



# השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי

כתיבה: רועי גולדשמידט | אישור: יובל וורגן  
תאריך: כ"ח בכסלו תשפ"א, 14 בדצמבר 2020

סקירה

## תוכן עניינים

1	תמצית	1
3	הקדמה	3
4	1. רקע טכנולוגי	4
4	1.1 טכנולוגיית זיהוי פנים	4
6	1.2 טכנולוגיות תמצות וידאו	6
7	1.3 טכנולוגיות זיהוי לוחיות רישוי (LPR ו-ALPR)	7
7	2. מידע אודות צילום, ניתוח וניטור בגופי הממשלה בישראל	7
8	2.1 מאגרים ביומטריים בממשלה והשימוש בטכנולוגיות ניטור	8
10	2.2 שאלת הצורך בהסדרה או בחקיקה ייעודית	10
12	2.3 דוגמאות לשימוש בניטור במסגרת תוכניות ממשלתיות	12
14	3. השימוש בטכנולוגיות ניטור ברשויות מקומיות	14
14	3.1 ירושלים	14
16	3.2 תל-אביב	16
17	3.3 פתח תקוה	17
18	3.4 ראשון לציון	18
18	4. אתגרים וסיכונים במערכות ניטור במרחב הציבורי	18
19	4.1 החשש מפגיעה בפרטיות ובחירויות אזרחיות נוספות	19
20	4.2 זליגת שימושים (Function Creep)	20
21	4.3 אפליה אלגוריתמית והחשש מטעויות מכונה	21

## תמצית

מסמך זה נכתב עבור ועדת המדע והטכנולוגיה של הכנסת, בראשות חה"כ עינב קאבלה, לקראת דיון בנושא **"הגנת הפרטיות והשלכות שונות של השימוש בטכנולוגיות זיהוי פנים במרחב הציבורי"**. הדיון נערך לציון היום הבינלאומי לזכויות אדם.

**יכולות ניתוח וידאו (Video Analytics)** מחליפות את הצופה האנושי, מאפשרות לתמצת צילומים של שעות ארוכות לכדי דקות בודדות של מידע תמציתי לפי מדדי חיפוש מרובים ומפורטים, בהם: מגדר, גיל, גזע, דפוסי לבוש, סוגי רכבים, צבע, מספר לוחית רישוי; לפענח התנהגויות של פרטים או קבוצות, ואנשים באמצעות זיהוי פנים ועוד. **זיהוי פנים** היא טכנולוגיה המאפשרת לאמת את זהותם של אנשים או לזהות אותם באמצעות צילום תווי הפנים שלהם. זיהוי פנים הוא חלק ממשפחה של טכנולוגיות ביומטריות, העושות שימוש במאפיינים פיזיים כגון: תווי פנים, קול, טביעת אצבע, רשתית ועוד, כדי לזהות אנשים באופן חד ערכי.

**בין השימושים המסחריים של טכנולוגיות זיהוי פנים בעולם ניתן לציין:** גישה למתקנים פיזיים או להתקנים דיגיטליים, אבטחה וביטחון בין השאר בבתי קזינו או אצל קמעונאים, תשלום באמצעות זיהוי פנים, זיהוי וניטור נוכחות עובדים או תלמידים, ניטור מגעים וזיהוי חולי קורונה, מיון וסידור תמונות ועוד.

**טכנולוגיות אלה מעוררת שאלות בדבר האיזונים בין התועלות שבהן לבין החשש מפגיעה בזכות לפרטיות ומיצירת מעקב מתמיד אחר אזרחים. יש החוששים כי יש להן אפקט מצנן על חירויות אזרחיות כמו חופש ביטוי, חופש דת, חופש התאגדות, חופש הפגנה ועוד.**

**בהכללה, מן המידע שקיבלנו נראה כי אין מדיניות כוללת וסדורה ביחס לפריסה של יכולות ניטור וניתוח וידאו.** רשויות מקומיות או משרדי ממשלה בוחרים ליישם טכנולוגיות ניטור תוך שרק בחלק מהמקרים הם מתייעצים עם גורמי המטה המומחים לנושא טרם ההטמעה או מבצעים הליך סדור הכולל היוועצות, כתיבה ופרסום של נוהל, עדכון ציבורי וכדומה. **היחידה להזדהות ויישומים ביומטריים במערך הסייבר מקיימת עבודת מטה לגיבוש קווים מנחים לשימוש מאוזן בטכנולוגיית זיהוי פנים במרחב הציבורי תוך התייחסות לשיקולים השונים.**

עוד עולה מן המידע, כי **השימוש במצלמות בכלל, ובטכנולוגיות זיהוי לוחית רישוי, נפוץ מאוד. השימוש בניתוח וידאו נפוץ פחות, אך קיים. אף גורם לא ציין כי נציגיו עושים כיום שימוש בטכנולוגיות זיהוי פנים.** נציין כי לצד משרדי ממשלה ורשויות מקומיות אשר השיבו בפירוט לבקשת המידע שלנו בנושא, כגון המשרד לחיזוק וקידום קהילתי ועיריית ירושלים, ישנם גופים אשר לא התקבל מהם כל מענה (רשות שדות התעופה) או שהתקבל מהם מענה כללי ביותר אשר אין בו את פירוט המידע המבוקש ואף נלוותה לו בקשה שלא לפרסמו בפומבי (משטרת ישראל, באמצעות המשרד לביטחון פנים).

לפי גורמי המטה אליהם פנינו אין חקיקה ספציפית המסדירה באופן קונקרטי מטרות לגיטימיות לשימוש בטכנולוגיות ניטור מתקדמות כגון זיהוי פנים.

לפי מידע שנתקבל מרשות הגנת הפרטיות, **במאי 2020 היו בישראל יותר מ-130 מאגרי מידע שנרשמו אצל רשם מאגרי המידע וכללו רכיבי ביומטריה כגון: תמונת פנים, טביעות אצבע, הקלטות קול ועוד.** יצוין כי כריית

מידע מאפשרת כיום ליצור מאגרי תמונות פנים או מאפיינים ביומטריים אחרים שימשו להשוואה בעת ניטור. כך כאשר אדם מנוטר במרחב הציבורי ניתן לזהותו באמצעות השוואה למאגר קיים.

**לפי דוח מבקר המדינה 70 ממאי 2020, מאגר תמונות רישיונות הנהיגה של משרד התחבורה משמש גופי ממשלה רבים** בהם: משטרת ישראל, משרד ראש הממשלה, המשרד לשוויון חברתי, המשרד לביטחון פנים, רשות המיסים ומצ"ח בצה"ל. **למרות שכבר בשנת 2005 המליץ המשנה ליועץ המשפטי לממשלה דאז להסדיר את השימוש במאגר בחקיקה ראשית, עד אוגוסט 2019 לא הוסדר הנושא.** שר התחבורה לשעבר, חה"כ סמוטריץ' החליט על ביטול מאגר תמונות רישיונות הנהיגה המצוי בידי משרד התחבורה וגורמי המקצוע בודקים את המשמעויות של החלטה זו והנגזרות שלה.

#### דוגמא לשימוש בניטור וידאו ופריסת מצלמות במעורבות גופי ממשלה

לפי תשובת המשרד לחיזוק וקידום קהילתי כחלק מהתוכנית לחיזוק הביטחון האישי במרחב הכפרי השתתף המשרד לביטחון פנים במימון התקנת מרכיבי ביטחון פיזיים וטכנולוגיים ב-17 מועצות אזוריות, **במטרה לשפר את התמודדות עם אירועי פשיעה חקלאית ופשיעת רכוש.** המשרד השתתף במימון התקנת מצלמות זיהוי **לוחית רישוי-LPR.** המצלמות הותקנו בכניסות למס' יישובים במועצות אזוריות שהפעילו את התוכנית. **סה"כ הוקמו במסגרת התוכנית כ-63 מצלמות LPR.** מאגר הצילומים מחובר למזכירות היישובים בהן הוצבו ונבדק מול מאגר הרכבים של תושבי היישוב בלבד. לפי נציג המשרד לחיזוק וקידום קהילתי בחלק מהיישובים חוברו המצלמות למערכת "עין הנץ" המשטרית לטובת פעילות המשטרה במסגרת סמכויותיה. ללא חיבור הרשויות למאגרי המידע המשטרתיים.

#### דוגמאות לשימוש בניטור וידאו ופריסת מצלמות ברשויות מקומיות

**ירושלים:** העירייה משתמשת בטכנולוגיית ניתוח וידאו לעיבודי תנועה או לזיהוי פעילות חריגה לטובת ניהול המרחב הציבורי ומערכת התחבורה. העירייה אינה עושה שימוש בעיבוד מידע ביומטרי ואינה עושה שימוש בזיהוי פנים במצלמות אבטחה. סך הכל בכל העיר יש כ-1,000 מצלמות. בידי העירייה מצויה טכנולוגיה של זיהוי לוחיות רישוי, ניתוח וידאו ברמה של חוקים (הגדרות לפעילות המערכת) המבוססים על פרמטרים קבועים כגון, כיוון תנועה, השתנות הרקע, כמויות של עצמים או אנשים, חציית קוים, ובנוסף לכך יכולת של זיהוי חריגים במרחב לאור למידת השיגרה.

**תל אביב:** לפי נציגת העירייה טכנולוגיות ניתוח וידאו הן הבסיס לעיר חכמה ועתידות לשמש כאמצעי מרכזי לניהול העיר. מאידך, אין לעירייה צורך בזיהוי של אדם במרחב הציבורי, ועל כן לא נעשה על ידיה כל שימוש בטכנולוגיות ניטור מתקדמות על אדם, כגון זיהוי פנים, זיהוי קול, לבוש, שפת גוף וכיו"ב. פיתוח המערכת ועיצוב המענה לצרכים נעשה על בסיס תפיסת Privacy by Design.

**מצלמות ביטחון:** כ-1,200 מצלמות הוצבו במרחב הציבורי והן מחוברות למשל"ט הביטחון העירוני. במצלמות אלה מופעלת אנליטיקה בסיסית של זיהוי תנועה במרחב נתון, בשעות חריגות וכד'. מצלמות ביטחון ללא אנליטיקה הותקנו גם במתקני עירייה ובמוסדותיה. הצבת המצלמות ופעילותן נעשית בהתאם לנוהל.

