השימוש בטכנולוגיות ביומטריות – היבטים נורמטיביים ומשפטיים

לימור עציוני

התפתחות הטכנולוגיה לזיהוי מגוון מאפיינים (פיזיים ונפשיים) והשימוש בטכנולוגיות ביומטריות הגיעו לרמת בשלות ותפוצה כזו, המחייבת בחינה והתייחסות משפטית ונורמטיבית מפורשת לכלל היבטיהם. הריצה חסרת המעצורים קדימה של חברות הטכנולוגיה בישראל ובעולם גורמת לכך שהיבטים אלה נותרים מאחור. מאמר זה בוחן את התפתחות השימוש בטכנולוגיות ביומטריות ואת ההיבטים האתיים והמשפטיים הנגזרים ממנו. לישראל יש עניין רב בפיתוח הכלכלי הנגזר מיישומים ביומטריים, ולכן מציע המאמר להוביל מהלך בין־לאומי שמטרתו יצירת דיון ערכי ומשפטי בשאלות החשובות העולות מתפוצת הטכנולוגיה הביומטרית. בדרך זו תוכל מדינת ישראל להמשיך ולהשפיע על נורמות שיתפתחו בעתיד בתחום זה.

מילות מפתח: ביומטריה, זיהוי פנים, פרטיות, מאגרי מידע

מבוא

בדצמבר 2018 פרסם העיתון הבריטי "גארדיאן" כתבה על שימוש באמצעים ביומטריים בהופעתה של הזמרת טיילור סוויפט, לרבות שימוש במצלמות נסתרות לזיהוי פנים במטרה להצליב את תמונות הקהל עם מאגר של תמונות מטרידנים (Stalkers) של הזמרת – מעריצים כפייתיים העלולים להוות בעיה ביטחונית למושא הערצתם. אין להקל ראש באתגרים הביטחוניים היוצרים מטרידנים אלה: לזמרת מספר מטרידנים מוכרים, שנגדם אף הוצאו צווי הרחקה, ואחד מהם אף

ד"ר לימור עציוני היא דקאנית בית הספר למשפטים במרכז האקדמי שערי מדע ומשפט וחוקרת בכירה בתוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.

איים עליה באונס וברצח. הבעיה היא שהשימוש במצלמות הנסתרות נעשה מבלי שהקהל ידע על קיומן ותפקידן.[1]

היו כמובן אירועים שקדמו להצבת המצלמות הנסתרות בהופעתה של טיילור סוויפט: באפריל 2019 פורסם שנער אמריקאי תובע את חברת "אפל" בעקבות מעצר שווא שלו שנגרם על ידי החברה, אשר הפעילה תוכנת זיהוי פנים בחנויותיה תוך פגיעה קשה בפרטיות הקונים.[2] האירוע החל אחרי ששוטרים עצרו את הצעיר בניו יורק בעקבות תלונה שהגישה חברת "אפל". הצעיר נעצר מכיוון שאדם אחר השתמש בתעודת הזהות שלו, שלא נשאה תמונה, ובפרטים נוספים שגנב מתוכה, כדי לבצע גניבות בחנויות החברה בניו ג'רזי, דלאוור ומנהטן. בעקבות הגניבות עשתה החברה שימוש בפרטי זהותו שהיו ידועים לה, כדי לאתר את תמונתו ולהשוות אותה עם מערכות זיהוי הפנים המותקנות בחנויותיה. הזיהוי הביא להגשת תלונה נגדו במשטרה. לשוטרים התברר כי העצור הינו קורבן לתרמית וכי אינו הגנב האמיתי. בתביעתו של הנער נגד החברה הועלתה הטענה שהקישור שעשתה "אפל" בין פרטים שנגנבו ובין זהותו האמיתית, כולל תמונת פנים שלו שהוזנה למערכות האבטחה של החנויות, פוגע בזכויות יסוד שלו מבלי שלחברה יש סמכות לכך. בעקבות הגשת התביעה התעורר ויכוח בין מומחי משפט בשאלה האם יש לתביעה בסיס איתן והאם חברת "אפל" עברה על החוק. היו אף מי שטענו שמדובר במימוש חזונו של ג'ורג' אורוול, כאשר חברת טכנולוגיה מסוגלת להפוך ל"אח הגדול" ולעקוב אחרי כל אדם.

