



זיהוי פנים במרחב הציבורי בישראל עקרונות למדיניות וקריאה לאסדרה

היחידה להזדהות וליישומים ביומטריים

מערך הסייבר הלאומי

יולי 2021



תוכן העניינים

3 מבוא

4 ההתפתחות הטכנולוגית של זיהוי פנים

5 זיהוי פנים במרחב הציבורי

8 קריאה לאסדרה

8 הסיכונים הכרוכים בשימוש בזיהוי פנים במרחב הציבורי

9 אסדרת השימוש באמצעי זיהוי פנים במרחב הציבורי בעולם

12 עקרונות מדיניות – שימוש באמצעי זיהוי פנים במרחב הציבורי בישראל

14 סיכום

15 תודות

16 נספח טכנולוגי

16 עקרונות פריסת מערכת לצילום או זיהוי פנים במרחב הציבורי (היבטי סייבר)

17 עקרונות ניהול תקין של מערכת ביומטרית (היבטים ביומטריים)

מבוא

1. היחידה להזדהות וליישומים ביומטריים במערך הסייבר הלאומי גיבשה מדיניות לאומית וקוים מנחים ליישומים ביומטריים בהתאם להחלטת ממשלה מספר 4510 מיום 1.4.12. מדיניות זו מתייחסת להיבטים טכנולוגיים וכן היבטי פרטיות, ביטחון ואתיקה הנוגעים הן לפעילות ממשלתית והן לכלל המשק¹. מסמך המדיניות עוסק ביישומים ביומטריים באופן כללי ואינו מתמקד בטכנולוגיה ביומטרית מסוימת או ביישום ספציפי.
2. זיהוי פנים במרחב הציבורי הוא יישום ביומטרי בו נעשה צילום וזיהוי פנים מול קהל בלתי מסוים המצוי במרחב הציבורי, ומבוצעת השוואה ביומטרית אל מול מאגר, ללא שיתוף פעולה מצד הקהל (Face Recognition of Non-Cooperative Subjects). עם השיפור הדרמטי שחל בשנים האחרונות בשיעור הדיוק של טכנולוגיית זיהוי הפנים, העלייה בשימוש במצלמות במרחב הציבורי, רגישות הנושא והיבטיו הטכנולוגיים המיוחדים ומתוך הסתכלות צופה פני עתיד נוכח המגמות בעולם בשימוש במערכות ביומטריות, הוחלט לגבש עקרונות למדיניות בנושא, ובהתאמה לקרוא לאסדרת תחום זה.
3. ראשית עבודה זו הוצגה בדיון וועדת המדע והטכנולוגיה בכנסת מיום 15.12.2020, לקראתו פורסם דו"ח מרכז המחקר של הכנסת, ששימש כרקע לדיון². כפי שצוין בדו"ח זה ובדיון בכנסת, לא קיימת מדיניות כוללת וסדורה בישראל או חקיקה ספציפית המסדירה שימוש בטכנולוגיות ניטור מתקדמות כגון זיהוי פנים.
4. **אנו סבורים כי יש לפעול לאסדרתו של נושא רגיש זה בחקיקה ראשית, תוך קיום דיון ציבורי, בפורום רחב יותר, אשר בו יהיה ניתן לשקול את הסיכונים מול התועלות, וכן מתן דגש לשיקולים אתיים ואחרים הכרוכים בו.** קיימת חשיבות רבה בהסדרת "כללי המשחק" אשר מחד יאפשרו לגורמי אכיפה (או גורמים אחרים) לממש את תפקידיהם ומשימותיהם תוך מינוף הטכנולוגיה, ומאידך ישרטטו את גבולות ריסון הכוח הנדרשים כדי להימנע מפגיעה לא רצויה בתושבי ישראל ובחברה ככלל.
5. **מטרת העבודה המוצגת להלן היא הצגת מכלול הסוגיות אשר יש לבחון במסגרת זו.** המסמך שלפניכם כולל דוגמאות נבחרות להסדרת הנושא בעולם המערבי, כאשר הבולטת בהן היא הצעת הרגולציה ל AI של האיחוד האירופאי, אשר מתייחסת באופן ספציפי לשימוש מערכת האכיפה במערכות ביומטריות לזיהוי מרחוק של אדם³. כמו כן, מצורף דו"ח סקירה בינ"ל מקיף של מכון יובל נאמן באוניברסיטת תל אביב המציג היבטים שונים הכרוכים באסדרת שימוש במערכות אלה.
6. המסמך אינו מציג דיון ערכי מקיף ביחס לגיטימיות המטרות בהפעלת מערכת לצילום במרחב הציבורי, אשר רגישותו מועצמת ככל שמדובר במערכות המכוונות לזיהוי פנים. דיון מקיף יידרש לטעמינו בפורום רחב יותר, כאמור.

¹ מדיניות לאומית אינטגרטיבית ליישומים ביומטריים

https://www.gov.il/he/departments/news/bio_biopolicy_app

² דו"ח הממ"מ של הכנסת בנוגע לשימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי

https://fs.knesset.gov.il/globaldocs/MMM/2503c32b-2f94-ea11-8104-00155d0aee38/2_2503c32b-2f94-ea11-8104-00155d0aee38_11_16517.pdf

³ https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

7. למען הסר ספק, מסמך זה אינו נוגע לפרויקט התיעוד הלאומי החכם המשלב ביומטריה והכולל זיהוי פנים (המוסדר בחקיקה ייעודית)⁴. כמו כן, היא אינה נוגעת לשימוש בזיהוי פנים במערכות נוספות אחרות המצריכות שיתוף פעולה של המשתמש (כגון מערכות בקרת כניסה), או לזיהוי פנים בעולם הווירטואלי (כגון ברשתות החברתיות).
8. מסמכי רקע ממשלתיים רלוונטיים הם מסמך ההמלצות שפורסם על ידי מערך הסייבר הלאומי בנושא צמצום סיכוני סייבר ממצלמות אבטחה (אפריל 2018)⁵; מסמכי הרשות להגנת הפרטיות⁶; והמדיניות הלאומית ליישומים ביומטריים. המסמך הנוכחי מפרט דגשים טכנולוגיים נוספים המתאימים למערכות אלה (בפרט בהיבטי הביומטריה).

ההתפתחות הטכנולוגית של זיהוי פנים

9. מערכת זיהוי פנים (Facial Recognition System) היא אפליקציית מחשב הכוללת אלגוריתם המסוגל לזהות או לאמת זהותו של אדם, באופן אוטומטי או אוטומטי למחצה, על בסיס תצלום דיגיטלי או מקור וידאו. אחת הדרכים לעשות זאת היא על ידי השוואה בין תמונה ספציפית לבין תמונות המצויות במאגר נתונים (מה שמכונה בשפה המקצועית 1: Many או 1: Few), או על ידי השוואה בין תמונה ספציפית לבין רשומה ספציפית (מה שמכונה בשפה המקצועית 1: 1).
10. מערכות לזיהוי פנים משמשות היום למגוון תכליות, לרבות לצרכים אזרחיים ומסחריים, החל מתהליכי אימות וזיהוי במגזר הפיננסי (פתיחת חשבונות בנק, הנגשת שירותים דיגיטליים וכיו"ב), בקרת כניסה למקומות עבודה, זיהוי חולה במערכות בריאות, זיהוי לקוח בבתי עסק שונים, רשתות חברתיות, מעברי גבול, זיהוי לטובת הנפקת תיעוד לאומי/רשמי. מערכות אלה משמשות גם לצרכים ביטחוניים שונים, אכיפה ושמירה על הסדר הציבורי וסיכול טרור.
11. עד לשנים האחרונות פעלו אלגוריתמים לזיהוי פנים על בסיס השוואות גאומטריות של תווי הפנים, למשל מרחקים בין איברי הפנים: עיניים, אף, פה, אוזניים וכדומה. כמו כן אלגוריתמים מסוימים בדקו פקטורים נוספים הנוגעים למבנה הפנים, כגון טקסטורת עור הפנים. בשנים האחרונות אנו עדים לשינוי בסוג האלגוריתמים שעומדים בבסיס טכנולוגיות לזיהוי פנים, כך שיותר ויותר טכנולוגיות נשענות על אלגוריתמים מסוג Deep Convolutional Neural Network, המבוססת על רשתות נוירונים ולמידת מכונה (תת קבוצה בתוך התחום שנקרא בינה מלאכותית). בשיטה זו, שפותחה בהשראת תהליכים קוגניטיביים המתרחשים ברשת עצבית טבעית, כמו למשל תהליכים במוח האדם, כל מעבד ברשת מבצע פעולה מתמטית פשוטה, ובעזרת שילוב כלל פעולות המעבדים במערכת מסוגלת הרשת לבצע התנהגות מורכבת.
12. השינוי המתואר באופן הפעולה של האלגוריתמים לזיהוי הפנים אפשר קפיצת מדרגה משמעותית ביכולת הביצוע שלהם, קרי, הפחתה ניכרת של שיעורי השגיאה בתהליכי ההשוואה (שיפור של פי 100

⁴ הממונה על היישומים הביומטריים (העומד בראש היחידה להזדהות ויישומים ביומטריים במערך הסייבר הלאומי) מבצע פיקוח על פרויקט התיעוד הלאומי החכם, וממליץ על מדיניות הנוגעת לפרויקט זה, מכוח חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע התשי"ע 2009.