מסמך זה נכתב עבור ועדת המדע והטכנולוגיה של הכנסת, בראשות חה"כ עינב קאבלה, לקראת דיון בנושא "הגנת הפרטיות והשלכות שונות של השימוש בטכנולוגיות זיהוי פנים במרחב הציבורי". הדיון נערך לציון היום הבינלאומי לזכויות אדם. במסמך מוצג בקצרה מידע בנושא טכנולוגיות ניתוח תמונה; התייחסויות משרדי ממשלה רלבנטיים לנושא ומידע מכמה מהרשויות המקומיות הגדולות בישראל באשר לפריסת מצלמות ולשימוש שלהן בניתוח וידאו, ומידע על האתגרים והסיכונים בניטור במרחב הציבורי. מפאת היקפו של הנושא, המסמך איננו ממצה את כלל הנעשה בתחום זה.

## הקדמה

אנו חיים בעידן מתועד מתמיד. כמויות התוכן והנתונים שאנו יוצרים ושנאספים עלינו גדלות כל העת. "העקבות הדיגיטליים" שלנו לא מסתמנים רק במילים, בתמונות או בסרטונים שאנו יוצרים, מעלים ומשתפים עם אחרים באמצעות טלפונים חכמים ומחשבים, אלא גם במכשור "חכם" אחר כגון: רמקולים, טלוויזיות, מוני חשמל ומים ועוד. לא זו בלבד, אלא שהיקפי הצילום במרחב הציבורי גדלים גם הם כל העת, וכוללים מצלמות של טלפונים ניידים, מצלמות דרך של נהגים, מצלמות דרך של רשויות, מצלמות אבטחה נייחות שמציבות רשויות או עסקים פרטיים, צילום מרחפנים, מצלמות גוף של שוטרים, מצלמות משטרה ניידות ועוד.

לא רק היקף התייעוד גדל, אלא גדלה גם היכולת לנתח, לפענח ולהפיק תובנות עלינו באמצעות שימוש בהררי המידע והנתונים. אם פעם היתה מקובלת הטענה כי רק מעט מאוד מן התוכן המצולם, נצפה בפועל על ידי בנאדם ולכן הוטל ספק באשר להשלכות הצילום; הרי שהטכנולוגיות העכשוויות מאפשרות לנטר מקומות, התנהגויות ואנשים בצורה מקיפה, גם ללא מעורבות אנושית מלאה. תפקידו של "הצופה האנושי" בניתוח והסקת מסקנות מצטמצם ומשתנה.

החיבור של יכולות ניתוח תמונה ולמידת מכונה עם מגמות אוטומציה אחרות מתחומי הבינה המלאכותית מאפשר כבר כיום הפעלת מערכים אוטונומיים מלאים, תוך צמצום חלקו של הגורם האנושי. עם זאת, נראה כי פרקטיקות כאלה עדיין אינן נפוצות בזירה האזרחית אלא שכיחות יותר במערכים צבאיים או ביטחוניים גרידא.

נטען כי משטרים שמציבים את זכויות האדם נמוך בסדר יומם, מאמצים מערכים טכנולוגיים המשלבים את שלל הטכנולוגיות שהוזכרו לעיל כדי לשלוט בסדר החברתי.<sup>1</sup> אזרחים במדינות מסוימות, מצולמים ומקבלים דירוג לא רק בשל "עבירות קלות" הנעשות במרחב הציבורי ומתועדות במצלמות, אלא גם על בסיס דפוסי רכישה בחנויות, התנהגויות מקוונות, ועוד.<sup>2</sup>

הטכנולוגיות  
העכשוויות מאפשרות  
לנטר מקומות,  
התנהגויות ואנשים  
בצורה מקיפה, גם  
ללא מעורבות  
אנושית מלאה

<sup>1</sup> Steven Feldstein, "The Global Expansion of AI Surveillance", Carnegie Endowment for International Peace, September 2019.

<sup>2</sup> Liang et al., "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure", Policy & Internet, Vol. 10, No. 4, 2018.

**הזמינות הגוברת של טכנולוגיות ניתוח ומעקב מציעה מחד הזדמנות לייעול פעולות שיטור ושמירה על הסדר הציבורי; ומאידך מעוררת שאלות בדבר השלכותיהן על זכויות הפרט ועל אופיו של המרחב הציבורי.** חדירתן המדורגת של טכנולוגיות אלה גורם כפי הנראה לכך שלא תמיד נערך דיון ציבורי מקיף בשאלת האיזונים הרצויים בין זכויות וערכים שונים כחלק מהטמעתן של הטכנולוגיות האמורות במרחב הציבורי.

מסמך זה אינו עוסק במכלול הטכנולוגיות האמורות, אלא ממוקד בשאלות של: (1) השימוש; (2) הניתוח; (3) והאגירה של "צילומי וידאו" במרחב הציבורי על ידי רשויות מקומיות או גופי ממשל.

## 1. רקע טכנולוגי

השימוש במצלמות במרחב הציבורי בישראל ובעולם איננו תופעה חדשה. ועדת המדע והטכנולוגיה של הכנסת עסקה בנושא לפני כעשור ודנה בסוגיית פריסת המצלמות בערים, בבתי ספר ועוד.<sup>3</sup> עם זאת, כדרכה של טכנולוגיה, בעשור החולף היא התפתחה, מוצרים שהיו יקרים לשימוש הוזלו ובעיקר היכולת לנתח מידע מקבצי וידאו גדולים השתפרה משמעותית.

בעוד בעבר נסב הדיון על עצם התייעוד במרחב הציבורי, נראה כי כיום ניתן למקד אותו בשאלת האגירה והניתוח (אנליטיקה) של הצילומים. בעבר הרחוק דובר על מערכות "טלוויזיה במעגל סגור" (CCTV) או על תיעוד וידאו הנשמר על גבי קלטות, ובהמשך על דיגיטציה של המידע. בשנים האחרונות ניתן לדבר על **יכולות ניתוח וידאו (או Video Analytics) המחליפות את הצופה האנושי, ומאפשרות לתמצת צילומים של שעות ארוכות לכדי דקות בודדות של מידע תמציתי לפי מדדי חיפוש מרובים ומפורטים, בהם: מגדר, גיל, גזע, דפוסי לבוש, סוגי רכבים, צבע, מספר לוחית רישוי; לפענח התנהגויות של פרטים או קבוצות, ואנשים באמצעות זיהוי פנים ועוד.**

השימוש בביומטריה בכלל ובתמונות פנים בעשורים האחרונים כחלק מהשימוש במוצרים דיגיטליים כגון רשתות חברתיות, טלפונים חכמים ועוד, הפך את שפע המידע הביומטרי שלנו ובראשו תמונותינו לכר פורה לכרייה שלו על ידי שחקנים שונים. כריית המידע מאפשרת ליצור מאגרי תמונות פנים או מאפיינים ביומטריים אחרים (כגון קבצי קול) שישמשו להשוואה בעת ניטור. כך כאשר אדם מנוטר במרחב הציבורי ניתן לזהותו באמצעות השוואה למאגר קיים.

להלן יוצגו בקצרה כמה טכנולוגיות נבחרות: זיהוי פנים, תמצות וידאו, זיהוי לוחית רישוי (LPR).

### 1.1 טכנולוגיית זיהוי פנים

זיהוי פנים היא טכנולוגיה המאפשרת לאמת את זהותם של אנשים או לזהות אותם באמצעות צילום תווי הפנים שלהם. זיהוי פנים הוא חלק ממשפחה של טכנולוגיות ביומטריות, העושות שימוש במאפיינים פיזיים כגון: תווי פנים, קול, טביעת אצבע, רשתית ועוד, כדי לזהות אנשים

<sup>3</sup> ועדת המדע והטכנולוגיה של הכנסת, "שימוש במצלמות מעקב במרחב הציבורי", 6 בדצמבר 2011.

באופן חד ערכי. זיהוי פנים מבוסס על היכולת להפיק מצילום תבניות כגון מרחק בין העיניים, בין האוזניים וכדומה, כך שייצרו תבנית שמתאימה אך ורק למצולם, אותה ניתן להשוות לפנים (1-1) או לתמונות אחרות (one to many).<sup>4</sup>

בתמצית, טכנולוגיות זיהוי פנים כוללות את: (1) היכולת לזהות שהתמונה כוללת פנים; (2) **אימות זהות** (Verification): היכולת לוודא כי הזהות שייכת למי שמחזיק בה (לרוב באמצעות השוואה בין תווי הפנים לתמונת פנים); (3) **זיהוי** (Identification) היכולת לזהות אדם באמצעות השוואה בין צילום פנים שלו (כולל כזה המצולם בזמן אמת - LFR) לבין מאגר מידע הכולל תווי פנים של מספר רב של אנשים.

לפי מידע שנתקבל מהיחידה להזדהות ויישומים ביומטריים במערך הסייבר השימוש במערכות מורכבות לזיהוי פנים הולך ומתגבר בשנים האחרונות בין השאר: לצרכי אכיפה וסדר ציבורי בשדות תעופה, באירועי ספורט, ברשויות מקומיות, במגזר הפיננסי, במגזר הבריאות, בפרייקטים לאומיים להנפקת תיעוד, ועוד.<sup>5</sup>

בין הגורמים לעליית השימוש בזיהוי פנים: שיפור טכנולוגי משמעותי ברמת האמינות, קלות יחסית בהרכשה ובגישה לתיעוד המשמש להשוואה. דוח של מכון התקנים האמריקאי (NIST) מציין כי בעשור האחרון שיעורי השגיאה של מערכות אלגוריתמיקה לזיהוי פנים פחתו פי 100, מה שהדוח מכנה מהפיכה. עם זאת, מציינים נציגי מערך הסייבר, ביצוע זיהוי פנים במרחב הציבורי כאשר הצילום נעשה בתנאים סביבתיים שונים, רזולוציה משתנה ועוד, מורכב יותר מהשוואה של תמונות מבוקרות ושיעורי השגיאה בו גבוהים יותר.<sup>6</sup>

**לפי דוח של ה-GAO<sup>7</sup> בארה"ב בין השנים 2016-2019 גדלה ההכנסה משוק טכנולוגיות זיהוי הפנים בעולם מ-3 מיליארד דולר ל-5 מיליארד דולר. מספר הפטנטים שנרשמו אצל רשם הפטנטים בארצות הברית לטכנולוגיות הקשורות בזיהוי פנים גדל מ-631 בשנת 2015 ל-1,497 בשנת 2019.**

לפי דוח ה-GAO בין השימושים המסחריים של טכנולוגיות זיהוי פנים בעולם ניתן לציין:

✓ **גישה בטוחה:** טכנולוגיות זיהוי פנים משמשות כדי לאפשר גישה למתקנים פיזיים (דלת כניסה; אירוע וכו') או התקנים דיגיטליים כגון טלפון נייד, מחשב וכדומה או שירותים מקוונים - כתחליף או בנוסף לסיסמא.

