מאמר זה טרם עבר עימוד סופי ומספרי העמודים ישתנו לכשיתפרסם הכרך המודפס. כן צפויים שינויים נוספים.

פגיעה בזכויות אדם בשל שימוש משטרתי באמצעים טכנולוגיים למעקב ושיטור מנבא

ד״ר רותם קדוש נוסבאום**

תקציר

בעשור האחרון גדל באופן משמעותי היקף השימוש המשטרתי בטכנולוגיות חדשניות למעקב ושיטור מנבא. כלים טכנולוגיים כגון: מצלמות, מיקרופונים, איכון טלפונים ניידים ותוכנות רוגלה מאפשרים למשטרת ישראל לאסוף מידע רב על מעשים, שיחות ומחשבות אנושיים. בינה מלאכותית משמשת את משטרת ישראל לניתוח המידע שנאסף לשם זיהוי אנשים, מכוניות ואירועים חריגים. בנוסף, בהסתמך על המידע שנאסף, ניתן להפיק באמצעות בינה מלאכותית תחזיות לפשיעה עתידית. במאמר זה אני דנה בהשלכות השימוש באמצעים אלו על זכויות הפרט ובמיוחד על הזכות לפרטיות. אני מבקשת להציע דרכי פיקוח והסדרה מחודשת לשימוש בכלים טכנולוגיים אלו. בנוסף, אני מבקשת להצביע על הגורמים והסיבות לעלייה בהיקף השימוש המשטרתי בטכנולוגיות מעקב ושיטור מנבא.

תחילה, אני בוחנת את חוקיות השימוש באמצעים טכנולוגיים למעקב ושיטור מנבא. השימוש המשטרתי בכלים אלו מוסדר בחלקו. הסדרה זו לוקה בחסר מאחר שהיא אינה מאפשרת פיקוח שיצמצם את הפגיעה בזכויות אדם. כמו כן, קיים פער עצום בין החוק המיושן לטכנולוגיה המתפתחת במהירות רבה. במצב הקיים, משטרת ישראל יכולה לאסוף מידע בעצמה באופן המאפשר את עקיפת מנגנוני הפיקוח הקיימים בנוגע למידע שנאסף ונשמר על ידי גופים אחרים. לאחר מכן, אני מצביעה על הפגיעה בזכות לפרטיות בשל שימוש לא מפוקח ולא מוסדר בכלים טכנולוגיים אלו. בהמשך לכך, אני בוחנת את מידתיות הפגיעה בזכות לפרטיות.

לסיום אני מציגה הצעה להסדרת השימוש המשטרתי באמצעים טכנולוגיים למעקב לשם איסוף מידע. לגישתי, ההתמקדות בסוג המידע שמשטרת ישראל מוסמכת לאסוף, לשמור ולנתח, ולא בכלי הטכנולוגי שמשמש לשם כך, תאפשר גמישות רגולטורית. באופן זה, ההסדרה תכיל התפתחויות טכנולוגיות מבלי שהחוק יהפוך למיושן ולא רלוונטי. המיקוד בסוג המידע מאפשר האחדה של נוהלי הפיקוח המשפטיים לכל הכלים הטכנולוגיים. בנוסף, טענתי כי ראוי להקים גוף אשר יפקח על הפעלת הכלים שבשליטת המשטרה.

מבוא; א. מהו שיטור יזום וכיצד הוא מוביל לפרקטיקות מעקב אחר אוכלוסייה; ב. אמצעים טכנולוגיים למעקב ושיטור מנבא; ב.1. שלב ראשון – איסוף המידע; ב.1.א. מעקב אחר האוכלוסייה באמצעות טכנולוגיה על ידי משטרת ישראל במרחב הציבורי/במרחב הפרטי; ב.1.ב. איסוף המידע בידי גופים אחרים במרחב הציבורי/במרחב הפרטי; ב.2. שלב שני – שמירת המידע; ב.2.א. מאגרי מידע המנוהלים על ידי המשטרה; ב.2.ב. מאגרי מידע המנוהלים על ידי רשויות אחרות; ב.3. שלב שלישי – ניתוח המידע; ב.3.א. זיהוי וחיפוש חשודים; ב.3.ב. חיזוי תרחישים פליליים; **ג. חוקיות השימוש באמצעים טכנולוגיים למעקב ושיטור מנבא;** ג.1. הסמכת משטרת ישראל בחוק לאיסוף מידע באמצעות כלי מעקב טכנולוגיים; ג.2. הסמכת משטרת ישראל בחקיקה ראשית לשמירת המידע; ג.3. הסמכת משטרת ישראל בחקיקה ראשית לעיבוד המידע; **ד. הסיבות**

** דוקטור למשפטים, אוניברסיטת תל אביב. מרצה במכון לקרימינולוגיה באוניברסיטה העברית.
ברצוני להודות לראש המכון לקרימינולוגיה באוניברסיטה העברית פרופ׳ באדי חסייסי על ההזדמנות לפתח תכנים אלו במסגרת המכון.

להרחבת השימוש בטכנולוגיה לשם מעקב; ד.1. עיתות משבר; ד.2. שיפור ביכולות הטכנולוגיות; ד.3. הטכנולוגיה זולה, קלה לשימוש וזמינה; ד.4. השימוש בטכנולוגיה יעיל; **ה. הפגיעה בזכות לפרטיות בעקבות השימוש המשטרתי באמצעים טכנולוגיים למעקב ושיטור מנבא;** ה.1. הזכות לפרטיות – מהי?; ה.2. פגיעה בזכות לפרטיות בשלב איסוף המידע; ה.3. פגיעה בזכות לפרטיות בשלב שמירת המידע; ה.4. פגיעה בזכות לפרטיות בשלב ניתוח המידע; **ו. בחינה חוקתית;** ו.1. הסיבות שבגינן לא ראוי לבצע איזון אנכי; ו.2. הסיבות שבגינן ראוי לבצע איזון אופקי; **ז. הסדרת השימוש בכלים אלו**; ז.1. הסדרת שלב איסוף המידע בחקיקה חדשה; ז.2. הסדרה בחוק של שלב ניתוח המידע; ז.3. כמה הערות כלליות לסיכום; **סיכום.**

מבוא

ג׳ורג׳ אורוול כתב בספרו ״1984״: ***״בכל מישורת שבראש גרם מדרגות, מול תא המעלית, צופות מעל הכותל הפנים הגדולות שבכרזה. הרי זו אחת מאותן תמונות דיוקן שהצייר התחכם לעשותן באופן שהעיניים עוקבות אחריך בכל אשר תפנה. ״האח הגדול עינו פקוחה״ נאמר בכתובת שמתחתיה״.***[1] ברומן דיסטופי זה מתוארים חיים המתנהלים תחת שלטון טוטליטרי קיצוני. המשטר המתואר בספר מפעיל אמצעים רבים של שליטה פיזית ומנטלית מוחלטת. אחד מהאמצעים הללו הוא ניהול מעקב אחר האזרחים. התוצר הסופי הוא היעדר חופש מחשבה. מקורו של המושג ״האח הגדול״ הוא בספר זה, והוא מתייחס למצב שבו בני אדם נתונים לפיקוח מתמיד של השלטון. בספר מוצג מכשיר פיקוח שנקרא מסך הטלסקרין, שנמצא בכל פינה ומאפשר ל״אח הגדול״ לראות הכול ולשמוע הכול. ***״הטלסקרין הוא גם משדר וגם קולט... בשום פנים אין לדעת אם עוקבים אחריך ברגע מסוים, באיזו תדירות, או על פי איזו שיטה נוהגת משטרת המחשבות לצותת לחוט מסוים... מתקבל אפילו על הדעת שהם עוקבים אחרי הכל כל הזמן... ושומה עליך לחיות – ואתה חי, מכח ההרגל שנעשה טבע – בהנחה ששומעים כל קול שאתה מוציא מפיך, ורואים... כל תנועה שאתה עושה״.***[2] כיום, מדינות רבות מחזיקות באמצעים טכנולוגיים המאפשרים להן לפעול באופן דומה למפלגה הדמיונית שארוול תיאר בספרו.[3]

בעשור האחרון עלה היקף השימוש של סוכנויות משטרה במדינות רבות ברחבי העולם, וביניהן ישראל, באמצעים טכנולוגיים למעקב ושיטור מנבא, במטרה למנוע פשיעה.[4] משטרת ישראל משתמשת בכמה מערכות של מצלמות בעלות טכנולוגיה מתקדמת. חלקן מאפשרות זיהוי לוחיות רישוי, כגון מערכת ״עין הנץ״.[5] חלקן מאפשרות זיהוי תווי פנים.[6] דוגמאות נוספות למערכות

---

[1] ג׳ורג׳ ארוול **1984** 5 (ארז וולק מתרגם, עם עובד מהדורה חדשה 2019).

[2] שם, בעמ׳ 6.

[3] תהילה שוורץ אלטשולר ורחל ארידור הרשקוביץ ״מעקב אחר אזרחים – מה קורה בעולם?״ **פרלמנט** 84: נגיף הקורונה - התמודדות עם משבר עולמי (2020).

[4] אסף וינר והדס תמם בן-אברהם **טכנולוגיות חדירה וחיפוש במכשירים חכמים ונכסים דיגיטליים על ידי רשויות האכיפה בישראל** (איגוד האינטרנט הישראלי 2023) (להלן: **מסמך איגוד האינטרנט**); ויקי אוסלנדר ״רואים לך הכל״ **כלכליסט** (14.10.2021) https://newmedia.calcalist.co.il/magazine-14-10-21/m01.html.

[5] רועי גולדשמידט **השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי** 7 (הכנסת, מרכז המחקר והמידע 2020); עמ׳ 3 לעתירה למתן צו על תנאי בבג״ץ 641/21 **האגודה לזכויות האזרח בישראל נ׳ משטרת ישראל** (נבו 28.1.2021) (להלן: **עתירת האגודה לזכויות האזרח**).

[6] השימוש בטכנולוגיית זיהוי תווי פנים יוחס למשטרת ישראל, אך היא לא הודתה בכך במפורש; ״חוות דעת בעניין תזכיר חוק לתיקון פקודת המשטרה [נוסח חדש] (מערכות צילום מיוחדות), התשפ״א–2021״ 6 (חוות דעת של תהילה שוורץ אלטשולר ועמיר כהנא 29.7.2021) (להלן: שוורץ אלטשולר וכהנא); לירן תמרי ״האם משטרת ירושלים עושה שימוש בטכנולוגיית זיהוי פנים באזור העיר העתיקה?״ **ynet** (7.10.2020) https://jerusalem.mynet.co.il/local_news/article/H1CrQgmIv#google_vignette; אלון חכמון ״בשל האיומים: המשטרה ביקשה להשתמש במערכת זיהוי פנים במצעד הגאווה בי-ם״ **מעריב** (2.6.2022) https://www.maariv.co.il/news/israel/Article-922404 (להלן: חכמון (2.6.2022)); רועי ינובסקי ״בשידור חי:

מצלמות אלו הן מצלמות המאפשרות זיהוי אירועי אלימות וזיהוי אירועים חריגים, כגון: מצלמות עירוניות בפרויקט עיר ללא אלימות.[7] הדבר נעשה באמצעות ניתוח בינה מלאכותית של המתרחש בעיר.[8] במרחב המרשתת אוספת משטרת ישראל תמונות ומידע בנוגע למיקום ומעשים של אזרחים.[9] גופי אכיפת החוק מסוגלים להתקין תוכנות רוגלה על גבי טלפונים חכמים ומחשבים ולדלות מתוכם את המידע האישי שנשמר על גבי המכשיר – תמונות, אימיילים, הודעות ועוד.[10] בימינו קיימת טכנולוגיה המאפשרת לעקוב אחר מיקומו של אדם באמצעות התקנת מכשיר GPS, באמצעות איכון טלפונים ניידים או באמצעות מעקב אחריו ברשת המצלמות הפרוסה ברחבי הארץ.[11]

מלבד טכנולוגיות איסוף מידע, אנו עדים לפיתוח טכנולוגיה לניתוח המידע. נעשה שימוש בבינה מלאכותית לטובת ניתוח המידע, באופן של חשיפת רשתות נוירונים מלאכותיים למידע רב על מנת שילמדו את דפוסי הפשיעה, בדרך שבני אדם אינם מסוגלים לה. באופן הזה לומדת בינה מלאכותית לזהות אירועים חריגים במרחב הציבורי, כגון, נסיעה בניגוד לכיוון התנועה, התקהלות חשודה, אזרחים שבורחים ממקום שבו אירע אירוע אלים ועוד.[12]

בחיפוש אחר הסברים לעלייה בשימוש בכלים טכנולוגיים לשם מעקב, ראוי להתייחס לדבריו של פוקו. הוא דן בשימוש של גופי משטרה בטכניקות מעקב אחר האוכלוסייה לשם ניהול הסדר הציבורי במדינה.[13] ארחיב בנוגע לכך **בפרק א'** במאמר ואתייחס ל"תאוריית המניעה המצבית". על פי תאוריה זו, על מנת למנוע פשיעה יעיל יותר לסכל את היכולת של העבריין להוציא את תוכניתו לפועל, מאשר להשפיע על המניע שלו לפשוע.[14] תאוריה זו מתבססת על ההנחה של "תאוריית הבחירה הרציונלית", לפיה העבריין בוחר לעסוק בפשיעה לאחר ששקל את האופציות הקיימות בפניו.[15] אציין טכניקות שונות של "מניעה מצבית" אשר משנות את תהליכי קבלת ההחלטות של עבריינים ומשפיעות על הערכת ההזדמנות לבצע עבירה.[16] לאחר שאציג תאוריות אלו, אתייחס למודלים השונים לשיטור. אתמקד ב"מודל השיטור היזום" שמטרותיו מניעת פשיעה ואי־סדר לפני התרחשותם.[17] אפרט בנוגע לענף "התערבות מבוססת מקום" ולטכניקות המשויכות אליו, כגון: מצלמות במעגל סגור, ניתוח נתונים סטטיסטיים בהתאם לתאוריית "נקודות חמות" ובשיטור

מאות מצלמות בירושלים יחוברו למשטרה" **ynet** (9.8.2016) https://www.ynet.co.il/articles/0,7340,L-4839406,00.html (להלן: ינובסקי "בשידור חי").

[7] עמיקם הרפז **אסטרטגיות שיטור סוגיות בעצוב מדיניות אכיפת החוק** 72 (2012); גלי וינרב "רחפנים מיקרופונים ומצלמות המהפכה הטכנולוגית במשטרה" **גלובס** (20.1.2017) https://www.globes.co.il/news/article.aspx?did=1001172925; אוסלנדר, לעיל ה"ש 4.

[8] גולדשמידט, לעיל ה"ש 5, בעמ' 12.

[9] Alexandra Mateescu et al., *Social Media Surveillance and Law Enforcement* (Data & Soc'y, Oct. 27, 2015), https://datasociety.net/wp-content/uploads/2015/10/Social_Media_Surveillance_and_Law_Enforcement.pdf.

[10] מיכאל בירנהק "מאוריך לפגסוס: על פרטיות חוקתית בחקירות משטרה" **ICON-S-IL Blog** (23.1.2022) (להלן: בירנהק "מאוריך לפגסוס") https://did.li/Dsyrl.

[11] חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007 (להלן: חסד"פ נתוני תקשורת); חוק התקשורת (בזק ושידורים), התשמ"ב–1982 (להלן: חוק בזק); ס' 13 לחוק שירות הביטחון הכללי, התשס"ב–2002 (להלן: חוק השב"כ). עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 11.

[12] גולדשמידט, לעיל ה"ש 5, בעמ' 4, 12.

[13] מישל פוקו **לפקח ולהעניש: הולדת בית הסוהר** 264–280 (2015).

[14] Ronald v. Clarke, *Situational Crime Prevention*, 19 CRIME & JUST. 91 (1995).

[15] הרפז, לעיל ה"ש 7, בעמ' 65.

[16] שם.

[17] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING AND MEDICINE, *PROACTIVE POLICING: EFFECTS ON CRIME AND COMMUNITIES* 12, 19 (David Weisburd & Malay K. Majmundar eds., National Academies Press 2018) (להלן: דו"ח האקדמיה בנושא שיטור מנבא).

מנבא.[18] זאת על מנת להסביר – כיצד השינוי בגישה בנוגע לתפקידה של המשטרה, הוביל לעלייה במעקבים שמבוצעים אחר האוכלוסייה.

בפרק ב׳ במאמר אפרט בנוגע ליכולות השונות של הכלים הטכנולוגיים הקיימים שבהם משתמשת משטרת ישראל לשם מעקב ושיטור מנבא.

שימוש בכלים טכנולוגיים אשר פוגעים בזכויות אדם יכול להיעשות מבחינה חוקתית רק בהתאם לפסקת ההגבלה.[19] כלומר, נדרשת הסמכת משטרת ישראל בחוק ההולם את ערכיה הדמוקרטיים של המדינה להשתמש בכלים טכנולוגיים שונים לשם מעקב ושיטור מנבא לתכלית ראויה ובאופן מידתי. על כן, **בפרק ג׳** במאמר אבחן האם משטרת ישראל מוסמכת באופן מפורש בחוק להשתמש באמצעים טכנולוגיים שונים לשם מעקב אחר האוכלוסייה? בהמשך לכך אבחן האם ההסמכה מתייחסת לאיסוף כל סוגי המידע? האם ההסמכה מתייחסת למקום איסוף המידע (תוך הבחנה בין הספרה הפרטית לציבורית)? בנוסף אבחן האם ההסמכה מתייחסת לכל הדרכים שבהן ניתן להשיג מידע זה? והאם ההסמכה מתייחסת לכל שלבי ההליך, שהם איסוף, שמירה וניתוח המידע? מסקנתי היא כי המצב המשפטי הקיים אינו מסדיר כראוי את השימוש המשטרתי באמצעים טכנולוגיים למעקב ושיטור מנבא.

בפרק ד׳ אדון בתרומה של הטכנולוגיה לעלייה בביצוע מעקבים. הגורמים והסיבות שאליהם אתייחס הם: עיתות משבר, התפתחויות טכנולוגיות שמאפשרות יכולות חדשות ושימוש קל, נוח, זמין, זול ויעיל.

בעקבות שימוש גופי אכיפת החוק באמצעים הטכנולוגיים האמורים נגרמת פגיעה חמורה בזכויות אדם. הזכויות אשר נפגעות הן הזכות לפרטיות, הזכות לחופש וחירות, הזכות להליך הוגן ותקין, זכות הקניין, הזכות לקניין רוחני, חופש התנועה, חופש ההפגנה, השם הטוב, חופש העיסוק ועוד.[20] **בפרק ה׳** במאמר אתמקד בזכות לפרטיות ואדון בפגיעה בה בהתאם לשלושת שלבי המעקב: איסוף המידע, אגירתו וניתוחו. אערוך הבחנה הנוגעת למקום איסוף המידע בין הספרה הפרטית לספרה הציבורית וכן אערוך הבחנה הנוגעת לסוג המידע שנאסף, כך שאבחין בין נתונים ביחס למעשים, דיבור ומחשבות.[21]

בפרק ו׳ במאמר אציג את מידת הפגיעה בזכות לפרטיות. במסגרת בחינת מידתיות הפגיעה אבחן האם הכלים הטכנולוגיים השונים למעקב ושיטור מנבא יעילים במניעת פשיעה.

אני סבורה כי ראוי לקדם שינויי חקיקה על מנת למלא את הלקונה בחוק ולהתיר את סבך החוקים הקיים. **בפרק ז׳** במאמר אדון בפתרונות אפשריים להסדרה הלקויה של התחום. כותבים רבים הצביעו על הליקויים בהסמכת משטרת ישראל להשתמש בכלים למעקב ושיטור מנבא והצביעו על הצורך בפיקוח.[22] בעוד מאמרים קודמים בחנו כל כלי בנפרד, אני מציעה הסתכלות רחבה על התחום בכללותו ובחינת מגוון הכלים הטכנולוגיים למעקב ושיטור מנבא יחד, זאת לשם הסדרה קוהרנטית ועקבית של התחום. אני מציעה חלוקה של הכלים השונים לקטגוריות בהתאם לסוג הנתונים

[18] שם, בעמ׳ S2; הרפז, לעיל ה״ש 7, בעמ׳ 63.

[19] ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו.

[20] **עתירת האגודה לזכויות האזרח**, לעיל ה״ש 5, בעמ׳ 2, ס׳ 5.

[21] שלושת האפיקים המגדירים את המצב האנושי. ראו חנה ארנדט **המצב האנושי** (עורכת ראשית עדית זרטל, אריאלה אזולאי ועדי אופיר מתרגמים 2013).

[22] שוורץ אלטשולר וכהנא, לעיל ה״ש 6, בעמ׳ 16–28; עומר טנא ״חוק המאגר הביומטרי: סיכונים והזדמנויות״ **המשפט** יז 421, 440–456 (התשע״ג).

הנאספים, למיקום האיסוף (פרטי או ציבורי) ולגוף המחזיק במערכת איסוף הנתונים ומאגר המידע (משטרת ישראל או גוף אחר). היות שהאמצעים הטכנולוגיים השונים כוללים השגת מידע מסוגים שונים, כגון: דיבור, מעשים, מחשבות, הרי שהחוקים הנפרדים אינם יכולים להסדיר את השימוש בהם בצורה מלאה.[23] בנוגע למאגרי מידע שנמצאים בשליטת גופים שאינם משטרת ישראל, אני סבורה כי יש להחיל נוהל אחיד לבקשת צו משופט לשם שימוש בהם. לשם הסדרת השימוש במאגרים הנמצאים בשליטת משטרת ישראל ראוי להקים גוף מפקח. ההתמקדות בתוצר הסופי, שהוא סוג המידע, ולא בתהליך, שהוא הטכנולוגיה המסוימת להשגת המידע, מאפשרת החלת נוהל זהה המאפשר פיקוח שיפוטי על כל אמצעי טכנולוגי עתידי שיאפשר השגת המידע באופן שונה. המאמר הנוכחי מוסיף לידע הקיים בהצעת כלי רגולטורי שניתן ליישם לשם הסדרת טכנולוגיה בתחומים נוספים, ולא רק בתחום השיטור.

<u>א. מהו שיטור יזום וכיצד הוא מוביל לפרקטיקות מעקב אחר אוכלוסייה</u>

בעבר, גופי משטרה לא נדרשו לנבא עבריינות מאחר שלא נדרשו להגיב לפשיעה לפני שהתרחשה.[24] בפרק זה אבקש לבחון מהם הגורמים והסיבות לעלייה בשימוש המשטרתי בפרקטיקות של מעקב אחר האוכלוסייה.

מודל השיטור האנגלו־אמריקאי הקלסי, שהיה נהוג לפני שנות ה־60 של המאה הקודמת, התבסס על התפיסה כי על המשטרה לעסוק במניעת פשיעה. לפי מודל זה, מניעת פשיעה תושג באמצעות תפיסת עבריינים והרחקתם מהחברה ובעצם נוכחות המשטרה, אשר מצמצמת את ההזדמנויות לפשיעה.[25] תפקידה של המשטרה נתפס כתפקיד הכבאי המגיע לזירה לאחר שהאש פרצה.[26] ההנחה של המודל הסטנדרטי הייתה כי כליאה אינטנסיבית של עבריינים תפחית את רמות הפשיעה. זאת, מאחר שלא יוכלו לבצע עוד פשעים בקהילה, בנוסף להרתעה שנוצרת מפני ביצוע עבירות, כאשר הסיכוי להיעצר עולה. אך המחקרים האמפיריים שנערכו בנוגע למודל זה מצאו כי לטקטיקות אלו הייתה השפעה מועטה, אם בכלל, על שיעורי הפשיעה.[27]

מחקרים אלו הובילו להטלת ספק בנוגע ליעילות הגישות הסטנדרטיות לשיטור. הצירוף של מחקרים אלו ועלייה בשיעורי הפשיעה בשנות ה־60 בארצות הברית הובילו למשבר אמון בשיטור.[28] בעקבות משבר זה החל חיפוש אחר עקרונות חדשים לפעולות המשטרה. אחדים מהם גובשו לכדי "מודל שיטור יזום".[29] המונח "שיטור יזום" מתייחס לאסטרטגיות שיטור שאחת ממטרותיהן היא מניעה או הפחתה של פשיעה ואי־סדר, ושאינה מתמקדת רק בתגובה לפשעים לאחר שהתרחשו.[30] האסטרטגיות החדשות של שיטור יזום חרגו מתפקידה המסורתי של המשטרה ובחנו שיטות פרואקטיביות שיש להן סיכוי למנוע פשיעה.[31]

---

[23] על ההסדר החוקי לעמוד בתנאי ס' 8 לחוק־יסוד: כבוד האדם וחירותו, כך שיהלום את ערכיה הדמוקרטיים של מדינת ישראל, לתכלית ראויה וכי הפגיעה בזכות לפרטיות תיעשה באופן מידתי.

[24] הרפז, לעיל ה"ש 7, בעמ' 61; דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בפרק 1 בעמ' 4.

[25] הרפז, לעיל ה"ש 7, בעמ' 61.

[26] שם, בעמ' 62; דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בפרק 1 בעמ' 4.

[27] שם, בפרק 1 בעמ' 12.

[28] דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**.

[29] שם, בפרק 1 בעמ' 12, 19.

[30] הרפז, לעיל ה"ש 7, בעמ' 63; דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש 17, בפרק 1 בעמ' 4.

[31] דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בעמ' 1 בפרק 1.1.

פוקו התייחס למעקב אחר האוכלוסייה כאחד האמצעים המאפשרים למוסדות המשטרה להכווין התנהגות אנושית בהפעלת שליטה. זאת בניגוד לאמצעים להפעלת כוח פיזי, אשר היו נהוגים בעבר.[32] פוקו מציין כי בממשלה מפותחת, תפקידה של המשטרה נתפס כניהול הגוף החברתי. מעקב אחר האוכלוסייה מאפשר שליטה בתנאי קיום, הישרדות ורווחה במדינה.[33] רעיון יישום תוכניתה של המדינה לניהול החיים התקינים, על פי פוקו, תואם את עקרונות מודל השיטור היזום.[34]

כיום, משתמשים באסטרטגיות של שיטור יזום באופן נרחב בישראל ובארצות הברית.[35] אחד מארבעת ענפי השיטור היזום הוא "ענף התערבויות מבוססות מקום".[36] על פי הגישה של ענף זה, יש למקד את משאבי השיטור באופן יעיל יותר במקומות שבהם ישנו ריכוז אירועי פשיעה.[37] "התערבות מבוססת מקום" נשענת על "תאוריית המניעה המצבית". לפי תאוריה זו, במקום להתמקד במניע של העבריין, בוחרים להתמקד בסיכויים שלו להוציא את התוכנית לפועל.[38]

"תאוריית המניעה המצבית" נשענת על ההנחות הבסיסיות של "תאוריית הבחירה הרציונלית". על פי תאוריית הבחירה הרציונלית, העבריין בוחר לבצע פשע על מנת לספק את צרכיו. העבריין בוחר בין אפשרויות שונות, אשר מוגבלות בשל אילוצי זמן, יכולת ומידע חסר או שגוי. הנחת יסוד נוספת של תאוריית המניעה המצבית היא כי רוב מעשי הפשע קשורים לניצול הזדמנויות. לאור הנחות אלו שוער כי על מנת למנוע את התרחשותו של אירוע עברייני, המשטרה נדרשת לצמצם את ההזדמנויות לביצוע הפשע. בנוסף, על המשטרה להגדיל את הסיכון של הפושע להיתפס ולהיענש.[39] שתיים מתוך חמש קטגוריות של טכניקות מניעה מצבית שנמצאו יעילות במחקר רלוונטיות להתערבות מבוססת מקום, והן: "הגברת מאמצי העבריין" ו"הגברת הסיכון לעבריין".[40] טכניקות אלה של מניעה מצבית משנות את תהליכי קבלת ההחלטות של עבריינים ומשפיעות על הערכת ההזדמנות לבצע עבירה.[41] דוגמה הממחישה את האפקטיביות של הטכניקות הללו אפשר לראות בהתקנת מצלמות במעגל סגור (CCTV), שנמצאה כמשפיעה על הפחתת הפשיעה ובעיקר זו הקשורה לרכוש.[42] אסטרטגית שיטור נוספת שנקראת "נקודות חמות" מבקשת לאתר באמצעים סטטיסטיים מקומות שבהם קיים ריכוז פשיעה חוזרת. זאת, לשם מיקוד משאבי השיטור באופן יעיל יותר.[43]

גישה זו לאיתור ריכוזי פשיעה עתידית שייכת לתחום רחב שנקרא "שיטור מנבא". מדובר בניסיון לקבוע היכן יתבצעו פשעים ומי עשוי לבצע אותם דרך ניתוח ממוחשב של מידע. זאת, בהתבסס על ההנחה כי פשיעה היא לא תמיד אקראית וכי יש לה מאפיינים קבועים, כגון: זמן, מקום, סוג הפשע וסוג הקורבנות. למערכת מוזן מידע סטטיסטי בנוגע למקרי פשיעה קודמים וגורמים שונים המשפיעים על פשע, כגון: גורמים סביבתיים, חברתיים, דמוגרפיים וכלכליים. התוכנה מנתחת את

32 פוקו, לעיל ה"ש 13; JEREMY BENTHAM, PAUPER MANAGEMENT IMPROVED PARTICULARLY BY MEANS OF AN APPLICATION OF THE PANOPTICON PRINCIPLE OF CONSTRUCTION (1812).

33 Stuart Elden, *Plague, Panopticon, Police*, 1 SURVEILLANCE & SOC'Y 240, 248 (2003).

34 אריק גוד **על הסטייה** 64–65 (האוניברסיטה הפתוחה 2002).

35 דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בעמ' 1S.

36 שם, בפרק 2 בעמ' 2.

37 שם, בעמ' 2S.

38 Clarke, לעיל ה"ש 14.

39 שם.

40 הרפז, לעיל ה"ש 7, בעמ' 65.

41 שם.

42 שם.

43 דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בעמ' S2; הרפז, לעיל ה"ש 7, בעמ' 63.

המידע, מאתרת דפוסים, וכך מנבאת מי יהיה מעורב בפשע והיכן.[44] נטען כי השימוש בטכניקות של שיטור מנבא נעשה לשם מתן מענה מתאים לפעילות הפלילית הגואה, אשר מאתגרת את מגבלות שיטות השיטור המסורתיות.[45]

למרות היתרונות המיוחסים לשימוש באמצעים טכנולוגיים לשם שיטור יזום, שימוש לא מבוקר באמצעים אלו עלול להוביל לפגיעה בזכויות אדם וביניהן בזכות לפרטיות. הסדרת השימוש בטכנולוגיה בחקיקה הנוכחית אינה מגינה על זכויות אלו באופן מספק. בשל כך, לאורכו של המאמר אבחן בעייתיות זו ואציע פתרון בדמות הסדרה חקיקתית חדשה. ההסדרה המוצעת תתמקד בסוג המידע שנאסף על ידי משטרת ישראל, ולא באמצעי הטכנולוגי שבאמצעותו הושג המידע. לאחר שהצגתי בפרק זה את הבסיס התאורטי להתמקדות בפעולות משטרתיות למעקב אחר האוכלוסייה, אפנה בפרק הבא לבחינת האמצעים הטכנולוגיים המשמשים למעקב ושיטור מנבא.

<u>ב. אמצעים טכנולוגיים למעקב ושיטור מנבא</u>

בפרק זה אבקש להציג את הכלים הטכנולוגיים השונים אשר נמצאים בשימוש משטרת ישראל לשם מעקב אחר אזרחים. לאחר מכן, אציג את הכלים הטכנולוגיים שבאמצעותם מנותח המידע. אבקש לסווג את האמצעים הטכנולוגיים השונים בהתאם לשלבי תהליך המעקב. השלב הראשון הוא שלב איסוף המידע, השלב השני הוא שלב שמירת המידע והשלב השלישי הוא שלב ניתוח המידע.

<u>ב.1. שלב ראשון – איסוף המידע:</u> בשלב הראשון משטרת ישראל משתמשת בכלים טכנולוגיים לשם איסוף המידע. ניתן לחלק את סוגי הנתונים שנאספים על ידי המשטרה לשלוש קבוצות: מעשים, דיבור ומחשבות.[46] תיעוד מעשי האדם יכול להיעשות על ידי צילום תמונות סטילס, צילום סרטי וידאו, איסוף נתונים בנוגע למיקום שלו, שימוש באפליקציות וגלישה באתרים שונים. מכל אלו ניתן ללמוד על הקשרים החברתיים שהאדם מקיים ועל לוחות הזמנים שלו.[47] על מנת לזהות את האדם נאספים הנתונים הביומטריים שלו, כגון: טביעת אצבע ותווי פנים.[48] תיעוד הדיבור יכול להיעשות באמצעות הקלטות קול (שמע), תמונות וידאו וטקסט, כגון: אימיילים, הודעות בטלפון הנייד ותכתובות על גבי נייר. על מחשבות האדם, אופיו ונטיותיו ניתן ללמוד מהצלבות נתונים ומניתוח מעשיו, שיחותיו וכתביו.[49] ישנם שני סוגים של כלים טכנולוגיים למעקב אחר האוכלוסייה: כלים שהוצבו על ידי משטרת ישראל לשם מעקב אחר האוכלוסייה וכלים שנמצאים בשימוש של גופים ואנשים אחרים, אליהם יש למשטרת ישראל גישה. אבחין בין שני סוגי הכלים באמצעות החלוקה בין המרחב הציבורי למרחב הפרטי. כן אבחין בין סוגי המידע שנאסף.

<u>ב.1.א. מעקב אחר האוכלוסייה באמצעות טכנולוגיה על ידי משטרת ישראל: במרחב הציבורי</u>: לשם איסוף מידע בנוגע למעשים משתמשת משטרת ישראל *בתמונות סטילס*

---

[44] חלק מתאוריות הניבוי התמקדו בגורמים סוציולוגיים המגבירים עבריינות לשם דירוג מסוכנות והתמקדות בעבריינים רצידיביסטיים או מקומות שבהם עלולה להתרחש פשיעה בעתיד. לעומת זאת, חלק אחר מהתאוריות התמקדו בגורמים ביולוגיים המגבירים עבריינות, כגון פיזיונומיה. ראו אלדר הבר ורותם קדוש נוסבאום ״זיהוי פנים מלאכותי: פרופיילינג אלגוריתמי בשירות שיטור מנבא״ **מחקרי משפט** לה 6 (צפוי להתפרסם ב־2024) (להלן: הבר וקדוש נוסבאום).

[45] פרוטוקול ישיבה 156 של הכנסת ה־20 (5.2.2018).