⁵ <https://www.gov.il/he/departments/policies/iotcameras>

⁶ https://www.gov.il/BlobFolder/policy/surveillance_cameras_guidelines/he/The%20use%20of%20security%20cameras.pdf ;

https://www.gov.il/BlobFolder/reports/drone_recommendations/he/PPA_DRONE_RECOMMENDATIONS.pdf

- במהלך העשור האחרון), ובפרט בכל הקשור לתמונות מבוקרות (תמונות הניטלות בשיתוף פעולה של נדגם, בסביבה מבוקרת ועל פי הגדרות ICAO).⁷
13. השיפור הטכנולוגי של טכנולוגיות לזיהוי הפנים הוביל בשנים האחרונות לעלייה משמעותית בשימוש במערכות אלה בתרחישים מגוונים. עלייה בשימוש כאמור גרמה בתורה לעלייה במוטיבציה של חברות מסחריות להשקעה ומאמץ בתחום זה⁸ ויצרה אתגרים טכנולוגיים חדשים הנוגעים בעיקר לצורך להתמודד עם הונאות, המכונות בשפה המקצועית PA (Presentation Attacks)⁹, ועם זיופים אחרים כגון זיופים מסוג Deep Fakes¹⁰. אנו סבורים שמגמת השיפור המתוארת לעיל תמשיך ותתרחב.
14. לצד השיפור הניכר ביכולות הביצוע של טכנולוגיית זיהוי פנים ישנם גורמים נוספים אשר הביאו לעליה בשימוש בטכנולוגיה, כגון: הקלות היחסית שבה ניתן ליטול תמונות פנים באיכות המאפשרת מימוש מיטבי של היישום הביומטרי תוך ביצוע השוואות בשיעורי דיוק גבוהים, והימצאותן של תמונות הפנים רבות במרחב הווירטואלי, מצב המקל גם על בניית מאגרים לצורכי השוואה או ייחוס.
15. התפתחויות אלו הביאו לעליה ניכרת בשווי הכלכלי של שוק טכנולוגיית זיהוי הפנים: בין השנים 2016-2019 הרווח העולמי עמד על 3-5 מיליארדי דולרים, וצפי הרווח לשנים 2022-2026 הוא כפול ועומד על 7-10 מיליארדי דולרים¹¹.
16. בישראל, קיימים מספר פרויקטים לאומיים בהם נעשה שימוש בזיהוי פנים באופן מבוקר. הבולטים שבהם הם פרויקט התייעוד הלאומי החכם (רשות האוכלוסין וההגירה והרשות לניהול המאגר הביומטרי), המאגרים הביומטריים המשטרתיים (חשודים, נאשמים ומורשעים), והפרויקט הביומטרי לזרים (רשות האוכלוסין)¹².
17. מתבצע שימוש בזיהוי פנים בשערים אוטומטיים בשדות התעופה (אימות מול דרכון), במערכת הבנקאית לצורך פתיחת חשבונות בנק באופן מקוון בתנאים מסוימים (במסגרת העיקרון של Electronic Know Your Customer או בקיצור EKYC), על ידי משתמשים ישראלים ברשתות החברתיות (כגון Facebook), לצורך "פתיחת" מכשירים סלולאריים ניידים, ועוד.

זיהוי פנים במרחב הציבורי

18. כאמור, זיהוי פנים במרחב הציבורי הוא יישום ביומטרי ספציפי בו נעשה צילום של תמונות הפנים של קהל בלתי מסוים המצוי במרחב הציבורי, וביצוע השוואה ביומטרית אל מול מאגר, ללא שיתוף פעולה מצד הקהל (Face Recognition of Non-Cooperative Subjects). **זיהוי פנים של אנשים בתוך קהל בלתי מסוים שאינו משתף פעולה עם תהליך הזיהוי** הוא קשה יותר ליישום מאשר זיהוי פנים באמצעות

⁷ Face Recognition: Performance, Measurement; Patrick Grother and Mei Ngan; NIST; [Biometrics Institute Workshop Sydney, AU; May 29](https://www.biometrics-institute.com/workshop-sydney-au-may-29/).

ראו פירוט נוסף בחוות הדעת הממונה על היישומים הביומטריים לפי סעיף 2ב לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים באמצעי זיהוי ובמאגר מידע התשי"ע-2009, מיום 27.5.2020 https://fs.knesset.gov.il/23/Committees/23_cs_bg_584569.pdf

תקן ICAO הוא תקן בינ"ל בתחום התעופה הקובע את אופן הצילום עבור דרכונים/מסמכי תיעוד לאומי.
⁸ דוגמאות למספר זירות שבהן מושקעים משאבים משמעותיים בטכנולוגיות לזיהוי פנים הן טלפונים חכמים, רשתות החברתיות ותחום הפינטק.

⁹ הצגת מצגי שווא למערכת, במטרה לגרום לשיבוש התהליך הביומטרי. אם מדובר במערכת לזיהוי פנים, התקפה כזו יכולה להיות הצגת תמונה מודפסת, לבישת מסכה וכיו"ב.

¹⁰ סנתוז תמונות פנים או קטעי וידאו מזויפים באמצעות עיבוד ממוחשב מבוסס בינה מלאכותית.
¹¹ United States Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses", July 2020 - <https://www.gao.gov/products/gao-20-522>

¹² ראו פירוט בדו"ח מרכז המחקר והמידע של הכנסת, ה"ש 2. פרויקטים אלה מוסדרים בחקיקה ראשית, למעט פרויקט הביומטריה לזרים, אשר לגביו פורסם תזכיר חקיקה אשר טרם נדון בכנסת.

שימוש בתמונות פנים מבוקרות. שיעורי הדיוק של מערכות לזיהוי פנים במרחב הציבורי הם נמוכים יותר, שכן מערכות אלה מתמודדות עם תזוזה של אנשים, הסתרות, צילום בזווית שונות, תנאים סביבתיים משתנים (מזג אויר, תאורה ועוד), המביאים לתמונות פנים באיכות משתנה ונמוכה ("Faces in the Wild")¹³.

19. בעת הפעלת יישומי זיהוי פנים במרחב הציבורי מצלמים בוודא את העוברים והשבים, אוגרים את תמונות פנים באופן קבוע או זמני, ומשווים תמונות אלה לרשימת "מוכללים"¹⁴ או למאגר אחר. עשויים להיות מקרים בהם נעשה צילום במרחב הציבורי ללא הפעלה מיידית של יכולת השוואה ביומטרית ("בזמן אמת"), אולם יש באגירת צילומים אלה כדי לאפשר בהמשך ביצוע השוואה ביומטרית, בדיעבד.
20. בעולם נעשה שימוש בזיהוי פנים במרחב הציבורי במספר מקומות ומתארים, כגון שדות תעופה לצורך "ניהול נוסע"¹⁵, מגרשי כדורגל ואירועי ספורט גדולים אחרים¹⁶, בהפגנות¹⁷ ועוד. השימוש נעשה על ידי גורמי האכיפה והביטחון בעולם¹⁸, על ידי רשויות מקומיות ("ערים חכמות")¹⁹, וכן עשוי לשמש גם לצרכים מסחריים שונים, לצורך זיהוי לקוח בבית עסק לשם הצעת מוצרים או מבצעים²⁰.
21. בהקשר מגפת הקורונה, קיימות ידיעות לפיהן ברוסיה נעשה שימוש נרחב בזיהוי פנים במרחב הציבורי לשם איתור מפרי בידוד, לרבות שימוש ב"רשימת מוכללים"²¹ וכן ידיעות דומות לגבי סין (תוך שילוב יכולת מדידת חום)²².
22. להתרשמותנו, במרחב הציבורי בישראל השימוש באמצעי זיהוי פנים מול קהל בלתי מסוים בעת הנוכחית²³, נעשה בהיקף נמוך יותר ביחס לנעשה בחו"ל בכלל ובמדינות המערב בפרט, בעת הנוכחית.

