכלל, ולפיו אין לאפשר מצב של חסינות דה־פקטו מפני חיפוש בחפציו ובניירותיו של חשוד שאינו חבר הכנסת, על סמך ההנחה שהחסינות היא חריג המתנגש עם עקרון השוויון בפני החוק, ועל כן ראוי לפרשו בצמצום, וראוי להכירו רק במקרה של הוראת חוק מפורשת המחילה אותו. השוו בג״ץ 507/81 **אבו חצירא נ׳ היועץ המשפטי לממשלה**, פ״ד לה(4) 561, 585 (1981); בג״ץ 620/85 **מיעארי נ׳ יו״ר הכנסת**, פ״ד מא(4) 169, 268 (1985).

הממוחשב במחשב, בטלפון הסלולרי או בשירות המקוון במקרה שבו יתעורר חשד נגד משתמש מסוים.[117] על בסיס הרציונל של טענה זו ניתן להוסיף ולטעון כי אי־מתן הסמכות לרשויות החקירה לכפות את מסירת הסיסמה, מפתח ההצפנה או המידע המפוענח עלול להוביל את רשויות אכיפת החוק לתפוס מחשבים וטלפונים סלולריים לתקופות זמן ארוכות יותר, בניסיון לפצח או להשיג את הסיסמה לפתיחתם.[118]

אחת המדינות שאימצו את מודל אי־התחולה של החיסיון בחקיקה היא בריטניה, שבה נקבע במפורש ב־Regulation of Investigatory Powers Act (RIPA) משנת 2000 כי שוטר רשאי לחייב אדם, באמצעות הוראה בכתב, למסור את הסיסמה או את מפתח ההצפנה שלו למחשב, לטלפון הסלולרי או לשירות המקוון במקרים של הגנה על הביטחון הלאומי, חקירת עבירות או הגנה על אינטרסים כלכליים של המדינה.[119] במקרה של אי־ציות להוראה זו נקבעה בחוק עבירה עצמאית שדינה עד שנתיים מאסר (או חמש שנות מאסר כשמדובר בחקירת עבירה על ביטחון המדינה).[120] בשנת 2008 פירש בית המשפט לערעורים בבריטניה את ההוראה ב־RIPA המאפשרת לחייב נחקר במסירת סיסמה או מפתח הצפנה וקבע כי הוראה זו קובעת חריג סטטוטורי לחיסיון מפני הפללה עצמית. בלשונו של בית המשפט:

> It is well understood that the principle [against self-incrimination] is subject to numerous statutory exceptions which limit, amend, or abrogate the privilege in specified circumstances. Thus, notwithstanding the privilege, individuals may sometimes be required to answer questions or provide information or documents which may incriminate them.[121]

לשם הדיוק נציין כי בית המשפט לא קבע כי אין תחולה לחיסיון במקרה שנדון לפניו, אלא קבע כי אומנם חל החיסיון מפני הפללה עצמית, אלא שהחוק מסייג אותו, במלואו, בנסיבות של דרישת מפתח הצפנה או סיסמה מנחקר, על פי התנאים הקבועים בחוק. על בסיס ניתוח זה של החיסיון מפני הפללה עצמית הרשיע בית המשפט באותו מקרה את הנאשמים בעבירה של אי־מסירת מפתח הצפנה.

117 טיעון זה העלה Ungberg, לעיל ה״ש 33, בעמ׳ 539.

118 כפי שהוזכר לעיל, שיטות טכנולוגיות לפיצוח הצפנה מחייבות לעיתים זמן רב (ולעיתים שנים רבות) עד למציאת מפתח ההצפנה, ולעיתים שיטות אלה אינן נושאות פרי כלל (ראו לעיל פרק א, ה״ש 35–37 ובטקסט הנלווה אליהן).

119 Regulation of Investigatory Powers Act, 2000, §49(3) (Eng.). הוראה זו נכנסה לתוקף בשנת 2007.

120 שם, ס׳ 53.

121 R v. S & A [2008] EWCA Crim. 2177, §17 (Eng.). לדיווחים על מקרים נוספים שבהם הועמדו לדין נאשמים על אי־ציות להוראה למסור מפתח הצפנה או סיסמה ראו *Man found guilty under UK Terrorism Laws after Refusing to Reveal Passwords,* REUTERS (Sep. 25, 2017), https://tinyurl.com/y5dzp5w2. ראו גם Tom Barnes, *Lucy McHugh: Murder Suspect Remanded in Custody for "Failing to Provide Facebook Password to Detectives"*, INDEPENDENT, (July 31, 2018), https://tinyurl.com/yxnkgqkr.

בדומה לדין בבריטניה, גם באוסטרליה קבע המחוקק כי ניתן לחייב אדם למסור את סיסמת הכניסה או את מפתח ההצפנה לחומרי המחשב שלו. עם זאת על פי החוק האוסטרלי, נדרש לשם כך צו שיפוטי, ואילו בבריטניה רק שוטר יכול לתת את ההוראה המחייבת. בית המשפט האוסטרלי רשאי להוציא צו כאמור במקרים שבהם יש חשד סביר שמידע רלוונטי לחקירה מצוי בחומרי המחשב של הנחקר, וכל עוד שוכנע בית המשפט כי יש יסוד סביר להניח (Reasonable Grounds) כי יש ראיות רלוונטיות בחומרי המחשב, וכן שוכנע כי הנחקר הוא חשוד או בעליו של המחשב. העונש על אי־ציות לצו כאמור הוא עד שישה חודשי מאסר.[122]

בניו זילנד נקבע בחוק כי חיסיון מפני הפללה עצמית יחול במקרים של דרישה מטעם הרשות החוקרת להמציא מידע דיגיטלי העלול להפליל את מוסר המידע, אולם כאשר המידע הנדרש הוא אך ורק הסיסמה או מפתח ההצפנה לחומרי המחשב, ולא הקבצים עצמם, הרי שלא יחול החיסיון מפני הפללה עצמית והוא יידחה מפני האינטרס של רשויות החקירה.[123]

במשפט האמריקני המחוקק לא הסדיר את הסוגיה שלפנינו. כפי שראינו לעיל, חלק מהפסיקה הכירה במודל תחולה מלאה של החיסיון, אולם כפי שנראה להלן, פסיקה אחרת קבעה דווקא את ההפך, כי יש להחיל מודל של אי־תחולת החיסיון על הדרישה לפתוח סיסמה או הצפנה לחומרי מחשב התפוסים כדין אצל הרשות החוקרת או להנגיש את המידע הממוחשב לאחר הסרת הסיסמה או ההצפנה. חלק מהפסיקה האמריקנית שקבעה את מודל אי־התחולה של החיסיון מפני הפללה עצמית התבססה על הדוקטרינה האמריקנית של ״מסקנה מובנת מאליה״ (Forgone Conclusion). דוקטרינה זו קובעת כי במקרים שבהם המידע שמתבקש החשוד למסור הוא מידע מובן מאליו מנקודת המבט של הרשות החוקרת, לא יקום לחשוד החיסיון מפני הפללה עצמית. במקרים שבהם קיומן של ראיות מפלילות במחשביו של החשוד היה ידוע זה מכבר לרשות החוקרת, וכן הרשות החוקרת הוכיחה כי היא יודעת שהחשוד הוא בעליו של המכשיר הנדון, הרי שגילוי המידע נכלל בגדר חריג מוכר לחיסיון מפני הפללה עצמית של ״מסקנה מובנת מאליה״, ועל כן אין לראות במסירת מידע זה משום "testimonial communications". כך פסק בשנת 2011 בית המשפט המחוזי במדינת קולורדו כי מסירת המידע האגור במחשב נייד של החשודה, לאחר פיענוחה אותו, לא תפגע בחיסיון מפני הפללה עצמית, בשל תחולתו של חריג המסקנה המובנת מאליה, שכן באותו מקרה עצם הימצאות המידע המפליל במחשבי החשודה היה ידוע זה מכבר לרשות החוקרת, ולכן המצאתו היא בגדר מסקנה מובנת מאליה ואיננה מפלילה כשלעצמה את החשודה.[124] כך נפסק גם בבית המשפט לערעורים של מדינת מסצ׳וסטס בשנת 2017

122 *Cybercrime Act 2001* s 3LA (Austl.).

123 Search and Surveillance Act 2012, s 130 (N.Z.). יוער כי בדין הניו זילנדי נקבע עוד כי הוראות אלה יחולו גם על חיפושים בחומרי מחשב שמבצעים פקידי מכס במכשיריהם האלקטרוניים של הנכנסים לתחומי המדינה. ראו Customs and Excise Act 2018, s 228 (N.Z.). לביקורת על החלה זו של הדין הניו זילנדי על הנכנסים למדינה ראו Charlotte Graham-McLay, *Fork Over Passwords or Pay the Price, New Zealand Tells Travelers,* N.Y. TIMES (Oct. 2, 2018), https://tinyurl.com/yarkcgx6.

124 United States v. Fricosu, 841 F.Supp. 2d 1232 (D. Colo. 2012).

בנוגע למסירה של סיסמת כניסה למכשיר מסוג iPhone.[125] כך פסק אף בית המשפט הפדרלי לערעורים ב־3rd Circuit באותה השנה, בדבר מסירת מפתח הצפנה למידע המצוי במחשב.[126]

יצוין כי בכל הנוגע למסירת טביעות אצבעות שישמשו את הרשות החוקרת לפתיחה של מחשבים, טלפונים סלולריים או שירותים מקוונים מסוימים, עמד בית המשפט לערעורים של מדינת מינסוטה על הצדקה מוגברת למודל אי־התחולה. על פי הצדקה זו, מסירת טביעת האצבע שונה ממסירת הסיסמה או מפתח ההצפנה, שכן טביעת האצבע אינה ״מידע״ הנמסר מפי הנחקר, בשונה ממפתח ההצפנה או הסיסמה. לפיכך פסק בית המשפט לערעורים של מדינת מינסוטה כי החלטת בית המשפט קמא לחייב את הנאשם למסור את טביעת האצבע שלו כדי לפתוח את הטלפון הסלולרי שלו אינה פוגעת בחיסיון הנאשם מפני הפללה עצמית.[127] הנימוק המרכזי לקביעה זו היה שמסירת טביעת אצבעו של הנאשם אינה בבחינת מסירה של מידע או עדות מפלילה כשלעצמה (כזכור, פורש התיקון החמישי כמגן על החשוד מפני כפייה למסור "factual assertion or disclose information").[128] בניגוד לכפייה על החשוד למסור סיסמה, מפתח הצפנה או את המידע המפוענח, נקבע כי טביעת אצבע אינה ״מידע״, ולכן אין התנגשות עם החיסיון מפני הפללה עצמית, שכן אין מתקיים מתקל בין האינטרס החקירתי לבין זכויות החשוד.[129]

עוד בהקשר זה יצוין כי גם המשפט הישראלי, ששותק בנוגע לסוגיה הכללית של חיוב הנחקר במסירת סיסמה, מפתח הצפנה או מידע ממוחשב בצורה מונגשת, הכיר במפורש בסמכות ליטול אמצעי זיהוי, לרבות טביעת אצבע, מחשוד[130] מבלי שהדבר ייחשב לפגיעה אסורה בחיסיון מפני הפללה עצמית.[131] המחוקק הישראלי אף הכיר בסמכות ליטול את טביעות האצבע בכוח סביר.[132]

מודל אי־התחולה המלא שפורט כאן אינו חף מקשיים. מובן כי על פי מודל זה, נפגעת במידה לא מבוטלת יכולתו של משתמש המחשב ליהנות ממרחב פרטי שבו יוכל לחשוב,

125 *In re* Grand Jury Investigation, 92 Mass. App. Ct. 531, 88 N.E.3d 1178 (2017).

126 United States v. Apple Mac Pro Comput., 851 F.3d 238 (3d Cir. 2017).

127 State v. Diamond, 890 N.W. 2d 143 (Minn. Ct. App. 2017).

128 ראו לעיל ה״ש 107.

129 פיליפ רייטינגר (Reitinger) העלה טיעון רחב יותר, הנוגע לא רק למסירת טביעת אצבע כי אם גם למסירה של כל סיסמה או מפתח הצפנה בידי החשוד. ראו Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, U. CHI. LEGAL F. 171, 195–197 (1996) (על פי טיעונו, כאשר החשוד ממציא לידי הרשות החוקרת את הסיסמה או את מפתח ההצפנה שלו, הוא ממציא לה ״מסמך״ קיים ואינו יוצר מסמך חדש יש מאין. כיוון שעצם קיומו של ״מסמך״ זה (הסיסמה או מפתח ההצפנה) אינו מוטל בספק, וכיוון שה״מסמך״ נפרד מהמידע המוצפן שאותו מבקשת הרשות החוקרת, ניתן לחייב את החשוד למסור את הסיסמה או את מפתח ההצפנה).

130 ראו ס׳ 3(ב), 11ז(ג) לחוק נטילת אמצעי זיהוי. מלבד זאת, נראה כי המחוקק החשיב נטילה של טביעת אצבע לפוגענית פחות מנטילתם של אמצעי זיהוי אחרים או מביצוע חיפוש בגוף החשוד. למשל, סעיף 2(ה)(3) לחוק נטילת אמצעי זיהוי קובע כי ככלל, חיפוש בגופו של החשוד ייערך בידי בן מינו, אולם נטילת טביעות אצבע יכול שתיעשה אף שלא בידי בן אותו מין של החשוד.

131 ראו קביעת בית המשפט העליון בעניין **חורי**, לעיל ה״ש 46.

132 ס׳ 3(ב), 11ז(ג) לחוק נטילת אמצעי זיהוי.

לצרוך תכנים ולהתבטא בחופשיות. כיוון שהמרחב הממוחשב הופך לחלק בלתי נפרד מאישיותו של האדם, שבו הוא לא רק מבצע פעולות ומתקשר עם אחרים, אלא גם מבצע שלל פעולות עצמיות, הרי שלהכרה הגורפת בסמכות המדינה להתגבר על אמצעי אבטחת המידע עלולה להיות השלכה מצננת מסוימת על האוטונומיה של הרצון של כלל משתמשי המחשב והרשת.[133] מלבד זאת, כאשר מדובר בחיוב אדם במסירת סיסמה או מפתח הצפנה יכולים להתעורר מצבים שבהם הנחקר ישכח את המידע האמור ולא יוכל לשחזרו. במקרה כזה אם תינקטנה סנקציות שונות נגד החשוד השכחן, הרי שהוא עלול להיפגע על לא עוול בכפו.[134]

כפי שנראה להלן בפרק ד למאמר, בכוונתנו להביע תמיכה במודל שמבקש לסייג באופן יחסי את החיסיון מפני הפללה עצמית כשעולה הצורך החקירתי לקבל סיסמה, לקבל מפתח הצפנה למחשב, לטלפון סלולרי או לשירות מקוון שנתפסו כדין על ידי הרשות החוקרת, או לקבל את המידע האגור בהם בצורה מונגשת. על פי הצעתנו, החיסיון יסויג על פי כמה תבחינים, שמטרתם ליצור איזון מדויק יותר בין האינטרס הציבורי, שאותו מייצגות רשויות החקירה – לאכוף את הדין הפלילי – לבין החיסיון מפני הפללה עצמית והחשש מפני אפקט מצנן על התנהגותם של כלל משתמשי המחשב והרשת.

3. מודל חיסיון השימוש

מודל זה מושתת על הרציונל שבבסיס פסיקתו של בית המשפט העליון בעניין **שרון**.[135] באותו עניין עסק בית המשפט העליון בשאלה אם זכות השתיקה של חשוד חלה גם על מסמכים, ויתאפשר לו אפוא שלא למסור אותם אף אם אינם מפלילים אותו. יוזכר בקצרה כי גלעד שרון היה חשוד בעבירות לפי חוק מימון מפלגות, התשל״ג–1973 ובעבירה של תיווך בשוחד. גלעד שרון התגורר בזמן החקירה תחת אותה קורת גג עם אביו, ראש הממשלה דאז אריאל שרון ז״ל. בשל חסינותו של ראש הממשלה שרון מפני חיפוש בביתו, לפי סעיף 2 לחוק חסינות חברי הכנסת, החליטה משטרת ישראל לבקש את המצאתם של מסמכים הקשורים לעבירות שבגינן נחקר גלעד שרון באמצעות צו המצאה לפי סעיף 43 לפסד״פ אשר יופנה אל גלעד שרון. צו כאמור ניתן בבית משפט השלום, אך גלעד שרון טען כי עומדת לו זכות השתיקה כחשוד בעבירות, ולכן באפשרותו שלא לשתף פעולה עם רשויות החקירה ושלא למסור אף מסמך אחד מהמסמכים שנדרשו ממנו – הן מסמכים אשר מפלילים אותו בעבירה הפלילית והן מסמכים אשר אינם מפלילים אותו בעבירה הפלילית.

133 אומנם חשש זה מתמתן בשל האיזון השיפוטי הקונקרטי שיערוך בית המשפט בבואו לאשר את צו החדירה לחומר המחשב (וראו עוד לעניין זה להלן פרק ד), אולם לא ניתן להתעלם מהאפקט המצנן האפריורי, שלא אגב מקרה קונקרטי שיעמוד לבחינת בית המשפט.