[46] ארנדט, לעיל ה״ש 21. את הנתונים הנוגעים לסטטוס, כגון: מצב רפואי וכלכלי, סיווגתי תחת קבוצת המעשים, למרות שלעיתים מדובר במצב סביל, ולא בפעולה.

[47] בירנהק מאוריך לפגסוס, לעיל ה״ש 10.

[48] טנא, לעיל ה״ש 22, בעמ׳ 424–425.

[49] בירנהק מאוריך לפגסוס, לעיל ה״ש 10.

המצולמות בכבישי הארץ ובכניסה לישובים רבים באמצעות מערכת "עין הנץ" ומצלמות מהירות חדשות.[50] "עין הנץ" היא מערכת אוטומטית שעוקבת אחר תנועתם של אזרחים הנוסעים בכבישי הארץ ומתעדת אותם, באמצעות פיענוח לוחית זיהוי הרכב וצילום נוסעי הרכב.[51] ככל הנראה חלק ניכר משטחה של מדינת ישראל מרושת במצלמות המערכת, והיא נמצאת בשימוש של יחידות שונות במשטרה.[52] אמצעי נוסף לאיסוף מידע על מעשים הוא *סרטי וידאו*. דוגמה לכך היא השימוש במצלמות מב"ט 2000 הפרוסות ברחבי העיר העתיקה בירושלים במחוז דויד. כארבע מאות וחמישים מצלמות מסייעות לכוחות המשטרה לחקור ולתפוס מבצעי פיגועים באירועים ביטחוניים וחשודים באירועים פליליים.[53] דוגמה נוספת לשימוש משטרת ישראל בצילומי וידאו לשם מעקב אחר מעשים היא מצלמות שהוצבו ברחבי הערים במסגרת פרויקט "עיר ללא אלימות", זאת כחלק ממערך של אמצעים טכנולוגיים לזיהוי ותחקור של אירועי אלימות ופשיעה במרחב הציבורי ביותר מ־150 ערים.[54]

אמצעי צילום וידאו נוספים המצויים בידי משטרת ישראל הם מצלמות על גבי רחפנים.[55] כמאה רחפנים בעלי יכולות תצפית, ניתוח תמונה וביצוע פעולות בשטח נמצאים בשימוש משטרת ישראל, בפריסה ארצית ובצירי תנועה שבהם מתרחשות תאונות דרכים רבות.[56] בנוסף, מצלמות הגוף של השוטרים מספקות סרטי וידאו המתעדים את מעשי האזרחים. מצלמות הגוף מוצמדות לכ־10,000 שוטרים, בעיקר ביחידות הסיור והתנועה.[57]

עבור זיהוי אדם נדרש איסוף *נתוני הביומטריים*.[58] האמצעים הביומטריים אשר נמצאים בשימוש לשם זיהוי הם: טביעת אצבע, תווי פנים, קול וסריקת קשתית או רשתית העין.[59] טביעות אצבע

---

[50] בנוגע למערכת "עין הנץ" ראו: גולדשמידט, לעיל ה"ש 5, בעמ' 2, 7, 13; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 3. בנוגע למצלמות המהירות החדשות, כגון מצלמות וידאו אנליטיקה, מצלמות מהירות ממוצעת וממא"ל – מד מהירות אלקטרוני, ראו תומר הדר "מערכת המצלמות החדשה של המשטרה תכלול גם מכוונת מהירות אלקטרונית ניידת מדגם חדש" **כלכליסט** (15.5.2023) https://www.calcalist.co.il/local_news/car/article/ryslzrjbh.

[51] נתונים אלו כוללים: מספר לוחית הרישוי, צילומי וידאו וצילומי סטילס, לרבות תמונת הרכב והנוסעים בתוכו וכן תמונות ממוקדות של לוחית הרישוי, שעליהן מוטבעים מועד הצילום ומיקום מדויק של המצלמה. לפי פרסומים בעיתונים מהשנים האחרונות, המערכת פרוסה בכבישים ראשיים בדרום הארץ, בכניסות לירושלים ולאשדוד, בשרון, במעברים בין ישראל לשטחים וייתכן שגם באזורים נוספים. גולדשמידט, לעיל ה"ש 5, בעמ' 13; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 9,5,1; דניאל דולב "המשטרה מחזיקה מאגר מידע סודי על תנועות של אזרחים" **וואלה חדשות** (6.5.2020) https://news.walla.co.il/item/3355178.

[52] מפרוטוקולים של דיונים פליליים שבהם הובאו ראיות ממערכת "עין הנץ" ניתן ללמוד כי השימוש במערכת נעשה באופן שגרתי על ידי חוקרים ובוחני תנועה בתיקי חקירה מסוגים שונים, כגון: גנבת רכבים, פשעים חמורים, תאונות דרכים ועוד, לרבות על ידי אגף התנועה, סיירי אגף המבצעים, שוטרי מג"ב ויחידות אח"ם ואג"ם ייעודיות. ראו: מ"ת (מחוזי ב"ש) 44808-05-20 **מדינת ישראל נ' אבו קטיפאן** (נבו 10.6.2020); מ"ת (מחוזי חי') 5518-09-20 **מדינת ישראל נ' חטיב** (נבו 15.10.2020) (להלן: עניין **חטיב**); בע"ח 1011-09-20 **אליאב נ' מדינת ישראל** (נבו 22.10.2022); כפי שצוין בעתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 4.

[53] ינובסקי "בשידור חי", לעיל ה"ש 6; תמרי, לעיל ה"ש 6.

[54] הרפז, לעיל ה"ש 7, בעמ' 72; אוסלנדר, לעיל ה"ש 4; וינרב, לעיל ה"ש 7; ינובסקי "בשידור חי", לעיל ה"ש 6.

[55] רענן בן צור "נהגים, שימו לב: המשטרה החלה להפעיל רחפנים בכבישים" **ynet** (11.7.2018) https://www.ynet.co.il/articles/0,7340,L-5308143,00.html (להלן: בן צור); אלון חכמון "מזהה עבירות ממאות מטרים: המשטרה החלה להפעיל רחפנים בכבישים" **מעריב** (11.7.2018) https://www.maariv.co.il/news/israel/Article-650785 (להלן: חכמון (11.7.2018)); וינרב, לעיל ה"ש 7.

[56] שם.

[57] נוהל אג"מ 220.003.16 "נוהל מצלמות גוף" (29.8.2021) (להלן: נוהל מצלמות גוף). כ־1,100 שוטרים מיחידות הסיור המיוחדות (יס"מ) צוידו במצלמות גוף. זאת, לאחר שהוצמדו כ־5,300 מצלמות מסוג זה לשוטרי סיור עירוני, תנועה ושיטור. כמו כן, יוצמדו כ־2,500 מצלמות לשוטרי מג"ב. בסופו של התהליך צופים במשטרה שכעשרת אלפים שוטרים יפעלו עם מצלמות גוף עליהם. ראו לירן לוי "המשטרה תצמיד 1,100 מצלמות גוף לשוטרי יס"מ" **וואלה חדשות** (16.6.2020) https://news.walla.co.il/item/3367350; אלי סניור, אלכסנדרה לוקש וניר כהן "ימנעו את ההרג הבא? מצלמות גוף יוצמדו לשוטרים" **ynet** (20.1.2019) https://www.ynet.co.il/articles/0,7340,L-5449740,00.html.

[58] טנא, לעיל ה"ש 22, בעמ' 424–425; BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED (Anil K. Jain et al. eds., 2006).

[59] טנא, לעיל ה"ש 22, בעמ' 424.

נאספו בעבר מאזרחים באופן וולונטרי לשם הנפקת תעודות זהות חכמות.[60] ניתן לזהות תווי פנים באמצעות שימוש במצלמות מיוחדות בעלות יכולות מוגברות לזיהוי תווי פנים או באמצעות מצלמות רגילות המחוברות לתוכנה של זיהוי פנים.[61] בישראל קודמה הצעת חוק שתאפשר למשטרת ישראל להשתמש בטכנולוגיות לזיהוי תווי פנים. נטען כי משטרת ישראל כבר משתמשת בטכנולוגיה זו בגדה המערבית ובמזרח ירושלים.[62]

אמצעים נוספים המסייעים למעקב אחר מעשים הם *חיישני קול* אשר מוצבים במרחב הציבורי ומזהים קולות ייחודיים, כגון: נפץ, צעקות או שבירת זכוכית, ומכוונים את המצלמה למקום ההתרחשות.[63] אמצעים נוספים המשמשים את משטרת ישראל לשם תיעוד מעשי האדם הם *נתוני מיקום*. הכלים הטכנולוגיים המאפשרים מעקב אחר מיקומו של אדם הם מכשיר GPS,[64] אזיק אלקטרוני ורשת המצלמות המשטרתית "עין הנץ" הפרוסה ברחבי הארץ.[65]

<u>*במרחב הפרטי*</u>: לשם תיעוד מעשי האדם בכלים טכנולוגיים במרחב הפרטי, המשטרה מתקינה תוכנות רוגלה ופריצה למחשבים וטלפונים ניידים. מדובר בתוכנות מחשב שאותן מחדירים למחשבים ומערכות מחשוב, ללא הסכמת המשתמש, למטרות איסוף מידע מסוגים שונים.[66] באמצעות תוכנות אלו ניתן לבצע מעקב על הקשות המקלדת של האדם. כמו כן, ניתן לעקוב אחר התוכנות, האפליקציות והאתרים שבהם הוא משתמש. בנוסף, ניתן לצלם את המסך ולפתוח את המצלמות בטלפונים הניידים ובמחשבים.[67] לאחרונה רכשה משטרת ישראל תוכנת רוגלה בשם "אקוי", המאפשרת השגת *נתוני מיקום* על סמך שימוש בטלפון נייד. באמצעות הזנת מספר טלפון או אזור גאוגרפי מתקבלים מיקומו של אדם ומסלול תנועתו ואף מידע נוסף מהאפליקציות שעל מכשיר היעד. עדיין לא ידוע האם משטרת ישראל משתמשת בתוכנה זו בפועל.[68] בשנים האחרונות השתמשה המשטרה ברוגלות ב־1,086 מקרים.[69]

לשם איסוף נתונים בנוגע לדיבור מבצעת משטרת ישראל *האזנת סתר לשיחות* באמצעות התקנת מכשירי האזנה פיזיים לטלפונים נייחים ובחדרים במבנים.[70] בכל שנה מתקבלים למעלה מ־3,000

---

[60] שם, בעמ' 421.

[61] רשת הטלוויזיה האמריקאית NBC פרסמה באוקטובר 2019 תחקיר, ולפיו משטרת ישראל משתמשת בטכנולוגיה לזיהוי תווי פנים במעקב אחר חשודים בגדה וברחובות ירושלים המזרחית. האגודה לזכויות האזרח בישראל עתרה לבית המשפט בדרישה לדעת אם משטרת ירושלים עושה שימוש בטכנולוגיה לזיהוי פנים באזור העיר העתיקה. מהמשטרה נמסר: "לא נעשה שימוש בטכנולוגיה הזו". לאחר מכן המשטרה והשר לביטחון פנים פנו ליועמ"שית בבקשה להתקין מערכת לזיהוי פנים לאורך רחובות שבהם יתקיים מצעד הגאווה בירושלים השנה; תמרי, לעיל ה"ש 6; חכמון (2.6.2022), לעיל ה"ש 6.

[62] ב־18.9.2023 אישרה ועדת השרים לחקיקה את טיוטת חוק לתיקון פקודת המשטרה (תיקון מס'40) (מערכות צילום מיוחדות), התשפ"ג–2023 (להלן: הצ"ח מערכות צילום מיוחדות).

[63] אוסלנדר, לעיל ה"ש 4.

[64] עתירת האגודה לזכויות האזרח, לעיל ה"ש 5.

[65] חסד"פ נתוני תקשורת, לעיל ה"ש 11; חוק בזק, לעיל ה"ש 11; חוק התקשורת (בזק ושידורים), התשמ"ב–1982; חוק השב"כ, לעיל ה"ש 11; עניין **חטיב**, לעיל ה"ש 52.

[66] טל מימרן ועדן פרבר "סייבר התקפי?" **תכלית – המכון למדיניות ישראלית** 2–3 (2023).

[67] עמרי רחום־טוויג "חיפושים ממוחשבים – על סמכויות חקירה בגישה מרחוק למחשבים ומידע דיגיטלי" **פורום עיוני משפט** מו (2022); אוסלנדר, לעיל ה"ש 4.

[68] טכנולוגיות מעקב של חברת רייזון מסוג ADINT משתמשות בנתוני מיקום ונתונים נוספים שהמשתמש בטלפון החכם אישר לתוכנות המותקנות אצלו בטלפון להשתמש בהם והן מוכרות מידע זה לגופים אחרים. ברגע פרסום המידע למכירה תוכנה זו מנצלת פרצה על מנת להגיע למידע. התוכנה נקראת "אקוי" ECHO. ראו תומר גנון "הדלת האחורית שמאפשרת למשטרה לקבל מידע מניידים" **כלכליסט** (30.5.23) https://www.calcalist.co.il/local_news/article/sytburfi2 (להלן: גנון (30.5.2023)).

[69] תומר גנון "הפרקליטות בוחנת בדיקת כל התיקים שבהם השתמשו ברוגלה" **כלכליסט** (6.6.2023) https://www.calcalist.co.il/local_news/article/h1wa1ssl3 (להלן: גנון (6.6.2023)); עמיר כהנא **רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה** 46–47 (מחקר מדיניות 123, המכון הישראלי לדמוקרטיה 2019); משרד המשפטים **דו"ח הצוות לבדיקת האזנות סתר לתקשורת בין מחשבים** (2022) (להלן: דו"ח מררי).

[70] חוק האזנת סתר, התשל"ט–1979 (להלן: חוק האזנת סתר).

היתרים להאזנת סתר במדינת ישראל.[71] בפסק דין זאבי מציינת השופטת פרוקצ׳יה את היקפה של האזנת הסתר: *״חיבור קו טלפון לאמצעי האזנת סתר מביא לקליטה פיסית של כל השיחות הנכנסות והיוצאות ממנו בלא אבחנה. שיחות אלה כוללות, בין היתר, שיחות של החשוד עם אחרים שאינן נוגעות כלל לפרשה הנחקרת; הן עשויות אף לכלול שיחות של אחרים שהחשוד כלל אינו שותף להן ואינו מעורב בתוכנן. וכך, האזנת הסתר על פי טיבה הטכני עשויה לכסות לא רק שיחות רלבנטיות לחקירה של החשוד אלא גם שיחות שאין להן כל קשר לפרשה הנחקרת, או שהזיקה שלהן לחקירה היא רחוקה ביותר וזניחה.״* [72]

גם בתוכנת רוגלה נעשה שימוש לשם איסוף מידע בנוגע לדיבור, באמצעות גישה לאימיילים והודעות טקסט ובאמצעות הפעלת המיקרופון שבטלפון החכם, כך שהוא מקליט את הדברים הנאמרים בסביבתו.[73]

__ב.1.ב. איסוף המידע בידי גופים אחרים:__

__במרחב הציבורי__: לשם איסוף מידע על מעשי האדם משטרת ישראל יכולה לפנות אל גופים ציבוריים ופרטיים בבקשה להעביר אליה *צילומי וידאו וסטילס* שצולמו במרחב הציבורי. לדוגמה, צילומים ממצלמות אבטחה של בתי עסק ומצלמות שהותקנו על גבי רכבים למטרות ביטוח.[74] אם בעלי המצלמות אינם מסכימים למסור את הצילומים, יכולה משטרת ישראל להגיש בקשה לצו חיפוש או צו להצגת חפץ.[75]

דוגמה נוספת למצלמות שלא הותקנו על ידי משטרת ישראל, אך יש לה גישה אליהן, היא מצלמות ״עיר חכמה״ שהותקנו על ידי העיריות השונות. בתל אביב לדוגמה, הוצבו ברחובות העיר כאלפיים מצלמות, כעשרים מצלמות גוף הוצמדו לפקחים ונעשה שימוש בשתי מצלמות על גבי רחפנים.[76] החברה הממשלתית נתיבי איילון מפעילה מערכת מצלמות דומה שמסייעת לאכיפת השימוש התקין בכבישים.[77] מערכת טרופיקון היא מערכת מצלמות הפרוסה במנהרות ומסייעת בניהול התנועה ואיתור אירועים חריגים,[78] ובחופי הים מותקנת מערכת מצלמות שתפקידה לאתר מקרי טביעה.[79] למשטרת ישראל יש גישה לצילומים אלו. לעיתים המשטרה מבקשת ישירות מהעירייה גישה לצילומים ולעיתים היא נדרשת לצו שופט.[80]

---

[71] גנון (6.6.2023), לעיל ה״ש 69; כהנא, לעיל ה״ש 69; דו״ח מררי, לעיל ה״ש 69.

[72] בש״פ 2043/05 **מדינת ישראל נ׳ זאבי**, עמ׳ 449 לפסק הדין של השופטת פרוקצ׳יה (נבו 15.9.2005) (להלן: עניין **זאבי**); בג״ץ 1563/96 **כץ נ׳ היועץ המשפטי**, פ״ד נה(1) 529 (1997).

[73] בירנהק מאוריך לפגסוס, לעיל ה״ש 10; עמיקם הרפז ומרים גולן **משפט ושיטור: זכויות אדם וסמכויות משטרה** 330 (2018).

[74] אוסלנדר, לעיל ה״ש 4.

[75] וינרב, לעיל ה״ש 7; ס׳ 43 לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ״ט–1969 (להלן: פסד״פ מעצר וחיפוש): ״ראה שופט שהצגת חפץ נחוצה או רצויה לצורכי חקירה או משפט, רשאי הוא להזמין כל אדם, שלפי ההנחה החפץ נמצא בהחזקתו או ברשותו להתייצב ולהציג את החפץ, או להמציאו בשעה ובמקום הנקובים בהזמנה״; ס׳ 23 לפסד״פ מעצר וחיפוש: ״רשאי שופט ליתן צו לערוך חיפוש בכל בית או מקום (להלן – צו חיפוש) אם – (1) החיפוש בו נחוץ כדי להבטיח הצגת חפץ לצורך כל חקירה, משפט או הליך אחר״; ב־15.5.2023 ניתנה הוראת שעה למשך שנה (ס׳ 25(ב) לפסד״פ מעצר וחיפוש) לפיה שוטר יכול להיכנס לחפש בבתים או מקומות ללא צו חיפוש כאשר ישנו חשד סביר שיש שם תיעוד או מצלמה שעשויים לשמש ראיה לביצוע פשע חמור או עבירה לפי סעיפים מסוימים המנויים שם.

[76] הרפז, לעיל ה״ש 7, בעמ׳ 72 ; אוסלנדר, לעיל ה״ש 4; וינרב, לעיל ה״ש 7.

[77] אוסלנדר, לעיל ה״ש 4.

[78] גולדשמידט, לעיל ה״ש 5, בעמ׳ 16.

[79] אוסלנדר, לעיל ה״ש 4.

[80] ס׳ 23,34 לפסד״פ מעצר וחיפוש.

משטרת ישראל עוקבת אחר פעילות הגולשים ברשת ויכולה לאתר צילומי סטילס ווידאו ברשתות החברתיות, אשר מועלים באופן וולונטרי על ידי המשתמשים ברשת.[81] לשם זיהוי האדם נדרש איסוף *נתונים ביומטריים* במרחב הציבורי. גם את תווי הפנים שנאספו במצלמות העירייה וגופים אחרים ניתן לזהות באמצעות תוכנות לזיהוי תווי פנים.[82]

סוג נוסף של מידע על מעשים הוא *נתוני מיקום*. ניתן להשיג נתונים על אודות מיקום האדם באמצעות *איכון טלפונים ניידים*.[83] כאשר מכשיר הקצה משדר, הוא ניתן לאיכון, כלומר, ניתן לקבוע את מיקומו על ידי הצלבת מידע מהאנטנות הסלולריות שבהן הוא נקלט. חברות סלולר מסוגלות לבצע איכון של מכשירי המנויים שלהן.[84] הנתונים הזמינים למשטרת ישראל שאותם אוספות חברות הסלולר הם נתונים טכניים של תקשורת טלפונים ואינטרנט, כגון: יעדי שיחות, מספרי ברזל של מכשירים, נתוני איכון וכתובות IP.[85] משטרת ישראל משתמשת בטכנולוגיה של "איכון הפוך" שבאמצעותה היא משיגה נתוני מיקום של מכשירים סלולריים בתא שטח מסוים מבלי לדעת מראש את זהותם או את זהות בעליהם על מנת לזהות חשודים.[86]

משרד התחבורה הוא גוף מנהלי נוסף שאוסף מידע בנוגע לנוסעי התחבורה הציבורית, באמצעות מעקב אחר תשלום עבור הנסיעה בכרטיס "רב קו" או באפליקציות. אפליקציות אלו מאפשרות גישה לנתוני המיקום המדויקים של הטלפונים הניידים שמסופקים גם כאשר המשתמש אינו נוסע בתחבורה ציבורית. מאגר זה אינו מוסדר בחוק, ולכן אין איסור מפורש של המחוקק על שימוש משטרתי במידע זה.[87]

לשם איסוף מידע בנוגע לדיבור באמצעים שלא הותקנו על ידי משטרת ישראל במרחב הציבורי, מחפשת המשטרה ברשתות חברתיות תכתובות וצילומי וידאו שהועלו באופן וולונטרי וחשופים לציבור.[88] בנוסף, המשטרה יכולה לבקש להשתמש במיקרופונים הפרוסים ברחובות הערים ומתעדים קולות. ייתכן כי שיחה שהתרחשה במרחב הציבורי תיקלט במיקרופונים אלו.[89]

במרחב הפרטי: אנשים רבים מתקינים מצלמות בתוך הבתים שלהם והן מתעדות מרחבים פרטיים.[90] מצלמות מותקנות גם בגני ילדים, בתי ספר ובתי חולים גריאטריים.[91] במקרים שבהם

---

81 אוסלנדר, לעיל ה"ש 4; מידע זה נאסף בשיתוף פעולה עם תאגידים פרטיים או גופים אחרים מכוחות הביטחון ומחלקת הסייבר במשרד המשפטים.

82 טנא ,לעיל ה"ש 22, בעמ' 431.

83 חסד"פ נתוני תקשורת; חוק בזק; חוק השב"כ.

84 עמיר כהנא "איכון הפוך (Reverse Geolocation): האם לתת למשטרה את 'כלי' השב"כ בזעיר אנפין?" **האוניברסיטה העברית בירושלים שיח.זכויות@מינרבה** (26.3.2023) (להלן: כהנא 2023). https://openscholar.huji.ac.il/minervacenter/blog/cahane.

85 תהילה שוורץ אלטשולר "משבר הקורונה – המשמעות של הסמכת השב"כ למעקב אחר אזרחים" **המכון הישראלי לדמוקרטיה** (17.3.2020) https://www.idi.org.il/articles/30991 (להלן :שוורץ אלטשולר); חסד"פ נתוני תקשורת.

86 כהנא 2023, לעיל ה"ש 84.

87 מבקר המדינה **דוח שנתי 70ב** 264–271 (2020) (להלן: **דוח שנתי 70ב**).

88 אוסלנדר, לעיל ה"ש 4.

89 וינרב, לעיל ה"ש 7.

90 וינרב, לעיל ה"ש 7.

91 ס' 3(א) לחוק התקנת מצלמות לשם הגנה על פעוטות במעונות יום לפעוטות, התשע"ט–2018: "מפעיל מעון יום לפעוטות אחראי להתקנת מצלמות שיתעדו את הנעשה במעון יום לפעוטות, בכל השעות שבהן פעוטות שוהים במעון, בהקלטת וידאו בלא קולי"; הנחיית רשם מאגרי מידע 4/2012 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן" (21.10.2012) (להלן: הנחיית הרשם למצלמות מעקב); הנחיית רשם מאגרי מידע 5/17 "שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה" (17.10.2017); חוזר מנכ"ל משרד החינוך 0119 "מצלמות במוסדות החינוך – הסדרת הכנסתן ואופן התקנתן" (3.5.2015); ס' 33 לפקודת בריאות העם, 1940; תקנות בריאות העם (התקנת מצלמות בבית חולים גריאטרי), התשע"ז–2017; בפסק הדין ת"א (שלום קר') 20750-03-18 **זוארץ נ' כהן**

בעלי המצלמות אינם מסכימים למסור את הצילומים למשטרת ישראל, ניתן לבקש צו חיפוש או צו להצגת חפץ משופט לשם קבלתם.[92]

משטרת ישראל יכולה לבקש צו חיפוש בחומר מחשב ולאסוף מחשבים וטלפונים ניידים מאזרחים. בהתאם לאמור בצו, יכולה משטרת ישראל לפרוץ אל המחשבים והטלפונים החכמים ולאסוף מהם מידע מסוגים שונים.[93] על כך הרחיבה השופטת חיות בעניין אוריך: *"המחשב, ובפרט הטלפון החכם, מהווה למעשה מעין "מאגר" מרוכז של מידע במלל, בתמונות, בהקלטות ובסרטונים, שממנו ניתן ללמוד על מחשבותיו, רגשותיו וחוויותיו של אדם, וכן על ההתקשרויות – לעתים האינטימיות ביותר – שלו עם אחרים."*[94] השופט אלרון כתב בעניין אוריך: *"באמצעות מחשבו ומכשיר הטלפון הנייד החכם של אדם ניתן לא פעם ללמוד על עברו ועל תוכניותיו לעתיד, כמו גם על תחביביו, לבטיו, רחשי ליבו, מכריו, אהוביו ושונאיו. מקומות בהם שהה מתועדים עם ציון גיאוגרפי מדויק, לעיתים בליווי תמונות, ונאגרים מידי יום במכשיריו ובחשבונותיו במרשתת; ובמקרים רבים, סודותיו וסודות חבריו שמורים במכשיר הטלפון החכם או במחשב שברשותו."*[95]

ניתן לאסוף *תמונות סטילס*, *וידאו*, *שמע וטקסט* המתעדים מעשים ודיבור ברשת החברתית במרחב הפרטי. כלומר, בפרופילים שאינם פתוחים לציבור הרחב. זאת על ידי פריצה לפרופיל, התחזות לאדם אחר או על ידי בקשת המידע מהרשת החברתית. אם גורמים מסחריים המנהלים פלטפורמות שונות באינטרנט יסרבו למסור מידע למשטרת ישראל, ניתן לבקש צו משופט להשגת המידע המבוקש.[96]

לשם זיהוי האדם נדרש איסוף *נתונים ביומטריים* במרחב הפרטי. דוגמה לכך היא בדיקות גנטיות, אשר מזהות נטיות רפואיות של האדם.[97] פרויקט מאגר מידע גנטי בשם "פסיפס" צפוי לשלב נתונים גנטיים עם מידע מקופות החולים כדי לבנות כלים לחיזוי מחלות ומניעתן.[98] נתונים נוספים המאפשרים תיעוד מעשים נאספים מרשת החשמל החכמה. רשת זו יכולה לדווח לחברת החשמל מתי האזרחים משתמשים במכשירים שונים בבית, כגון: דוד חשמלי, מכונת קפה, תנור, רמקולים וטלוויזיות.[99] נתונים נוספים שנאספים נוגעים להרגלי השימוש של בני אדם באינטרנט ובטלוויזיה. בכוונת משרד התקשורת לדרוש את המידע האישי של כל מנוי שמחובר לאינטרנט, לכבלים או לרשת הסלולרית.[100] לבסוף, בנוגע לנתונים כלכליים, בנק ישראל פעל לאיסוף כל המידע הפיננסי על הציבור הרחב שבידי חברות האשראי והבנקים, כולל הוצאות בכרטיסי אשראי, שימוש בצ'קים

(נבו 23.11.2021), בית משפט השלום פסק כי הרכוש המשותף בבניין הוא מרחב ציבורי, ובעל הדירה אינו יכול לצפות לפרטיותו באזורים המשותפים בבית המשותף. לכן ניתן להתקין מצלמות אבטחה בשטח המשותף.

[92] ס' 23, 43 לפסד"פ מעצר וחיפוש.

[93] ס' 23 לפסד"פ מעצר וחיפוש; 25(ב) הוראת שעה מיום ה־15.5.2023 למשך שנה.

[94] דנ"פ 1062/21 **אוריך נ' מדינת ישראל**, פס' 29 לפסק הדין של השופטת חיות (נבו 11.1.2022) (להלן: עניין **אוריך**). שם הדיון התמקד בשאלה מהם תכליתה והיקפה של הוראת סעיף 23א לפסד"פ מעצר וחיפוש. ההוראה מסדירה את סוגיית החדירה לחומר מחשב, הכולל גם טלפונים חכמים, לצורך חיפוש בו ואת הפגיעה בפרטיות הנובעת מהוראת סעיף זה. השופטת חיות הפנתה לקטע מע"פ 8627/14 **דביר נ' מדינת ישראל**, פס' 7 לפסק הדין של השופט עמית (נבו 14.7.2015).

[95] עניין **אוריך**, לעיל ה"ש 95, בפס' 4 לפסק הדין של השופט אלרון.

[96] Mateescu et al., לעיל ה"ש 9, בעמ' 4; ס' 23, 43 לפסד"פ מעצר וחיפוש.

[97] טנא, לעיל ה"ש 22, בעמ' 431.

[98] אוסלנדר, לעיל ה"ש 4.

[99] גולדשמידט, לעיל ה"ש 5, בעמ' 3; טנא, לעיל ה"ש 22, בעמ' 431.

[100] אוסלנדר, לעיל ה"ש 4.

ומשיכת מזומנים.[101] עד כה לא הוצגו ראיות לכך שמשטרת ישראל משתמשת בנתונים אלו, אך ייתכן שבעתיד תבקש משטרת ישראל להשתמש בנתונים אלו.[102]

ניתן לאסוף *נתוני מיקום ברשתות החברתיות ובאינטרנט* כאשר אנשים מתייגים את עצמם במקומות מסוימים או מפרסמים תמונות המסגירות את מקומם.[103] תוכנות מבוססות מיקום כמו ווייז משתפות מידע על מקום הימצאותו של המשתמש ומאפשרות מעקב פיזי אחר האדם. אם החברות המסחריות שבבעלותן תוכנות אלו לא ימסרו את המידע מרצון, יכולה משטרת ישראל לבקש צו חיפוש או צו השגת חפץ משופט.[104]

ב.2. שלב שני – שמירת המידע: בשלב השני, משטרת ישראל אוגרת את המידע שנאסף במאגרי מידע. ישנם שני סוגים של מאגרי מידע: מאגרים אשר מנוהלים על ידי המשטרה ומאגרים אשר מנוהלים בידי רשות אחרת ולמשטרה ניתנת גישה למידע.

ב.2.א. מאגרי מידע המנוהלים על ידי המשטרה: דוגמאות למאגרים שבהם נשמר מידע שנאסף באמצעים טכנולוגיים למעקב אשר מנוהלים על ידי המשטרה הן מאגר מערכת "עין הנץ" ומאגר צילומי מצלמות גוף של שוטרים.[105] מערכת "עין הנץ" שומרת תיעוד של כלי הרכב שצולמו על ידה לתקופה שאינה ידועה. במקרה שבו רכב, שלא היה מוכר לפני כן למשטרה, יהיה מעורב בפיגוע או באירוע פלילי, ניתן יהיה לחפש אותו במערכת ולבדוק את מסלול נסיעתו.[106] גם סרטי הווידאו המצולמים במצלמות גוף של שוטרים נשמרים בידי המשטרה. לדוגמה, תיעוד של מתן דו"ח תנועה נשמר למשך שמונה שנים, חומרים המסווגים כ"לא רלוונטיים" נשמרים לשנה לפחות.[107]

ב.2.ב. מאגרי מידע המנוהלים על ידי רשויות אחרות: דוגמה למאגר שמנוהל על ידי רשויות אחרות ולמשטרה יש גישה אליו הוא המאגר הביומטרי. לאזרחי ישראל הופקו תעודות זהות חכמות ודרכונים עם שבב אלקטרוני, הכוללים נתוני זיהוי ביומטריים (תמונת תווי פנים ולמי שהסכים לספקן גם תמונות שתי טביעות האצבעות המורות) שנשמרים במאגר מידע מרכזי.[108] עד היום הצטברו במאגר הביומטרי 5.5 מיליון תמונות פנים ו־3.8 מיליון טביעות אצבע.[109] למאגר מידע זה יש למשטרת ישראל גישה מוגבלת למטרות של ביטחון לאומי ואכיפת חוק.[110] משטרת ישראל משתמשת במאגר הביומטרי במצבים שבהם ישנו אדם שאינו רוצה או אינו יכול להזדהות (אין לו תעודת זהות או כשמדובר בגופה) ובמצבים שבהם אין התאמה בין האדם, טביעת האצבע שלו והתעודה שהציג.[111]

---

[101] אוסלנדר, לעיל ה"ש 4.

[102] לכן ראוי להתייחס לקטגוריות חדשות של מידע ולהעלות בפני המחוקק את השאלה האם ראוי שמשטרת ישראל תהיה מוסמכת בחוק לאסוף מידע מסוג זה.

[103] Mateescu et al., לעיל ה"ש 9, בעמ' 4.

[104] ס' 23, 43 לפסד"פ מעצר וחיפוש.

[105] לוי, לעיל ה"ש 57.

[106] עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 5, ס' 19.

[107] אוסלנדר, לעיל ה"ש 4.

[108] טנא, לעיל ה"ש 22, בעמ' 421; על פי חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009 (להלן: חוק זיהוי ביומטרי).

[109] אוסלנדר, לעיל ה"ש 4.

[110] טנא, לעיל ה"ש 22, בעמ' 422; עומר כביר "למרות הכישלון בבג"ץ: זו ההצלחה הגדולה ביותר של המאבק במאגר הביומטרי" **כלכליסט** (13.7.2022) https://www.calcalist.co.il/calcalistech/article/sjrdvehjc (להלן: כביר (13.7.2022)).