¹³ דו"ח מכון התקנים האמריקאי מ-2017 המציג את האתגרים בזיהוי פנים מול קהל שאינו משתף פעולה המצולם בוודא על ידי מצלמות מעקב- https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST_IR_8173.pdf

¹⁴ בתרחיש בטחוני רשימת מוכללים (watchlist) היא רשימת ישויות המהוות גורמי עניין כגון- חשודים, פעילי טרור וכיו"ב, המבוקשים על ידי כוחות האכיפה.

¹⁵ זיהוי הנוסע בשדה התעופה מהגעתו לשדה ועד ההמראה, בתחנות רלוונטיות. השימוש בזיהוי פנים בתרחיש זה נעשה לצרכים ביטחוניים ולצרכי שירות.

¹⁶ למשל, פרישת מערכת לזיהוי פנים עבור המשחקים האולימפיים בטוקיו 2020- <https://www.theverge.com/2018/8/7/17659746/tokyo-2020-olympic-games-face-recognition-nec>

¹⁷ ראו מחאת המפגינים בהונג קונג וניסיונות לשבש את שימוש גורמי האכיפה בזיהוי פנים- <https://www.diyphotography.net/hong-kong-protesters-are-using-laser-pointers-to-confuse-facial-recognition-and-theyre-frying-photographers-camera-sensors/>

¹⁸ מצלמות פנים משמשות היום את הממשל הסיני בהיקף משמעותי. ראו לדוגמה דיווח של ה-BBC, שלפיו פרושות היום בסין למעלה מ-170 מיליון מצלמות במרחב הציבורי: <https://www.bbc.com/news/world-asia-china-43751276> ; כתבה המתארת את השימוש הגובר של משטרת גרמניה במערכות לזיהוי פנים לשם השוואה 1: <https://digit.site36.net/2021/01/20/facial-recognition-at-german-police-authorities-increased-by-more-than-a-third>

¹⁹ שימוש הנעשה על ידי גורמי אכיפה בבריטניה, מתואר להלן, וראו גם באתר משטרת וויילס <https://afr.south-wales.police.uk/>

²⁰ <https://www.planetbiometrics.com/article-details/i/8636/> ; <https://www.youtube.com/watch?v=PZKgAuk6kLM> ; <https://www.youtube.com/watch?v=bpfvloDVle0>

²¹ <https://www.bbc.com/news/av/world-europe-52157131>

²² <https://www.dw.com/en/using-facial-recognition-against-covid-19/av-53868752> ; <https://www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes> ;

²³ דוח מרכז המחקר והמידע של הכנסת- השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי (פרק 2)- https://fs.knesset.gov.il/globaldocs/MMM/2503c32b-2f94-ea11-8104-00155d0aee38/2_2503c32b-2f94-ea11-8104-00155d0aee38_11_16517.pdf

ביחס לגורמי האכיפה הוגשו לאחרונה מספר עתירות הנוגעות לשימושים במערכות לזיהוי פנים במרחב הציבורי²⁴, וכן נעשה שימוש ביכולת זו באצטדיוני ספורט²⁵. בנוסף לכך, נערך צילום במרחב הציבורי בישראל, ללא הפעלה ישירה של יישום לזיהוי פנים, על ידי רשויות מקומיות²⁶ וחברות פרטיות²⁷, מטעמי ביטחון וטעמים נוספים²⁸. יש בצילום זה פוטנציאל להפעלת יישום לזיהוי פנים בדיעבד. כמו כן, קיימות ידיעות מעטות על שימוש בזיהוי פנים במרחב ציבורי בישראל לצרכים מסחריים²⁹.

23. ככלל, השימוש בזיהוי פנים בישראל על ידי גורמי אכיפה (בפרט המשטרה) או רשויות מקומיות הוא מוגבל. יש להניח כי השימוש בטכנולוגיה זו יגדל, כחלק ממגמה עולמית, בפרט על רקע מגפת הקורונה בשל הרצון להימנע ממגע והצורך בתהליכי זיהוי מרחוק.

24. **בהקשר מגפת הקורונה**, התקיימו התנסויות בשימוש בצילום במרחב הציבורי בישראל כדי לאתר את מי שאינו עוטה מסכה ולהתריע בפניו, ללא שימוש בזיהוי פנים³⁰, או עם שימוש בזיהוי פנים³¹.

²⁴ לאחרונה הוגשו עתירות חופש מידע ביחס לשימוש בזיהוי פנים במרחב הציבורי על ידי צה"ל והמשטרה (ראו עת"ם 47229-09-20 האגודה לזכויות האזרח בישראל נ' משטרת ישראל, וכן עת"ם 46723-09-20 האגודה לזכויות האזרח בישראל נ' הממונה על יישום חוק חופש המידע בצה"ל). למען שלמות התמונה יצוין כי הוגשה עתירה בנוגע למערכת המשטרתית "עין הנץ" שמבצעת זיהוי לוחיות רישוי של רכבים: בג"ץ 641/21 האגודה לזכויות האזרח נ' משטרת ישראל. https://01368b10-57e4-4138-acc3-01373134d221.usrfiles.com/ugd/01368b_0cb9878b629f405a8368cea5e9493927.pdf

²⁵ מצלמות לזיהוי פנים באצטדיון סמי עופר (2014) - <https://www.one.co.il/article/235161.html>

מצלמות לזיהוי פנים באצטדיון נתניה - <https://www.netanya.muni.il/?CategoryID=2524&ArticleID=5698>

מצלמות לזיהוי פנים באצטדיון טדי (2017) - <https://www.globes.co.il/news/article.aspx?did=1001197890>

²⁶ תכנית עיר ללא אלימות- משרד העבודה, הרווחה והשירותים החברתיים- <https://www.gov.il/he/Departments/General/molisa-community-innterventions-city-without-violence> ; כתבה בעיתון הארץ- מצלמות בעיר תל אביב יפו – <https://www.haaretz.co.il/news/education/premium-MAGAZINE-1.8445403> ; דוח מרכז המחקר והמידע של הכנסת- השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי (פרק 3) - https://fs.knesset.gov.il/globaldocs/MMM/2503c32b-2f94-ea11-8104-00155d0aee38/2_2503c32b-2f94-ea11-8104-00155d0aee38_11_16517.pdf

²⁷ שימוש בזיהוי פנים לצורך פתיחת קורקינט שיתופי של חברת WIND - <https://www.themarker.com/technation/premium-1.9233134>

²⁸ כתבה בערוץ 12 - https://www.mako.co.il/news-channel2/Channel-2-Newscast-q3_2019/Article-3b43a949840bc61027.htm?Partner=searchResults ; אתר החברה - <http://wise-sight.com/> ;

²⁹ רשת ויקטוריה הפעילה פיילוט של מצלמות העוקבות אחר התגובות הרגשיות של הלקוחות למוצרים בסניף- <https://m.calcalist.co.il/Article.aspx?guid=3846114>

³⁰ במאי 2020 הותקנה מערכת לזיהוי עטיית מסכות במספר בתי חולים בישראל, ביניהם בבית החולים שיבא- <https://www.globes.co.il/news/article.aspx?did=1001328104> ; <https://www.israelhayom.co.il/article/760909>

³¹ פיילוט מערכת לזיהוי פנים ומדידת חום בכניסה לבית החולים בני ציון <https://www.ynet.co.il/articles/0,7340,L-5716252,00.html>

קריאה לאסדרה

הסיכונים הכרוכים בשימוש בזיהוי פנים במרחב הציבורי

נפרט להלן את הסיכונים המרכזיים הכרוכים בשימוש באמצעי זיהוי פנים במרחב הציבורי (סיכונים אלה קיימים גם במערכות מבוקרות, אולם בעצימות נמוכה יותר).