<sup>4</sup> United States Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses", July 2020.

<sup>5</sup> יסמין ליבנה, ראש אגף מדיניות ותכנון, מערך הסייבר הלאומי, 25 ביוני 2020, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת. <sup>6</sup> שם.

<sup>7</sup> United States Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses", July 2020.

- ✓ **אבטחה וביטחון:** בתי עסק, קזינו, חנויות, מבני מגורים ועוד, משתמשים בטכנולוגיות זיהוי פנים למטרות ביטחון ואבטחה. כך לדוגמא, בתי קזינו עושים שימוש בטכנולוגיות כאלה כדי לזהות חברי ארגוני פשע או מי שחשוד בהונאות בתי הימורים. קמעונאים דיווחו גם הם על שימושים במערכות זיהוי פנים לשם מניעת גניבות.
- ✓ **זיהוי וסידור תמונות:** האפשרות למיין תמונות ולזהות אנשים משמשת ביישומי מדיה חברתית שונים כמו גם בכלים לתיוג תמונות המאפשרים גם חיפוש לפי אנשים.
- ✓ **תשלום באמצעות זיהוי פנים:** חברות שונות מציעות יישומים שמאפשרים לתת הרשאת תשלום באמצעות צילום פנים ובכך יקצר את תהליך ההזדהות מול ספק שירות התשלומים.
- ✓ **זיהוי וניטור נוכחות:** מוסדות לימודים מסתייעים במערכות זיהוי פנים כדי לזהות ולנטר נוכחות בכיתות וכן כדי לזהות משתתפים בשיעורים מרחוק ("אונליין").
- ✓ **ניטור מגעים וזיהוי חולי קורונה:** נטען כי מספר חברות וספקי בריאות מפתחים פתרונות שונים הכוללים שילוב של טכנולוגיות זיהוי פנים עם מצלמות תרמיות לזיהוי חום גוף או סימפטומים נוספים של וירוס הקורונה במטרה לאתר חולים או אנשים החשודים כחולים ואת מי שבא איתם במגע.
- ✓ **ספירת לקוחות וזיהוי דפוסי תנועה בחנות:** חברות מסוימות עושות שימוש ביכולות שאינן ממוקדות בזיהוי פרסונאלי אלא בזיהוי דפוסים כגון: מס' אנשים, אופן התנועה בחנות, משך הזמן שהם שוהים בכל מקום וכדומה, במטרה להבין את התנהגויות הצרכנים. חברות גם יכולות להשתמש בכלים כאלה כדי לזהות רגשות, גיל, מגדר וכדומה במטרה לספק פרסום ממוקד ללקוחות.
- ✓ **זיהוי רגשות, התנהגויות או חריגים במרחב.** בהקשרים ביטחוניים מקובל להשתמש בטכנולוגיות שונות המזהות דפוסים חריגים, כגון דפוסי תנועה שונים מהמקובל, ביגוד חריג או שאיננו תואם את מזג האוויר, התקהלות ועוד.

**כפי ששורחב בהמשך המסמך, טכנולוגיות אלה מעוררת שאלות בדבר האיזונים בין התועלות שבהן לבין החשש מפגיעה בזכות הפרטיות ומיצירת מעקב מתמיד אחר אזרחים. יש החוששים כי יש להן אפקט מצנן על חירויות אזרחיות כמו חופש ביטוי, חופש דת, חופש התאגדות, חופש הפגנה ועוד.**

## 1.2 טכנולוגיות תמצות וידאו

כאמור לעיל, בעוד בעבר היה צורך בצופה אנושי שיסרוק כמויות תוכן גדולות כדי לזהות פריטי מידע רלבנטיים, טכנולוגיות עיבוד וניתוח תמונה חדשות מאפשרות כיום לתמצת סרטים ארוכים לדקות ספורות, כך שכל קטע מתומצת ("פריים") יכול מידע שנאסף מקטעי וידאו רבים זה לצד זה וכן להגדיר פרמטרים לחיפוש (כגון: רוכב אופניים, הולך רגל, גבר, לובש בגד בצבע



כחול, נושא תיק ועוד, או אזורים בצילום עליהם טכנולוגיות מכילים כללים לחיפוש: "כל מי שחוצה את הכביש"; "כל מי שנוסע מעל מהירות א" וכדומה).

### 1.3 טכנולוגיות זיהוי לוחיות רישוי (LPR ו-ALPR)

טכנולוגיות זיהוי לוחיות רישוי (License plate Recognition) או זיהוי אוטומטי של לוחית רישוי (ALPR) מאפשרות לתעד או לקרוא מתוך קבצי תמונות ווידאו את פרטי לוחיות הרישוי של רכבים. בשל העובדה כי לוחית רישוי היא מזהה חד ערכי של כלי רכב, השימוש בטכנולוגיה זו יכול לאפשר לזהות כלי רכב, לתעד עבירות המבוצעות על ידי כלי הרכב או את מסלולי הנסיעה שלו, ככל שהם חולפים אל מול מצלמות בעלות יכולת כזו, או שהצילומים עוברים ניתוח כזה.

למרות שבהשוואה לזיהוי פנים, זיהוי לוחית רישוי נתפס כאיתור של מידע פחות פרטי או אינטימי, בין השאר כיוון שבחלק ניכר מכלי הרכב נעשה שימוש על ידי יותר מאדם אחד, הרי שהצלבת המידע ממצלמות LPR עם מאגרי מידע אחרים או אפילו עצם אגירתו, יוצרים למעשה מאגר מידע הכולל מידע מיקום של עוברי דרך רבים. במקרים בהן טכנולוגיות אלה מופעלות גם כלפי מי שלא עבר עבירה במהלך הנהיגה שלו, הרי שעל פניו ייתכן כי ניתן להטיל ספק באשר לעילת איסוף המידע.

**יצוין כי הצגת הדוגמאות של טכנולוגיות אלה והשימוש בהן, רחוקה מלמצות את כלל האפשרויות הקיימות והמפותחות בימים אלה (כגון זיהוי פנים גם בעת חבישת מסיכה). עם זאת, הצגה זו שבה ומדגישה את המעבר מעיסוק בעצם פרקטיקת הצילום במרחב הציבורי לשאלת הניתוח והניטור של מידע, הצורך בו, מידת הלגיטימיות שלו והסיכונים הטמונים בו.**

## 2. מידע אודות צילום, ניתוח וניטור בגופי הממשלה בישראל

מרכז המחקר והמידע של הכנסת החל לבחון את הנושא הנידון במאי 2020, טרם מיקוד הדיון בנושא "טכנולוגיות זיהוי פנים". בשל האמור כמו גם בשל העובדה כי טכנולוגיות זיהוי פנים הן חלק "ממשפחה" של טכנולוגיות ניתוח תמונה ווידאו, המידע שלהלן לא מתייחס אך ורק לשימושים בזיהוי פנים אלא גם לטכנולוגיות נוספות ומרכיבים רלבנטיים נוספים כגון מאגרים ביומטריים.

להלן יוצגו עיקרי המענה לפנייתנו שנתקבלו הן מגופי מטה שהנושא בכללותו באחריותם – כגון רשות הגנת הפרטיות במשרד המשפטים והיחידה להזדהות ויישומים ביומטריים במערך הסייבר, והן מגופים נוספים מהם ביקשנו מידע אודות שימוש בכלים כאלה. יצוין כי למרות פניות חוזרות ונשנות לרשות שדות התעופה בבקשה למידע על השימושים בטכנולוגיות ניתוח וניטור וידאו לא נתקבל מענה הרשות.

**בהכללה, מן המידע שקיבלנו ושיוצג בפירוט להלן נראה כי אין מדיניות כוללת וסדורה ביחס לפריסה של יכולות ניטור וניתוח וידאו. רשויות מקומיות או משרדי ממשלה בוחרים**

ליישם טכנולוגיות ניטור תוך שרק בחלק מהמקרים הם מתייעצים עם גורמי המטה המומחים לנושא טרם ההטמעה או מבצעים הליך סדור הכולל היועצות, כתיבה ופרסום של נוהל, עדכון ציבורי וכדומה. עוד עולה מן המידע, כי השימוש במצלמות בכלל, ובטכנולוגיות זיהוי לוחית רישוי, נפוץ מאוד. השימוש בניתוח וידאו נפוץ פחות, אך קיים. אף גורם לא ציין כי נציגיו עושים כיום שימוש בטכנולוגיות זיהוי פנים.

## 2.1 מאגרים ביומטריים בממשלה והשימוש בטכנולוגיות ניטור

למרות שנושא השימוש במאגרים ביומטריים איננו במוקד מסמך זה, הוא רלבנטי בשל העובדה כי מאגרים ביומטריים יכולים לשמש או משמשים בפועל לשם השוואה אל מול האדם עצמו, מול "תיעוד חי" שלו בצילום או מול צילומים ממקורות אחרים כחלק מניטור במרחב הציבורי או מהטמעת יישומים ביומטריים. בשל האמור, להיקף המאגרים, תנאי הגישה אליהם, אופן ההגנה עליהם ועוד, יש השלכות על האפשרות לעשות שימוש ביישומים ביומטריים כגון "זיהוי פנים", "זיהוי טביעות אצבע" ועוד.

איור 1. דוגמאות למאגרים ביומטריים בממשלה מתוך דוח מבקר המדינה 870ב

	רשות האוכלוסין וההגירה	מאגר עובדים זרים - מעו"ז	550,000 טביעות אצבעות ותמונות פנים
	רשות המאגר הביומטרי הלאומי *	תיעוד לאומי חכם - דרכונים ותעודות זהות	5.5 מיליון תמונות פנים 3.8 מיליון טביעות אצבעות
	שירות התעסוקה הישראלי	מערכת לזיהוי דורשי עבודה - התייצבומט	250,000 טביעות אצבעות
	משרד התחבורה והבטיחות בדרכים	מאגר תמונות רישיונות הנהיגה	4.5 מיליון תמונות פנים
	משטרת ישראל **	מאגר חשודים, נאשמים ומורשעים	1.3 מיליון טביעות אצבעות 960,000 תמונות פנים 450,000 דגימות DNA
	רשות שדות התעופה	מעבר גבול אוטומטי - זיהוי גב כף יד	1.3 מיליון תמונות גב כף יד
	שירות בתי הסוהר	מערכת זיהוי קולי לשיחות טלפון - שחף	5,500 דגימות קול
	צה"ל **	מאגר לזיהוי חללים, נפגעים ונעדרים	2.5 מיליון טביעות אצבעות 1.1 מיליון דגימות DNA

על פי נתונים שנאספו במהלך הביקורת, בעיבוד משרד מבקר המדינה.