134 Michael Wachtel, *Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone's Mind*, 14 PITT. J. TECH. L. & POL'Y 44 (2013).

135 עניין **שרון**, לעיל ה״ש 89.

באותו עניין קבע בית המשפט העליון כי לא תעמוד לחשוד זכות השתיקה בכל הנוגע למסירתם של מסמכים קיימים (בשונה מיצירתם של מסמכים חדשים, אשר בעניינם תחול זכות השתיקה). לפיכך אין באפשרותו של החשוד להתעלם כליל מהצו השיפוטי המורה לו למסור מסמכים.[136] לצד זאת קבע בית המשפט העליון כי החשוד רשאי לטעון טענה המושתתת על החיסיון מפני הפללה עצמית בנוגע למסמכים ספציפיים ולפנות לבית המשפט בבקשה מתאימה.[137] על פי המתווה שנקבע בבית המשפט העליון, בית המשפט שדן בבקשה יבחן את המסמכים המבוקשים, יעביר ליחידה החוקרת את המסמכים אשר אינם מעוררים חשש להפללה עצמית של החשוד, ויאפשר את העברת המסמכים אשר כן מעוררים חשש כאמור ליחידה החוקרת רק אגב הענקת ״חיסיון שימוש״ לחשוד. משמע, כי מסמכים אלה לא ישמשו בעתיד נגד החשוד בהליכים פליליים שינוהלו נגדו.[138]

המודל המתואר בעניין **שרון** עשוי לספק פתרון מסוים לאתגר הניצב במוקד מאמר זה. ההקבלה בין שתי הסיטואציות אפשרית משום שבשני המקרים, הן בעניין **שרון** והן במקרה שלפנינו, רשאיות רשויות החקירה לגשת למסמכים הנמצאים ברשותו של החשוד, על פי הרשאה שיפוטית קונקרטית, אך עומד בפניהן מחסום בלתי עביר לכאורה – בעניין **שרון** המחסום היה חסינותו של אביו של החשוד, שהתגורר עימו, ואילו בענייננו המחסום הוא הסיסמה או מפתח ההצפנה הידועים לבעל המכשיר בלבד.

החלת המודל של חיסיון שימוש על עניינו תאפשר לדרוש מהנחקר למסור את הסיסמה או את מפתח ההצפנה לחומרי המחשב שברשותו, או לחלופין להמציא מידע האגור במחשב, בטלפון הסלולרי או ביישום המקוון שברשותו, במצב מפוענח ולא מוגן־סיסמה. על הנחקר יהיה לפנות לבית המשפט כדי לבקש לפטור אותו מהחובה להמציא או להנגיש מסמכים מסוימים אשר עולה חשש כי יפלילו אותו. אם בית המשפט יקבע כי מסמכים או מידע מסוים האגורים במחשב, בטלפון הסלולרי או ביישום המקוון של הנחקר אכן עשויים להפלילו, יוענק חיסיון שימוש לבעל המכשיר וכך לא יהיה אפשר להשתמש במסמכים שנמצאו במכשיר נגדו בהליכים פליליים.

יוצא אפוא כי יישום מודל של חיסיון שימוש בענייננו עשוי להתאים לצורכיהן של רשויות החקירה רק במקום שבו מדובר בדרישה מעדים להמציא מסמכים האגורים במחשב, בטלפון הסלולרי או ביישום המקוון שלהם. משמע, שבמקרה שבו רשויות החקירה יבקשו להשתמש בסרטון המתעד את ביצוע העבירה בידי החשוד ושצולם בידי עד ראייה במכשיר הטלפון הסלולרי שלו, והעד יחשוש מהפללתו העצמית בעת מסירת מכשיר הטלפון שלו, אזי יהיה אפשר להעניק חיסיון שימוש לעד, כדי לאפשר לרשויות החקירה לחקור את החשדות נגד החשוד המרכזי בביצוע העבירה.

עם זאת כאשר עסקינן בסיטואציה השכיחה יותר, היא הסיטואציה שבה המידע הרלוונטי לחקר החשדות אגור במחשב, בטלפון הסלולרי או ביישום המקוון של החשוד עצמו – הרי שהמודל של חיסיון שימוש אינו יכול לספק מענה מקיף לאתגר הניצב במוקד מאמרנו, מן הטעם שהמודל של חיסיון שימוש מבוסס על העיקרון שלפיו החיסיון מפני

136 שם, פס׳ 14 לפסק דינו של השופט אור.

137 שם, פס׳ 17.

138 שם, פס׳ 18.

הפללה עצמית, בכל הנוגע למסמכים אשר אכן עשויים להפליל את החשוד, הוא עודנו חיסיון מוחלט במובן זה שבנוגע לכל מסמך המפליל את החשוד יעמוד החיסיון מפני הפללה עצמית במלואו, והמסמך לא ישמש נגד החשוד. מכאן נובע שתוצאה זו אינה מספקת כל פתרון מעשי לצורכי החקירה הממוקדים בראיות **שיוכלו לשמש נגד החשוד** מתוך המחשב, הטלפון הסלולרי או היישום המקוון של החשוד. כפי שפירטנו באריכות לעיל, האתגר המונח לפתחן של רשויות אכיפת החוק הוא ממשי, והוא אף צפוי להחריף ולהעמיק בשנים הקרובות, עם התפתחותם של אמצעי אבטחת מידע מתוחכמים ומתקדמים יותר. התמודדות עם אתגר זה תהפוך לכמעט בלתי אפשרית דה פקטו באמצעות החלת המודל של חיסיון שימוש, משום שנתח ניכר מהראיות נגד חשודים אגור במחשביהם, בטלפונים הסלולריים שלהם וביישומים המקוונים שלהם. בתוך כך ראוי להזכיר הבדל עובדתי חשוב בין עניין **שרון** לענייננו: אומנם המחסום שניצב בפני רשויות אכיפת החוק בעניין **שרון** נדמה היה כלא עביר, בשל חסינותו של ראש הממשלה דאז אריאל שרון ז״ל, אשר היה חשוד אף הוא, לצד בנו, בפרשה, אולם בפועל עמדה לפני משטרת ישראל האפשרות לבקש את הסרת חסינותו של ראש הממשלה מפני חיפוש לפי סעיף 13(ב) לחוק חסינות חברי הכנסת. לעומת זאת בענייננו, לעיתים אין כל אפשרות משפטית או מעשית לעקוף את המחסום הניצב בפני רשויות החקירה.

יצוין עוד כי בענייננו הדרישה מהנחקר תהיה למסור את חומרי המחשב התפוסים כדין אצל הרשות החוקרת, כשהם מפוענחים ואינם מוגני־סיסמה, ולחלופין למסור לרשות החוקרת את הסיסמה או את מפתח ההצפנה ובכך לאפשר לרשות החוקרת לבצע **בעצמה** את החיפוש במחשב, בטלפון הסלולרי או ביישום המקוון.[139] במילים אחרות, הגישה הראשונית – והיא בלבד – תימסר בידי הנחקר, ואילו את החיפוש עצמו תבצע הרשות החוקרת. לטעמנו, הפגיעה באוטונומיה של החשוד כאשר הוא נדרש להמציא מלכתחילה את חומרי המחשב הנחוצים לחקירה חריפה מזו שבמקרה של מסירה חד־פעמית של סיסמה או מפתח הצפנה, אשר לאחריהם תבצענה רשויות החקירה את החיפוש בעצמן בחומרי מחשב שהן תפסו בכוחות עצמן ועל פי דין.

נוסף על כך נציין, גם אם בשולי הדברים, כי מודל חיסיון השימוש מטיל חובה על החשוד לפנות לבית המשפט בבקשה כי יפטור אותו מהמצאתם של מסמכים ספציפיים בשל העובדה שהם עלולים להפלילו.[140] לטעמנו, ראוי למעט בהטלת חובות עשה על חשודים בשלב החקירה, הן ככלל והן במקרה הספציפי שלפנינו. תחת זאת ראוי בשלב החקירה להטיל חובה על רשויות החקירה לפנות לבית המשפט בבקשה לקבל הסמכה לבצע פעולות חקירה מסוימות, בכפוף לעמידה בנטל השכנוע.

לסיכום חלק זה נשוב ונציין כי מודל חיסיון השימוש המבוסס על פסיקת בית המשפט העליון בעניין **שרון** אומנם מציע מענה מסוים בכל הנוגע לדרישה למסירת סיסמה או מפתח

139 ראוי לציין כי בית המשפט העליון העיר לא פעם בעניין **שרון** (שם, פס׳ 25) כי המצאת מסמכים על ידי חשודים היא פרקטיקה נדירה, וראוי כי תישמר ככזו. מכאן שניתן להבחין בין הלכת **שרון** לבין מצב שבו הרשות החוקרת מבצעת בעצמה את החיפוש ואילו הנחקר מוסר לה רק את האמצעי המאפשר לה לפענח את המידע שנתפס בידיה כדין ושבו היא אמורה לחפש.

140 שם, פס׳ 24.

הצפנה בידי עדים, אך קשה לראות בו משום פתרון סביר לצורכי החקירה בכל הנוגע למסירת סיסמה, מסירת מפתח הצפנה או מסירת מידע מונגש ומפוענח בידי חשודים.

4. עקיפת ההתנגשות החזיתית עם החיסיון מפני הפללה עצמית

בפרק זה נבקש למנות כמה דרכי פעולה אפשריות אשר באמצעותן תוכלנה רשויות אכיפת החוק לנסות להימנע מ"התנגשות" בין צורכי החקירה לבין החיסיון מפני הפללה עצמית בכל הנוגע לצורך החקירתי להתגבר על הגנת סיסמה והצפנה. דרכי פעולה אלה, על יתרונותיהן וחסרונותיהן, יסייעו לחדד ולהבהיר את המודל המוצע שנציג בפרק הבא, אולם ייאמר מייד כי אין בהן כשלעצמן כדי להעניק פתרון מספק לבעיה שבמוקד מאמרנו.

דרך הפעולה **הראשונה** היא הטלת סנקציות בדין על החשוד או על העד שסירב למסור את מפתח ההצפנה או את הסיסמה לרשות החוקרת, או שסירב להנגיש את המידע המפוענח לרשות החוקרת. סנקציות אלה יכולות להיות בדרך של נקיטת הליכים לפי פקודת בזיון בית משפט[141] או בדרך של חקירה והעמדה לדין בגין עבירה של הפרת הוראה חוקית.[142] מבחינה תאורטית ניתן גם לקבוע עבירה פלילית ייעודית וספציפית, בדומה לנקבע בבריטניה בכל הנוגע לסירוב למסור את מפתח ההצפנה או הסיסמה.[143]

דרך הפעולה **השנייה**, אשר הוזכרה לעיל בהקשרים שונים, היא השימוש בכוח נגד החשוד או העד בכוונה להתגבר כך על אמצעי אבטחת המידע. דרך פעולה זו רלוונטית רק בתנאי שמפתח ההצפנה או הסיסמה מונגשים באמצעות זיהוי פנים או טביעת אצבע. מטבע הדברים, בכל הנוגע לקוד תווי, דגימת קול או דפוס השימוש של הנחקר במכשיר – סיסמה או מפתח הצפנה מן הסוגים הללו אינם ניתנים לנטילה בשימוש בכוח סביר.[144] במילים אחרות, השאלה אם ניתן להשתמש בכוח נגד החשוד או לא היא שאלה התלויה, הלכה למעשה, בטכנולוגיה שבה בחר החשוד להגן על הטלפון הסלולרי, על המחשב או על היישום המקוון שלו. עוד יצוין כי הסמכות להשתמש בכוח סביר נוגעת למארג זכויות אחר העומד לחשוד – לאו דווקא החיסיון מפני הפללה עצמית כי אם הזכות לכבוד ולשלמות הגוף – ואנו לא נרחיב בסוגיה זו בגדרי מאמר זה.[145]

141 סעיף 6 לפקודת בזיון בית משפט קובע את הסנקציות שבית המשפט רשאי להטיל על אדם שמסרב להישמע להוראות בית המשפט, וביניהן גם מאסר. כדוגמה להטלת עונש מאסר על בסיס פקודת בזיון בית משפט ראו ע"פ 7174/09 **רייפמן נ' ארז** (נבו 21.9.2009), שם דחה בית המשפט העליון את בקשתו של המבקש לעיכוב ביצוע עונש מאסר של 45 יום שהוטל עליו בגין אי־קיום צו שיפוטי שהורה לו להעביר את מניותיו בחברה לידי המנהל המיוחד.

142 ס' 287(א) לחוק העונשין, הקובע כי "המפר הוראה שניתנה כשורה מאת בית משפט או מאת פקיד או אדם הפועל בתפקיד רשמי ומוסמך לאותו ענין, דינו – מאסר שנתיים".

143 ראו לעיל ה"ש 119–120.

144 במקום אחר דנו בהרחבה בדבר הדרך הפרשנית שיש לנקוט לדעתנו, בהתבסס על ס' 45 לפסד"פ, כדי לאפשר שימוש בכוח שכזה, ודנו בהצדקות לדרך פעולה כזאת ובאופן ההתמודדות עם הביקורות שעשויות להתעורר נגד פרקטיקה זו. להרחבה ראו ויסמונסקי ואיתן "השימוש בכוח סביר", לעיל ה"ש 16.

145 השוו לחוק נטילת אמצעי זיהוי, המבחין בין מקרים שבהם ניתן לדרוש מנחקר להשתתף בחיפוש חיצוני או פנימי כהגדרתו בחוק, וכי סירובו יעלה כדי עבירה שדינה שנתיים מאסר (עבירה הדומה במהותה לעבירה של הפרת הוראה חוקית), לבין מקרים שבהם ניתן לאסוף את המידע הדרוש מהנחקר ללא

דרך הפעולה **השלישית** היא הסקת מסקנה שלילית, לחובת החשוד (ולא העד, כפי שיוצג בהמשך) בשל אי־שיתוף הפעולה שלו עם רשויות אכיפת החוק. במילים אחרות, הכוונה ל״השלמת״ המידע החסר לרשויות אכיפת החוק באמצעות סירובו של החשוד לשתף פעולה. מבחינה עיונית ניתן לחלק דרך פעולה זו לכמה רמות של ״השלמה״ בסדר ״משלימות״ עולה: חיזוק לראיות התביעה, סיוע לראיות התביעה ואף יצירת חזקה הניתנת לסתירה לחובת החשוד בכל הנוגע למידע קונקרטי שהתבקש החשוד למסור ושלגביו בחר להימנע מלשתף פעולה עם חוקריו.

אשר לקביעה כי תקום תוספת ראייתית מסוג ״דבר לחיזוק״, הוראות ברוח זו נהוגות במשפט הישראלי בכל הנוגע לסירוב החשוד להשתתף בהליכי החקירה. כך הוא למשל בכל הנוגע לשמירה על זכות השתיקה בחקירה,[146] סירוב להשתתף בעימות או במסדר זיהוי,[147] ועל פי הצעת חוק החיפוש, כך יהיה גם במקרה של סירוב חשוד למסור את הסיסמה או את מפתח ההצפנה.[148]

אשר לדרגה הגבוהה יותר של ״משלימות״, שלפיה תקום תוספת ראייתית מסבכת מסוג ״סיוע״ במקרה של סירוב למסור את הסיסמה או את מפתח ההצפנה, גם כאן ניתן למצוא מקורות משפטיים בדין הישראלי הנוקטים גישה זו במצבים מסוימים של אי־שיתוף פעולה מצידו של חשוד או נאשם. כך הוא למשל בכל הנוגע להימנעותו של נאשם מלהעיד בבית המשפט במסגרת פרשת ההגנה.[149]

אשר לרמה הגבוהה ביותר של השלמה, של קביעת אשם במקרה של סירוב למסור את מפתח ההצפנה או הסיסמה, ייאמר מייד כי היא אינה נוהגת, ככלל, בשיטת משפטנו. ברמה העיונית ניתן לבסס השלמה זו על דוקטרינה שפותחה במשפט המקובל והשתרשה במשפט האמריקני במאה התשע־עשרה בשם "The Missing Witness Instruction".[150] דוקטרינה זו מאפשרת לבית המשפט להסיק מסקנה נגד צד שהיה אמור להביא עד מטעמו, אך החליט לבסוף שלא להביאו. ג׳ון לארקין (Larkin) הציע להשתמש בדוקטרינה זו גם בהקשר של פיצוח הצפנות והגנות סיסמה. לטענתו, ניתן להשתמש בדוקטרינה זו במקרים שבהם שימוש בכלים של ביזיון בית המשפט או חיזוק וסיוע לראיות התביעה אינם מספקים תמריץ מדויק מספיק לחשוד למסור את מפתח ההצפנה או את הסיסמה. במקרים אלה יהא בית המשפט רשאי לאפשר לתביעה לדרוש מידע מסוג ספציפי מידי הנאשם. אם יסרב הנאשם

הסכמתו, בשימוש בכוח סביר. סעיף 12(א) לחוק נטילת אמצעי זיהוי קובע את המקרים שבהם החשוד המסרב לחיפוש פנימי או חיצוני יעבור עבירה פלילית. סעיף 3(ב) לחוק נטילת אמצעי זיהוי מאפשר לרשות החוקרת לבצע סוגים מסוימים של חיפושים חיצוניים בשימוש בכוח סביר במקרה שבו החשוד מסרב לחיפוש, לאחר שיובא לפני קצין משטרה ולאחר שישמיע את טעמי סירובו ויובהר לו כי ניתן לבצע את החיפוש בכוח. כאמור, בעניין זה הרחבנו במקום אחר. ראו ויסמונסקי ואיתן ״השימוש בכוח סביר״, לעיל ה״ש 16.