25. הטרדת תמימים בשל שגיאות וכשלים של אמצעי זיהוי פנים - ניהול מערכת ליישום ביומטרי היא משימה מורכבת, שכן גורמים סביבתיים וחיצוניים רבים עשויים להשפיע על הצלחתה. ביצוע כושל של המערכת עלול להביא לזיהוי שגוי והטרדת אנשים תמימים (FPIR), ומנגד עלול לגרום להחמצת זיהוי חשודים (FNIR)³².

כישלון זה יכול להתרחש בשל מספר סיבות, ובכלל זה קביעת סף נמוך מדי להתאמה, בדיקה בלתי מיומנת של תוצרי המערכת, אינטגרציה לקויה של רכיבי המערכת או בחירה שגויה של רכיבים, הצבה לא נכונה של מצלמות, מאפיינים מיוחדים של קהל היעד שלא נלקחו בחשבון, הטיות דמוגרפיות של האלגוריתם ועוד. כלומר, לא די בקביעת גבולות "מנהליים" ויישום מידתי שלהם, אלא נדרשת **הטמעה טכנולוגית** נכונה של מערכת לזיהוי פנים, שכן קיימים מקרים בהם היישום בפועל כשל בשל הטמעה טכנולוגית שגויה³³.

למותר לציין כי זיהוי שגוי של תמימים יכול להוביל לפגיעה קשה בזכויותיהם, כתלות בתכלית המערכת³⁴.

26. מעקב, פגיעה פרטיות ו-"תחושת מעקב" - כאמור, זיהוי פנים במרחב הציבורי משמש היום בעולם בין היתר למטרות "ניהול הסדר הציבורי" באצטדיוני ספורט, הופעות, הפגנות, אזורים "מועדים" לפורענות ועוד. כמו כן אמצעי זיהוי פנים במרחב הציבורי עשויים לשמש לצרכים מסחריים, כגון איתור לקוחות VIP ו"טירגוט" אישי שלהם לצורך פרסומות או מבצעים. פרקטיקה זו עשויה להביא לאגירת יתר של תמונות פנים של אנשים רבים, אשר יתועדו במקומות שונים, באופן שעלול לשמש למעקב אחריהם, תיעוד תנועותיהם, תיעוד עמדתם הפוליטית (השתתפות בהפגנה למשל) והרגלי הצריכה שלהם, ובין היתר מהווה גורם ממשמע וממסטר של האוכלוסייה. בכך עשויה להיפגע הפרטיות, תחושת החירות של האדם וחופש הביטוי שלו בשל האפקט המצנן, כתוצר של מעקב מסוג זה. יתר על כן, קיים חשש כי המידע הביומטרי עצמו ישמש גם למטרות נוספות אשר לא נקבעו או הובהרו מראש ("זליגת שימושים").

27. דליפת המידע ושימוש לרעה על ידי בלתי מורשים - דליפת מידע ביומטרי ממאגרים המשמשים זיהוי פנים במרחב הציבורי עשויה להביא לשימוש לרעה בכלים ויכולות בידי גורמים בלתי מורשים וללא פיקוח ובקרה אפקטיביים. התממשות סיכון זה תביא לפגיעה בפרטיות כמפורט לעיל, ו/או לפגיעה

³² FPIR- False Positive Identification Rate ; FNIR- False Negative Identification Rate
³³ כתבה ב BBC המתארת מערכת לזיהוי פנים במרחב הציבורי בה נעשה שימוש בבריטניה בה שיעורי התראות השווא עמד על כ 90% <https://www.bbc.com/news/technology-44089161>
³⁴ למשל, משטרת ניו ג'רזי עצרה אדם חף מפשע מאחורי סורג ובריח למשך של 10 ימים בשל טעות בזיהוי של מערכת זיהוי פנים : <https://futurism.com/lawsuit-claims-facial-recognition-ai-sent-wrong-man-jail> ;
כתבה ב' 60 minutes על זיהוי שגוי של מנוע לזיהוי פנים שהוביל לעצר אדם חף מפשע-
<https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16>
מקרה נוסף בו דווח על זיהוי שגוי של אדם-
<https://www.law.com/njlawjournal/2021/01/15/rise-of-the-machines-facial-recognition-technology-heralds-upswing-in-litigation/?slreturn=20210109042210>

באינטרסים נוספים, לרבות ביטחוניים (למשל, באמצעות איסוף מודיעין, מעקב אחר יעדים ועוד) ובריונות רשת (למשל Deepfake).

28. ריבוי השימוש בטכנולוגיה לזיהוי פנים, האפשרות ליטול אמצעי ביומטרי ללא ידיעת אדם בצילום פשוט, והימצאות תמונות פנים במאגרים גדולים ונגישים יחסית – מגבירים ביתר שאת את הסיכונים שנמנו לעיל.

אסדרת השימוש באמצעי זיהוי פנים במרחב הציבורי בעולם

29. עקב חששות המתעוררים מהשימוש בזיהוי פנים במרחב הציבורי, התרחב בתקופה האחרונה השיח הציבורי בעולם המערבי בנושא זה – במסגרת דיוני פרלמנט בממשלות שונות, פרסומים עיתונאיים, גילויי דעת של ארגוני המגזר השלישי ואף על ידי החברות המסחריות עצמן.

להלן מספר דוגמאות לתהליכי חקיקה בעולם העוסקים בזיהוי פנים במרחב הציבורי (פירוט נוסף מופיע בדו"ח מקיף יותר מאת מכון יובל נאמן באוניברסיטת תל אביב, המצורף למסמך זה):

30. **בארה"ב** הוצעו הצעות חוק רבות, ברמה המקומית, המדינתית והפדרלית, בתחום זיהוי הפנים באופן ככלי וזיהוי פנים במרחב הציבורי בפרט.

מדינת אילינוי היא הראשונה בארה"ב שעסקה באסדרת תחום הביומטריה באופן כללי, בחקיקה משנת 2008, אולם חקיקה זו אינה עוסקת ספציפית בזיהוי פנים במרחב הציבורי³⁵.

עשור לאחר מכן, בחודש מאי 2019, אושרה הצעת חוק בסן פרנסיסקו, לפיה נאסר השימוש בטכנולוגיות זיהוי פנים במרחב הציבורי על ידי מוסדות העירייה³⁶. בחודש ספטמבר 2020, אימצה העיר פורטלנד את החוקים הנוקשים ביותר בארה"ב בנושא זיהוי הפנים³⁷, כאשר אסרה כל שימוש פרטי, או ממשלתי בטכנולוגיה לזיהוי פנים.

במדינת וושינגטון קיימת פעילות חקיקתית רבה שנועדה להסדיר את השימוש באמצעי זיהוי פנים, כולל זיהוי המתבצע במרחב הציבורי. החל משנת 2019 הוגשו תשע (!) הצעות חוק שעוסקות בנושא. כיום, ישנם שלושה חוקים המתייחסים לאיסוף ביומטריה ולזיהוי פנים במרחב הציבורי במדינת וושינגטון, כששניים מהם (HB.1717³⁸ ו-SB.6280³⁹) חלים על גופי ממשל מדינתיים ומקומיים ואחד (HB.1493⁴⁰) על המגזר הפרטי.