טכנולוגיות ביומטריות לזיהוי פנים התפתחו מאוד בשנים האחרונות ומשמשות ארגוני ביטחון במגוון יישומים ביטחוניים, ביניהם זיהוי מַפגעים במקומות הומי אדם (תחנות רכבת, שדות תעופה וכדומה) על ידי השוואה למאגר נתונים ביומטריים קיים. טכנולוגיה זו משמשת גם לצורכי הכנסה יעילה ומהירה של קהל למתחמים גדולים.

מאמר זה בוחן את הדילמות האתיות והמשפטיות הנובעות מהתקדמות השימוש בטכנולוגיות ביומטריות במגוון יישומים, תוך בחינת ההיבטים השונים של המסגרת החוקית הקיימת. כבר עתה ברור כי התפתחות הטכנולוגיה הגיעה לרמת בשלות ותפוצה כזו, המחייבת בחינה והתייחסות משפטית ונורמטיבית מפורשת לכלל ההיבטים של השימוש בטכנולוגיות ביומטריות ובמאגרי מידע ביומטריים.

---

1 Laura Snapes, "Taylor Swift Used Facial Recognition Software to Detect Stalkers at LA Concert", *The Guardian*, December 13, 2018.

2 Bob Van Voris, "Apple Face-Recognition Blamed by N.Y. Teen for False Arrest", *Bloomberg*, April 23, 2019.

רקע תיאורטי

התקדמות טכנולוגיית הזיהוי הביומטרי הובילה וממשיכה להוביל מגוון יישומים רחב במרחב הפרטי, כמו גם במרחב הציבורי. מקומות עבודה רבים הם הראשונים לאמץ יישומים ביומטריים. אולם, למרות שטכנולוגיות ביומטריות מאפשרות למעסיקים לחסוך במשאבים ואף להגביר את האבטחה במקום העבודה, עובדים מהססים לעיתים קרובות לאפשר שימוש בנתונים אלה. זאת, משום שאיסוף ואחסון של נתונים ביומטריים של עובדים מעלים חששות לגבי שימוש נאות במידע האישי המצטבר.

דארל קרפנטר ועמיתיו[3] בחנו מספר היבטים של השימוש בטכנולוגיות ביומטריות בהקשר של פרטיות, וזאת בשלושה ממדים: הראשון נוגע לשאלה כיצד האחריות לפרטיות נתפסת על ידי העובדים; השני נוגע לתפיסת הפגיעות שהמערכות הביומטריות יוצרות; השלישי מתייחס לתפיסת חוסר האמון כלפי הארגון. במסגרת מחקרם הם בחנו את ההתפתחויות ביחסם של העובדים בארגון שהתקין מערכות ביומטריות. התוצאות הצביעו על כך ששיתוף עובדים בניסוח כללי השימוש במערכות אלו מילא תפקיד משמעותי בכל הקשור להקטנת החשש בנוגע לפגיעה בפרטיות, וזאת בכל שלושת הממדים.

מחקר אחר בחן היבטים הנוגעים לשימוש ביישומים ביומטריים במגזר הבריאות. החוקרים בחנו היבטים של שימוש בנתוני גנום בהקשר למחלות סרטן ומחלות נדירות, אשר התלוו לו שימושים משניים שעלולים היו לקבל תפוצה רחבה ביותר.[4] המחקר בחן עד כמה ניתן לקבל הסכמות לשימוש במידע ביומטרי פרטי (בהקשר זה, מידע הנוגע למיפוי הגנום האישי), והראה שמטופלים עשויים לבחור לאחסן חלק מהמידע שלהם, כגון מידע גנטי, באופן מקוון ולאפשר לאנשי מקצוע בתחום הבריאות לגשת אליו. המחקר נגע בצורך לוודא שבתהליך האחסון והשימוש של המידע הרגיש, כל מי שייגש אליו תאומת זהותו בצורה נכונה, וזאת כדי להגן על פרטיות המטופלים. המחקר הראה כי לאימות כזה יש שני תפקידים: מניעת התחזות, והוכחה של כוונת השימוש במידע – המהווים צעד חיוני להבטיח שמחקר רפואי וחילופי מידע בנושאי בריאות מתבצעים לשם מטרה ראויה מבחינה אתית.