[111] טנא, לעיל ה"ש 22, בעמ' 428, 448; ס' 17 לחוק זיהוי ביומטרי מאפשר לבית משפט השלום להתיר העברת מידע מהמאגר הביומטרי למשטרה לצורך חקירת עבירות או לצורך אימות או בירור זהותו של אדם ,לרבות גופה, שזהותו

רשויות נוספות אשר מנפיקות תעודות שומרות נתונים ביומטריים. למשטרת ישראל יש גישה למאגרים אלו. כך, למשל, מאגר תמונות רישיונות הנהיגה של משרד התחבורה משמש גם את משטרת ישראל.[112] הרשות הארצית לתחבורה ציבורית מחזיקה במאגר של 6.1 מיליון תמונות משתמשים המזוהים בשם ובמספר זהות ולכל אחד היסטוריית תנועה מפורטת.[113] במצלמות של החברה הממשלתית נתיבי איילון, האוכפות שימוש בנתיבי פלוס, המידע נשמר במאגר אנונימי, כלומר, כזה שאינו כולל את צילומי פני הנוסעים.[114] בלשכת התעסוקה אספו רבע מיליון טביעות אצבע של דורשי העבודה המזדהים באמצעות מערכת "התייצבומט".[115] ברשות שדות התעופה נאספו 1.3 מיליון טביעות כף יד באמצעות מערכת לזיהוי מהיר שהותקנה בנתב"ג.[116] בשירות בתי הסוהר משתמשים במערכת "שחף" לזיהוי קולי של אסירים. לשם כך מחזיקים במאגר דגימות קול של כ־5,500 אנשים.[117] תיתכן גישה של משטרת ישראל למאגרים אלו. במסגרת חוק איסור הלבנת הון הוקם מאגר מידע למטרות איסור הלבנת הון ומימון טרור. משטרת ישראל מוסמכת להשתמש במאגר לשם חקירת עבירות נוספות שאינן מנויות בחוק כ"עבירות מקור".[118]

__ב.3. שלב שלישי – ניתוח המידע:__ בשלב השלישי משטרת ישראל וגופים נוספים במערכת אכיפת החוק משתמשים במידע שנאסף ומנתחים אותו לצרכים שונים, כגון: זיהוי (פנים, רכבים והתרחשויות) ויצירת תחזיות פשיעה.

__ב.3.א. זיהוי וחיפוש חשודים__: מערכות המצלמות השונות אשר נמצאות בשימוש משטרת ישראל הן בעלות טכנולוגיה מתקדמת אשר מאפשרת זיהוי כגון: זיהוי לוחיות רישוי, זיהוי תווי פנים וזיהוי אירועים והתרחשויות.[119] *זיהוי פנים* הוא תהליך אוטומטי של השוואת שתי תמונות שונות של פנים על מנת לבחון אם מדובר באותו אדם. מערכות לזיהוי פנים מאפשרות להשתמש בפרמטרים ביומטריים המאפיינים פנים של אדם מסוים כדרך לאימות זהותו. מאפיינים ביומטריים נוספים המשמשים את משטרת ישראל לשם זיהוי האדם הם טביעות אצבע ודנ"א.[120] בשלב ניתוח המידע מערכות אלה משוות בין הדגימות הביומטריות לבין נתונים הנאגרים במאגר ומחליטות האם הושג זיהוי או היעדר זיהוי.[121]

זיהוי לוחיות רישוי מתבצע במערכת "עין הנץ" ובמצלמות "עיר חכמה". טכנולוגיית LPR/ALPR מאפשרות לזהות את מספרי לוחיות הרישוי של רכבים המופיעים בצילום.[122] מערכת "עין הנץ" מסוגלת לזהות כלי רכב ולתעד עבירות שבוצעו ברכב. בנוסף, מאפשרת המערכת שליחת התראות

אינה ידועה או מוטלת בספק, ולצורך איתור נעדרים או שבויים. ס' 18 לחוק מתיר העברת מידע מהמאגר למשטרה אף בלא צו של שופט, אם הדבר דרוש לצורך חקירת חשד בדבר גנבת זהות או זיוף פרטים בתעודה מקורית.

112 **דוח שנתי 70ב**, לעיל ה"ש 87, בעמ' 260–261.

113 אוסלנדר, לעיל ה"ש 4.

114 שם.

115 **דוח שנתי 70ב**, לעיל ה"ש 87, בעמ' 272–276.

116 שם, בעמ' 230.

117 שם, בעמ' 282.

118 טנא, לעיל ה"ש 22, בעמ' 435.

119 גולדשמידט, לעיל ה"ש 5, בעמ' 7; שוורץ אלטשולר וכהנא, לעיל ה"ש 6; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 3–4; תמרי, לעיל ה"ש 6; חכמון (2.6.2022), לעיל ה"ש 6.

120 שוורץ אלטשולר וכהנא, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בעמ' 4.

121 טנא, לעיל ה"ש 22, בעמ' 424–425. כפי שציינתי בשלב איסוף הנתונים הביומטריים ישנן טענות כי משטרת ישראל משתמשת בזיהוי פנים ללא הסמכה בחוק בגדה ובמזרח ירושלים. בנוסף, ישנה הצעת חוק המקדמת את הסמכת המשטרה להשתמש בטכנולוגיה זו.

122 עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 3; המשרד לביטחון פנים – משטרת ישראל "מכרז פומבי: אספקת מערכת LPR נישאות/ניידות/מחסומים" **החשב הכללי** סעיף 2.1 (17.10.2012) https://mr.gov.il/ilgstorefront/he/p/540121 (להלן: מכרז המשטרה).

בזמן אמת על מיקומים של כלי רכב. מערכת זו מתעדת את מיקומם של כלי רכב בזמנים נקובים ואת מסלול נסיעתם. בשל כך, ניתן לבחון את היסטוריית הנסיעה של כלי הרכב.[123] המערכת מסוגלת להשוות את מספרי הרישוי למאגרים שהוגדרו מראש, כמו מאגר כלי הרכב שדווחו כגנובים ומאגר הרכבים שתוקף רישיון הרכב שלהם פג, ולהתריע עליהם.[124] המערכת בעלת יכולת חיפוש ואחזור מידע גבוהה. ניתן לשלוף מידע לפי פרמטרים, כגון: חתכי זמן הצילום ומיקומו. במקרים מסוימים קיימות יכולות זיהוי אוטומטיות, או אוטומטיות למחצה, של אובייקטים שונים בתמונה, למשל: זיהוי של כלי רכב, או הפרדה של הפריטים המופיעים בתמונה כמו אנשים, כלי רכב, בעלי חיים וכדומה.[125]

זיהוי אירועים חריגים: את סרטי הווידאו שנקלטו במצלמות עירוניות בפרויקט "עיר חכמה" ניתן לעבד באמצעות טכנולוגיית ניתוח וידאו לעיבודי תנועה או לזיהוי פעילות חריגה. ניתוח המידע מתחלק לשתי יכולות טכנולוגיות: האחת מתבססת על זיהוי פרמטרים קבועים מצילומי וידאו וסטילס ומהקלטות שמע. הפרמטרים הקבועים בניתוח צילומי הווידאו הם: כיוון תנועה, זיהוי התנועה במרחב נתון, זיהוי התנועה בשעות חריגות, השתנות הרקע, כמויות של עצמים או אנשים, חציית קווים, כניסה למתחם והסרה או הוספה של עצם במרחב. היכולת הטכנולוגית השנייה היא זיהוי התנהגויות חריגות במרחב, לאור למידת השגרה של המתרחש במרחב, באמצעות בינה מלאכותית. ההתנהגויות החריגות המזוהות הן: חציית קו לבן או נסיעה בניגוד לכיוון התנועה, התקהלות חשודה, אזרחים שבורחים ממקום שבו אירע אירוע אלים ועוד.[126] בנוסף, ישנן תוכנות אשר מאפשרות לזהות איומים ביטחוניים או כוונות עברייניות בהתבסס על שפת גוף או הבעות פנים. המצלמות בפרויקט "עיר ללא אלימות" לא כללו מערכות מתקדמות לניתוח הנתונים, אבל במקרים רבים הרשויות רכשו את הטכנולוגיה על דעת עצמן.[127]

כלי מעקב באינטרנט מאפשר לרשויות אכיפת החוק לבצע באופן אוטומטי ניטור רציף של פעילות מקוונת באמצעות אלגוריתמים לשם איתור מילים וביטויים מסוימים ברשתות החברתיות. נעשה שימוש בבינה מלאכותית על מנת לנתח ולזהות התבטאויות חריגות בתמונות ובטקסט.[128] בנוסף, קיים שימוש בתוכנות תיוג גאוגרפי להשגת נתוני מיקום מהרשתות החברתיות. זאת, לשם תגובה ראשונית למצבי חירום ולשם מעקב אחר אזורי התקהלויות, כגון: קונצרטים והפגנות ציבוריות.[129]

__ב.3.ב. חיזוי תרחישים פליליים__: משטרת ישראל אוספת מידע מהרשתות החברתיות וממאגרי מידע נוספים.[130] את המידע הנאסף מנתחים באמצעות בינה מלאכותית. זאת, באמצעות חשיפת מערכת הנוירונים המלאכותית למידע רב על מנת שהיא תלמד את דפוסי הפשיעה, בדרך שבני אדם אינם מסוגלים לה. לבסוף מפיקה המערכת תחזיות פשיעה.[131] משטרת ישראל משתמשת בכמויות המידע האין־סופיות הללו ומייצרת ידע שמתיימר למנוע פשיעה מראש.[132] דוגמאות לכלים מסוג זה הן: תוכנת PredPol שמספקת תחזיות פשיעה בנוגע למיקום על גבי מפה וזמן היתכנות התרחשות

---

[123] גולדשמידט, לעיל ה"ש 5, בעמ' 7.

[124] מכרז המשטרה, לעיל ה"ש 122, בס' 2 בעמ' 27; ראו גם עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 3.

[125] הנחיית הרשם למצלמות מעקב, לעיל ה"ש 91; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 6.

[126] גולדשמידט, לעיל ה"ש 5, בעמ' 16.

[127] שם.

[128] Elena M. Egawhary, *The Surveillance Dimensions of the Use of Social Media by UK Police Forces*, 17 SURVEILLANCE & SOC'Y 89 (2019) (להלן: Egawhary).

[129] Mateescu et al., לעיל ה"ש 9, בעמ' 4.

[130] Egawhary, לעיל ה"ש 128, בעמ' 89.

[131] הבר וקדוש נוסבאום, לעיל ה"ש 44, בעמ' 10.

[132] Mateescu et al., לעיל ה"ש 9, בעמ' 4.

פשעים, בהתבסס על נתוני עבר.[133] תוכנת HunchLab אשר מתייחסת לגורמים מגוונים כגון: פעילות כנופיות, תנאי מזג אוויר ואירועים חברתיים – כדי לחזות פעילות פלילית.[134] תוכנה לניבוי עבריינות מתווי פנים של חברת פייספשן היא דוגמה נוספת למערכת שמבוססת על בינה מלאכותית לשם הפקת תחזיות פשיעה ושיטור מנבא. משטרת ישראל לא הודתה כי היא משתמשת בתוכנה זו.[135]

בפרק זה הצגתי את הטכנולוגיות השונות שבהן משתמשת משטרת ישראל לשם מעקב אחר האוכלוסייה ויצירת תחזיות פשיעה ליישום טכניקות של שיטור מנבא. כעת אפנה לבחון את החוקים המסמיכים את משטרת ישראל להפעיל אמצעים טכנולוגיים אלו. לאחר מכן ברצוני להציג את הפגיעה בזכות לפרטיות הנגרמת בעקבות שימוש בטכנולוגיות אלו ולהציע חקיקה שתפחית פגיעה זו.

ג. <u>חוקיות השימוש באמצעים טכנולוגיים למעקב ושיטור מנבא</u>

עתה, לאחר שהצגתי את היקף השימוש בכלים טכנולוגיים למעקב ושיטור מנבא, אבחן את המסגרת החוקית המסמיכה את משטרת ישראל להשתמש בכלים אלו. סבך החוקים והנהלים הקיים יוצר כמה מצבים בעייתיים בכל הנוגע להסמכה זו. אבחן את הסמכת משטרת ישראל להשתמש בכלים טכנולוגיים אלו בהתאם לשלושת שלבי ההליך: איסוף, שמירה ועיבוד. בשלב איסוף המידע אתייחס לאמצעים שאין לגביהם הסמכה בחוק. לאחר מכן, אדון בהסמכה הנפרסת על פני כמה חוקים, אשר מנהיגים נהלים שונים, כאשר לא ברור מתי חל כל חוק. לבסוף, אתייחס להסדרים המאפשרים עקיפת בקרה שיפוטית. בשלב שמירת המידע אתייחס להיעדר הסמכה בחוק להפעלת מאגרים ולכך שחלקם אינם רשומים כנדרש. בנוסף, אדון בקטגוריות מידע חדשות שאינן נמצאות בשימוש המשטרה, אך ייתכן שימוש עתידי בהן. בשלב ניתוח המידע אתייחס להיעדר הסמכה בחוק לשימוש בבינה מלאכותית ובאמצעים סטטיסטיים לשם שיטור, ולהסמכה חלקית שאינה מתייחסת להתקדמות הטכנולוגית.

ג.1. הסמכת משטרת ישראל בחוק לאיסוף מידע באמצעות כלי מעקב טכנולוגיים:

<u>כלים טכנולוגיים למעקב שמשטרת ישראל משתמשת בהם ללא חקיקה המסמיכה אותה באופן מפורש להשתמש בהם</u>: דוגמה לכך היא כריית מידע מרשתות חברתיות. אין בחוק הישראלי איסור כללי על פעילות של איסוף תקשורת ומתן היתר במקרים חריגים תוך שמירה על פגיעה מידתית. חסרה התייחסות בחוק הישראלי להסקת מסקנות סטטיסטיות ממידע שהושג באמצעות מעקב מקוון והצלבתו עם מאגרי מידע ממשלתיים אחרים.[136] בנוגע למידע החבוי בפרופילים פרטיים, נדרשת הסמכת המשטרה להשגת המידע, בין אם בדרך של התחזות לאחר לשם קבלת הסכמה של בעל הפרופיל למסירת המידע ובין אם בדרך של פריצה לפרופיל או קבלת המידע בהסכמה ממנהל הפלטפורמה. מצבים אלו דורשים התייחסות, דיון ציבורי ונהלים, המגבילים את אופן הפעולה של השוטרים באיסוף המידע, זאת על מנת למנוע פגיעה לא מידתית בזכות לפרטיות.[137]

---

[133] הבר וקדוש נוסבאום, לעיל ה״ש 44, בעמ׳ 12.

[134] ״הפרופיילינג המשטרתי מעלה חשש לאפקט מצנן שישפיע על שורת זכויות אדם״ (חוות דעת של תהילה אלטשולר שוורץ ועמיר כהנא 22.5.2023).

[135] הבר וקדוש נוסבאום, לעיל ה״ש 44, בעמ׳ 14.

[136] כהנא, לעיל ה״ש 69, בעמ׳ 10–11.

[137] Egawhary, לעיל ה״ש 128, בעמ׳ 93–94. ס׳ 28 לחוק הסדרת סמכויות חקירה, Regulation of Investigatory Powers Act, 2000 (להלן: RIPA), מספק מבנה רגולטורי מקיף המסדיר את היירוט של התקשורת, גישה לנתוני

המדינה טוענת כי השימוש באמצעים טכנולוגיים אלו נעשה בסמכות, שכן הפעלתם נועדה לאפשר למשטרת ישראל לבצע את תפקידה בגילוי עבירות ומניעתן, תפיסת עבריינים והעמדתם לדין ושמירה על הסדר הציבורי, כפי שהוגדרו בפקודת המשטרה.[138] מקור סמכות נוסף שאליו מפנה המדינה הוא החובה המוטלת על משטרת ישראל לחקור עבירות פליליות מכוח הוראות חוק סדר הדין הפלילי.[139]

מנגד, בית המשפט העליון קבע כמה פעמים בעבר כי צורך אינו מקור הסמכה.[140] עצם העובדה שסמכות כזו או אחרת עשויה לסייע למשטרה בשמירה על הסדר הציבורי, אין בו כדי להצדיק את השימוש בה.[141] פעולה מנהלית העלולה להביא לפגיעה בזכויות הפרט חייבת להיות מעוגנת בהסמכה ברורה ומפורשת בחקיקה ראשית.[142] הפניה להוראת חוק כללית ולא מפורשת אינה מספיקה.[143] פעולה בחוסר סמכות היא הפרה של עקרון חוקיות המנהל. לפי עיקרון זה, לרשות מנהלית אין סמכות זולת אותה סמכות שהוענקה לה לפי חוק. החוק הוא לא רק המקור של הסמכות, אלא גם הגבול שלה. ישנה חשיבות יתרה לכך כאשר מדובר בסמכויות המאפשרות פגיעה בזכויות אדם, ובעיקר כאשר מדובר בסמכויותיה של משטרת ישראל לפגוע בזכויות הבסיסיות ביותר של האדם.[144]

דוגמה נוספת לשימוש בכלי טכנולוגי למעקב ללא הסמכה מפורשת בחוק נוגעת לשימוש במיקרופונים במרחב הציבורי. כעיקרון אין להשתמש במצלמות מעקב לצורך הקלטת קול, אלא לפי הוראות חוק האזנת סתר. אך בפועל הרשויות המקומיות ומשטרת ישראל משתמשות במיקרופונים במרחב הציבורי בניגוד לחוק.[145] לאחרונה התקבלה הצעת חוק "מערכות צילום מיוחדות" המסדירה את השימוש במערכת "עין הנץ",[146] זאת לאחר שבמשך שנים השתמשה המשטרה במערכת זו ללא הסמכה מפורשת בחוק. החוק קודם לאחר עתירה של האגודה לזכויות האזרח לבג"ץ בדרישה למנוע שימוש משטרתי במערכת "עין הנץ" ללא הסדרה חוקית.[147] בחוק

תקשורת, מעקב סמוי, שימוש במודיעין ועוד מקורות מודיעין אנושיים סמויים ופיענוח של חומר מוצפן. אסור לשוטרים להשאיר הודעות על קירות ולהצטרף לקבוצות. כל מידע ששוחזר כתוצאה ממחקר סמוי חייב להיות מתועד. כל הפרסונות המזויפות שנוצרו כדי לאפשר לשוטרים לגשת לאתרי מדיה חברתית חייבים להיות רשומים ברשומה של דמות מזויפת. על השוטרים לבקש אישור לבצע מעקב מכוון במסגרת ס' 29 ל־RIPA. על מנת לקיים אינטראקצייה סמויה באינטרנט לשם השגת מידע נדרשים הכשרה נוספת של קצין סמוי ואישור מקור מודיעין אנושי סמוי.

138 ס' 3, 5 לפקודת המשטרה [נוסח חדש], התשל"א–1971.

139 חוק סדר הדין הפלילי [נוסח משולב], התשמ"ב–1982; המדינה טוענת כי ניתן להשתמש באמצעים טכנולוגיים למעקב אחר האוכלוסייה, תוך פגיעה בזכות לפרטיות, מכוח הפטור שניתן למשטרה בס' 19 לחוק הגנת הפרטיות, התשמ"א–1981 (להלן: חוק הגנת הפרטיות); סעיף זה פוטר את רשויות הביטחון מאחריות לפגיעות שנעשו במסגרת תפקידן ולמען מילוי התפקיד כל עוד המעשה נעשה באופן סביר. אך הפטור ניתן רק בדיעבד, ואינו יכול להכשיר מראש מדיניות כללית של רשות מנהלית הכרוכה בפגיעה בפרטיות. ראו עתירת האגודה לזכויות האזרח, לעיל ה"ש 5.

140 עתירת האגודה לזכויות האזרח, לעיל ה"ש 5.

141 שם; טנא, לעיל ה"ש 22.

142 בג"ץ 1437/02 **האגודה לזכויות האזרח נ' השר לביטחון פנים**, פ"ד נח(2) 746, 762 (2004) (להלן: בג"ץ **האגודה לזכויות האזרח**); בג"ץ 2109/20 **בן מאיר נ' ראש הממשלה** (נבו 26.4.2020) (להלן: בג"ץ **בן מאיר**); אודי עציון "המשטרה: לא נפסיק להשתמש במערכת 'עין הנץ' למעקב אחרי נהגים" **כלכליסט** (22.05.2022) https://www.calcalist.co.il/local_news/car/article/bjrtwbdp9; יצחק זמיר **הסמכות המנהלית** כרך א' 73 (2010).ד

143 בג"ץ 6824/07 **מנאע נ' רשות המסים**, פ"ד סד(2) 479, פס' 14 לפסק הדין של השופט פוגלמן (2010) (להלן: בג"ץ **מנאע**); בג"ץ **האגודה לזכויות האזרח**, לעיל ה"ש 142, בעמ' 746, 762; בג"ץ 5870/14 **חשבים ה.פ.ס מידע עסקי בע"מ נ' הנהלת בתי המשפט**, פס' יז' לפסק הדין של השופט רובינשטיין (נבו 12.11.2015).

144 רע"פ 10141/09 **בן חיים נ' מדינת ישראל**, פס' 22 לפסק הדין של הנשיאה ביניש (נבו 6.3.2012) (להלן: עניין **בן חיים**).

145 וינרב, לעיל ה"ש 7; תקנות התעבורה (הפעלת מצלמות בידי רשות מקומית לשם תיעוד שימוש שלא כדין בנתיב תחבורה ציבורית), התשע"ו–2016; חוק לתיקון פקודת התעבורה (מס' 113), התשע"ה–2015, ס"ח 238.

146 החוק לתיקון פקודת המשטרה (מס' 40), התשפ"ד–2024, ס"ח 446 (להלן: תיקון פקודת המשטרה (מס' 40)).

147 עתירת האגודה לזכויות האזרח, לעיל ה"ש 5; בינואר 2022 בית המשפט קרא למשטרה להסדיר בחוק את השימוש במערכת וביקש לנמק מדוע משטרת ישראל אינה מפסיקה להשתמש במערכת עד הסדרת השימוש בחקיקה. המשטרה השיבה במאי 2022 כי "המערכת מונעת פשיעה ופעילות חבלנית עוינת"; עציון, לעיל ה"ש 142; מתן וסרמן "בית המשפט הורה למדינה להסדיר את מערכת המעקב עין הנץ בתוך 45 יום" **מעריב** (27.05.21) https://www.maariv.co.il/breaking-news/Article-843295.

״מערכות צילום מיוחדות״ נקבע כי תיתכן התקנת מצלמה מיוחדת שהיא חלק ממערכת צילום מיוחדת על גוף שנע במרחב.[148] ניתן להבין זאת כסעיף שמסמיך שימוש ברחפנים וגם שימוש במצלמות גוף ומצלמות על ניידות. אך אף בתיקון זה לחוק חסרה הסמכה להפעלת מיקרופונים במרחב הציבורי.

השימוש של שוטרים במצלמות גוף מוסדר בנוהל. נוהל זה קבע את מטרות השימוש במצלמות גוף, אופן השימוש בהן, לכמה זמן נשמר התיעוד, השימוש בחומרי התיעוד והגישה אליהם.[149] לעומת זאת, נוהל שימוש ברחפנים ונוהל השימוש במערכת ״עין הנץ״ אינם חשופים לציבור. לכן אי אפשר לדעת האם ההסדרה של הכלים הללו עומדת באותו סטנדרט של הקפדה על שמירת זכויות הפרט.[150] כבר נאמר בפסיקה כי השמירה על חסיון המערכת תמוהה,[151] שכן, החשש שפרסום הכלים עלול לפגוע ביכולת לתפוס עבריינים הוא חשש שקיים לגבי כל מערכות האכיפה. נאמר שם כי על משטרת ישראל חלה החובה להתמודד עם מקרים אלו.[152] הסדרת השימוש בכלים טכנולוגיים למעקב ושיטור מנבא בחוק ופרסומו יאפשרו שקיפות של פעולות השלטון ושמירה על ערכי הדמוקרטיה. כמו כן, תגבר המודעות הציבורית לסכנות הפשיעה ותתאפשר הרתעה מפני ביצוע עבירות. אם משטרת ישראל תפעל בשקיפות בנוגע לאיסוף, שמירה ועיבוד הנתונים, תגבר הלגיטימציה לשימוש בהם. נוהלי השימוש צריכים לכלול הגבלות ברורות וסנקציות במקרים של הפרה.[153]

מצלמות התחבורה של העיריות השונות הוסדרו בחקיקה ראשית.[154] אך המצלמות החכמות שמשמשות את העירייה לצורכי ניהול העיר ולמשטרת ישראל יש גישה אליהן אינן מוסדרות בחקיקה ראשית, אלא רק בנוהל.[155] גם יישום התוכנית ״עיר ללא אלימות״ נעשה ללא הסדרה משפטית הולמת.[156] נטען כי השימוש במצלמות נעשה בהתאם לנוהל הצבת מצלמות במרחב הציבורי.[157] האופן שבו משטרת ישראל יכולה לפנות לעיריות בבקשה למידע שונה מעירייה לעירייה. ישנן עיריות שמבקשות ממשטרת ישראל למלא טופס בקשה לגישה לחומרים אשר צולמו ברחבי העיר, בעוד עיריות אחרות דורשות צו שופט על מנת למסור את הנתונים. כמובן שהנושא אינו מוסדר בחקיקה ראשית. יש להסדיר את אופן קבלת התצלומים מהעיריות בבקשת צו משופט, ולא בטופס פנימי של העירייה.

אם כן, אנו עדים לשימוש בנהלים לשם הסדרת הסמכת משטרת ישראל לשימוש בכלים טכנולוגיים למעקב. אך נהלים אינם מחליפים חקיקה ראשית. כאשר מבקשים לבצע פעולה מנהלית אשר עלולה לפגוע בזכויות הפרט, נדרשת הסמכה ברורה ומפורשת בחקיקה ראשית.[158] מ״עקרון הפרדת הרשויות״ נובעת חובתה של הכנסת להכריע בנושאים חשובים ועקרוניים, כגון: שימוש משטרתי

---

[148] ס׳ 10א להצ״ח מערכות צילום מיוחדות, לעיל ה״ש 62.

[149] נוהל מצלמות גוף, לעיל ה״ש 57; נוהל מצלמות גוף נשען על פקודת המשטרה; חוק הגנת הפרטיות; ״מצלמות גוף לשוטרים: איך לעשות את זה נכון״ **האגודה לזכויות האזרח בישראל** (10.1.2019) https://www.acri.org.il/post/__161 (להלן: המלצות האגודה למצלמות גוף); סניור, לוקש וכהן, לעיל ה״ש 57.

[150] הנחיית הרשם למצלמות מעקב, לעיל ה״ש 91.

[151] פ״ל (תעבורה י-ם) 63/08/19 **מדינת ישראל נ׳ דענא** (נבו 23.6.2020) (להלן: עניין **דענא**); אוסלנדר, לעיל ה״ש 4.

[152] שם.

[153] המלצות האגודה למצלמות גוף, לעיל ה״ש 149.

[154] ס׳ 27א1 לפקודת התעבורה [נוסח חדש], התשכ״א–1961 (להלן: פקודת התעבורה).

[155] אוסלנדר, לעיל ה״ש 4. הרשות להגנת הפרטיות הסדירה את התקנתן והפעלתן באמצעות חוות דעת והנחיות ב־2010, 2012 ו־2016 .

[156] בר פלג ״דו״ח של הכנסת: אלפי מצלמות מוצבות ברחבי ישראל, ללא הסדרת פעילותן בחוק״ **הארץ** (17.12.2020) https://www.haaretz.co.il/news/law/2020-12-17/ty-article/0000017f-e6ac-dc7e-adff-f6ad64450000; אוסלנדר, לעיל ה״ש 4.

[157] שם.

[158] בג״ץ **האגודה לזכויות האזרח**, לעיל ה״ש 142, בעמ׳ 746, 762; בג״ץ **בן מאיר**, לעיל ה״ש 142; **עציון**, לעיל ה״ש 142.

בכלים טכנולוגיים למעקב, בחקיקה ראשית, שכן מדובר בהסדרים ראשוניים. הכנסת אינה יכולה להאציל את סמכויותיה לרשות המבצעת לקביעת מגבלות לשימוש בכלים טכנולוגיים אלו,[159] זאת מאחר שהדבר פוגע בעקרון חוקיות המנהל.[160]

__הסדרים המאפשרים עקיפת בקרה ודרישת צו שיפוטי__: על מנת לקבל מידע ממאגרי נתוני התקשורת של חברות הסלולר החוק קובע כי על המשטרה לקבל צו מבית המשפט.[161] החוק מסדיר מתן היתר מנהלי, בלא פנייה לבית המשפט, לקבלת נתוני תקשורת במקרים המפורטים בחוק.[162] הפריסה של מצלמות מערכת "עין הנץ" בכבישי הארץ מאפשרת מעקב אחר מיקום רכבים ברחבי הארץ. כך משטרת ישראל עוקפת את ההגבלות לקבלת נתוני מיקום שהוטלו על איכון טלפונים.[163] פעולת מעקב של המשטרה שהוגבלה והוסדרה באופן מפורט בחוק מתאפשרת ללא כל הגבלה חוקית באמצעים טכנולוגיים אחרים. אם יש הכרה בפגיעה בפרטיות ובצורך לבקש צו על מנת לפעול, מדוע הדבר שונה בין המנגנונים השונים?[164] בנוסף, מערכת "עין הנץ" פוגענית יותר מאיכון טלפונים, שכן, את הטלפון הנייד ניתן להשאיר בבית, בעוד על מנת להתחמק מ"עין הנץ" יש להימנע מהנסיעה.[165]

כלי נוסף שמאפשר את עקיפת הדרישה לצו שופט עבור איכון טלפונים והשגת נתוני מיקום, אשר נרכש על ידי המשטרה לאחרונה, נקרא "אקו". כלי זה יכול בפועל לספק למשטרה נתונים בדבר מיקומו של אדם. רכישת הכלי על ידי משטרת ישראל לא הובאה לבחינה ולאישור של היועץ המשפטי לממשלה.[166] השימוש בכלי זה אינו חוקי. על פי חוק נתוני תקשורת, קבלת נתוני תקשורת טעונה צו מאת בית המשפט. בבג"ץ נקבע כי משטרת ישראל אינה מוסמכת לקבלת צו איסוף גורף של כלל נתוני התקשורת, אלא לגילוי עבירות או עבריינים קונקרטיים, ואין ביכולתה להקים "כלי" משלה.[167]

__חוסר בהירות משפטי – איזה חוק חל?__ הסמכת משטרת ישראל להשתמש בתוכנות רוגלה מבוססת על מקטעים מחוקים שונים. חסרה התייחסות סדירה ושיטתית לכלל היכולות הטכנולוגיות החדשות ואף התייחסות להתפתחויות עתידיות. איזה חוק חל על השגת ראיות מטלפונים ניידים ומחשבים? האם חוק האזנת סתר?[168] האם חוק המחשבים?[169] האם פקודת סדר הדין הפלילי מעצר וחיפוש?[170] האם חוק נתוני תקשורת?[171]

---

159 טנא, לעיל ה"ש 22, בעמ' 444–443.

160 זמיר, לעיל ה"ש 142, בעמ' 73; עניין **בן חיים**, לעיל ה"ש 144, בפס' 22 לפסק הדין של השופטת ביניש.

161 בהתאם לחסד"פ נתוני תקשורת, לעיל ה"ש 11, שנכנס לתוקף ביום 27.06.08 מאפשר לרשויות החקירה בישראל לקבל לרשותן נתוני תקשורת של כלל מנויי בזק, בהתאם להגדרתם בחוק בזק, לעיל ה"ש 11. בהתאם להסדר הקיים בס' 13 לחוק השב"כ, לעיל ה"ש 11.

162 בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (נבו 28.05.12) (להלן: **בג"ץ האגודה נ' משטרת ישראל**).

163 בחסד"פ נתוני תקשורת, לעיל ה"ש 11.

164 אוסלנדר, לעיל ה"ש 4.

165 עתירת האגודה לזכויות האזרח, לעיל ה"ש 5.

166 גנון (30.5.23), לעיל ה"ש 68.

167 כהנא 2023, לעיל ה"ש 84; בג"ץ **האגודה נגד משטרת ישראל**, לעיל ה"ש 162; משרד המשפטים **דו"ח הסנגוריה הציבורית** (2021).

168 חוק האזנת סתר.

169 חוק המחשבים, התשנ"ה–1995 (להלן: חוק המחשבים).

170 פסד"פ מעצר וחיפוש.

171 חסד"פ נתוני תקשורת.

חוק הגנת הפרטיות מגדיר האזנת סתר כהתנהגות פלילית. על פי חוק האזנת סתר הוסדר השימוש בהאזנות סתר ככלי בידי רשויות האכיפה לשם מאבק בפשיעה.[172] משטרת ישראל נדרשת לפנות לבית משפט מחוזי בבקשה לצו לביצוע האזנות סתר.[173] האזנת סתר כוללת גם האזנה או העתקה של תקשורת המועברת בין מחשבים וגם בין טלפונים ניידים.[174] בירנהק מסביר, כי חוק האזנות סתר אינו מאפשר לשופט לאשר בצו שימוש משטרתי ברוגלות לטלפונים ניידים. חוק האזנת סתר עוסק בהאזנה ל"שיחה", שכוללת גם שיחה בקול, בכתב, בתמונה בטלפון, טלפון נייד ותקשורת בין מחשבים.[175] אבל תוכנת הרוגלה אוספת גם תכנים שאינם "שיחה", כמו פרופיל באתר היכרויות או קבצים מסוגים שונים ששמורים במכשיר. התוכנה יכולה לשלוט במצלמה ובמיקרופון של המכשיר, ועוד. כל עוד החוק מסמיך צווי האזנת סתר לשיחות בלבד, אין מקום לפרשנות מרחיבה.[176]

חדירה לחומר מחשב והפקת פלט המייצג את תוכנו נחשבים כ"חיפוש" המחייב צו של שופט. חוק המחשבים[177] מתייחס לפעילויות אסורות של חדירה לחומר מחשב שלא כדין ולזכות הגישה והאיסוף של מידע אגור במחשבים וטלפונים סלולריים (מידע במנוחה), לפיו ניתן לגשת בגישה חד־פעמית למידע שאגור במחשב בתאריך הצו בלבד, ולא בהתקשרות סמויה למכשיר.[178] רחום־טוויג התייחס לתוכן שאינו נופל תחת ההגדרה של האזנה לשיחה בחוק האזנות סתר והסביר כי שימוש בסעיף 23א לפקודת סדר הדין הפלילי לשם קבלת צו חיפוש בחומר מחשב אינו מסמיך את משטרת ישראל להשתמש בתוכנות רוגלה בנוגע לכל המידע המצוי במכשיר הנחקר לתקופת זמן ממושכת וללא מגבלות. גם מבחינה נורמטיבית לא ראוי לאפשר חיפוש רחב כל כך לצורכי חקירה.[179]

שימוש בצו שופט מסוג הזמנה להציג חפץ לשם הסדרת השימוש המשטרתי בתוכנות רוגלה הוא בעייתי.[180] זאת, מאחר שצו זה הוא כללי מדי, ואינו מתייחס ספציפית לנתוני תקשורת. הוא אינו מאפשר קבלה של קובצי מידע ממאגרי מידע ואינו מסדיר מצבי חירום שבהם נתוני תקשורת נדרשים בדחיפות, כגון: איתור נעדרים ומניעת מעשי רצח.[181] זאת, בעוד שחוק נתוני תקשורת מסדיר את הקבלה והשימוש בנתוני תקשורת לצרכים של אכיפת החוק. החוק מגדיר שלוש דרכים שבהן תוכל המשטרה לקבל את הנתונים: דרך צו שופט שלום, במקרים דחופים ישירות על ידי קצין בדרגת סגן ניצב, ודרך מאגר נתונים שיועבר לרשות המשטרה.[182]

מלבד ההבחנה בין תכנים של שיחה לתכנים אחרים, ישנה הבחנה בנוגע למסר שנמצא בדרכו לבין מסר שכבר הגיע למחשב. לא ברור איזה חוק חל על חדירה למחשב ויירוט מסר שכבר הגיע ליעדו

172 הרפז וגולן, לעיל ה"ש 73, בעמ' 329; ס' 2(2) לחוק הגנת הפרטיות.
173 במקרים חריגים מפכ"ל המשטרה מאשר האזנות סתר; הרפז וגולן, לעיל ה"ש 73, בעמ' 333.
174 ס' 6, 7 לחוק האזנת סתר; רע"פ 8873/07 **היינץ ישראל בע"מ נ' מדינת ישראל** (נבו 2.1.2011).
175 ס' 1 לחוק האזנת סתר.
176 בירנהק מאוריך לפגסוס, לעיל ה"ש 10.
177 ראו חוק המחשבים אשר נחקק בין היתר למטרת ההתאמה של דיני האזנת הסתר לתחום המחשבים.
178 מקור הסמכות הוא ס' 23א לפסד"פ מעצר וחיפוש.
179 רחום־טוויג, לעיל ה"ש 67.
180 ס' 43 לפסד"פ מעצר וחיפוש.
181 הצעת חוק סדר הדין הפלילי (סמכויות אכיפה - המצאה, חיפוש ותפיסה), התשע"ד—2014, ה"ח 574; הצעת החוק מסדירה בפירוט את הסמכויות, הכללים והעילות לחדירה (סמויה או גלויה) למחשב ולגישה לחומר האגור בו. יש לציין שהצעת החוק אינה מתייחסת להאזנות סתר ואינה מחליפה את הוראות חוק האזנת סתר.
182 כמו כן נוסחו תקנות סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת) (מאגר נתוני זיהוי תקשורת), התשס"ט—2008; ס' 3(א) לחסד"פ נתוני תקשורת; הכללים למתן צו לקבלת נתוני תקשורת ממאגר מידע של ספק תקשורת: את הבקשה יש להגיש לבית משפט השלום, ובית המשפט רשאי להתיר, בכפוף לעמידה בפסקת ההגבלה ואם המטרה היא הצלת חיים, גילוי עבירות, חקירתן או מניעתן, העמדת עבריינים לדין או חילוט רכוש.