חוק SB 6280 ("AN ACT Relating to the use of facial recognition services") מתייחס להפעלת יישומים לזיהוי פנים על ידי סוכנויות ממשלתיות, ובפרט מתייחס לזיהוי פנים במרחב הציבורי. הוא קובע, בין היתר, כי לא יעשה שימוש בזיהוי פנים למעקב מתמשך, אלא אם מדובר בעבירות חמורות ובכפוף להוצאת צו שיפוטי שיתיר זאת (במקרים בהולים ניתן יהיה לפעול באישור ראש הסוכנות, ובתנאי להוצאת צו תוך 48 שעות). כמו כן, קובע החוק חובת ניהול קפדני של מערכות אלה, לרבות התייחסות לשיעורי השגיאה שלה, הטיה אפשרית של האלגוריתם, אמצעי הביטחון הננקטים, ביקורת על ידי צד שלישי למערכת, סקר השפעה על פגיעה בזכויות (ועוד) וכן חובת הגשה של דוחות ציבוריים

³⁵ The Illinois Biometric Information Privacy Act ("BIPA")

³⁶ <https://www.wired.com/story/san-francisco-could-be-first-ban-facial-recognition-tech/>

³⁷ <https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/facial-recognition-and-the-us-capitol-insurrection>

³⁸ <https://app.leg.wa.gov/billsummary?BillNumber=1717&Year=2017>

³⁹ <https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false>

⁴⁰ <https://app.leg.wa.gov/billsummary?BillNumber=1493&Year=2021&Initiative=false>

המפרטים על המערכות המופעלות לרשות המחוקקת, ופרסומם לציבור. כמו כן, קובע החוק כי תתקיים ביקורת בתוך הרשות השופטת בדבר צווים שניתנו לשימוש בזיהוי פנים, ובדבר בקשות שנדחו. החוק מוסיף וקובע את הקמתו של "כוח משימה" המורכב מנציגים שונים (ממשל, אקדמיה, תעשייה, מגזר שלישי), ואשר תפקידו לפרסם המלצות להתמודדות עם האיומים הנשקפים מהשימוש בטכנולוגיית זיהוי פנים; בחינת יעילות החוקים הקיימים במדינה בנושא; ובחינת האיכות, הדיוק והיעילות של שירותי זיהוי פנים בשנתיים האחרונות הוצעו ואושרו חוקים בנושא זה במדינות נוספות, וכן הוצעו חוקים בסנאט האמריקאי⁴¹, אך טרם הגיעו לכדי אישור.

31. **בבריטניה** לא קיימת חקיקה ייעודית לזיהוי פנים במרחב הציבורי, אולם הנושא הגיע לדיונים ודוחו"ת פרלמנטריים, וניתנה לגביו התייחסות על ידי מספר בעלי תפקיד ובראשם הממונה על הביומטריה ומצלמות המעקב⁴². ההקשר המרכזי בו נדון נושא זה בבריטניה הוא השימוש על ידי גורמי האכיפה במרחב הציבורי. נושא זה הגיע לדיונים בערכאות משפטיות⁴³ בפסק הדין של בית המשפט האזורי בערכאות הערער, אשר עסק בהפעלת אמצעי זיהוי פנים מול קהל על ידי משטרת וויילס שם, התקבלו חלק מטענות של העותר ונקבע כי במסגרת המשפטית הכללית הקיימת בבריטניה חסר מענה הולם לשתי שאלות חשובות: אילו אנשים מוכללים ברשימות המעקב והיכן ניתן לפרוס את מערכת הזיהוי. בית המשפט הוסיף וקבע כי במצב זה, לקציני המשטרה בשטח נתון מרחב גדול מדי לשיקול דעת וכי הערכת הסיכונים לחירויות האזרח שהמשטרה ביצעה לגבי השימוש במערכות לזיהוי פנים לא הייתה מספקת. חשוב לציין כי בית המשפט לא אסר באופן גורף על הפעלת הטכנולוגיה כאמור, אלא הדגיש את החשיבות של הפעלתה באופן מידתי והכפיף אותה להגבלות מסוימות.

32. בתחילת שנת 2020 הודיע **האיחוד האירופי** כי הוא שוקל איסור לשימוש בזיהוי פנים במרחב הציבורי למשך פרק זמן של 5 שנים, אולם לאחר מכן חזר בו והדגיש את הצורך בקריטריונים ברורים בנושא⁴⁴. **באפריל 2021 הוצעה המסגרת החוקית**⁴⁵ הראשונה **שמתייחסת לסיכונים שבשימוש ב AI**, בכלל זה בשימוש בזיהוי פנים במרחב הציבורי (RBI Systems- Remote Biometric Identification systems), ובתפקיד שעל האיחוד האירופי למלא בנושא זה. ההצעה נועדה להבטיח כי שימוש במערכות AI באיחוד האירופי יעשה באופן בטוח, שקוף, אתי, בלתי מוטה ותחת בקרה אנושית.

The Facial Recognition and Biometric Technology Moratorium Act-⁴¹ <https://www.markey.senate.gov/imo/media/doc/acial%20Recognition%20and%20Biometric%20Technology%20Moratorium%20Act.pdf> ;

Ethical Use of Facial Recognition Act- <https://www.congress.gov/bill/116th-congress/senate-bill/3284/text> עד 2021 היו בבריטניה רגולטורים נפרדים לביומטריה ומצלמות מעקב, אולם תפקיד זה אוחד. דוחו"ת בעלי תפקיד אלה פורסמו בנושא זיהוי פנים במרחב הציבורי :

בנובמבר 2020 פרסם הממונה על מצלמות המעקב מסמך קווים מנחים ושיטת עבודה מומלצת לשימוש המשטרה במצלמות מעקב הכוללות זיהוי פנים במרחב הציבורי⁴², לאיתור חשודים ברשימות מעקב.

<https://www.gov.uk/government/publications/police-use-of-automated-facial-recognition-technology-with-surveillance-camera-systems>

הממונה מאמין כי **יש לתת הרשאה** לשימוש בזיהוי פנים באופן יחי (LFR) לצורכי המשטרה, אך **נדרש לכך פיקוח דרך חקיקה**. בנוסף אמר כי על הפרלמנט להחליט האם יש לאפשר שימוש בטכנולוגיות לזיהוי פנים באופן יחי למשטרה ולאילו שימושים. <https://www.gov.uk/government/news/biometrics-commissioner-on-the-police-use-of-live-facial-recognition>

<https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/>⁴³

<https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q>⁴⁴

<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>⁴⁵

לפי הצעת רגולציה זו, אסור לרשויות האכיפה להשתמש במערכות ביומטריות לצורכי זיהוי מרחוק בזמן אמת' במרחב הציבורי, אלא במקרים הכרחיים ולמטרות מסוימות: חיפוש ממוקד למציאת קורבנות פשע (לדוגמה מציאת קטינים נעדרים); התמודדות עם מצבי חירום הנוגעים לביטחון הציבור ומניעת מתקפת טרור; או איתור וזיהוי נאשם שיש להעמידו לדין בגין פשעים חמורים⁴⁶.

גם באותם במקרים חריגים אלה יש לקחת בחשבון את נסיבות האירוע, פוטנציאל הנזק וההשלכות האפשריות על זכויות הפרט. כמו כן, מקרים ייחודיים אלו יוסדרו באופן שיגביל את משך הזמן, האזור הגיאוגרפי ומערכי הנתונים בהם יעשה שימוש במערכת.

זאת ועוד, הצעת הרגולציה קובעת כי מערכות ביומטריות הפועלות מרחוק (RBI) ב'זמן אמת' (real-time), או בסמוך לזמן אמת (post) לזיהוי בני אדם הן מערכות בעלות סיכון גבוה, ולכן הן נדרשות לעבור בדיקה והערכה לשם אישור על ידי צד שלישי (בית משפט, או רשות עצמאית), בטרם ההפצה וההטמעה. בית המשפט, או הרשות יאשרו שימוש כאמור רק לאחר בחינת ראיות אובייקטיביות, או אינדיקציה ברורה שהמערכת נחוצה ומידתית, לשם אחד משלוש התכליות האמורות ותוך בחינת השיקולים שלעיל.

לגבי מערכות אלה, הצעת הרגולציה דורשת שיבוצעו ניהול סיכונים ובקרה עתית, בשל הסיכון הגבוה במיוחד להפרת זכויות בסיסיות בעת השימוש בהן. כמו כן מתייחסת ההצעה לצורך באימות ותיקוף הנתונים והקפדה על דיוק ממצאיה (דגש על מניעת הטיה), שילוב בקרה אנושית בתהליך קבלת ההחלטות, תיעוד ורישום פעולות המערכת, שקיפות, חוסן והגנת סייבר, הוראות הנוגעות לספקים והמפתחים, עיצומים כספיים שיוטלו במקרה של הפרה, ועוד.

33. **חברות מסחריות** התייחסו לנושא זה במספר הזדמנויות. בחודש יוני 2020 בעקבות ביקורת ציבורית, הודיעו שורה של חברות גדולות כי יגבילו את שימוש המטרה ורשויות החוק במערכות לזיהוי פנים, ביניהם חברת IBM שהודיעה כי תפסיק להציע, לייצר ולחקור טכנולוגיה לזיהוי פנים⁴⁷. באותה העת, הודיעה חברת מייקרוסופט כי תפסיק לספק את טכנולוגיית זיהוי הפנים שלה למטרה, עד לחקיקה בנושא⁴⁸. כמו כן, בחודש מאי 2021 הודיעה חברת אמזון כי לא תספק את טכנולוגיית זיהוי הפנים שלה למטרה, עד להודעה חדשה⁴⁹, בהמשך להודעה מטעמה בחודש יוני 2020 על השעיית פעילותה בנושא זה למשך שנה⁵⁰.