<sup>8</sup> דוח מבקר המדינה 870ב', "היבטים בהסדרת השימוש במאגרים ביומטריים", מאי 2020, עמ' 13.

לפי תשובת הרשות להגנת הפרטיות במשרד המשפטים<sup>9</sup> **באשר לשאלה אילו גופי ממשלה עושים שימוש בטכנולוגיות ניטור מתקדמות כגון: זיהוי פנים, זיהוי קול; זיהוי דפוסי תנועה; לבוש; שפת גוף; זיהוי נתונים ועוד, השיב נציג הרשות כי ישנם מספר משרדי ממשלה העושים שימוש בטכנולוגיות ניטור מתקדמות, בהם:**

- **שירות בתי הסוהר** (זיהוי קולי),
- **רשות האוכלוסין** (טביעות אצבע ותמונת פנים של עובדים זרים),
- **לשכת התעסוקה** (טביעת אצבע מדורשי עבודה),
- **רשות שדות התעופה** (גב כף יד)
- **במערכת הביטחון ובמשטרה ישנם גם שימושים שונים בזיהוי פנים ובזיהוי לוחיות רישוי.**
- **התקנת מצלמות בבתי חולים סיעודיים** לשם מניעת פגיעה בחולים היא חובה (ע"פ תיקון לפקודת בריאות העם (מס' 33) התשע"ט - 2018. המערכת עושה שימוש במצלמות וידיאו לשם ניתוח תנועה.
- **רשות הטבע והגנים** מטמיעה מערכת מצלמות וידאו הכוללות ניתוח תנועה בחופים במסגרת פרויקט של חברת סייטביט.

לפי תשובת נציג הרשות, בחלק מהמקרים בהם מוטמעים יישומים מבוססי ביומטריה בממשלה נערכת היוועצות עם הרשות. בין השאר ביחס לנוהל שימוש בדגימות קול בשב"ס, השתתפות בצוות החשיבה ביחס לרכיב הביומטרי בתעודות הזהות החדשות, הנחיית רשם מאגרי מידע ביחס למפעילי כרטיס חכם בתחבורה הציבורית. עם זאת, לא בכל המקרים הרשות מעורבת.<sup>10</sup> נציגת מערך הסייבר השיבה לפנייתנו כי אין ליחידה להזדהות ויישומים ביומטריים נתונים על כלל הגופים וסוגי המידע הביומטרי המצויים ברשותם. עם זאת, יש ברשות המערך מידע על חלק מן המאגרים הביומטריים הגדולים המוחזקים בידי גופים ממשלתיים וציבוריים כגון: רשות האוכלוסין, שירות התעסוקה, משרד התחבורה, שב"ס ועוד (כמפורט לעיל).<sup>11</sup>

**יצוין כי לפי דוח מבקר המדינה 70 ממאי 2020, מאגר תמונות רישיונות הנהיגה של משרד התחבורה משמש גופי ממשלה רבים** בהם: משטרת ישראל ומשרד ראש הממשלה המקבלים בתדירות יומית שיקוף מלא של המאגר; המשרד לשוויון חברתי, המשרד לביטחון פנים, רשות

<sup>9</sup> עו"ד עדן אברהם, עוזר ראשי, הרשות להגנת הפרטיות, משרד המשפטים, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 30 ביוני 2020.

<sup>10</sup> שם.

<sup>11</sup> יסמין ליבנה, ראש אגף מדיניות ותכנון, מערך הסייבר הלאומי, 25 ביוני 2020, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת.

המיסים ומצ"ח בצה"ל – המקבלים גישה בהיקפים קטנים יותר. **עוד יצוין, כי לפי דוח המבקר למרות שכבר בשנת 2005 המליץ המשנה ליועץ המשפטי לממשלה דאז להסדיר את השימוש במאגר בחקיקה ראשית, עד אוגוסט 2019 לא בוצעה הסדרה של הנושא.**<sup>12</sup> לפי תשובת נציגת משרד התחבורה לפנייתנו<sup>13</sup>, שר התחבורה לשעבר, חה"כ סמוטריץ' החליט על ביטול מאגר תמונות רישיונות הנהיגה המצוי בידי משרד התחבורה וגורמי המקצוע בודקים את המשמעויות של החלטה זו והנגזרות שלה.

**באשר לשימוש בטכנולוגיות ניטור מתקדם במגזר הפרטי** השיב נציג הרשות להגנת הפרטיות כי קיימים שימושים בטביעות אצבע במערכות נוכחות של עובדים. הזדהות ותשלום לשירותים מקוונים באמצעות טביעת אצבע או זיהוי פנים, ומערכות זיהוי לוחית רישוי בחניונים. **יצוין כי לפי מידע שנתקבל מרשות הגנת הפרטיות היו במאי 2020 יותר מ-130 מאגרי מידע שנרשמו אצל רשם מאגרי מידע וכללו רכיבי ביומטריה כגון: תמונת פנים, טביעות אצבע, הקלטות קול ועוד. מעיון ברשימה נראה כי חלק ניכר מן המאגרים הם מאגרי ניהול משאבי אנוש של גופים מסחריים.** יובהר, כי רשימה זו לא בהכרח כוללת את כלל המאגרים הביומטריים המצויים, אלא רק את אלה שביצעו רישום שלהם כנדרש לפי חוק.<sup>14</sup>

נציגת מערך הסייבר ציינה כי לא ידוע להם על שימוש בזיהוי פנים במרחב הציבורי על ידי המגזר הפרטי בישראל, אם כי קיים פוטנציאל לשימוש כזה.<sup>15</sup>

## 2.2 שאלת הצורך בהסדרה או בחקיקה ייעודית

לפי נציג הרשות להגנת הפרטיות אין חקיקה ספציפית המסדירה באופן קונקרטי מטרות לגיטימיות לשימוש בטכנולוגיות ניטור מתקדמות, מלבד חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, תש"ע-2009, והתקנות מכוחו. חוקי הגנת הפרטיות בישראל מבוססים על **עקרון ההסכמה** ולכן ניטור מתקדם שבוצע לאחר הסכמת נושא המידע הן לכאורה לגיטימיות. עם זאת, בתרחישים מסוימים על המפעיל של מערכות כאלה מוטלת אחריות מוגברת. כך לדוגמא במקרה של צילום במקום העבודה:

הנחיית רשם מאגרי מידע מס' 5/17 "שימוש במצלמות מעקב במקום העבודה ובמסגרת יחסי עבודה" מפרטת כי "הדרישה המוגברת המוטלת על המעסיק להגינות, מידתיות ושקיפות ביחס לאיסוף ועיבוד מידע אישי על העובדים, מחייבת אותו להקפיד הקפדה יתרה להשתמש בצילומים אך ורק למטרה הלגיטימית הברורה והספציפית אותה הביא באופן הולם וברור לידיעת העובדים. זאת מפני שהמידתיות והלגיטימיות של היקף המעקב, סוג מערכת הצילום המותקנת

<sup>12</sup> דוח מבקר המדינה 70 ב', "היבטים בהסדרת השימוש במאגרים ביומטריים", מאי 2020, עמ' 27-37.

<sup>13</sup> ענבר הרשקוביץ, משרד התחבורה, 4 ביוני 2020, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת.

<sup>14</sup> עו"ד עדן אברהם, עוזר ראשי, הרשות להגנת הפרטיות, משרד המשפטים, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 30 ביוני 2020.

<sup>15</sup> יסמין ליבנה, ראש אגף מדיניות ותכנון, מערך הסייבר הלאומי, 25 ביוני 2020, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת.

ומידת החודרנות שלה – נקבעות לפי חיוניות המטרה וחשיבות האינטרס עליו המצלמה מיועדת להגן." ההנחיה מבהירה בין השאר כי צילום בחדר השירותים או במלתחות העובדים הינה פעולה אשר יהיה קשה, אם בכלל ניתן, להצדיקה, ולכן אינה לגיטימית.

קריטריונים נוספים להגדרת מטרות לגיטימיות הם בין השאר: קיומה של הצדקה משמעותית - אינטרס לגיטימי משמעותי וכבד משקל, אשר התועלת מקידומו תהיה גדולה מספיק כדי לעלות על הנזק המוגבר לפרטיות ולהצדיק אותו.

המידתיות והלגיטימיות של ניטור תיבחן ביתר שאת ביחס לאיסוף מידע על קטין, שלא לטובתו; ניטור לצרכי פרסום או מכירת מידע שניתנה למונופול המספק מצרך חיוני או כאשר מפעיל טכנולוגיית הניטור הוא גוף ציבורי או גוף אחר המבקש להסתמך על הגנת תום הלב בסעיפים 18 ו-20 לחוק הגנת הפרטיות.