146 ע״פ 230/84 **חג׳בי נ׳ מדינת ישראל**, פ״ד לט(1) 785 (1985).

147 ע״פ 4988/08 **פרחי נ׳ מדינת ישראל**, פ״ד סה(1) 626, פס׳ 22 לפסק דינו של השופט לוי (2011).

148 ראו ס׳ 95(ג) להצעת חוק החיפוש.

149 ס׳ 162 לחסד״פ. ליישום בפסיקה ראו ע״פ 2132/04 **קייס נ׳ מדינת ישראל**, פס׳ 33–41 לפסק דינה של השופטת פרוקצ׳יה (נבו 28.5.2007), והמובאות שם.

150 Graves v. Unites Stats, 150 U.S. 118 (1893).

להמציא את המידע לרשויות התביעה, הרי שבית המשפט יראה במידע ככזה אשר תומך בתזה של התביעה בעניין תוכנו.[151] לדוגמה, במקרה של החזקת חומר תועבה פדופילי יהיה אפשר לבקש מהנאשם להמציא את כל התמונות האגורות בחומרי המחשב שלו, וסירובו לעשות כן יתמוך בתזה של התביעה שהתמונות הללו הן תמונות הכוללות חומר תועבה פדופילי. עם זאת נראה כי גישתו זו של לארקין לא אומצה בשיטות המשפט השונות, ככל הנראה בשל העובדה שגישה זו מגלמת פגיעה בזכותו של החשוד (ולימים הנאשם) להליך הוגן.

במאמר מוסגר יצוין עוד כי במקרה אחד לפחות במשפט הפלילי בישראל הוכרה הוראה דומה במקרה של סירוב הנחקר להשתתף בהליכי חקירה – במקרה של ״חזקת השכרות״ הקמה נגד נהג המסרב לבצע בדיקת אלכוהול. פקודת התעבורה קובעת כי במקרה שבו סירב הנוהג ברכב לתת דגימה של אוויר נשוף, יוחזק הנהג בכל מקרה כמי שנהג בשכרות ובכך ביצע עבירה פלילית של נהיגה בשכרות לפי סעיף 62(3) לפקודת התעבורה.[152] בית המשפט העליון דן בעבר בסעיף 64ד לפקודת התעבורה, הקובע את ״חזקת השכרות״, וקבע כי תכלית הסעיף היא ״למנוע מחשודים להתחמק מדרישת שוטר להיבדק [...] קרי, לצמצם פרצות בגדר האכיפה, לשים סייג לאפשרות לחמוק מהן״.[153]

ראוי להבחין דרך פעולה זו – של הסקת מסקנה שלילית בשל אי־שיתוף פעולה – משתי דרכי הפעולה הקודמות שנמנו לעיל. **ראשית**, כאמור לעיל, דרך הפעולה גובה מחיר מחשודים בלבד ולא מעדים. במילים אחרות, אין בכוחה לתמרץ עד למסור את הסיסמה או את מפתח ההצפנה שלו או להנגיש את חומרי המחשב שלו כשהם מפוענחים. אומנם מרבית העדים צפויים לשתף פעולה במסגרת חקירות, אולם אפשר שייחקרו גם עדים עוינים, שצורכי החקירה מחייבים עיון בחומרי מחשב שלהם. **שנית**, ככל שעולים במחיר שגובה דרך הפעולה הזאת מהחשוד המסרב למסור את סיסמתו או את מפתח ההצפנה שלו, כך גובר החשש להפללת חף מפשע ולתוצאה משפטית שגויה. לעיתים המוטיבציה לסרב למסור את הסיסמה או את מפתח ההצפנה יכולה לנבוע מחשש שיתגלה מידע אישי רגיש במיוחד על החשוד או על צד ג שהחשוד חפץ ביקרו. כיוון שכך, לא ניתן להניח הנחה חד־ערכית כי החשוד־הסרבן הוא בהכרח החשוד־האשם. יתרה מזאת, השימוש בדרך הפעולה הזאת לא תמיד יאפשר להגדיר במפורש את היקף העבירה ואת טיבה. ניטול לדוגמה מקרה של חשוד בעבירה של החזקת חומרי תועבה פדופיליים, לפי סעיף 214(ב3) לחוק העונשין. במקרה שבו החשוד יסרב לאפשר לחוקרים גישה אל מחשבו, אל הטלפון הסלולרי שלו או אל השירות המקוון שבו הוא משתמש כיוון שלא ימסור להם את הסיסמה או את מפתח ההצפנה, הרי שגם אם ניישם את ההשלמה ה״מחמירה״ ביותר בדרך פעולה זו, של קביעת אשם בגין הסירוב של הנחקר לשתף פעולה, עדיין ייתכן שלא יהיה אפשר לדעת כמה מידע מחזיק החשוד, מאיזה סוג (סרטים או תמונות), ובעיקר – מה חומרת

151 ראו Larkin, לעיל ה״ש 30, בעמ׳ 276–277.

152 ס׳ 62(3), 64ד לפקודת התעבורה [נוסח חדש].

153 רע״פ 8135/07 **גורן נ׳ מדינת ישראל**, פס׳ ל״ה–ל״ו לפסק דינו של השופט (כתוארו אז) רובינשטיין (נבו 11.2.2009).

התוכן.[154] **שלישית**, בכל הנוגע לשתי רמות ה״משלימות״ הראשונות שמנינו לעיל – של חיזוק או סיוע לראיות התביעה – עשויים להיות מקרים לא־מעטים שבהם תוספות ראייתיות אלה למעשה לא יחזקו ולא יסייעו לדבר, שכן לא תימצא ראיה עיקרית לחובתו של החשוד. ייתכנו מקרים שבהם הראיות היחידות הרלוונטיות להוכחת אשמתו של החשוד תימצאנה במחשב, בטלפון הסלולרי או ביישום המקוון אשר אליו רשויות החקירה אינן מסוגלות לגשת. במקרים אלה סירובו של החשוד לאפשר את העיון בחומרי המחשב המפוענחים שאינם מוגני־סיסמה אומנם יוביל לחיזוק או לסיוע נגדו, אולם בה בעת הסירוב ימנע השגה של ראיות עיקריות נגדו.

דרך הפעולה **הרביעית** לעקיפת ה״התנגשות״ בין צורכי החקירה לבין החיסיון מפני הפללה עצמית מתמקדת בביצוע תחבולות בחקירה, בין פרונטלית מול הנחקר ובין בחקירה הסמויה ובלא ידיעתו. תחבולות אלה יאפשרו לרשות החוקרת להשיג את הסיסמה או את מפתח ההצפנה למחשב, לטלפון הסלולרי או לשירות המקוון.[155] כדוגמה לתחבולות בחקירה הסמויה ניתן לציין למשל פעולות של האזנת סתר או ניטור הקלדות מקלדת (באמצעות שימוש ב־Key Logger) שיאפשר לרשות החוקרת לגלות מבעוד מועד את הסיסמה או את מפתח ההצפנה של החשוד או העד. דוגמה אחרת במסגרת החקירה הגלויה אפשר למצוא במקרים שבהם אמצעי האבטחה שבו השתמש החשוד או העד הוא זיהוי פנים. במקרה כזה יוכל החוקר להציג את מכשיר הטלפון הסלולרי מול פניו של הנחקר מבלי שישים לב לכך, וכל עוד הדבר עומד במבחני התחבולה הנהוגים[156] – נראה שיהיה

154 חומרת התוכן הפדופילי היא אחד מהשיקולים העיקריים בבואה של הפרקליטות להחליט על העמדה לדין ובבואו של בית המשפט לגזור את עונשו של הנאשם (הגם שאין לחומרת התוכן משמעות ראייתית כזו או אחרת לשאלת עצם ההרשעה בעבירה). ראו ס׳ 14(2) להנחיית פרקליט המדינה 2.22 ״פרסום, החזקה וצריכה של חומר תועבה ובו דמותו של קטין״ (31.8.2016). עם זאת, השוו ת״פ (שלום ראשל״צ) 42667-02-15 **מדינת ישראל נ׳ לוריא** (נבו 15.1.2017), שם הורשע הנאשם בהחזקת תוכן פדופילי שהיה מוצפן, חרף העובדה שהרשות החוקרת, התביעה, ההגנה ובית המשפט לא עיינו בקבצים אלה. לביקורת על פסיקה זו ראו אסף הרדוף ״קבצים מוצפנים, חוק מוצפן – על מונח התועבה ועל הרשעה בהחזקת חומר תועבה ללא עיון בחומר – בעקבות ת״פ 42667-02-15 מדינת ישראל נ׳ לוריא״ **המשפט ברשת: זכויות אדם** 70, 5 (2017).

155 בבסיסו של מודל זה ניתן להציב את העמדה המוכרת שביטא השופט ויתקון בע״פ 216/74 **כהן נ׳ מדינת ישראל**, פ״ד כט(1) 340, 352–353 (1974): ״חקירתו של פושע אינה משא־ומתן בין שני סוחרים שלווים והגונים המנהלים את עסקם על בסיס אמון הדדי מירבי [...] מחוקר משטרה המשתדל לדובב חשוד [...] אין אני דורש ׳הגינות׳ כזאת. זכותו של חשוד היא לשתוק ולא ל׳הישבר׳; זכותו וחובתו של חוקר להשתמש באמצעים סבירים כדי להשיג מהנחקר ידיעה״.

156 בכל הנוגע למבחנים במשפט הישראלי בעניין תחבולה מותרת ראו ע״פ 2831/95 **אלבה נ׳ מדינת ישראל**, פ״ד נ(5) 221, פס׳ 57–59 לפסק דינו של השופט (כתוארו אז) מצא (1996), שם נקבע כי ככלל רשאיות רשויות אכיפת החוק לבצע תחבולות בזמן החקירה כל עוד יעמדו בשני סייגים עיקריים: הראשון הוא שלא תופר זכותו של החשוד להימנע מהפללה עצמית; השני הוא שלא ינקטו אמצעי חקירה שהשימוש בהם פוגע ״בשורת עשיית הצדק״. עוד נפסק כי ״תחבולה נפסדת היא תחבולה השומטת את הקרקע תחת יכולתו של הנחקר לעשות שימוש בזכות השתיקה ובזכותו להימנע מהפללה עצמית, ולמעשה שוללת, על רקע המצג הכוזב שבבסיסה, את יכולת הבחירה של הנחקר אם למסור הודאתו אם לאו״. ראו לעניין זה את ע״פ 4109/15 **מירז נ׳ מדינת ישראל**, פס׳ 25 לפסק דינו של השופט זילברטל (נבו 9.7.2017). עוד ראו בהקשר זה את יישום המבחנים בע״פ 1301/06 **עזבון אלזם נ׳ מדינת**

אפשר לומר שמדובר בתחבולה לגיטימית בחקירה שמטרתה להשיג את המידע המוגן באמצעות הסיסמה או את מפתח ההצפנה. כדוגמאות לתחבולות פוטנציאליות אחרות העשויות להוביל לאיתור הסיסמה או מפתח ההצפנה (אם כי הדבר תלוי בהתפתחויות טכנולוגיות) ניתן למנות את שתי אלה: האחת, נניח כי הרשות החוקרת תוכל לקחת את טביעת אצבעו של נחקר מכוס ששתה ממנה ולהיעזר בטכנולוגיה מתקדמת כדי להופכה למודל טביעת אצבע שמאפשר פתיחתו של טלפון סלולרי; השנייה, נניח שהרשות החוקרת תגרום לנחקר לדבר במהלך חקירה מוקלטת, ולאחר מכן באמצעות שימוש בכלים טכנולוגיים מתקדמים יומרו דבריו והוא יחזור אפוא על מילת הקוד בקולו שבאמצעותה ניתן לפתוח את מכשיר הטלפון הסלולרי.

דרך פעולה זו מעוררת מעט קשיים יחסית בכל הנוגע לחיסיון מפני הפללה עצמית. אומנם תחבולה מביאה את הנחקר להפליל הלכה למעשה את עצמו או אחרים באמצעות דבריו או מעשיו, אולם כל עוד התחבולה לא שללה מהנחקר את חופשיות הרצון שלו, הרי שאין בכך כדי לפגוע בתקפותה.[157] עם זאת הקושי בדרך פעולה זו נעוץ בעובדה שהוא מספק פתרון חלקי בלבד לקושי שנוצר לרשויות אכיפת החוק. הצלחתה של התחבולה תלויה במידת היצירתיות של צוות החקירה ובאופן התנהלותו של הנחקר, ועל כן דרך פעולה זו אינה מעניקה ודאות מספקת המאפשרת להבין את נקודת האיזון החוקתי העקרוני שהתבצע בין צורכי החקירה מחד גיסא, לבין החיסיון מפני הפללה עצמית מאידך גיסא. כמו כן כפי שראינו, חלק מהתחבולות דורשות יכולות טכנולוגיות ופורנזיות, וחלקן אף תלויות בפיתוחים טכנולוגיים עתידיים. על כן, השימוש בתחבולות מצריך הכשרה ייעודית והצטיידות במכשור תואם ברשויות החקירה, במיוחד בשים לב לכך שטכנולוגיות אבטחת מידע עשויות להתפתח בקצב מהיר מזה שבו רשויות אכיפת החוק יכולות להצטייד בטכנולוגיה נגדית, שכן חברות ענק כמו Apple או Google עוסקות ללא הרף בפיתוח טכנולוגיות מתקדמות יותר ויותר להגנה על פרטיותם של המשתמשים בהן.[158]

דרך הפעולה **החמישית** תאפשר לרשויות החקירה לפנות לצד ג המחזיק באפשרות הגישה אל חומר המחשב הדרוש ולקבל ממנו את הגישה הישירה אל המידע.[159] ידוע כי רשויות החקירה האמריקניות פנו כמה פעמים בעבר להשיג גישה למידע ממוחשב של חשוד דרך צד ג, בדרך כלל מדובר בחברות הטכנולוגיה הגדולות. למשל, בפרשת סן ברנרדינו שהוזכרה לעיל בפרק המבוא פנתה ה־FBI לחברת Apple בבקשה שזו תסייע לה

ישראל, פ״ד סג(2) 177, פס׳ 5–9 לפסק דינה של השופטת (כתוארה אז) חיות (2009), שם קבע בית המשפט העליון כי שכנוע המדובבים את הנאשם להחליף את סנגורו, הוא תחבולה אסורה בחקירה, וכך גם כאשר ניסו המדובבים לשכנע את הנאשם שלא לשמור על זכות השתיקה.

157 שם.

158 להרחבה על הפיגור המובנה של רשויות אכיפת החוק אחר התפתחות הפשיעה המקוונת ראו Marc C. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J. L. & TECH. 465, 482–488 (1997).

159 להרחבה ראו ויסמונסקי **חקירה פלילית**, לעיל ה״ש 22, בעמ׳ 218.

לעיין בתוכנו של המכשיר הסלולרי.[160] כך נעשה גם בפרשה נוספת בארצות הברית, שם ביקשה ה־FBI מחברת Google כי תמסור לה את סיסמת הכניסה למכשיר הטלפון הסלולרי של החשוד.[161]

בדרך פעולה זו ניתן להבחין בין כמה סוגי מעקפים: **האחד**, קבלת המידע מידיו של בעל גישה חוקית אחר המשתמש גם הוא באותו חומר מחשב או המחזיק בגישה כדין אל המידע; **השני**, קבלת המידע מהחברה המייצרת את המחשב או את הטלפון הסלולרי או מעניקה את השירות המקוון; **השלישי**, חיוב החברה המייצרת את המחשב או את הטלפון הסלולרי או המעניקה את השירות המקוון ביצירת ״דלת אחורית״ שתאפשר לרשויות לגשת דרך קבע למידע.

אשר למעקף מן הסוג **הראשון**, דומה כי כאן אין מתעוררת כל התנגשות עם החיסיון מפני הפללה עצמית. עם זאת יש לשים לב כי לא תמיד יימצא בעל גישה חוקית נוסף כאמור.