ונמצא בו. בית המשפט העליון השאיר שאלה זו ב"צריך עיון" בפרשת בדיר.[183] אהרוני־גולדנברג הציעה כי: כאשר החדירה למחשב כוללת קריאת דואר אלקטרוני שכבר נתקבל ונשמר, אין מדובר בהאזנת סתר ל"שיחה", אלא בחדירה למידע האצור במחשב הממתין באופן פסיבי. לעומת זאת, אם מדובר בתקשורת דינמית כאשר אותו מסר בדיוק מיורט בדרך למחשב היעד, בעודו "נח" בשרת, כלומר כאשר הדבר נעשה בזמן אמת, אז יחול חוק האזנת סתר, שכן הדבר נחשב ל"שיחה".[184]

כדי ליירט תקשורת דינמית נדרש היתר של נשיא בית המשפט המחוזי.[185] לעומת זאת, חדירה לחומר מחשב והפקת פלט המייצג את תוכנו של חומר זה נחשבת "חיפוש" המחייב צו של שופט שלום.[186] הבדל נוסף בין החוקים נמצא באפשרות לבצע האזנות סתר במקרים דחופים ללא צו שופט על פי חוק האזנות סתר, בעוד פקודת סדר הדין הפלילי מעצר וחיפוש אינה מאפשרת זאת.[187] מוטלת בספק היכולת של שוטר להבחין ברגע האמת בין תוכן שנמצא בדרכו לבין תוכן שכבר הגיע ליעדו ולהספיק להגיש את הבקשה לצו לבית המשפט הרלוונטי, שכן מדובר בתהליך שאורך לעיתים כמה שניות.

על פי שוורץ, אלטשולר וכהנא לא די בחוק האזנות סתר, חוק המחשבים, פקודת סדר הדין הפלילי וחוק נתוני תקשורת להסדרת השימוש המשטרתי בתוכנות רוגלה. כל אחד מהם מתייחס לסוג אחר של מידע: שיחות טלפון, מטא־דאטה ונתוני מיקום, וחומר שנמצא בתוך מחשב וטלפון חכם. כביכול, על משטרת ישראל לבקש האזנות סתר משופט מחוזי, בנוסף לצו חיפוש בחומר מחשב משופט שלום. מצב זה, שבו נדרשת משטרת ישראל לפנות לכמה שופטים לבקשת צווים שונים על מנת לכסות את כל סוגי המידע שניתן להשיג באמצעות תוכנות רוגלה, פותח פתח להעלמת מידע משופטים בנוגע לבקשות שהוגשו או לא הוגשו לשופטים אחרים ולניסיונות המשטרה לשכנע שופט אחד בזמן שהאחר מסרב לבקשתם. מצב שבו השופטים החתומים על הצו בעלי מעמד שונה במערכת המשפט יוצר מדרג נורמטיבי לא ראוי בין כלים טכנולוגיים שונים באופן שאינו הולם את עוצמת הפגיעה בזכות לפרטיות. ריכוז כלל סמכויות המעקב המכוון תחת דבר חקיקה אחד יוביל לקוהרנטיות והרמוניה באופן השתת הביקורת השיפוטית על השימוש המשטרתי בתוכנות רוגלה.[188]

<u>ג.2. הסמכת משטרת ישראל בחקיקה ראשית לשמירת המידע:</u> בשלב שמירת המידע אתייחס לשני סוגים של כשלים. הראשון נוגע להיעדר הסמכה בחוק של משטרת ישראל לשמירת המידע שנאסף באמצעות כלי מעקב טכנולוגיים ואי־רישום מאגרי המידע. השני הוא היעדר הסדרת מאגרי מידע שמוחזקים בידי רשויות מנהליות אחרות והיעדר הסמכת משטרת ישראל להשתמש במאגר או לחלופין איסור מתן גישה למשטרת ישראל לסוגי המידע הנאספים במאגרים אלו.

---

[183] ת"פ (מחוזי ת"א) 40250/99 **מדינת ישראל נ' בן קסאם בדיר** (נבו 4.9.2001).
[184] לפי ס' 1 לחוק האזנות סתר.
[185] שם, בס' 6(א).
[186] לפי ס' 23(א) לפסד"פ מעצר וחיפוש, חדירה לחומר מחשב והפקת פלט יראו אותם כחיפוש; על פי סעיף 23א(ב) לא ייערך חיפוש, אלא על פי צו שופט המציין במפורש היתר לחדור לחומר מחשב, את מטרות החיפוש והתנאים שקובעים שלא יפגעו בפרטיותו של אדם מעבר לנדרש. על פי סעיף 23א(ג) קבלת מידע מתקשורת בין מחשבים תוך כדי חיפוש אינה האזנת סתר.
[187] חוק המחשבים; ס' 23(א) לפסד"פ מעצר וחיפוש; רחום־טוויג, לעיל ה"ש 67.
[188] "חוק מעקבים דיגיטליים: דרושים פיקוח פרלמנטרי והגברת שקיפות השימוש ברוגלות" (חוות דעת של תהילה שוורץ אלטשולר ועמיר כהנא 14.3.2023).

<u>מאגרי מידע משטרתיים שלא הוסדרו בחקיקה</u>: חוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר על בעל מאגר המידע, מנהל מאגר המידע והמחזיק בו.[189] אחת מהחובות של בעל מאגר מידע היא רישום מאגר המידע.[190] ידוע כי קיימים מאגרי מידע משטרתיים, כגון: מאגרי "טביעות אצבע", "מאגרי דנ"א" ומאגר "תצלומים" של חשודים. מאגרים אלה מוסדרים בחקיקה והם רשומים כמאגרי מידע.[191] אך ישנם מאגרי מידע משטרתיים שאינם רשומים. המידע שנאסף באמצעות מערכת "עין הנץ" נופל תחת ההגדרה "מאגר מידע" מאחר שמדובר בנתונים על אודות אדם, כאשר המידע על אודותיו מזוהה או ניתן לזיהוי.[192] הידיעה על הימצאותו של אדם במקום נתון ובזמן נתון או חזותו עשויים לכלול נתונים על צנעת אישיותו, כגון: עם מי הוא נמצא ובאילו נסיבות. לדוגמה: הימצאות במרפאה מלמדת על מצבו הבריאותי, הימצאות בבית תפילה של עדה מסוימת או לבוש מסוים מעידים על אמונה דתית. אלה הם נתונים העונים על הגדרת המונח "מידע" ואף "מידע רגיש" בסעיף 7 לחוק הגנת הפרטיות.[193]

כבר ב־2012 הוציא משרד המשפטים הנחיה שלפיה תיעוד ממצלמות שמזהות לוחיות רישוי ייחשב "מאגר מידע" לפי חוק הגנת הפרטיות, אשר מחייב את רישום המאגר במשרד המשפטים. משטרת ישראל לא רשמה את המאגר אצל רשם מאגרי המידע, בניגוד להנחיית משרד המשפטים, ואין גוף אשר מפקח על השימוש המשטרתי במאגר.[194]

<u>מאגרי מידע של קטגוריות מידע חדשות</u>: דוגמה למאגר מידע שבו נאסף מידע מסוג חדש אשר אינו מוסדר בחוק הוא מאגר קולות מוקלטים של אסירים המנוהל בשירות בתי הסוהר. מאגר זה משמש את המערכת לשם שליטה ובקרה על ניהול שימוש אסירים בטלפונים לשם מניעה וסיכול של פשיעה מתוך כותלי בית הסוהר.[195] ישנם מאגרים נוספים אשר מנוהלים על ידי רשויות אחרות שבהם נאספים סוגים חדשים של מידע, כגון: נתוני שימוש בחשמל, נתונים כלכליים ונתונים רפואיים. גם מאגרים אלו אינם מוסדרים בחוק. בנוסף, לא קיימים איסור או הסמכה בחוק למשטרת ישראל להשתמש במידע שבמאגרים אלו.

<u>ג.3. הסמכת משטרת ישראל בחקיקה ראשית לעיבוד המידע:</u> בשלב עיבוד המידע אתייחס לשני כשלים. האחד הוא שינוי בהבחנה בין מרחב פרטי למרחב ציבורי לאור ההתפתחויות הטכנולוגיות. השני הוא היעדר הסמכה של משטרת ישראל בחוק לשימוש בבינה מלאכותית וכלים סטטיסטיים לשם עיבוד מידע שנאסף בשימוש בטכנולוגיות מעקב.

<u>שינויים במשמעות מרחב ציבורי ומרחב פרטי לאור ההתפתחות הטכנולוגית</u>: תחום הכיסוי של מצלמה המוצבת ברשות הרבים עלול להיכנס לגדר "צילום אדם כשהוא ברשות היחיד" לפי חוק

---

189 פרק ב' לחוק הגנת הפרטיות; ס' 3 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו–1986; Jason Tooley, *The future of biometrics in policing worldwide*, 2020 BIOMETRIC TECH. TODAY 5 (2020).

190 אוסלנדר, לעיל ה"ש 4.

191 כגון תקנות סדר הדין הפלילי (סמכויות אכיפה – חיפוש בגוף ונטילת אמצעי זיהוי) (המאגר ואבטחתו, עיון בו, מחיקה, ביעור והפקה חוזרת), התשס"ז–2007.

192 ס' 7 לחוק הגנת הפרטיות; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 5. הנחיית הרשם למצלמות מעקב, לעיל ה"ש 125 .

193 הנחיית הרשם למצלמות מעקב, לעיל ה"ש 125; עניין **דענא**, לעיל ה"ש 151.

194 עניין **דענא**, לעיל ה"ש 151; ס' 19 לחוק הגנת הפרטיות, מעניק פטור למשטרה מאחריות על פגיעה שנעשתה באופן סביר במסגרת מילוי תפקידה, אולם פטור מאחריות אין משמעו פטור מחובת הסדרת מאגר המידע ורישומו. החוק לא החריג את משטרת ישראל מחובתה לרישום מאגרי המידע. על משטרת ישראל לרשום את כל מאגרי המידע שברשותה ברשם מאגרי המידע.

195 **דוח שנתי 70ב**, לעיל ה"ש 87, בעמ' 282.

הגנת הפרטיות.[196] זאת, מאחר שלפי חוק הגנת הפרטיות אסור השימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה שלשמה נמסרה,[197] ובנסיבות מסוימות אף כדי פרסומו של עניין הנוגע לצנעת חייו האישיים של אדם או למצבו הבריאותי.[198] חל שינוי בהגדרת הזכות לפרטיות בכל הנוגע להבחנה בין מעקב ברשות היחיד למעקב ברשות הרבים.[199] כיום, עם התפתחות הטכנולוגיה, ניתן לאסוף מידע אישי על אודות אדם בעת שהוא נמצא במרחב הציבורי, באופן שלא היה קיים בעבר. למידת נתונים על מצב בריאותי, רגשות, הרגלים ונטיות של אדם פוגעת במרחב האישי של האדם גם בזמן שהוא נמצא במרחב הציבורי. בשל ההתפתחויות הטכנולוגיות נדרש עדכון של הגדרת האיזונים הנוגעים ביחס לזכות לפרטיות.[200] בשל היכולת להסיק מהנתונים המצטברים מידע בנוגע להיבטים הפרטיים ביותר בחיי האדם, מתעורר צורך להגן על הזכות לפרטיות ולהגביל את איסוף המידע על אודות האזרחים.[201]

<u>היעדר הסמכה בחוק</u>: חסרה הסמכה בחוק של משטרת ישראל לעבד מידע ממערכות שבשליטתה וממערכות שלא בשליטתה במרחב הציבורי והפרטי באמצעים טכנולוגיים מתקדמים, כגון בינה מלאכותית. משטרת ישראל אינה מוסמכת בחוק להשתמש בכלים לניבוי עבריינות כגון תוכנות לניבוי עבריינות מתווי פנים.[202]

לא מתקיים דיון ציבורי מספק בהטיות של מערכות המסתמכות על הכרעות בינה מלאכותית בדבר ניבוי פשיעה. לחברי הכנסת חסר ידע מקצועי שיאפשר להם לפקח על תהליכים אלו. לאור כשלים אלו בולט היעדר גוף שיבקר את החלטות הבינה המלאכותית.[203]

כאשר יקבע המחוקק הישראלי חוק בדבר השימוש המשטרתי במערכות בינה מלאכותית, מן הראוי שיתייחס להצעת החוק לאימוץ מדיניות רגולציה בתחום הבינה המלאכותית של האיחוד האירופי, שבה נמנים כמה סוגים של מערכות בינה מלאכותית מזיקות במיוחד, אשר מאיימות על זכויות הפרט ולכן מוגדרות כבעלות סיכון בלתי מתקבל על הדעת. בין יתר מערכות אלה נמנות: מערכות סיווג ביומטריות המסווגות אנשים לפי מאפיינים מסוימים; מערכות בינה מלאכותית שמשמשות לצורך דירוג חברתי והערכה אישיותית או התנהגותית של פרטים; מערכות בינה מלאכותית המשמשות לצורך הערכה לביצוע עבירות פליליות על ידי אנשים, אשר מבוססות על פרופיילינג והמעריכות תכונות ומאפייני אופי, לרבות מיקומו של אדם וכן עבר פלילי; מערכות בינה מלאכותית המייצרות מאגר נתונים של זיהוי פנים באמצעות צילומי פנים שנאספו מהאינטרנט או באמצעות מצלמות אבטחה; מערכות בינה מלאכותיות אשר מטרת פעולתן היא להסיק מסקנות בנוגע לרגשות של אנשים לצורך אכיפת חוק; מערכות בינה מלאכותית המשמשות לניתוח צילומים מוקלטים ממרחבים ציבוריים באמצעות מערכות זיהוי ביומטריות, כאשר מותר השימוש בהן על פי חוק בנוגע

---

[196] ס׳ 2(3) לחוק הגנת הפרטיות.
[197] ס׳ 2(4), 2(9) לחוק הגנת הפרטיות.
[198] ס׳ 2(11) לחוק הגנת הפרטיות.
[199] הרפז וגולן, לעיל ה״ש 73, בעמ׳ 206, 327.
[200] שוורץ אלטשולר וכהנא, לעיל ה״ש 6, בעמ׳ 6.
[201] שם.
[202] הבר וקדוש נוסבאום, לעיל ה״ש 44, בעמ׳ 27–28.
[203] שוורץ אלטשולר וכהנא, לעיל ה״ש 6, בעמ׳ 5; הבר וקדוש נוסבאום, לעיל ה״ש 44, בעמ׳ 44; תהילה שוורץ אלטשולר ״תזכיר חוק לתיקון פקודת המשטרה [נוסח חדש] (מערכות צילום מיוחדות), התשפ״ג–2023״ **המכון הישראלי לדמוקרטיה** (19.2.2023) https://did.li/k0UlC (להלן: מכתב שוורץ אלטשולר). שוורץ אלטשולר טענה כי הסעיף המאפשר שימוש במידע שנאגר לצורך חקירת דפוסים של ביצוע עבירות ומחקר הוא בעייתי. לגישתה יש לאסור את השימוש במידע ביומטרי אישי לצורכי מחקר ויש להשתמש במידע מותמם. תמונות פנים ביומטריות אי אפשר להתמים.

לעבירות פליליות מסוימות.[204] לאור הגדרת מסוכנותן כבלתי מתקבלת על הדעת, ראוי לבחון איסור שימוש משטרתי במערכות כגון אלו.

שר החדשנות, המדע והטכנולוגיה הישראלי התייחס לרשימת העקרונות האתיים לשימוש בבינה מלאכותית לפי חוק הבינה המלאכותית של האיחוד האירופי: שימוש בבינה מלאכותית ייעשה תוך כיבוד זכויות יסוד ובפרט תוך שמירה על הזכות לפרטיות. העיקרון השלישי לחוק בינה מלאכותית האירופי קובע כי אי־שוויון והטיות במערכת הבינה המלאכותית והפליה פסולה יעמדו לנגד עיניהם של המפתחים והמשתמשים בבינה המלאכותית.[205] ראוי כי המחוקק הישראלי יתייחס לעקרונות אלו ויאמץ אותם כאשר יחוקק חוק בדבר השימוש המשטרתי במערכות בינה מלאכותית.

מהאמור בפרק זה ניכר כי המחוקק הישראלי אינו עומד בקצב ההתפתחות הטכנולוגית. הוא נשען על חוקים מיושנים אשר חלוקת העבודה ביניהם בעייתית, לא ברורה ולא הגיונית. השימוש בטכנולוגיה מתרחש כבר היום, אך הליכי החקיקה טרם הסתיימו והדיונים בהצעות החוק נמשכים לאורך שנים. הפעלת כלים טכנולוגיים למעקב משטרתי אחר האוכלוסייה לפני הסמכתה בחוק מפורש אינו חוקי ואינו ראוי. כאשר המערכת כבר נמצאת בשימוש, המחוקק נאלץ להתאים את פרטי החוק לאופן השימוש הקיים בשטח, במקום לקבוע מהם הכללים הראויים. בדרך זו עוקפת הרשות המבצעת את הכנסת, מונעת דיון ציבורי וקובעת עובדות בשטח.[206]

<u>ד. הסיבות להרחבת השימוש בטכנולוגיה לשם מעקב</u>

כפי שציינתי בפרק א', המעקב המשטרתי אחר הציבור הורחב ממעקב למטרת מציאת ראיות לביצוע פשע למעקב למטרת מניעת פשיעה מראש.[207] ניתן להבחין במגמת עלייה בהיקף השימוש המשטרתי בטכנולוגיות מעקב, מעיון בנתונים סטטיסטיים הנוגעים להאזנות סתר ונתוני תקשורת בישראל. בתחום האזנות הסתר הוגשו בשנת 2004 רק 962 בקשות להאזנת סתר, בעוד בשנת 2016 מספר הבקשות שהוגשו מזנק ל־3,309 בקשות. נתון נוסף המדגים את מגמת העלייה הוא מספר הפרשיות שטופלו בהאזנות סתר. בשנת 2007 דובר ב־346 פרשיות, אך בשנת 2012 המספר עלה ל־816 פרשיות. נתונים נוספים שבהם נצפית מגמת עלייה הם מספר הבקשות להיתרים מכוח חוק נתוני תקשורת. בשנים 2008–2009 הוגשו רק 9,603 בקשות, בעוד שבשנת 2016 המספר מטפס ל־24,801 בקשות.[208] השימוש בטכנולוגיה לשם מעקב התרחב בשל כמה סיבות: עיתות משבר, עלייה ביכולת הטכנולוגית, ירידה בעלות הפעלת הטכנולוגיה, זמינותה הגוברת, קלות השימוש בטכנולוגיה וייעול עבודת המשטרה. כעת אפרט בנוגע לכל אחת מהסיבות.

---

[204] הסוג השלישי עד השמיני של מערכות בינה מלאכותית מסוכנות שנכלל במאמרם של טל מימרן וגל דהן "הצעת הרגולציה של האיחוד האירופאי בתחום הבינה המלאכותית Artificial Intelligence Act" **תכלית – המכון למדיניות ישראלית** (2023) (להלן: "רגולציה לבינה מלאכותית של האיחוד האירופי"). ב־14 ביוני 23 פרסם הפרלמנט האירופי גרסה מעודכנת של הצעת הרגולציה.

[205] משרד החדשנות, המדע והטכנולוגיה ומשרד המשפטים ייעוץ וחקיקה **עקרונות מדיניות, רגולציה ואתיקה בתחום הבינה המלאכותית** 35–37 (2023). (להלן: מסמך **מדיניות בינה מלאכותית ישראלי**).

[206] הרשות למשפט, טכנולוגיה ומידע **דו"ח לשנת 2011** 33 (2012). ראו שם את הערות המועצה להגנת הפרטיות; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 23.

[207] וינרב, לעיל ה"ש 7.

[208] עמיר כהנא ויובל שני "כיסוי חלקי: ביקורת שיפוטית על מעקב מדינה מקוון בישראל" **פרלמנט** 83 (2019). כהנא ושני, לעיל ה"ש 69, בעמ' 72; מגמת עלייה זו ניכרת גם בנתונים סטטיסטיים הנוגעים לבקשות והיתרים להאזנות סתר בארצות הברית למטרות אכיפת חוק ומניעת פשיעה. בשנת 2006 אושרו בארצות הברית 1,839 בקשות להאזנות סתר, ובשנת 2015 אנו רואים גידול במספר הבקשות שאושרו אשר מגיע ל־4,148 בקשות.

ד.1. עיתות משבר: ניכר כי מצבי משבר מעודדים את הגברת מאמצי המעקב המשטרתי והרחבת השימוש בטכנולוגיה לשם כך. לדוגמה, לפני אסון התאומים התמודדות עם פשע וטרור נעשתה באמצעות גישות משפטיות ומבצעיות אשר הגיבו לאירועים לאחר התרחשותם. בהתאם לגישה זו, עיקר הפעילות המשטרתית היא בביצוע חקירה והעמדה לדין של עבריינים לאחר ביצוע הפשע. המצב השתנה לאחר התקפות הטרור במגדלי התאומים. הצורך במעקב ואיסוף מודיעין התגבר כחלק מן המאמץ לצמצם איומים ולשמור על ביטחון הציבור, בעידן של פיגועי טרור בין־לאומיים ופשיעה מתוחכמת טכנולוגית. יכולות המעקב של המדינה הורחבו על ידי הפעלת גורמים מסחריים פרטיים לשם השגת נתונים אישיים וציתות לציבור. לאחר 11 בספטמבר, המערכת המשפטית והמבצעת בארצות הברית עברה שינוי מהותי. סמכויות המעקב והחיפוש של המשטרה הורחבו תחת הגדרת תפקיד חדשה בשם "אכיפת חוק מניעתית". המחוקקים ובתי המשפט הגיבו לאיומים הטרוריסטיים והפשע הבין־לאומי על ידי הפחתת ההגנות על פרטיות האזרחים, דבר אשר הקנה לרשויות סמכויות נרחבות יותר לצורך מעקב אחר פעילויות האזרחים. זאת, תוך שינוי ניכר באיזון בין ההגנה על הפרטיות לבין אינטרס הציבור לשמירה על הביטחון.[209]

דוגמה נוספת היא הרחבת סמכויות משטרת ישראל והשב"כ בתקופת התפרצות מגפת הקורונה למעקב אחר האוכלוסייה באמצעות איכון טלפונים. זאת, במטרה לבלום את התפשטות הנגיף. לפני התפרצות מגפת הקורונה, המעקב אחר אזרחים על ידי רשויות האכיפה בישראל הוגבל לצרכים פליליים וביטחוניים המוגדרים במסגרת החוק. על מנת לבצע פעולות מעקב טכנולוגיות נדרשה משטרת ישראל לקבל אישור מבית המשפט. הליך זה יושם לשם שמירה על זכויות האדם ופרטיותו. עם התפרצות נגיף הקורונה והצורך למנוע את התפשטותו, ממשלת ישראל החליטה להרחיב את סמכויות המעקב של המשטרה והשב"כ. השינוי שחל היה מהותי, בהחלטת ממשלה אושר השימוש בטכנולוגיית איכון טלפונים למעקב אחר מיקומם של אנשים שאובחנו כחולים או נחשדו ככאלה וכן אנשים שנמצאו בקרבתם. כלי המעקב הזה, שהיה שמור בעיקר למטרות ביטחוניות ולמלחמה בטרור, הפך לכלי מרכזי במאבק במגפה. המטרה העיקרית הייתה לאתר מהר יותר אנשים שעלולים להדביק אחרים ולבודדם, בכדי למנוע התפשטות נוספת של הווירוס. אך בשל השימוש הנרחב בטכנולוגיה זו, התעורר חשש בנוגע לפגיעה בפרטיות והשפעותיו ארוכות הטווח של ניטור ופיקוח ממשלתי על האזרחים במדינת ישראל.[210]

דוגמה נוספת לגורם המשפיע על העלייה בשימוש בכלים טכנולוגיים למעקב בעיתות משבר הוא אירועי הטרור המתרחשים בישראל. את התפקידים שהוטלו על משטרת ישראל בקום המדינה ניתן לתאר כתפקידי שיטור קלסיים, כגון: התמודדות עם פשיעה, מניעת עבריינות, תפיסת עבריינים והבאתם לדין. אך בשנת 1974 התווספה לתפקידי המשטרה גם האחריות לביטחון הפנים. שינוי זה השפיע באופן מהותי על אופייה של המשטרה.[211] העובדה כי משטרת ישראל מבצעת תפקידים של שיטור טרור ("שיטור גבוה"), בנוסף לתפקידי השיטור הקלסיים שלה, משפיע על השימוש הגובר בטכנולוגיות מעקב. זאת, מאחר שעיסוק המשטרה בשיטור טרור מחזק את "המגמה הצבאית" המאפשרת פגיעה מוגברת בזכויות אדם ומנגד פוגע ב"מגמת מתן שירות משטרתי לקהילה". זמינות

---

[209] William Bloss, *Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects*, 4 SURVEILLANCE & SOC'Y 208 (2022).

[210] ס' 7(ב)(6) לחוק שירות הביטחון הכללי, התשס"ב–2002; אשר נדון בבג"ץ **בן מאיר**, לעיל ה"ש 142.

[211] באדי חסייסי ויעל ליטמנוביץ "משילות ויעילות בשיטור מיעוטים בחברות שסועות: נקודת המבט של מפקדי תחנות משטרה על החברה הערבית בישראל" **משפט ומשטרה** 265, 271 (2021) (להלן: חסייסי וליטמנוביץ).

הכלים המבצעיים בידי משטרת ישראל מובילה לשימוש בהם גם לצורך מילוי תפקידים קלסיים של אכיפת חוק וסדר ציבורי מול אזרחי המדינה.[212]

ד.2. שיפור ביכולות הטכנולוגיות: שינויים בטכנולוגיה תרמו ליכולת של המשטרה לעסוק במעקב אלקטרוני אחר אזרחים. אחת מפריצות הדרך הטכנולוגיות בשנים האחרונות הייתה השיפור המשמעותי ביכולות של זיהוי תמונה ועיבוד תמונה.[213] במקביל, השתכללו גם יכולות ה״ביג דאטה״ והבינה המלאכותית, המאפשרות למחשבים לנתח את התמונות הללו.[214] בעבר היה צורך בצופה אנושי שיסרוק כמויות תוכן גדולות כדי לזהות פריטי מידע רלוונטיים. טכנולוגיות עיבוד וניתוח תמונה חדשות מאפשרות כיום לתמצת סרטים ארוכים לדקות ספורות, כך שכל פריים יכלול מידע שנאסף מקטעי וידאו רבים. בנוסף, ניתן להגדיר פרמטרים לחיפוש, כגון: רוכב אופניים, הולך רגל, גבר, לובש בגד בצבע.[215] כמו כן, היכולת ליירט תקשורת אלקטרונית אישית, כגון: אינטרנט, טלפון סלולרי ושידור אלחוטי, הפכה לקלה יותר ומצריכה חדירה פיזית פחותה מבעבר.[216]

ד.3. הטכנולוגיה זולה, קלה לשימוש וזמינה: כיום, במקום לשלוח אלפי בלשים לאסוף מידע, ניתן לכרות מידע רב מרשתות חברתיות וממערכת המצלמות הפרוסה ברחבי הארץ באמצעות בינה מלאכותית. מדובר בדרך מעקב זולה מאוד, יעילה וקלה לשימוש.[217] הפעלת רחפנים, לדוגמה, זולה יותר מהפעלת מסוק, והשימוש בתוכנות רוגלה במחשבים וטלפונים ניידים מאפשר האזנות סתר בדרך שאינה מחייבת הצבת מכשיר ציתוט פיזי, כפי שנעשה בעבר, ובעלויות פחותות.[218] דוגמה נוספת לזמינות הגוברת של כלים טכנולוגיים אלו היא קיום מאגרים ביומטריים רבים, אשר מאפשר בקלות ובעלויות נמוכות לאמת את זהותו של אדם.[219]

ד.4. השימוש בטכנולוגיה יעיל: סיבה נוספת לעלייה בשימוש בכלים טכנולוגיים למעקב היא ההנחה כי אלה יסייעו למשטרת ישראל לבצע את תפקידיה ביעילות מוגברת.[220] יעילות איסוף המידע מרשתות חברתיות מתבטאת ביכולת לתפוס טרוריסטים ומבצעי תקיפות אלימות כאשר הם מפרסמים את כוונותיהם לפני שביצעו את המעשה.[221] יתרון נוסף לאיסוף המידע באמצעות כלים טכנולוגיים למעקב הוא השימוש במערכת ״עין הנץ״ ובטכנולוגיות זיהוי פנים, אשר מאפשר איתור אירועים חריגים ואיתור מחבלים ועבריינים באמצעות הרבה מצלמות ומעט כוח אדם. בכך המערכת מייעלת את עבודת המשטרה בהתמודדות עם פשיעה ופעולות טרור, פיענוח עבירות, סיכול פיגועים והצלת חיים.[222] טכנולוגיה זו עשויה לסייע למשטרה באימות זהותו של אדם, בזיהוי חשוד שזהותו אינה ידועה ואף באיתור מיקומו של אדם החשוד בעבירה.[223]

---

212 גדעון פישמן **איזון בפעולות המשטרה: טרור וסדר ציבורי** 36–37, 41 (2004).
213 וינרב, לעיל ה״ש 7.
214 וינרב, לעיל ה״ש 7.
215 גולדשמידט, לעיל ה״ש 5, בעמ׳ 8.
216 Bloss, לעיל ה״ש 209, בעמ׳ 211.
217 .Mateescu et al, לעיל ה״ש 9, בעמ׳ 7.
218 בן צור, לעיל ה״ש 55; חכמון (11.7.2018), לעיל ה״ש 55.
219 גולדשמידט, לעיל ה״ש 5, בעמ׳ 4.
220 Bloss, לעיל ה״ש 209, בעמ׳ 211; עתירת האגודה לזכויות האזרח, לעיל ה״ש 5.
221 .Mateescu et al, לעיל ה״ש 9, בעמ׳ 1, 7.

222 שוורץ אלטשולר וכהנא, לעיל ה״ש 6, בעמ׳ 4; גולדשמידט, לעיל ה״ש 5, בעמ׳ 16; חכמון (2.6.2022), לעיל ה״ש 6.
223 בהקשר זה, אימות זהות מתבצע בהשוואת תמונת פנים לתווי פנים; זיהוי חשוד מתייחס להשוואת תמונה למאגר תמונות; וחיפושו של אדם באמצעות מערכת לשימוש בתמונה כנגד מאגרי תמונות או וידאו אשר חושפים את מיקומו; Clare Garvie et al., *The Perpetual Line–Up: Unregulated Police Face Recognition in America*, GEORGETOWN L. CENTER ON PRIV. & TECH. (Oct. 8, 2016), https://www.perpetuallineup.org;

השופט אלרון עמד על יעילות השימוש בחיפוש במכשירים ניידים בפסק הדין בעניין אולריך: *"ומכאן גם היעילות המשמעותית שעשויה להיות לביצוע חיפוש במכשירים אלו במסגרת חקירה משטרתית. גישה למכשיר הטלפון הנייד של נחקר עשויה להוביל לפריצת דרך משמעותית בחקירה ולקיצור ניכר של הליכיה. לעיתים ניתן לאתר במכשיר הטלפון הנייד של חשוד עקבות למעשיו, הקושרות אותו למעשה עבירה – או לחלופין, מידע המלמד על חפותו. הערך הרב שניתן להפיק מן המידע המצוי במכשיר הטלפון הנייד של הנחקר מציב פיתוי של ממש בפני חוקרי המשטרה בחדר החקירות ובזירת אירוע, "להושיט יד" אל עבר המכשיר ולעיין בכלול בו, מאחר שתשאול הנחקר על בסיס תכתובות מחשידות עשוי להביא לבירור החשדות באופן מהיר ויעיל."*[224]

בכמה מחקרים נמצא כי מצלמות גוף של שוטרים מייעלות את מאמצי השיטור. שכן, שימוש במצלמות גוף הביא לירידה בפשיעה ועלייה בכמות כתבי האישום שהוגשו, בוצעו יותר מעצרים, חלה ירידה בהפעלת כוח על ידי השוטרים והצטמצם מספר התלונות שהוגשו כנגד שוטרים.[225] בנוגע לרחפנים נטען כי הם מייעלים את עבודת המשטרה בכך שהם מאפשרים לראות את השטח ממבט עילי מבלי שמבחינים בהם. הם מהירים, ראשונים בזירה, ניידים ולא מאוישים, כך שניתן לשגר אותם לאזור מסוכן.[226] בנוגע להאזנות סתר נטען כי הן מייעלות את עבודת המשטרה מאחר שהן מאפשרות לאסוף ראיות שאי אפשר היה להגיע אליהן בדרכים הרגילות.[227] לבסוף נטען כי הפשיעה משתכללת כל הזמן וכי ללא אמצעים טכנולוגיים, מערכת אכיפת החוק לא תעמוד בקצב ההתקדמות הטכנולוגית ולא יתאפשר מאבק אפקטיבי בפשיעה.[228]

על אף היתרונות שהוצגו לשימוש באמצעים טכנולוגיים לשם שיטור יזום, הרחבת השימוש ואופן השימוש באמצעים אלו משפיעים באופן ישיר על הפרת זכויות אדם ובפרט הזכות לפרטיות. ההסדרה המוצעת בחוק אינה מספקת כדי להגן מפני הפגיעה האמורה. בשל כך, אבקש לבחון בעייתיות זו ואציע פתרון בדמות הסדרה חקיקתית, אשר מתמקד בסוג המידע שנאסף על ידי משטרת ישראל, ולא באמצעי הטכנולוגי שבאמצעותו הושג המידע.