---

3 Darrell Carpenter, Alexander McLeod, Chelsea Hicks and Michele Maasberg, "Privacy and Biometrics: An Empirical Examination of Employee Concerns", *Information Systems Frontiers*, Vol. 20, No. 1 (February 2018).

4 Atsushi Kogetsu, Soichi Ogishima and Kazuto Kato, "Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy and Trustworthiness", *Front Genet*, Vol. 9 (June 1, 2018).

אנטון אלתרמן בוחן היבטים אתיים בזיהוי ביומטרי.[5] טענתו היא שבזיהוי ביומטרי קיים אינטרס פרטי לצד אינטרס ציבורי, וכי שני אלה נדרשים לצורך האיזון; כך מתקיים מעין סחר חליפין בין הפרטי לציבורי בשימוש בטכנולוגיה ביומטרית לצורכי זיהוי. מסקנתו העיקרית היא שהזכות הכללית לפרטיות כוללת גם את הזכות לשלוט במידע שנאסף ובשימוש במרכיבים הביומטריים, וכי זכות זו חייבת להיות זכות גוברת. המשמעות מבחינתו היא שיש לנהוג בזהירות יתר ולשקול היטב את ההחלטה לאפשר גישה למידע ביומטרי אישי לגורמים אחרים. לדעתו, יש לשקול את הדברים לאור מספר היבטים: הפיכת מידע ביומטרי לזמין לאור אפשרות אובדן השליטה על המידע; אבטחת המידע; הסיכונים של שימוש לרעה במידע.

השימוש הגובר והולך בזיהוי ביומטרי מחייב את הפרט לבחון עד כמה הוא מוכן שנתוניו האישיים יועברו לגורמים אחרים בכדי לקבל שירות מהיר וטוב יותר. השאלה הנשאלת בהקשר זה היא עד כמה יש לַפרט יכולת לשלוט בשימוש שנעשה במידע הביומטרי עליו. אלתרמן מציע שכל מי שיתבקש לספק מידע ביומטרי יהיה בעל יכולת להבין את התוצאות ואת ההשפעה של העברתו, אל מול שיפור השירות הצפוי כתוצאה מזיהוי ביומטרי מהיר, וגם מודע לסיכונים הפוטנציאליים הכרוכים בכך.

בישראל הוקמה בשנת 2011 יחידה לפיתוח תחום היישומים הביומטריים במשרד ראש הממשלה. זאת בהמשך לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע התש"ע– 2009, הקובע כי ראש הממשלה ימנה "ממונה על יישומים ביומטריים". היחידה עברה בהמשך לאחריות מערך הסייבר הלאומי.[6] בישראל גם הוקם מאגר נתונים ביומטרי לאומי. המאגר הביומטרי הלאומי הוקם במטרה למנוע התחזות וגניבת זהויות. באתר האינטרנט של רשות המאגר הביומטרי הלאומי נכתב: "כיום, במצב הנוכחי, ואפילו במצב של תיעוד ביומטרי חכם אך ללא מאגר ביומטרי, יכול עדיין אדם להתחזות ולהנפיק בו־זמנית מספר תעודות בזהויות שונות. זאת, מפני שבהיעדר מאגר נתונים ביומטרי, לרשות האוכלוסין אין דרך לוודא שמבקש התעודה אינו מתחזה".[7] יש לזכור, בהקשר זה, כי צריך להבחין בין מערכת ביומטרית המאפשרת זיהוי המשווה נתונים של אדם למאגר רחב והמנסה לאתר את זהותו מתוך המאגר הזה (לדוגמה, זיהוי עבריין לפי טביעות אצבע, צילומים או נתוני DNA) ובין מערכת המאפשרת אימות זיהוי,

5 Anton Alterman, "'A Piece of Yourself': Ethical Issues in Biometric Identification", *Ethics and Information Technology*, Vol. 5 (2003).