אשר למעקף מן הסוג **השני**, כאן עשויות להתעורר כמה סוגיות: הסוגיה **הראשונה** היא שלא תמיד יהיה באפשרותה הטכנית של החברה לגשת אל המידע. לפי המעקף מן הסוג השני, הרשות החוקרת אומנם דורשת מהחברה לסייע בידה, אולם אין היא יכולה לגרום לחברה לשנות את האופן שבו מערכותיה מעוצבות מלכתחילה. אם המערכות מעוצבות באופן שלא ניתן, במאמץ סביר, לגשת אל המידע של ה״לקוח״, קרי החשוד או העד במקרה שלפנינו, הרי שגם אם תוכר הסמכות לדרוש סיוע כאמור, לא יהיה אפשר, מעשית, לספק את הסיוע. מלבד זאת, בשנים האחרונות החלו חברות האינטרנט הגדולות, ובראשן Apple, להימנע במכוון משמירת סיסמת הכניסה או מפתח ההצפנה של לקוחותיהן.[162] גם שירות WhatsApp הפופולרי החל, משלב מסוים, להצפין מקצה לקצה את כל התעבורה בין המשתמשים, והוא אינו שומר ברשותו את מפתח ההצפנה או התוכן המועבר בין המשתמשים.[163]

160 למעשה, באותו עניין הייתה בקשתה של ה־FBI מרחיקת לכת יותר – הסוכנות ביקשה מחברת Apple לייצר גרסה חדשה של מערכת ההפעלה כדי שניסיונות הפריצה של ה־FBI לא יובילו למחיקת המידע מהטלפון הסלולרי.

161 Affidavit in Support of Search Warrant Application, *In re* Search of Google Inc., No. 3:12-mj-00882-NLS (S.D. Cal. 9, 2012), https://bit.ly/3mU7DJ1.

162 לסקירה על שינוי מדיניות זו של חלק מחברות האינטרנט הגדולות ראו שם, בעמ׳ 8. כן ראו Orin Kerr, *Apple's Dangerous Game*, WASH. POST (Sep. 9, 2014), https://tinyurl.com/y6kwebju. קר טען במאמרו נגד מדיניותה של חברת Apple שלא לשמור את הסיסמאות ומפתחות ההצפנה של לקוחותיה, ובהמשך שינה מעט מעמדתו זו. ראו Orin Kerr, *Apple's Dangerous Game, part 2: The Strongest Counterargument*, WASH. POST (Sep. 22, 2014), https://tinyurl.com/y34qow65.

163 כך למשל, מדיניותה הרשמית של חברת WhatsApp, המצפינה את התוכן אשר מועבר בין לקוחותיה גם כלפי עצמה ומוחקת אותו משרתיה. ראו *WhatsApp Terms Of Service*, WHATSAPP (2021), https://bit.ly/3arpH76. הסעיף הרלוונטי בתנאי השימוש קובע כך: "We do not retain your messages in the ordinary course of providing our Services to you. Once your messages (including your chats, photos, videos, voice messages, files, and share location information) are delivered, they are deleted from our servers. Your messages are stored on your own device".

הסוגיה **השנייה** נוגעת לעובדה שעצם הסמכות לחייב את החברה לספק את המידע כאמור מטילה נטל על צד ג שאינו צד להליך הפלילי. ״החצנה״ זו של פעולת החקירה ועירובו של צד ג, שהוא בדרך כלל חברה פרטית שאינה קשורה כלל לחקירה – מגלמת פגיעה מסוימת באותו צד ג. בהקשר זה כדאי לציין את פרשת **מפקד מחוז תל־אביב יפו במשטרת־ישראל**, שבה דן בית המשפט העליון בשאלה אם רשאית משטרת ישראל להסתייע בספקיות הגישה לאינטרנט כדי להגביל גישה של משתמשיהן לאתרי אינטרנט המשמשים להימורים אסורים בהתאם להוראת סעיף 229 לחוק העונשין (שבוטל בינתיים), שהסמיך מפקד מחוז להורות על סגירת מקום המשמש לארגון הימורים, הגרלות או משחקים אסורים. בית המשפט העליון קבע ברוב דעות כי המשטרה אינה רשאית להסתמך על סעיף החוק האמור, ועל המחוקק, אם יסבור שכך ראוי, לקבוע בחקיקה ראשית מפורשת את הסמכות לדרוש מספקיות הגישה לאינטרנט לחסום גישה כאמור.[164]

שאלת ההחצנה בכפייה של פעולות החקירה לחברות האינטרנט מתעוררת כמובן רק במקרה שבו חברת האינטרנט מסרבת לציית להוראה שניתנת לה וטוענת לפגיעה מיוחדת בה המצריכה הסמכה מפורשת. לעיתים מושג שיתוף פעולה עם חברת האינטרנט והסוגיה אינה מתעוררת אפוא. למשל, בשנת 2009 דרשה ה־FBI מחברת Google למסור לידיה מסמכים שאוחסנו בשרתיה (באמצעות שירות Google Drive) וחברת Google צייתה לצו. בשנת 2011 אישר דובר מטעם חברת Dropbox כי גם הם מעסיקים מספר מצומצם של עובדים אשר רשאים לגשת לכלל המידע האגור בשרתי החברה כדי לציית לצווים שיפוטיים שיוציאו להם רשויות החקירה בארצות הברית.[165]

הסוגיה **השלישית** היא סוגיית הפגיעה בציבור משתמשי המחשב והרשת, לקוחותיהן של חברות האינטרנט, שתחושת החירות־מפני־מעקב שלהם תיפגע במידה ניכרת. פגיעה זו תיצור אפקט מצנן של פן אופטיקון[166] על כל משתמשי המחשב והרשת. האמון הבסיס של המשתמשים בחברות המספקות להם את השירותים – ייפגע אסטרטגית.[167]

164 עע״מ 3782/12 **מפקד מחוז תל אביב־יפו במשטרת ישראל נ׳ איגוד האינטרנט הישראלי**, פ״ד סו(2) 159, פס׳ 14 לפסק דינו של השופט פוגלמן (2013). ובלשונו של בית המשפט: ״לא ניתן – בהיעדר הסדר חקיקתי מתאים – להעניק סמכויות אכיפה למי שאיננו חלק ממערך האכיפה. סמכות האכיפה הפלילית היא מן הסמכויות המובהקות של המדינה. בגדרי סמכות זו, המדינה מגשימה את אחריותה לאכיפת החוק הפלילי על־ידי כך שהיא מבצעת בעצמה את תפקיד האכיפה הפלילית. המדינה היא אף זו שמפעילה את כוח המרות השלטוני כלפי הפרט בהליך הפלילי. משכך, המדינה – כמי שגיבשה את נורמות ההתנהגות וכמי שמופקדת על אכיפתן – היא הגורם האחראי באופן ישיר על הריסון ועל המעצורים הנדרשים בהפעלת הכוח. היא הגורם שאמור לתת דין וחשבון לציבור על אופן ביצוע סמכויותיה בהליך הפלילי״. יוער כי לאחר פרסום פסק הדין אכן נחקק חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע״ז–2017, שבו נקבעה במפורש הסמכות של שופט בית המשפט המחוזי שהוסמך לכך, להורות בצו על חסימת גישה לאתרי אינטרנט הכוללים עבירות של ארגון הימורים אסורים ועבירות נוספות.

165 Wachtel, לעיל ה״ש 134, בעמ׳ 44–45.

166 על הפן אופטיקון כתב במקור ג׳רמי בנת׳האם (Bentham), ומישל פוקו (Foucault) חזר אל המודל הארכיטקטוני של הפן אופקטיקון. כן ראו OSCAR H. GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993), שם המחבר דן בפן אופטיקון בשל השימוש ההולך וגובר בטכנולוגיות מעקב ובמחשוב, נכון לתקופת כתיבת הספר. ראו גם מיכאל בירנהק ״שליטה

עוד ראוי לציין בהקשרנו זה כי לאחרונה פרסמו ממשלותיהן של ארצות הברית, בריטניה, קנדה, אוסטרליה וניו זילנד (מדינות ה־Five Eyes) הצהרה משותפת, העוסקת בשאלת אחריותן של חברות פרטיות לפתרון בעיית הגישה של רשויות אכיפת החוק למידע מוצפן.[168] באותה הצהרה קבעו הממשלות כי על חברות הטכנולוגיה הפרטיות מוטלת אחריות משותפת, גם עם ממשלות, לפתרון בעיית הגישה האמורה למידע.

אשר למעקף מן הסוג **השלישי**, בדבר חיוב החברה המייצרת את המחשב, את הטלפון הסלולרי או המעניקה את השירות המקוון ביצירת ״דלת אחורית״ שתאפשר לרשויות לגשת דרך קבע למידע – כאן ללא ספק מדובר בפגיעה הרחבה ביותר בחברה, שכן מדובר בהתערבות יסודית בארכיטקטורה של המוצרים שאותם מספקת החברה ובתהליכי הפיתוח והייצור של החברה, והכול לתועלתן של רשויות האכיפה. יתרה מזאת, פעולה זו אף מגלמת את הפגיעה הרחבה ביותר בכלל ציבור המשתמשים בדרך של הגברת תחושת המעקב (הפן אופטיקון). המעקף השלישי מגלם, ללא ספק, את הפגיעה ההיקפית הקולקטיבית הקשה ביותר בציבור המשתמשים בשירותיהן של חברות האינטרנט.

החקיקה הרוסית והחקיקה הסינית מחייבות את חברות האינטרנט והטכנולוגיה הפועלות בשטחן לפענח מידע מוצפן עבור הממשלה, לפי דרישה, ולא רק להמציא מידע שנגיש להן מלכתחילה.[169] לעומת זאת ברוב מדינות המערב מוכרת ההבחנה בין חברות פרטיות לחלוטין, שאז הפגיעה בחופש העיסוק שלהן, בקניינן ובחובת הנאמנות שלהן ללקוחותיהן מוגברת, לבין חברות שניתן לראות בהן משום גופים דו־מהותיים, כיוון שהן מקבלות רישיון מטעם המדינה למשל, או כיוון שהן מספקות שירות חיוני שהוא בבחינת משאב ציבורי. בהקשר זה ניתן לציין למשל את הוראת סעיף 13(ב)(2) לחוק התקשורת (בזק

והסכמה: הבסיס העיוני של הזכות לפרטיות״ **משפט וממשל** יא 9, 60–67 (2007); ויסמונסקי **חקירה פלילית**, לעיל ה״ש 22, בעמ׳ 263–264.

167 Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties are Forced to Hand Over Passwords*, 30 BERKELEY TECH. L.J. 1, 9–16 (2015).

168 FIVE COUNTRY MINISTERIAL, STATEMENT OF PRINCIPLES ON ACCESS TO EVIDENCE AND ENCRYPTION (Aug. 30, 2018), https://bit.ly/3mF5iBk.

169 LEWIS, ZHENG & CARTER, לעיל ה״ש 38, בעמ׳ 18–21. להרחבה בנוגע למשטר המשפטי הרוסי ראו Federal'nyĭ Zakon RF o Grazhdanstve Rossiĭskoĭ Federatsii [Federal Law of the Russian Federation on the Federal Security Service of the Russian Federation], ROSSIĬSKAIA GAZETA [ROS. GAZ.], art. 15, Feb. 22, 1995 (Russ.), *Translation available at* https://bit.ly/3AqvWTv (שכותרתו Collaboration with Russian and foreign establishments, קובע כך: "Physical persons and legal entities in the Russian Federation providing postal communications services and electronic communications services of all types, including scrambled, confidential, satellite communications systems, shall be under obligation, at the request of federal security service organs, to include in the apparatus additional hardware and software and create other conditions required by federal security service organs to implement operational/technical measures"). להרחבה בנוגע למשטר המשפטי הסיני ראו Christopher T. Cloutier & Jane Y. Cohen, *Casting a Wide Net: China's Encryption Restrictions*, WORLDECR (Aug. 2, 2012), https://bit.ly/3iHA8bd (במאמר נסקרת האסדרה הסינית בנושא הצפנה, אשר מגבילה הכנסה של הצפנה מסוגים רבים אל תחומי המדינה, בין היתר הצפנה של טלפונים סלולריים ומחשבים).

ושידורים), התשמ״ב–1982, הקובעת שראש הממשלה רשאי להורות לבעלות רישיון בזק להתקין מתקן או לבצע התאמה טכנולוגית למתקן בזק, לרבות מתן גישה למתקן הבזק, והכול כדי לאפשר לרשויות הביטחון, בכלל זה המשטרה, למלא את תפקידיהן. ההוראה חלה על ספקיות התקשורת (טלפונית, סלולרית, גישה לאינטרנט) בעלות רישיון בזק בלבד, ומכאן שהיא מוגבלת בהיקף פריסתה. במילים אחרות, סמכות איסוף זו קיימת במשפט הישראלי חלקית בלבד. בארצות הברית קיימת חקיקה משנת 1994 המחייבת ספקיות תקשורת לבנות תשתית טכנולוגית שתאפשר לרשויות החקירה ביצוע האזנות סתר.[170] גם בבריטניה יש הוראות חוק המתייחסות לסוגיית החיוב של ספקיות תקשורת, ובכללן ספקיות גישה לאינטרנט, לבנות תשתית טכנולוגית שתאפשר לרשויות החקירה האזנת סתר.[171]

לאחרונה עברה באוסטרליה חקיקה חדשה, המגלמת במידה מסוימת חריגה מהגישה הנהוגה במדינות המערב. בדצמבר 2018 התקבל חוק בשם The Telecommunications and Other Legislation Amendment (Assistance and Access) Act (2018).[172] חוק זה מטיל חובה על חברות המספקות שירותי תקשורת המוצפנים מקצה אל קצה (כגון WhatsApp או iMessage) לבנות ״דלת אחורית״ שתאפשר לרשויות החקירה והביטחון גישה לתוכן המועבר בתווך המוצפן. החקיקה האוסטרלית אף מטילה קנסות על חברות שלא תיענינה לדרישות החוק, ומאפשרת לרשויות החקירה והביטחון גם לפנות ישירות לעובדים ספציפיים בחברות הפרטיות אגב הטלת סנקצייה עונשית במקרה של אי־ציות של העובד.[173]

הנה כי כן, דרך פעולה זו כוללת מדרג של רמות שונות של ״עקיפה״. ברמה הנמוכה ביותר אין מתעוררים קשיים משפטיים ניכרים, אולם רמה זו מספקת פתרון חלקי ביותר לצרכיה של הרשות החוקרת, כיוון שמטבע הדברים לא תמיד יהיה אפשר להשיג בדרך זו גישה לסיסמה או למפתח ההצפנה. ככל שעולים, עד לרמה השלישית, גוברים ״מחיר״ הפגיעה בפרטיותם של כלל משתמשי המחשב והרשת והאפקט המצנן המוגבר על פעילותם. נוסף על כל האמור, יש לזכור כי אף אם מדינה מסוימת הייתה מיישמת את כל הרמות אשר הוצגו לעיל, עדיין לא היה בכוחה לכפות את סמכותה על חברות אינטרנט זרות שאינן פועלות בשטחה מבחינה פיזית אך מספקות שירותים למשתמשים בשטחה. במקרה

170 47 U.S.C. §1001-1010.

171 ראו Regulation of Investigatory Powers Act, 2000, c. 23, §12 (Eng.).

172 *The Telecommunications and Other Legislation Amendment* (Assistance and Access) Act 2018 (Austl.).

173 לא ברור כיצד, אם בכלל, מתכוונת אוסטרליה לאכוף את החוק על חברות זרות המספקות שירותים מקוונים הזמינים לתושבי המדינה. לביקורת נוספת על החקיקה האוסטרלית ראו למשל Lily Hay Newman, *Australia's Encryption-Busting Law Could Impact Global Privacy,* WIRED (June 7, 2018), https://tinyurl.com/y87reuod. ראו גם Herbert Smith Freehills LLP, *The Assistance and Access Act 2018: The Crypto Wars' Final Act for 2018,* LEXOLOGY (Dec. 11, 2018), https://tinyurl.com/1cxnl7pe.

כזה באפשרותה של המדינה מבחינה טכנית לחסום גישה אל השירותים של אותה חברה זרה,[174] אולם יש לזה מחיר חוקתי כבד במיוחד ולא מוצדק.[175]

הצגנו אפוא חמש דרכי פעולה פרקטיות המבקשות לעקוף את ההתנגשות החזיתית עם החיסיון מפני הפללה עצמית של הנחקר. ה״עקיפה״ באה לידי ביטוי בכך שעל פי כל אחת מדרכי הפעולה שמנינו לעיל, נמנע החוקר ממתן הוראה ישירה לנחקר למסור את הסיסמה, את מפתח ההצפנה או את המידע המפוענח שאינו מוגן־סיסמה. כפי שהראינו לעיל, הוראה זו אינה מתאפשרת במודל של תחולה מלאה של החיסיון וכן במודל של חיסיון שימוש בכל הנוגע לחשודים.

כעת נבחן באילו מדרכי הפעולה הפרקטיות שנמנו לעיל ניתן להשתמש במשטר המשפטי של כל אחד מהמודלים של החיסיון מפני הפללה עצמית (תחולה מלאה; אי־תחולה; חיסיון שימוש). בכל הנוגע למודל של תחולתו המלאה של החיסיון מפני הפללה עצמית ברי כי לא יהיה אפשר להשתמש בדרך הפעולה של נקיטת סנקצייה בדין (הליכי ביזיון בית משפט או עבירה פלילית). הוא הדין אף בנוגע לאפשרות להשתמש בכוח סביר על מנת להתגבר על הסיסמה או על ההצפנה, שכן משמעות החיסיון היא כי עומדת לחשוד זכות שאותה לא ניתן ליטול ממנו בדרך של שימוש בכוח (ולמעשה הדבר עלול להיחשב לתקיפה שלא כדין בנסיבות אלה). כן נראה שכשהחיסיון מפני הפללה עצמית חל, הרי שבדומה לחסיונות אחרים העשויים לעמוד לטובתו של החשוד בנסיבות מסוימות (למשל טענה לקיומו של חיסיון עורך־דין–לקוח, חיסיון רפואי וכדומה), אין הצדקה להסיק מסקנה ראייתית שלילית לחובת הנחקר המשתמש בחיסיון זה (חיזוק, סיוע או חזקה נגדו).