ה. הפגיעה בזכות לפרטיות בעקבות השימוש המשטרתי באמצעים טכנולוגיים למעקב ושיטור מנבא

בפרק הקודם תיארתי את הסיבות השונות להתרחבות השימוש בטכנולוגיה לשם ביצוע מעקב ושיטור מנבא. אך במקביל ליתרונות השימוש בכלים הטכנולוגיים, נגרמת פגיעה חמורה בזכויות אדם.[229] בחיבור זה אבקש להתמקד בפגיעה בזכות לפרטיות. ההתייחסות לזכויות האחרות שהוזכרו לעיל היא משנית, כזכויות שנגזרות מהזכות לפרטיות או מתקיימות בשל הזכות לפרטיות.

Eldar Haber, *Racial Recognition*, 43 CARDOZO L. REV. 71, 84–5 (2021).

224 עניין **אוריך**, לעיל ה"ש 94, בפס' 4 לפסק הדין של השופט אלרון.

225 John Oritz Smykla et al., *Police Body-worn cameras: Perceptions of Law Enforcement Leadership*, 41 AM. J. CRIM. JUST. 424 (2016); לוי, לעיל ה"ש 57.

226 בן צור, לעיל ה"ש 55; חכמון (11.7.2018), לעיל ה"ש 55; וינרב, לעיל ה"ש 7.

227 הרפז וגולן, לעיל ה"ש 73, בעמ' 333.

228 שם, בעמ' 330.

229 גולדשמידט, לעיל ה"ש 5, בעמ' 4. עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 2. הזכויות אשר נפגעות הן הזכות לפרטיות, עקרונות החופש והחירות הנובעים מכבוד האדם ומהווים בסיס לחברה דמוקרטית, פגיעה בהליך הוגן ותקין, פגיעה בזכות הקניין (בפריצה לטלפונים ניידים ומחשבים), פגיעה בקניין רוחני (בהעתקת תמונות, קובצי אודיו ועוד), פגיעה בחופש התנועה, חופש ההפגנה, השם הטוב, חופש העיסוק, בזכות לשוויון ועוד.

ה.1. הזכות לפרטיות – מהי? זכות זו משתייכת לקבוצת זכויות האדם הבסיסיות בישראל.[230] בחוק־יסוד: כבוד האדם וחירותו נקבע כי כל אדם זכאי לפרטיות ולצנעת חייו.[231] בפסיקה נקבע כי הזכות לפרטיות כזכות חוקתית גוברת אף על חופש הביטוי.[232] הזכות לפרטיות שבסעיף 7 אינה בלתי מוגבלת. בכפוף לתנאי פסקת ההגבלה שבסעיף 8 לחוק היסוד, ניתן לפגוע בה *"בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה, ובמידה שלא עולה על הנדרש, או לפי חוק כאמור מכוח הסמכה מפורשת בו."*[233]

הזכות לפרטיות מוסדרת בחקיקה על ידי החוק להגנת הפרטיות, כאשר הסעיף הראשון בו קובע עיקרון בסיסי מנחה, האוסר על פגיעה בפרטיותו של אדם ללא הסכמתו.[234] בסעיף השני לחוק מוגדרים מקרים המהווים פגיעה בזכות לפרטיות. כלומר, כל אחד מהמקרים המנויים בסעיף שתיים אשר נעשה ללא הסכמת הפרט, מייצר פגיעה בזכות לפרטיות. המקרים המנויים בחוק אשר אליהם התייחס המאמר הם: בילוש, התחקות או מעקב וצילום אדם ברשות היחיד. סעיף שתיים הוא סעיף רחב היקף האוסר את מרבית הדרכים לאיסוף המידע כפי שנעשה כיום על ידי משטרת ישראל. סעיף 6 הוא החריג לחוק אשר מתיר פגיעה בזכות לפרטיות במקרים שבהם הפגיעה היא בשולי הזכות.

בשנים האחרונות התעוררו שאלות רבות בנוגע לטיבה והיקפה של הזכות לפרטיות, לאור פיתוחים טכנולוגיים עכשוויים.[235] גופים מסחריים אוספים מידע רב על הרגלי הצריכה של האזרחים ופוגעים בזכות לפרטיות.[236] נטען כי לאור זאת, משמעות המונח "פרטיות" השתנתה, ולכן לא ניתן לצפות כי משטרת ישראל תשמור על הפרטיות של האזרח.[237] אך לגישתי, המשמעות של הזכות לפרטיות אינה משתנה בשל העובדה שישנם גופים מסחריים או מנהליים שרומסים אותה. בנוסף, דין גופים פרטיים אינו כדין גופים מנהליים, בעיקר כאשר מדובר בגוף בעל סמכות מנהלית, שלה פוטנציאל לפגיעה עמוקה בזכויות האדם הבסיסיות.[238]

הזכות לפרטיות היא חלק מעקרונות היסוד של השיטה המשפטית בחברה דמוקרטית המונהגת בישראל. במציאות החיים המודרנית מתרחשת פגיעה תמידית בזכותו של האדם לפרטיות, זאת בשל שימוש באמצעי ציתות, מעקב, תיעוד ועיבוד מידע, כמו למשל, צילום הרכב באמצעות מערכת משטרתית ואיכון הטלפון הנייד. ההנחה כי ההמון מגן על הפרט כאשר בוחנים את המידע על אודותיו כחלק מנתונים סטטיסטיים מטעה ומשלה. ההתפתחויות הטכנולוגיות המהירות מאפשרות פגיעה בפרטיות ומגבירות את אשליית הפרטיות.[239] הפגיעה בפרטיות מתבטאת הן בפן החברתי והן בפן האישי של האזרחים. פגיעה זו מלווה בתחושה קשה של פגיעה באוטונומיה

---

230 טנא, לעיל ה"ש 22, בעמ' 429.

231 ס' 7(א) לחוק־יסוד: כבוד האדם וחירותו.

232 הרפז וגולן, לעיל ה"ש 73, בעמ' 325; בג"ץ 2481/93 **דיין נ' מפקד מחוז ירושלים**, פ"ד מח(2) 456 (1994).
233 חוק־יסוד: כבוד האדם וחירותו.
234 חוק הגנת הפרטיות.
235 טנא, לעיל ה"ש 22, בעמ' 430–431.
236 הרפז וגולן, לעיל ה"ש 73, בעמ' 327.
237 טנא, לעיל ה"ש 22, בעמ' 430.

238 שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 2.
239 מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 72 (2007) (להלן: בירנהק "שליטה והסכמה").

ובבחירות האישיות שאדם מבצע במרחב הפרטי שבו הוא רוצה לפעול בחופשיות, ללא חשש מביקורת.[240]

אבקש להציג את הפגיעה בזכות לפרטיות בהתאם לחלוקה של בירנהק למעגל הפרט, מעגל היחסים הבין־אישיים והמעגל הדמוקרטי. בבחינת הפגיעה הנגרמת במעגל הפרט אתייחס לכבוד האדם, הזכות להיעזב במנוחה, פרטיות כגישה ופרטיות כשליטה. לאחר מכן אציג את הצרכים הפסיכולוגיים של האדם.

בירנהק מסביר כי פגיעה בפרטיות תפגע ביכולת של האדם להגן על המרחב האוטונומי שלו ועל היכולת שלו לשלוט בחייו. שכן, התערבות חיצונית בחיי האדם פוגעת בכבודו, מצמצמת את השליטה העצמית שלו ומכפיפה אותו לאחרים.[241] על פי גישה אחת, הזכות לפרטיות נובעת מהזכות להיעזב במנוחה, בשל צורך פסיכולוגי בשלווה, כדי להתנתק מהחברה באופן שיאפשר לאדם לבנות אישיות שאינה מופרעת על ידי אחרים.[242] על פי עמדה אחרת, הזכות לפרטיות מובנת במונחים של גישה. בהתאם לעמדה זו, כל אדם הוא אטום נפרד ולו הצורך בסודיות, באנונימיות וביחידות. לפרט קיים צורך במרחב אישי, שבו הוא יכול להיות עצמו ללא התערבות חיצונית. בידולו של האדם מהחברה הוא הבסיס לקיומו, ופגיעה בזכות לפרטיות לא תאפשר זאת.[243] בהמשך לכך, פגיעה בזכות לפרטיות תפגע ביכולת של האדם לשמור את זהותו האנושית ולא להפוך לעוד נתון במסד הנתונים.[244]

לגישתו של בירנהק, הפגיעה בזכות לפרטיות תפגע ביכולת של השליטה של האדם בעצמו ובמידע על אודותיו. הפגיעה בשליטת האדם על המידע שלו מעמיקה כיוון שכיום המידע נשמר לנצח. איננו יכולים עוד לסמוך על שכחה ומגבלות הזיכרון האנושי. המידע שנאגר על אודותינו רודף אחרינו לכל מקום בכל זמן. השליטה של המדינה והמשטרה במידע על אודות אדם שקולה לשליטה שלהם באדם עצמו. לפעמים מי שאוסף מידע על האדם מכיר אותו יותר מכפי שהוא מכיר את עצמו. האוטונומיה של האדם נפגעת כאשר המידע משמש לסיווג הפרטים לקבוצות. זאת מאחר שאין לאדם השפעה על הסיווג ואין לו יכולת לערער על כך.[245] האדם הוא שמייצר את המידע, והמידע משקף אותו, לכן ראוי שהוא ישלוט במידע.[246]

כחלק מהפגיעה במעגל הפרט אציג את הניתוח של בירנהק בנוגע לפגיעה הנגרמת לצרכים הפסיכולוגיים של האדם כאשר נפגעת הזכות לפרטיות. אתייחס לצורך במרחב אישי, לצורך במגן מפני מבט זר שיש לו כוח ממשמע וממשטר ולצורך לשמור על אינדיווידואליות, כאשר מוציאים את האדם מההקשר העצמי שלו. צרכים אלה חשובים לרווחה של בני האדם ולאפשרותם לממש את עצמם באופן המיטבי.[247] ראשית, הפגיעה בזכות לפרטיות פוגעת בצורך במרחב אישי. ללא מרחב אישי וניתוק מהסביבה לא יוכל האדם להתנסות, לטעות, לחפש ולחרוג מעבר לנורמות המקובלות

---

[240] שם.
[241]בירנהק "שליטה והסכמה", לעיל ה"ש 239, בעמ' 58.
[242] Samuel Warren & Louis Brandeis*, The Right to Privacy*, 4 HARV. L. REV. 193 (1980); בירנהק "שליטה והסכמה", לעיל ה"ש 239, בעמ' 39.
[243] רות גביזון "הזכות לפרטיות ולכבוד" **זכויות אדם בישראל: קובץ מאמרים לזכרו של ד"ר חמן שלח** 61 (1989); בירנהק "שליטה והסכמה", לעיל ה"ש 239, בעמ' 40.
[244] שם, בעמ' 59.
[245] שם, בעמ' 41.
[246] שם, בעמ' 44.
[247] שם, בעמ' 60.

בחברה שבה האדם נמצא, ללא פיקוח ובאנונימיות. הדבר עלול לפגוע בהתפתחות הפסיכולוגית התקינה של האדם.[248]

שנית, פגיעה בזכות לפרטיות פוגעת בצורך של האדם באינדיווידואליות. היא פוגעת בשסתום שדרכו בני אדם בוחרים להציג את עצמם בפני אחרים. ללא הזכות לפרטיות, אחרים יכולים לערוך רדוקציה של האדם לפרט אחד ויחיד ולהתעלם מהמכלול שהופך את האדם למי שהוא. כך נפגעת השליטה של האדם בהצגתו לעולם בצורה שהוא מעוניין בה.[249]

שלישית, הפגיעה בזכות לפרטיות פוגעת בצורך במגן מפני מבט זר ובהגנה מפני כוחו הממשמע והממשטר של המבט.[250] עצם הצילום, בהינתן היכולות הטכנולוגיות הקיימות, מהווה פגיעה בפרטיות.[251] הנוכחות של המצלמות במרחב הציבורי מייצרת מצב חדש אשר ממשטר וממשמע את האזרחים. בני אדם מודעים לכך שעוקבים אחריהם ומקבלים מצב זה כנורמה.[252] לא נדרש מעקב בפועל, אלא די בכך שהאדם יודע שהמדינה שולטת במידע האישי שלו ויכולה לעקוב אחריו.[253] לאור זאת, תיתכן צנזורה עצמית של דיבור, מעשים ומחשבות על מנת להתאימם לתפיסה של הממשל אשר צופה באזרחים.[254] בכך נפגעת הזכות של האדם לחירות וחופש פעולה.[255]

לבסוף, הפגיעה בזכות לפרטיות לא פוגעת רק במעגל הפרט, אלא גם במעגל הקשרים הבין־אישיים. מערכות יחסים מסוימות זקוקות לתנאי רקע של פרטיות שיאפשרו את מימושן המיטבי. קשרים משפחתיים, זוגיים, רפואיים, כלכליים ויחסי אמון.[256]

המעגל השלישי אליו אתייחס בהקשר של פגיעה בזכות לפרטיות הוא המעגל הדמוקרטי.[257] חשיבותה הרבה של הזכות לפרטיות היא בהשפעתה על כינון יחסי הכוחות בין האזרח לשלטון.[258] הזכות לפרטיות אינה זכות מודרנית פריווילגית, שכן, היא הכרחית לשם הגבלת הפיקוח החברתי המוגזם שמושת על האזרחים.[259] חשיבותה הרבה של הזכות לפרטיות נעוצה בכך שהיא מהווה תנאי מקדמי להתפתחותה של חברה חופשית ודמוקרטית. ללא פרטיות אין חופש ביטוי, חופש דת או חירות תנועה.[260] פוקו טען כי אזרחים שחשים שהם נמצאים תחת מעקב והאזנות חוששים לנקוט עמדות מעוררות מחלוקות ונוטים לקונפורמיזם ולפסיביות פוליטית.[261] מערכות איסוף מידע כלליות מאפשרות למשטרת ישראל גישה למידע לא קונקרטי, בדומה לצבא,[262] ומשנות את מערך

---

[248] שם, בעמ׳ 60.

[249] שם, בעמ׳ 62.

[250] שם, בעמ׳ 61.

[251] שוורץ אלטשולר וכהנא, לעיל ה״ש 6, בעמ׳ 6.

[252] פלג, לעיל ה״ש 156.

[253] הנחיית הרשם למצלמות מעקב, לעיל ה״ש 125; מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 182, 429 (2010); פלג, לעיל ה״ש 156; טנא, לעיל ה״ש 22, בעמ׳ 440; עתירת האגודה לזכויות האזרח, לעיל ה״ש 5, בעמ׳ 14.

[254] טנא, לעיל ה״ש 22, בעמ׳ 440.

[255] אילון אורון ״מצלמות משטרה שמצלמות לתוך המכוניות – פגיעה בפרטיות״ **גלובס** (4.9.2018) https://www.globes.co.il/news/article.aspx?did=1001252390.

[256] בירנהק ״שליטה והסכמה״, לעיל ה״ש 239, בעמ׳ 63.

[257] שם, בעמ׳ 67.

[258] טנא, לעיל ה״ש 22, בעמ׳ 429.

[259] אורון, לעיל ה״ש 255.

[260] שם.

[261] טנא, לעיל ה״ש 22, בעמ׳ 430–433; פוקו, לעיל ה״ש 13.

[262] מכתב שוורץ אלטשולר, לעיל ה״ש 203. במכתבה לוועדת השרים לחקיקה שוורץ אלטשולר ביקרה את הצעת החוק.

הכוחות בין המשטרה לאזרחים ובין המשטרה לדרג הפוליטי.[263] היעדר הסימטרייה במצב זה בא לידי ביטוי בכך שהצופה הוא בעל כוח רב, ולנצפה אין שליטה על המידע האישי שלו: מי צופה בו? מה היקף המידע שנאסף על אודותיו? הנצפה אינו יכול להפעיל את אותו הכוח על הצופה.[264]

חלק ניכר מהפעילויות הנתפסות בכלים הטכנולוגיים למעקב הוא פעילויות שגרתיות, שאינן מהסוג שהחברה מבקשת למנוע.[265] אנשים שומרי חוק אינם צריכים לחשוש כל הזמן שמסתכלים עליהם.[266] הזמינות והאוטומציה של מערכות אלו עלולות להוביל לאכיפת יתר בעבירות דוגמת השלכת פסולת, עבירות חנייה ועבירות תנועה זניחות.[267]

המעקב אחר האזרחים פוגע גם בחזקת החפות ובזכות להליך הוגן. גופי אכיפת החוק אינם רשאים לעקוב אחר אזרחים ולאסוף לגביהם מידע ולפגוע בפרטיותם, אלא במקרים שקיים לגביהם חשד לביצוע עבירה.[268] לכן, כאשר משטרת ישראל מפעילה סמכויות שלטוניות כלפי בני אדם בשל דברים שהם עלולים לעשות בעתיד, היא פוגעת ב"עקרון חזקת החפות". לא חוקי ולא ראוי לאסוף נתונים אחר מיליוני בני אדם שאינם חשודים בביצוע עבירה, שלא נשקף מהם סיכון לחברה, והסיכוי שיהיו מעורבים במעשים פליליים הוא אפסי.[269]

מעבר לפגיעה המיידית בזכות לפרטיות, השימוש בטכנולוגיות מעקב ושיטור מנבא עלול להוביל להחרפת החשדות ולהתעצמות הפערים הקיימים בין קבוצות המיעוט לגופי השלטון, ובפרט למשטרה. כאשר טכנולוגיות שיטור מתקדמות מיושמות באופן לא מאוזן ומתמקדות בקבוצות מסוימות, הדבר עלול להקנות תחושה של מעקב אובססיבי ופגיעה בפרטיות של אותן קבוצות, מה שמוביל לדעיכה של אמון הציבור במוסדות המשטרה והשלטון. כמו כן, השימוש בטכנולוגיות אלו עלול להגביר את התפיסה של אוכלוסיות מסוימות בחברה כ"אחרים" או כאיום. תפיסות אלו בתורן מייצרות קרקע פורייה לסטיגמות ולדיכוי חברתי. בחברה הישראלית, שבה השסעים הפוליטיים והתרבותיים עמוקים, ההשלכות הסוציולוגיות של פרקטיקות אלו עשויות להיות משמעותיות במיוחד, שכן, הן מסיטות את מוקד השיח מגיבוש מדיניות שיטור הוגנת ומאוזנת לכיוון של פילוג וסכסוך חברתי מתמשכים.[270] לאחר הצגת חשיבותה של הזכות לפרטיות, אבקש להתייחס לפגיעה בזכות לפרטיות בהתאם לחלוקה לפי שלבי הליך המעקב: איסוף, שמירה וניתוח המידע.

ה.2. פגיעה בזכות לפרטיות בשלב איסוף המידע: על פי חוק הגנת הפרטיות, אין פוגעים בפרטיות של אדם ללא הסכמתו, וצילום האדם כשהוא ברשות היחיד פוגע בפרטיותו.[271] ייתכן מצב שבו מצלמה שהוצבה ברחוב עלולה לצלם מרחבים פרטיים בבית של אדם מבעד לחלון או בחצרו. בנוסף,

---

263 לפי ס' 10כד, 10יד להצ"ח מערכות צילום מיוחדות, לעיל ה"ש 62, שימוש בנתוני זיהוי ביומטרי שזוהו בזמן אמת מותר בהתאם למטרות: (2) לצורך פלילי מכל סוג שהוא. כלומר, עצם הצבת המצלמות מותר רק כדי למנוע פשע חמור, אבל משנאגר המידע אפשר להשתמש בו כדי לאכוף עבירות במדרג נורמטיבי נמוך יותר.

264 DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY, 178–179 (Yale Un. Press 2011); כפי שצוטט בעתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 14.

265 הנחיית הרשם למצלמות מעקב, לעיל ה"ש 105; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 14.

266 פלג, לעיל ה"ש 156.

267 שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 9.

268 עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 2.

269 בג"ץ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים** (נבו 10.5.2002) (להלן: בג"ץ **האגודה נ' משרד הפנים**); עתירת האגודה לזכויות האזרח לעיל ה"ש 5, בעמ' 2, 14 וה"ש 68 שם.

270 חסייסי וליטמנוביץ, לעיל ה"ש 211, בעמ' 265–266, 268.

271 ס' 1 לחוק הגנת הפרטיות.

מערכת מצלמות "עין הנץ" מצלמת את הרכב על מנת לזהות את לוחית הרישוי ומבצעת גם תמונות תקריב שבהן נראים בבירור פניהם של הנוסעים ברכב.[272] נטען כי פנים הרכב הוא שטח פרטי, ולכן מדובר בפגיעה אסורה בפרטיות.[273] אך טיעון זה לא התקבל בסופו של דבר בבית המשפט.[274] מצלמות גוף של שוטרים מצלמות את המתרחש גם בבתים פרטיים של אזרחים לאחר יידוע האזרח על הפעלת המצלמה.[275] לעיתים הן מקליטות את האירועים ללא יידוע המצולם.[276]

על פי חוק הגנת הפרטיות, גם צילום אדם במצלמה ברשות הרבים יכול לפגוע בפרטיות, שכן הוא עשוי להגיע כדי "בילוש או התחקות אחרי אדם העלולים להטרידו" והוא לכל הפחות יוצר סיכון לפגיעה בפרטיות שעניינה "פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול להשפילו".[277] אך בשורה של פסקי דין קבע בית המשפט העליון כי השימוש במצלמות רחוב לשם תיעוד עבירות תנועה וחנייה מותר, זאת, נוכח הפגיעה המועטה בפרטיות העוברים והשבים.[278]

בניגוד לכך אני סבורה כי מצלמות מעקב הפרוסות במרחב הציבורי מאפשרות איסוף נתונים בנוגע למעשים, מייצרות פנאופטיקון מודרני אשר מגביל את חירות האדם ופוגע בזכויות אדם ומצמצמות את המרחב האישי במרחב הציבורי.[279] אזרחים רבים עלולים להיפגע מפריסת המצלמות ומהחומר שייאסף בהן, לדוגמה, במקרה שבו המצלמות יקלטו אדם שנסע לבלות בקניון במקום ללכת לעבודה. בנוסף, ישנם צילומים שעלולים לבזות או להשפיל אזרחים במקרים ומצבים אישיים, שפרסומם עלול להוביל לפגיעה בפרטיות.[280] בשימוש בטכנולוגיה לזיהוי פנים נפגעת זכותם של כל האנשים שנקלטים בעין המצלמה, ולא רק של החשוד שאותו מבקשת המשטרה לזהות.[281]

אחד המאפיינים של הכלא הפנאופטי של בנת'ם היה היכולת לעקוב אחר סוהרים, ולא רק אחר אסירים. בהתאם לכך, מצלמות המעקב הרבות מאפשרות מעקב גם אחר שוטרים, ולא רק אחר אזרחים.[282] מצלמות אלו משפיעות על עבודת המשטרה. במחקר נמצא כי שוטרים נמנעו בכמה מקרים מלהתערב בקטטות שזוהו על ידי המצלמות. לעיתים נוכחות המצלמות הובילה את

---

[272] בפרוטוקול דיון בת"פ 69298-11-18 **מדינת ישראל נ' אלקיעאן** (נבו 16.6.2019).
[273] אורון, לעיל ה"ש 255.
[274] תת"ע (תעבורה אשד') 8342-05-22 **מדינת ישראל נ' חזיזה**, פס' 63 לפסק הדין (נבו 11.12.2022).
[275] ס' 6ג, 9(א) לנוהל מצלמות גוף, לעיל ה"ש 57.
[276] Tooley, לעיל ה"ש 189, בעמ' 5; ס' 6.ג.9(ב) לנוהל מצלמות גוף, לעיל ה"ש 57; ס' 10ג להצ"ח מערכות צילום מיוחדות, לעיל ה"ש 62; נכתב כי לא תופעל מצלמה במערכת צילום מיוחדת באופן המאפשר צילום אדם כשהוא ברשות היחיד, ואולם, לגבי מצלמה ניידת תחול הוראה זו ככל הניתן. בסעיף 10ט. (ג). נאמר כי לא מחויבים ליידע את הציבור על קיום המצלמה.
[277] ס' 2(1) לחוק הגנת הפרטיות.
[278] עפמ"ק (מחוזי ת"א) 50075-11-18 **מדינת ישראל נ' מזרחי** (נבו 21.1.2019), נדונה הסוגיה של אי־הגנה על פרטיות בצילום במצלמה נייחת תוך שהדו"ח נרשם על ידי פקח בחדר הבקרה. בית המשפט המחוזי התיר את ביצוע תיעוד עבירות באמצעות מצלמה נייחת נוכח הפגיעה המועטה בפרטיות העוברים והשבים. ערעור שהוגש לבית המשפט העליון, ברע"פ 1492/19 **מזרחי נ' מדינת ישראל** (נבו 6.4.2020) (להלן: עניין **מזרחי**), נדחה. בג"ץ 867/15 **אור-הכהן נ' שר הפנים** (נבו 16.5.2018) במסגרתו גובש נוהל על ידי משרד הפנים לגבי אכיפת עבירות באמצעות מצלמות. בית המשפט העליון קבע כי ישנה הסדרה לגבי הצבת מצלמות ניידות ונייחות, וככל שקיימת השגה בדבר הפעלתן אזי יש לפנות להליך מתאים אחר. ח"נ (מחוזי י–ם) 16303-04-19 **מדינת ישראל נ' שרביט** (נבו 27.3.2020) במסגרתו נקבע כי תיעוד עבירת חניה באמצעות מצלמה נייחת הוא חוקי. ח"נ (ת"א) 66470-10-18 **מדינת ישראל נ' ויזנברג** (נבו), שם נדונה הצעת החוק של פקודת התעבורה עליה התבסס סעיף 27א (1)לפקודת התעבורה ולפיה סעיף זה לא נועד לפגוע בסמכויות הנתונות לעירייה לפעול לאכיפת עבירות חנייה בתחומה בהתאם לחוק העזר העירוני, אלא להרחיבן.
[279] טנא, לעיל ה"ש 22, בעמ' 429, 440.

[280] לעתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בס' 31; ס' 10ג להצ"ח מערכות צילום מיוחדות, לעיל ה"ש 62. נכתב כי לא תופעל מצלמה במערכת צילום מיוחדת באופן המאפשר צילום אדם כשהוא ברשות היחיד, ואולם, לגבי מצלמה ניידת תחול הוראה זו ככל הניתן; דן חי "עיר ללא אלימות, אזרחים ללא פרטיות" **וואלה כסף** (15.8.2016) https://finance.walla.co.il/item/2988417.
[281] שוורץ אלטשולר וכהנא, לעיל ה"ש 7.
[282] Benjamin J. Goold, *Public Area Surveillance and Police Work: The Impact of CCTV on Police Behavior and Autonomy,* 1 J. SURVEILLANCE & SOC'Y 191 (2003).

השוטרים להישאר מחוץ לטווח הצילום. בנוסף, נמצאו ראיות לכך שקלטות נמחקו מחשש שיכילו צילומים של התנהגות בלתי הולמת של שוטרים.[283] בכך נפגעת זכותם של השוטרים לפרטיות וזכותם של האזרחים להליך הוגן.

דוגמה לפגיעה בזכות לפרטיות לשם דיכוי הדמוקרטיה היא השימוש של מדינות שונות בתוכנת פגסוס, לשם מעקב אחרי עיתונאים, מנהיגי מדינות, פעילים למען זכויות אדם ומתנגדי משטר.[284] השימוש במערכת "עין הנץ" ובטכנולוגיות לזיהוי פנים מאיים גם הוא על חופש המחאה ועלול לשמש את השלטון לשם דיכוי הפגנות ופעילות פוליטית.[285] צילום המכוניות שנכנסות לעיר במועד ההפגנה מאפשר איסוף נתונים בנוגע למספר הפעמים שביקרו בה, כמה זמן ארך הביקור, מהיכן הגיעו והצלבה עם נתונים מהפגנות אחרות. באופן זה ניתן להכין מאגר של מפגינים "חוזרים" ואף לאפיין דפוסי התנהגות של כל מפגין ומפגינה. ידיעתו של אדם כי הגעתו להפגנה מתועדת מייצרת אפקט מצנן על מימוש הזכות להפגין.[286] דוגמה נוספת למעקב משטרתי טכנולוגי שפוגע בחופש הביטוי ובזכות להשתתפות פוליטית היא איסוף מידע מרשתות חברתיות על אודות אנשים שהביעו כוונה לתכנן או להשתתף בהפגנות ונקיטת פעולות מקדימות כנגדם.[287]

פגיעה נוספת המתרחשת בשל זיהוי האדם היא הפגיעה בזכות של היחיד לאנונימיות ולביטוי אנונימי, שחשיבותה הוכרה בפסיקת בית המשפט העליון.[288] מצלמות מעקב במרחב הציבורי וטכנולוגיות זיהוי תווי פנים פוגעות באנונימיות במרחב הציבורי. הנצחת מעשים לא תאפשר לנו להיפרד מעברנו ומטעויות שלא מסכנות את הציבור.[289]

נגזרת נוספת של הפגיעה בזכות לפרטיות היא הפגיעה בזכות לאוטונומיה אישית וזכות האדם על גופו.[290] תהליך הדגימה הביומטרי כולל איסוף מידע מגופו של אדם, לכן הוא עלול להיחוות כחודרני ומשפיל.[291] צמצום האדם לאוסף נתונים ביומטריים תורם להחפצה של גוף האדם.[292] הפיכתו לפרופיל שזמין לכל פקיד פוגעת בכבוד, בשליטה של אדם בגורלו ובאוטונומיה שלו.[293]

מתרחשת פגיעה בזכות נוספת בשימוש בכלים טכנולוגיים למעקב, והיא הפגיעה בחופש התנועה.[294] לדוגמה, השימוש במערכת "עין הנץ" מוביל לעיכובם של אנשים הנוסעים בכביש. זאת כאשר המערכת מוצאת התאמה ומתריעה על כלי רכב או נהגים שנמצאים ברשימת מבוקשים.[295] העובדה שפעולות הפיענוח וההשוואה לרשימות מבוקשים מבוצעות באופן אוטומטי ומבלי לעכב את הנהג אינה מבטלת את הפגיעה בפרטיות, שכן הפגיעה נגרמת מעצם הבדיקה והחיפוש שמבצעת המשטרה

---

283 שם.

284 עומר כביר "דו"ח מררי מראה על פגיעה קשה בפרטיות ובזכויות חשודים" **כלכליסט** (2.8.2022) https://www.calcalist.co.il/local_news/article/hj2eihlt9.

285 שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 2.

286 שם. עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 14. הצעת חוק "עין הנץ" הציעה להסמיך את המשטרה לאכוף הוראות המגבילות את חופש התנועה במרחב הציבורי, כגון איסורי כניסה וצווי הרחקה ממקומות ציבוריים. ליכולת אכיפה זו יש אפקט מצנן על מימוש זכויות יסוד נוספות, כגון חופש הביטוי וחופש האספה.

287 אוסלנדר, לעיל ה"ש 4.

288 רע"א 4447/07 **מור נ' ברק אי.טי.סי החברה לשירותי בזק בינלאומיים בע"מ**, פ"ד סג(3) 664, פס' 11–16 לפסק הדין של השופט ריבלין (2010).

289 טנא, לעיל ה"ש 22, בעמ' 433; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 2.

290 שם, בעמ' 429.

291 שכן לקיחת טביעות אצבע מאדם נתפסת כאקט שמבוצע על עבריינים. שם, בעמ' 433.

292 שם, בעמ' 433–434; Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421, 428 (1980).

293 טנא, לעיל ה"ש 22, בעמ' 434.

294 עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 2.

295 שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 7; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 15–18.

באופן קבוע אחרי כל הנהגים שעוברים בכביש, אשר פוגעים בשליטה של האדם במידע האישי שלו.[296]

נתוני מיקום הם פרטי מידע בעלי רגישות גבוהה ביותר. שכן, ממעקב אחר מיקום האדם ניתן להסיק נתונים בנוגע לפרטים אישיים ורגישים.[297] הפגיעה בפרטיות היא מעצם הידיעה של נתונים אלו, ולא רק מהשימוש בהם לצורכי חקירה משטרתית.[298] כאשר משטרת ישראל משתמשת ב"איכון הפוך" היא פוגעת בזכות לפרטיותו של כל מי שנמצא באותו אזור שהיא בוחנת, מאחר שבביצוע "איכון הפוך" ניתן לדעת מיהם כלל האנשים שהטלפון שלהם אוכן באזור מסוים, גם אם הם אינם חשודים בביצוע עבירה.[299]

כאשר המשתמשים ברשת מעלים מידע אישי על אודותיהם, הם יוצרים מערכת וולונטרית של מעקב שזכתה לכינוי "פנאופטיקון דיגיטלי".[300] לעיתים ילדים ונוער מפרסמים ברשת מידע שעלול לפגוע בזכותם לפרטיות. העובדה שהם נידבו את המידע אין משמעה ויתור על זכותם לפרטיות, אלא חוסר הבנה של השלכות מעשיהם. פגיעה נוספת ברחבי האינטרנט מתרחשת כאשר נאספות ראיות כנגד אנשים חפים מפשע, תחת הנחה מוטעית כי הם ביצעו פשע.[301] לדוגמה, לעיתים בני נוער מתבטאים באופן מסוים על מנת להשתייך לקבוצות חברתיות מבלי להתכוון לדבריהם. בשל כך מתעורר חשש לניטור מוגזם של בני נוער השייכים לאוכלוסיות מוחלשות.[302] לאורך הזמן התגבשה ההבנה כי שיתוף ללא גבולות יכול להזיק, והחלה צנזורה עצמית אשר פוגעת בחופש הביטוי. כתוצאה מכך נפגעת גם הדמוקרטיה.[303] על מנת להשיג מידע מפרופילים פרטיים אשר חסומים לגישה ציבורית, תיתכן התחזות שוטרים לאדם אחר. מצב זה עלול לפגוע בזכות האדם לפרטיות, שכן המידע הושג מהספרה הפרטית הווירטואלית.[304]

בחוק הגנת הפרטיות נאסר בין היתר על האזנת סתר ועל העתקת מכתב או כתב, כולל מסר אלקטרוני.[305] לכן, כאשר משטרת ישראל אוספת נתונים בנוגע לשיחות ודיבור נפגעת הזכות לפרטיות. בפסק הדין זאבי התייחסה השופטת פרוקצ'יה לפגיעה בזכות לפרטיות בהאזנות סתר: *"הפער האמור בין ההגדרה הדווקנית של היקף צו ההאזנה לבין היכולת הטכנית להגשימו טומן בחובו סיכון רב לפגיעה קשה בפרטיותם של בני אדם – בין של הנחקר עצמו, ובין של צדדים אחרים שאינם קשורים כלל לפרשה הנחקרת. מערכות אכיפת החוק מצוות להקטין את הסיכון שבפגיעה האמורה, ככל הניתן, תוך הגנה על תכליות החקירה ועל המטרות שלהשגתן ניתן צו ההאזנה."*[306]

בחיפוש במחשב ובטלפונים ניידים נגרמת פגיעה בזכות לפרטיות, שכן נחשפים עולמו האישי, העסקי והמשפחתי והמידע האינטימי ביותר על אודות האדם. בנוסף, המכשירים כוללים מידע

---

[296] בג"ץ **בן מאיר**, לעיל ה"ש 142, בפס' 37, 58 לפסק הדין של השופטת חיות.