**לפי תשובת הרשות, נציגיה טרם גיבשו עמדת רשמית ביחס לשאלה האם נדרשת חקיקה או הסדרים ספציפיים לנושא של טכנולוגיות ניטור ומעקב מבוסס יישומים מתקדמים.** זאת מאחר שקיימים סוגים שונים של נתונים מזהים וטכנולוגיות שונות שרמת הרגישות שלהן מבחינת פגיעה בפרטיות או שיקולי אבטחת המידע שלהם שונים (עד כמה המידע האמור זמין במרחב הציבורי – תמונה; או מחייב גישה פיזית לאדם- טביעת אצבע; האם הנתון עצמו הוא מידע רגיש – DNA או רק מפתח לגישה למידע ועוד) ולכן יש קושי לתחום אותם תחת מסגרת משפטית אחת.<sup>16</sup>

עו"ד דן אור-חוף חבר **המועצה להגנת הפרטיות** ציין במענה לפנייתנו למועצה כי יש חובה ליישם אמצעים טכנולוגיים מצמצמי פגיעה, מגבלות שימוש ובקרה חיצונית על גופים ציבוריים המשתמשים ביכולת הזו. לטענתו, לשקיפות יש תפקיד משני - יותר כמפחית חרדה ופחות כמחולל שליטת הפרט במידע עליו.<sup>17</sup>

**נציגת מערך הסייבר ציינה באשר לרגולציה ספציפית או חקיקה** כי לא מוכרת להם רגולציה ספציפית בנושא למעט הנחיות של מערך הסייבר ביחס להיבטי סייבר במצלמות אבטחה והנחיות של הרשות להגנת פרטיות ביחס למצלמות אבטחה ולשימוש ברחפנים, ולחוק המצלמות לשם הגנה על פעוטות במעונות יום לפעוטות, תשע"ט-2018, אשר לא ברור אם ניתן להגדירו כעוסק ב"מרחב הציבורי".<sup>18</sup>

עוד צוין בתשובה כי המדיניות הלאומית ליישומים ביומטריים כוללת קווים מנחים, בין השאר ביחס לתכנון המערכת לפרטיות, הפרדת מידע ביומטרי ממידע ביוגרפי והקישור בניהם, הצורך לצמצם את היקף האיסוף, העיבוד והשמירה של מידע ביומטרי וביוגרפי ועוד. באשר לשאלת

<sup>16</sup> עו"ד עדן אברהם, עוזר ראשי, הרשות להגנת הפרטיות, משרד המשפטים, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 30 ביוני 2020.

<sup>17</sup> עו"ד אורית פודמסקי, יו"ר המועצה להגנת הפרטיות, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 8 בדצמבר 2020.

<sup>18</sup> יסמין ליבנה, ראש אגף מדיניות ותכנון, מערך הסייבר הלאומי, 25 ביוני 2020, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת.

הצורך ברגולציה או חקיקה, צוין כי נושא זה יידון בשלב מאוחר יותר לאחר גיבוש הקווים המנחים (ראו להלן).

לפי תשובת מערך הסייבר, **היחידה להזדהות ויישומים ביומטריים מקיימת עבודת מטה לגיבוש "קווים מנחים" לשימוש מאוזן בטכנולוגיית זיהוי פנים במרחב הציבורי תוך התייחסות לשיקולים השונים**. בין היתרונות: שמירה על הסדר הציבורי, אכיפה, חקירה והרתעה מפני עבריינות; והחסרונות: חשש מפני מעקב, פגיעה בפרטיות והחשדת תמימים בשל טעויות בהטמעת מערכות מורכבות כאלה.<sup>19</sup>

**מהתשובות משתמע כי המרחב הרגולטורי פועל כיום על בסיס חוק כללי, וסדרה של הנחיות או המלצות שפרסמה רשות הגנת הפרטיות בנושאים שונים בתחום (כגון: הצבת מצלמות במרחב הציבורי, שימוש במצלמות במקום העבודה, היבטי פרטיות של השימוש ברחפנים ועוד).**

### 2.3 דוגמאות לשימוש בניטור במסגרת תוכניות ממשלתיות<sup>20</sup>

בשל העובדה כי תחת המשרד לחיזוק וקידום קהילתי מצויה הרשות למאבק באלימות, בסמים ובאלכוהול שהפעילה מערכי מצלמות כחלק מתכנית "עיר ללא אלימות" וכחלק מהתכנית למאבק באלימות, סמים ואלכוהול, פנינו אל המשרד לחיזוק וקידום קהילתי בבקשה למידע על השימוש של יחידות המשרד במצלמות וניטור.

לפי התשובה, המשרד לביטחון פנים, ומאז יוני 2020 המשרד לחיזוק וקידום קהילתי **השתתפו במימון, רכש והקמה של אמצעים טכנולוגיים לטובת איתור, מניעה ותחקור אירועי אלימות וונדליזם במרחב הציבורי**. הרכש והצבת המצלמות הוסדרו בנוהל מול משרד הפנים, משטרת ישראל ומשרד המשפטים. **בהתאם לנוהל המצלמות המוצבות ברשויות כחלק מהתוכניות האמורות הן מצלמות חוזי בלבד ללא יכולות מתקדמות של ניתוח וידאו**. המצלמות מוצבות על ידי הרשויות בהתאם לסמכויותיהן לפי פקודת העיריות ובתאום ובאישור משטרת ישראל.<sup>21</sup>

למרות שכאמור המצלמות אינן כוללות ניתוח וידאו, מציין נציג המשרד כי **חלק מן הרשויות רכשו באופן עצמאי מערכות ניתוח וידאו** (ניתוח תנועה או וידאו אנליטיקה) המסייעות להכוונת המוקדן הצופה במוקד. לטענת נציג המשרד, **הן אינן כוללות יכולות זיהוי ביומטרי כלשהן**.

בנוסף, בשנת 2017 ביצע המשרד לביטחון פנים **פיילוט בהובלת משטרת ישראל במסגרתו שולבו סנסורים (חיישנים) המזהים חריגה (אנומליה) ברעשים, במצלמות בשני פארקים**

<sup>19</sup> ש.ם.

<sup>20</sup> ישראל שטרית, ראש אגף בכיר אכיפה וביטחון אישי, המשרד לחיזוק וקידום קהילתי, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 6 באוגוסט, 2020, התקבל ממר דני שחר, ראש הרשות למאבק באלימות, סמים ואלכוהול

<sup>21</sup> ראו גם: חוזר המנהל הכללי 4/2018, "נוהל שימוש במצלמות וידאו לצורך אכיפת עבירות חניה ברשויות המקומיות" משרד הפנים.

**בעיר לוד.** החיישנים אינם מקליטים או מאפשרים האזנה לקולות. המידע נשמר בשרתי החברה שביצעה את הפיילוט ולפי נציג המשרד לא חלה התקדמות בנושא מאז ביצוע הפיילוט. עוד צוין כי כחלק מהתוכנית לחיזוק הביטחון האישי במרחב הכפרי השתתף המשרד לביטחון פנים במימון התקנת מרכיבי ביטחון פיזיים וטכנולוגיים ב-17 מועצות אזוריות, **במטרה לשפר את התמודדות עם אירועי פשיעה חקלאית ופשעת רכוש. המשרד השתתף במימון התקנת מצלמות זיהוי לוחית רישוי-LPR.** המצלמות הותקנו בכניסות למס' יישובים במועצות אזוריות שהפעילו את התוכנית. **סה"כ הוקמו במסגרת התוכנית כ-63 מצלמות LPR. מאגר הצילומים מחובר למזכירות היישובים בהן הוצבו ונבדק מול מאגר הרכבים של תושבי היישוב בלבד.**

**לפי נציג המשרד בחלק מהיישובים חוברו המצלמות למערכת "עין הנץ" המשטרית לטובת פעילות המשטרה במסגרת סמכויותיה. ללא חיבור הרשויות למאגרי המידע המשטרתיים.** תפיסת ההפעלה של מצלמות ה-LPR נבחנה על ידי הלשכה המשפטית של המשרד לביטחון פנים המעניק שירותי ייעוץ משפטי כרגע גם למשרד לחיזוק ולקידום קהילתי.

**יצוין כי המשרד לביטחון פנים מסר תשובה כללית וסרב להתייחס במפורש לדפוסי השימוש שלו במערכות ביומטריות בכלל ובמערכת "עין הנץ" בפרט** בטענה כי המידע נוגע לשיטות ואמצעים בהם עושה המשטרה שימוש לצורך מילוי תפקידיה. בפרסומים בתקשורת נטען כי המערכת המוצבת גם על גבי מצלמות ניידות בכבישים מתעדת מספרי לוחית רישוי ומשווה אותם אל מול מאגרי מידע שונים, ואף שומרת את המידע במאגר, גם כאשר לא נעשתה עבירת תעבורה כלשהי. עם זאת, כאמור, אין בידינו תשובה רשמית של המשרד או המשטרה המאפשרים לאמת טענות אלו.

יצוין גם כי לאחרונה שופט בית המשפט השלום בירושלים התייחס לנושא בפסיקה שלו, ומלבד תמיהה על הבחירה של המשטרה לשמור את דבר קיומה של המערכת האמורה כסוד ציין כי **"אין חולק כי אותה "מערכת" יכולה לשמש כלי אפקטיבי למאבק בפשיעה. אולם נראית בעיניי בעייתית העובדה שהשימוש בה נעשה עד כה ללא שהעניין הוסדר בחקיקה כלשהי."** השופט גם תמה **מדוע המשטרה לא הסדירה את השימוש במערכת בנוהל**, בדומה לנוהל שהפיצה ביחס לשימוש במצלמות גוף במשטרה וציין כי **העדר ההסדרה "מעלה חשש לפגיעה בזכויות יסוד"**.<sup>22</sup>

עוד יש לציין כי **לפי תשובת שירות בתי הסוהר, כיום אין בשב"ס שימוש בטכנולוגיות ניתוח וידאו לשם זיהוי ביומטרי, אך הנושא מצוי בבחינה ואם יאושר יש כוונה להתחיל להשתמש**

<sup>22</sup> פל (י-ם) 63-08-19 מדינת ישראל נ' דענא (פורסם בבנו).

בטכנולוגיות ניתוח וידאו וכן ניתוח מתקדם של זיהוי ביומטרי. בנוסף, במהלך שנת 2018 פרסם שב"ס מרכז להקמת תשתית ביומטרית לזיהוי טביעות אצבע אך מרכז זה בוטל בשל עלותו הגבוהה. כיום בוחן שב"ס בשנית את האפשרות להשתמש במאגר טביעות אצבע של משטרת ישראל ולהקים מאגר כלואים.<sup>23</sup> רשות הכבאות וההצלה ציינה במענה לפנייתנו כי היא אינה עושה שימוש בטכנולוגיות ניתוח וידאו וטכנולוגיות ביומטריות וכי השימוש במצלמות במסגרת עבודתה משמש לצרכי אבטחה ותחקור ואינו כולל אנליטיקה.<sup>24</sup>

### 3. השימוש בטכנולוגיות ניטור ברשויות מקומיות

פנינו אל חמש הרשויות המקומיות הגדולות בישראל. למעט עיריית חיפה, כולן השיבו לפנייתנו. להלן עיקרי המענה שלהן. אמנם המידע האמור אינו מספק מידע אודות הנעשה בכלל הערים, וייתכן כי אף אינו ממצה את הנעשה בערים הנסקרות, אך ניתן להניח כי ככלל ערים גדולות הן בעלות משאבים ואינטרס ניכר יותר להטמיע מערכות שליטה מרחוק דוגמת מצלמות וכלי ניטור מתקדמים. יצוין כי התשובות מתייחסות לפעילות של הרשויות עצמן בנושא וייתכן כי גופי ביטחון או שיטור מדינתיים עושים שימוש בטכנולוגיות הנידונות בתחומי הערים, ללא זיקה ישירה לרשות.