יתרה מזאת, ניתן לחשוב – ולו ברמה התאורטית בלבד – על מודל מקסימליסטי של תחולה מלאה של החיסיון מפני הפללה עצמית, שלפיו לא זו בלבד שיימנעו דרכי הפעולה שציינו, אלא גם תימנע האפשרות להשתמש בתחבולות כדי להוציא את המידע המבוקש מהנחקר,[176] ואף תימנע האפשרות לפנות לצד ג כדי להשיג את המידע הדרוש (האפשרות

174 כמה מדינות ברחבי העולם חסמו את הגישה של תושביהן לאתרי אינטרנט מסוימים, ובהם אתרי אינטרנט פופולריים כמו YouTube, Amazon או Bing. להרחבה בדבר חסימות כאמור שאירעו בסין ראו Nithin Coca, *China's Digital Protectionism Puts the Future of the Global Internet at Risk*, WASH. POST (Feb. 25, 2019), https://tinyurl.com/y3mmrpyx. להרחבה בדבר חסימות כאמור שאירעו בטורקייה ראו Tom Zeller JR., *YouTube Banned in Turkey After Insults to Ataturk*, N.Y. TIMES (Mar. 7, 2007), https://tinyurl.com/y6rqq4zp. להרחבה בדבר חסימות כאמור באיראן ראו Robert Tait, *Censorship Fears Rise as Iran Blocks Access to Top Websites*, GUARDIAN (Dec. 4, 2006), https://tinyurl.com/yxumzhlo.

175 אין זאת אומרת שלא ראוי לה למדינה לחסום גישה לאתרי אינטרנט הכוללים פעילות עבריינית, בדומה לַקֶבוּעַ למשל בחוק סמכויות לשם מניעת ביצוע עברות באמצעות אתר אינטרנט. כוונתנו הייתה לבקר מהלך של חסימת גישה כוללת לשירות מקוון המציע תכנים לגיטימיים אך ורק בשל העובדה שאינו מוכן לספק ״דלת אחורית״ לרשויות החקירה של מדינות זרות.

176 כאמור לעיל, במצב המשפטי הנוהג כיום בישראל תחבולה הוגנת שאינה שוללת את חופשיות הרצון של הנחקר, מותרת כאמצעי להשגת מידע, לרבות אמרות מפלילות, מאת הנחקר (ראו לעיל ה״ש 156). על כן האיסור על נקיטת דרך פעולה זו מגלם תפיסה מרחיבה מן המקובל כיום במשפט הישראלי בכל הנוגע לחיסיון מפני הפללה עצמית.

האחרונה היא מרחיקת הלכת ביותר, כיוון שאינה קשורה עוד במישרין בנחקר אלא בצד ג).[177]

בכל הנוגע למודל של אי־תחולת החיסיון מפני הפללה עצמית, ברי כי יהיה אפשר לנקוט כל אחת מדרכי הפעולה הפרקטיות שפורטו לעיל: נקיטת סנקצייה בדין, שימוש בכוח סביר, הסקת מסקנה ראייתית שלילית לחובת הנחקר, הפעלת תחבולות לצורך קבלת המידע מהנחקר ופנייה לצד ג לצורך קבלת המידע הדרוש.

בכל הנוגע למודל של חיסיון שימוש, מדובר למעשה בתרכובת של שני המודלים שנמנו לעיל. בכל הנוגע ל**חשודים**, מודל חיסיון השימוש מכיר למעשה בתחולתו של החיסיון מפני הפללה עצמית בדומה למודל התחולה המלאה, ואילו בכל הנוגע ל**עדים** שאינם חשודים, מודל חיסיון השימוש אינו מכיר בתחולתו של החיסיון מפני הפללה עצמית בדומה למודל אי־התחולה.

לסיום הדיון בדרכי הפעולה הפרקטיות לעקיפת ההתנגשות עם החיסיון מפני הפללה עצמית נשוב ונציין כי בכוחן של דרכי הפעולה שמנינו לעיל לצמצם – אך לא לאיין – את ההיזקקות למידע מידי הנחקר עצמו. לנוכח שכיחותם של אמצעי אבטחת המידע כמעט בכל מכשיר טלפון סלולרי, מחשב או יישום מקוון; לנוכח העובדה שאין די בנקיטת סנקצייה כלפי הנחקר כדי להניעו למסור את הסיסמה, את מפתח ההצפנה או להנגיש את המידע שכשהוא מפוענח ולא־מוגן סיסמה; לנוכח העובדה כי אמצעי אבטחה אלה אינם בהכרח ניתנים להתגברות בדרך של שימוש בכוח סביר; לנוכח העובדה שלעיתים קרובות אין די בהסקת מסקנה ראייתית שלילית כלפי הנחקר בשל סירובו למסור את המידע הדרוש; לנוכח העובדה שהשגת אמצעי האבטחה לא תמיד ניתנת לנטילה בדרך של תחבולה; לנוכח העובדה כי המידע הדרוש לצורך התגברות על אמצעי האבטחה לא מצוי בהכרח ברשותם של צדדים שלישיים – לנוכח כל אלה סביר מאוד להניח שהצורך במסירת הסיסמה, מפתח ההצפנה או הנגשת המידע הממוחשב כשהוא מפוענח ולא מוגן־סיסמה מאת הנחקר עצמו ייוותר צורך שגרתי למדי במהלך החקירה.

ד. המודל המוצע: חיסיון יחסי מפני הפללה עצמית

בפרק הקודם הצגנו שלושה מודלים להתבוננות על החיסיון מפני הפללה עצמית בהקשרנו הנדון כאן, וכן הצגנו חמש דרכים פרקטיות, ובחנו כיצד ניתן ליישם אותן בפועל במשטר משפטי של כל אחד משלושת המודלים. כזכור, המודל הראשון מכיר בחיסיון מפני הפללה עצמית הכרה מלאה. כפי שהראינו, מודל זה אינו בר־קיימה, שכן הוא בעל תחולה גורפת, על כל החקירות של כל העבירות, בכל הנסיבות, ועלול ליצור הלכה למעשה מרחב חסינות שלא יאפשר לרשויות החקירה להגיע למידע ממוחשב הדרוש לצורכי חקירה, מבלי לאפשר

177 האיסור על נקיטת דרך פעולה זו מגלם תפיסה שלפיה החיסיון מפני הפללה עצמית נועד בעיקרו להגן על פרטיותו של הנחקר. כשהערך המוגן האולטימטיבי בבסיס מודל התחולה המלאה של החיסיון מפני הפללה עצמית הוא של שליטת הנחקר על זרימת המידע על אודותיו, הרי שרק כך ניתן להסביר את האיסור על פנייה לצד השלישי שבידיו הופק המידע האמור. מכל מקום, במצב המשפטי הנוהג כיום בישראל אין מניעה לנקוט דרך פעולה זו.

לבית המשפט את הגמישות הנדרשת לשם התמודדות עם הבעיה שבמוקד המאמר. המודל השני הוא מודל אי־התחולה של החיסיון. גם מודל גורף זה אינו ראוי, שכן הוא עלול לפגוע יתר על המידה ובאופן גורף באחד הרציונלים שבבסיסו של החיסיון מפני הפללה עצמית, שאותם הצגנו לעיל בפרק ב, קרי ביכולתו של משתמש המחשב ליהנות ממרחב פרטי שבו יפעל ויתבטא בחופשיות. כמו כן מודל זה אינו מאפשר להתמודד עם מצבים שבהם ישכח באמת החשוד את סיסמתו או את מפתח ההצפנה, וכן עלול להפלות לא־עניינית בין חשודים שונים, על בסיס אמצעי האבטחה שבו בחרו להשתמש. המודל השלישי, של חיסיון שימוש, אומנם מספק כאמור מענה מסוים בכל הנוגע למידע האגור בחומרי המחשב של עדים, אך אינו מאפשר פתרון כוללני ורחב בכל הנוגע לחיפוש בחומרי מחשב של חשודים בשל שלילה גורפת של האפשרות של רשויות אכיפת החוק להשתמש במידע שיימצא בחומרי המחשב הללו נגד החשוד. דרכי הפעולה הפרקטיות שהוצגו לאחר מכן אינן מספקות גם הן מענה מעשי מלא, אף לא באחד מהמודלים שהוצעו, אלא לכל היותר פתרונות נקודתיים על פי נסיבותיהם של חלק מתיקי החקירה.

1. החיסיון מפני הפללה עצמית כיחסי ולא מוחלט

לגישתנו, שאותה נפרט בהמשך פרק זה, יש לפתח תפיסה של החיסיון מפני הפללה עצמית כחיסיון יחסי. תפיסה זו צריכה להיות גמישה ולהותיר מרווח לעריכת איזון קונקרטי בכל מקרה נתון, בניגוד למודלים שנסקרו בפרק הקודם, אשר מבקשים לתת פתרון אחד קטגורי, גורף, ולפיכך גם נוקשה יותר, לכל המקרים השונים. מטבע הדברים, המודל שאותו נציג יתייחס קונקרטית לסוגיה שבמוקד המאמר, קרי שאלת החיוב של נחקר למסור את הסיסמה או את מפתח ההצפנה למחשב, לטלפון הסלולרי או לשירות המקוון שבו הוא משתמש, או למסור את המידע במצב מפוענח ולא מוגן־סיסמה לרשויות החקירה. עם זאת נראה לנו כי התפיסה שבבסיס המודל שנציע להלן, שלפיה החיסיון מפני הפללה עצמית הוא **יחסי**, וניתן לאזנו עם אינטרסים כבדי משקל אחרים – אינה תחומה לגדרי ענייננו במאמר זה בלבד, ולמעשה ניתן לראות במודל המוצע משום מודל עיוני להתבוננות וליישום החיסיון מפני הפללה עצמית בכל ההקשרים הנוספים שבהם הוא רלוונטי. יתרה מזאת, נבקש להראות כיצד התפיסה שלפיה החיסיון מפני הפללה עצמית הוא יחסי זכתה ל״ניצני הכרה״ בחקיקה ובפסיקה הישראלית בהקשרים אחרים מן ההקשר שבמוקד מאמרנו. עם זאת ניצני הכרה אלה טרם הבשילו לכדי דוקטרינה מפותחת, קוהרנטית ומגובשת של החיסיון מפני הפללה עצמית כחיסיון יחסי.

בטרם נציג את המודל המוצע נבחין תחילה בין שני סוגים עיקריים של חסיונות – חסיונות יחסיים וחסיונות מוחלטים. הדין הישראלי מכיר בשני חסיונות מוחלטים – חיסיון עורך־דין–לקוח[178] וחיסיון כהן דת.[179] שאר החסיונות המוכרים הם יחסיים, במובן זה

178 ס׳ 48 לפקודת הראיות (הקובע כי ״דברים ומסמכים שהוחלפו בין עורך דין לבין לקוחו או לבין אדם אחר מטעם הלקוח ויש להם קשר עניני לשירות המקצועי שניתן על ידי עורך הדין ללקוח, אין עורך הדין חייב למסרם כראיה, אלא אם ויתר הלקוח על החסיון״). הוראה זו, לצד הוראת הסודיות החלה על עורך הדין שבסעיף 90 לחוק לשכת עורכי הדין, התשכ״א–1961, קובעת חיסיון מוחלט. העובדה שמדובר

שניתן, בנסיבות מתאימות ולפי קביעה שיפוטית קונקרטית, לגבור על החיסיון. כך הוא למשל בכל הנוגע לחסיונות המקצועיים האחרים: חיסיון רופא, פסיכולוג, עובד סוציאלי[180] וכן עיתונאי ובנקאי.[181] כך הוא גם בכל הנוגע לחסיונות מטעמי אינטרס ציבורי או מטעמי ביטחון המדינה.[182]

נרחיב מעט על החיסיון שממנו נהנה עורך הדין כדי ללמוד ממנו לענייננו. בית המשפט העליון פסק כי העובדה שחיסיון זה הוא מוחלט נועדה ״להבטיח בראש ובראשונה יחסים של כנות ופתיחות בינו [הלקוח] לבין עורך הדין בבואו להיזקק לשירותיו המקצועיים של האחרון״,[183] ומשמעות הדברים היא שבית המשפט אינו רשאי לשקול ״האם הצורך לגלות את המסמך לשם עשיית צדק עדיף מן הענין שלא לגלותו״.[184] בשל העובדה שחיסיון עורך־דין–לקוח הוגדר כחיסיון מוחלט, ועל מנת לפתור בעיות פרקטיות שהתגלגלו לפתחם של בתי המשפט ולמנוע מצב ששולי החיסיון מקיפים מרחבים גדולים מדי במסגרת חקירות פליליות, צמצם בית המשפט את גדרי החיסיון. הצמצום לא נעשה בדרך של הגדרת החיסיון כחיסיון יחסי והתגברות עליו במקום שבו שיקולי צדק גוברים על העניין שלא לגלות את המידע, אלא בדרך של הוצאת ״תחומים״ שונים אל מחוץ לתחולת החיסיון. משמע, לא בדרך של איזון ״אופקי״ בין הזכות לחיסיון לבין שיקולי צדק, אלא בדרך של איזון ״גאוגרפי״, של קביעת נושאים שונים ככאלה שאינם נכנסים בגדרו של חיסיון עורך־דין–לקוח כלל. אסטרטגיה משפטית זו נבעה מעצם טיבו של החיסיון. כיוון שהחוק בישראל הגדירו כחיסיון מוחלט, לא הייתה לבית המשפט האפשרות לסייגו מתוך עצמו אלא לבחור נושאים שהם מחוץ לתחום. כך נפסק למשל בנוגע להתייעצות של הלקוח עם עורך הדין בדבר ביצועה של עבירה פלילית עתידית;[185] בכל הנוגע לשיח הנוגע לסכום שכר הטרחה וחשיפת חשבוניות המס;[186] בכל הנוגע לעצם זהותו של הלקוח;[187] בכל

בחיסיון מוחלט נלמדת מכך שבניגוד לסעיפי החסיונות האחרים שיפורטו להלן, בית המשפט אינו מוסמך בשום תנאי להתגבר על החיסיון.

179 ס׳ 51 לפקודת הראיות. גם על חיסיון זה, כמו על החיסיון שבין עורך הדין ללקוחו, בית המשפט אינו מוסמך להתגבר.

180 ס׳ 49 לפקודת הראיות (הקובע כי רופא אינו חייב למסור כראיה דבר הנוגע לאדם שנזקק לשירותו, אלא אם ויתר המטופל על החיסיון או ״שמצא בית המשפט כי הצורך לגלות את הראיה לשם עשיית צדק עדיף מן הענין שיש לא לגלותה״). כך הדבר גם באשר לעדות של פסיכולוג, כקבוע בסעיף 50 לפקודת הראיות, או עדות של עובד סוציאלי, כקבוע בסעיף 50א לפקודת הראיות.

181 חסיונות אלה מעוגנים בפסיקה ולא בחוק. לעניין חיסיון עיתונאי (יחסי), ראו ב״ש 298/86 **ציטרין נ׳ בית הדין המשמעתי של לשכת עורכי־הדין במחוז תל־אביב**, פ״ד מא(2) 337, פס׳ 15 לפסק דינו של הנשיא שמגר (1987). לעניין חסיון בנקאי (יחסי), ראו את רע״א 1917/92 **סקולר נ׳ ג׳רבי**, פ״ד מז(5) 764, פס׳ 10 לפסק דינו של השופט גולדברג (1993).

182 סעיפים 44–45 לפקודת הראיות קובעים את החסיונות מטעמי ביטחון המדינה ואינטרס ציבורי (בהתאמה). גם חסיונות אלה הם יחסיים, במובן זה שבית המשפט רשאי לקבוע בעניין קונקרטי כי ״הראיה עשויה להועיל להגנת הנאשם ומידת התועלת שבה להגנה עולה על העניין שיש לא לגלותה, או שהיא חיונית להגנת הנאשם״.

183 על״ע 17/86 **פלונית נ׳ לשכת עורכי־הדין**, פ״ד מא(4) 770, 780 (1987).

184 עניין **היינץ**, לעיל ה״ש 14, פס׳ 29.

185 עניין **פלונית**, לעיל ה״ש 183, בעמ׳ 781–782.

186 רע״פ 751/15 **אברג׳יל נ׳ מדינת ישראל**, פס׳ 24 לפסק דינו של השופט שהם (נבו 9.12.2015).