Article 5(d)⁴⁶
<https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software>;
<https://www.bbc.com/news/technology-52978191>
<https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/>⁴⁸
<https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/>⁴⁹
<https://news.sky.com/story/amazon-pauses-police-use-of-facial-recognition-technology-for-a-year-due-to-lack-of-laws-12004598>;
<https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/>⁵⁰

עקרונות מדיניות – שימוש באמצעי זיהוי פנים במרחב הציבורי בישראל

34. כפי שמצוין בדו"ח של מרכז המחקר של הכנסת (עמודים 7, 10), "אין מדיניות כוללת וסדורה ביחס לפריסה של יכולות ניטור וניתוח וידאו" וכן "אין חקיקה ספציפית המסדירה באופן קונקרטי מטרות לגיטימיות לשימוש בטכנולוגיות ניטור מתקדמות כגון זיהוי פנים".
- העדר מדיניות ואסדרה רוחבית של הנושא, מביאה ליצירת עובדות בשטח ללא פיקוח או הכוונה מחד, ומאידיך, מביאה לקבלת החלטות או הכרעות שיפוטיות אד-הוק, ללא הסתכלות רחבה על התמונה בכללותה.
35. הממונה על היישומים הביומטריים במערך הסייבר הלאומי סבור כי לאור השיפור הדרמטי בשיעור הדיוק של טכנולוגיית זיהוי הפנים, ונוכח הסיכונים הטמונים במימוש טכנולוגיה לזיהוי פנים במרחב הציבורי, יש לאסדר נושא זה. ראוי שהאסדרה שתהיה כזו שתאפשר מימוש מדוד של יכולות אלו לצורך מטרות לגיטימיות, תוך מתן דגש לאיזונים והבלמים הנדרשים לנוכח הרגישות הרבה, הסיכונים, ופוטנציאל הנזק.
36. להלן יפורטו הנושאים המרכזיים אליהם יש להתייחס בעת גיבוש מדיניות לאומית לזיהוי פנים במרחב הציבורי ואשר צריכים לשמש בסיס לאסדרה בחקיקה ראשית. העקרונות שלהלן מבוססים על המדיניות הלאומיים ליישומים ביומטריים וכן על סקירה משווה שהתייחסה לנושאים אלה כפי שבאו לידי ביטוי בתהליכי אסדרה בעולם המערבי.

שאלת לגיטימיות המטרה

בתהליך גיבוש מדיניות יש לבחון האם לגיטימי להפעיל יכולת לזיהוי פנים במרחב הציבורי ואם כן, באלו נסיבות.

מסקירת הנעשה בעולם, עולה כי קיימים תרחישים בהם שימוש מגודר במערכות לזיהוי פנים במרחב הציבורי הוא לגיטימי (דוגמת מניעת מתקפת טרור⁵¹) ומנגד, קיימים תרחישים לגביהם יש סימן שאלה⁵² (הפעלת היכולת באזור מאופיין בריכוז גבוה של קטינים כגון בחצר בית הספר⁵³).

לאור האמור לעיל נראה כי שימושים של זיהוי פנים במרחב הציבורי, בנסיבות מסוימות, הינם לגיטימיים, ומכאן הצורך לגבש עקרונות מדיניות אשר יגדרו ויסדירו את אופן הביצוע.

עקרון צמידות המטרה

צילום וזיהוי פנים במרחב הציבורי ייעשה למטרה ממוקדת, ובהתאם לביסוס החוקי. תוך הקפדה, לאורך זמן, כי הביצוע נעשה בהתאם לתכלית המקורית שנקבעה ולא מתקיימת זליגת שימושים.

⁵¹ ראו הצעת הרגולציה ל-AI של האיחוד האירופי, ה"ש 43

⁵² לפי הצעת החוק של האיחוד האירופי (ראו סעיף 31), מערכות המוגדרות כבעלות סיכון גבוהה הן מערכת לזיהוי וסיווג ביומטרי של בני אדם שאינן פועלות מרחוק (remote), ו/או שאינן בזמן אמת (real-time), או בסמוך לזמן אמת (post).

⁵³ ראו לדוגמה את התייחסות הממונה על מצלמות המעקב בבריטניה לנושא, במסמך הקווים המנחים לשימוש המשטרה בזיהוי פנים במרחב הציבורי - <https://bit.ly/3oUS1V3>
נוסף על כך, עיבוד מידע של ילדים הוא אחד מהמקרים המצריך ביצוע הערכת השפעות (DPIA), בהתאם לחוק ההגנה על המידע משנת 2018 בבריטניה - <https://bit.ly/2Ks8Uri>

עקרון המידתיות

השימוש בצילום או זיהוי פנים במרחב הציבורי ייעשה באופן המבטיח איזון בין הצורך והיתרון בשימוש בתהליכים אלה ובין הפגיעה הפוטנציאלית בזכויות אדם ובפרטיות. כך למשל, הצעת הרגולציה של האיחוד האירופי קובעת כי בעת השימוש במערכות לזיהוי פנים על ידי רשויות האכיפה בזמן אמת צריך להביא בחשבון מספר שיקולים, כגון חומרת הפגיעה האפשרית שתיגרם בשל אי שימוש במערכת, הסתברות הפגיעה והיקפה, וכן את השלכות השימוש על זכויות וחירויות. בהקשר זה נכון לבחון את מסגרת הזמנים שבה המערכת מופעלת, היקף השטח המצולם, מאפייני האתר המצולם, היקף האוכלוסייה, סוג האוכלוסייה שבמקום (למשל צילום קטינים בבית ספר), משך הזמן בו נשמר המידע וכיו"ב.

עקרון האחרייות

ההחלטה על שימוש בזיהוי פנים במרחב הציבורי או צילום במרחב הציבורי נדרשת להישען על ניתוח מקדים שיעשה בגוף המחליט ויתועד על ידו. תיעוד הניתוח יכול שיקלט חלופות לעצם השימוש ביישום כזה, כולל ניתוח היתרונות אל מול הסיכונים הכרוכים בכך, לרבות בהתחשב בשיקולי פרטיות ועיצוב לאבטחה.

יודגש כי בחירה בשימוש המערכת ע"י חברה במיקור חוץ אינה מסירה את אחרייות הגוף המנהל לגבי הפעלת יישום זה.

עקרון האחרייות מכתוב גם את החובה לנהל באופן תקין את המערכות הביומטריות, ולבצע בקרה שוטפת על כך.

עקרון הניהול תקין של מערכות ביומטריות

בעת תכנון המערכת ופריסתה בשטח יש לקחת בחשבון פרמטרים טכנולוגיים, תנאים סביבתיים וגורמים נוספים, העשויים להשפיע על הפעלתה התקינה ועל תהליכי ההשוואה הביומטרית. בכלל זה, יש להבטיח שימוש ללא אפליה (למשל על רקע אתני, מגדרי וכו') באופן שווה בקרב הציבור לרבות ביחס לנסיבות בהן היישום מופעל, קבלת ההחלטות והטיה באופן הפעלתו. הפעלה שאינה תקינה תביא לשיעורי שגיאה גבוהים ולטעויות בזיהוי, אשר עלולה להביא לפגיעה ולהטרדה של תמימים (לרבות החשדת שווא), ולאי עמידה במטרות המערכת עד כדי כישלון המימוש. קיימת חשיבות לבדיקות שיבוצעו על ידי גורמים אובייקטיביים, אשר יעידו על עמידה בסטנדרטיים נאותים.

בנספח הטכנולוגי המצורף למסמך זה נמצא פירוט על היבטים אלה עליהם יש לתת דגש בעת פריסה של מערכת לזיהוי פנים במרחב הציבורי.