6 אתר מערך הסייבר הלאומי, על היחידה להזדהות וליישומים ביומטריים, פורסם במאי 2018: https://www.gov.il/he/departments/news/bio_aboutbiometric.

7 אתר רשות המאגר הביומטרי הלאומי: https://www.gov.il/he/departments/general/target_goals.

תוך בחינת פרטים ביומטריים של אדם שנדגמו בעבר (לדוגמה, המעבר במסלול הדרכון הביומטרי בשדה התעופה).

ויכוח ער מתנהל סביב מכלול ההיבטים הנוגעים לשימוש ביישומים ביומטריים, ועוד יותר – באשר לעצם הקמתו של המאגר הביומטרי הלאומי. עומר טנא מראה במאמרו[8] עד כמה חוק המאגר הביומטרי בישראל יוצר סיכונים לפגיעה בזכות לפרטיות, כשזו לא נעשית לתכלית ראויה ההולמת את ערכיה של מדינת ישראל. לטענתו, מערכות ביומטריות מעוררות בעיות אתיות כתוצאה מאופן השימוש במידע, כאשר זה משלב אותו במערכות נוספות, כמו מצלמות אבטחה ומעקב. בדרך זו, המטרות הביטחוניות והאבטחתיות של המאגר עלולות לפגוע באופן לא מידתי בערכי יסוד, כמו פרטיות והזכות לאוטונומיה של אדם על גופו. התפתחות הטכנולוגיה נוגסת בזכות לפרטיות באופן קבוע ומתמשך: חברות הטכנולוגיה אוספות מידע רב על משתמשים ברשת האינטרנט דרך מנועי החיפוש, נתוני הגלישה, נתוני המיקום, קשרים ברשתות חברתיות ועוד. בצורה זו מתקיים זיהוי באמצעות מידע ביומטרי שאינו ניתן להכחשה. לטענתו של טנא, אף שלמערכות ביומטריות עשויה להיות השפעה חיובית על הזכות לפרטיות, לאור העובדה שהן מאפשרות זיהוי ואיתור תוך שימוש במידע מינימלי, עלולה להיות לשימוש זה גם השלכה שלילית על הזכות לפרטיות, כאשר זהותו של אדם תצומצם "לאוסף של נתונים ביומטריים".

ברשות לניהול המאגר הביומטרי בישראל הוחלט לאמץ קוד אתי.[9] בקוד נקבע שהרשות נושאת באחריות המעשית לעיבוד הנתונים הביומטריים, שמירתם, אבטחתם והנגשתם לשימוש על פי דין. כמו כן, הרשות מתחייבת לשמור על הפרטיות של בעלי הנתונים הביומטריים שבידיה ולמנוע כל שימוש בנתונים הביומטריים שלא על פי דין. עוד נקבע בקוד האתי שהרשות ועובדיה מבצעים כל פעילות במסגרת הפרויקט הביומטרי הלאומי בהתאם לתפיסה של שירות לטובת הכלל, שמירה על כבוד האדם ושמירה על זכויות האזרח בהתאם לעקרונות המשטר הדמוקרטי. קביעה נוספת של הקוד נוגעת לדרישה שהרשות תפעל על יסוד נתונים ביומטריים מינימליים, כאשר הדבר נדרש לעיצוב תעודות זהות ודרכונים אמינים, להגנה על הזהות האישית ולסיכול כל ניסיון לעשות שימוש מזויף בתעודות זהות ובדרכונים.

---

8 עומר טנא, "חוק המאגר הביומטרי: סיכונים והזדמנויות", **המשפט**, יז (2) תשע"ג–2013.