[297] מיכאל בירנהק "פרטיות במשבר: הנדסה חוקתית והנדסת פרטיות" **משפט וממשל** כד 149 (2022) (להלן: בירנהק "פרטיות במשבר"); בירנהק מאוריך לפגסוס, לעיל ה"ש 10.

[298] בג"ץ **האגודה נ' משטרת ישראל**, לעיל ה"ש 162; חסד"פ נתוני תקשורת.

[299] כהנא 2023, לעיל ה"ש 84.

[300] מיכל **לביא אחריות מתווכי תוכן לעוולות ביטוי: הקשר חברתי** 26–29 (2018). שם דובר על תרומתן של טכנולוגיות חדשות לשיתוף המידע באינטרנט וכיצד הובילו בסופו של דבר למעקב אחר אזרחים ואיסוף מידע על אודותיהם; *Communications in Contemporary China: Orchestrating Thinking* 4 (Nicole Talmacs & Altman Yuzhu Peng eds., 2024).

[301] Mateescu et al., לעיל ה"ש 9, בעמ' 1.

[302] שם, בעמ' 7.

[303] שם, בעמ' 3.

[304] Egawhary, לעיל ה"ש 128, בעמ' 94; Mateescu et al., לעיל ה"ש 9, בעמ' 4.

[305] ס' 2(2), 2(5) לחוק הגנת הפרטיות.

[306] עניין **זאבי**, לעיל ה"ש 72, בפס' 18 לפסק הדין של השופטת פרוקצ'יה.

פרטי בנוגע לצדדים שלישיים. מתרחשת גם פגיעה בקניין, כאשר נעשה שינוי במכשירים שהם קניינו של אחר. פגיעה נוספת היא הפגיעה בקניין הרוחני של האדם, שכן המכשיר הנייד מכיל יצירות כגון תמונות, קובצי קול ועוד.[307] בפסק דין אוריך התייחסה השופטת חיות לפגיעה המיוחדת בזכות לפרטיות בהקשר של חדירה לטלפון הנייד: [308]*"חדירה למחשב או לטלפון החכם יכולה לחשוף נפח עצום של פרטים מתוך סיפור חייו של אדם; עובדה זו, בצירוף היכולות הטכנולוגיות שבאמצעותן ניתן להרכיב פרופיל שלם לגבי אדם תוך שימוש במידע המצוי במכשירים אלה, מוליכות אל המסקנה שפוטנציאל הפגיעה בפרטיות עקב חיפוש במחשב הוא, במקרים רבים, גבוה לאין שיעור בהשוואה לחיפוש "המסורתי" בחצרו או בכליו של אדם, והוא נוגע גם לצדדים שלישיים רבים שחייהם נקשרו בצורה כזו או אחרת – ולו לרגע – עם המחזיק במחשב או בטלפון החכם."*

השופט אלרון ציין ממדים נוספים לפגיעה בזכות לפרטיות בחדירה לטלפון הנייד: *"דפדוף ברשימת התכתובות שבמכשיר הטלפון הנייד חושף בפני החוקר מידע החורג באופן ניכר מהמידע הנחוץ לחקירה – כגון פרטי מכריו, טיב הקשר עימם ותמונותיהם. מלבד הפגיעה העצמאית בפרטיות הנחקר ומכריו, הנחקר אף עלול לחשוש כי יעשה שימוש במידע רגיש המתגלה בהודעותיו בכדי לגרום לו לשתף פעולה בחקירה – באופן שיש בו כדי לפגום בטוהר ההליך הפלילי. הפגיעה בפרטיות הנחקר עלולה אף להחריף אם המידע ייאגר על גבי שרתי המשטרה שלא לצורך, במיוחד כאשר מדובר במידע אשר מלכתחילה לא נדרש לצורך החקירה. זאת ועוד, הנחקר אינו מודע תמיד להיקף החומר השמור במחשבו ובמכשיר הטלפון הנייד החכם שברשותו, ויכולתו להסכים לחיפוש מתוחם בלבד, שימנע פגיעה בפרטיותו שלא לצורך, מוגבלת – אם בכלל קיימת. על כן, דומה שהפגיעה בפרטיותו של הנחקר כתוצאה מביצוע חיפוש ראשוני במכשירו במהלך החקירה, אינה מקבלת מענה מְסַפק בהסכמתו לאפשר לחוקרים לעיין בתכתובות המצויות במכשירו; וממילא, ספק בעיני אם ניתן לראות בהסכמתו לביצוע חיפוש במכשירו ללא צו משום "הסכמה מדעת" אשר עשויה להכשיר חיפוש שנעשה ללא צו ובהיעדר מקור סמכות אחר בדין."* [309]

ה.3. <u>פגיעה בזכות לפרטיות בשלב שמירת המידע</u>: מאגר מרכזי של נתונים ביומטריים מכיל בחובו סכנות רבות ופגיעה בזכות לפרטיות, כגון: סכנות אבטחה, פריצה על ידי האקרים, הדלפה על ידי עובדים רשלנים או מושחתים, שינוי המידע או אובדנו עקב תקלות מערכת או אסון טבע, "זחילת פונקציות" ושימוש שניוני שלא למטרה המוצהרת שלשמה הוקם המאגר.[310]

סכנות אבטחה ופריצה: ארגוני טרור ופשיעה ורשויות ביטחון של מדינות זרות עשויים לבצע מתקפת סייבר. כך עלול המידע המצוי במאגרים השונים לשמש גורמים אלו לשם פגיעה באזרחים

---

[307] אחד מהליקויים שנחשפו בדוח מבקר המדינה לשנת 2001 הנוגעים להאזנת סתר נוגע לקיומם של תמלילים הכוללים מידע אישי שיש בו פגיעה בפרטיות במידה העולה על הנדרש. הליקוי השני הוא מיעוט החומר הרלוונטי שהופק מהאזנות סתר המבוצעות ביחידות משטרה מחוזיות. נטען שלאור העלייה בכמות האזנות הסתר המאושרות, מנגנון הפיקוח בדמות צו שיפוטי הפך לחותמת גומי. מאחר שמעקב אחר אזרחים הפך להיות זול, ההיקף שלו עולה. העלות הכספית הגבוהה של ביצוע מעקב לפני ההתפתחויות הטכנולוגיות, שהוזילו והקלו על השימוש בהאזנות סתר, שימשה כמחסום אשר אילץ את משטרת ישראל להפעיל שיקול דעת ולהשתמש בהאזנות סתר במקרים חמורים ביותר המצדיקים פגיעה בפרטיות. היום, כאשר המעקב זול ונערך בהיקפים יוצאי דופן, נעדרת הבחינה של פגיעה בפרטיות באופן מידתי לחומרת המעשה שבוצע. בירנהק מאוריך לפגסוס, לעיל ה"ש 10; הרפז וגולן, לעיל ה"ש 73, בעמ' 330–337.

[308] עניין **אוריך**, לעיל ה"ש 94, בפס' 29 לפסק הדין של השופטת חיות.

[309] שם, בפס' 4 לפסק הדין של השופט אלרון.

[310] המלצות האגודה למצלמות גוף, לעיל ה"ש 149; טנא, לעיל ה"ש 22, בעמ' 423, 426, 428.

ישראלים.[311] במערכות מצלמות רבות, המצויות בשימוש העיריות השונות, יש אפשרות גישה מרחוק ברשת אל המחשב המכיל את המידע המצולם, ולכן סיכוני האבטחה גדולים יותר. כמו כן, לרשויות המקומיות אין את היכולת הכלכלית להגן על הנתונים.[312] דוגמה נוספת למאגר שאינו מאובטח דיו היא המאגר ברשות האוכלוסין. מדובר במאגר ביומטרי מיותר, מאחר שישנו מאגר ביומטרי ברשות הביומטרית, שם האבטחה וההגנה על המידע רבות.[313]

פריצה למאגר הביומטרי אפשרית במסגרת מבצע מתוכנן או כתוצאה מטעות וחוסר תשומת לב.[314] החשש לפריצה למאגר נתונים ביומטריים גדול אף יותר מדליפת נתוני מיקום, לוחיות רישוי, כרטיסי אשראי ומספרי תעודות זהות. זאת מאחר שמידע ביומטרי אינו ניתן להחלפה, ודליפתו עלולה לגרום לנזק בלתי הפיך.[315] נטען כי כאשר פני האנשים מטושטשים, הדבר מונע פגיעה בפרטיות. לאור זאת, בעיריות השונות נשמרים סרטונים של מבצעי עבירות ברזולוציה נמוכה,[316] כפי שבמאגר תמונות הפנים של רשות האוכלוסין נשמרות תמונות באיכות ירודה, שכן, בעבר לא ניתן היה להשתמש בהן לזיהוי ביומטרי. אך בשל התפתחויות טכנולוגיות שהתרחשו לאחרונה ניתן לזהות את האדם ביומטרית באמצעות תמונות אלו. על כן, אמצעי טשטוש ורזולוציה נמוכה אינם מבטיחים עוד כי לא תתקיים פגיעה בפרטיות.[317]

שימוש לרעה במאגרים: מתעורר חשש מפני ריכוז כוח רב בידיה של המדינה באיסוף מידע לגבי אזרחים, שכן ייתכן שימוש לרעה באותו מידע, כגון: שימוש חורג ובלתי מורשה על ידי בעלי סמכות.[318] כל אחד ממאגרי המידע שבידי המשטרה מתנהל לפי מערכת כללים נפרדת, שקשה להתחקות אחריה, וכך מתאפשר ניצול המידע גם לרעה.[319] לדוגמה: ישנה גישה למידע על תנועות של כלי רכב במערכת "עין הנץ" ללא הגבלה או בקרה בנוגע לצורך במידע ולשימוש ראוי. כבר נמצא בעבר כי במשטרת ישראל נעשה שימוש חורג במידע באופן לא חוקי לצרכים פרטיים.[320] המשטרה פעלה לסילוק שוטרים שהוטל ספק בטוהר מידותיהם, ואף בפסיקה התייחסו לתופעה חוזרת של שימוש משטרתי שלא כדין במאגרי מידע.[321]

---

[311] שם, בעמ' 423, 435, 437; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 15.

[312] אוסלנדר, לעיל ה"ש 4.

[313] עומר כביר "טביעות אצבע למאגר הביומטרי כבר לא נחוצות יותר" **כלכליסט** (23.12.2021) https://www.calcalist.co.il/calcalistech/article/bjw4r6gof (להלן: כביר (23.12.2021)).

[314] טנא, לעיל ה"ש 22, בעמ' 438; שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 10.

[315] טנא, לעיל ה"ש 22, בעמ' 423, 432, 436; שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 10; כביר (13.7.2022), לעיל ה"ש 110; כביר (23.12.2021), לעיל ה"ש 313.

[316] גולדשמידט, לעיל ה"ש 5, בעמ' 16; אוסלנדר, לעיל ה"ש 4.

[317] עומר כביר "תביעה נגד המאגר הביומטרי הסודי: "פגיעה בפרטיות" **כלכליסט** (9.6.2022) https://www.calcalist.co.il/calcalistech/article/hyaamvau5.

[318] בג"ץ **האגודה נ' משרד הפנים**, לעיל ה"ש 269; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 2, 15.

[319] אוסלנדר, לעיל ה"ש 4.

[320] עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 15 (מכתב הוועדה המייעצת למינויים לתפקידים בכירים בעניין "מועמדותו של יעקב שבתאי לתפקיד המפקח הכללי של משטרת ישראל"). במקרה אחד, שוטרת שבן זוגה נפרד ממנה השתמשה במערכות המשטרתיות כדי לאסוף פרטים על זוגתו החדשה ואז הגיעה לביתה ותקפה אותה. במקרה אחר, שוטר שחשד שאשתו בוגדת בו אסף פרטים על גבר שהיה לכאורה בקשר איתה, כולל כתובתו, מספר הרכב שלו, קשריו המשפחתיים ונסיעותיו לחו"ל. שוטרת העבירה מידע מתוך מערכת "עין הנץ" לצורך איתור רכבים שהועברו מעבר לקו הירוק וזאת ,לדבריה, על פי הנחייתו של המועמד לתפקיד מפכ"ל המשטרה, יעקב שבתאי. המפכ"ל הגיב ואמר, "שלא נתן אישור חופשי להשתמש במערכת המשטרתית. ייתכן שנתן אישור לסייע לניצב בדימוס כפי שנתן אישור לסייע לאיתוראן ולפוינטר ולכל מי שהחזיק צי רכב". אך מידע ממערכת "עין הנץ" עבר מהמשטרה לגורמים פרטיים, והעברות מידע שכאלו אינן מוסדרות. ב־2018 המשטרה סקרה שוטרים שעברו תחקיר ביטחוני לפני העברה לתפקיד רגיש. יותר מ־80% מהם העידו כי השתמשו במאגר המשטרתי לצרכים אישיים, לעיתים למען רווח. בבדיקה שערכה הקליניקה למניעת תביעות השתקה, הפועלת במסגרת התנועה לזכויות דיגיטליות, נמצא כי 6.3% מהרשעות שוטרים בעבירות משמעת היו בגין שימוש לרעה במאגרים. ראו אוסלנדר, לעיל ה"ש 4.

[321] עניין **דענא**, לעיל ה"ש 151; בג"ץ 78/01 **טקסירו נ' השר לביטחון פנים** (נבו 7.11.2001).

"זחילת פונקציות": קיימת תופעה של שימושים שניוניים או העברות מידע בין גופים שונים או מדינות שונות. לדוגמה: מאגר טביעות אצבע, שנאסף למטרות הנפקת תעודות זהות, משמש את משטרת ישראל.[322] שימוש במידע לצורכי מחקר יוצר חשש מפני זיהוי חוזר של המידע.[323] מצב שבו משטרת ישראל אוגרת מידע שאספה באמצעות כלי מעקב טכנולוגיים אחר האוכלוסייה פותח פתח לשימוש במידע זה כנגד אזרחים לשם אכיפת עבירות פחות חמורות מאלה שלשמן היה מותר לאסוף את המידע מלכתחילה.[324]

ה.4. <u>פגיעה בזכות לפרטיות בשלב ניתוח המידע</u>: בשלב ניתוח המידע ניתן לזהות שתי קטגוריות של התרחשויות המובילות לפגיעה בזכויות אדם. האחת נוגעת להיקף המידע שניתן להסיק על אודות האדם, והשנייה נוגעת לכשלים בטכנולוגיית בינה מלאכותית.

היקף המידע שניתן להסיק על אודות האדם: ככל שפריסת המצלמות רחבה יותר, המידע נצבר לאורך זמן רב ויכולות הניתוח משתפרות ומשתכללות, כך ניתן להסיק יותר מסקנות בנוגע לקטגוריות חדשות של מידע.[325] לדוגמה, באמצעות מערכת "עין הנץ" ניתן לדעת מהו צבע הרכב, סוג הרכב, מספר לוחית הרישוי, המקומות אליהם נסע, מספר הפעמים שנסע ליעד מסוים ואנשים שהתלוו אל הנהג בנסיעה. בנוסף, לוחית הרישוי מוצלבת מול רשימת מבוקשים, מאגר כלי הרכב או כל מאגר מידע משטרתי אחר. נתוני מיקום הם פרטי מידע בעלי רגישות גבוהה ביותר, שכן ממעקב אחר מיקום האדם ניתן להסיק נתונים בנוגע לפרטים אישיים ורגישים,[326] כגון: מצב בריאותו, הרגלי הצריכה שלו והעדפותיו המיניות. מנתונים אלו ניתן אף לחזות את התנהגותו בעתיד.[327]

דוגמה נוספת ליכולת טכנולוגית לניתוח מידע אשר פוגעת בזכות האדם היא ניתוח וידאו ותמונות סטילס באמצעות בינה מלאכותית. הבינה המלאכותית מחליפה את הצופה האנושי ומאפשרת לתמצת צילומים של שעות ארוכות לדקות בודדות המכילות מידע רלוונטי לשם הסקת מסקנות. סוגי הנתונים שניתן להסיק על בני אדם מניתוח צילומי סטילס או וידאו הם: מגדר, גזע, שיוך אתני, גיל, לבוש, השקפה דתית, עמדות פוליטיות, מאפייני התנהגות, מבנה אישיות, נטייה לאלימות, נטייה מינית, ניתוח רגשות ומצבי רוח מתווי פנים, טיב אינטראקציה חברתית ואופי הקשרים, מאפייני תנועה של התקהלויות חשודות ואירועים אלימים.[328]

בחוק "מערכות צילום מיוחדות" מאפשרים חקירת דפוסים של ביצוע עבירות במידע שייאגר ממערכות צילום "עין הנץ" ומצלמות זיהוי פנים ביומטריות. זאת כל עוד המידע לא כולל פרטים מזהים ולא ייעשה זיהוי בפועל.[329] אך גם תחת הגבלות אלו, סעיף זה מאפשר שימוש במערכת חיזוי פשיעה משטרתית לצורך אימון מערכות בינה מלאכותית, על מנת להבחין בין אנשים נורמטיביים

---

[322] טנא, לעיל ה"ש 22.
[323] שם, בעמ' 439.

[324] מכתב שוורץ אלטשולר, לעיל ה"ש 203.
[325] שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 7.
[326] בירנהק "פרטיות במשבר", לעיל ה"ש 297; בירנהק מאוריך לפגסוס, לעיל ה"ש 10. ס' 2(4) לתזכיר חוק הגנת הפרטיות (תיקון מס') (הגדרות וצמצום חובת הרישום), התש"ף–2020 https://did.li/0yEaa.
[327] טנא, לעיל ה"ש 22, בעמ' 440; בג"ץ **בן מאיר**, לעיל ה"ש 142, בפס' 37 לפסק הדין של השופטת חיות.
[328] שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 7–8; טנא, לעיל ה"ש 22, בעמ' 432, 439; בירנהק מאוריך לפגסוס, לעיל ה"ש 10; מנתונים ביומטריים אחרים כמו טביעות אצבע וסריקות קשתית ניתן להסיק נתונים נוספים. טביעות אצבע עשויות להעיד, למשל, על תסמונת דאון, וסריקת קשתית יכולה לחשוף שימוש באלכוהול או סמים.
[329] סעיף 10יב(א)(6) לתיקון פקודת המשטרה (מס' 40); מכתב אלטשולר שוורץ, לעיל ה"ש 203.

לפושעים. מאחר שמדובר במערכות אשר סובלות מכשלים טכניים, סיבתיים וערכיים, עלולה להיגרם פגיעה בזכות לשוויון ובזכות להליך הוגן.[330]

מהנתונים הנאספים ממחשבים, טלפונים ניידים ורשתות חברתיות, כגון: נתוני מיקום, טקסט, תמונות, הקלטות, סרטונים ושימוש באפליקציות שונות, ניתן ללמוד על מחשבותיו, לבטיו, סודותיו, רגשותיו, חוויותיו, עברו, תוכניותיו לעתיד, תחביביו, העדפות דת ותרבות פנאי, מצבו הכלכלי, נטייתו המינית, מצבו הבריאותי וקשריו עם אחרים של האדם.[331] את המידע הזה ניתן לנתח באופן אוטומטי ולייצר פרופילים אישיותיים עמוקים. היכולות החדשות מייצרות קטגוריות חדשות של מידע ומקשרות בין זהות האדם לפרטים אישיים על אודותיו.[332] בנוסף, לא ידוע לאדם מה עושה המדינה במידע שנצבר על אודות האדם ומהן המסקנות שהוסקו לגביו באמצעות ניתוח המידע.[333]

החשש מיצירת פרופילים עמוקים: מתעורר חשש כי המדינה תייצר פרופילים עמוקים משילוב נתוני אשראי וניבוי פשיעה ותשתמש במידע הזה לשם הענקת זכויות, אכיפה וגזרות כלכליות כלפי מי שאינו משתף פעולה עם השלטון, כפי שקורה בסין.[334] בסין האזרחים מצולמים ומקבלים דירוג בשל עבירות תנועה ורכוש באמצעות טכנולוגיית זיהוי פנים וגם על בסיס דפוסי רכישה בחנויות והתנהגויות מקוונות. הדבר מתאפשר בשל גישה כמעט בלתי מוגבלת למידע מאפליקציות ורשתות חברתיות.[335] במנגנון המעקב משתמשים בסין כלפי מתנגדי משטר, בני מיעוטים וכל מי שנחשד כי הוא אינו ממושמע דיו. אנשים שמסומנים נלקחים לחקירה ומעצר ואף מופעלים כנגדם אמצעי כפייה ושליטה נוספים.[336] ישנו חשש מפני התפתחויות דומות בישראל, שיובילו לשימוש במידע לשם מניעת הפגנות והפליית אוכלוסיות מוחלשות.[337] אך גם עתה רשויות בישראל עוקבות אחרי אזרחים ללא צורך, אינן מקפידות על שימוש באמצעים פחות פוגעניים בפרטיות ומסתירות חלק מהמידע שנאסף.[338]

לאחר שמיפיתי בפרק זה את הפגיעה בזכות לפרטיות ובזכויות נוספות בשל השימוש בכלים טכנולוגיים למעקב, אפנה לבחון את מידת הפגיעה בזכות לפרטיות. בנוסף, אתייחס לצורך באיזון בין זכות זו לבין האינטרס הציבורי לשמירה על שלום הציבור. לאחר מכן, אציע דרך להסדרת השימוש בכלים אלו, אשר תאפשר פיקוח על שיקול הדעת המשטרתי לשם שמירה על זכויות אדם, תוך איזון בין הזכות לפרטיות לזכויות אזרחים להגנה על חייהם.

ו. <u>בחינה חוקתית</u>

בפרק הקודם הדגמתי את עצם קיומה של פגיעה בזכות לפרטיות. אך הזכות לפרטיות היא לא זכות מוחלטת. לעיתים ייתכן כי היא תיסוג מפני זכויות אדם אחרות. לאור מתקפות טרור חוזרות ונשנות המלוות את מדינת ישראל מיום היווסדה, מתעורר צורך אקוטי לספק בידי משטרת ישראל

---

[330] מכתב אלטשולר שוורץ, לעיל ה״ש 203; ראו הבר וקדוש נוסבאום, לעיל ה״ש 44.
[331] בירנהק ״פרטיות במשבר״, לעיל ה״ש 297; .Mateescu et al, לעיל ה״ש 9, בעמ׳ 4.
[332] שוורץ אלטשולר וכהנא, לעיל ה״ש 6, בעמ׳ 7–8; טנא, לעיל ה״ש 22, בעמ׳ 432.
[333] שם, בעמ׳ 433.

[334] שוורץ אלטשולר וכהנא, לעיל ה״ש 6, בעמ׳ 6; אוסלנדר, לעיל ה״ש 4.
[335] גולדשמידט, לעיל ה״ש 5, בעמ׳ 3.
[336] שוורץ אלטשולר וכהנא, לעיל ה״ש **שגיאה! הסימניה אינה מוגדרת.**, בעמ׳ 11; טנא, לעיל ה״ש 22, בעמ׳ 440.
[337] .Mateescu et al, לעיל ה״ש 9, בעמ׳ 3; טנא, לעיל ה״ש 22, בעמ׳ 432; כביר (13.7.2022), לעיל ה״ש 110.
[338] אוסלנדר, לעיל ה״ש 4.

אמצעים לשמירה על ביטחון הציבור וחיי אדם. במצב זה נדרש ביצוע איזון בין הזכות לפרטיות לבין זכויות אחרות ואינטרסים אחרים. אם כן, מהו הליך האיזון שראוי לבצע בכל הנוגע לשימוש המשטרתי בטכנולוגיות מעקב וניבוי פשיעה? האם נדרש ביצוע איזון אנכי בין הזכות לפרטיות לאינטרס הציבורי לשמירה על ביטחון הציבור? או שמא מדובר באיזון אופקי בין הזכות לפרטיות לזכויות אזרחים אחרים לחיים ולביטחון.[339]

נטען כי עריכת איזון אנכי תוביל להכרעה בין הערכים המתנגשים, ואילו עריכת איזון אופקי ושימוש במבחני המידתיות יובילו לפשרה.[340] לכן, ההכרעה בשאלה האם מדובר באיזון אנכי או אופקי תשפיע על הבחירה בסוג הבחינה החוקתית – איזון אנכי או בחינת מידתיות הפגיעה. נטען כי שופטים בוחרים באיזון האנכי במקרים שבהם הם מבקשים הכרעה לטובת האינטרס הציבורי, בעוד בחירה באיזון האופקי ושימוש במבחני המידתיות נעשים במקרים שבהם השופטים מעוניינים בפשרה.[341]

1.1. <u>הסיבות שבגינן לא ראוי לבצע איזון אנכי</u>: הטוענים לאיזון אנכי בין הזכות לפרטיות לבין האינטרס הציבורי לשמירה על ביטחון הציבור מחזיקים בדעה כי לשימוש המשטרתי בכלים טכנולוגיים לשם מעקב ושיטור מנבא ישנם יתרונות רבים. בהמשך לכך נטען, כי ראוי שלא להגביל את השימוש המשטרתי בכלים אלו, שכן, השמירה על האינטרס הציבורי לביטחון עדיפה על שמירה על הזכות לפרטיות. בעידן המודרני משטרת ישראל לא תוכל להגן על חיי אזרחיה ללא שימוש בטכנולוגיה מתקדמת.[342] על משטרת ישראל חלה החובה להגן על חיי אדם ועל ביטחון הציבור.[343] במדינה שחווה מתקפות טרור רבות ראוי לאפשר למשטרת ישראל לפעול ללא מגבלות, לשם הגנה על האזרחים. נטען כי הגנה רחבה מדי על הזכות לפרטיות תפגע בהגנה על חיי אדם ותייקר את עלויות החקירה והמאמצים המושקעים בה. בנוסף, צמצום השימוש בכלים טכנולוגיים לשם מעקב ושיטור מנבא עלול להגביר את תחושת חוסר הביטחון ואף להוביל לפגיעה ממשית בחיי אדם.[344]

אך לגישתי, הפגיעה בזכות לפרטיות כלל אינה מבטיחה שמירה על חיי אדם ומניעת פשיעה. הטכנולוגיה הקיימת אינה מדויקת וסובלת מכשלים רבים. שימוש בכלים טכנולוגיים אלו לשם מעקב וניבוי עבריינות לא יוביל בהכרח להפחתה ברמות הפשיעה ולהגנה על חיי אדם. בהמשך לכך, שמירה על הזכות לפרטיות במהלך ביצוע פעולות מעקב משטרתיות אינה בהכרח הגבלת צעדי המשטרה והעמסה מיותרת, שכן, לעיתים מדובר בצעדים פשוטים וזולים שלא יכבידו על ביצוע פעולות משטרתיות.

טיעון נוסף התומך בהעדפה מוחלטת של האינטרס הציבורי לשמירה על חיי אדם על פני השמירה על הזכות לפרטיות נוגע להיות הזכות לפרטיות "זכות עמומה" שקשה להגדיר את גבולותיה מראש. בבג"ץ אוניברסיטת חיפה[345] נאמר כי הגדרתו של בירנהק את הזכות לפרטיות כעמומה מטבעה[346]

---

[339] ברק מדינה והגר שגב "'התנגשות' בין זכויות: אפיון מחדש של איזון אנכי ואופקי" **משפטים** מו 535, 536–541 (2017).

[340] גדעון ספיר "ישן מול חדש– על איזון אנכי ומידתיות" **מחקרי משפט** כב 471 (2006).

[341] שם, בעמ' 471–472.

[342] מבקר המדינה **דוח שנתי 67ב** (2016).

[343] ס' 3 לפקודת המשטרה.

[344] "תפקידה של בינה מלאכותית בשיטור חזוי ורפורמה במשפט פלילי" **בינה מלאכותית ישראל** (18.7.2023) https://katzr.net/f2e9b3.

[345] בג"ץ 844/06 **אוניברסיטת חיפה נ' עוז**, פ"ד סב(4) 167, פס' 20 לפסק הדין של השופטת חיות (2008) (להלן: בג"ץ **אונ' חיפה**).

[346] בירנהק "שליטה והסכמה", לעיל ה"ש 239, בעמ' 9, 72.

היא נכונה ומשקפת את הקושי ליצוק את הזכות לפרטיות לתבניות מוגדרות ותחומות מראש. נטען כי ראוי לשקול את התכונה האמורפית של הזכות לפרטיות כאשר מבצעים איזונים בין הזכות לפרטיות לבין האינטרס הציבורי לשמירה על ביטחון הציבור.

אך אני סבורה כי הקושי בהצבת הזכות לפרטיות בתבניות מוגדרות אינו מאיין לחלוטין אפשרות זו. הטיעון שלפיו מונח משפטי מסוים הוא עמום ולכן חשיבותו פחותה הוא בעייתי. כל הרעיונות והמושגים המשפטיים נתונים לפרשנות. הם יחסיים ומשתנים בהתאם לערכים חברתיים משתנים. לכן, הקושי להגדיר את גבולותיה של הזכות לפרטיות מראש אינו מפחית מחשיבותה באיזון בין זכויות לאינטרסים חברתיים. בבג"ץ אוניברסיטת חיפה דובר על חשיפת ראיות במשפט ועל חסינות, בעוד בחיבור זה נדונה הזכות לפרטיות בשלב החקירה במשטרה.[347] אמות המידה שנשקלו בפסיקה כאשר ביקשו לייצר חיסיון ראייתי חדש בשל הזכות לפרטיות אינן אמות המידה שראוי להשתמש בהן כשבוחנים את גבולות הזכות לפרטיות בהקשר של חקירה משטרתית. מדובר בשלב בהליך הפלילי שבו הפיקוח דל ושם ראוי להקפיד יותר על הזכות לפרטיות. במסגרת זו לזכות לפרטיות יש מעמד שונה.

נקודה נוספת שבה מובחן הנושא הנדון במאמר הנוכחי מבג"ץ אוניברסיטת חיפה נוגעת לכך שבבג"ץ דנו בשיחות שערכו אנשים אחרים על אודות אדם מסוים. בית המשפט קבע כי אלו אינם נתונים שהאדם עצמו ייצר, הם לא נבעו ממנו ולכן לא אמורים להיות בשליטתו. מוקד המידע או הנתונים היה דבריהם של בני אדם אחרים.[348] לכן, הדברים האמורים בבג"ץ אוניברסיטת חיפה פחות רלוונטיים לענייננו, שכן, בחיבור זה מדובר בנתונים שבהם חלקו של הפרט המבקש הגנה הוא עיקרי, ולא שולי.

לגישתי לא ראוי לבחור באיזון אנכי המסמן את האינטרס הציבורי לביטחון ושמירה על חיי אדם כזכות שגוברת באופן מוחלט על הזכות לפרטיות. זאת מאחר שהפגיעה בחייהם של הקורבנות הפוטנציאליים היא פגיעה ערטילאית. כלל לא בטוח שתתרחש פגיעה בחיי אדם. לעומת זאת, הפגיעה בזכות לפרטיות היא ודאית וחמורה.[349] כמו כן, קיים שוני בין פגיעה במעשה לפגיעה במחדל. פגיעה בזכויות האזרחים לפרטיות במעשה המעקב, החיפוש והמעצר שבעקבותיו חמורה יותר מהמחדל לפעול על מנת לנחש מי יפשע בעתיד. בנוסף, הגדרת אי־עשייה זו כמחדל היא בעייתית, מאחר שהפוטנציאל לבצע עבירות קיים בכל בני האדם.[350]

2.1. *<u>הסיבות שבגינן ראוי לבצע איזון אופקי</u>*: לגישתי ראוי לבצע איזון אופקי בין הזכות לפרטיות לבין הזכות לחיים ולביטחון. לשם כך, ראוי להשתמש במבחני המידתיות מאחר שמבחני המידתיות מעודדים פשרה, אשר משקפת גישה ערכית נכונה יותר מן האיזון האנכי. מבחני המידתיות מפורטים יותר, ובמסגרתם נשקלים שיקולים רבים יותר מאלו הנבחנים במסגרת האיזון האנכי. הניתוח המפורט שמבחני המידתיות מציעים מבטיח רגישות גבוהה יותר לנסיבותיו של כל מקרה

---

[347] בג"ץ **אונ' חיפה**, לעיל ה"ש 345, בפס' 20 לפסק הדין של השופטת חיות.

[348] שם.

[349] בג"ץ 73/53 **חברת "קול העם" בע"מ נ' שר הפנים**, פ"ד ז 871 (1953) (בו נקבע מבחן האיזון האנכי אשר כולל רכיב הסתברותי, המכונה "מבחן הוודאות הקרובה", שלפיו ניתן להגביל זכות חוקתית או לפגוע בה רק אם מימושה יגרום, בוודאות קרובה, נזק ממשי וחמור לאינטרס ציבורי).

[350] ראו את הדיון בהבחנה בין מעשה למחדל במאמר של רוני רוזנברג "על אפשרות ההרשעה בעברת ההריגה במחדל – מקרה קרפ כמבחן" **עלי משפט** יא 107, 111–119 (התשע"ד). ראו את הדיון בהבדל בין זכויות לפעולה לזכויות לאי־פעולה אצל אהרון ברק "הזכות החוקתית והפגיעה בה: תורת שלושת השלבים" **משפט וממשל** יט 119, 133–138 (התשע"ח) (להלן: ברק "הזכות החוקתית").