עקרון הבקרה והפיקוח

נדרש להגדיר אם שימוש במערכות לזיהוי פנים במרחב הציבורי דורש אישור מראש של גורם חיצוני נוסף, ואם כן באילו נסיבות ומיהו אותו גורם. יש לקיים תהליכי בקרה ופיקוח שוטפים מתאימים על הפעלת מערכת לזיהוי פנים במרחב הציבורי, לרבות בתחום הגנת המידע והסייבר, על ידי גוף בלתי תלוי, בפרט כאשר יש בה כדי להשפיע על זכויותיו של אדם באופן משמעותי.

עקרון הגנת הסייבר על המידע

צילום וזיהוי פנים במרחב הציבורי ייעשה תוך שימוש במערכות מאובטחות ומהימנות המקנות רמה נדרשת של הגנת סייבר, להתמודדות עם סיכוני דליפת מידע, שיבוש מידע או שימוש על ידי גורמים בלתי מורשים. קיימת חשיבות לתכנון מאובטח של מערכות האלה, תוך שימוש בכלי אבטחה מתאימים למניעת מימוש האיומים האמורים, והקפדה על תהליכי בקרה שוטפים הן בהקמת המערכת והן בהמשך מעגל החיים שלה.

בנספח הטכנולוגי המצורף למסמך זה נמצא פירוט על היבטים אלה עליהם יש לתת דגש בעת פריסה של מערכת לזיהוי פנים במרחב הציבורי.

עקרון צמצום המידע

יש לצמצם ככל שניתן את המידע הביומטרי הנאסף והנשמר. אין לשמור מידע עודף אשר לא נדרש להשגת המטרה ויש לפעול למחיקת המידע הנאסף במועד המוקדם ביותר האפשרי לאחר עיבודו. עקרון זה יש לאזן למול הצורך בניהול תקין הכולל איסוף מידע איכותי שיאפשר שיעור שגיאות נמוך וימנע הטרדת תמימים וכן למול צורך אפשרי בשמירת ראיות בשל הוראות הדין.

עקרון השקיפות

גורם המפעיל מערכת מסוג זה יביא לידיעת הציבור הרלבנטי מידע על כך בהתאם לנסיבות ולהקשר בדרכים אפקטיביות ויפרט אודות המערכת והיקפי פעילותה או פניות אחרות של הציבור בנושא זה, וכל זאת תוך איזון עם שיקולי ביטחון והגנה על אמצעים ושיטות. עשויים להיות חריגים לכלל זה, מטעמי ביטחון.

עקרון שיתוף המידע עם צד שלישי

נקודת המוצא היא שאין לשתף עם צד שלישי את המידע הנאגר בצילום במרחב הציבורי, בפרט ביחס למידע ביומטרי. העברה כאמור יכולה להיעשות לצד שלישי רק בהסכמה מפורשת של המצולם או בכפוף לדין ולשיקולים ביטחוניים.

מודעות, הדרכה והטמעה של נושא הגנת הפרטיות והשפעה על זכויות האדם

גוף המנהל מערכת לזיהוי פנים במרחב הציבורי לקיים פעילויות הדרכה בנושא הגנת הפרטיות והשפעה על זכויות אדם אחרות בקרב העוסקים במימוש זיהוי פנים במרחב הציבורי (גורמי תמיכה, שירות וכו').

סיכום

37. בשנים האחרונות חל שיפור דרמטי בדיוק של טכנולוגיה לזיהוי הפנים - פי 100 במהלך העשור האחרון. שיפור זה, יחד עם פריסה נרחבת של מצלמות אבטחה ואחרות במרחב הציבורי מאפשר, טכנולוגית, לבצע זיהוי פנים במרחב הציבורי בהיקפים משמעותיים, הגדלים משנה לשנה.
38. עם זאת, כיום, לא קיימת בישראל מדיניות כוללת וסדורה בישראל או חקיקה ספציפית המסדירה שימוש בטכנולוגיות ניטור מתקדמות כגון זיהוי פנים.
39. בשל הרגישות המיוחדת של נושא זיהוי הפנים במרחב הציבורי, וההיבטים הטכנולוגיים הייחודיים, אנו סבורים כי יש לקדם אסדרה כוללת של הסוגיה, תוך קיום דיון בעקרונות שפורטו לעיל ביחד עם כלל הגורמים הרלבנטיים בממשלה ותוך קיום דיון ציבורי.

תודות

הממונה על היישומים הביומטריים מבקש להודות לעובדי מערך הסייבר הלאומי, עובדי היחידה להזדהות וליישומים ביומטריים, יועצי היחידה, אשר תרמו לעבודתו וסייעו לגיבוש ההמלצות המובאות במסמך זה:

- גב' נעמה בן צבי, רת"ח בכיר פרויקטים ביומטריים
- מר מישל שגיא, מנהל מדעי
- מר יובל שגב ראש מרכז טכנולוגיות מתקדמות
- מר זוהר בן דוד, רת"ח בכיר הנחיית תמ"ק
- מר יואב טייטלבוים, אגף מדיניות
- גב' קשת מולכו, סטודנטית (סיוע במחקר משווה)
- מר משה בוארון, מהנדס ראשי, רשב"ג, רשות האוכלוסין (יועץ)
- מר יורם אורן, יועץ
- מר אבנר בן אפרים, יועץ
- חוקרי מכון יובל נאמן, אוניברסיטת תל אביב: ד"ר גיל ברעם, אופיר הראל ועומרי וקסלר

נספח טכנולוגי**(א) עקרונות פריסת מערכת לצילום או זיהוי פנים במרחב הציבורי (היבטי סייבר):**

צילום וזיהוי פנים במרחב הציבורי ייעשה תוך שימוש במערכות מאובטחות ומהימנות המקנות רמה נדרשת של הגנת סייבר, להתמודדות עם סיכוני דליפת מידע, שיבוש מידע או שימוש על ידי גורמים בלתי מורשים. קיימת חשיבות לתכנון מאובטח של מערכות האלה, תוך שימוש בכלי אבטחה מתאימים למניעת מימוש האיומים האמורים, והקפדה על תהליכי בקרה שוטפים הן בהקמת המערכת והן בהמשך מעגל החיים שלה.

בקרה תהליכית:

- 4.1 הנהלת הגוף מחזיקה באחריות העיקרית לתהליכי קבלת ההחלטות הנוגעות לפריסת המערכת, לתכנון אמצעי ההגנה ובקרה שוטפת לאורך מחזור חייה.
- 4.2 יש לבצע בדיקות מהימנות מתאימות לגורמים המורשים.
- 4.3 יש לשקול ביצוע מבחני חדירה (PT) עיתיים לוודא את עמידות המערכת כנגד פריצה, הן מצד גורמי חוץ והן מצד משתמשי הארגון.

בקרה טכנולוגית:

- 4.4 נכון לנקוט במדיניות סיסמאות קשיחה למניעת ABUSE, וכן לעשות שימוש בהגבלה לוגית, פיזית וטכנולוגית לצורך מידור ומניעת גישה לא מורשית. ההעדפה תהיה שימוש במנגנון הזדהות חזק הכולל מספר פקטורים (MFA).
- 4.5 חשוב לעקוב וליישם את הגדרות האבטחה של היצרן, בהפעלה הראשונית ובאופן כללי, בפרט ביחס להקצאת הרשאות גישה. הרשאות גישה לצפייה, למידע הנוצר, למערכת עצמה, לרכיבי התקשורת או לאמצעי האיסוף הפזורים במרחב הציבורי תצומצם לגורמים רלוונטיים בלבד, ובאופן מינימאלי, על בסיס "צורך במידע" (NEED TO KNOW BASIS).
- 4.6 קיימת עדיפות לבידוד מערכת הצילום ברשת עצמאית או מבודלת בהקצאת VLAN ייעודי.
- 4.7 יש להעדיף לשמור את המידע הביומטרי הנאגר (הצילומים) בנפרד/במחיצה נפרדת ממידע אחר של הגוף.
- 4.8 יש לבחון הצפנת תווך התקשורת בהצפנה מסחרית חזקה. הצפנה כזו היא קריטית כאשר נעשה שימוש בתשתיות אינטרנטיות.
- 4.9 יש לדאוג לבצע עדכוני תוכנה וקושחה בהתאם להמלצות היצרן בערוצים מאובטחים, לרבות הטמעת עדכוני תוכנה במערכות ההפעלה ובמערכות התומכות ביישום הביומטרי.
- 4.10 יש לפעול להקשחה לוגית ופיזית של המערכת וכן לנקוט בתשומות למניעת גישה פיזית למצלמות (הגבהה, נעילה, בידוד וכיו"ב).
- 4.11 יש לפעול לצמצום סיכוני סייבר ביחס לשרשרת האספקה, בתהליכי התחזוקה, התמיכה והטיפול במצלמות, ולוודא כי לא ניתן להתקין על המצלמות מוצרי תוכנה צד ג' שאינם מאושרים.
- 4.12 חובה להפעיל ניטור על אופן הגישה למערכת והשימוש שנעשה בה ע"י המשתמשים. בייחוד יש לאתר אירועי שימוש לא נאותים ע"י משתמשי המערכת (ABUSE) כמו גם ניסיונות פריצה וגניבה של

המידע וזיהוי אנומליות/דפוסים חורגים מההתנהלות הרגילה. בפרויקטים רגישים יותר, נכון לשקול הוספת מערכות לשיטוי והונאה של התוקף.