9 "הרשות לניהול המאגר הביומטרי – הקוד האתי", *מדינת ישראל, משרד הפנים, הרשות לניהול המאגר הביומטרי*, 2015. להרחבה על היבטים אתיים של זיהוי ביומטרי ראו: Annemarie Sprokkereef, Paul De Hert, "Ethical Practice in the Use of Biometric Identifiers within the EU", *Science and Policy*, 3(2007): 177-201; Emilio Mordini, Carlo Petrini, "Ethical and Social Implications of Biometric Identification Technology", *Annali dell'Istituto superiore di sanita*, 43 (2017): 5-11.

ישראל אינה לבדה בתחום זה; מדינות נוספות הקימו מאגרים ביומטריים: באפריל 2019 קיבל הפרלמנט האירופי החלטה להקים מאגר ביומטרי, העשוי להפוך למאגר הגדול בעולם.[10] מטרתו היא לאפשר בקרה ושליטה טובות יותר בגבולות מדינות האיחוד האירופי. המאגר הביומטרי האירופי, הידוע בשם Common Identity Repository (CIR), מיועד לאחסן כ־350 מיליון זהויות ולכלול פרטים רבים, בכללם: שמות, תאריכי לידה, מספרי דרכון ופרטי זיהוי אחרים, לצד פרטים ביומטריים כגון טביעות אצבעות וסריקות פנים. נתונים אלה יהיו זמינים לרשויות הגבול וגורמי האכיפה במדינות האיחוד. אף שהפרלמנט האירופי והמועצה האירופית הבטיחו "אמצעי הגנה נאותים" כדי להגן על זכותם של האנשים לפרטיות ולהסדיר גישה של גורמי האכיפה לנתונים, לא ברור עדיין על אילו אמצעי הגנה מדובר.

תקנות הפרטיות שאומצו באיחוד האירופי (GDPR) העמידו אתגר גם בפני הגורמים באיחוד העוסקים בביומטריה. ראול סנצ'ס־רֶיו ועמיתיו בחנו את השאלה כיצד ניתן לאמץ את הרגולציה האירופית בכל הקשור לשמירה של נתונים ביומטריים.[11] בעבודתם הם מתארים את האתגר וממליצים על סדרה של צעדים שנועדו להגן על רכישת מידע ביומטרי ושימוש בו. מדובר בהליך המבוסס על 11 שלבים, ביניהם: קביעת רמת הגנה לפי רגישות הנתונים; בנייה של סביבות עבודה מבודלות במטרה למזער את הסיכוי לגישה לא מורשית ואת הסיכויים להתקפה ישירה על הרשת; הקפדה על עבודה עם יישומים מקומיים במקום יישומים המבוססים על האינטרנט; מחיקה או הסרה של הנתונים לאחר גמר המחקר עליהם.

התפתחות השימוש ביישומים ביומטריים והיבטים משפטיים אתיים

קצב התפתחות השימוש ביישומים ביומטריים הינו גבוה מאוד. מאמר שפורסם בעיתון "ניו יורק טיימס" תיאר את הקלות שבה ניתן להקים מערכת לזיהוי פנים של אנשים במרחב הציבורי.[12] לפי המאמר, המחשבה שתנועה במרחב הציבורי מאפשרת שמירה על פרטיות הינה שגויה. כך, למשל, זיהוי הפנים המופעל ברשת המצלמות הקיימת ברוב הערים מהווה איום על הפרטיות. המאמר גם מראה את הקלות שבה ניתן לעקוב אחרי אנשים ללא ידיעתם: במהלך תשע שעות נאספו

10 Catalin Cimpanu, "EU Votes to Create Gigantic Biometrics Database", *zdnet*, April 22, 2019.

11 Raul Sanchez-Reillo, Ines Ortega-Fernandez, Wendy Ponce-Hernandez, Helga C. Quiros-Sandoval, "How to Implement EU Data Protection Regulation for R&D in Biometrics", *Computer Standards & Interfaces*, Vol. 61 (January 2019).

12 Sahil Chinoy, "We Built an 'Unbelievable' (but Legal) Facial Recognition Machine", *The New York Times*, April 16, 2019.

תמונות של אנשים באחד הגנים בעיר ניו יורק. התמונות הורצו דרך שירות זיהוי הפנים של חברת "אמזון", ומתוכן זיהתה המערכת פנים של 2,750 אנשים.