ומקרה ומונע מצב של החלת תפיסות זהות על מצבים שונים. מעבר לכך, נטען כי פסקת ההגבלה מאיינת את מבחן האיזון האנכי.[351]

בבחינת האיזון הראוי בין האינטרס הציבורי לביטחון לבין הזכות לפרטיות יש לבדוק את עומק הפגיעה בזכות לפרטיות. אם הפגיעה היא מידתית, אז האינטרס הציבורי לשמירה על ביטחון הציבור יגבר. *בשלב הראשון* של הבחינה החוקתית הצבעתי על עצם הפגיעה בזכות לפרטיות (בפרק ה׳). *בשלב השני* בבחינה החוקתית נבחנת השאלה האם הפגיעה בזכות לפרטיות נעשית כדין, כלומר האם החוק מקיים את דרישותיה של פסקת ההגבלה?[352]

הסמכה בחוק: לפי פסקת ההגבלה ניתן לפגוע בזכות לפרטיות רק אם משטרת ישראל מוסמכת בחוק באופן מפורש להשתמש באמצעים טכנולוגיים אלו.[353] בפרק ג׳ הצבעתי על הכשלים בהסמכת משטרת ישראל להשתמש בכלים הטכנולוגיים למעקב ושיטור מנבא. בנוגע לחלק מכלים אלו השימוש המשטרתי אינו עומד בתנאי פסקת ההגבלה ואף נוגד את עקרון חוקיות המנהל.[354]

הלימת הערכים: בנוגע לכלים אשר ניתנה לגביהם הסמכה באופן מפורש בחוק, יש לבחון את הלימת החוקים לערכיה של מדינת ישראל כמדינה יהודית ודמוקרטית. בפרק ה׳ ציינתי את הפגיעה בדמוקרטיה המתרחשת בעקבות הפגיעה בזכות לפרטיות. השימוש בכלים הטכנולוגיים למעקב ושיטור מנבא עלול לפגוע בזכויות בסיסיות במשטר דמוקרטי דוגמת הזכות להליך הוגן וחזקת החפות.[355]

תכלית ראויה: בשלב הבא במסגרת הבחינה החוקתית נבחנת הסוגיה – האם החוק נועד לתכלית ראויה? כביכול, תכליתם של החוקים הקיימים המסמיכים את משטרת ישראל לבצע מעקב היא מניעת פגיעה בחיי אדם וסיוע למשטרת ישראל בביצוע תפקידה במניעת פשיעה ושמירה על ביטחון הציבור והסדר הציבורי. ניתן להסכים כי זו אכן תכלית ראויה.[356] אך קיים חשש כי קיימת מטרה נסתרת – לאפשר למשטרת ישראל לעקוב אחר האוכלוסייה ולשלוט בה, באופן שאינו הולם את ערכיה הדמוקרטיים של המדינה. התנהלות זו אף עלולה לפגוע בזכויות אדם, כגון: חופש ההפגנה, חופש התנועה, חופש הביטוי ועוד.

מידתיות הפגיעה: השלב הבא בבחינה החוקתית הוא בחינת מידתיות הפגיעה. בשלב זה נעזרים בשלושת מבחני המידתיות: מבחן הקשר הרציונלי, בחינת הצורך ומבחן האיזון בין התועלת לנזק. אבקש להתייחס לטכנולוגיות מעקב בנפרד ולטכנולוגיות ניבוי עבריינות בנפרד.[357]

<u>מידתיות הפגיעה בזכות לפרטיות בשימוש בטכנולוגיות מעקב:</u> המבחן הראשון שאותו בוחנים לשם הכרעה בשאלת מידתיות הפגיעה בזכות הוא מבחן הקשר הרציונלי בין מטרת החוק להגשמתה באמצעים שנקבעו בחוק. האם האמצעי, שהוא שימוש בכלים טכנולוגיים למעקב, ישיג ברמה ממשית וגבוהה, ולא בהסתברות זניחה, את מטרת החוק להגן על שלום הציבור?[358] לשם כך

---

[351] ספיר ״ישן מול חדש – על איזון אנכי ומדתיות״, לעיל ה״ש 340, בעמ׳ 471–472.
[352] ברק ״הזכות החוקתית״, לעיל ה״ש 350, בע״מ 120–123; ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו.
[353] ס׳ 8 לחוק־יסוד: כבוד האדם וחירותו.
[354] ראו לעניין זה בג״ץ **מנאע**, לעיל ה״ש 143, בפס׳ 14 לפסק הדין של השופט פוגלמן.
[355] הבר וקדוש נוסבאום, לעיל ה״ש 44, בעמ׳ 40.
[356] ראו ברק ״הזכות החוקתית״, לעיל ה״ש 350, בעמ׳ 163.
[357] אהרון ברק **מידתיות במשפט: הפגיעה בזכות החוקתית והגבלותיה** 225–262 (2010) (להלן: ברק **מידתיות במשפט**).
[358] ראו בג״ץ 6298/07 **רסלר נ׳ כנסת ישראל**, פ״ד סה(3)1, פס׳ 55 לפסק הדין של השופטת ביניש (2012) (להלן: בג״ץ **רסלר**); ברק ״הזכות החוקתית״, לעיל ה״ש 350, בעמ׳ 165.

יש לבחון את יעילות הכלים הטכנולוגיים למעקב. האם מעקב אחר האוכלוסייה באמצעים טכנולוגיים אכן מוביל לירידה ברמות הפשיעה? ממסמך של איגוד האינטרנט הישראלי עולה כי חסרים נתונים סטטיסטיים שישפכו אור על הנושא, דוגמת – כמה חיפושים במכשירים חכמים מניבים כתבי אישום והרשעות.[359]

על מנת שהכלים הטכנולוגיים למעקב יועילו בהפחתת פשיעה עליהם לספק נתונים אמינים בנוגע לביצוע עבירות. אך נמצא כי מרכיבי התוכנה של הכלים הפורנזיים לחיקור טלפונים ניידים שרשויות החקירה משתמשות בהם עשויים לכלול חולשות אבטחה שבגללן ניתן לשבש או לשנות את הדו״ח הפורנזי של הסריקה ואת הנתונים של מכשירים אחרים השמורים במערכת.[360] ניתן להוסיף או להסיר טקסט, אימייל, תמונות, אנשי קשר ועוד. גם בנוגע לכלים פורנזיים לחדירה מרחוק מסוג תוכנות רוגלה יש בעיות אמינות. זאת מאחר שהפעלת כלים אלו מחייבת שינוי של נתונים על גבי המכשיר כדי להסתיר את פעולתם.[361] דוגמה זו ממחישה מצב שבו יעילות הכלי מוטלת בספק ופוגעת בסיכויים להשיג ברמה ממשית את מטרת החוק להגן על שלום הציבור. על מנת לצלוח מבחן זה יידרשו התמודדות עם כשלים טכנולוגיים אלו ואיסוף מידע בנוגע לתרומת השימוש בכלים טכנולוגיים למעקב להפחתת פשיעה.

השלב הבא בבחינת המידתיות הוא בחינת הצורך. לשם צידוק הפגיעה יש להוכיח כי לא ניתן להשיג את המטרה על ידי אמצעים אחרים שפגיעתם בזכות החוקתית פחותה. משטרת ישראל משתמשת בכלים טכנולוגיים רבים לשם מעקב אחר האוכלוסייה, כגון: כריית מידע מרשתות חברתיות, איכון טלפונים, האזנות סתר, חדירה למחשבים וטלפונים ניידים, מצלמות אבטחה ועוד. איזה מאמצעים אלו פוגעני פחות?

בניסיון שלי לדרג את פוגעניות השימוש בכלים השונים נתקלתי בקושי. הצעתי חלוקה למידע מסוג שיחות, מעשים והתנהגות. כביכול מחשבות הן הקטגוריה הפרטית ביותר שכן הן התהליך שמתרחש בין האדם לבין עצמו, ולו הזכות להחליט האם לחלוק בהן עם אחרים. אך ייתכנו מעשים אינטימיים שפרסומם יפגע בפרטיות האדם באופן חמור יותר ממחשבות מסוימות, שתוכנן פחות פוגע בפרטיות. ניתן לומר בזהירות כי הקטגוריה הבעייתית ביותר היא מחשבות ומאפיינים שהאדם עצמו אינו מודע אליהם, כגון: תסמונות רפואיות, נטיות ותכונות אופי שהאדם אינו מכיר בהן. לטכנולוגיה האפשרות לחשוף נתונים אלו ובכך לפגוע בפרטיות האדם באופן שלא היה אפשרי קודם לכן.

החלוקה לדיבור, מעשים ומחשבות נעשית על מנת למנוע את ההתעסקות של המחוקק בכלי הטכנולוגי ולהפנות את תשומת ליבו לסוג המידע שהושג, ולא לשם ייצור מדרג שיסייע בפתרון השאלה – מהו האמצעי הפחות פוגעני למעקב? ראוי לקבוע כי ההגנה צריכה להינתן לכלל הקטגוריות: דיבור, מעשים ומחשבות, וציון עומק הפגיעה ייעשה בכל מקרה לפי נסיבותיו. ראוי לבחון – האם ישנם אמצעי שיטור אחרים שעשויים להוביל להפחתת הפשיעה והגנה על חיי אדם מבלי לפגוע בפרטיות האזרחים? האם אופן הפעלת האמצעים הטכנולוגיים למעקב עשוי להשיג את המטרה בצורה שתוביל לפגיעה פחותה בזכות לפרטיות?

---

[359] מסמך איגוד האינטרנט, לעיל ה״ש 4, בעמ׳ 7–8.
[360] שם, בעמ׳ 32.
[361] שם, בעמ׳ 33.

השלב האחרון בבחינת המידתיות הוא שלב האיזון בין התועלת לבין הנזק, על פיו נדרש יחס ראוי בין התועלת החברתית, שהיא הפחתת הפשיעה, לבין הנזק העלול להיגרם בשל כך לזכות החוקתית.[362] על היקף הפגיעה בזכות לפרטיות ניתן ללמוד מהיקף השימוש בכלים טכנולוגיים לשם מעקב, ביניהם: מצלמות אבטחה, מצלמות רמזור, מצלמות "עין הנץ", מצלמות "עיר חכמה", מצלמות על גבי רחפנים ומצלמות הגוף של השוטרים. השימוש בכלים רבים לזיהוי ביומטרי, כגון זיהוי תווי פנים וטביעות אצבע, תורם אף הוא לפגיעה נרחבת בזכות לפרטיות. כלים טכנולוגיים נוספים המשמשים את משטרת ישראל ומרחיבים את היקף הפגיעה בזכות לפרטיות הם תוכנות רוגלה, מעקב אחרי נתוני מיקום והאזנות סתר. מלבד הפגיעה בזכות לפרטיות קיים חשש לגרימת נזקים נוספים בשל השימוש בטכנולוגיות אלו, כגון שימוש לרעה של גורמים בשירות המדינה בסמכות שניתנה להם למעקב והענקת כוח רב למדינה. נזק אפשרי נוסף עלול להיגרם בשל דליפות מידע כתוצאה ממתקפת סייבר או חשיפת גורם זר למידע, כמו גם מ"זחילת פונקציות" שתוביל לשימושים שניוניים או להעברות מידע בין גופים שונים או מדינות שונות. בנוסף, ישנו חשש מפני הדרה חברתית של אוכלוסיות מוחלשות שכלפיהן מופנה שיטור יתר וחשש מפני צמצום חופש הביטוי וההתכנסות בשל מבטו התמידי של "האח הגדול".[363] לכן, באיזון שבין הפגיעה הנרחבת בזכות לפרטיות והסיכונים העצומים הנשקפים מטכנולוגיות מעקב לבין יתרונות השימוש בכלים אלו, לאור הספק המוטל ביעילות השימוש בכלים אלו, ניכר כי הפגיעה המתרחשת כיום אינה מידתית. על מנת לצלוח מבחן זה יש להקפיד על צמצום הפגיעה בזכות לפרטיות בנוסף לשיפור יעילות השימוש בכלים בהפחתת פשיעה והצלת חיי אדם.

הכרעה בדבר מידתיות הפגיעה בזכות לפרטיות לאור השימוש המשטרתי בכלים טכנולוגיים למעקב תוכל להתקבל לאחר איסוף מידע בדבר השגת האמצעי את מטרת החוק לשמירה על שלום הציבור. בנוסף, נדרשת בחינת כל כלי בנפרד בהתאם למצב המתרחש בפועל, כגון שימוש במצלמה מסוימת באופן מסוים. זאת על מנת להכריע בשאלה – האם ישנם כלים פחות פוגעניים לשמירה על שלום הציבור? מידתיות הפגיעה בזכות לפרטיות מושפעת מאופן השימוש באמצעי המעקב ומהיקף השימוש בהם. כלומר, לא נדרשת הפסקת השימוש בכלים טכנולוגיים למעקב לשם הגנה על הזכות לפרטיות, אלא הקפדה על שימוש מידתי בהם.

<u>מידתיות הפגיעה בזכות לפרטיות בשימוש בטכנולוגיות ניבוי עבריינות</u>: בבחינת מידתיות הפגיעה אבחן ראשית את הקשר הרציונלי בין מטרת החוק להגשמתה באמצעים שנקבעו בחוק. האם האמצעי, שהוא שימוש בכלים טכנולוגיים לניבוי עבריינות, ישיג ברמה ממשית וגבוהה, ולא בהסתברות זניחה, את מטרת החוק להגן על שלום הציבור?[364] כביכול טיעון היעילות מצדיק את השימוש בטכנולוגיה ומוביל לחיסכון במשאבים. בהסתמך על ההנחה ששיעור קטן יחסית מהאוכלוסייה מבצע את רוב הפשעים, ראוי לייעל את השימוש במשאבי המשטרה ולמקד את מאמצי השיטור באנשים שמבצעים את מרבית הפשעים.[365] טכנולוגיות ניבוי עבריינות עשויות כביכול להשיג מטרה זו.[366]

---

[362] ברק "הזכות החוקתית", לעיל ה"ש 350, בעמ' 167.

[363] ראו אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 10. טנא, לעיל ה"ש 22**שגיאה! הסימניה אינה מוגדרת.**, בעמ' 423, 435; אוסלנדר, לעיל ה"ש 4.

[364] בג"ץ **רסלר**, לעיל ה"ש 358, בפס' 55 לפסק הדין של השופטת ביניש; ברק "הזכות החוקתית", לעיל ה"ש 350, בעמ' 165.

[365] דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בעמ' 48.

[366] שם, בעמ' 41–43.

אך בפועל, שיטה זו, הממקדת את מאמצי המשטרה באנשים שהוחלט לגביהם כי יש סיכוי רב שיבצעו פשעים, לא הוכחה אמפירית כשיטה יעילה.[367] גישה זו עלולה להוביל להתמקדות השיטור באוכלוסיות מוחלשות המופלות גזעית.[368] התוצאות ארוכות הטווח של תיוג אנשים ועבריינים טרם פשעו הן הדרה של אוכלוסיות שלמות ופגיעה בכבוד האדם, בשוויון ובזכות לפרטיות. שיטה זו של ניבוי עבריינות עלולה להוביל לניכור חברתי, אובדן האמון במערכת הצדק הפלילי, חוסר שיתוף פעולה עם המשטרה ובסופו של דבר הגברת רמת הפשיעה.[369] בהמשך לכך, נטען כי נדרש איזון בין צדק תהליכי לבין יעילות המשטרה. כאשר ההנחה הרווחת בציבור היא שהמשטרה בעלת חסרונות רבים, תפיסה זו עשויה ליצור חוסר שיתוף פעולה מצד האזרחים ואף לפגוע בעבודת השיטור.[370]

מעבר לכך, מתעוררים ספקות רבים בנוגע ליכולת של כלים טכנולוגיים כגון בינה מלאכותית לנבא עבריינות. שכן, ישנם פערים גדולים בין היכולות המיוחסות למערכות בינה מלאכותית לבין יכולותיהן בפועל, בשל כשלים בניתוח המידע.[371] ייתכנו טעויות בזיהוי ובדיוק ההכרעות בשל סיבות רבות, כגון: כשלים טכניים, בעיות בהגדרת הנתונים, בעיות בהליך הלמידה והכיול ובעיות במאגר המידע שעליו מתאמנת המערכת. כשלים טכניים באים לידי ביטוי בשגיאות קבלה ודחייה של מערכות ביומטריות, מאחר שקיימים הבדלים דקים בתנאי נטילת הדגימה.[372] תנאים כגון תאורה לקויה ולבישת אביזרים משפיעים על תפקוד הטכנולוגיה. כך ניתן להערים על מערכות זיהוי פנים באמצעות מסכות פנים ותמונות "זיוף עמוק" המיוצרות במחשב.[373] בעיות בהגדרת הנתונים מתבטאות בניסיון להפוך רגשות והתנהגויות מורכבות שהגדרתן אמורפית, עמומה ונתונה לפרשנות לערכים בינריים. כשלים בהליך הלמידה מתרחשים כאשר מערכות לומדות לא נבדקו כראוי. לעיתים נעשה כיול לא ראוי למערכת הלומדת אשר עשוי להשפיע על הדיוק שלה ויוביל לטעויות.[374]

ייתכנו בעיות בבסיס הנתונים שעליו מתאמנת מערכת בינה מלאכותית בשיטת למידת מכונה עמוקה. בסיס הנתונים משפיע על איכותה של המערכת. מערכות בינה מלאכותית מבוססות על נתונים וסטטיסטיקה, ואת אלה יוצרים בני אדם מוטים ומערכת מוטה. כאשר מאגר הנתונים שממנו לומדת המכונה הוא חלקי או מוטה, מדובר בייצוג חסר אשר אינו מהווה מדגם מייצג של כלל האוכלוסייה. לדוגמה, מערכות לזיהוי פנים שתהליך האימון שלהן נעשה בעיקר בחשיפה לפנים של אנשים בהירי עור מבצעות טעויות כשהן נדרשות לזהות פנים כהים.[375] הדבר עלול להוביל למסקנות מוטעות ולהטיות גזעניות ומגדריות.[376] הטיות אלו עלולות להוביל לפגיעה בזכויות

---

[367] ראו ענבר פלד ואח' **פרופיילינג: תמונת מצב בישראל ולקחים מהעולם** (נייר עמדה מאת הקליניקה לרב תרבותיות ומגוון 2017).

[368] ראו דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**, בעמ' 95.

[369] אדם שנער "יעילות, לוגיקה מוסרית ותרופות חוקתיות: שלוש הערות על פסק דין Floyd V. City Of New York" **המשפט ברשת: זכויות אדם** 17, 23 (2013).

[370] ג'סיקה סאונדרס ואח' **שיטור יעיל לישראל של המאה ה-21** (2014).

[371] אוסלנדר, לעיל ה"ש 4

[372] למשל, הזווית שבה נשענת כף היד על הסורק או התאורה בחדר. והן במאפיינים הביומטריים של אותו אדם, תווי הפנים למשל משתנים עם הזמן. טנא, לעיל ה"ש 22, בעמ' 425.

[373] אוסלנדר, לעיל ה"ש 4.

[374] הבר וקדוש נוסבאום, לעיל ה"ש 44, בעמ' 17. .

[375] Tooley, לעיל ה"ש 189, בעמ' 5.

[376] שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 4; Tooley, לעיל ה"ש 189, בעמ' 5.

ובהליך הוגן, להנצחת פערים והפליה. בהמשך לכך , ניתוח המידע האוטומטי יוביל להפליה אלגוריתמית, שתעצים את הגזענות כלפי אוכלוסיות מוחלשות.[377]

כשל נוסף המתגלה בשימוש בבינה מלאכותית לשם ניבוי עבריינות מתעורר בשלב פירוש התוצאות של התוכנות בידי בני אדם, בעלי תפקידים במערכת אכיפת החוק. קיים חשש כי הגורמים המובילים בפועל לתחזית לא יובנו כראוי.[378] נהוג להניח כי המחשב פועל ללא הטיות ולכן אין להטיל ספק במסקנותיו.[379] אך בפועל, הטיות בני האדם פוגמות בהליך הסקת המסקנות של הבינה המלאכותית. תוכנות אשר מתיימרות לנבא פשיעה מודדות בפועל דברים אחרים, כגון ההבניה החברתית של עבריינות, ולא את הנטייה של אדם לפשוע.[380]

השימוש בכלים טכנולוגיים על מנת לנבא עבריינות לא ישיג את מטרת החוק להגן על שלום הציבור. זאת, מאחר שהבינה המלאכותית אינה יכולה לחזות את העתיד. הסתמכות על טכנולוגיות ניבוי עבריינות מתעלמת מההבדל בין הפוטנציאל לבצע משהו, הכוונה להוציא אותו אל הפועל והביצוע עצמו. הבינה המלאכותית מנבאת את הסיכוי לאירועים עתידיים, ולא את האירועים עצמם. לאור הסברים אלו ניכר כי השימוש בכלים טכנולוגיים לניבוי עבריינות לא ישיג את מטרת החוק להגן על שלום הציבור ולהפחית פשיעה.

השלב הבא בבחינת המידתיות הוא בחינת הצורך. לשם צידוק הפגיעה יש להוכיח כי לא ניתן להשיג את המטרה על ידי אמצעים אחרים שפגיעתם בזכות החוקתית פחותה. כביכול, די בשימוש בכלים טכנולוגיים למעקב לשם הפחתת פשיעה, ואין צורך בעיבוד המידע על ידי בינה מלאכותית לשם יצירת פרופילים עמוקים על כל אזרח. חלק מהאמצעים הטכנולוגיים למעקב עשויים להיות פחות פוגעניים, ועל כן הם מהווים חלופה לשימוש בטכנולוגיות לניבוי עבריינות.

בהקשר זה נטען כי הפגיעה בזכות אדם שנוצרת בעקבות השימוש בבינה מלאכותית לשם קבלת החלטות, פחותה מזו שעלולה להיווצר בעקבות קבלת החלטות על ידי השוטרים. כלומר, כביכול על פי מבחן השימוש באמצעים פחות פוגעניים, דווקא השימוש בטכנולוגיה יוביל לפגיעה פחותה בזכויות אדם. נתי פרל גורס כי ראוי שאלגוריתמים יחליפו את השוטרים בתחום קבלת ההחלטות. לדידו, אלגוריתמים צולחים באופן מובהק ומדויק יותר את הדרישות המשפטיות לעומת השוטרים האנושיים. כמו כן, אלגוריתמים מקבלים החלטות מושכלות, שוויוניות ואפקטיביות יותר כיוון שהם אינם מושפעים מהטיות אנושיות וגורמים שונים.[381]

איני מסכימה עם עמדה זו שכן אני סבורה כי אלגוריתמים אינם מסוגלים לבצע הכרעות ערכיות טובות ובני אדם עדיפים עליהם במשימה זו, מאחר שבינה מלאכותית בשיטת למידה עמוקה אינה

---

377 Mateescu et al., לעיל ה"ש 9, בעמ' 3; טנא, לעיל ה"ש 22, בעמ' 432, 434; שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 4; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 14.

378 Walter L. Perry et al., Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations XIII 1–2, XXI-XX (2013).

379 Xiaolin Wu & Xi Zhang, *Automated inference on criminality using face images*, arXiv preprint arXiv: 1611.04135 4038 (2016).

380 עמית לגו "הטכנולוגיה של אפל אולי מקדימה את זמנה, אבל בכל הקשור ליחס לנשים הם תקועים במאה ה-19" **וואלה טכנולוגיה** (12.11.2019) https://tech.walla.co.il/item/3322986; רותי לוי "השיעור הכי חשוב שלא מלמדים בחוג למדעי המחשב" **TheMarker** (4.1.2019) https://www.themarker.com/technation/.premium-MAGAZINE-1.6807483.

381 נתי פרל "החלטה על קיומו של 'חשד סביר' בעולם ה-Big-Data: מהנמקה אנושית לאלגוריתמים לחיזוי פשיעה" **דין ודברים** יד 237 (2019).

מחויבת לערכים אנושיים.[382] הבינה המלאכותית אינה מבינה את משמעות ההחלטות שהיא מקבלת שכן היא אינה מסוגלת ליצור קשרים אשר מבוססים על רגש, מחויבות חברתית וזיכרון קולקטיבי. רכיבים אלו מייצרים את ההבנה והמחויבות לערכים חברתיים עליונים. לכן לגישתי, אי אפשר להסתמך באופן עיוור על החלטות של ישות שלא צמחה וגדלה באופן אנושי.[383] הבינה המלאכותית לא תשמור בהכרח על ערכים חשובים לאדם בניסיון שלה להתגבר על המגבלות של הנוסחאות המתמטיות, אשר מגדירות קבלת החלטות נכונה בעיני בני האדם שניסחו אותן.

גם אם נגביל את תהליך הלמידה של הבינה המלאכותית באמצעות הכלים הקיימים, כגון: למידה מחוזקת, למידה מפוקחת וניקוי בסיס המידע, יישאר אלמנט של "קופסה שחורה". לאור זאת מתעוררות השאלות: האם זה נכון לתת ל"קופסה השחורה" להכריע בנוגע לגורלו של אדם, ובפרט – לבינה מלאכותית שאין לה רגש ולכן אין לה תכלית. ישנה גישה שלפיה ה"קופסה שחורה" ואלגוריתמים מקריות משחררים את האנושות מהכרעות מוסריות קשות והן יושארו ליד המזל. אבל לדעתי ראוי להשאיר את ההכרעה בידי בני האדם. לגישתי קיים פגם מוסרי במצב שבו נגרם נזק בשל הסתמכות על החלטותיה של "קופסה שחורה".

הסתמכות עיוורת על הכרעות בינה מלאכותית תוביל לחוסר אמון של הציבור במערכת אכיפת החוק. החלטות הבינה המלאכותית צפויות להתבסס על אלגוריתמים מורכבים. לכן צפויים קשיים בהבהרת תהליך קבלת ההחלטות. אזרחים שאינם בקיאים בנוסחאות מתמטיות יתקשו לברר את העובדות. במצב דברים זה משטרת ישראל והאזרחים מתבקשים למעשה לסמוך על החישובים של המתכנתים.[384] אך מתכנתים של בינה מלאכותית בשיטת למידת מכונה עמוקה אינם יכולים להסביר לגמרי כיצד המערכת הגיעה למסקנותיה. לא ברור מהם המשתנים המסבירים המשפיעים על התוצאה. משטרת ישראל אינה יכולה להסביר לציבור כיצד פועלות המערכות שבהן היא משתמשת, כאשר הן מבוססות על בינה מלאכותית בשיטת למידת מכונה עמוקה. באופן כזה אי אפשר לממש את "עקרון השקיפות השלטונית".[385] התוצר של מצב זה הוא תחושת חוסר אונים של האזרחים, אשר אינם מסוגלים להבין את תהליך קבלת ההחלטות בנוגע אליהם ואינם יכולים להשפיע עליו.

פגם נוסף בטיעון של נתי פרל נוגע להנחה השגויה כי אלגוריתמים אינם מושפעים מהטיות אנושיות. בשל הטיות בבסיס הנתונים, הטיות מתכנתים והטיות חשיבה של גורמי אכיפת החוק שישתמשו בפלט התוכנה, השימוש בטכנולוגיה אינו נקי מהטיות. תוכנות ניבוי עבריינות מבצעות "הפליה אלגוריתמית" אשר משכפלת ומעבירה הטיות חשיבה אנושיות למנגנון קבלת החלטות ממוחשב.[386] במצב הנוכחי הטכנולוגיה לא תוביל להתגברות על הטיות חשיבה, אלא תשכפל ותעצים את הפגיעה בזכות לשוויון ואת הפגיעה בזכות לפרטיות של אוכלוסיות מוחלשות, אשר בתורן יובילו לעלייה ברמות הפשיעה. הטכנולוגיה עצמה מסווה את אותן ההטיות, מסתירה אותן מאחורי "הקופסה

[382] Nora Osmani, *The Complexity of Criminal Liability of AI Systems*, 14 MASARYK U. J. L. & TECH. 53, 61 (2020).

[383] David C. Vladeck, *Machines without Principals: Liability Rules and Artificial Intelligence*, 117 WASH. L. REV 129 (2014).

[384] Alexander Hevelke & Julian Nida-Rumelin, *Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis*, 21 SCI. & ENGINEERING ETHICS 619 (2015).

[385] שורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 5.

[386] Haber, לעיל ה"ש 223, בעמ' 90–91. לקריאה נוספת על גזענות וטכנולוגיה, ראו למשל RUHA BENJAMIN, RACE AFTER TECHNOLOGY (2019).

השחורה" ומציגה את החלטותיה כאובייקטיביות. הטיות החשיבה של השוטרים לא ישתנו בשל השימוש בטכנולוגיה. גם במצב שבו נעזרים בטכנולוגיות לשיטור מנבא נדרשת פעולה אנושית. השוטרים אשר מסתמכים על התחזיות נדרשים לבצע בעקבותיהן פעולות שיטור. הטיפול במי שסומן כעבריין פוטנציאלי יוביל אף הוא להפליה גזעית, ולא יאיין את הטיות החשיבה.[387]

חשוב להדגיש כי נתי פרל מתייחס לפגיעה בזכות לשוויון, בעוד אני דנה במאמר זה בעיקר בפגיעה בזכות לפרטיות. התאמה של טענה זו לפגיעה בזכות לפרטיות תבחן - האם חל צמצום בפגיעה בזכות לפרטיות בשימוש באמצעים טכנולוגיים לשם ניבוי עבריינות? נטען כי האלגוריתם הוא זה שנחשף אל הנתונים. לכן, כאשר האדם לא נחשף למידע רגיש, לא נגרמת פגיעה בזכות לפרטיות. אך המצב הנוכחי, שבו ניתן להפיק מידע רלוונטי מחומר רב, פוגע פגיעה חמורה יותר בזכות לפרטיות. זאת מאחר שבעבר לא ניתן היה לעבד את כמויות המידע הרבות, והסיכוי שייעשה בהן שימוש היה נמוך יותר.[388] עצם הפעלת התוכנה פוגע כשלעצמו בזכות לפרטיות. בהתאם לקביעות האיחוד האירופי, מידע ביומטרי הוא מידע רגיש,[389] ועצם עיבוד המידע ללא הסכמה מהווה פגיעה בפרטיות.[390] היקף הפגיעה בפרטיות ייבחן גם בהתאם ליישום של פלט התוכנה.

אכן, חוק הגנת הפרטיות מעניק פטור לרשויות הביטחון לגבי פגיעה בפרטיות שנעשתה באופן סביר במסגרת תפקידן ולשם מילויו.[391] בהתאם לכך, משטרת ישראל יכולה להחליט שעיבוד המידע שנאסף לצורך חיזוי פשיעה הוא חלק ממילוי תפקידה. אך מדובר בפטור גורף בשל גודל הפגיעה בזכויות אדם. פטור זה אינו מעניק למשטרת ישראל זכות מראש לפגוע באופן שיטתי בפרטיות.[392] מעבר לכך, חוק הגנת הפרטיות אינו מאפשר פטור מפגיעה בזכויות אדם אחרות.

השלב האחרון בבחינת המידתיות הוא שלב האיזון בין התועלת לבין הנזק. בהתאם למבחן זה נדרש יחס ראוי בין התועלת החברתית שהיא הפחתת הפשיעה ושמירה על חיי אדם, לבין הנזק העלול להיגרם לזכות החוקתית בשל השימוש בכלים הטכנולוגיים.[393] עומק הפגיעה בשימוש בטכנולוגיה לשם שיטור מנבא בשלב ניתוח המידע באמצעות בינה מלאכותית הוא עצום. התוכנות עלולות לאסוף מידע אישי על בני האדם בנוגע למצב רפואי ונפשי שהאדם עצמו אינו מודע לו. עומק הפרופילים האישיים שניתן לייצר באמצעות טכנולוגיה זו הוא חסר תקדים.[394] חוסר הסימטריה בין האזרח שאין בידיו כלים אלו, לבין המדינה, עלול לפגוע באופיו הדמוקרטי של המשטר.[395] העיבוד האוטומטי של המידע עלול להוביל להפליה אלגוריתמית ולתוצאות אבסורדיות ושגויות.[396] בהתחשב בפגיעה ההרסנית בזכות לפרטיות ובדמוקרטיה למול הספק הרב ביעילות השימוש בכלי להפחתת פשיעה והגנה על חיי אדם, ניכר כי מבחן זה אינו צולח. העלות היא גבוהה, בעוד התועלת

---

387 דו"ח האקדמיה בנושא שיטור יזום, לעיל ה"ש 17**שגיאה! הסימניה אינה מוגדרת.**, בעמ' 26, 48.

388 תמרי, לעיל ה"ש 6.

389 פרט 1 לתוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017.

390 Tal Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2017).

391 ס' 19 לחוק הגנת הפרטיות; רע"א 2558/16 **פלונית נ' קצין התגמולים משרד הביטחון**, פס' 59 לפסק הדין של השופטת ברק־ארז (נבו 5.11.2017).

392 תהילה שוורץ אלטשולר "טכנולוגיות מעקב וזיהוי פנים – בקרוב בירושלים?" **המכון הישראלי לדמוקרטיה** (16.7.2019) https://www.idi.org.il/articles/28234.

393 ברק "הזכות החוקתית", לעיל ה"ש 350, בעמ' 167.

394 שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 6; אוסלנדר, לעיל ה"ש 4.

395 SOLOVE J., לעיל ה"ש 264; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 14.

396 Mateescu et al., לעיל ה"ש 9, בעמ' 3; טנא, לעיל ה"ש 22, בעמ' 432, 434; שוורץ אלטשולר וכהנא, לעיל ה"ש 6, בעמ' 4; עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 14.

היא נמוכה. על מנת לצלוח מבחן זה נדרש שיפור משמעותי ביכולות הטכנולוגיה והקפדה על צמצום היקף הפגיעה בזכות לפרטיות.

לסיכום, הקפדה על פגיעה מידתית בזכות לפרטיות לא תחסום את משטרת ישראל מלהשתמש בכלים טכנולוגיים למעקב ולשיטור מנבא. מבחני המידתיות מאפשרים פגיעה מידתית בזכות לפרטיות לשם שמירה על אינטרס ציבורי לביטחון ולהגנה על חיי אדם. אך הם גם מציבים חובה להשתמש בכלים טכנולוגיים למטרה המקורית לשמה הותר איסוף המידע, להקפיד על היקף המידע וסוג המידע שהושג ולשמור ככל האפשר על פרטיות האזרחים. שמירה על מידתיות הפגיעה משמעותה מודעות לכשליה של הטכנולוגיה והימנעות מהסתמכות עיוורת עליה. משטרת ישראל תידרש להפעיל שיקול דעת בהסתמכות על הטכנולוגיה ולהקפיד על שמירה על הזכות לפרטיות של האזרחים, בשל חשיבותה הרבה לכינון משטר דמוקרטי.