#### 3.1 ירושלים<sup>25</sup>

כאמור מרכז המחקר והמידע של הכנסת פנה אל עיריית ירושלים בבקשה למידע אודות שימושים בניתוח וידאו וטכנולוגיות ביומטריות הנעשים על ידי העירייה, היקפם ועילת השימוש בהם. להלן עיקרי תשובת נציג עיריית ירושלים.

**עיריית ירושלים משתמשת בטכנולוגיית ניתוח וידאו לעיבודי תנועה או לזיהוי פעילות חריגה לטובת ניהול המרחב הציבורי ומערכת התחבורה. העירייה אינה עושה שימוש בעיבוד מידע ביומטרי ואינה עושה שימוש בזיהוי פנים במצלמות אבטחה. (המענה אינו מתייחס לשימושים במבנים של העירייה או לאבטחת מתקני העירייה עצמם).**

שני הגופים המרכזים את השימוש בטכנולוגיות אלה הם **אגף חירום וביטחון** המנהל חמ"ל של מצלמות ביטחון הפרוסות ברחבי העיר ומרכז **ניהול תנועה של אגף תחבורה ותשתיות** המנהל חמ"ל ניהול תנועה בעיר.

**אגף חירום וביטחון** עושה שימוש במצלמות וידאו בגנים ציבוריים ומערכת כריזה למניעת ונדליזם ושמירה על הסדר הציבורי, וכן במצלמות בשוקים ברחבי העיר ובצמתים מרכזיים.

<sup>23</sup> גונדר משנה, אילן יום טוב, רמ"ח פיתוח יישומי ידע, מינהל טכנולוגיות, שירות בתי הסהר, 18 במאי 2020. נתקבל מהגב' גל יונה, לשכת השר לביטחון פנים.

<sup>24</sup> סגן טפסר, משה שחר ראש לשכת נציב כבאות והצלה, 25 במאי 2020, נתקבל מהגב' גל יונה, לשכת השר לביטחון פנים.  
<sup>25</sup> מר אבנר סעדון, מנהל האגף למדיניות ותכנון אסטרטגי, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 4 ביוני 2020.



האיסוף נעשה באמצעות מצלמות קבועות המותקנות במרחב הציבורי ובמתקני העיריה השונים.

**סך הכל בכל העיר יש כ-1,000 מצלמות.** חלק מן המצלמות כוללות יכולות אנליטיקה מבוססת עצמים (אובייקטים) במצלמה עצמה, וכ-100 מהן מחוברות לשרתים (server) המאפשרים ביצוע אנליטיקה מבוססת למידה.<sup>26</sup>

**בידי העירייה מצויה טכנולוגיה של זיהוי לוחיות רישוי, ניתוח וידאו ברמה של חוקים (הגדרות לפעילות המערכת) המבוססים על פרמטרים קבועים כגון, כיוון תנועה, השתנות הרקע, כמויות של עצמים או אנשים, חציית קוים, ובנוסף לכך יכולת של זיהוי חריגים במרחב לאור למידת השיגרה.** במערכות אגף חירום וביטחון לא מתבצעת השוואת מידע מול מאגרי מידע כלשהם, ובכלל זה לא מול מאגרי לוחיות רישוי. כל המידע שנאגר נמחק על פי הגדרות מאגר המידע לאחר פרק זמן קצוב.

**מרכז ניהול תנועה של אגף תחבורה ותשתיות (מנת"י)** התקין מצלמות לאורך צירי התחבורה המרכזיים בעיר ומפעיל בנוסף מצלמות לבקרת כניסה ברחובות מסוימים. לפי נציג העירייה חלק מן המצלמות של מנת"י כוללות יכולות אנליטיקה כגון: זיהוי כניסה לאזור שהוגדר (במקור "פוליוגון") יציאה של עצם מאזור מוגדר, נפילה או תזוזה של אובייקט ועוד. עם זאת, בפועל מנת"י לא עושה כיום שימושים כאלה במצלמות.

### **בין המערכות שמפעילה מנת"י:**

- **בקרת כניסה** לרחובות או מקומות מסוימים באמצעות מחסומים ומצלמות עם יכולת זיהוי לוחית רישוי (LPR) - מותקנת ב-7 מחסומים;
- **מערכת בקרת כניסות** המופעלת בשני חניוני חנה וסע ברחבי העיר;
- **מערכת אכיפת כלי רכב מזהמים** - מצלמת LPR המזהה לוחית רישוי ומשווה אותם למאגר מידע של משרד התחבורה על כלי רכב מזהמים;
- **מערכת לאכיפת חניה אסורה** - מצלמות המזהות עמידה של כלי רכב לא מורשים במקומות אסורים כגון סימון אדום לבן ותחנות אוטובוס.
- **מערכת אכיפה בצירי תחבורה ציבורית** - מערכת מצלמות LPR המזהות מספר רישוי ומשווה את הנתונים עם מאגר של משרד הרישוי הכולל נתוני הרשאה לנסוע בנתיב תנועה ציבורי.

<sup>26</sup> אנליטיקה מבוססת עצמים: חציית קו, התקהלות, נסיעה בניגוד לתנועה, כניסה למתחם, הסרה או הוספה של עצם במרחב. אנליטיקה מבוססת למידה (AI): מערכת שיש לה יכולת למידה של המתרחש במרחב ויכולת הבנה של מה הוא החריג. דוא"ל מענה ממר שביט שקד, הממונה על המשל"ט העירוני ומנהל מערכות אבטחה, אגף חרום וביטחון, 9 בדצמבר 2020.

- **מערכת מצלמות במנהרות התחבורה "טרפיקון"** – המערכת כוללת אנליטיקה כגון: זיהוי רכב תקוע במנהרה או רכב הנוסע נגד כיוון התנועה ועוד. במקרים מוגדרים תיסגר המנהרה בשל זיהוי של המערכת עד לטיפול בבעיה.

**חשוב לציין כי לפי נציג העירייה "במערכות האכיפה האלקטרוניות תמונות הנוסעים מטושטשות. וככל שמופק דוח הוא נשלח לעובדי העבירה על ידי פקח עירוני. סרטונים ברזולוציה נמוכה נשמרים למורשים בלשכה המשפטית לצרכי בירור מול האזרח."**

לפי נציג העירייה היתרון בשימוש בטכנולוגיות המוזכרות לעיל הוא התייעלות ביכולת לאתר אירועים חריגים בהינתן הרבה מצלמות ומעט כוח אדם צופה; וניהול יעיל ומהיר של התנועה המאפשר איתור מהיר של תקלות וחוסך כוח אדם לאיוש מחסומים.

באשר להיוועצות בגורמי ממשלה או רשויות אחרות ציין נציג העירייה כי העירייה מתייעצת עם יועצים מקצועיים ועם שותפים אסטרטגיים כגון משטרה ונציגי ציבור טרם החלטה על הצבת מצלמות או שימוש ביכולות אנליטיקה. לדבריו העירייה אינה חולקת מידע או ניתוח ממאגרי תמונות עם גופים אחרים ואינה מקבלת מידע שכזה מגופים אחרים.

### 3.2 תל-אביב<sup>27</sup>

להלן עיקרי תשובת נציגת עיריית תל-אביב לפנייתנו:

טכנולוגיות ניתוח וידאו הן הבסיס לעיר חכמה ועתידות לשמש כאמצעי מרכזי לניהול העיר. עם זאת, **הנחת העבודה היא, כי אין לעירייה כל צורך בזיהוי של אדם במרחב הציבורי, ועל כן לא נעשה על ידינו כל שימוש בטכנולוגיות ניטור מתקדמות על אדם, כגון זיהוי פנים, זיהוי קול, לבוש, שפת גוף וכיו"ב.** פיתוח המערכת ועיצוב המענה לצרכים נעשה על בסיס תפיסת Privacy by Design. **העירייה הקימה בשיתוף עם אוניברסיטת תל אביב סטארט-אפ שמטרתו להחליף את פניהם של האנשים אשר נקלטים במצלמות העירייה. נציגת העירייה ציינה כי הם מקווים שבמהלך 6 החודשים הקרובים יצליחו ליישם את הטכנולוגיה על מקור וידאו בזמן אמת.**

כלי איסוף בהם עושה העירייה שימוש או עתידה לעשות שימוש:

- **מצלמות ביטחון: כ-1,200 מצלמות הוצבו במרחב הציבורי והן מחוברות למשל"ט הביטחון העירוני. במצלמות אלה מופעלת אנליטיקה בסיסית של זיהוי תנועה במרחב נתון, בשעות חריגות וכד'. מצלמות ביטחון ללא אנליטיקה הותקנו גם במתקני עירייה ובמוסדותיה. הצבת המצלמות ופעילותן נעשית בהתאם לנוהל.**

<sup>27</sup> ליאורה שכטר, מנהלת אגף מחשוב ומערכות מידע, עיריית ת"א, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 11 ביוני 2020.

נבחנת האפשרות לעשות שימוש באנליטיקה לטובת זיהוי מפגעים אוטומטי במרחב הציבורי, כגון תברואה (ערימת אשפה שאינה בתוך כלי קיבול), תאורה (עמוד תאורה פגום או תקול), שפ"ע (נזילת מים בגינה).

- **מצלמות לאכיפת עבירות חניה:** 20 מצלמות נייחות ו-6 ניידות, אשר פועלות בהתאם לחוזר מנכ"ל משרד הפנים 4/2018. מיושמת אנליטיקה המזהה רכב החשוד כעובר עבירה, ההחלטה על מתן דו"ח הינה אנושית- על ידי פקח.
- **מצלמות לאכיפת שימוש שלא כדין בנת"צ** – 65 מצלמות, אשר פועלות מכוח סעיף 1א27. לפקודת התעבורה ותקנות התעבורה (הפעלת מצלמות בידי רשות מקומית לשם תיעוד שימוש שלא כדין בנתיב תחבורה ציבורית), תשע"ז-2016. מיושמת אנליטיקה המזהה רכב החשוד כעובר עבירה (לוחית רישוי שלא הוגדרה ע"י משרד התחבורה כרכב שנסיעתו בנת"צ מותרת) ההחלטה על מתן דו"ח הינה אנושית, ע"י הפקח.
- **מצלמות גוף** – אושר ביצוע פיילוט באגף הפיקוח באמצעות 20 פקחים על יסוד טיוטת נוהל העבודה. הפיילוט טרם החל. ללא אנליטיקה.
- **רחפנים** – אושר ביצוע פיילוט באגף סיירת לביטחון עירוני (סל"ע) באמצעות 2 רחפנים. טרם גובש נוהל עבודה.