השימוש בטכנולוגיות זיהוי פנים הואץ עם שילוב הטכנולוגיה במצלמות CCTV רגילות המותקנות בקרנות רחוב, בחנויות ובבתי עסק. שימוש זה יוצר עולם שבו אזרחים מנוטרים באופן אינטנסיבי וקבוע.[13] בריטניה מובילה בהטמעת טכנולוגיה זו. במהלך עשרות השנים האחרונות הותקנו בבריטניה מיליוני מצלמות רחוב. התפתחות מערכות זיהוי ביומטריות מאפשרת כיום שימוש במצלמות אלו לזיהוי אנשים ולהקמת מערכות מעקב בעלויות זניחות. בפועל, אין מגבלה חוקית על פעולות אלו, והשימוש בטכנולוגיות זיהוי פנים נעשה כמעט ללא פיקוח. כך, אין כל מסגרת משפטית המסדירה את השימוש במצלמות המבוססות על טכנולוגיה של זיהוי פנים ואין כל מנגנון פיקוח על התקנת הטכנולוגיה והשימוש בה. כתוצאה מכך, לא נבחנת המידתיות של השימוש בכלים אלה, ואין איזון בין ערכי החירות והפרטיות ובין ערכי הביטחון.

השימוש שנעשה בבריטניה במצלמות CCTV נתקל בביקורת גוברת על היעדר כל דיון ציבורי סביב הטכנולוגיה המתפתחת או היעדר בסיס משפטי להפעלתה. בהקשר זה מועלות שאלות כבדות משקל, כמו החדירה לפרטיות האזרחים וההידרדרות לתופעות של "האח הגדול".[14] בדוח שפורסם בבריטניה במאי 2018[15] נטען שהשימוש בטכנולוגיה זו מהווה איום חסר תקדים על פרטיותם וחירותם של אזרחים ועלול אף לערער את הזכויות הבסיסיות שלהם במקומות ציבוריים. בדוח נטען כי משטרת המטרופולין בבריטניה סובלת מדיוק ירוד של שני אחוזים בלבד במערכת הזיהוי האוטומטי אותה היא מפעילה, וכי שיעור התרעות השווא מגיע ל־91 אחוזים, כלומר, אדם תמים מזוהה לעיתים קרובות כאדם מנוטר. האו"ם הצטרף לביקורת זו כשפרסם דוח שביקר את השימוש בזיהוי פנים במהלך הפגנה בדרום ויילס. בדוח, שנכתב על ידי ג'וזף קנטאצ'י, שמונה על ידי ארגון זכויות האדם של האו"ם לבחון את הנושא, נטען שההפגנה הייתה שקטה והשימוש בטכנולוגיה היה לא מידתי לאור רמת האיום שהיא הציבה על הביטחון הציבורי.[16]

---

13 להרחבה על פגיעה בפרטיות ומיגור פשיעה באמצעות מצלמות CCTV ראו: Andrei Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks and Mitigations", TrustED, 16 Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, 2016, pp. 45-54.

14 Michael Friedewald, Ronald J. Pohoryles, eds., *Privacy and Security in the Digital Age: Privacy in the Age of Super-Technologies* (Routledge, 2016).

15 "Face Off – The Lawless Growth of Facial Recognition in UK Policing", *Big Brother Watch*, May 2018.

16 Chris Burt, "UN Privacy Rapporteur Criticizes Accuracy and Proportionality of Wales Police Use of Facial Recognition", *Biometric*, July 3, 2018.