(ב) עקרונות ניהול תקין של מערכת ביומטרית (היבטים ביומטריים):

בעת תכנון המערכת ופריסתה בשטח יש לקחת בחשבון פרמטרים טכנולוגיים, תנאים סביבתיים וגורמים נוספים, העשויים להשפיע על הפעלתה התקינה ועל תהליכי ההשוואה הביומטרית. אי הפעלה תקינה תביא לשיעורי שגיאה גבוהים ולטעויות בזיהוי, אשר עלולה להביא לפגיעה ולהטרדה של תמימים (לרבות החשדת שווא), ולאי עמידה במטרות המערכת עד כדי כישלון המימוש. פרמטרים טכנולוגיים אלה כוללים, בין היתר: איכות הצילום והמערכת ושמירת המידע; אופן פריסת המצלמות – מיקום, תאורה, זווית, מיקוד; איכות ההשוואה הביומטרית ותהליכים נוספים הנוגעים לעבודת המערכת.

כאשר מטמיעים תיקון או שינוי במודולים ביומטריים, יש לעשות זאת תוך היוועצות עם מומחי הביומטריה ולא להסתפק בביצוע QA בהיבטי תוכנה, כדי לוודא ששינויים לא הביאו להשפעה בלתי רצויה על ביצועי המערכת (היבטים ביומטריים), גם אם תיקוני התוכנה עובדים כשורה מבחינה תפעולית.

1. איכות הצילום והמערכת ושמירת המידע

- 1.1 יש להעדיף את הרזולוציה המינימלית הנדרשת בהתאם לתרחיש- במקרה בו מדובר על צילום שאינו מיועד לזיהוי פנים, יש להעדיף רזולוציה נמוכה יותר (פחותה באיכותה) אשר תאפשר את השגת מטרתו של היישום⁵⁴, כל עוד ניתן לעשות זאת טכנולוגית.
- 1.2 יש לקחת בחשבון את השיפור התמידי במנועי זיהוי הפנים ואת האפשרות העתידית לזהות גם ברזולוציה נמוכה כיום.
- 1.3 כאשר מדובר בצילום המיועד לזיהוי פנים, יש להחליט על רזולוציה אופטימאלית בהתחשב בצורך ב-FPIR נמוך, אשר לא יביא להתרעות שווא מרובות ולהתאמות שגויות, כמפורט להלן, על פני שיעור FNIR.
- 1.4 יש לקחת בחשבון תשתית טכנולוגית מתאימה להעברת המידע למרכז בקרה ועיבודו באופן שלא יעוות את המידע הנאסף.
- 1.5 יש להקפיד על שמירה של מקטעי התמונות הרלבנטיות (חיתוך) בהתאם לאפליקציה – Sanitization -ע"פ תקן NIST SP800-88R1. עקרון זה רלוונטי בפרט בתרחיש צילום שאינו מיועד לזיהוי פנים.

2. אופן פריסת המצלמות – מיקום, תאורה, זווית, מיקוד

- בתרחיש המיועד לצילום וזיהוי פנים:
- 2.1 יש למפות את תנאי השטח ולהבין את השפעתם על תהליכי הצילום
 - 2.2 יש להתמודד עם תנאים משתנים בשטח: תנועת מצולמים, מרחק, הסתרות, הצללות או רקע מרצד/מפריע, רמת תאורה (קרינה ישירה של השמש/חשכה), תנאי מזג אוויר שונים ולתכנן את פריסת המצלמות בהתחשב בתנאים אלה.

⁵⁴ יש להניח כי בעתיד לא יהיו מצלמות ברזולוציה נמוכה ועל כן ייתכן כי לא יהיה ניתן ליישם קו מנחה זה.

2.3. מספר המצלמות הנדרש: יש לבחון מהו המספר האופטימאלי של המצלמות אשר מחד יביאו לכיסוי תא השטח הרלוונטי ומאידך לא ייאסף מידע עודף שאינו נדרש ו/או אף מעמיס על המערכת.

2.4. יש לבחון מהו המרחק אליו מתמקדת המצלמה, ולהגדיר את השטח המצולם ושדה הראיה האופטימאלי, אשר מחד יאפשרו את איסוף המידע הרלוונטי ומאידך לא יביאו לאיסוף מידע עודף שאינו נדרש.

3. איכות השוואה הביומטרית ועבודת המערכת

העקרונות שלהלן יהיו בעלי חשיבות גבוהה יותר ככל שמדובר בתרחיש רגיש/בטחוני ובעל השפעה על זכויות אדם:

3.1. יש לבחור במנוע זיהוי פנים (אלגוריתמיקה) בעל ביצועים גבוהים, כאשר בנושא זה יש להעדיף הסתמכות על בדיקה מקצועית של צד ג' (כגון מבדקי NIST). ככל שהתרחיש רגיש יותר, רצוי לעשות שימוש בשני מנועי השוואה שונים, ולאחד בין תוצאותיהם בשיטת FUSION, למשל שימוש במנוע השוואה "קלאסי" ומנוע השוואה DCNN (מבוסס בינה מלאכותית).

3.2. בתרחיש של איתור חשודים יש לשאוף ל-FPIR נמוך ככל האפשר באופן שמאזן בין הצורך התפעולי לבין הצורך להקטין את שיעור התרעות השווא, שתגרומנה ל"הטרדת תמימים" (כלומר, שתקבע התאמה שגויה לרשימת המוכללים).

3.3. יש לבצע בקרה על שיעורי הדיקוק של המערכת ולבצע כיוול ספים באופן עיתי, לפחות פעם בשנה.

3.4. יש לשאוף להכללת תמונות איכותיות ככל הניתן ברשימת המוכללים watchlist, בתרחיש שבו הרשימה נוצרת בצילום מבוקר, הוא יעמוד בתקן ISO 19794-5. אין לעשות שימוש בתמונות "מטופלות" (ערוכות, מתוקנות וכיו"ב או מקטעי תמונות).

3.5. יש לשלב בקרה אנושית בקבלת ההחלטה הסופית לאחר ביצוע השוואה ממוכנת, וכן לוודא כי כוח האדם המשמש בתפקיד זה הוא בעל הכשרה מתאימה.

3.6. יש לשאוף למערכת אשר תמעט בהטיות (על רקע מגדר, גיל, מוצא אתני וכיו"ב) ככל הניתן, בין היתר, בדרכים הבאות:

3.6.1. לוודא כי מאגר האימון שעל בסיסו פותח מנוע ההשוואה הוא הטרוגני דיו ומכיל קבוצת אוכלוסייה באופן מייצג.

3.6.2. להעדיף מנוע השוואה מוכח אשר הציג ביצועים גבוהים באופן כללי, במבדקים בלתי תלויים.

3.6.3. לבצע ניתוח עיתי של התרעות השווא, כדי לבקר את ביצועי המנוע בהיבט זה ולשפר אותם.

3.7. יש לבצע עדכוני גרסאות/עדכוני מערכת ע"פ הגדרות הספק.

3.8. יש לקחת בחשבון שיעורי שגיאה גבוהים יותר בהתחשב בעטיית מסכת פנים בשל מגפת הקורונה, ולבחון את ביצועי המערכת בנסיבות אלה.

3.9. יש לבחון שימוש במנגנונים לגילוי זיופים ("מנגנוני חיות") בתרחישים מסוימים. בהקשר זה יש לקחת בחשבון פגיעה נוספת בפרטיות ויידוע הציבור למול צורך בטחוני.