הנוגע למסמכים שנתפסו ברשותו של עורך הדין במסגרת חקירות של מס הכנסה או מס ערך מוסף.[188]

מעניין כי הטכניקה הפסיקתית האמורה ניתנת לזיהוי גם במשפט האמריקני בהקשר אחר והוא בכל הנוגע לפסיקה הדנה בחופש הביטוי. חופש הביטוי מעוגן בתיקון הראשון לחוקה האמריקנית, אשר על פי ניסוחה הוא מוגדר זכות מוחלטת.[189] עם השנים נדרש בית המשפט העליון האמריקני להתייחס למצבים שמבחינה טכנית הם ״ביטוי״ אולם ברי כי נדרש לסייגם או אף לאסור עליהם.[190] במצבים אלה בחר בית המשפט להוציא את אותם סוגי ביטויים מגדרי ההגנה של חופש הביטוי וראה בהם משום ביטוי שאינו מוגן כלל, כיוון שלא היה באפשרותו של בית המשפט לערוך איזונים קונקרטיים בין הביטוי לבין אינטרסים אחרים שעלולים להיפגע מהביטוי. לפיכך באותם מצבים פורשה עצם הזכות ל״חופש הביטוי״ פירוש שלפיו תחומים שלמים מתוך קשת הביטויים האפשריים הוגדרו כאלה שאינם ״חופש ביטוי״. כך קבעו בתי המשפט בארצות הברית כי הגבלתם של ביטויים כאלה אינה בבחינת פגיעה בחופש הביטוי המוחלט הקבוע בתיקון הראשון לחוקה האמריקנית.[191]

כיצד נתפס החיסיון מפני הפללה עצמית עד היום בפסיקת בתי המשפט בישראל – האם כחיסיון בעל אופי מוחלט או יחסי? ככלל, נראה כי החיסיון מפני הפללה עצמית במשפט הישראלי נתפס כחיסיון שימוש בעל אופי מוחלט. משמע, החיסיון לא אפשר לנחקר להימנע כליל ממסירת המידע, וניתן לחייב אותו למסור את המידע, אך הוא לא ישמש נגד הנחקר עצמו אלא רק נגד אחרים.[192] כלומר החיסיון הוא מוחלט אך מוגבל בהיקפו.

187 בעניין זה ראו דבריה של השופטת ברק־ארז בע״א 5739/18 **מפעילי האתר www.oligarchescorts.com נ׳ מדינת ישראל**, פס׳ 37 (נבו 15.10.2018), שם נדונה השאלה אם יכולים מפעיליו של אתר המפרסם שירותי זנות לטעון בהליך לפי חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע״ז–2017 באמצעות עורך דינם, ומבלי להתייצב בהליך עצמו, בשל חששם פן התייצבותם תפגע בחיסיון מפני הפללה עצמית. באותו עניין קבע בית המשפט העליון כי ״חיסיון עורך דין–לקוח אינו חל על זהותו של הלקוח״, ולכן אין באפשרותם של מפעילי האתר להימנע מהתייצבות בהליך, אם ברצונם לטעון לגופו של עניין.

188 וראו ס׳ 235א–235ד לפקודת מס הכנסה [נוסח חדש], וס׳ 143 לחוק מס ערך מוסף, התשל״ו–1975. יש ״תחומים״ נוספים אשר הוצאו מתחום החיסיון בין עורך הדין ללקוחו. להרחבה, ראו לימור זר־גוטמן ״הבטחת תקשורת חופשית בין עורך דין ללקוח באמצעות חסיון עורך דין–לקוח וחובת הסודיות האתית – קריאה לרפורמה״ **ספר דויד וינר** 79, 96 ואילך (2009).

189 לחלק הרלוונטי בתיקון הראשון בחוקה האמריקנית ראו U.S. CONST. amend. I (“Congress shall make no law […] abridging the freedom of speech”).

190 כך למשל פסק בעבר בית המשפט העליון הפדרלי בארצות הברית כי חופש הביטוי לא חל על ביטויים מסוכנים כמו לצעוק ״שרפה!״ בתיאטרון הומה אדם. ראו Schenck v. United States, 249 U.S. 47 (1919). במקרה אחר פסק בית המשפט העליון הפדרלי בארצות הברית כי גם הצגת תועבה איננה מוגנת בחופש הביטוי. ראו Roth v. United States, 354 U.S. 476 (1957).

191 להרחבה בעניין זה ראו אהרן ברק **מידתיות במשפט** 176–177 (2010).

192 למקרים שבהם הוחלט על החלתו של חיסיון שימוש ראו עניין **חכמי**, לעיל ה״ש 95, פס׳ 12 לפסק דינה של השופטת שטרסברג־כהן. עוד ראו ת״פ (מחוזי ת״א) 66313-12-15 **ארוש נ׳ מדינת ישראל**, 5 (נבו 3.7.2017); ת״פ (מחוזי י-ם) 46180-12-12 **מדינת ישראל נ׳ בקשי דורון**, פס׳ 26 (נבו 2.5.2013). ראו גם עניין **שרון**, לעיל ה״ש 89.

עם זאת המשפט הישראלי מכיר בהגבלות נוספות על החיסיון מפני הפללה עצמית, אף בכל הנוגע לתחולתו על החשוד עצמו. למשל, נקבע בעבר כי חלה על החשוד החובה למסור לחוקריו מסמכים ״ציבוריים״, קרי מסמכים שנוצרו מכוח הוראה מחייבת בדין. נפסק כי החשוד יחויב במסירת מסמכים אלה ולא יחול בעניינם החיסיון מפני הפללה עצמית.[193] כך נקבע גם כי החיסיון מפני הפללה עצמית חל ברגיל על תוכן הדברים או המסמכים שמוסר אדם – בעל דין או עד בהליך משפטי – ולא על עצם זהותו של מוסרם.[194] במקרה אחר פסק בית המשפט העליון כי סעיף 135 לפקודת מס הכנסה [נוסח חדש] (להלן: ״פקודת מס הכנסה״) מסמיך את פקיד השומה לדרוש דוחות, ידיעות ופנקסים ״כדי להגיע לידיעה מלאה בדבר הכנסתו של אדם״. בית המשפט העליון קבע כי חששו של נישום פן יפליל את עצמו לא יוכל לשמש לו צידוק לסרב לדרישתו של פקיד השומה. נקבע כי האינטרס של גביית מס אמת על בסיס תמונת מידע מלאה לפני פקיד השומה גובר על החשש שגילוי האמת עלול להפליל את הנישום.[195]

יתרה מזאת, ניתן לאתר בפסיקה הישראלית, כאמור, ניצני הכרה בכך שהחיסיון מפני הפללה עצמית הוא דווקא חיסיון יחסי אף כשמדובר בחשוד עצמו. אזכור ראשון לניצני הכרה אלה בחיסיון מפני הפללה עצמית כחיסיון יחסי ניתן למצוא בעניין **קריתי**, שם פסק השופט הלוי כי בישראל, בניגוד לארצות הברית, אין כל ״ערובה חוקתית״ לחיסיון מפני הפללה עצמית, ולכן רשאי המחוקק ״לבטלו או לשוללו״.[196] ביטוי נוסף לקביעה זו ניתן למצוא בעניין **קלקודה**, שם פסק השופט חשין כי ״כולנו נסכים, כי זכותו של אדם שלא להפליל את עצמו [...] אינה זכות־על, וכי חוק מן־המניין יכול היה שישלול אותה מפורשות בתחומיו״.[197] יתרה מזאת, באותו עניין קבע השופט חשין כי אף אם המסמכים הגיעו לרשות המפקח כחלק מהליך פיקוח מנהלי, אין מניעה כי רשויות אכיפת החוק תשתמשנה באותם המסמכים לצורך נקיטת הליכים פליליים נגד המפוקח.[198] קביעה דומה ניתן למצוא בעניין **לגזיאל**, שם פסקה השופטת שטרסברג־כהן כי ״ככלל, חל חיסיון מפני הפללה עצמית גם על מסירת מסמכים שבידי אדם שיש בהם להפלילו. אלא שכלל זה אינו מוחלט ויש לו חריגים״.[199] גם המנגנון הקבוע בסעיף 135 לפקודת מס הכנסה, אשר הוזכר לעיל, מדגים במידה מסוימת את יחסיותו של החיסיון מפני הפללה עצמית. בית המשפט העליון קבע בעבר כי מסירת המסמכים מאת הנישום לידי פקיד השומה היא חובה המתקיימת גם

193 ע״פ 725/97 **קלקודה נ׳ הרשות לפיקוח חקלאי**, פ״ד נב(1) 749, פס׳ 27 לפסק דינו של השופט (כתוארו אז) חשין (1998). להרחבה בדבר הבחנה דומה במשפט האמריקני ראו רע״פ 4574/99 **מדינת ישראל נ׳ לגזיאל**, פ״ד נד(2) 289, פס׳ 4 לפסק דינה של השופטת שטרסברג־כהן (2000).

194 עניין **מפעילי האתר**, לעיל ה״ש 187, פס׳ 35.

195 ע״פ 524/72 **מדינת ישראל נ׳ הירש**, פ״ד כז(2) 776, 781 (1973).

196 ע״פ 242/63 **קריתי נ׳ היועץ המשפטי לממשלה**, פ״ד יח(3) 477, פס׳ 6 לפסק דינו של השופט הלוי (1964).

197 עניין **קלקודה**, לעיל ה״ש 193, פס׳ 19. ליישומה של הלכת **קלקודה** בעניין לחוק חומרים מסוכנים, התשנ״ג–1993, ולקביעה כי גם בנוגע לחוק זה היה המחוקק רשאי לסייג את תחולתו של החיסיון מפני הפללה עצמית ראו ע״ח (מחוזי חי׳) 32562-02-16 **תעשיות קיסריה פולימרים בע״מ נ׳ מדינת ישראל** (נבו 10.4.2016).

198 עניין **קלקודה**, לעיל ה״ש 193, פס׳ 31.

199 עניין **לגזיאל**, לעיל ה״ש 193, פס׳ 2 לפסק דינה של השופטת שטרסברג־כהן.

כשהנישום סבור כי יש בדבר כדי להפלילו בעבירה פלילית, בין שמדובר בעבירה לפי פקודת מס הכנסה ובין שמדובר בעבירה אחרת.[200]

הקשר אחר שבו ניתן לראות ביטוי מסוים להכרה בכך שהחיסיון מפני הפללה עצמית הוא יחסי הוא תחקירים צבאיים. הוראות חוק השיפוט הצבאי, התשט״ו–1955 קובעות כי ״הדברים שהושמעו בתחקיר, פרוטוקול התחקיר, כל חומר אחר שהוכן במהלכו, וכן הסיכומים, הממצאים והמסקנות [...], לא יתקבלו כראיה במשפט״.[201] עם זאת נקבע בהמשך כי הפרקליט הצבאי הראשי רשאי לבקש תחקיר צבאי מסוים, לקבלו לידיו, ואם מצא כי חומר התחקיר מגלה חשד לביצועה של עבירה פלילית, רשאי הפרקליט הצבאי הראשי להורות על פתיחה בחקירה פלילית. להוראה על פתיחה בחקירה פלילית לא יצורף חומר הנלווה לתחקיר הצבאי, וההוראה לא תצביע ישירות על חשד כלפי אדם ספציפי שהיה מעורב באירוע שבבסיס התחקיר.[202]

הביטויים שמנינו לעיל מן הדין הישראלי מכירים ב״אתרים״ מסוימים של המשפט הפלילי שבהם החיסיון מפני הפללה עצמית מעוצב כחיסיון יחסי מבחינת היקף פריסתו על החשוד. באותם ״אתרים״ הדין הישראלי עורך איזון קטגורי בין החיסיון לבין האינטרס הציבורי, משמע שבתחום מסוים של המשפט (למשל עבירות מס) נקבע קטגורית שהחיסיון מפני הפללה עצמית ייסוג מקידום אינטרס ציבורי מסוים. עם זאת לא מצאנו בפסיקה הישראלית ביטויים לכך שהחיסיון מפני הפללה עצמית פורש כחיסיון יחסי במובן זה שיהיה אפשר לאזנו במקרה קונקרטי, ובנסיבות קונקרטיות, עם אינטרס ציבורי אחר. כפי שנפרט להלן, המודל שאותו נבקש להציע להתמודדות עם הסוגיה שלפנינו מבקש ליישם תפיסה של החיסיון מפני הפללה עצמית כחיסיון יחסי, העומד לבחינה של איזונים קונקרטיים בין צורכי החקירה הפלילית – כל חקירה – לבין זכויותיו של החשוד: במקרים המתאימים יוכל בית המשפט להחליט כי בשל העובדה שהמידע תורם להפללתו של הנחקר, באפשרותו להימנע ממסירתו, ואילו במקרים אחרים יוכל בית המשפט לקבוע כי חרף העובדה שהמידע המבוקש תורם להפללתו של הנחקר, אין באפשרותו, בנסיבות העניין, להימנע ממסירתו.

הסוגיה שלפנינו נבדלת מן הסוגיות הנקודתיות שאליהן נדרשו המחוקק ובתי המשפט בבואם לסייג את תחולתו של החיסיון מפני הפללה עצמית. כיוון שמידע ממוחשב מוגן־סיסמה או מוצפן נוגע לכל סוגי העבירות הפליליות, לכל סוגי החקירות, להיקפי מידע משתנים ולאמצעי אבטחת מידע משתנים – קשה יותר להכריע הכרעה קטגורית גורפת בשאלת תחולתו של החיסיון. לפיכך ראוי לפתח מודל גמיש, יחסי, שיאפשר איזון קונקרטי בכל מקרה נתון של האינטרס החקירתי עם הזכויות של הנחקר, בייחוד החשוד, העלולות להיפגע.

200 ע״פ 143/73 **מדינת ישראל נ׳ זיידל**, פ״ד כח(2) 19, פס׳ 6 לפסק דינו של הנשיא זוסמן (1974). לביקורת על הלכה זו של בית המשפט העליון, ראו ניצה אורצקי ״מיסוי הכנסה בלתי־חוקית״ **עיוני משפט** יד 503, 532–534 (1989).

201 ס׳ 539א(ב)(1) לחוק השיפוט הצבאי.

202 שם, ס׳ 539א(ב)(4).

2. המודל לבחינת סירובו של נחקר למסור מידע מפוענח ולא מוגן־סיסמה – כללים ותבחינים

נציג עתה את מהותו של המודל המוצע. להלן נציע כמה קווים מנחים לעריכת האיזון הקונקרטי בין צורכי החקירה לבין החיסיון מפני הפללה עצמית בכל הנוגע למסירת מפתח ההצפנה או הסיסמה, או לחלופין מסירת חומר המחשב בידי הנחקר כשהוא מפוענח ולא מוגן־סיסמה. הקווים המנחים יתחלקו לשניים – כללים נוקשים ותבחינים (גמישים יותר במהותם) במסגרת הפעלת שיקול הדעת. נמנה תחילה שלושה כללים:

ראשית, ההתגברות על החיסיון מפני הפללה עצמית תיעשה בסמכות בית המשפט ולא בסמכות מנהלית, בדומה לחסיונות היחסיים האחרים, שבעניינם נקבע כי מי שרשאי להורות על נסיגת החיסיון מפני האינטרס הציבורי הוא בית המשפט.[203] כאן המקום לחדד שמבחינה מעשית הליך הדיון בשאלת הפגיעה בחיסיון מפני הפללה עצמית ייעשה במסגרת ביקורת שיפוטית שנייה, ואולי אף שלישית, בעניינו של אותו מחשב, טלפון סלולרי או שירות מקוון שנתפס מידי המחזיק: החיפוש הראשוני במקום שבו ייתפסו המחשב או הטלפון הסלולרי כ"חפץ", יכול שיוצא במסגרת צו חיפוש במקום לפי סעיף 23 לפסד"פ.[204] לאחר מכן החדירה ה"רגילה" לחומר המחשב יכול שתתבצע במסגרת צו חדירה לחומר מחשב,[205] לפי הוראות סעיף 23א(ב) לפסד"פ, הקובע כי –

> על אף הוראות פרק זה, לא ייערך חיפוש כאמור בסעיף קטן (א),[206] אלא על־פי צו של שופט לפי סעיף 23, המציין במפורש את ההיתר לחדור לחומר מחשב או להפיק פלט, לפי הענין, והמפרט את מטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש.

לעיתים שלב התפיסה של המחשב או של הטלפון הסלולרי כ"חפץ" ושלב החדירה ה"רגילה" לחומר המחשב יאוחדו ויידונו בבית המשפט במסגרת בקשה מאוחדת להוצאת צו חיפוש במקום וצו חדירה לחומר המחשב. צו החיפוש במקום, ולעיתים אף צו החדירה לחומר המחשב, יוצאו בשלב החקירה הסמויה בטרם המעבר לחקירה הגלויה. עם זאת שלב

203 עוד על ההבחנה בין סמכות שיפוטית לסמכות מנהלית בכל הנוגע לאישור פעולות חקירה בסביבה ממוחשבת ראו ויסמונסקי **חקירה פלילית**, לעיל ה"ש 22, בעמ' 318–321. יוער כי במסגרת סעיף 95(א) להצעת חוק החיפוש נקבע כי מי שיוכל לחייב נחקר במסירת סיסמה או מפתח הצפנה יהיה בית המשפט.