ניסיונות להתמודד עם נושא זה בישראל הובילו להקמת יחידה ליישומים ביומטריים במשרד ראש הממשלה, ובהמשך לחקיקת חוק המאגר הביומטרי שאושר במארס 2017.[17] אחת ממטרות החוק היא להתמודד עם הבעיות החמורות הקיימות בישראל בכל הנוגע למסמכי זיהוי, דוגמת דרכונים ותעודות זהות. החוק שם לו למטרה לקבוע הסדרים שיאפשרו אימות זהות וזיהוי של תושבי ישראל, תוך שימוש באמצעים ביומטריים ובנתונים ביומטריים שיופקו מהם. נתונים אלה ייכללו במסמכי הזיהוי ובמאגר ביומטרי מרכזי, באופן שיקשה מאוד על זיוף התיעוד, ניפוק תיעוד כפול לאותו אדם ושימוש בזהות גנובה. אחת הטענות נגד החוק הייתה שאיסוף נתונים ביומטריים אינו מסייע במיגור תופעת הזיוף, וכי לכל היותר נתונים אלה יוכלו לסייע בשלב אימות זהותו של בעל התעודה. עוד נטען כי ניתן היה להסתפק ביצירה של תעודות אותן יהיה קשה לזייף.[18]

באשר לשימוש במצלמות במרחב הציבורי בישראל, עוד בשנת 2012 פרסמה הרשות להגנת הפרטיות מסמך הדן בשימוש במצלמות במרחב הציבורי ובמידע הנאגר בהן.[19] זאת, מתוך הבנת הפוטנציאל הבעייתי של הדבר, הנובע מהתרחבות השימוש במערכות במעגל סגור למגוון צרכים, ובהם: מניעת עבירות, הכְוונת תנועה ואיסוף מידע חזותי אחר. התפתחות נוספת בנושא זה נרשמה בישראל בעקבות יישום התוכנית "עיר ללא אלימות" ולנוכח היוזמה המשטרתית לצייד שוטרים במצלמות לבישות. בהמשך למסמך ההנחיה הראשוני, ולאור התפתחות הטכנולוגיה והאתגרים שהיא מציבה, פרסמה הרשות להגנת הפרטיות בשנת 2017 טיוטה מעודכנת של ההנחיה כדי לקבל עליה את הערות הציבור.[20] מטרת ההנחיה הייתה להבהיר את עמדת רשם מאגרי המידע ביחס לתחולת הוראות חוק הגנת הפרטיות התשמ"א–1981 על שימוש במצלמות מעקב במרחב הציבורי, במיוחד במקרים שבהם הצילומים הנקלטים בהן נאגרים במאגרי מידע.

טיוטת ההנחיה החדשה כוללת התייחסות למגוון היבטים, בהם: דרישה שהשימוש במצלמות במרחב הציבורי יעמוד בתבחינים של תכלית ראויה ומידתיות ולאחר בחינת חלופות פוגעניות פחות; דרישה שלפני התקנת המערכות ייבחן היקף חשיפת הציבור להן וייעשה הדרוש כדי למזער חשיפה זו ככל האפשר; איסור שימוש במצלמות ובמידע הנקלט בהן למטרות אחרות זולת התכלית שלשמה הותקנו, בתנאי שהתועלת מהשימוש במצלמות תגבר על הפגיעה בפרטיות שתיגרם בעטיין.

---

17 לדיון מעמיק ביתרונות ובחסרונות של המאגר הביומטרי ראו: קרין נהון, "קול פרטי: הפוליטיקה של המאגר הביומטרי", **משפט, חברה ותרבות**, ב 9, 2019, עמ' 271.

18 טנא, "חוק המאגר הביומטרי".

19 "הנחיית רשם מאגרי מידע מס' 4/2012 – שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן", *משרד המשפטים, הרשות להגנת הפרטיות*, 21 באוקטובר 2012.

20 "שימוש במצלמות מעקב ובמאגרי הצילומים הנקלטים בהן", *משרד המשפטים, הרשות להגנת הפרטיות*, 11 בספטמבר 2017.

עוד נקבע בהנחיה שהתקנת מצלמות באזורי קטינים תחייב הסכמה מפורשת של ההורים. ההנחיה גם מחילה מגבלות באשר למיקום המצלמות ומספרן. כך נדרש בה למקם את המצלמות רק במרחב הרלוונטי ולמנוע צילום ואגירת נתונים ממרחבים שאינם במסגרת התכלית האמורה.