בפרק זה בחנתי את השאלה – האם הפגיעה בזכות לפרטיות נעשית בהתאם לפסקת ההגבלה? הסברתי מדוע הפגיעה בזכות לפרטיות אינה מידתית כאשר מדובר בטכנולוגיות לניבוי עבריינות. בנוסף, הסברתי מדוע נדרשת בחינת מידתיות הפגיעה בטכנולוגיות מעקב בנוגע לכל כלי טכנולוגי בנפרד, בהתאם למידת הפגיעה שתתרחש במציאות. כעת אפנה לשלב השלישי בבחינה החוקתית ואציע סעד חוקתי בדמות שינוי חקיקה. ההסדרה החוקית המוצעת תאפשר הפעלת כלים טכנולוגיים למעקב תוך שמירה על פגיעה מידתית בזכויות אדם. מטרה זו תושג באמצעות פיקוח הולם על פעולות המשטרה. בנוסף, אציע לאסור שימוש בטכנולוגיות ניבוי עבריינות ללא ביצוע מחקר מעמיק בנוגע ליכולות האמיתיות של הטכנולוגיה להגן על חיי אדם. אם טכנולוגיית ניבוי עבריינות תאושר בעתיד, יש לעשות זאת לאור מודעות לכשלי הטכנולוגיה ומגבלותיה.

ז. הסדרת השימוש בכלים אלו

התחום הטכנולוגי הוא ייחודי במשפט ורווי בחילוקי דעות על סוגיותיו. השופט פרנק איסטרברוק טען כי לא ראוי להתייחס לטכנולוגיה כתחום בפני עצמו. לגישתו, לא נדרשים "דיני סייברספייס" כשם שאין צורך ב"דיני סוסים".[397] בהתאם לגישה שלפיה טכנולוגיה אינה מהווה תחום משפטי נפרד, ההתייחסות המשפטית לטכנולוגיה נעשית בגדרי תחומים משפטיים מסוימים או בהקשר של דוקטרינות ספציפיות.[398]

לעומת זאת, לורנס לסיג סבור כי הסייברספייס מציג אתגרים ייחודיים שדורשים שיקולים חדשים בנוגע לרגולציה.[399] אף אלקין־קורן ובירנהק ביקשו לבחון את ההשקה בין הטכנולוגיה למשפט ממבט־על, ולא להגביל את עצמם לדוקטרינות משפטיות מסוימות.[400] דוגמה נוספת להכרה בייחודיות המשפטית של התחום הטכנולוגי ניתן לראות בטענת ניסנבאום ופרידמן כי נדרשת רגולציה ייחודית של טכנולוגיה המבוססת על תוכנת מחשב לשם הגנה על זכויות אדם.[401] בהתאם

---

[397] .Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999)

[398] כגון: אחריות ספקי שירות, עבירות מחשב או עבירות אחרות שיש להן פן מחשובי וראיות אלקטרוניות. ראו ניבה אלקין־קורן ומיכאל בירנהק "הקדמה: משפט וטכנולוגיות מידע" **רשת משפטית: משפט וטכנולוגיית מידע** 11,12 (ניבה אלקין־קורן ומיכאל בירנהק עורכים 2011).

[399] Lessig, לעיל ה"ש 397, בעמ' 1–2, 46–47.

[400] אלקין־קורן ובירנהק, לעיל ה"ש 398, בעמ' 12.

[401] דניאל בן־אוליאל "ארגוני תקינה והמשבר הדמוקרטי בעידן המידע" **רשת משפטית: משפט וטכנולוגיית מידע** 246 (ניבה אלקין־קורן ומיכאל בירנהק עורכים 2011); Batya Friedman & Helen Nissenbaum, *Bias in Computer*, 14 ACM TRANSACTIONS ON INFO. SYS. 300 (1996).

לכך, בהנחיות האיחוד האירופי בנוגע להסדרת בינה מלאכותית[402] והצו הנשיאותי שניתן לאחרונה בארצות הברית לשם הגנה על זכויות מפני בינה מלאכותית,[403] ניכרת הכרה ב"דינים טכנולוגיים" כתחום העומד בפני עצמו. למרות זאת, קבעה שרת הטכנולוגיה בישראל כי "אין מקום בעת זו לקידום רגולציה באמצעות חקיקה רוחבית שהיא ייחודית לתחום הבינה המלאכותית."[404]

אני סבורה כי ראוי להתייחס למאפיינים הייחודיים של התחום הטכנולוגי בכל הקשור לרגולציה. נדרשת התייחסות לכלל הכלים הטכנולוגיים שנמצאים בשימוש רשויות מנהליות,[405] זאת לשם הסדרה קוהרנטית ועקבית של התחום. ההתייחסות הפרטנית לכל כלי בנפרד היא בעייתית בשל יצירת נהלים כפולים, שונים זה מזה, המובילים לבלבול ולמדרג נורמטיבי משובש. בנוסף, התנהלות זו מאפשרת יצירת מסלולים שעוקפים את הביקורת השיפוטית והדרישה לצו שופט לשם השימוש בכלים מסוימים.

אני מציעה חלוקה של הכלים השונים לקטגוריות בהתאם לסוג הנתונים הנאספים, למיקום האיסוף, בספרה הפרטית או הציבורית, ולגוף המחזיק במערכת איסוף הנתונים ומאגר המידע, במשטרת ישראל או בגוף אחר. זאת מאחר שהאמצעים הטכנולוגיים השונים כוללים השגת מידע מסוגים שונים, כגון: דיבור, מעשים, מחשבות, כך שהחוקים הנפרדים אינם יכולים להסדיר את השימוש בהם בצורה מלאה.[406] ההתמקדות בתוצר הסופי, שהוא סוג המידע, ולא בתהליך, שהוא האופן שבו טכנולוגיה מסוימת משיגה את המידע, מאפשרת הגנה ראויה לזכות לפרטיות.

בשל ההתפתחויות הטכנולוגיות המהירות וההתקדמות האיטית של המחוקק, נדרשת הסדרה שתאפשר קדמה טכנולוגית ללא שינוי בהגנה על זכויות אדם. החוקים הקיימים שמתמקדים בכלי הטכני הם מיושנים ויש לעדכנם. לפיכך, בפרק זה אציג את פרטי החקיקה המצריכים עדכוני חקיקה לאור התמורות הטכנולוגיות ואציע "קריאת כיוון" לשינויים הנדרשים, ברוח האמור במאמר. את השינויים אציג בנפרד בנוגע לשלב איסוף המידע ושלב עיבוד המידע.

ז.1. __הסדרת שלב איסוף המידע בחקיקה חדשה__:

__חוק האזנת סתר יהפוך ל"חוק המסדיר איסוף מידע באמצעים טכנולוגיים מרוחקים ממרחבים פרטיים ובאמצעים טכנולוגיים לחיפוש פיזי"__: בחוק האזנת סתר הנוכחי מוסדר איסוף מידע מסוג דיבור ושיחות אף בטקסט.[407] אך נדרשת הסדרה גם של מידע הנוגע לדיבור ושיחות בתמונות ובווידאו. עד לפיתוח תוכנות הרוגלה לא נהגה משטרת ישראל לאסוף ראיות ממצלמות במרחבים פרטיים. אך כעת הטכנולוגיה מאפשרת זאת, ומשטרת ישראל משתמשת בכלים אלו. על כן, ראוי להתייחס בחוק החדש למידע מסוג זה ולקבוע כי פתיחת מצלמות מרחוק בטלפון הנייד או במחשב

402 רגולציה לבינה מלאכותית של האיחוד האירופי, לעיל ה"ש **שגיאה! הסימניה אינה מוגדרת.**.

403 *Excutive order on the safe, secure, and trustworthy development and use of artificial intelligence*, THE WHITE HOUSE (October 30, 2023), https://did.li/kzEaa. צו מנהלי בנושא קביעת סטנדרטים חדשים לפיתוח ושימוש אחראי בבינה מלאכותית. הצו מבקש לשפר את תקני הבטיחות והפרטיות של מערכות בינה מלאכותית לקידום שוויון וזכויות אזרח, זאת על ידי הימנעות מאלגוריתמים של בינה מלאכותית המקדמים הפליה, יצירת אמות מידה מיטביות לשימוש בבינה מלאכותית במערכת המשפט, פיתוח הנחיות לשימוש ורכש של סוכנויות פדרליות של בינה מלאכותית והאצת גיוס עובדים מיומנים בתחום לזרועות הממשל.

404 מסמך מדיניות בינה מלאכותית ישראלי, לעיל ה"ש 205, בעמ' 3.

405 עתירת האגודה לזכויות האזרח, לעיל ה"ש 5, בעמ' 2; הרפז וגולן, לעיל ה"ש7373, בעמ' 336.

406 על ההסדר החוקי לעמוד בתנאי ס' 8 לחוק־סוד: כבוד האדם וחירותו כך שיהא הולם את ערכיה הדמוקרטיים של מדינת ישראל, לתכלית ראויה וכי הפגיעה בזכות לפרטיות תיעשה באופן מידתי.

407 ס' 1 לחוק האזנת סתר.

תיעשה רק במצבים של סיכון לחיי אדם, מאחר שמצלמות אלו עלולות לקלוט מצבים אישיים ביותר ולפגוע בזכות לפרטיות באופן לא מידתי.

מאחר שהטלפון הנייד מכיל גם מידע ביומטרי, על המחוקק להתייחס גם לאיסוף מידע מסוג זה. חוק סדר הדין הפלילי (סמכויות אכיפה – חיפוש בגוף ונטילת אמצעי זיהוי), התשנ״ו–1996 מסמיך שוטרים לאסוף נתונים ביומטריים במסגרת הליך חיפוש פיזי. אך כיום אמצעים טכנולוגיים מאפשרים איסוף נתונים ביומטריים מרחוק באמצעות תוכנות מעקב המאפשרות פריצה למאגרי המידע שעל גבי המכשיר. על המחוקק להסמיך במפורש בחוק את משטרת ישראל לבצע פעולות אלו. בנוסף עליו להגדיר את התנאים שבהם ניתן לבצע פעולות כגון אלו במסגרת חקירת עבירות מסוג פשע, לשם הצלת חיי אדם ולצורכי מלחמה בטרור.

בנוסף, ראוי להסדיר בחוק זה השגת מידע מסוג מעשים בנוגע לפעולות האדם באפליקציות ואתרים ובנוגע לנתוני מיקום, כמו גם נתונים השייכים לקטגוריית סטטוס, כגון: מצב רפואי ומצב כלכלי. ישנם כלים טכנולוגיים המשמשים את משטרת ישראל לשם השגת נתונים אלו, והם אינם מוסדרים בחוק. על המחוקק להכריע באילו מצבים ניתן לאסוף נתונים אלו וראוי שיאפשר זאת בעבירות מסוג פשע בלבד ובמצבים שבהם קיים סיכון לחיי אדם. איסוף המידע הקיים ברשתות חברתיות בספרה הציבורית אינו מצריך בקשת צו משופט או מנגנוני פיקוח פנימיים. אך חדירה לתוכן המצוי ב״ספרה הפרטית הווירטואלית״, בפרופילים פרטיים, שקול לביצוע האזנת סתר או שימוש בתוכנת רוגלה לשם מעקב. אם פעולה זו מבוצעת באמצעים טכנולוגיים לחדירה מרוחקת או באמצעים טכנולוגיים לחדירה פיזית לאחר תפיסת המכשיר ראוי כי תוסדר תחת חוק זה.

ראוי כי חוק זה יסדיר גם איסוף נתונים המתעדים מחשבות, כגון: טקסט, וידאו, אודיו, יומן דיגיטלי ועוד, לשם מניעת פגיעה לא מידתית בפרטיות. ראוי לקבוע כי הדבר ייעשה רק בעבירות מסוג פשע ולשם הצלת חיי אדם ותחת נהלים אשר יבטיחו תיעוד הפעולות המשטרתיות ושקיפות הנהלים המסדירים את פעולות המשטרה.

אופן הגשת צו בקשה לשופט: לשם איחוד נוהלי בקשת צו משופט ראוי כי כל הפניות ייעשו לשופט שלום. הסיבה שבגללה ראוי לקבוע כי השופט שיאשר בקשות למעקב יהיה שופט שלום היא שהקצאת שופט מחוזי לשם קבלת החלטות בתחום האזנות סתר לא הוכיחה את עצמה כמנגנון פיקוח חזק. לראיה, אחוזי דחיית בקשות להאזנות סתר הם נמוכים ביותר.[408] לאור זאת, ראוי לנסות גישה אחרת של הקצאת שופט שלום, שכל תפקידו יהיה לפקח באופן יום יומי על בקשות משטרת ישראל להאזנת סתר, התקנת תוכנת רוגלה, שימוש בתוכנה לשם איתור מיקום האדם, קבלת נתוני תקשורת ואיכון טלפונים ניידים. כך הטיפול בכלים טכנולוגיים לשם פעולות שיטור ייעשה על ידי אותו השופט, ויימנע מצב שבו מוגשות בקשות כפולות לשופטים שונים. בצו הבקשה מהשופט משטרת ישראל תציין מהו סוג המידע המבוקש ותוכל לאסוף רק סוג מידע זה. אם אין אפשרות להפריד בין סוגי המידע, והחדירה המרוחקת למכשיר חושפת את השוטר לכל סוגי המידע הקיימים במכשיר, על משטרת ישראל לציין זאת בבקשה לצו.

---

[408] החוק הקיים מאפשר ביצוע מעקב אף ללא צו שופט במקרים דחופים. המקרים שמגיעים לבית המשפט מאושרים כמעט אוטומטית. שיעור הבקשות לצווים מכוח חוק האזנות סתר וחוק נתוני תקשורת שנדחו בבית המשפט נמוך מ־0.5% לאורך כל התקופה המדווחת. ראו למשל כהנא ושני, לעיל ה״ש 69, בעמ׳ 12–14.

יש לשמר מהחוקים הקיימים את המנגנון בסעיף 7 לחוק האזנות סתר המאפשר פנייה למפכ״ל המשטרה במקרים שאינם סובלים דיחוי לשם מניעת פשע או גילוי מבצעיו. כמו כן, יש לשמר את מנגנוני הדיווח, הערעור והבקרה שבסעיף 6 לחוק ולהחיל אותם על כל סוגי הנתונים החדשים שיוספו לחוק. השארת הסעיפים המאפשרים אישור במקרים דחופים על ידי מפכ״ל המשטרה במקום פנייה לשופט יאפשרו איזון בין פגיעה בזכות לפרטיות לשמירה על האינטרס הציבורי להגנה על שלום הציבור.

סעיף 11 בחוק המחשבים וסעיף 23(א) בפקודת סדר הדין הפלילי ייכנסו ל״חוק האזנות סתר החדש״.[409] הם יסדירו איסוף מידע באמצעים טכנולוגיים פיזיים, כלומר, לאחר תפיסה פיזית של מחשבים וטלפונים ניידים בפרק נפרד בחוק. יש לציין בבקשה משופט כשמדובר בחדירה פיזית למכשיר שאינה מאפשרת סינון המידע הנדרש משאר הנתונים הנשמרים במכשיר. יש לציין בבקשה כאשר מדובר בהעתקת כל החומר השמור על גבי המכשיר. בנוסף, על משטרת ישראל להתייחס בבקשה לצו החיפוש לאפשרות להעתיק חומרים השמורים ב״ענן״ על גבי שרתים מרוחקים. כעיקרון, מדובר בחריגה מחיפוש פיזי, והפעולה הזו מחזירה אותנו לחיפוש טכנולוגי מרחוק. לכן, חשוב להכניס תחת חוק זה גם את סעיפי החיפוש הפיזיים תחת פרק נפרד, על מנת שנוהלי הגשת הבקשה לצו משופט יהיו אחידים. אם הנהלים יהיו אחידים, ניתן יהיה להגיש בבקשה אחת גם חיפוש פיזי וגם חיפוש מרוחק מבלי שהדבר יהווה חריגה מסמכות.

בנוסף, נדרשת הטלת חובת תיעוד של פעילות הכלים הפורנזיים לחדירה ולחיפוש במכשירים חכמים, כגון: ניהול רשומות ברורות, יומני ביקורת מפורטים והקלטות מסך אוטומטיות.[410] כמו כן, ראוי להטיל חובות שקיפות, דיווח ורישום ציבורי על האופן שבו רשויות אכיפת החוק משתמשות בכלים הטכנולוגיים לשם מעקב וניבוי עבריינות.[411]

__חוק נתוני תקשורת יהפוך ל״חוק המסדיר קבלת מידע אשר נאסף ומוחזק בידי רשויות אחרות״__:

בחוק נתוני תקשורת הנוכחי מוסדרת העברת מידע מסוג נתוני זיהוי, נתוני מיקום, נתוני מנוי ונתוני תעבורה. אך ישנן קטגוריות מידע שאליהן החוק אינו מתייחס, כגון: מידע ביומטרי (המוסדר בחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש״ע–2009), מידע רפואי, מידע כלכלי (המוסדר בחוק איסור הלבנת הון בסעיף 30), נתוני צריכת חשמל, נתוני נסיעה בתחבורה ציבורית ועוד. תחת חוק זה תוסדר גם העברת מידע מהעיריות השונות למשטרת ישראל בנוגע לתכנים שנקלטו במצלמות העירוניות ברחובות, בכבישים, על גבי רחפנים וממצלמות הגוף של פקחים. השגת נתונים מרשתות חברתיות וחדירה לתוכן המצוי בספרה הפרטית הווירטואלית, בפרופילים פרטיים, אשר תיעשה בפנייה לספק או בעל פלטפורמה, תוסדר תחת חוק נתוני תקשורת החדש ולשם כך יידרשו לצו משופט.

לגישתי, ראוי להסדיר את כל סוגי הנתונים תחת חוק אחד לשם איחוד נהלים על מנת שבכל המקרים הללו תידרש משטרת ישראל לצו שופט, ולא תתאפשר העברת מידע בפנייה ישירה לגופים

---

[409] ס׳ 23,43 לפסד״פ מעצר וחיפוש.
[410] מסמך איגוד האינטרנט, לעיל ה״ש 4, בעמ׳ 61.
[411] שם, בעמ׳ 63.

השונים. ראוי להסדיר את כל סוגי הנתונים תחת חוק אחד על מנת להתייחס לקטגוריות מידע חדשות שעדיין לא הוסדרו על ידי המחוקק.

אופן הגשת צו בקשה לשופט: לשם איחוד נוהלי בקשת צו משופט, ראוי כי כל הפניות ייעשו לשופט שלום. הנוהל של קבלת צו משופט בחוק זה יהיה זהה לחוק שמסדיר התקנת אמצעי מעקב מרוחקים במרחב הפרטי. זאת על מנת שלמשטרת ישראל לא יהיה תמריץ לעקוף מסלול אחד באמצעות מסלול אחר מקל יותר. יש להשוות את רמת הפיקוח בנוגע לכל האמצעים הקיימים.

חוק מצלמות מיוחדות יהפוך ל"חוק המסדיר איסוף מידע באמצעים טכנולוגיים שבשליטת המשטרה ממרחבים ציבוריים": מלבד תמונות ווידאו שהוסדרו כבר בחוק, על המחוקק להתייחס להקלטות קול במרחב הציבורי. בחוק האזנות סתר נאמר כי אין צורך בבקשת צו להאזנה במרחב ציבורי במקום שבו אדם סביר יכול היה לצפות ששיחותיו יישמעו ללא הסכמתו אם ההאזנה נעשתה באקראי ובתום לב או בידי מי שהוסמך לכך לשם מניעת עבירות או גילוי עבריינים.[412] אך המצלמות אינן אדם שהוסמך לכך וההקלטות לא נעשות באקראי, אלא למטרה של גילוי פשיעה. כמו כן, לא בכל מקום במרחב הציבורי אדם נמצא תחת ההנחה כי המדינה מקליטה את שיחותיו. ראוי לטעמי לאפשר עיבוד קולי של ירי והמולה, אך לאסור הקלטת שיחות במרחב הציבורי. הדבר ייעשה בהאזנה תמידית של תוכנה למתרחש, וללא הקלטת הדברים. כאשר התוכנה תזהה קולות ירי או המולה תדווח על כך על מנת לסייע בהצלת חיי אדם. מאחר שלא תתבצע שמירה של ההאזנות תימנע פגיעה בפרטיות השיחות המתרחשות במרחב הציבורי. כל זאת בהנחה כי טכנולוגיית זיהוי קולות ירי יעילה באיתור ומניעת טרור ופשיעה. אם הטכנולוגיה אינה מספקת את אשר היא מבטיחה, נעדרת ההצדקה המאפשרת שימוש בה.

חדירה לתוכן המצוי בספרה הפרטית הווירטואלית בפרופילים פרטיים, שנעשית באמצעות התחזות לפרופיל מזויף, ראוי שתוסדר תחת החוק המוצע אשר יסדיר איסוף מידע באמצעים טכנולוגיים שבשליטת המשטרה ממרחבים ציבוריים. הליך זה מתאים לאמצעי פיקוח פנימיים, ולא לבקשת צו משופט, מאחר שאופן הפעלת שיקול הדעת של השוטר בהליך זה מורכב, ונדרש פיקוח ישיר ויום יומי עליו.

לשם שימוש בכלים טכנולוגיים שבשליטת המשטרה, ראוי להקים גוף מפקח. לשם קבלת נתונים ממערכות שבשליטת המשטרה נדרש אישור מפקח. כך יתאפשר מסלול אחיד להתמודדות עם כל הכלים הטכנולוגיים הקיימים והעתידיים. נדרשת הקמת גוף פיקוח עצמאי שיבקר את פעילות המעקב של משטרת ישראל, בעל סמכויות פיקוח, סמכויות חקירה ובירור וסמכויות ייעוץ והנחיה מקצועית. על המפקח להקפיד כי משטרת ישראל תשתמש בחלופות שפגיעתן בפרטיות פחותה ולהבטיח כי לא ייעשה שימוש במידע למעלה מן הנדרש.[413]

הקמת גוף מפקח נדרשת על מנת לאחד בין מאגרים שבשליטת המשטרה למאגרים בניהול גוף אחר בכל הקשור לביקורת שיפוטית. אם לא יקודם מערך פיקוח שכזה, הדבר יתמרץ את משטרת ישראל לפתח ולרכוש טכנולוגיות שיעקפו את הדרישה לצו שיפוטי לשם השגת חומרים ומידע המצויים

---

[412] ס' 8(1) לחוק האזנת סתר.

[413] את המלצות כהנא ושני לייעול והגברת הפיקוח על מעקב מקוון בישראל ראו כהנא ושני, לעיל ה"ש 69, בעמ' 15–16.

בידיים אחרות. כלומר, משטרת ישראל תשיג כלים שמאפשרים לה לאסוף ולשמור את המידע בעצמה.[414]

הצדקה נוספת לפיקוח הצמוד הנדרש על המידע המופק מהמצלמות היא התפתחות טכנולוגיית הזיוף העמוק (Deepfake). על מנת שניתן יהיה להוכיח בבית המשפט כי הצילומים אינם מזויפים, תידרש משטרת ישראל להקפיד על שלמות שרשרת הראיות, דבר אשר יושג באמצעות פיקוח על איסוף המידע ושמירתו. שקיפות הפעלת המערכות ופיקוח עליהן אף יגבירו את ההרתעה מפני עבריינות. בנוסף, פעולה בשקיפות תגביר את הלגיטימציה של השימוש בטכנולוגיות אלו לשם שיטור.[415]

כתוצאה מחקיקה זו ומהקמת גוף מפקח, שיטת השיטור היזום לא תיפגע ואף לא תוגבל. הפתרון המוצע יאפשר הפעלת כלים טכנולוגיים לשם מעקב לצורכי לחימה בפשיעה והגנה על חיי אדם תוך הקפדה על פגיעה מידתית. בנוסף, הפתרון המוצע יאפשר את הסמכת משטרת ישראל בחוק לשימוש בטכנולוגיה המתפתחת מבלי שהפיתוחים השונים בטכנולוגיה יהפכו את החקיקה למיושנת ויובילו לחריגה מסמכות. מטרת הפתרון המוצע היא הצבת חסמים בפני השלטון להשתמש בכלים הטכנולוגיים על מנת לשרת מאבקים פוליטיים ולשם הגנה על הדמוקרטיה.

ז.2. הסדרה בחוק של שלב ניתוח המידע: לגישתי ראוי לאסור שימוש בבינה מלאכותית לצורך ניבוי עבריינות, ובכלל זה: לאסור סיווג ביומטרי של אנשים על סמך תווי פניהם, טביעות אצבעותיהם או נתונים ביומטריים אחרים. כמו כן, ראוי לגישתי לאסור דירוג חברתי של אנשים על סמך נתונים אישיים, כגון הכנסה, השכלה או מקום מגורים. בהמשך לכך, ראוי לאסור הערכה אישיותית או התנהגות של פרטים והסקת מסקנות בנוגע לרגשות. לסיום, אני סבורה כי ראוי לאסור הערכת ביצוע עבירות פליליות על ידי אנשים המבוססת על פרופיילינג. איסורים אלו קבועים בחוק הבינה המלאכותית האירופי.[416] אני מחזיקה בעמדה זו מאחר שפעולות אלו הן בעלות פוטנציאל רב לפגיעה בזכויות אדם. לגישתי מדובר בטכנולוגיה שאינה מנבאת כרגע נטייה לעבריינות, אלא הבניה חברתית. לכן, נכון לעכשיו אין בה תועלת. בהמשך לכך, הנזק שנגרם מהשימוש בתוכנות אלו עולה על התועלת.

היכולות הטכנולוגיות של בינה מלאכותית בשיטת למידת מכונה עדיין מוגבלות. לכן, לא ראוי להסתמך עליהן באופן אוטומטי בתחום קבלת החלטות ממשלתיות באכיפת החוק. אם יותר שימוש במערכות בינה מלאכותית לשם קבלת החלטות משטרתיות, ראוי לחייב את משטרת ישראל להשתמש רק במערכות אשר יכולות להסביר ולנמק את החלטות הבינה המלאכותית למי שהכרעותיה משפיעות עליו.[417]

ז.3. כמה הערות כלליות לסיכום: לאור ההשלכות הנרחבות שיש לשימוש בכלים טכנולוגיים לשם מעקב משטרתי ושיטור מנבא על זכויות אדם ולאור העובדה כי מדובר בתופעה חדשה שהשפעותיה עדיין נלמדות, ראוי לאסוף נתונים ולבצע מחקרים בנוגע להשפעתה על מידתיות הפגיעה בזכויות

---

[414] הרפז וגולן, לעיל ה״ש 73, בעמ׳ 334, 337; כהנא 2023, לעיל ה״ש 84.

[415] המלצות האגודה למצלמות גוף, לעיל ה״ש 149.

[416] כהנא ושני, לעיל ה״ש 69, בעמ׳ 10–11.

[417] European Parliament and Council of the European Union, Regulation 2016/679 of April 27, 2016, On the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) (L 119).

אדם.[418] על כן, קמה חובה על המדינה לבדוק – האם הכלי המוצע לשימוש יעיל בהפחתת פשיעה? לשם כך נדרשת עריכת מחקר בטרם יותר שימוש כלשהו בטכנולוגיות אלו במערכת אכיפת החוק.[419]

איני מסתייגת משימוש בטכנולוגיה לטובת הפחתת פשיעה. איני סבורה כי ראוי להגביל את יכולות המשטרה לפעול, אלא שלגישתי ראוי שמשטרת ישראל תפעל בשקיפות ובהתאם לחוק. שימוש במאגרי מידע באופן חוקתי אינו מוביל בהכרח למגבלות שיפגעו ביעילות השיטור. כחלק מהיעילות יש לבחון את הפגיעה באוכלוסייה האזרחית. טכניקות של ניבוי עבריינות נפגעות ומוגבלות בשל היותן לקויות מלכתחילה, ולא בשל הדרישה כי המדינה תפקח על כך שמשטרת ישראל לא תשתמש בטכנולוגיות לקויות. מנגנון מפקח על פעולות משטרת ישראל בתחום המעקב אחר האוכלוסייה יוביל להפחתה בפשיעה ולהגנה על חיי אדם גם בטווח הארוך. בנוסף, הוא יאפשר הקפדה על ערכיה הדמוקרטיים של המדינה ועל מידתיות הפגיעה בזכות לפרטיות, אשר בתורה מאפשרת את הדמוקרטיה.

לבסוף, ניתן ליישם את עקרון ההתמקדות בתוצאה ולא בתהליך לשם הסדרת תחומים טכנולוגיים נוספים. העיקרון של התמקדות בתוצאה ולא בתהליך יכול לשמש ככלי בידי מחוקקים ומפקחים כאחד, ביישום רגולציה על תחומים טכנולוגיים נוספים. במקום לנסות ולהגדיר מראש את הכלים הטכנולוגיים הספציפיים שעשויים להיווצר, המחוקק יוכל להגדיר את המטרות והערכים המבוקשים, כגון: הגנה על הזכות לפרטיות ושקיפות. מאפיין זה יאפשר גמישות חקיקתית המותאמת לשינויים טכנולוגיים מהירים, תוך כדי שמירה על העקרונות הבסיסיים של המשפט. כמו כן, גישה זו תייתר את הצורך בתיקוני חקיקה תכופים, שכן המחוקק מתקשה לעמוד בקצב החדשנות הטכנולוגית. המעבר לגישה רגולטורית המבוססת על תוצאות יכול לסייע לחברה להתמודד עם אתגרים אתיים וחברתיים שנובעים מטכנולוגיות חדשות, בעודו מקדם חדשנות ופיתוח טכנולוגי.

סיכום

במאמר זה דנתי בשימוש משטרתי באמצעים טכנולוגיים שונים לשם מעקב ושיטור מנבא, כגון: מערכות מצלמות מיוחדות לזיהוי לוחיות רישוי, זיהוי תווי פנים, זיהוי אירועי אלימות וזיהוי אירועים חריגים, כריית מידע מרשתות חברתיות, שימוש בתוכנות רוגלה במחשבים ובטלפונים ניידים, השגת נתוני מיקום באמצעות איכון טלפונים, מערכת "עין הנץ" ותוכנות רוגלה, ביצוע האזנות סתר וניתוח מידע באמצעות בינה מלאכותית.

העלייה בשימוש באמצעי מעקב משטרתי חלה בשל המעבר ממודל שיטור קלסי למודל שיטור יזום, אשר הוביל להישענות על תאוריות קרימינולוגיות, כגון: תאוריית המניעה המצבית ותאוריית הבחירה הרציונלית והתמקדות בהגברת מאמצי העבריין לשם מניעת פשיעה מראש. בהמשך לכך, ניכר כי התפתחות הטכנולוגיה תרמה לעלייה במעקבים משטרתיים, זאת בשל כמה סיבות: עיתות משבר, שיטור טרור, עלייה ביכולת הטכנולוגית, ירידה בעלות הפעלת הטכנולוגיה, זמינותה הגוברת וקלות השימוש בטכנולוגיה.

418 המלצות האגודה למצלמות גוף, לעיל ה"ש 149.
419 שם.

ניכרת פגיעה בזכות לפרטיות בשלושת שלבי המעקב – בשלב איסוף המידע, בשלב שמירת המידע ובשלב ניתוח המידע. בשלב איסוף המידע, נאסף מידע אישי רב על אנשים ללא ידיעתם או הסכמתם. כמו כן, נאסף מידע מיותר שאינו רלוונטי למטרה שלשמה הוא נאסף. בשלב שמירת המידע, מידע אישי מאוחסן למשך זמן ארוך ללא צורך. בנוסף, גורמים לא מורשים עשויים לקבל גישה למידע. כמו כן, אבטחת מידע לקויה עלולה להוביל לדליפות מידע. בשלב ניתוח המידע, נעשה שימוש במידע אישי למטרות שאינן ידועות לאדם. נוצרים פרופילים אישיים על סמך מידע אישי. מתקבלות החלטות גורליות על סמך מידע אישי ללא שיתוף האדם. הפגיעה בפרטיות חמורה במיוחד במקרים שבהם מידע אישי נאסף במרחב הפרטי או כאשר נאספים נתונים בנוגע למחשבותיו של אדם.

הפגיעה בזכויות חוקתיות מתאפשרת רק בהסמכה מפורשת בחוק של משטרת ישראל להשתמש בכלים טכנולוגיים למעקב ושיטור מנבא. במאמר זה בחנתי האם דרישה זו מתמלאת. בהמשך לכך, בחנתי האם ההסמכה מתייחסת לכל סוגי המידע, למקום איסוף המידע, סיווג המידע כפרטי או ציבורי ולכל הדרכים שבהן ניתן להשיג מידע זה לאורך שלבי ההליך (איסוף, שמירה וניתוח המידע).

לטענתי המצב המשפטי הקיים אינו מסדיר כראוי את השימוש המשטרתי באמצעי מעקב טכנולוגיים ובכלים לניתוח מידע לשם יישום פרקטיקות של שיטור מנבא. הסוגים השונים של היעדר הסדרה חוקית מתאימה הם: היעדר הסמכה בחוק; הסמכה המתפצלת על פני כמה חוקים המקיימים נהלים שונים; שימוש בכלים טכנולוגיים שעוקפים מנגנוני פיקוח שיפוטי; היעדר התייחסות לקטגוריות חדשות של נתונים; והסמכה חלקית ומיושנת.

בהמשך נבחנה מידתיות הפגיעה בזכות לפרטיות ובוצע איזון אופקי בין זכות זו לזכות האזרחים לשמירה על חייהם וביטחונם. טענתי כי שימוש בטכנולוגיית בינה מלאכותית לניבוי עבריינות הוא בעייתי ולא עומד במבחני המידתיות. בנוסף טענתי כי יש להקפיד על שימוש מידתי בטכנולוגיות מעקב. לשם כך נדרשות הקמת גוף מפקח והאחדת נוהלי הפיקוח כך שלא ניתן יהיה לעקוף מסלול השגת מידע אחד באמצעות מסלול אחר.

במאמר הוצעו עקרונות הסדרה כלליים שניתן ליישם גם בנוגע לטכנולוגיות מעקב ושיטור מנבא. טענתי כי ההסמכה בחוק צריכה להתמקד בסוג המידע שנאסף, ולא בכלי הטכנולוגי שבו משתמשת המשטרה, זאת בשל התפתחויות טכנולוגיות מהירות שמשאירות את החוק המיושן מאחוריהן, בקצב שהמחוקק מתקשה לעמוד בו. המיקוד בסוג המידע מאפשר האחדה של נוהלי הפיקוח המשפטיים בנוגע לכל הכלים הטכנולוגיים לאיסוף, שמירה וניתוח המידע. ניתן ליישם עיקרון זה לשם הסדרת תחומים טכנולוגיים נוספים.