נציגת העירייה צירפה לתשובתה נוהל של העירייה מס' 843 "הצבת מצלמות במתקנים ובמרחב הציבורי" הנוהל כולל התייחסות להליך הגשת בקשה להצבת מצלמה, אופן בחינת הבקשה ויישום ההחלטה בנושא. בנוסף, צורף נוהל לשימוש במצלמות גוף לתקופת הפיילוט.

### 3.3 פתח תקוה<sup>28</sup>

לפי תשובת נציג עיריית פתח תקוה העירייה אינה עושה שימוש חיצוני בטכנולוגיות ניתוח וידאו ומידע ביומטרי פרט לאיכון רכבי העירייה הנמצאים בשימוש פנימי.

- **העירייה משתמשת במצלמות LPR** קבועות עבור מעקב אחר רכבי העירייה בשני אתרים: באתר "סירקין" שבאחריות אגף הרכב ולשם מעקב אחרי משאיות באתר פינוי פסולת. נתוני המצלמות מושוים למאגר רכבי העירייה.
- **מצלמות גוף ומצלמות קבועות ללא אנליטיקה** נמצאות בשימוש פקחי העירייה, אגף הביטחון ושמירת הסדר הציבורי;

#### היקפי הפריסה של מצלמות לפי תשובת נציג עיריית פתח תקוה הם:

- 550 מצלמות ב-43 אתרים ברחבי הערי לשם ביטחון עירוני ושמירת הסדר הציבורי;

<sup>28</sup> יניב בניטה, רו"ח, מנכ"ל עיריית פתח תקוה, מענה לפניית מרכז המחקר והמידע של הכנסת, 15 ביוני 2020.

- 200 מצלמות ב-40 מתחמי גני ילדים;
- 100 מצלמות ב-8 בתי ספר;
- 25 מצלמות גוף עבור בטחון ופיקוח עירוני.

לפי תשובת נציג העירייה המידע מן המצלמות נשמר עד 30 יום וזאת לדבריו בהתאמה לחוק ולתקנות הגנת הפרטיות. לדבריו קיים נוהל הצבת מצלמות תיעוד והוא בהליכי אשרור, אך אין נוהל ביחס למעקב אחר רכבי העירייה. עוד ציין נציג עיריית פתח תקוה כי העירייה לא חולקת מידע או מקבלת מידע מגופים אחרים בנושא ניתוח וידאו או מידע ביומטרי.

### 3.4 ראשון לציון<sup>29</sup>

מרכז המחקר ומהידע של הכנסת פנה אל הנהלת עיריית ראשון לציון שבחרה להשיב באמצעות נציג החברה העירונית ראשון לציון לביטחון וסדר ציבורי.

לפי תשובת נציג החברה העירייה עושה שימוש במערכות זיהוי לוחית רישוי אוטומטי (ALPR) לשם בקרת כניסה לחניונים ולבקרת כניסה לאתרי עירייה.

- **בחניונים** – לצורך חישוב משך החנייה ועלותה או מתן הנחה בתעריף. המידע מלוחית הרישוי מושווה למאגר "תווי תושב" הכוללים פרטי תושבים ורכביהם. יישום זה קיים ב-4 חניוני העירייה.
- **בקרת כניסה באתרי עירייה** – לצורך בקרת כניסה ופתיחת שער לרכבים מורשים בשלושת מתקני העירייה נעשית הצלבה של פרטי לוחית הרישוי עם מאגר ניהול המשתמשים בחניונים.

**נציג עיריית ראשון לציון לא ציין בתשובתו מהו היקף פריסת המצלמות ברחבי העיר.** אך ציין כי נקבעו כללים למשך השמירה של מידע ממצלמות: בתוך מבני מוסדות חינוך 3 ימים; בחצרות מוסדות חינוך, במוסדות ציבור או במרחב הציבורי, עד 10 ימים. במקרים חריגים ובאישור מראש לכל רכיב עד 28 ימים. מידע ממערכות ה-ALPR באתרי העירייה נשמר ל-7 ימים. לפי נציג העירייה היא מעבירה מידע למשטרת ישראל על פי דרישתה או לכל גורם הממציא צו שיפוטי מתאים.

## 4. אתגרים וסיכונים במערכות ניטור במרחב הציבורי

**לצד היתרונות הברורים בשימוש במערכות ניטור וניתוח וידאו ותמונה לשם שמירה על הסדר הציבורי, חקירת פשעים וטענות בדבר צמצום פשיעה (נושא השנוי במחלוקת),**

<sup>29</sup> מוטי נחמני, מנכ"ל החברה העירונית ראשון לציון לביטחון ולסדר ציבורי, דוא"ל מענה לפניית מרכז המחקר והמידע של הכנסת, 7 ביולי 2020.

**ויישומים מסחריים אחרים כמפורט לעיל, קיימים בשימושים במערכות אלה אתגרים וסיכונים שיש לתת עליהם את הדעת ולבחון דרכים למתן אותם.**

#### **4.1 החשש מפגיעה בפרטיות ובחירויות אזרחיות נוספות**

במסמך קודם שעסק בנושא מצלמות<sup>30</sup> צוין בין השאר כי:

פרטיות הינה מושג עמום, סבוך ויחסי. הגבולות בין הפרטי והציבורי משתנים תדיר בין חברה לחברה ולעיתים קרובות בין פרטים שונים באותה החברה. למרות שמקובל לראות בזכות לפרטיות – זכות מודרנית, ניתן לזהות התייחסות לנושא הפרטיות כבר בחוקי חמורבי ובמשנה. הניסוח המשפטי הבולט והמפורסם הראשון של זכות זו שייך לוורן וברנדייס שטענו בשנת 1890 **כי הזכות לפרטיות היא "הזכות להיעזב במנוחה" (The right to be let alone) ומכוחה זכותו של האדם לשלוט במידע פרטי אודותיו.**

הסוציולוג אלן וסטיין הגדיר פרטיות כיכולתו של הפרט לשלוט במידע אודותיו. שליטה זו באה לידי ביטוי בקביעה איך, מתי ולמי יימסר המידע על האדם, מהם השימושים המותרים בו ומהי מידת התפוצה שלו. פרופ' מיכאל בירנהק מגדיר גישה זו "פרטיות כשליטה". הדגש בגישה זו איננה על תביעה למידת גילוי או שמירת סודיות כזו או אחרת אלא לעצם היכולת של הפרט להכריע באשר למידת השימוש במידע עליו, מועדו ותנאיו. פרופ' בירנהק מצוין, כי שני עקרונות נלווים מסייעים בעיגונה של הזכות לפרטיות: **עקרון ההסכמה** – האדם מסכים לאיסוף, עיבוד והעברת מידע ממנו, **ועקרון צמידות המטרה** – השימוש במידע שנאסף מבוצע רק בהתאם לצורך שלשמו הסכים האדם לגילוי ולכן למשל המידע לא מועבר לצד שלישי או משמש למטרות אחרות מזו שלשמן נמסר.

בנוסף, פרטיות היא צורך אנושי בהגבלת הפיקוח החברתי והמשמיע של הפרטים בחברה. לידיעה כי ישנה "עין פקוחה" שיכולה לעקוב אחריו יש השפעה מיידית על החירות שלך לחיות את חייך כפי שאתה מעוניין.<sup>31</sup>

**העמימות של מושג הפרטיות עלולה לגרום לכך שתהיה נטייה מוסדית לוותר עליה אל מול תועלות שהן כביכול ברורות ומדידות יותר כגון צמצום פשיעה, תוך התעלמות מהשלכותיו של ויתור זה.**

לעניינו, נראה כי בהטמעתן של יכולות ניטור וידאו מתקדמות מתעוררת שאלה בדבר הפוטנציאל של טכנולוגיות אלו לפגוע בצורה ניכרת בחירויות הפרט תוך יצירת תיעוד מתמיד שלו, הניתן לחיפוש ולאחזור בכל רגע נתון כך שישמש כנגדו. כמו כן, נשאלת השאלה האם תיעוד כזה מתיישב עם עקרון ההסכמה וצמידות המטרה במקרים בהם אין

<sup>30</sup> רועי גולדשמידט, "מצלמות מעקב לצרכי אבטחה במרחב הציבורי", מרכז המחקר והמידע של הכנסת, 5 בדצמבר 2011.

<sup>31</sup> שם.