בנוסף, חוק הגנת הפרטיות מקנה למצולמים זכות לעיין בהקלטות הנוגעות אליהם. החוק ותקנות הגנת הפרטיות (אבטחת מידע) התשע"ז–2017 מחייבים לאבטח את המידע הנקלט ונאגר במערכות המצלמות. ההנחיה מ־2017 מתייחסת במפורט להיבטי זיהוי ביומטרי והשוואה עם מאגרי מידע, אולם נעדרת התייחסות מפורשת למגבלות של טכנולוגיה זו ולהשפעתן על חירות האזרח ופרטיותו.

מהנדסים ומומחי אלגוריתמיקה נשענים לעיתים נדירות על מחקרים חברתיים. תופעה דומה מתרחשת גם בכיוון ההפוך. כך נתפסים יישומים ביומטריים כ"קופסה שחורה" ומסתורית וכמחזיקים מידע חד־ערכי על אנשים ונהלים, תהליכי אימות זהות, השוואה והתאמה. השילוב של חישובים מתמטיים עם נתונים ביולוגיים מעניק לכאורה לגיטימציה טכנית ומדעית־אובייקטיבית לתחום היישומים הביומטריים. יש לזכור בהקשר זה שטכנולוגיות ביומטריות מעורבות יותר ויותר בקבלת החלטות אוטומטית, ללא התערבות אנושית. כתוצאה מכך, גדֵלה הדילמה האתית באשר למיון חברתי העלול ליצור אפליה הנשענת על מאפיינים ביולוגיים חיצוניים.

סיכום

התפתחות הטכנולוגיה הגיעה לרמת בשלות ותפוצה כזו, המחייבת בחינה והתייחסות משפטית ונורמטיבית מפורשת לכל היבטי השימוש בה, ובכלל זה בטכנולוגיות ביומטריות לזיהוי מגוון מאפיינים (פיזיים ונפשיים). הריצה חסרת המעצורים קדימה, בה נמצאות חברות הטכנולוגיה בישראל ובעולם, גורמת להיבטים אלה להיוותר מאחור. לישראל עניין רב בפיתוח הכלכלי הנגזר מיישומים ביומטריים, ולכן טוב יהיה אם הגורמים הממשלתיים הרלוונטיים (משרד המשפטים, הרשות להגנת הפרטיות) יובילו מהלך בין־לאומי שמטרתו פיתוח דיון ערכי ומשפטי בשאלות החשובות העולות לאור תפוצת הטכנולוגיה בכלל והטכנולוגיה הביומטרית בפרט. בדרך זו תוכל מדינת ישראל להמשיך ולהשפיע על נורמות שיתפתחו בעתיד בתחום זה.

בעבר, הטכנולוגיה הביומטרית הייתה תחומה לצורכי ביטחון ואכיפה, אולם המצב כיום שונה. השימוש ביישומים ביומטריים גובר הן במגזר האזרחי והן במגזר המסחרי. התפוצה הנרחבת של יישומים ביומטריים מקנה חשיבות ממעלה ראשונה לטיפול בבעיות האתיות הטמונות בפיתוח טכנולוגיה בעלת תפוצה רחבה ופריסתה. מוטלת עלינו חובה לחקור ולפתח את הידע בדבר ההשלכות האתיות והמשפטיות של מצב זה על ארגונים אזרחיים ועיסקיים. נושא מפתח אותו יש לבחון במסגרת זו הוא שאלת הפרטיות.

למרות התפשטות הטכנולוגיה הביומטרית, יש מחקר אמפירי מועט על ביומטריה יישומית ואתיקה במגזר האזרחי והעיסקי. תהליך פיתוח הידע מחייב, לפיכך, תשומת לב גם לבחינת פוטנציאל הפגיעה והנזק העלולים להיגרם תוך כדי מעקב ביומטרי.

אין לראות בתחום הביומטריה פיתוח טכנולוגי גרידא. יש להעמיק בבחינת ההשלכות המשפטיות והאתיות שלו, כדי לגבש מסגרת חוקית ורגולטורית משוכללת שתוכל להתמודד עם מגוון האתגרים הצפוי בעתיד מכיוון זה.