204 בהתקיים אחת מהעילות המנויות בסעיף 25 לפסד"פ, יכול להתקיים חיפוש במקום ללא צו. כמו כן, על פי פסיקת בית המשפט העליון ברע"פ 10141/09 **בן חיים נ' מדינת ישראל**, פ"ד סה(3) 305 (2012), יכול שיתקיים חיפוש במקום בהסכמה מדעת של הנחפש, ללא צו שיפוטי, אף אם אין מתקיימות העילות המנויות בסעיף 25 לפסד"פ.

205 גם בכל הנוגע לחיפוש בחומרי מחשב עשוי לעיתים להתבצע חיפוש על בסיס הסכמת הנחפש, שלא בצו שיפוטי. מאמר זה לא יתמקד בשאלת הפרשנות המאפשרת קיומה של פרקטיקה זו ברשויות החקירה בישראל.

206 ס' 23א(א) לפסד"פ, הקובע כך: "חדירה לחומר מחשב וכן הפקת פלט תוך חדירה כאמור, יראו אותן כחיפוש וייעשו על־ידי בעל תפקיד המיומן לביצוע פעולות כאמור; לענין זה, 'חדירה לחומר מחשב' – כמשמעותה בסעיף 4 לחוק המחשבים, תשנ"ה–1995".

הוצאת צו שיפוטי לשם התגברות על הגנת סיסמה או הצפנה יהיה, ככלל, בשלב החקירה הגלויה, משמע לאחר תפיסתם הפיזית של המחשבים או הטלפונים הסלולריים, ולאחר שהנחקר יביע התנגדות למסור את מפתח ההצפנה או הסיסמה, או יתנגד להנגיש את חומר המחשב המפוענח לרשות החוקרת. בשלב זה סביר להניח כי הדיון יתקיים במעמד שני הצדדים, בשונה מהצווים הקודמים, אשר ככלל מוצאים במעמד צד אחד (Ex parte).

שנית, ניתן להתגבר על החיסיון מפני הפללה עצמית רק במקרים שבהם הרשות החוקרת מחזיקה כדין במחשב, בטלפון הסלולרי או בגישה ליישום המקוון המדובר. במילים אחרות, אם המחשב, הטלפון הסלולרי או היישום המקוון אינם אצל הרשות החוקרת, הרי שלא יהיה אפשר להשיג את האחיזה בהם בשל מידע שמסר החשוד שביקש להימנע מהפללה עצמית וחויב להשיב.

שלישית, על הרשות החוקרת להניח את דעתו של בית המשפט כי הנחקר המסרב למסור את הסיסמה, את מפתח ההצפנה או את חומר המחשב המפוענח זוכר את הסיסמה או את מפתח ההצפנה שלו. לעיתים, כמובן, עניין זה לא יהיה במחלוקת, והחשוד או העד יתנגדו ברמה העקרונית למסירת המידע הדרוש. אולם במקרים שבהם הנחקר יכחיש כי הוא יודע את הסיסמה או את מפתח ההצפנה, או במקרים שבהם למשל ישמור החשוד על זכות השתיקה ויסרב להתייחס לשאלה בעניין זה, תוכל הרשות החוקרת להביא למשל עדים שיוכיחו כי החשוד או העד נהגו להשתמש במכשיר הטלפון הסלולרי הספציפי שבמחלוקת במשך זמן רב לפני תפיסתו במסגרת החקירה, או שהרשות החוקרת תשיג צילומים או הקלטות שיראו את החשוד או את העד משתמשים בטלפון הסלולרי שבמוקד המחלוקת. קו מנחה זה נועד לסייע להימנע ממצב שיינקטו סנקציות נגד נחקרים ששכחו בתום לב את הסיסמה או את מפתח ההצפנה שלהם, לעומת נחקרים שיבקשו לטעון בכזב כי שכחו בתום לב את הסיסמה או מפתח ההצפנה ולזכות בהגנה מפני נקיטת סנקציות שונות.

כעת נציג כמה תבחינים הרלוונטיים לתהליך הבניית שיקול הדעת השיפוטי במהלך הבחינה של בקשה לחייב נחקר למסור את הסיסמה או את מפתח ההצפנה או למסור את המידע הממוחשב כשהוא מפוענח ולא מוגן־סיסמה.

האחד, על בית המשפט לשקול מי הוא הנחקר שעליו מבקשים לכפות את מסירת המידע. ככל שמידת המעורבות של הנחקר בעבירה שביסוד החקירה היא קטנה יותר, כך הפוטנציאל להתנגשות עם החיסיון מפני הפללה עצמית הוא נמוך יותר. מכאן שתגבר הנטייה במקרה כזה לחייב את הנחקר בצו למסור את המידע הדרוש, כיוון שממילא קטן הסיכוי שיהיה בכך כדי לתרום להפללתו. לפיכך כאשר הנחקר הוא עד שאינו במעמד חשוד, ממילא האינטרס החיסיוני למנוע את הפללתו העצמית (לפחות בכל הנוגע לעבירות שבבסיס החקירה הנדונה) אינו אמור להתקיים בעניינו. גם בכל הנוגע לנחקר שהוא במעמד עד מדינה, הרי שממילא מובטחת לו התוצאה העונשית בכל הנוגע למעורבותו בעבירות הנחקרות (לעיתים אף מובטחת לו חסינות מלאה מפני העמדה לדין בגין אותן עבירות), ולכן לכאורה אין במסירת מפתח ההצפנה או הסיסמה או במסירת המידע כשהוא מפוענח כדי להרע את מצבו.[207]

207 יתרה מזאת, ייתכן שעצם סירובו של עד המדינה למסור את הסיסמה או את מפתח ההצפנה שלו יעלו כדי אי־שיתוף פעולה המצדיק חזרה מההסכם שנחתם עימו. בהקשר זה ראו ס׳ 7(ב) להנחית היועץ

השני, על בית המשפט לשקול אם היה אפשר במאמץ סביר להגיע למידע הדרוש מבלי להסתייע בנחקר. ראוי כי על הרשות החוקרת יוטל הנטל לשכנע את בית המשפט כי אין חלופה סבירה, פוגענית פחות, שבאמצעותה ניתן להגיע למידע הדרוש. הרעיון הכללי שבבסיסו של הקו המנחה האמור הוא לתמרץ את רשויות החקירה להשיג ראיות החיצוניות לחשוד, ולא לפנות להסרת החיסיון מפני הפללה עצמית בנקל. נובע מהאמור כי ככל שאמצעי האבטחה שבו השתמש החשוד או העד קשה יותר לפיצוח, וכאשר מחיר פיצוחו יהיה בלתי נסבל מבחינת הרשות החוקרת, כך ייטה בית המשפט לחייב את הנחקר במסירת המידע המבוקש. כך תוגשם גם אחת התכליות שבבסיס החיסיון מפני הפללה עצמית, כמפורט לעיל בפרק ב, ולפיה החיסיון נועד להבטיח שרשויות החקירה לא תימנענה מאיסוף ראיות חיצוניות, כאשר באפשרותן לאסוף ביתר קלות ראיות מפיו של החשוד או של העד.

השלישי, ככל שהעבירה הנחקרת חמורה יותר, כך תגבר הנטייה לחייב את הנחקר במסירת המידע הממוחשב, התפוס אצל הרשות החוקרת, בצורה נגישה וקריאה לרשויות החקירה. יוער כי בהצעת חוק החיפוש נקבע כי צו למסירת סיסמה או מפתח הצפנה יוצא רק במקרים שבהם מדובר בעבירות מסוג פשע (או עבירות המנויות בתוספת השלישית להצעת החוק – עבירות מחשב).[208] המנגנון שבהצעת החוק הוא נוקשה – קביעת תנאי סף שמצידו האחד עבירות שלא יאפשרו לחייב נחקר במסירת הסיסמה או מפתח ההצפנה ומצידו האחר עבירות שיאפשרו חיוב כאמור. לגישתנו, ייתכן לקבוע תנאי סף לסינון מוחלט של עבירות קלות, למשל עבירות חטא,[209] ומלבדו – נכון שחומרת העבירה תישקל כמשתנה במערך של כלל שיקולי בית המשפט בבואו להורות לנחקר למסור את המידע שדורשות רשויות החקירה.

הרביעי, ככל שעוצמת החשד והראיות אשר בבסיס הבקשה להוצאת צו החדירה לחומרי המחשב חזקות יותר ומבוססות יותר, הרי שתתחזק הנטייה לגבור על החיסיון, כדי להימנע משימוש בחיסיון באופן שמיטיב עם החשוד־האשם. נעיר כי הדבר נכון לטעמנו הן במקרה שבו החשוד הוא אשר מסרב למסור את המידע, והן במקרה שבו מדובר בנחפש שהוא עד.

החמישי, ככל שניתן להתרשם כי המידע הממוחשב, האגור במחשב, בטלפון הסלולרי או ביישום המקוון צפוי להיות רלוונטי ונחוץ לקידום החקירה, כך תיטה הכף לכיוון התגברות על החיסיון מפני הפללה עצמית. מנגד, ככל שההערכה היא כי המידע הממוחשב, האגור במחשב, בטלפון הסלולרי או ביישום המקוון עשוי להימצא כפריפריאלי לחשדות, כך ראוי להעניק משקל מכריע יותר לחיסיון.

השישי, על הרשות החוקרת להניח את דעתו של בית המשפט כי החיוב במסירת מפתח ההצפנה, הסיסמה או חומר המחשב המפוענח נדרש ישירות כראיה במסגרת החקירה

המשפטי לממשלה 4.2201 "עד מדינה" (30.8.2005), שם נקבע כי המדינה רשאית לחזור בה מההסכם עם עד המדינה במקרים שבהם הפר העד את ההסכם. סעיף 4(ב) להנחיה זו קובע כי בנוסח ההסכם תופיע גם "התחייבות העד לשתף פעולה עם רשויות אכיפת החוק ככל שיידרש ממנו".

208 ראו ס' 95(א)(1) להצעת חוק החיפוש.

209 בדומה להגדרה של עבירה "בת מעצר". סעיף 23(א)(7) לחוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996 קובע כי כל עבירה היא עבירה "בת מעצר", לבד מעבירות חטא.

המתנהלת, ואין נדרשת מסירת המידע כדי להפליל באמצעותה, כשלעצמה, את הנחקר. הכוונה ביסודו של תבחין זה היא להימנע ממצבים שבהם מטרת קבלת המידע הדרוש היא ליצור את ה"חיבור" בין הנחקר לבין המכשיר ובכך להפלילו. לשם המחשה ננית מקרה שבו נמצא מכשיר טלפון סלולרי בזירת פשע, והרשות החוקרת חשדה כי אדם מסוים הוא הבעלים והמשתמש במכשיר זה. בחיובו של החשוד למסור את מפתח ההצפנה, את סיסמת הכניסה או את המידע שבטלפון הסלולרי כשהוא מפוענח וללא סיסמה, מבקשת למעשה היחידה החוקרת לקשור בין המכשיר עצמו לבין נוכחותו של החשוד בזירת הפשע האמורה, אף מבלי שיש רלוונטיות ספציפית למידע האגור במכשיר. במקרה כזה, הרי שההתנגשות שבין החיסיון מפני הפללה עצמית לבין האינטרס החקירתי מתחזקת ומתחדדת, ולמעשה – כפי שציינו לעיל – יש כאן התנגשות חזיתית עם זכות השתיקה של אותו אדם החשוד בביצוע העבירה.[210] נראה לנו כי במקרה מעין זה ניתן למנות כמה שיקולים שיובילו, ככלל, למסקנה כי אין להתיר התגברות על החיסיון מפני הפללה עצמית וזכות השתיקה: **ראשית**, במקרה כזה דומה הדבר יותר לאמרה בעל פה של הנחקר, ודומה הדבר כאילו מסר הנחקר לחוקריו בעל פה "המכשיר התפוס בידיכם הוא בבעלותי": **שנית**, במקרה כזה לא נערך החיפוש מטעם הרשות החוקרת במחשב, בטלפון הסלולרי או ביישום המקוון של הנחקר, אלא הראיה הדרושה כולה היא ה"אמרה" של הנחקר כי המכשיר הוא בבעלותו; **שלישית**, גם בעת בחינת התכליות שבבסיסו של החיסיון מפני הפללה עצמית נראה כי ה"חיבור" האמור בין הנחקר לבין המכשיר התפוס פוגע יותר בתכליות אלה: הוא מעמיד את הנחקר בצורה "חזיתית" יותר עם הטרילמה המוסרית, שכן הוא בבחינת הודאה של ממש; הוא יוצר תמריץ בקרב רשויות החקירה להתבסס על הודאה זו ולא על ראיות חיצוניות; הוא פוגע בצורה חזיתית יותר בזכותו של הנחקר לפרטיות, שכן הוא בבחינת הודאה ישירה שלו בבעלות על המכשיר.

לצד ששת התבחינים שמנינו לעיל עשויה להתעורר השאלה אם ראוי לבחון שוב את צורכי החקירה בראי זכותו של הנחקר לפרטיות, כמו גם זכותם של צדדים שלישיים שהמידע על אודותיהם עשוי להימצא בחומר המחשב. מבחינה אנליטית, בחינת הזכות לפרטיות נעשית בשלב של הוצאת צו החדירה הראשוני לחומר המחשב. כך עולה מלשונו של סעיף 23א(ב) לפסד"פ. אומנם לכאורה בשלב הדיוני שבו עסקינן – קרי שלב הוצאת צו שיפוטי מאוחר למועד התפיסה של המחשב, של הטלפון הסלולרי או של היישום המקוון ואף מאוחר למועד שבו קמה סמכות החדירה לחומרי המחשב – החיסיון מפני הפללה עצמית הוא העומד במוקד מלאכת האיזון הנדרשת, אולם מבט מעמיק יותר מלמד כי לא ניתן, ואף לא נכון, להפריד הפרדה חדה בין השיקול של החיסיון מפני הפללה עצמית לבין השיקול של הפגיעה בפרטיות. אם בית המשפט יבחן אם ניתן לגדר את החיפוש במחשב, בטלפון הסלולרי או ביישום המקוון למידע מסוים בלבד, אשר רק בו יותר לעיין, ורק מתוכו יהיה אפשר להפיק ראיות לתיק החקירה, תהיה לכך משמעות לא רק מבחינת הפגיעה בזכות לפרטיות אלא גם מבחינת היקף ההפללה העצמית הפוטנציאלית. מכאן שהשיקולים כרוכים זה בזה. אומנם במוקד דיוננו כאן ניצב החיסיון מפני הפללה עצמית, אולם יש לזכור כי

210 ראו לעיל פרק ב.

הסיסמה או ההצפנה הן טכנולוגיות מגבירות פרטיות שנועדו להגן על הנחקר מפני חשיפה לתכניו הפרטיים ולמידע האישי על אודותיו. בצד החיסיון יש לזכור כי במקרה שבו הנחקר מוסר לחוקרים את הסיסמה או את מפתח ההצפנה שלו, או כשהוא מנגיש לחוקרים, על פי דרישתם כחוק, את המידע האישי שלו כשהוא מפוענח וללא הגנת סיסמה, הרי שמסירת המידע עלולה להוביל לא רק להפללתו אלא גם לפגיעה בפרטיותו. במילים אחרות, הפללה עצמית משמעה גם פגיעה עצמית בפרטיות הנחקר וצדדים שלישיים. מכאן שצמצום גדרי צו החדירה לחומר המחשב כדי לצמצם את הפגיעה בפרטיות משמעו, פעמים רבות, גם צמצום היקף הפגיעה בחיסיון מפני הפללה עצמית במקרה שבו יידרש הנחקר למסור מידע האגור במכשיר כשהוא מפוענח ונגיש לרשות החוקרת.[211]

בהקשר האמור עשויה להישמע הטענה שלפיה במסגרת המודל המוצע, שיקול הפגיעה בפרטיות הנובע מצו בית המשפט בא לידי ביטוי זה מכבר בשלב מוקדם יותר – שלב הוצאת צו החדירה לחומר המחשב לפי סעיף 23א לפסד״פ. משמע שבית המשפט ערך זה מכבר את האיזונים הנדרשים אל מול הפגיעה הנטענת בפרטיות,[212] ולכן אין טעם בעריכתם פעם נוספת בשלב מאוחר יותר. עם זאת חרף הפוטנציאל לכפילות מסוימת בעניין בחינת שיקול הפגיעה בפרטיות, אין להימנע מבחינה חוזרת של האפשרות למקד את החיפוש במידע מסוים מתוך חומרי המחשב, כמובן בשים לב לכך שהבחינה נעשית כעת לאורם של יתר השיקולים והקריטריונים שנמנו לעיל. יש לזכור כי בשלב זה הדיון עשוי להתקיים במעמד שני הצדדים, ובאפשרותו של בית המשפט לקבל מידע נוסף מהנחקר, אשר לא היה

211 ראו בהקשר זה את הדיון שנערך לעיל בפרק ב, בדבר ההצדקות לזכות השתיקה ולחיסיון מפני הפללה עצמית. כפי שצוין לעיל, אחת ההצדקות המרכזיות לזכות ולחיסיון אלה נובעת למעשה בזכותו של החשוד לפרטיות ולאוטונומיה. משמע, שעל פי הצדקה זו קיימת זיקה תאורטית יסודית בין מקורן של זכות השתיקה והחיסיון מפני הפללה עצמית לבין זכותו של החשוד לפרטיות ולאוטונומיה. כן ראו את טיעונו של אנדרו אונגברג (Ungberg, לעיל ה״ש 33, בעמ׳ 556–557), שלפיו התייחסות ״משולבת״ לתיקון הרביעי ולתיקון החמישי לחוקה האמריקנית תוביל לפרשנות שלפיה בעת הוצאת צו חיפוש בחומר מחשב מוצפן או מוגן־סיסמה, יהיה על בית המשפט לציין ברמת פירוט גבוהה במיוחד את הקבצים שאחריהם תרה הרשות החוקרת. בעניין קבצים אלה, ובעניינם בלבד, תהיה הרשות החוקרת רשאית לדרוש מהחשוד את הסיסמה או את מפתח ההצפנה, ורק בהם תהא הרשות רשאית לחפש ולעיין. אם במהלך החיפוש יתגלו ממצאים המעידים על ביצוע עבירות נוספות שהצו השיפוטי לא התייחס אליהן, ייאסר על הרשות החוקרת להשתמש בממצאים האמורים.