## לאדם ידיעה, שליטה או אפשרות לסרב לתיעוד שלו או כאשר המטרה איננה מוגדרת בבירור ויכולה לשמש גורמים ומטרות שונות.

קיים חשש כי מעקב מתמיד אחר אזרחים, ייצור קונפורמיות עם מה שייתפס כנורמות ממסדיות, ויפגע בחירויות אזרחיות שונות. השימוש בזיהוי פנים, נטען כי הטכנולוגיה "טומנת בחובה פוטנציאל לפגיעה נרחבת בחירויות היסוד: חופש הביטוי, חופש הדת, חופש ההתאגדות, חופש ההפגנה ואפילו בזכות לחירות. לטכנולוגיה המאפשרת מעקב מתמשך אחר תנועות של אזרחים אפקט ממשמע וממשטר הגורם לאדם להימנע מפעילויות שונות שהוא חופשי לעשות. אדם שיודע שמהלכיו מנוטרים וחשופים לעיני השלטון ישנה את התנהגותו ואף ייזהר בהתבטאויותיו.<sup>32</sup>

תשומת לב ציבורית רבה הופנתה בשנה האחרונה לאחת מהחברות המספקת שירותי זיהוי פנים על בסיס אגירה של תמונות מהאינטרנט. במכתב של יו"ר ועדת המדע, החלל והטכנולוגיה של בית הנבחרים לחברה<sup>33</sup>, הוא הביע חשש מפעילות החברה ומדיווחים לפיהם שרתי החברה נפרצו והמידע שבהם נגנב. לפי פרסומים נרחבים בנושא בעיתונות, מה שמייחד את פעילותה של החברה היא העובדה כי היא יצרה מאגרי מידע עצומים על בסיס תמונות מרחבי רשת האינטרנט וכך מאפשרת לבצע חיפוש המתבסס על תמונה אותה מעלה המשתמש, ולקבל תוצאות הכוללות את כלל התמונות המצויות באינטרנט של האדם המופיע בתמונה, והפניות למקור שלהן (זאת בניגוד לדרך הנפוצה יותר ביישומי זיהוי פנים, בהם ההשוואה נעשית אל מול מאגרים קבועים מראש – כגון מאגר תמונות רישיון נהיגה). היישום של החברה, כך נטען גם אמור להתממשק עם משקפי "מציאות רבודה" וכך לאפשר לחפש כל אדם אותו רואה המשתמש. לפי כתבה בנושא בניו-יורק טיימס, יותר מ-600 סוכנויות אכיפה בארצות הברית החלו להשתמש ביישום של החברה.<sup>34</sup>

## 4.2 זליגת שימושים (Function Creep)

אחת מן ההנמקות המקובלות כנגד שימוש ביכולות ניטור מתקדמות או בטכנולוגיות אחרות השנויות במחלוקת היא החשש מפני זליגת שימושים. כלומר מצב שבו עילת האיסוף, הניטור והניתוח של מידע תהיה אחת, אך בפועל היא תשמש גם או בעיקר לעילות אחרות משניות, שהצידוק שלהן פחות. דוגמא לזליגת שימושים ולדיון באשר למידתיות בשימוש בטכנולוגיות מעקב, ניתן לראות בשימוש במעקבי שב"כ שנועדו במקור כאמצעי למאבק בטרור לשם זיהוי וניטור מגעים עם חולי קורונה. בהקשר דנן, נשאלת השאלה **מהן עילות מוצדקות לצילום**

<sup>32</sup> עת"מ 47229-09-20 האגודה לזכויות האזרח נ' משטרת ישראל.

<sup>33</sup> לנוסח המלא של המכתב ראו [כאן](#).

<sup>34</sup> Kashmir Hil, "[The Secretive Company That Might End Privacy as We Know It](#)", **New York Times**, updated February 10, 2020.

**וניטור ומה אינן עלילות מוצדקות וכיצד ניתן למנוע מצב בו כלי שעוצב למטרה אחת ישמש בפועל למטרות אחרות נוספות?**

### 4.3 אפליה אלגוריתמית והחשש מטעויות מכונה<sup>35</sup>

אפליה אלגוריתמית היא מצב שבו אלגוריתם (למשל במערכת מיון מועמדים לעבודה, או במצלמה בכניסה למקום) מזהה, במישרין או בעקיפין, מידע ביחס למשתני רקע, כגון מגדר, גזע או נטייה מינית, ומפיק תוצאה בהינתן משתנים אלה.

**מחקרים שונים הצביעו על נטייה של מערכות בינה מלאכותית לשעתק אפליה אנושית גם כאשר המידע המפלה לא הוצג למערכת הממוחשבת.** היכולות המועצמות של טכנולוגיות ניטור לזהות "סוגי אנשים"; התנהגויות, צורות לבוש, מגדר ועוד יכולות להיות גם כלי בידי המפעילים שלהן לשם שימוש מפלה או לשימוש לרעה.

**מידת הדיוק של מערכות בינה מלאכותית שונה מאוכלוסייה לאוכלוסייה. לדוגמה, מכון התקנים האמריקאי מצא כי שיעור הטעויות של תוכנות זיהוי פנים בזיהוי אנשים ממוצא אפריקני או מזרח אסיאתי היה גבוה במידה ניכרת משיעור הטעויות בזיהוי אנשים ממוצא אירופי. כמו כן נמצאה שיעורי ההצלחה בזיהוי של נשים היה נמוך מזה של גברים, ושל תינוקות וקשישים נמוך מזה של מבוגרים.<sup>36</sup>**

חברות שונות מבטיחות לנטר מצבי רוח או מצב קוגניטיבי על בסיס צילומי פנים או ניתוח קול. לפי דוח של האגודה לזכויות האזרח בארה"ב, מערכות כאלה לא הוכחו עד היום כאמינות מבחינה מחקרית למרות ניסיונות גוברים לעשות שימוש במערכות כאלה כדי לזהות פשיעה או טרור וקיים חשש מטעויות בהחלטות שיתקבלו על בסיס מערכות כאלה או מייחוס משמעות למידע מדעי כביכול אודות "חשודים".<sup>37</sup>

**לעניינו, במצבים בהם גישה למקום או זיהוי פושע ומעצר שלו תלויים ברמת הדיוק של החלטות מכונה, יכולות להיות לשימוש במערכות כאלה השלכות ניכרות.** כאמור לעיל, מלבד החשש מטעויות מכונה, קיים גם חשש מטעויות בפענוח או הפרשנות של הממצאים על ידי המפעיל של הטכנולוגיה.

**חברות שונות מבטיחות לנטר מצבי רוח או מצב קוגניטיבי על בסיס צילומי פנים או ניתוח קול. לפי דוח של האגודה לזכויות האזרח בארה"ב, מערכות כאלה לא הוכחו עד היום כאמינות מבחינה מחקרית**

<sup>35</sup> רועי גולדשמידט, "אפליה אלגוריתמית במערכות המבוססות בינה מלאכותית", מרכז המחקר והמידע של הכנסת, יוני 2020.

<sup>36</sup> Grother, P. et al, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects", National Institute of Standards and Technology", December 2019.

<sup>37</sup> Jay Stanley, "The Dawn of Robot surveillance: AI, Video Analytics and Privacy", American Civil Liberties Union, June 2019.

**הדין הציבורי בארה"ב ביחס לטכנולוגיות זיהוי פנים**

לפי דוח של אוניברסיטת ג'ורגטאון משנת 2016 ב-1 מכל 4 מחלקות משטרה מקומיות או מדינתיות יש אפשרות לבצע חיפוש מבוסס זיהוי פנים אל מול מערכות המצויות ברשותם. בלפחות 26 מדינות מותר לרשויות אכיפת החוק לבצע חיפושים בהשוואה למאגרי רישיונות נהיגה או תעודות זהות. חיפושים כאמור לא מבוצעים רק במקרים של מעצר חשודים אלא גם ככלי לסריקה של עוברי אורח במרחב הציבורי באמצעות צילום וידאו בזמן אמת (Live Face Recognition – LFR).<sup>38</sup>

**בדצמבר 2018 קרא נשיא חברת מייקרוסופט, בראד סמית', לממשלות לקדם חקיקה להסדרת השימוש בטכנולוגיות זיהוי פנים. לדבריו "השד של זיהוי פנים בדיוק יוצא מהבקבוק" ואם לא נפעל כעת, אנו מסתכנים בכך שנתעורר עוד חמש שנים לגלות שטכנולוגיות זיהוי פנים הפכו לנפוצות באופנים שהחמירו את הבעיות החברתיות הנלוות.** בשלב זה יהיה קשה הרבה יותר להתעלם מאתגרים אלה.<sup>39</sup>

בצד היתרונות של טכנולוגיות אלה ציין סמית' מקרים בהם השתמשה המשטרה בטכנולוגיה לזיהוי ילדים נעדרים; היסטוריונים השתמשו בה לזיהוי חיילים אלמונים בתמונות, חוקרים השתמשו בה לזהות מחלה גנטית נדירה ושירותי בנקאות מימשו יישום המאפשר למשוך כסף באמצעות זיהוי פנים וקוד. **נשיא מייקרוסופט ציין כי החברה מאמצת עקרונות לשימוש בזיהוי פנים: הוגנות, שקיפות, אחריותיות, אי-אפליה, הודעה והסכמה, ומעקב על פי חוק.**<sup>40</sup> בעקבות מותו של ג'ורג' פלויד ואירועי "black Lives Matter" התעורר בארצות הברית דיון ציבורי ער ביחס לניטור במרחב הציבורי בכלל וביחס לשימוש שזיהוי פנים בפרט.

במכתב שהפנו 35 חברי קונגרס ביוני 2020 אל ראשי כמה מסוכנויות הביטחון בארצות הברית<sup>41</sup> הם מציינים בין השאר את השימוש בצילומים אלקטרו-אופטיים ואינפרא-אדום, איסוף נתוני מיקום מאנטנות סלולר, צילומי וידאו מרחפנים, איסוף מידע אישי מטלפונים ניידים ושימוש בטכנולוגיות זיהוי פנים וזיהוי לוחית רישוי אוטומטי - כולם כאמצעי מעקב שנעשה בהם שימוש כנגד מפגנים במדינות שונות בארצות הברית במהלך ההפגנות. לטענתם, למעקב מדינתי יש אפקט מצנן על מימוש זכות ההפגנה (התיקון הראשון לחוקה) ועל הזכות להיות מוגנים מפני חיפוש (התיקון הרביעי לחוקה).<sup>42</sup>

בעקבות אותם אירועים הצהיר מנכ"ל חברת המחשוב הגדולה **IBM כי החברה לא תספק יותר מערכות זיהוי פנים מתוצרתה או תוכנות לניתוח מערכות כאלה.** וכי החברה מתנגדת לשימוש בכל טכנולוגיה, כולל טכנולוגיות זיהוי פנים של ספקים אחרים, שתוצע לצורך מעקב המונים, או מיון מבוסס גזע (Racial profiling) או הפרה של זכויות אדם בסיסיות וחירויות. במכתבו לנציגי הקונגרס והסנאט, ציין המנכ"ל כי **"כעת הוא הזמן לפתוח בדיאלוג לאומי באשר לשאלות האם וכיצד על סוכנויות החוק הפועלות בתוך ארה"ב להשתמש בטכנולוגיות זיהוי פנים."**<sup>43</sup>

<sup>38</sup> Clare Garvie et al., "[The Perpetual Line – Up: Unregulated police Face recognition In America](#)", Georgetown Law, October 18, 2016.

<sup>39</sup> Brad Smith, "[Facial recognition: It's Time for Action](#)", December 6, 2018.

<sup>40</sup> Ibid.

<sup>41</sup> FBI, DEA, National Guard Bureau, Customs and Border Protection

<sup>42</sup> לנוסח המלא של המכתב ראו [כאן](#).

<sup>43</sup> לנוסח המכתב ראו באתר החברה, [כאן](#).