212 בהקשר זה יצוין כי בשנת 2005 תוקן סעיף 23א(ב) לפסד״פ וצוין במפורש שצו החדירה לחומר המחשב יכלול פירוט של מטרות החיפוש ותנאיו ״שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש״. בדברי ההסבר להצעת החוק נקבע כך: ״מוצע לקבוע כי על בית המשפט לפרט את מטרות החיפוש ואת תנאיו, תוך הנחיה ברורה כי בצווי החיפוש הנוגעים למחשב וחומר מחשב, על בית המשפט לשקול באופן מיוחד את הפגיעה בפרטיותו של התופס במחשב וצדדים נוספים״. דברי ההסבר להצעת חוק לתיקון פקודת סדר הדין הפלילי (מעצר וחיפוש) (מס׳ 11) (חיפוש ותפיסת חומר מחשב), התשס״ה–2005, ה״ח הכנסת 149, 150. גם הפסיקה, בהתייחסה לצו החדירה לחומר המחשב, הדגישה את שיקול הפגיעה בפרטיות של בעלי המחשב, הטלפון הסלולרי או החשבון ביישום המקוון, המשתמש בהם, וכן צדדים שלישיים שהמידע על אודותיהם אגור בחומרי המחשב (ראו למשל את עניין **פישר**, לעיל ה״ש 11, פס׳ 11).

לפניו בשלב הוצאת צו החדירה הראשוני.[213] כמו כן בשלב זה תמונת החשדות שלפני בית המשפט עשויה להיות בהירה יותר, שכן בינתיים התבצע מעבר לחקירה גלויה, וייתכן שהתקבלו הודעות ראשוניות של המעורבים בחקירה. על כן ייתכן שיהיה באפשרותו של בית המשפט לערוך איזונים מדוקדקים יותר בנוגע לצורכי החקירה עם הזכויות שעל הפרק.

אם המשתנים האמורים יובילו למסקנה כי יש מקום לחייב את הנחקר למסור את הסיסמה או את מפתח ההצפנה למחשב, לטלפון הסלולרי או ליישום המקוון, או לחייבו להנגיש את המידע הממוחשב כשהוא מפוענח, נשאלת השאלה מה תהיה משמעותו המעשית של צו שיפוטי מחייב כזה. לדעתנו, ראוי להכיר במשמעויות האלה: **ראשית**, אם סירב הנחקר למסור את המידע לאחר שנדרש לעשות כן בצו שיפוטי, יש לראות בו מי שמבצע לכאורה עבירה של הפרת הוראה חוקית, וטענה כי הסירוב נובע מהחיסיון מפני הפללה עצמית או זכות השתיקה – לא תעמוד לו כטענת הגנה; **שנית**, יהיה אפשר לשקול לנקוט נגד הנחקר הסרבן צעדי אכיפה לפי פקודת בזיון בית משפט, דהיינו קנס או אף מאסר למטרות אכיפה;[214] **שלישית**, אם יסרב נחקר־חשוד לדרישת הצו למסור את הסיסמה, את מפתח ההצפנה או את המידע המפוענח, ישמש סירובו חיזוק לראיות התביעה נגדו. יוער כי מטבע הדברים סנקצייה זו רלוונטית לנחקרים־חשודים ולא לעדים. עם זאת כאשר הנחקר יהיה עד מדינה, יהיה אפשר לראות בסירובו למסור את המידע האמור עילה לנסיגת המדינה מההסכם שנחתם עימו; **רביעית**, כשפיענוח הסיסמה או מפתח ההצפנה נעשה באמצעות זיהוי פנים או טביעת אצבע, יהיה אפשר לאכוף את הצו השיפוטי גם בדרך של שימוש בכוח סביר על מנת להוציא אל הפועל את דרישת הצו. לעומת זאת במצב שבו הסיסמה או מפתח ההצפנה טמונים בהקלדת קוד תווי, בדגימת קול או בדפוס התנהגות, שאז לא ניתן להשתמש בכוח על מנת לגרום לפעולות להתבצע.

להשלמת התמונה יצוין כי ללא קשר להוצאת הצו השיפוטי נגד הנחקר יהיה אפשר לפעול בשתי דרכי פעולה פרקטיות נוספות על מנת להשיג את מפתח ההצפנה או את הסיסמה הנדרשים: **האחת**, שימוש בתחבולה נגד הנחקר כדי להשיג את המידע האגור

213 הפרקטיקה הנוהגת היא כי אין ניתנת לחשודים זכות עמידה בעת הליך להוצאת צו חדירה לחומר מחשב, ולרוב הדיון אינו מתקיים במעמד שני הצדדים. כמקרה חריג ניתן לציין את עניין **אוריך הראשון** (לעיל ה״ש 12), ואת עניין **כהנא** (לעיל ה״ש 13), אשר בשניהם התקיים דיון במעמד שני הצדדים בעת הבקשה להוצאת צו חדירה למחשב. עם זאת העמדה שלפיה ניתן לקיים דיון במעמד שני צדדים בשלב הבקשה להוצאת צו החדירה נדחתה לאחרונה בבית המשפט העליון בבש״פ 4705/20 **פלונית נ׳ מדינת ישראל** (נבו 8.7.2020), שם נקבע כי ״אין בסעיפים [הכוונה לסעיפים 23, ו־23(א) לפסד״פ] כדי להקנות זכות למבקש להשיג על מתן צווים בעניין זה עובר לביצועם״. שאלה זו הגיעה פעם נוספת לפתחו של בית המשפט העליון, בבש״פ 5105/20 **שמעון נ׳ מדינת ישראל** (נבו 25.5.2021). ביום 25.5.2021 פורסם פסק דינו של בית המשפט העליון בתיק זה, שם נקבע ברוב דעות כי לחשוד אין זכות ערר או ערעור על צווי חדירה לחומר מחשב וכן נקבע ברוב דעות כי לחשוד אין זכות עמידה בשלב הגשת הבקשה לצו חדירה לחומר מחשב (הגם שהשופטים הנדל וברון נחלקו ביניהם בשאלה האם ההכרעה בעניין זכות העמידה היא רציו או אוביטר). על פסק דין זה הוגשה בקשה לדיון נוסף (דנ״פ 4072/21 **שמעון נ׳ מדינת ישראל**), וביום 27.7.2021 התקיים דיון נוסף בהרכב מורחב של שופטי בית המשפט העליון בעניין. נכון למועד כתיבת מאמר זה, טרם פורסמה הכרעת בית המשפט העליון בדיון הנוסף.

214 ראו ס׳ 5–7 לפקודת בזיון בית משפט. יצוין כי פקודת בזיון בית המשפט אינה מבחינה בין עדים לבין חשודים בכל הנוגע לחובת הציות לצווי בית המשפט.

במכשיר; **השנייה**, פנייה לצד ג בבקשה או בדרישה על פי צו הממונן אליו על מנת שימציא לרשות החוקרת את מפתח ההצפנה או הסיסמה.

3. המודל המוצע בראי הצעת חוק החיפוש

כפי שציינו לעיל,[215] הצעת חוק החיפוש מתייחסת לאפשרות לחייב בצו שיפוטי בעל גישה לחומר מחשב למסור את מפתח ההצפנה או הסיסמה לחומר מחשב הדרוש לחקירה. סעיף 95 להצעת החוק מונה חלק מהכללים והתבחינים שמנינו לעיל לצורך בחינת ההצדקה לחייב את הנחקר למסור את הסיסמה ואת מפתח ההצפנה. על פי סעיף 95 להצעת חוק החיפוש, ההתגברות על סירובו של הנחקר יכול שתיעשה בצו שיפוטי בלבד ולא בהוראה של גורם מינהלי, או כנגזר מהצו הכללי המתיר חדירה לחומר מחשב.

כמו כן מוצע בסעיף 95 כי יהיה אפשר לבקש צו להתגברות על סיסמה או על מפתח הצפנה רק כשמדובר בעבירות מסוג פשע או בעבירות נוספות המנויות בתוספת השלישית להצעת החוק, קרי עבירות עוון המנויות בחוק המחשבים. תנאי נוסף הקבוע בסעיף 95 הוא כי על בית המשפט להתרשם כי אין דרך אחרת לחדור לחומר המחשב זולת הוצאת צו המחייב את מסירת הסיסמה או מפתח ההצפנה. התנאי השלישי המנוי בסעיף 95 הוא כי על בית המשפט להתרשם כי –

> הצורך בהעתקת חומר המחשב או בעיון בו לשם חקירת העבירה גובר על הפגיעה בבעל הגישה לחומר המחשב הכרוכה בחיובו למסור את מפתח ההצפנה או הסיסמה.

בהצעת החוק אין התייחסות לשאלה על איזו פגיעה מדובר: פגיעה בחיסיון מפני הפללה עצמית, או שמא פגיעה בפרטיות, בזכות להליך הוגן או בזכויות אחרות. על פי דברי ההסבר להצעת חוק החיפוש, הנחת המוצא שבבסיס סעיף 95 להצעה היא כי החיסיון מפני הפללה עצמית אינו חל במקרה של דרישה למסור סיסמה או מפתח הצפנה למחשב, לטלפון סלולרי או לשירות מקוון.[216] עם זאת נקבע בדברי ההסבר כי –

> עם זאת, אין במתן הצו כדי למנוע טענות בנוגע לחיסיון מפני הפללה עצמית, ככל שנטען כי עצם מסירת הסיסמה הוא המפליל (למשל, מסירת סיסמה תקשור את האדם לביצוע העבירה, בגלל הכינוי שנעשה בו שימוש כסיסמה).

במילים אחרות, נראה כי הגישה המבוטאת בהצעת חוק החיפוש היא במידה רבה **גישה דיכוטומית**: מחד גיסא, במצב דברים שבו עצם מסירת הסיסמה או מפתח ההצפנה לא יישיך את הנחקר למחשב, לטלפון הסלולרי או לשירות המקוון – הרי שהחיסיון מפני הפללה עצמית לא יחול, ואילו כאשר יש במסירת הדברים כדי לקשור לעצם הזיקה של

215 בפרק המבוא.

216 ראו דברי ההסבר לס׳ 95 בהצעת חוק החיפוש (״עצם מסירת הסיסמה אינו פוגע בחיסיון מפני הפללה עצמית, ככל שהטענה היא כי החומר המוצפן הוא מפליל, שהרי מדובר בחומר שהמשטרה היתה יכולה לתפוס, לולא היה מוצפן, ועצם ההצפנה אינו משנה את טיב סמכות המשטרה, או את טיבו של החומר״).

הנחקר לחומר המחשב – החיסיון מפני הפללה עצמית יחול. בשולי הדברים יוער כי הגישה הדיכוטומית המשתקפת מדברי ההסבר לסעיף 95 בהצעת חוק החיפוש, סותרת במידה מסוימת את האיזונים שמופיעים בנוסח הסעיף. למשל, בסעיף 95 להצעת החוק מצוין כי ניתן לתת צו למסירת סיסמה או מפתח הצפנה רק בעבירות מסוימות ולא בכל עבירה. ניתן לתהות מדוע יש צורך לערוך איזון שכזה כשמדובר באי־תחולה מוחלטת של החיסיון מפני הפללה עצמית (וזכות השתיקה).

בפועל המודל המוצע כאן הוא מודל **גמיש** יותר, יחסי במהותו, הכולל כמה תבחינים לצד כללים נוקשים יותר (אשר חלקם נמנו בהצעת חוק החיפוש וחלקם נחסרים ממנו) ומכיר בצורך באיזון שיפוטי קונקרטי בנסיבותיו של כל מקרה ומקרה. יש לראות בחיסיון מפני הפללה עצמית כיחסי, וככזה המוחל על כל הסיטואציות החקירתיות. בנסיבות מסוימות משקל הפגיעה בחיסיון מפני הפללה עצמית יהיה רב יותר, ובנסיבות אחרות – פחות.

ה. סיכום

ההתפתחויות הטכנולוגיות המואצות בתחום אבטחת המידע והפיכתה של הגנת הסיסמה וההצפנה לאמצעי הגנה שכיחים שקיימים בחלק ניכר מהמחשבים, מהטלפונים הסלולריים ומהשירותים המקוונים של כלל משתמשי המחשב והאינטרנט – מחייבות לחדד את הדיון המשפטי הנוגע בדבר. במתח המובנה בין המשפט לטכנולוגיה, שעליו מרבים לדבר חוקרי המשפט וטכנולוגיות מידע,[217] אין לראות בטכנולוגיה כ**מצריכה תיקון והתאמה של המשפט**, אלא יש לראות בטכנולוגיה כ**מחדדת ומאירה ערכים יסודיים של המשפט**. התהליך הוא של מירוק ערכים ולא התאמתם או שינוּיָם. השינוי הטכנולוגי עשוי להאיר את הכשלים או החסָרים בביטוּיָם של הערכים עלי כתב במסגרת הדין הקיים ופסיקת בתי המשפט.

כפי שהראינו במאמר, מודל התחולה המלאה של החיסיון מפני הפללה עצמית על מסירת מפתח הצפנה, סיסמה או מידע ממוחשב שנתפס כדין בתצורה מפוענחת, עלול להוביל, הלכה למעשה, ל**חסינות** מפני העמדה לדין. כך הוא גם בכל הנוגע למודל של חיסיון שימוש, הפועל למעשה כחיסיון מלא בכל הנוגע לחשוד עצמו. בעבר לא נדרשו רשויות החקירה להתמודד עם מצבים שבהם לא ניתן להתגבר בכוח ובזמן סביר על מנעולים, כספות או כיו״ב, ואילו בשנים האחרונות, לראשונה, מתמודדות רשויות החקירה עם קושי שיכול לאיין לחלוטין את יכולתן להגיע למידע ממוחשב הדרוש לצרכי חקירה ולעיין בו. להבדל איכותי זה השלכה על האפשרות לאמץ את המודלים של חיסיון מלא או

217 כדוגמה בלבד ראו Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1998); Yochai Benkler, *Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1232–1261 (2000). ראו גם Yochai Benkler, *Technology, Law, Freedom and Development*, 1 INDIAN J. L. & TECH. 1 (2005); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 85–99, 235–239 (1999).

חיסיון שימוש. מנגד, גם המידע האישי בעידן האינטרנט והטלפונים הסלולריים ה״חכמים״ ויכולת המעקב אחר מחשבותיו, פעולותיו והתקשרויותיו של אדם – גדלו במידה ניכרת, ועל כן מודל של אי־תחולה של החיסיון מפני הפללה עצמית עלול אף הוא להוביל לפגיעה גורפת בחופש השימוש באמצעים הממוחשבים.

שינוי נקודת שיווי המשקל בין צורכי הרשות החוקרת לבין החיסיון של החשוד מפני הפללה עצמית, כמו גם זכויות אחרות המושפעות מהעניין (פרטיות החשוד, פרטיותם של צדדים שלישיים, חופש העיסוק של חברות האינטרנט היכולות להיות מושפעות מחובה לסייע לרשויות החקירה) – הביא אותנו לבחון מודל מעודכן של החיסיון מפני הפללה עצמית, לאחר שבחנו את המודלים האלטרנטיביים ומצאנו אותם לא מתאימים, חלקיים או לחלופין גורפים מדי וחד־ממדיים. בסופו של דבר הצענו את המודל המבקש להתבונן על החיסיון מפני הפללה עצמית כחיסיון יחסי, בעל תחולה מוגבלת, וכך יספק המודל פתרון הוליסטי ושלם, אך לא כוללני ו״גס״, לבעיה שבמוקד המאמר. פתרון זה מורכב, כפי שהצגנו לעיל, מכללים נוקשים ומתבחינים ״רכים״ שיספקו יחדיו הבניה לשיקול דעתו של השופט שיידרש לערוך את האיזון הקונקרטי בין צורכי החקירה לבין זכויותיו של החשוד ושל צדדים שלישיים נוספים העלולים להיות מושפעים מההתגברות על הסיסמה או על ההצפנה של המחשב, של הטלפון הסלולרי או של השירות המקוון. אנו מאמינים שקווים מנחים אלה יאפשרו שמירה מיטבית על זכויותיהם של נחקרים לצד אכיפה אפקטיבית של הדין הפלילי ושמירה על שלטון החוק.